Integrating Blockchain and Smart Card Technologies for Secure Healthcare Data Management

Zayneb Gaouzi, Imad Bourian, Khalid Chougdali
Engineering Sciences Laboratory-National School of Applied Sciences, Ibn Tofail University, Kénitra, Morocco

***Abstract*—In recent years, the healthcare sector has faced growing challenges in managing patient data securely and efficiently, especially when it comes to data privacy and the way information is shared across healthcare providers. A number of digital solutions have been proposed over time, but more recently, blockchain has started to gain serious interest. Its structure allows data to remain intact and traceable, while also offering a strong layer of security. This paper explores how blockchain based smart contract might be used alongside smart cards to offer a more robust system for protecting patient information. Smart cards bring in a physical barrier that helps limit access to only those who are authorized, while blockchain makes it much harder to tamper with information or centralize control. The suggested method demonstrates how the decentralized and immutable nature of blockchain, combined with the physical authentication provided by smart cards and the automation of smart contracts improve data security and restrict unauthorized access. The proposed framework is evaluated through smart contract deployment and testing on both the Hardhat local network and the Celo public testnet. The results confirm the practicality and efficiency of the solution and support its potential for real world application in secure healthcare data management.**

***Keywords*—Healthcare; security; blockchain; smart contracts**

I. Introduction

Healthcare systems are transforming at a breakneck pace with the widespread use of advanced digital technologies. From AI and cloud solutions to IoT devices, these new technologies are transforming the way care is delivered as well as patient data managed [1]. While they make the care more personalized and effective, they also raise very significant cybersecurity challenges, particularly concerning the protection of patient data and healthcare operations [2]. With increasing digital infrastructures and connectivity, so too does the risk of unauthorized access, cyberattacks, and data breaches that undermine the privacy and integrity of health records [3] [4].

The key problem is the lack of a tamper-proof and privacy-preserving infrastructure that can enable safe access and data exchange of healthcare systems across various entities. Most of existing solutions tend to depend on centralized authorities, which introduces single points of failure and often fails to guarantee transparency and data integrity. Moreover, smart cards have today become a widely adopted hardware device utilized to help in the mitigation of some of the foregoing issues, with a simple means of storing and managing sensitive medical information in a secure portable format [5][6]. They are used for identity or access validation purposes, allowing only access to covered data by certified individuals [7]. Smart card systems offer several advantages, but they are not without limitations. Issues like poor compatibility between different systems and occasional security breaches still persist, and in many cases, these issues have become more noticeable as healthcare technology gets more complex [8] [9] [10]. One of the more promising ways to strengthen healthcare data management systems is with the introduction of blockchain technology. Its decentralized, tamper-proof character renders blockchain a very trusted guarantor of system performance, data integrity, and privacy across diverse industries [11] [12]. Blockchain allows sensitive information to be shared in a more controlled and transparent manner, while reducing reliance on centralized databases that are more susceptible to be cyberattacked [13]. Particularly, blockchain based smart contract frameworks offer the potential for automated access controls and dynamic identity management within the scenario of no third-party intermediaries [14]. These automated controls can impose sophisticated data-sharing policies and provide inherent auditability, two critical characteristics for distributed health trust and compliance. This paper proposes a secure healthcare data management system based on the integration of smart cards and blockchain technologies. It explores how blockchain can make smart card–based systems more resilient, transparent, and privacy-preserving. Rather than focusing on a particular implementation, the study contrasts different design options, technical considerations, and performance implications to evaluate how this combined approach can offer a safer and better system for managing patient data in today's health industry.

The main contributions of this work are as follows:

- To propose a novel healthcare data management framework that integrates blockchain and smart card to ensure secure and decentralized access to patient records.
- To design and implement a set of smart contracts that automate rule based access control and data management processes among healthcare stakeholders.
- To evaluate the system through deployment on both a local Hardhat network and the Celo public testnet.
- To compare our model with existing blockchain-based healthcare solutions and demonstrate its advantages in terms of completeness and security.

The remaining sections of this paper follow this structure: Section II provides a concise background information of related works. Our proposed approach is presented in Section III. Section IV sheds light on simulation setup and results discussion. Lastly, Section V concludes the study and outlines directions for future work.

II. Related Work

This section presents a review of recent and significant contributions in the literature concerning the application of blockchain technology to enhance the security of healthcare systems. In [15], the authors propose a scalable blockchain architecture that incorporates Zero Knowledge Proof (ZKP) mechanisms to ensure data integrity, coupled with the InterPlanetary File System (IPFS) for efficient off-chain storage. The authenticated data is subsequently utilized within a deep learning framework for intrusion detection in healthcare networks. In [16], the authors develop a secure blockchain-based application that functions as a communication interface between IoT devices, the blockchain infrastructure and stakeholders such as hospitals, patients, healthcare professionals. The solution enforces essential security properties such as confidentiality, authentication, and access control through the use of smart contracts. In [17], the authors present FL-BETS, a framework that combines federated learning with blockchain to support task scheduling in healthcare contexts. The system is designed to work under both strict and flexible constraints, using dynamic heuristics to adapt to the needs of each scenario. Its primary goals include safeguarding patient privacy, reducing the risk of fraud, and improving system performance—particularly in terms of energy consumption and response time. The authors of [18] propose MedShare, a decentralized framework for the secure sharing of Electronic Health Records (EHRs) through blockchain-based smart contracts. To support fine-grained access control, a constant-size Attribute-Based Encryption (ABE) scheme is integrated, embedding access policies directly into blockchain-stored search results. Additionally, a multi-keyword boolean search mechanism is implemented to improve usability for authorized users. In [19], the focus shifts to protecting IoT-based healthcare systems from cyber threats. The authors design a security architecture for healthcare multimedia data, utilizing cryptographic hashes to ensure data integrity. Unauthorized alterations are detectable and traceable across the blockchain network, thus enhancing both system performance and cost efficiency in patient care. The author in [20] presents a novel approach to privacy preservation for EHRs by combining blockchain technology with deep learning. A convolutional neural network (CNN) is used to detect and block abnormal user activity, integrated within a federated learning module operating atop the blockchain to ensure distributed, secure access control. Lastly, [21] proposes a lightweight, fog enabled blockchain architecture for remote patient monitoring. The system exhibits high security and responsiveness, with simulation results indicating that fog computing integration improves system responsiveness by up to 40%, while simultaneously strengthening defenses against potential security breaches.

As previously mentioned, a great deal of effort has been explored in integrating blockchain technology to enhance security in healthcare systems. However, critical gap remains unaddressed and security challenges need to be explored. Most prior works fail to incorporate a physical security layer, such as smart cards, to mitigate unauthorized access at the user level. Similarly, many smart card based systems lack a robust backend capable of ensuring data traceability and integrity. As a result, there is a disconnect between physical level access control and backend data management in many proposed models. To bridge this gap, it is essential to design a combined architecture where blockchain ensures data security, integrity, and transparency, while smart cards act as a front end authentication tool. Unlike previous work, our framework emphasizes a dual approach that contributes to the development of a more secure and efficient healthcare information system that is resilient to both external cyber threats and internal misuse.

III. Proposed Approach

A. Architecture System

In this section, we present the proposed architecture of our solution that focuses mainly on enhancing security in smart card-based healthcare management systems by integrating blockchain technology. In fact, our contribution consists of creating a model as depicted in Fig. 1 that uses blockchain technology to securely manage patient health records while ensuring seamless interaction among key stakeholders, including the patient's smart card, hospital entities, pharmacies and insurance providers. The system is organized around four main layers, each focusing on a different aspect of how healthcare data is handled. Together, they support secure access, reliable data exchange, and stakeholder coordination—without depending on a central authority.

1) Stakeholders layer: This layer includes all participants involved in accessing or updating patient health records. To identify themselves, patients use a smart card that acts as their personal key to the system. Access for others, such as healthcare providers or insurers, is based on defined roles. The stakeholders include:

a) Hospitals: interact with the system to consult and update medical information, and to exchange data with doctors, labs, or administrative staff when needed.

b) Pharmacies: confirm prescriptions through the platform and dispense medications accordingly. The goal here is to reduce risk from manual errors or unauthorized changes.

c) Insurance providers: access patient histories to assess claims. Since the data is immutably stored, the process becomes more trustworthy and less prone to manipulation.

2) Interface layer: Users interact with the system through a dedicated app. Behind the scenes, the interface applies access rules based on each user's role. For the user, the process feels straightforward; they don't see the underlying blockchain operations. This layer is designed to simplify access while maintaining security.

3) Smart contracts layer: Here, the rules of the system are enforced automatically. Any time a user tries to update a file, verify a prescription, or submit a claim, a smart contract checks the conditions. If they match, the action is approved. This helps prevent mistakes and keeps a record of what happened.

4) Blockchain ledger layer: At the core is the blockchain itself. It keeps a permanent log of every interaction with the system—whether it's viewing, editing, or transferring information. Because this ledger can't be altered after the fact, it offers a reliable audit trail. And since no single server controls it all, the system is more resilient by design.

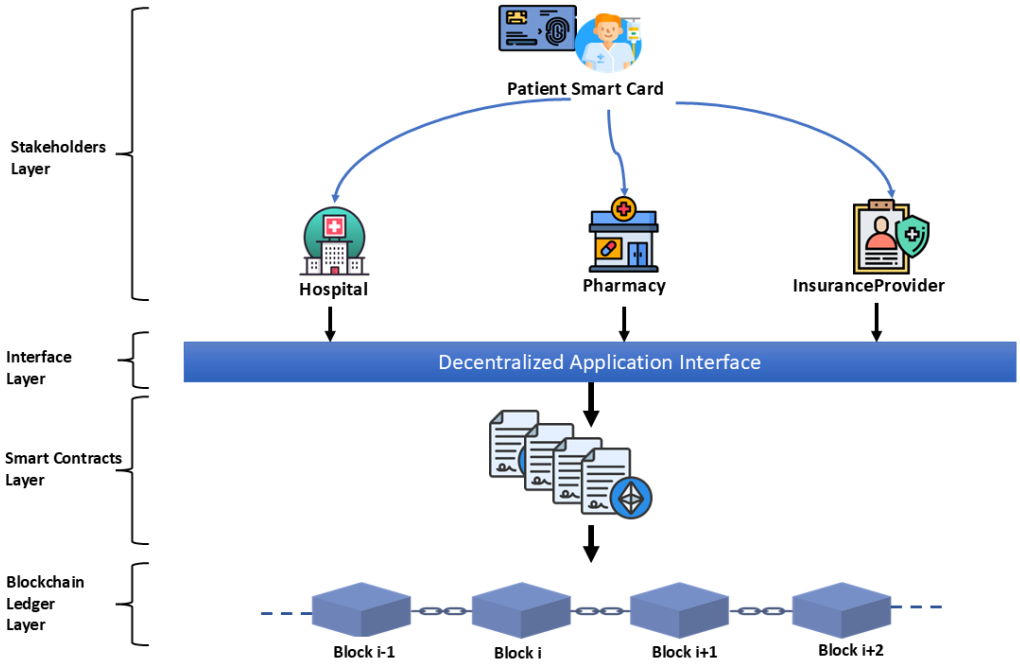

Fig. 1. Overview of the proposed architecture.

B. Worflow Diagram

To process the logic and statements that defines conditions and interactions between all stakeholders applied in our system, we propose the workflow diagram presented in Fig. 2.

1) Patient check-in and identity verification: When a patient arrives at the hospital, they authenticate themselves using their smart card. The hospital system, through the Decentralized Application Interface (DApp), verifies the patient's identity on the blockchain. Once authenticated, the hospital gains role-based access to the patient's medical history.

2) Consultation with a doctor: The doctor accesses the patient's medical records stored on the blockchain to review past diagnoses, treatments, allergies, and medications. The patient and doctor discuss symptoms, and the doctor records a new diagnosis along with the recommended treatment plan. The diagnosis and treatment plan are securely written to the blockchain and linked to the patient's record.

3) Prescription and pharmacy interaction: If medication is required, the doctor issues a blockchain-based prescription. The patient presents their smart card at an authorized pharmacy, which verifies the prescription on-chain. Upon dispensing the medication, the pharmacy updates the blockchain, marking the prescription as "fulfilled" to prevent misuse.

4) Insurance claim processing: If the patient has medical insurance, the hospital submits a blockchain-verified claim to the Insurance Provider. The insurance provider accesses the patient's treatment record and approves or denies the claim based on coverage rules. Once approved, the hospital receives direct payment from the insurance provider via a smart contract transaction.

To implement the logic of this proposed architecture, we suggest to create and deploy the following four smart contracts: PatientSmartCard, HospitalRecord, PharmacyAccess and InsuranceProvider. Table I presents an overview of the objective of each contract.

TABLE I. SMART CONTRACTS AND THEIR OBJECTIVES

Smart Contracts	Objective
`PatientSmartCard.sol`	Manages patient identity, authentication, and authorization using a smart card.
`HospitalRecord.sol`	Allows hospitals to update, store, and retrieve patient medical records securely.
`PharmacyAccess.sol`	Allows pharmacies to verify prescriptions and dispense medications securely.
`InsuranceProvider.sol`	Manages insurance claims, approvals, and payment processing for medical services.

IV. SIMULATION AND RESULTS DISCUSSION

In this section, we present the simulation scenarios for our proposed model. To do so, we use different technologies listed in Table II.

The analysis of deployed smart contracts on the Hardhat local network, as depicted in Fig. 3 and 4, reveals varying costs in ETH, reflecting differences in contract complexity, functionalities and storage requirements. The InsuranceProvider contract has the highest deployment cost, likely due to extensive data management and computational logic, followed by HospitalRecord, which also involves significant processing. The PatientSmartCard contract incurs a moderate cost, managing identity interactions, while PharmacyAccess has the lowest cost, suggesting a simpler structure.

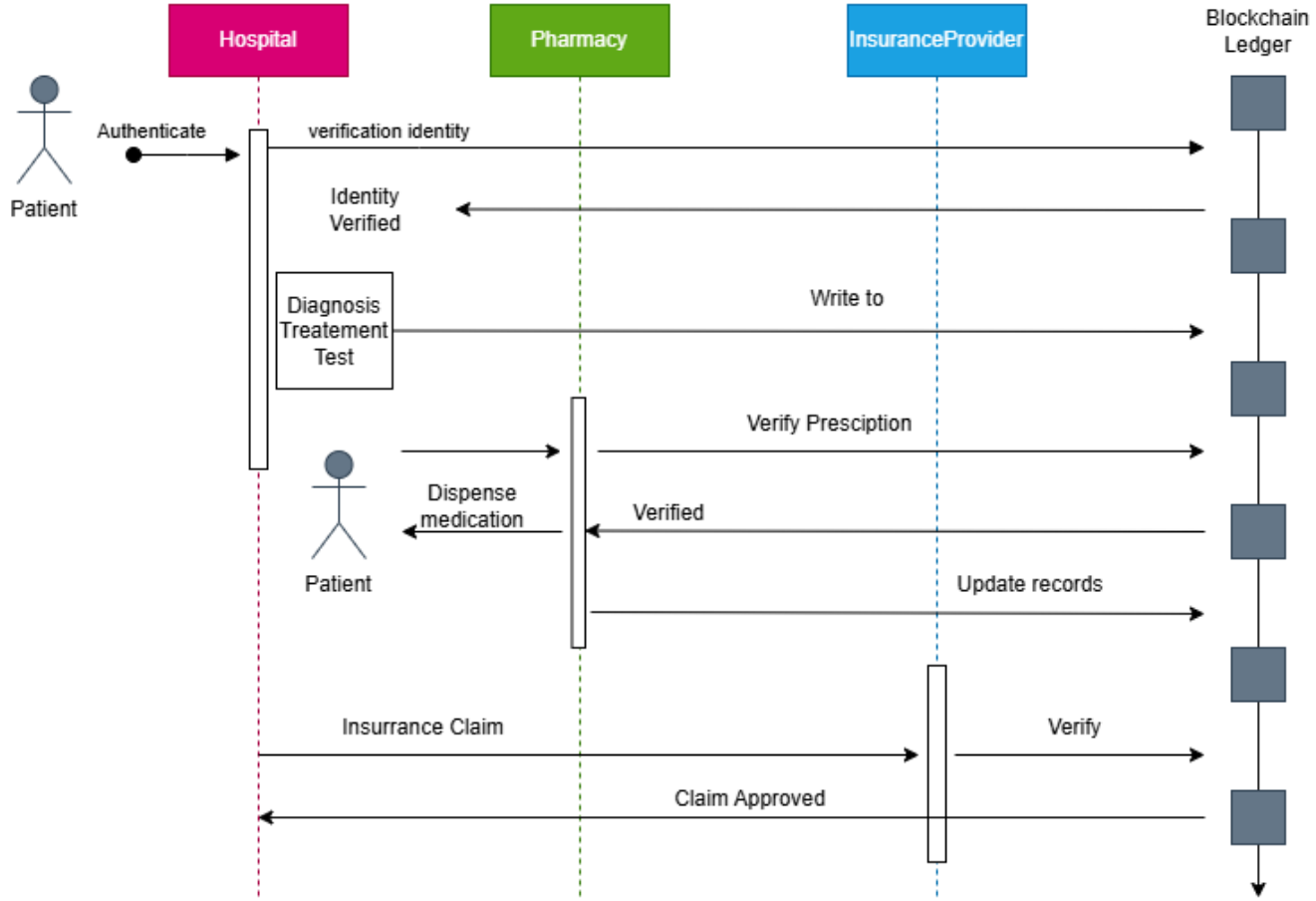

Fig. 2. System workflow diagram.

TABLE II. OVERVIEW OF TECHNOLOGIES USED

Technology	Description
Hardhat	is an Ethereum development environment for professionals. It facilitates performing frequent tasks, such as running tests, automatically checking code for mistakes, or interacting with a smart contract.
Solidity	is a programming language for implementing smart contracts on various blockchain platforms, most notably Ethereum.
Ethers.js	is a JavaScript library and toolkit that provides a convenient and reliable interface with the Ethereum Blockchain for developers.
JSON RPC	serves as a protocol for communication between a client and a server. It is widely used in various applications, including web development, notably in blockchain networks.
Environment	Computer CPU: i7; RAM: 8GB.

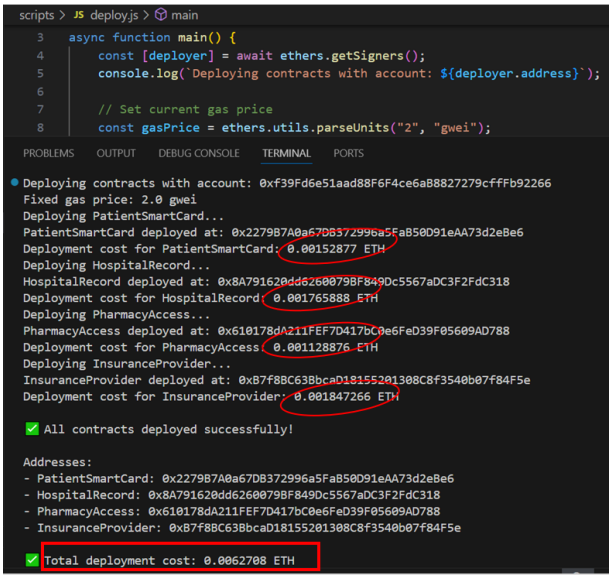

Fig. 3. Smart contracts deployment.

This can be explained by the fact that gas usage varies according to transaction complexity. It depends on the smart contract function being executed. More complex operations (e.g. loops, storage writes) consume more gas. Simpler operations (e.g. pure/view functions) consume less gas. However, the gas price can be fixed. It stands for the amount of wei per unit of gas that you are willing to pay. For significant results, we fixed the gas price in Hardhat's local network, in

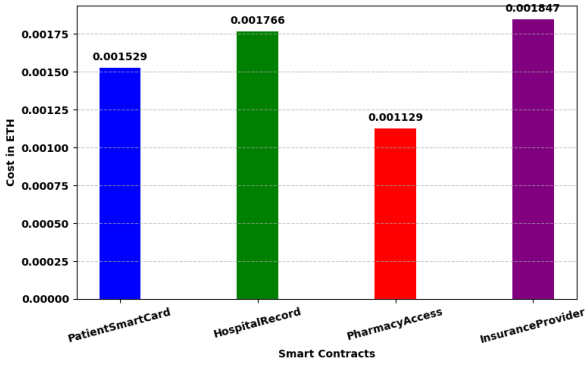

Fig. 4. Cost of deployed Smart contracts.

the hardhat.config.js file by defining a specific gas price for the local network at 2 Gwei = 2000000000 wei, as depicted in Fig. 5.

```
JS hardhat.config.js > ...
4   module.exports = {
5     solidity: {
6       version: "0.8.0",
7       settings: {
8         optimizer: {
9           enabled: true,
10          runs: 200,
11        },
12      },
13    },
14    networks: {
15      hardhat: {},
16      localhost: {
17        url: "http://127.0.0.1:8545",
18        gasPrice: 2000000000,
19      },
```

Fig. 5. GasPrice fixed in hardhat.config.js file.

Further analysis was conducted to compare the execution costs in ETH across different smart contract functions, as listed in Table III, exploring the interactions between stakeholders and the system. The results, as shown in Fig. 6, illustrate the relationship between gas usage and cost (ETH) for various smart contract functions deployed on the local blockchain network. The plot includes two main data points for each function: "Gas Used", which represents the computational resources required to execute each smart contract function. Since gas consumption directly affects transaction fees, it plays a crucial role in system efficiency. The second data point, "Cost (ETH)", is derived from the amount of gas used, converted to ETH based on gas price. It reflects the price that users or operators would pay to execute a given function on the Ethereum network. We notice that functions such as addMedicalRecord and registerPatient require significantly higher gas (187,731 and 119,237 gas units, respectively). This suggests that these functions involve complex computations, storage operations, or multiple interactions with the blockchain state, leading to increased gas costs. In contrast, functions such as getPatientInfo and registerPharmacy consume significantly less gas, requiring 34,491 and 25,152 gas units, respectively. These functions likely involve simple retrieval operations rather than modifying blockchain data, resulting in lower execution costs.

TABLE III. GAS USAGE PER FUNCTION IN SMART CONTRACTS

Function	Gas Used	Smart Contract
registerPatient	119237	PatientSmartCard
getPatientInfo	34491	
updateMedicalHistory	97050	
registerHospital	94419	HospitalRecord
addMedicalRecord	187731	
getMedicalRecords	40354	
registerPharmacy	25152	PharmacyAccess
getPatientFullInfo	42354	
approveClaim	98045	InsuranceProvider
processPayment	151058	
getClaimStatus	44219	

This analysis highlights the trade-offs between gas usage and cost for smart contract functions and shows that this cost primarily depends on the complexity of the function's logic: functions that modify blockchain data (e.g. storing medical records or registering new entities) require higher gas fees. On the other hand, functions that retrieve data (view functions) consume significantly less gas, as they do not require writing to the blockchain state.

A. Deployment of Smart Contracts on the Celo Testnet

Moreover, we deployed our smart contracts on the Celo testnet (Alfajores), ensuring a decentralized and transparent environment for managing patient records. The system interacts with the blockchain through the MetaMask wallet, enabling seamless and secure authentication for users, as illustrated in Fig. 7.

The execution of transactions on the Celo testnet blockchain ensures transparency and traceability, as depicted in Fig. 8. Each transaction, whether it involves registering a patient, updating medical history, or granting access to stakeholders, is permanently recorded on the blockchain ledger, making it immutable and auditable. This mechanism prevents unauthorized modifications and enhances trust among all participants in the healthcare ecosystem.

By leveraging Celo's blockchain infrastructure, our system guarantees:

- Tamper-proof data storage: Once recorded, patient data cannot be altered or deleted.
- Decentralized access control: Only authorized stakeholders (e.g. hospitals, pharmacies, insurance providers) can interact with patient records.
- Security and fraud prevention: The transparency of blockchain transactions minimizes the risk of data manipulation and fraudulent activities. This approach reinforces the reliability and security of patient record management, establishing a trustworthy framework for healthcare services based on blockchain technology.

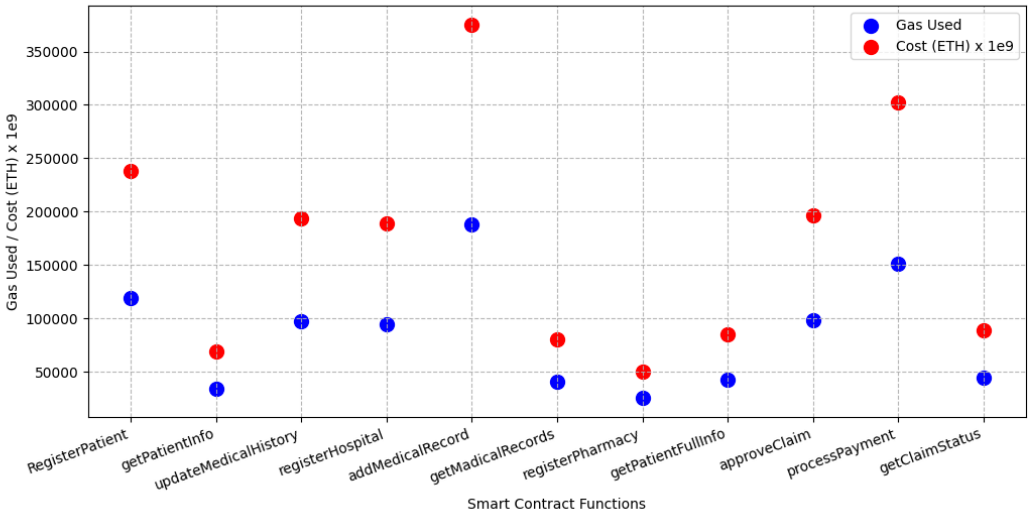

Fig. 6. Cost for smart contract functions vs Gas used.

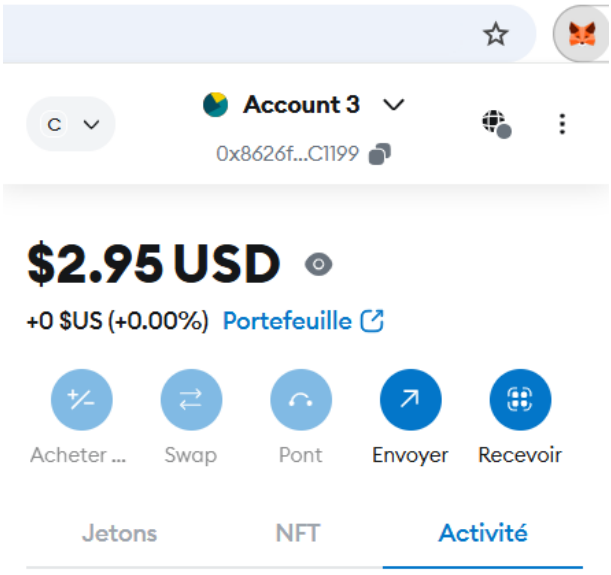

Fig. 7. Metamask account connected to celo.

This framework is fully adaptable for deployment on the mainnet, allowing real-world integration into national healthcare systems or private medical networks. The transition from the testnet to the mainnet would involve optimizing gas fees to ensure cost-efficient transactions. By deploying the system on the mainnet, patient record management could become globally accessible and fully secure, revolutionizing how medical data is stored and shared in a blockchain-powered healthcare ecosystem.

B. Comparison with Other Related Works

In this chapter, we compare our research with some relevant studies in the field of blockchain-based healthcare systems. Table IV highlights the integration of blockchain, the use of smart contracts, the application of smart cards, and the level of experimentation in each approach. We observe that our work integrates all the key components: blockchain, smart contracts, and smart cards, making it the most comprehensive solution compared to the others. Furthermore, we include detailed experimentation to validate the performance and feasibility of the proposed system, ensuring both theoretical and practical robustness. This comparison underscores the novelty and completeness of our approach, combining secure data management through blockchain, automated contract execution via smart contracts, and real-time patient data access with smart cards, backed by empirical experimentation.

TABLE IV. COMPARISON WITH OTHER WORKS

Ref	Blockchain integrated	Smart contract enabled	Smart card	Experimentation
[22]	✓	×	×	✓
[23]	✓	✓	×	✓
[24], [25]	✓	✓	×	×
Our work	✓	✓	✓	✓

V. CONCLUSION

Finally, blockchain technology has the potential to transform the health sector, particularly when dealing with patient information. Through ensuring a safe and transparent means of storing and sharing medical records, blockchain can enhance the privacy and the security of data, boost efficiency, and facilitate better cooperation between healthcare professionals. In addition, integrating smart card technology with

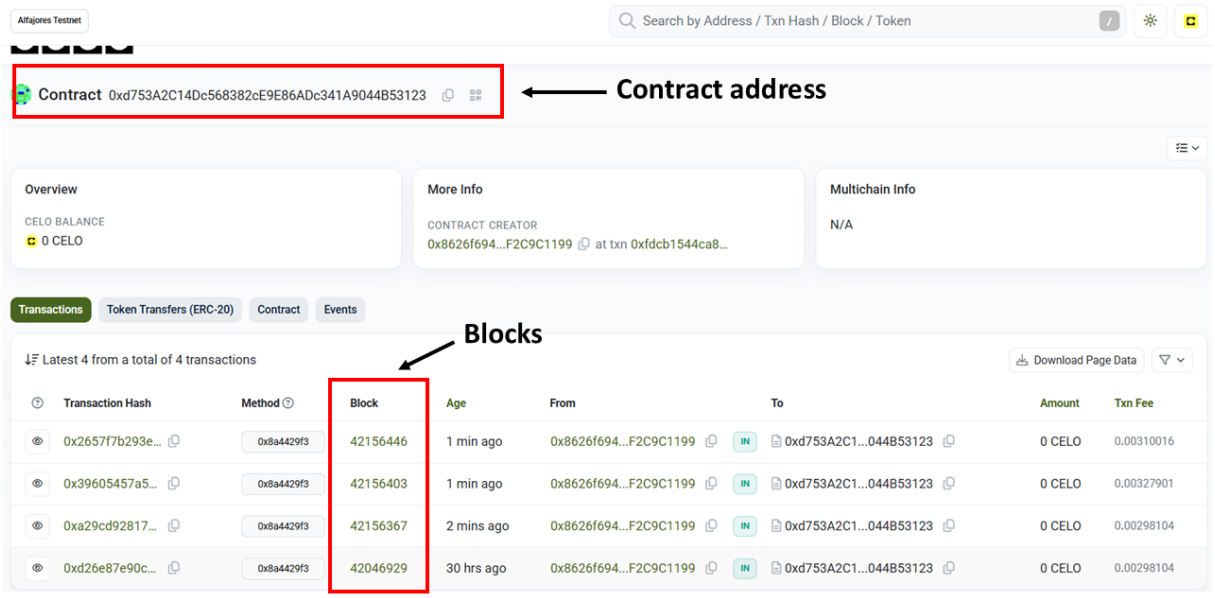

Fig. 8. Transactions in the celo tesnet.

a blockchain-based healthcare management system can also boost the security and the privacy of patient information. Smart cards provide a physical level of security used to safeguard patient information and block unauthorized access, whereas blockchain technology has the capability to ensure data is safely stored and transparently shared. Although there are still barriers to be overcome, for example, regulatory compliance and data interoperability with current healthcare systems, the prospects of a blockchain-enabled health management system with the application of smart cards are promising. With the best of blockchain and smart card technologies combined, healthcare providers are able to enhance patient outcomes and provide more effective and efficient care. As such, additional research and development in this field are necessary to achieve the full potential of blockchain in healthcare.

Our future work will focus on exploring a large-scale deployment scenarios, integrating the current system with IoT medical devices, and exploring other framework like Zero-Knowledge Proofs technique to reinforce the system's privacy. In addition, our study will work with healthcare organizations to create and evaluate a working prototype of the suggested system. This include analyzing system performance using real-time data, reviewing patient and provider user experiences, and making that ethical standards are being followed.

REFERENCES

[1] R. Sinha, "The role and impact of new technologies on healthcare systems," *Discover Health Systems*, vol. 3, no. 1, p. 96, Nov. 2024.

[2] F. ALmojel and S. Mishra, "Advancing Hospital Cybersecurity Through IoT-Enabled Neural Network for Human Behavior Analysis and Anomaly Detection," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 5, pp. 49–57, 2024.

[3] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," *Cyber Security and Applications*, vol. 1, p. 100016, Dec. 2023.

[4] K. S. Bhosale, M. Nenova, and G. Iliev, "A study of cyber attacks: In the healthcare sector," in *2021 Sixth Junior Conference on Lighting (Lighting)*, Sep. 2021, pp. 1–6.

[5] K. B, M. A, K. H, and R. J, "E-Smart Health Card System," in *2024 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)*, Oct. 2024, pp. 1–6.

[6] I. Srivastava, A. Raj, and D. S. Gupta, "Blockchain-based Secure Storage and Management of Electronic Health Record using a Smart Card," in *2023 5th International Conference on Recent Advances in Information Technology (RAIT)*, Mar. 2023, pp. 1–6.

[7] M. A. Khan, H. Alhakami, W. Alhakami, A. V. Shvetsov, and I. Ullah, "A Smart Card-Based Two-Factor Mutual Authentication Scheme for Efficient Deployment of an IoT-Based Telecare Medical Information System," *Sensors*, vol. 23, no. 12, p. 5419, Jan. 2023, number: 12 Publisher: Multidisciplinary Digital Publishing Institute.

[8] R. Drake and E. Ridder, "Healthcare Cybersecurity Vulnerabilities," *International Conference on Cybersecurity and Cybercrime*, vol. 9, pp. 49–56, Apr. 2022.

[9] N. El Madhoun and B. Hammi, *Blockchain Technology in the Healthcare Sector: Overview and Security Analysis*, Jan. 2024.

[10] C. M. Mejía-Granda, J. L. Fernández-Alemán, J. M. Carrillo-de Gea, and J. A. García-Berná, "Security vulnerabilities in healthcare: an analysis of medical devices and software," *Medical & Biological Engineering & Computing*, vol. 62, no. 1, pp. 257–273, Jan. 2024.

[11] Y. Bentayeb, K. Chaoui, and H. Badir, "Integrating Blockchain and Edge Computing: A Systematic Analysis of Security, Efficiency, and Scalability," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1, pp. 622–632, 2025.

[12] A. Osilaja, A. Raheem, and E. Edmund, "Enhancing software security with blockchain integration for decentralized and tamper-proof application architectures," *World Journal of Advanced Research and Reviews*, vol. 24, pp. 2750–2767, Dec. 2024.

[13] C. E. Filali, I. Bourian, and K. Chougdali, "Privacy-Preserving And Access Control Scheme For IoT-Based Healthcare Systems Using Ethereum Blockchain," in *2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet)*, Dec. 2024, pp. 1–6, iSSN: 2771-7402.

[14] I. BOURIAN, A. SEBBAR, K. CHOUGDALI, and E. M. Amhoud, "SSHCEth: Secure Smart Home Communications based on Ethereum Blockchain and Smart Contract," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, Dec. 2023, pp. 2674–2679, iSSN: 2576-6813.

[15] P. Kumar, R. Kumar, G. Gupta, R. Tripathi, A. Jolfaei, and A. Najmul Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *Journal of Parallel and Distributed Computing*, vol. 172, pp. 69–83, 2023.

[16] P. Sharma, S. Namasudra, R. Gonzalez Crespo, J. Parra-Fuente, and M. Chandra Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Information Sciences*, vol. 629, pp. 703–718, 2023.

[17] A. Lakhan, M. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, and W. Wang, "Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 664–672, 2023.

[18] M. Wang, Y. Guo, C. Zhang, C. Wang, H. Huang, and X. Jia, "MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain," *IEEE Transactions on Services Computing*, vol. 16, no. 1, pp. 438–451, 2023.

[19] A. Taloba, A. Elhadad, A. Rayan, R. Abd El-Aziz, M. Salem, A. Alzahrani, F. Alharithi, and C. Park, "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare," *Alexandria Engineering Journal*, vol. 65, pp. 263–274, 2023.

[20] J. Alzubi, O. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1080–1087, 2023.

[21] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. Moosavi, "A lightweight blockchain and fog-enabled secure remote patient monitoring system," *Internet of Things (Netherlands)*, vol. 22, 2023.

[22] L. S. Anderson and U. J, "MedSecure: Blockchain-enhanced patient data security with asymmetric cryptography and MFA," *World Journal of Advanced Engineering Technology and Sciences*, vol. 13, no. 2, pp. 718–727, 2024, last Modified: 2025-01-05T12:19+00:00 Publisher: World Journal of Advanced Engineering Technology and Sciences.

[23] S. Alsofyani and A. Alelayani, "Securing Patients' Healthcare Records Using Blockchain-Based Smart Contracts," in *2024 1st International Conference on Logistics (ICL)*, Aug. 2024, pp. 1–15.

[24] U. Ullah Tariq, F. Sabrina, M. Mamunur Rashid, S. Gordon, Y. Lin, Z. Wang, and S. Azad, "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review," *IEEE Access*, vol. 13, pp. 45 415–45 435, 2025.

[25] S. Cihan, N. Yılmaz, A. Ozsoy, and O. D. Beyan, "A systematic review of the blockchain application in healthcare research domain: toward a unified conceptual model," *Medical & Biological Engineering & Computing*, Jan. 2025.