

Blockchain-based Electronic Health Record (EHR) System

Seema¹, Dr. Gajendran Malshetty²

¹M.Tech Student, Department of Artificial Intelligence and Data Science, Sharnabasva University.
seemakulkarni2002@gmail.com

²Guide, Department of Artificial Intelligence and Data Science, Sharnabasva University.

ABSTRACT

Conventional Electronic Health Record (EHR) systems improve access to patient information but commonly depend on centralized databases, creating concerns related to single points of failure, unauthorized access, limited transparency, interoperability, and patient control. This project develops a blockchain-based EHR management system that combines Ethereum, Solidity smart contracts, Angular, MetaMask, Ethers.js, Hardhat, Anvil, and the InterPlanetary File System (IPFS). The system supports Administrator, Doctor, and Patient roles. MetaMask is used for wallet-based authentication; smart contracts manage registration, appointments, medical-record references, and access permissions; and IPFS stores healthcare documents while only cryptographic hash references are maintained on the blockchain. The application was implemented and tested in a local blockchain environment. The thesis reports successful operation of user registration, authentication, appointment scheduling, medical record upload, permission management, and authorized record retrieval. The resulting architecture provides a patient-centric workflow in which access can be granted or revoked and important healthcare transactions are recorded on the blockchain to provide a transparent audit trail. The prototype demonstrates the feasibility of combining blockchain and decentralized storage for secure and transparent EHR management.

Keywords: Electronic Health Record; Blockchain; Ethereum; Smart contracts; IPFS; MetaMask; Access control

I. INTRODUCTION

Electronic Health Records provide digital access to patient histories, prescriptions, laboratory reports, diagnostic information, treatment plans, and other healthcare records. Although digital records reduce paperwork and accelerate access to information, the thesis identifies important limitations in conventional centralized EHR systems, including single points of failure, privacy risks, unauthorized modification, limited auditability, and difficulty sharing records between healthcare institutions.

Blockchain technology is proposed as a decentralized mechanism for preserving transaction integrity and maintaining a transparent history of healthcare operations. Because storing large medical documents directly on-chain is inefficient, the project combines Ethereum with IPFS: medical documents are stored in the decentralized file system, while the blockchain maintains the associated cryptographic hash reference.

The resulting system is designed around three users - Administrator, Doctor, and Patient - and integrates Angular for the frontend, Solidity smart contracts for application logic, MetaMask for wallet authentication, Ethers.js for blockchain interaction, Hardhat and Anvil for local development and testing, and IPFS for decentralized document storage.

II. OBJECTIVES

- To develop a decentralized Electronic Health Record management system using Ethereum Blockchain.
- To implement secure authentication and user identity verification using MetaMask digital wallets.
- To develop Solidity smart contracts for patient registration, doctor registration, appointment scheduling, medical records, and access permissions.
- To integrate IPFS for secure and decentralized storage of medical documents.
- To ensure that only authorized healthcare providers can access patient records after obtaining patient consent.
- To provide patients with ownership and control over their healthcare information.
- To maintain an immutable audit trail of healthcare transactions and prevent unauthorized modification or deletion of records.
- To improve interoperability through secure sharing of healthcare information.
- To develop an Angular web interface for administrators, doctors, and patients.

III. LITERATURE SURVEY

The literature reviewed in the thesis establishes blockchain as a recurring approach for decentralized healthcare access control, auditability, and data sharing. MedRec demonstrated blockchain-based medical data access and

permission management [1], while Ancile examined privacy-preserving access control and interoperable EHRs [2]. MeDShare explored blockchain-assisted medical data sharing [3], and related work addressed mobile healthcare data collaboration [4] and distributed personal health records [5].

Further studies discussed blockchain in healthcare more broadly, including healthcare applications [6], security and privacy in healthcare cloud environments [7], and systematic review of blockchain use in healthcare [8]. The thesis uses these works to motivate a prototype that combines smart-contract access control with decentralized document storage rather than relying solely on a centralized database.

IV. SYSTEM DESIGN AND METHODOLOGY

System architecture

The architecture contains five major layers: User Layer, Frontend Layer, Blockchain Layer, Decentralized Storage Layer, and Development Environment. The User Layer includes Administrator, Doctor, and Patient roles. Angular provides the interactive frontend, Ethers.js connects the frontend to Ethereum smart contracts, and MetaMask provides wallet-based authentication and transaction signing. Solidity smart contracts implement registration, appointment management, access control, IPFS hash storage, and immutable transaction logging. IPFS stores healthcare documents, while Hardhat and Anvil provide the smart-contract development and local blockchain environment.

System Architecture of Blockchain-Based Electronic Health Record (EHR) System

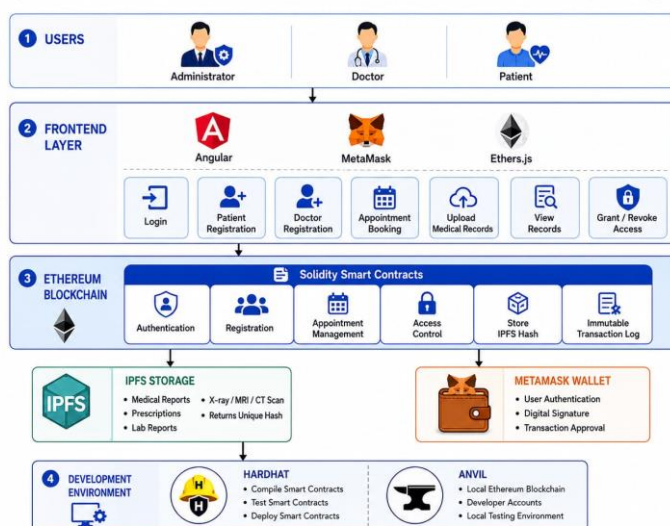


Fig. 1. System architecture of the blockchain-based EHR system retained from the thesis.

System workflow

The user opens the Angular application and connects a MetaMask wallet. After authentication, the administrator registers doctors and patients, patients can book appointments, and doctors can upload medical records. Uploaded documents are transferred to IPFS, which generates a unique hash. The smart contract stores the hash on Ethereum. Patients can grant or revoke doctor permissions, and an authorized doctor can retrieve a record after blockchain-based permission verification. Every transaction is recorded on Ethereum.

Flowchart of Blockchain-Based Electronic Health Record (EHR) System

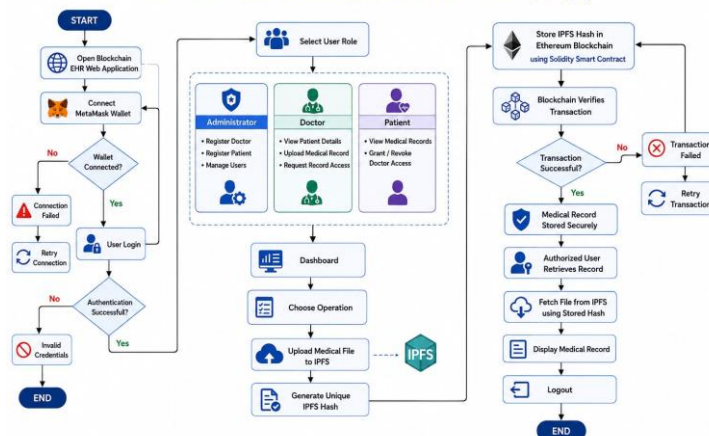


Fig. 2. System workflow retained from the thesis.

Technology stack

Table 1. Technology components reported in the thesis

Component	Role in the proposed system
Angular	Frontend interface for Administrator, Doctor, and Patient users.
Ethereum Blockchain	Maintains healthcare transactions and IPFS hash references.
Solidity Smart Contracts	Implements registration, appointments, access permissions, and record transactions.
MetaMask	Wallet-based authentication and digital transaction approval.
Ethers.js	Communication bridge between Angular and Ethereum smart contracts.
IPFS	Decentralized storage for medical reports and other healthcare documents.
Hardhat	Compilation, testing, debugging, and deployment of smart contracts.
Anvil	Local Ethereum blockchain used during application development and testing.

Implementation sequence

- User opens the Angular application and connects the MetaMask wallet.
- Authentication is completed and users are registered according to their roles.
- Patients book appointments and doctors upload medical records.
- Medical documents are uploaded to IPFS and a unique hash is generated.
- The IPFS hash is stored on Ethereum through the smart contract.
- Patients grant or revoke access permissions.
- Authorized doctors retrieve records after blockchain verification.
- Transactions are permanently recorded on the Ethereum ledger.

V. RESULTS AND DISCUSSION

The thesis reports that the Blockchain-Based EHR Management System was successfully implemented and tested in a local blockchain environment. User registration, wallet authentication, appointment scheduling, medical record upload, permission management, and record retrieval were tested successfully. The screenshots retained below provide the principal implementation evidence for the working prototype.

Application entry and authentication

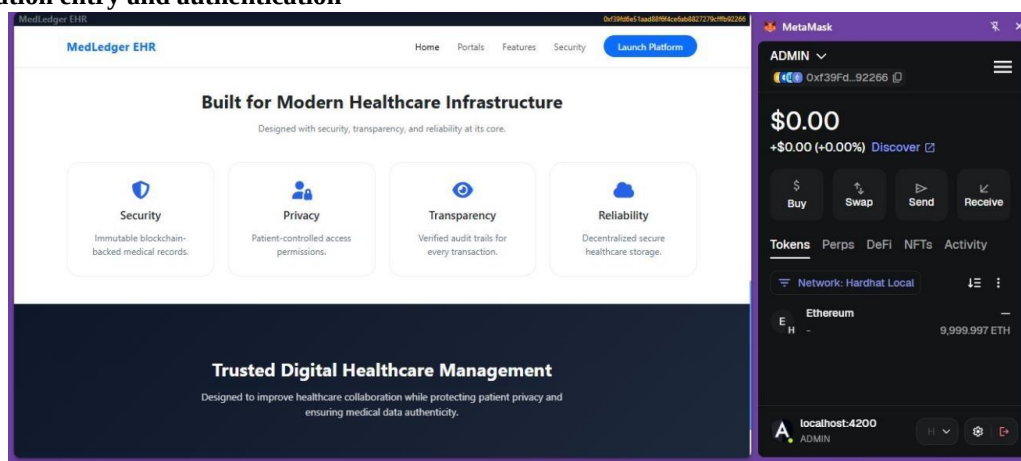


Fig. 3. Home page of the developed EHR application.

The home page serves as the entry point to the application and presents the major system features. Users connect a MetaMask wallet before accessing role-specific functions.

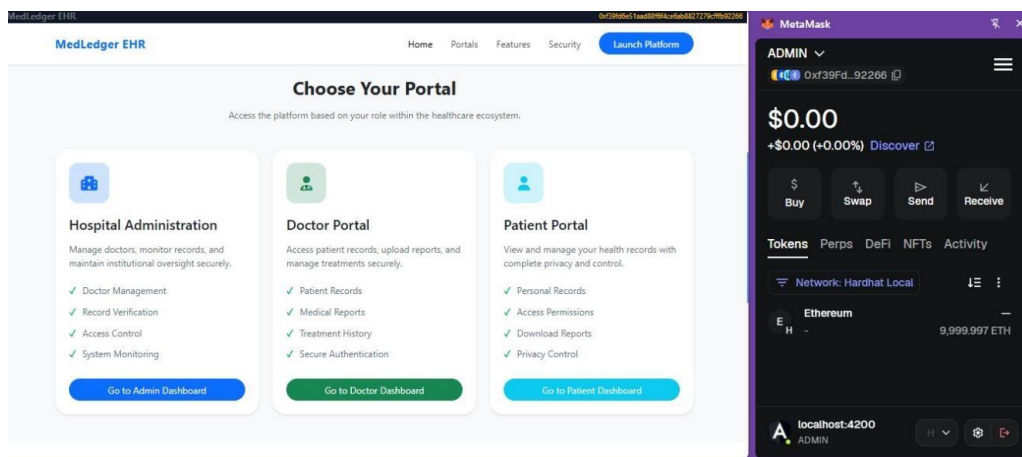


Fig. 4. MetaMask wallet connection and portal selection.

The wallet connection is used instead of conventional username-password authentication. The thesis states that blockchain transactions require user approval through MetaMask, providing wallet-based identity verification.

Administrator and doctor functions

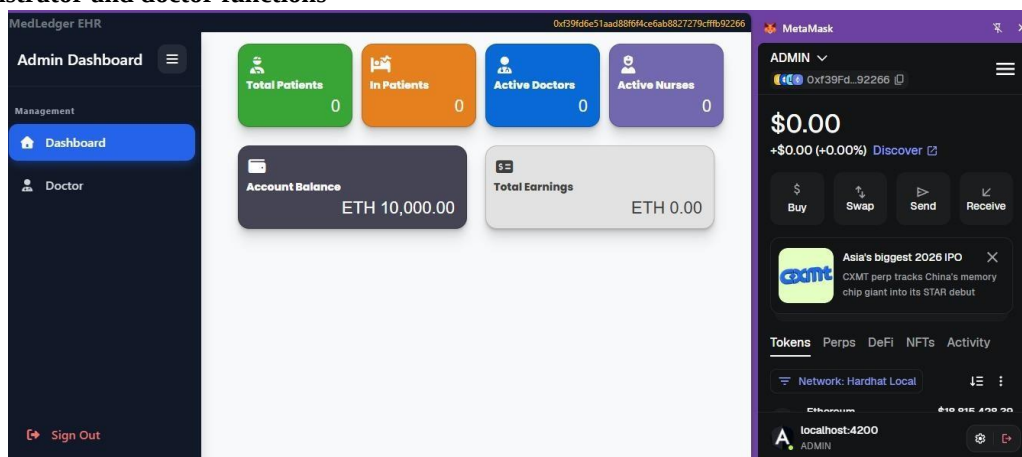


Fig. 5. Administrator dashboard.

The Administrator dashboard provides registration and management functions for doctors and patients and supports monitoring of system activities.

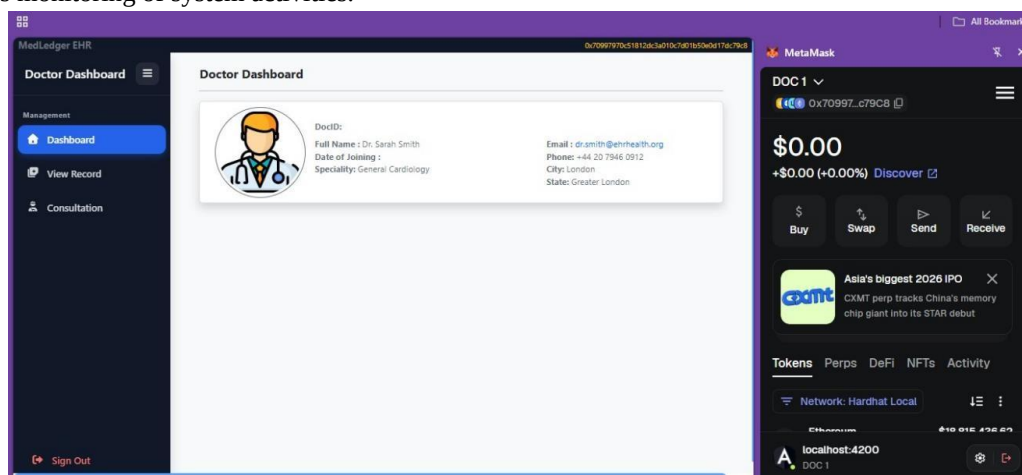


Fig. 6. Doctor dashboard.

The Doctor dashboard supports management of appointments, medical reports, and authorized patient records. Access to patient information is conditioned on patient authorization.

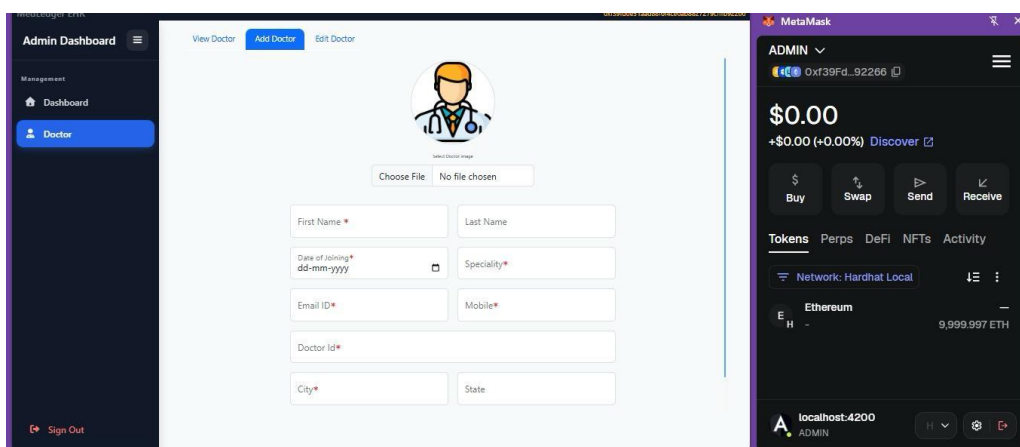


Fig. 7. Add Doctor page.

The administrator can register a new doctor by entering personal and professional details. The page is integrated with the wallet-enabled blockchain workflow described in the thesis.

Authorized record retrieval and consultation

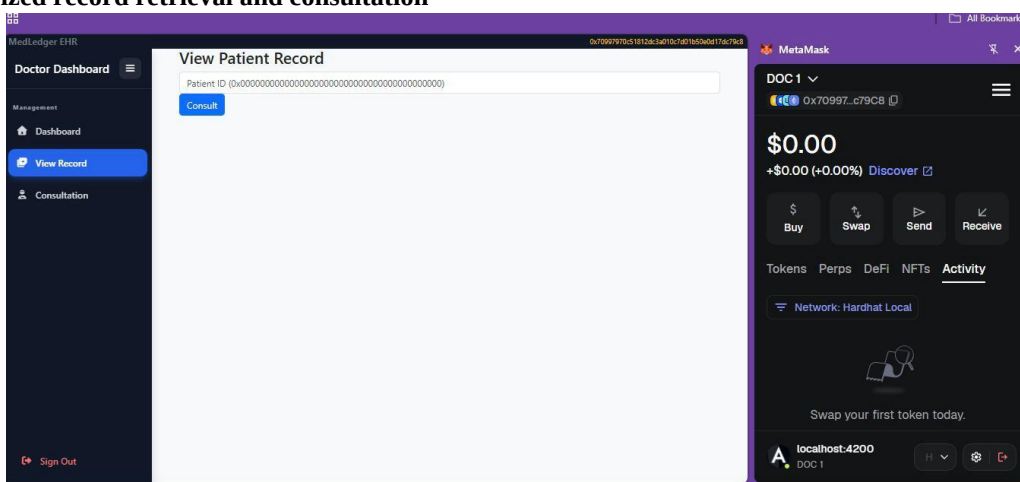


Fig. 8. View Patient Record page.

The doctor retrieves a patient's medical record by patient ID. The thesis describes the retrieval process as authorization-controlled and intended to preserve record integrity.

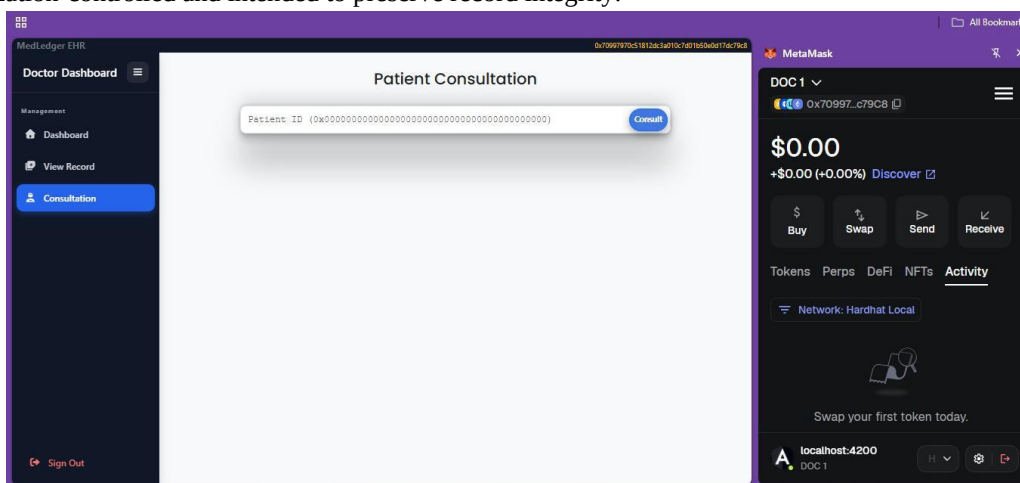


Fig. 9. Patient Consultation page.

The consultation module enables a doctor to access patient information after verification and enter consultation details within the blockchain-backed workflow.

Overall discussion

The implementation evidence supports the thesis conclusion that Ethereum smart contracts can automate access-control and healthcare-record operations while IPFS provides an off-chain mechanism for large document

storage. Patient-controlled grant and revoke operations are central to the proposed privacy model, and the blockchain transaction history provides a persistent audit trail. The system was evaluated in a local blockchain environment; the thesis does not report public-chain deployment, transaction-cost benchmarks, throughput measurements, or clinical interoperability trials. These are therefore not claimed in this article.

VI. CONCLUSION

- The project successfully demonstrates a blockchain-based EHR management prototype using Ethereum, Solidity, Angular, MetaMask, Ethers.js, Hardhat, Anvil, and IPFS.
- The system supports Administrator, Doctor, and Patient roles with wallet-based authentication, appointment management, medical record handling, and patient-controlled permissions.
- IPFS is used to store healthcare documents while cryptographic hash references are maintained on-chain, reducing the need to store large files directly on Ethereum.
- The local implementation successfully demonstrated registration, authentication, appointment scheduling, medical record upload, permission management, and authorized record retrieval.
- The proposed architecture emphasizes transparency, tamper resistance, patient ownership, and a persistent blockchain audit trail.
- Future work identified in the thesis includes public or consortium blockchain deployment, multi-hospital integration, mobile support, AI-assisted healthcare functions, wearable/IoT integration, stronger access control, cloud deployment, Layer-2 scaling, and zero-knowledge proofs.

REFERENCES

- [1] G. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," *Proc. IEEE Open & Big Data Conference*, 2016.
- [2] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-Preserving Framework for Access Control and Interoperable Electronic Health Records Using Blockchain Technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.
- [3] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers via Blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
- [4] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2017.
- [5] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A Distributed Architecture Model to Integrate Personal Health Records," *Journal of Biomedical Informatics*, vol. 71, pp. 70–81, 2017.
- [6] A. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," *IEEE International Conference on e-Health Networking, Applications and Services*, 2016.
- [7] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.
- [8] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," *Symmetry*, vol. 10, no. 10, 2018.
- [9] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.
- [10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.