A Blockchain-Based Architecture for Auditable and Privacy-Preserving Maintenance Ticketing in Hospital Environments

(Article begins on next page)

A Blockchain-Based Architecture for Auditable and Privacy-Preserving Maintenance Ticketing in Hospital Environments

***Abstract*—This paper introduces a blockchain-based platform, designed to speed-up the process of ticketing inside the hospital environment. The system combines two primary components: a web application, developed for tickets creation and management depending on the user's role, and a smart contract, devoted to the storage of data on-chain while preserving the data-privacy. The proposed solution aims at making more efficient and transparent the maintenance process, from users' segnalation to the actual maintenance intervention. The user-friendly interface together with an evaluation of the smart contract implementation with respect to the costs and to the trade-off between data-privacy and data-transparency demonstrate the potential of the system to make the whole ticketing process easier to manage and control.**

***Index Terms*—blockchain, smart contract, smart contract analysis, maintenance, ticketing**

I. Introduction

Blockchain technology has gained increasing attention as a foundational infrastructure for distributed systems requiring transparency, integrity, and auditability. By enabling tamper-resistant records and verifiable execution of operations, it is particularly suitable for multi-stakeholder environments characterized by strict accountability and traceability requirements, such as healthcare infrastructures [1], [2]. Despite its potential, the adoption of blockchain in real-world healthcare systems presents several challenges due to scalability limitations, transaction costs, and strict data privacy regulations, which limit the direct storage of sensitive information on-chain [13], [14], [16]. In parallel, healthcare organizations are increasingly facing the need to improve the efficiency and reliability of non-clinical operational processes, such as maintenance of medical devices and facilities which play a critical role in ensuring safety, continuity of care, and overall service quality [3], [4]. Traditional healthcare maintenance relies on centralized Computerized Maintenance Management Systems (CMMS), which implement structured ticket-based workflows supporting corrective, preventive, and condition-based strategies [7]. However, increasing system complexity and the availability of real-time data are driving a shift toward data-driven and predictive maintenance approaches enabled by IoT and Big Data technologies [18]. These approaches have been shown to reduce failures and improve service reliability, further supported by Digital Twin solutions integrating real-time data for advanced decision-making [5], [6], [17]. Hospital maintenance workflows are inherently complex due to the involvement of multiple stakeholders and dynamic, unplanned events under strict regulatory constraints. Managing fault reporting, task assignment, and intervention tracking requires coordination mechanisms capable of handling multi-actor and asynchronous processes beyond traditional static models [7]. This challenge is also recognized in blockchain-based healthcare studies, which highlight workflow orchestration and accountability as key issues [1]. Nevertheless, existing hospital ticketing and maintenance platforms are predominantly centralized, relying on mutable databases managed by a single authority. While they provide mature workflow support, they lack immutable audit trails and verifiable records, making post-hoc verification dependent on trust and limiting transparency [9]. Moreover, scientific literature explicitly addressing maintenance ticketing systems with built-in accountability mechanisms in healthcare remains limited, revealing a gap between operational requirements and current technological solutions. Another relevant aspect concerns user involvement in maintenance and reporting processes. User involvement remains limited, as healthcare information systems typically treat users as passive reporters with minimal visibility into request life-cycles [10]. Evidence from other domains shows that active user participation can improve situational awareness and decision-making [11]. Applying these principles to healthcare requires mechanisms that enhance transparency and engagement while complying with regulatory constraints. When appropriately designed, blockchain-based systems enable immutable logging of maintenance activities, supporting accountability and transparent auditing [1], [12]. However, healthcare data are highly sensitive and subject to strict regulatory constraints, requiring privacy-preserving solutions [13], [14], [16]. While cryptographic techniques can enhance data confidentiality, they often introduce computational and cost overheads, motivating the adoption of lightweight hybrid on-chain/off-chain architectures that preserve auditability while minimizing data exposure [15]. This paper proposes a blockchain-based platform for hospital maintenance ticketing, combining a role-based web application with a smart contract acting as an immutable audit layer. The system adopts a hybrid on-chain/off-chain architecture, where only hashes and essential metadata are stored on-chain while detailed data remain off-chain. This design ensures auditability and accountability while preserving privacy and limiting computational and financial costs.

The main contributions of this work are:

- a blockchain-based ticketing platform for hospital main-

tenance workflows;
- a hybrid on-chain/off-chain data management strategy ensuring privacy and auditability;
- the integration of role-based user interaction with immutable ticket life-cycle tracking;
- an evaluation of transaction costs and privacy-transparency trade-offs.

The remainder of the paper is organized as follows. Section II reviews related work, Section III presents the system architecture, Section IV reports the experimental evaluation, Section V and VI discuss the results, and conclude the paper.

II. Related Work

Healthcare maintenance management is a critical function for ensuring service continuity, patient safety, and operational efficiency. Traditional Computerized Maintenance Management Systems (CMMS), which implement structured ticket-based workflows for request submission, task assignment, and intervention tracking [7], provide mature operational support, but rely on centralized architectures, where data integrity and traceability depend on a single authority. As a result, maintenance records remain mutable and lack verifiable auditability.

Recent research has explored data-driven approaches to enhance maintenance processes, including predictive maintenance, IoT-based monitoring, and Digital Twin technologies [5], [6], [8], [17], [18]. These solutions improve efficiency and enable proactive interventions, but primarily focus on asset management and data analytics, without addressing accountability and transparency in multi-actor workflows. Blockchain technology has been proposed as a promising solution to enhance trust, transparency, and accountability in distributed systems. By enabling immutable and tamper-resistant records, blockchain can support verifiable tracking of maintenance operations and responsibility attribution without relying on centralized control [2], [12]. In healthcare contexts, blockchain-based approaches have been applied to asset maintenance and equipment management [1], demonstrating improved auditability. However, these solutions are generally asset-centric and do not explicitly address user-driven ticketing processes and workflow-level interactions. A key challenge in healthcare systems concerns the trade-off between transparency and data privacy. While blockchain enables immutable logging, direct on-chain storage of sensitive data is incompatible with privacy regulatory requirements [13], [14], [16]. Hybrid on-chain/off-chain architectures have therefore emerged as a common approach, where only hashes or minimal metadata are stored on-chain while detailed data remain off-chain [15]. However, existing works mainly focus on data protection and storage, with limited attention to how privacy-preserving mechanisms can be integrated into user-facing maintenance workflows. Overall, the literature highlights a gap at the intersection of healthcare maintenance management, user-driven ticketing systems, and blockchain-based accountability. To the best of our knowledge, no existing work jointly integrates active role-based user interaction [9], [10], immutable auditability, and privacy-preserving data management within hospital maintenance workflows. This gap motivates the decentralized architecture proposed in this paper.

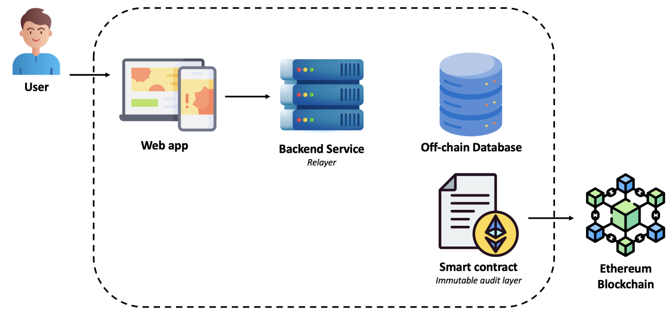

Fig. 1. System architecture

The comparison reported in Table I shows that existing solutions address healthcare maintenance, ticketing systems, user involvement, blockchain adoption, and data privacy as largely independent dimensions. While several works focus on maintenance optimization and predictive strategies, and others explore blockchain-based accountability or user-driven reporting models, none of the analyzed approaches jointly integrate these aspects within a unified healthcare ticketing framework. The proposed platform positions itself at the intersection of these research directions by combining role-based ticket management, reporting, auditability, and privacy-preserving data storage within a single decentralized architecture.

III. System Architecture

The proposed system adopts a hybrid architecture designed to support auditable and privacy-preserving maintenance ticketing in hospital environments. As illustrated in Fig. 1, the platform is structured according to a three-tier model comprising a web-based application layer, a backend service layer, and a blockchain-based audit layer. The web application provides role-based interfaces for healthcare staff, maintenance operators, and administrators, enabling fault reporting, ticket tracking, and workflow management without requiring direct interaction with blockchain technologies. The frontend is implemented using a web stack based on React and Next.js, with TypeScript for type safety and modular UI components to ensure usability, accessibility, and responsiveness across heterogeneous profiles and devices. The backend service implements the core business logic, access control policies, and workflow orchestration. It is developed using server-side JavaScript and TypeScript technologies and exposes RESTful APIs for frontend interaction. The backend manages off-chain data persistence through a relational database accessed via an ORM layer, and mediates all interactions with the blockchain through a controlled relayer component. This design enables validation, rate limiting, and policy enforcement before transactions are submitted on-chain. The blockchain layer hosts a smart contract implemented in Solidity and deployed on an Ethereum-compatible network. Rather than acting as a primary datastore, the blockchain serves as an immutable audit layer

TABLE I

COMPARISON OF RELATED WORKS ON HEALTHCARE MAINTENANCE, TICKETING, AND BLOCKCHAIN-BASED ACCOUNTABILITY

Work	Healthcare	Maintenance	Ticketing	User-Driven Reporting	Blockchain-Based	Privacy-Preserving
Yousefli *et al.* [7]	✓	✓	✓	–	–	–
Fotovatfard and Heravi [3]	✓	✓	–	–	–	–
Maktoubian and Ansari [8]	✓	✓	–	–	–	–
Manchadi *et al.* [6]	✓	✓	–	–	–	–
Ebiloma *et al.* [17]	✓	✓	–	–	–	–
Tran *et al.* [12]	–	✓	–	–	✓	–
Omar *et al.* [1]	✓	✓	–	–	✓	✓
Alyami [9]	✓	–	✓	✓	–	–
Schmittinger [10]	✓	–	–	✓	–	–
Cohen *et al.* [11]	–	–	✓	✓	–	–
This work	✓	✓	✓	✓	✓	✓

Checkmarks indicate explicit support or conceptual equivalence as discussed in the literature.

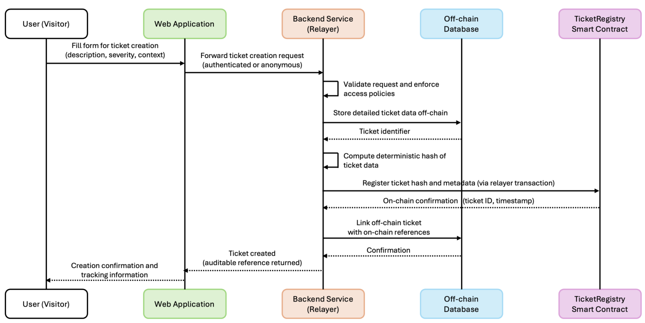

Fig. 2. End-to-end life-cycle of tickets creation

where only minimal, non-sensitive metadata and cryptographic hashes are recorded. Detailed operational data are maintained off-chain in a traditional database. This hybrid design balances performance, usability, and regulatory compliance, while ensuring verifiable integrity and traceability of maintenance processes.

A. End-to-End Ticket Life-cycle

Fig. 2 illustrates the end-to-end life-cycle of a maintenance ticket creation in the proposed platform. A ticket is first created by a user through the web application, where input data are validated and stored off-chain. The backend service then computes a deterministic hash of the canonical ticket representation and submits a corresponding transaction to the blockchain via the platform relayer. On-chain, the smart contract records the ticket creation event and initializes its life-cycle state. Subsequent actions, such as assignment and status updates, follow the same interaction pattern and are immutably logged as state transitions. Maintenance operators may update the ticket status directly, while detailed operational data remain off-chain. This workflow ensures auditability and traceability of maintenance processes while preserving user privacy and usability.

B. Smart Contract Design and On-Chain Logic

The core on-chain component of the platform is the *TicketRegistry* smart contract, which implements an immutable and auditable registry for maintenance tickets and tasks. The contract follows a permissioned-write model enforced through an ownership-based access policy, whereby all ticket and task creation operations are restricted to a platform-controlled relayer account operated by the backend service. The overall structure of the smart contract, including data models, inheritance relationships, and exposed interfaces, is summarized in the class diagram shown in Figure 3. Each ticket is identified by a unique identifier and associated with a cryptographic hash computed off-chain from a canonical representation of the ticket data. This approach enables integrity verification of off-chain information without exposing sensitive content on-chain. In addition to the hash, the contract stores a set of metadata, including severity level, department, life-cycle status, timestamps, and the address of the assigned maintenance operator, if any. Tickets and tasks are modeled as on-chain structures, while their life-cycle and assignment logic is encapsulated within the *TicketRegistry* contract. The ticket life-cycle is modeled through a set of states (*Open, InProgress, Resolved, Closed, Canceled*), enabling transparent tracking of maintenance progress over time. While ticket creation and assignment are restricted to the relayer, status updates can be performed by the relayer or by the maintenance operator. This design supports operational accountability while maintaining controlled access to information. All state changes emit dedicated on-chain events, allowing external observers to reconstruct the complete life-cycle of tickets and tasks in a tamper-resistant manner. By limiting on-chain storage to essential metadata and leveraging event-based logging, the smart contract acts as a lightweight audit layer with predictable transaction costs, while detailed data management remains off-chain.

C. User Interaction and Role-Based Platform Access

Users interact with the system exclusively through a web-based application implementing a role-based interaction model tailored to the heterogeneous stakeholders involved in hospital maintenance workflows. The platform supports user-driven fault reporting while abstracting all blockchain-related complexity from end users. As shown in Figure 4, healthcare staff, facility users, and visitors can submit maintenance requests through intuitive forms capturing fault descriptions, severity levels, and contextual information such as department, loca-

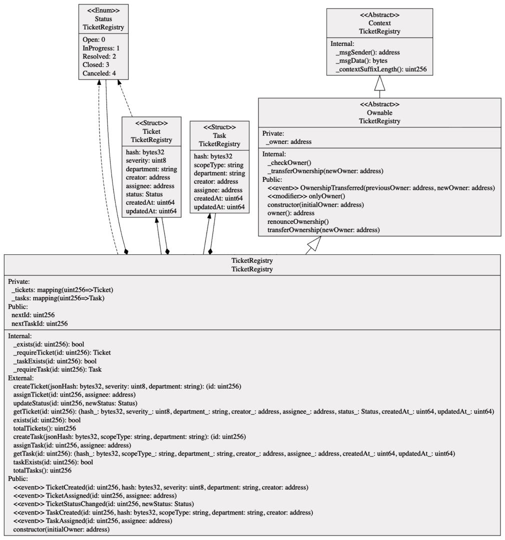

Fig. 3. UML Class Diagram

tion, or equipment identifiers, optionally supported by image uploads. Ticket creation can be performed by authenticated users as well as anonymously, lowering the barrier to reporting issues in critical environments. Once a new ticket has been created by a authenticated user, it is added to the user's ticket list, as shown in Figure 5, and to the list accessible by the administrator containing tickets created by all the users, as shown in Figure 6. In all cases, users are not required to manage blockchain accounts, cryptographic keys, or transaction fees, making the system suitable for deployment in clinical settings. Maintenance operators access dedicated dashboards displaying assigned tickets and tasks together with their life-cycle status, priority, and historical context. When authorized, operators can update the status of assigned tickets, enabling accountable recording of maintenance progress. These interactions are immutably logged on-chain through the backend relayer, without exposing sensitive operational data. Administrative users and facility managers are provided with aggregated views of maintenance activities across the organization. Through administrative dashboards, they can monitor ticket volumes, resolution timelines, and workflow performance, as well as create new maintenance tasks or assign a technician to a required maintenance intervention, as shown by the green button in Figure 7, thus acting as the coordination layer of the maintenance process. To support operational monitoring and decision-making, the platform integrates analytics functionalities accessible to administrative roles, including real-time status overviews, resolution-time analysis, detection of recurring issues by location or equipment, and workload indicators for maintenance personnel. Visual indicators highlight overdue tasks and high-severity tickets, enabling proactive intervention. Overall, the interaction model enforces a clear separation of concerns across roles while maintaining a unified user experience. Operational data and workflow logic are managed off-chain, whereas integrity guarantees, timestamps, and life-

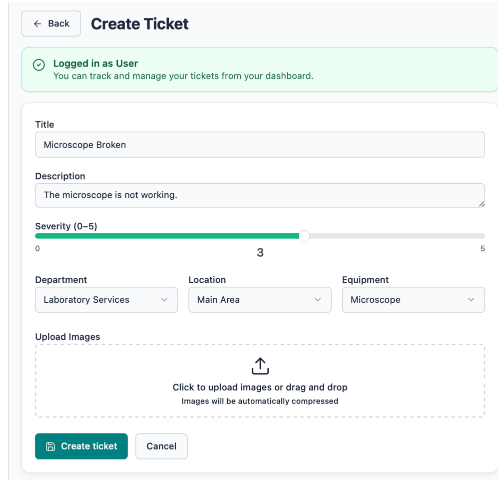

Fig. 4. Form to create a new ticket

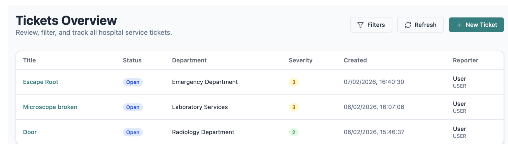

Fig. 5. List of tickets created by a user

cycle events are anchored on-chain, as shown in Figure 8, thus enabling user-centric ticketing workflows with verifiable accountability.

D. Privacy, Transparency, and Actor Unlinkability

A central design goal of the proposed architecture is to balance transparency and accountability with the strict privacy requirements of healthcare environments. While blockchain technology inherently enables immutable and transparent logging of events, user-to-blockchain interaction models may expose sensitive metadata and introduce unwanted linkability between users and operational activities.

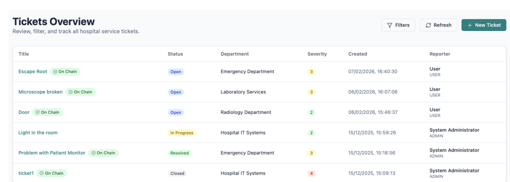

Fig. 6. Administrator's overview of all tickets created by the users

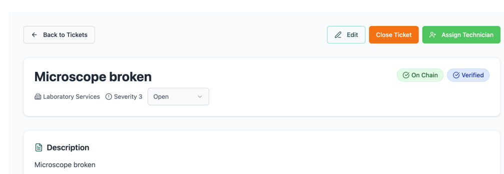

Fig. 7. Assigning a maintenance intervention to a technician

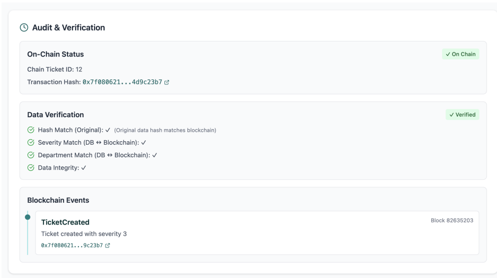

Fig. 8. Data stored at the blockchain level

To address this issue, the system adopts a relayer-based interaction model in which all blockchain transactions are submitted by a platform-controlled account. Ticket and task creation events are therefore always recorded on-chain under the same originating address, independently of the actual reporter. The identity of healthcare staff or facility users who submit maintenance requests is managed exclusively off-chain through the application's access control mechanisms.

This design provides actor unlinkability at the blockchain level: external observers cannot correlate on-chain activity patterns with individual users or departments. At the same time, transparency and auditability are preserved through immutable timestamps, life-cycle state transitions, and cryptographic hashes anchoring off-chain data to the blockchain.

From a data management perspective, the architecture enforces a clear separation between on-chain and off-chain information. As shown in Figure 8, only minimal, non-sensitive metadata, such as ticket hashes, severity levels, departments, status updates, and timestamps, are stored on-chain. Detailed descriptions, contextual information, personal data, and operational artifacts remain in off-chain databases. This approach supports data minimization, regulatory compliance, and system scalability, while enabling post-hoc verification of data integrity through hash comparison.

The relayer-based model introduces an explicit trust shift. While blockchain guarantees the immutability and integrity of recorded events, the backend relayer is responsible for faithfully materializing user actions on-chain and for enforcing access control policies. This assumption is consistent with typical hospital IT governance models, where backend systems are already trusted intermediaries. Importantly, blockchain-based audit trails mitigate this trust requirement by making any alteration or omission of recorded events detectable.

Overall, the proposed architecture decentralizes verification and accountability without requiring full decentralization of transaction submission. By combining data minimization, actor unlinkability, and immutable audit logs, the system achieves a pragmatic balance between privacy, usability, and transparency, aligned with the operational and regulatory constraints of healthcare maintenance workflows.

IV. Test and Results

The smart contract was tested using a local Ethereum-compatible environment based on Anvil, the development node provided by the Foundry framework. The evaluation focused on the execution of the core operations implemented by the *TicketRegistry* smart contract, covering the maintenance ticket life-cycle, including ticket creation, assignment, and status updates. All measurements were obtained from actual executions of the smart contract logic using Foundry's built-in gas reporting capabilities. Read-only functions were also evaluated to confirm that view operations do not incur any gas cost, as they do not modify blockchain state. Transaction costs were estimated based on measured gas consumption and current gas price data. Table II reports the gas consumption measured for the main operations implemented in the *TicketRegistry* smart contract. The results show that write operations exhibit low and predictable gas usage. In particular, ticket creation requires approximately 85,000 gas units, while ticket assignment and status updates consume approximately 45,000 and 35,000 gas units, respectively.

TABLE II
Gas cost analysis (gas price: 2.796 gwei, ETH: $2,500).

Operation	Gas Used	Cost (USD)
Contract Deployment	1,647,139	11.514
createTicket()	85,000	0.594
assignTicket()	45,000	0.315
updateStatus()	35,000	0.245
getTicket()	0	0.000
exists()	0	0.000
totalTickets()	0	0.000

The smart contract deployment cost amounts to approximately 1,647,139 gas units and represents a one-time initialization expense that does not scale with the number of tickets or users. All read-only operations are implemented as view functions and therefore incur no gas cost.

Costs were computed using measured gas consumption, a gas price of 2.796 gwei, and an ETH/USD rate of 2,500 USD. Under these assumptions, the cost of creating a ticket corresponds to approximately $0.60 USD, while ticket assignment and status update operations incur proportionally lower costs of approximately $0.32 USD and $0.25 USD, respectively (read-only operations do not incur any gas cost).

These results confirm that the blockchain-based audit trail can be maintained at a negligible per-ticket cost in the context of hospital maintenance workflows. The low gas consumption is primarily attributable to the minimal on-chain data model adopted by the proposed architecture. By storing only cryptographic hashes and essential metadata rather than complete ticket information, the smart contract avoids the high storage costs associated with more complex on-chain designs.

V. Discussion

The results highlight that the proposed architecture effectively balances transparency, privacy, and economic efficiency in blockchain-based healthcare maintenance workflows. By leveraging blockchain as an immutable audit layer rather than a primary data store, the system enables verifiable tracking of ticket life-cycle events while avoiding the exposure of sensitive information. This design choice addresses the lack of trusted auditability, one of the main limitations of existing centralized maintenance systems. Privacy requirements are satisfied through a hybrid on-chain/off-chain model combined with a relayer-based interaction mechanism, ensuring data minimization and preventing the linkability of user activities at the blockchain level. This approach aligns with regulatory constraints while maintaining system usability.

From an economic perspective, the measured gas consumption confirms that auditability can be achieved at negligible cost, making the solution viable for real-world deployment where frequent ticket operations are required.

VI. Conclusion

This paper presented a hybrid blockchain-based architecture for auditable and privacy-preserving maintenance ticketing in hospital environments. The proposed solution leverages blockchain technology as an immutable audit layer while keeping operational data and workflow logic off-chain, thereby balancing accountability, privacy, and economic feasibility.

The system integrates a role-based web platform, a backend relayer service, and a lightweight smart contract deployed on an Ethereum-compatible network. By adopting a permissioned-write model and a relayer-mediated interaction pattern, the platform ensures actor unlinkability at the blockchain level and prevents the exposure of sensitive metadata, while still enabling transparent and verifiable tracking of maintenance ticket life-cycles.

Experimental evaluation focused on the blockchain component demonstrated that the proposed design introduces minimal and predictable economic overhead. Gas cost measurements showed that all write operations required to manage ticket life-cycles incur low transaction costs, while read-only operations are gas-free. Even when evaluated under current Ethereum mainnet gas prices (2.796 gwei), the resulting per-ticket costs remain negligible ($0.59 for ticket creation), confirming the economic viability of the solution for real-world hospital maintenance workflows.

Overall, the results indicate that blockchain-based auditability can be effectively integrated into healthcare maintenance systems without compromising usability, privacy, or scalability. By decentralizing verification rather than transaction submission, and by combining minimal on-chain data with a user-centric reporting workflow, the proposed architecture provides a practical and compliant approach to enhancing transparency, accountability, and operational efficiency in regulated healthcare environments.

Future work will focus on extending the evaluation beyond economic analysis by incorporating performance and usability assessments in real hospital settings. Additional research directions include exploring alternative trust-reduction mechanisms, such as commit–reveal schemes or zero-knowledge proofs, to further reduce reliance on backend intermediaries, and investigating deployment on alternative Ethereum Virtual Machine compatible networks to assess cost and scalability trade-offs. The modular design of the platform supports these extensions without requiring fundamental architectural changes.

Acknowledgment

The contribution made by [......], who carried out the implementation, is gratefully acknowledged.

References

[1] I. A. Omar, H. R. Hasan, W. AlKhader, R. Jayaraman, K. Salah, and M. Omar, "Blockchain-based trusted accountability in the maintenance of medical imaging equipment," *Expert Systems with Applications*, vol. 241, p. 122718, 2024.

[2] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[3] A. Fotovatfard and G. Heravi, "Identifying key performance indicators for healthcare facilities maintenance," *Journal of Building Engineering*, vol. 42, p. 102838, 2021.

[4] M. Dolcini *et al.*, "Facility management costs for hospital infrastructures," *Healthcare*, vol. 13, no. 8, p. 924, 2025.

[5] D. Andrițoi, C. Luca, C. Corciovă, and R. Ciorap, "Predictive maintenance application for health technology management," in *Proc. 8th Int. Symp. Advanced Topics in Electrical Engineering (ATEE)*, May 2013, pp. 1–4.

[6] F.-E. Manchadi, F. Ben-Bouazza, and B. Jioudi, "Predictive maintenance in healthcare system: A survey," *IEEE Access*, vol. 11, pp. 61313–61330, 2023.

[7] Z. Yousefli, F. Nasiri, and O. Moselhi, "Healthcare facilities maintenance management: A literature review," *Journal of Facilities Management*, vol. 15, no. 4, pp. 352–375, 2017.

[8] J. Maktoubian and K. Ansari, "An IoT architecture for preventive maintenance of medical devices in healthcare organizations," *Health and Technology*, vol. 9, pp. 233–243, 2019.

[9] A. A. Alyami, "Smart e-health system for real-time tracking and monitoring of patients, staff and assets for healthcare decision support in Saudi Arabia," Ph.D. dissertation, Staffordshire Univ., Stafford, U.K., 2018.

[10] F. Schmittinger, "Adapting design tools to incentivize the development of design capability in healthcare: A case study," Ph.D. dissertation, 2017.

[11] M. C. Cohen, M.-D. Fiszer, A. Ratzon, and R. Sasson, "Incentivizing commuters to carpool: A large field experiment with Waze," *Manufacturing & Service Operations Management*, vol. 25, no. 4, pp. 1263–1284, 2023.

[12] V. H. Tran, B. Lenssens, A. Kassab, *et al.*, "Machine-as-a-service: Blockchain-based management and maintenance of industrial appliances," *Engineering Reports*, vol. 5, no. 7, p. e12567, 2023.

[13] A. G. de Moraes Rossetto, C. Sega, and V. R. Q. Leithardt, "An architecture for managing data privacy in healthcare with blockchain," *Sensors*, vol. 22, no. 21, 2022.

[14] N. Yadav, S. Pandey, A. Gupta, P. Dudani, S. Gupta, and K. Rangarajan, "Data privacy in healthcare: In the era of artificial intelligence," *Indian Dermatology Online Journal*, vol. 14, no. 6, pp. 788–792, 2023.

[15] K. Salah, M. H. U. Rehman, N. Nizamuddin, and R. Jayaraman, "Privacy and security of blockchain in healthcare," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 574–602, 2021.

[16] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Procedia Computer Science*, vol. 113, pp. 73–80, 2017.

[17] D. O. Ebiloma, C. O. Aigbavboa, and C. J. Anumba, "Key drivers of digital twin maintenance management for healthcare facilities in Nigeria," *Engineering, Construction and Architectural Management*, early access, 2025.

[18] N. Arunraj and J. Maiti, "Risk-based maintenance—techniques and applications," *Journal of Hazardous Materials*, vol. 142, no. 3, pp. 653–661, 2007.