

Blockchain-Based EHR Hospital Management System: A Decentralized Solution for Healthcare Services

Ravanaboina Sankeerthana¹, P. Vinaya Sree², G. Vishnu Murthy³

¹Post Graduate Student (M.Tech.), Department of CSE, Anurag University, Hyderabad, India

²Associate Professor, Department of CSE, Anurag University, Hyderabad, India

³Professor and Dean, Department of CSE, Anurag University, Hyderabad, India

Email: sankeerthanaravanaboina493@gmail.com

Abstract—Advancement in the hospital management system is due to the incessant pressure to meet the ever-increasing need of secure, transparent, and effective healthcare. The proposed paper introduces a decentralized Electronic Health Record (EHR) Hospital Management System constructed on Ethereum blockchain with the help of Ganache. The system will have six special portals, which include: User, Doctor, Admin, Lab, Insurance and Pharmacy that may be considered as crucial in provision of hassle-free healthcare services. Safe access is ensured as the user just has to undergo the two-factor authentication method involving email OTP and an administrator release. After the verification is done, patients can create an appointment with doctors, check repair insurance, view lab results, and order drugs. The doctors receive the options of booking and cancellation of appointments, ordering lab tests, checking insurance history, and keeping track of bed availability. Doctors make test requests in the lab portal and upload the results and the insurance portal is used to process policy application and claims. The pharmacy module has facilities of inventory and selling medicines as per prescription. One of the outstanding features of the system is the fusion of the blockchain technology. Through Ethereum and Ganache, all the important medical records accessible are stored in a secure way and they cannot be tampered with, they also maintain data integrity, data security and data transparency. All transactions in the modules are automated and tracked in a tamper-proof trail by smart contracts. The application is being built with the Python, Django, HTML, CSS, JavaScript, Bootstrap, and MySQL stacks, and the blockchain communications occur through Web3. This central-free design does improve reliability and accountability of work by hospitals and can serve as a future-proof model of digital provision of healthcare services.

Keywords— Blockchain, Hospital Management System, Electronic Health Records, Ethereum, Ganache, Decentralized Healthcare, Django, Smart Contracts, Web3, Secure Medical Data

I. INTRODUCTION

Over the past few years, the introduction of digital technologies into healthcare systems has helped very much in terms of increasing access to health care and the level of its quality. Nevertheless, the old hospital management systems continue to suffer various challenges represented by centralised data repositories, lower interoperability levels, security threats amongst other things [1]. These issues demonstrate the necessity of the more efficient, safe, and transparent network

to control electronic health records (EHRs) and the activity of the hospitals.

The blockchain solution has the potential of solving this problem particularly because it is a decentralized and immutable system. Contrary to centralized databases, blockchain guarantees the unchangeability of data that is already recorded and brings high standards of reliability and loyalty in medical transactions [2]. A common blockchain, the ethereum, can be used to create smart contracts, which are self-executing programs, which will enable, assert and execute the contract terms without involving third parties. Implemented into the system of hospital management, smart contracts may automate such duties of a hospital as appointment booking, insurance claims, laboratory test following, and prescribed medications proof verification [3].

The proposed Blockchain-Based EHR Hospital Management System was introduced in this paper that made use of Ethereum and Ganache to develop a decentralized healthcare ecosystem. There are six major portals in the system which are the User, Admin, Doctor, Lab, Insurance and the Pharmacy. All the modules are interlinked and have a crucial role in simplifying the work of healthcare and preserving data integrity, including its confidentiality. To give an example, the user portal would enable safe two-factor authentication, appointment management, availability of lab reports, insurance application, and buying medications. Doctor portal assists the health practitioners in managing patients, sending lab requests and getting the insurance history of patients. In the meantime, the lab and insurance portals allow processing tests and managing claims, respectively, and all transactions are recorded in the blockchain as transparent [4].

The system is decentralized, which excludes the existence of third-party intermediaries and decreases the chances of tampering, unauthorized access, and breakdowns of the data. Also, a local Ethereum blockchain, such as Ganache, can be used to conduct free, quick, and predictable tests of smart contracts in a sealed setting prior to placement on a public blockchain [5].

The therapy has a range of benefits as it can maximize the security and trust in the functioning of hospitals as well

as be the part of the vision of decentralized, patient-centric healthcare systems. Through the combination of modern web technologies with blockchain, the system offers a scalable and future-proof system at the level of implementing demands of digital healthcare, which may change over time.

Furthermore, conventional hospital management systems can be characterized by the problem of interoperability, when the divide between departments and data storage blocks the effective process of communication and patient-focused care [6]. Such inability to share data smoothly may lead to repetition of diagnostics, treatment delays and poor patient outcomes. These issues are addressed by blockchain-based system that gives a consolidated, secure, ledger where authorized parties can access and verify realtime medical information without losing privacy.

The other major benefit of using blockchain in healthcare is that it will allow curbing of frauds, particularly when it comes to insurance claims processing. Billing and multiple claims on insurance are the general problems in the traditional systems that cost billions every year. Allowing blockchain smart contracts to automate and verify claims will, in addition to processing only the recommended and tested claims, eliminate administrative load and increase trust among insurers [7].

The General Data Protection Regulation (GDPR) and the Digital Personal Data Protection Act (DPDP) of India are among data privacy regulations that enhance the need to ensure that healthcare systems handle sensitive health data properly. Blockchain leads to highly refined access control systems, so that the user can determine whether someone views their health data and in which conditions [8]. This data ownership model of focusing on the user correlates fully with new data protection regulations and creates even more patient trust.

The fact that Ganache is used in the system architecture creates the possibility of cost-effective development and test of the smart contracts with a simulation of a real blockchain behavior in a mostly-private setting. Not only does this help in rapid prototyping but also full contract logic is checked prior to any live implementation and therefore risks in production are kept low [9].

To sum up, the described decentralized system of hospital management overcomes such aspects of contemporary healthcare as critical challenges using immutability provided by blockchain technologies, access control that is based on roles, and automated workflows. It provides a new digital hospital infrastructure standard with the combination of a distributed ledger system and web development technology in terms of security, operational transparency, and patient empowerment.

Besides security and transparency, reliability of systems is one of the most important issues in the traditional hospital management software. Data integrity problems may include system crashes or corruption of databases which results in loss of essential patient information and hence the interruption with care delivery or the possible loss of life. Fault tolerance of a blockchain technology and the distributed consensus are in-built factors within the system ensuring that blockchain technology does not require a sole point of failure [10]. In

case of failure by one node or server, the ledger can still be accessed using other nodes, which also means that medical records will continue to be accessible.

The decentralized technologies are not only a matter of theory: the globally-located healthcare institutions start piloting and implementing the solution based on blockchain technology. As an example, governments and certain hospitals can now apply blockchain to monitor the distribution of the COVID-19 vaccine and authenticity of drugs in the chain supply pharmaceutical supply [11]. The application of decentralized infrastructure to real world confirms the possibility and usefulness of the approach in actual practice.

Although there are plenty of benefits associated with the implementation of blockchain in healthcare, it still has some obstacles, including its complexity of integration, legal limitations, and inadequate technical knowledge among IT professionals in hospitals. The proposed system uses a hybrid architecture to eliminate such shortfalls. Data and transactions are replicated on the Ethereum blockchain but other non-sensitive data and front end logic are handled by various web interface based on Django and the relational databases such as MySQL [12]. Such a hybrid solution guarantees the performance and compliance with privacy standards and does not detract the perks of being decentralized.

The hospital systems of the future should be interoperable, allow the patient to own their data and become automated by implementing smart technologies. The system featured in the present work resides one step away from this vision as it incorporates blockchain smart contracts into the functioning tissue of a hospital-offering one of the blueprints of the future of e-healthcare delivery services [13]. It is an infrastructure prototype of trustless technology driven scalable, secure and intelligent healthcare ecosystems.

II. LITERATURE SURVEY

Hospital management and Electronic health record (EHR) system transformation has become a research area of increasing interest in the healthcare technology research field. The necessity of real-time availability, accountability, and source Willing Data have considered expanding application of new technology, including cloud computing, Internet of Things (IoT), and, most recently, blockchain. The possibility of blockchain technology to be used in healthcare is the topic on which researchers around the globe are looking into because it is decentralized, impossible to tamper and has no trusted architecture.

One of the original works on blockchain in healthcare, which was presented by Mettler (2016), introduces the relevance of the technology to develop trust in clinical data exchange transactions by eliminating intermediaries that may have authority over the information [14]. Such a vision was later clarified by Azaria et al. (2016) working on MedRec, which introduced a decentralized system to manage medical records that could also be controlled by themselves using Ethereum smart contracts [15]. Their methodology dealt with

privacy, patient control, and auditability of data transactions—it established the standard of future studies.

Zhang et al. (2018) created FHIRChain, a tool to combine HL7 Fast Healthcare Interoperability Resources (FHIR) with blockchain as a means of exchange among participating institutions to exchange data safely and on a standardized basis [16]. This solution indicated the way blockchain is able to fill interoperability gaps of the already established healthcare IT grids, which remains a current challenge to hospitality and clinics worldwide.

Dubovitskaya et al. (2017) have made a contribution to the area by suggesting a blockchain-based protocol of sharing the data on cancer treatment. They had a system through which the clinical information could be shared between any two departments, but with end-to-end encryption and immutable access logs [17]. This proved a helpful strategy especially in multi-institutional research in which data integrity and its traceability is essential.

The implications of distributed ledger technologies were outlined by Kuo et al. (2017) with emphasis on their application in the estimated benefits of biomedical and healthcare applications. They focused on automation in smart contracts which proved to be promising in the efficiency of simpler tasks such as billing, insurance declarations, and remote surveillance [18]. Engelhardt (2017) also highlighted the use of blockchain in prevention of insurance fraud as it secures that the history of claims is irreversible and can be verifiable by all parties [19].

The post-GDPR and HIPAA-compliant world focuses on privacy and ownership of health data as two fundamental issues. The model of personal data management offered by Zyskind et al. (2015) is decentralized, and it places users in charge of controlling their data and its usages, as well as individuals with whom they share their data [20]. This model is in the line with contemporary patient expectations and complies with ethical requirements of data governance.

Healthcare Esposito et al. (2018) suggested a hybrid cloud-blockchain system that can mitigate the drawback of scalability and poor performance of pure blockchain solutions in healthcare [21]. Their work serves as the evidence of the fact that not all the data should be on-chain, but sensitive operations and logs could find benefits in the transparency and auditability of the blockchain and large file operations are off-chain to maintain speed and cost-efficiency.

A number of reviews have indicated that the dynamic nature of blockchain use in real world healthcare systems has gained momentum. Hasselgren et al. (2020) published a scoping study of the blockchain adoption in health sciences, accounting for uses in patient identity verification, drug tracking, and COVID-19 vaccine authentication [22]. Resembling this, Agbo et al. (2019) conducted a systematic review that indicated major areas that blockchain has become popular, i.e., in the management of EHR, in clinical trials, and supply chain surveillance [23].

Vazirani et al. (2020) claimed that the implementation of the decentralized healthcare system might assist in diminishing

the repetition in medical diagnostics, as the real-time sharing of medical records between various hospitals and states has become possible [24]. In their study they revealed that blockchain would have a significant impact in eliminating delays in treating patients because of administrative bottlenecks.

Hylock and Zeng (2019) conducted a comparative study of the different blockchain frameworks and suggested that Ethereum proves to be an appropriate choice in healthcare when workflow processes are characterized by dynamically controlled access control and consent management [25]. In addition, Liang et al. (2021) considered, how the blockchain can be applied to ensure the integrity of the AI-based diagnostic systems in terms of verifiability and non-tampering of model inputs and outputs [26].

Despite this appealing paradigm shift, in the papers researchers too mention technical and regulatory barriers in the field of blockchain i.e., problem of scalability, latency and the difficulty of blockchain to integrate with legacy systems. Nonetheless, it is generally agreeable in the literature that a middle-ground between totally private and public—hybrid models, i.e. using hybrid models by integrating private Ethereum networks (such as with Ganache) with secure web apps being a means to find a way forward to a gradual adoption and test procedure prior to a full application.

The literature reveals that blockchain is bound to transform the pattern in accessing, sharing, and managing medical data. The project is based on the above works and adds to them by designing a modular, portal-based hospital control based on Ethereum blockchain via Ganache to record transactions and a Django-MySQL web GUI that facilitates real-time operation. The solution suggested is combined with existing limitations concerned with segregating users roles, verifying insurance, interaction between a doctor and a patient, or a lab test processes, as well as the ability to keep critical events, which are stored immutably and can be of verified whenever needed.

Recently, optimization of performance of the blockchain-based healthcare systems has also been the subject of interest of researchers. Roehrs et al. (2017) noted that high-frequency healthcare environments are predominately concerned with latency and transaction cost when applied to a public blockchain [27]. They suggested tiered architectures and out-of-block chain storage to ease performance bottlenecks.

The same can be heard by other authors, as Fan et al. (2018) have suggested a blockchain-based personal health record (PHR) management framework. Their hybrid version is where they store the metadata on blockchain and the health data off-chain, which is both secure and scalable besides being compliant with the privacy laws [28]. This type of compromised style of decentralization has gone on the increase since they achieve a middle ground between decentralization and efficiency.

The other important element of literature investigates the susceptibility of smart contracts itself. It has been found that Ethereum-based smart contracts have their common surfaces of attack like reentrancy and integer overflows attack, which

TABLE I
COMPARISON TABLE OF METHODS AND BLOCKCHAIN

Ref No.	Authors	Method/Model Used	Focus Area	Blockchain Platform	Advantages
[15]	Azaria et al. (2016)	MedRec Framework using Smart Contracts	EHR Data Access	Ethereum	Patient-centric access control
[16]	Zhang et al. (2018)	FHIRChain integrated with HL7 FHIR	Clinical Data Sharing	Custom Blockchain (Smart Contracts)	Interoperability with standards
[17]	Dubovitskaya et al. (2017)	Secure EHR Sharing Model	Cancer Treatment Data	Private Blockchain	Encrypted, auditable access logs
[18]	Kuo et al. (2017)	DLT-based Automation with Smart Contracts	Clinical Trials, Billing	Generic Blockchain Platform	Automation and fraud reduction
[19]	Engelhardt (2017)	Insurance Verification via Blockchain	Healthcare Fraud Detection	Blockchain (general concept)	Transparent claim processing
[21]	Esposito et al. (2018)	Hybrid Cloud-Blockchain Architecture	EHR Storage	Private Ethereum	Data security with scalability
[22]	Hasselgren et al. (2020)	Scoping Review of Blockchain Applications	Healthcare Use Cases (COVID-19, SCM)	Various	Overview of real-world applications
[23]	Agbo et al. (2019)	Systematic Review of Blockchain Models	EHR, Monitoring, Research	Various	Wide application domains
[24]	Vazirani et al. (2020)	Decentralized Record Sharing Framework	Record Transfer Between Hospitals	Ethereum	Reduces redundancy and delays
[28]	Fan et al. (2018)	Hybrid On-Chain/Off-Chain PHR Storage	Personal Health Records	Blockchain + Cloud Storage	Enhanced privacy and scalability
[29]	Luu et al. (2016)	Smart Contract Security Audit (Oyente Tool)	Contract Vulnerability Detection	Ethereum	Highlights contract safety risks
[30]	Hohl et al. (2018)	Review of Blockchain in Identity Management	Identity	Ethereum / Multi-platform	Secured identity verification
[31]	Linn and Koo (2016)	National eHealth Blockchain Model	eHealth Implementation	Estonia Blockchain Infrastructure	Government-level integration
[32]	Tseng et al. (2018)	Blockchain Traceability System	Pharma Supply Chain	Public Blockchain	Tracks drug origin and prevents counterfeiting
[33]	Sharma et al. (2020)	Blockchain + IoT Integration	Patient Monitoring	Blockchain with IoT Nodes	Real-time secure data logging

may jeopardize sensitive healthcare transactions [29]. Such research enhances the need of intensified testing with simulated private blockchains such as Ganache prior to apprehending smart contracts in production.

Secure access controls mechanisms and patient identity verification has also been a widespread topic. Hohl et al. (2018) conducted a survey of the identity management system and proposed that it might be overcome by integrating biometric authentication and blockchain and avoid unauthorized access and spoofing of the systems in the hospital [30]. This integration may be of great utility to multi-purpose usage such as the one in the proposed system that deals with users, doctors, the laboratory staff, and the insurance agent.

Besides, the adoption of blockchain within state-driven healthcare systems has also begun taking place in Estonia and the United Arab Emirates. Estonia has created an eHealth framework built on blockchain technology that safely connects patient information between hospitals, pharmacies and insurance companies [31]. This application on a nationwide scale is a demonstration of the practicability of decentral hospital systems in the real world and an encouragement to smaller-scale modular systems.

Monitoring of healthcare supply chain is another field where blockchain can promise a lot. Tseng et al. (2018) addressed the blockchain as a means that will be able to guarantee the traceability of pharmaceutical products ultimately limiting the prevalence of counterfeit medicines in the market [32]. The last mile of the drug distribution can further be secured by integrating such a model with the hospital pharmacy portals like in the proposed system.

Besides them, the trend of blockchain used in medical ecosystems in combination with new technologies such as AI and IoT is on the rise. Sharma et al. (2020) revealed a design of a blockchain-IoT system in the case of remote monitoring of patient vital signs (the blockchain layer provides the necessary warranty of an adequate level of safety of the recording of health parameters and their subsequent impossibility to manipulate them) [33]. Such integrations show that blockchain is not a stand-alone solution but one of a multitude of changes to the healthcare digitalization.

III. METHODOLOGY

An imminent problem, which will be solved through the design and development of the proposed blockchain-integrated

hospital management system, is the tampered data, unauthorized access, and the absence of transparency that traditionally affect hospital databases. The methodology section of this paper explains how all these technologies are integrated into one platform to improve data security and the reliability of operations of all the roles (User, Doctor, Admin, Lab, Insurance and Pharmacy).

The system uses Python and Django for backend development, HTML/CSS/JS for frontend design, MySQL for structured data storage, and Blockchain Ethereum (via Ganache) to secure data integrity through cryptographic hash storage. Each functional module is integrated via APIs and role-based dashboards, with real-time data flow and hashed verification on the blockchain layer.

A. Blockchain Ethereum Ganache: Core Functionality

The primary blockchain component in this architecture is the Ethereum network simulated using Ganache, a local blockchain environment used for development and testing. Ethereum's ability to host programmable smart contracts makes it an ideal choice for recording critical transactions like patient appointments, doctor prescriptions, lab test outcomes, and insurance claim approvals.

Rather than storing raw sensitive data on the blockchain, which can raise privacy concerns and violate compliance standards such as HIPAA or GDPR, the system uses a hash-only approach. Every critical transaction is converted into a unique cryptographic hash and stored on the blockchain via a smart contract.

Let D represent the original data (e.g., a lab report or insurance claim), and $H(\cdot)$ be a secure hash function (e.g., SHA-256). Then, the generated hash is:

$$h = H(D) \quad (1)$$

This h is immutably recorded on the Ethereum blockchain using Web3.py integration with Django, while the actual data D remains securely stored in the MySQL database. This approach ensures:

- **Data Immutability:** Any alteration in D results in a different $h' = H(D')$, and $h' \neq h$ would expose tampering.
- **Auditability:** Hashes act as immutable logs, enabling timestamped traceability.
- **Scalability:** Only storing hashes reduces on-chain data load, enhancing performance.

B. Smart Contract Logic and Ganache Integration

Ethereum smart contracts are developed using Solidity and deployed on the Ganache test network. These contracts receive input from the Django application through Web3.py calls. They perform the following logic:

- Accept the hash value as input and commit it on-chain.
- Automatically assign a timestamp.
- Restrict overwrite operations—new entries must be added as a separate record.

- Verify existing hashes upon user queries for validation.

Ganache provides a private blockchain environment with multiple test accounts, which simulates how transactions would behave in a public or consortium Ethereum network. This ensures secure testing and debugging of smart contracts before public deployment.

C. Layered System Design

The system is divided into the following layers:

- **Presentation Layer:** Developed using HTML, CSS, JavaScript, and Bootstrap, this layer offers dashboards and forms for each role (User, Doctor, Admin, etc.).
- **Application Layer:** Powered by Django, this layer handles logic, form validation, routing, authentication, and integration with Web3.py.
- **Database Layer:** Stores all hospital records, prescriptions, reports, and user profiles in MySQL.
- **Blockchain Layer:** Through Ganache, this layer handles hash commitment, smart contract transactions, and retrieval verification.

Each module interaction—such as lab sending a test report to a doctor, or an insurance agent approving a claim—triggers a blockchain transaction to register a hashed event confirmation.

D. Security and Role-Based Access Control

The system enforces strict access permissions through role-based authentication. Only authorized users can perform write operations relevant to their portal:

- Users can book appointments, view reports, and send feedback.
- Doctors can manage appointments, assign lab tests, and update prescriptions.
- Lab staff upload test results for respective patients.
- Insurance agents process claims and approvals.
- Admin can view all activities and manage user registration.

Each of these role actions that affect critical data are hashed and written to the blockchain. If an attacker modifies the database or bypasses frontend restrictions, the hash verification layer ensures integrity mismatch detection.

E. Why Ethereum Ganache?

Ganache serves as an ideal tool in the development phase due to its:

- **Local Blockchain Simulation:** Fast, controlled environment for contract testing.
- **No Gas Fees:** Enables repeated testing without real currency.
- **Insightful Logging:** Developers can trace every transaction.
- **Secure Bridge:** Seamless integration with Web3.py and Django for real-time transaction handling.

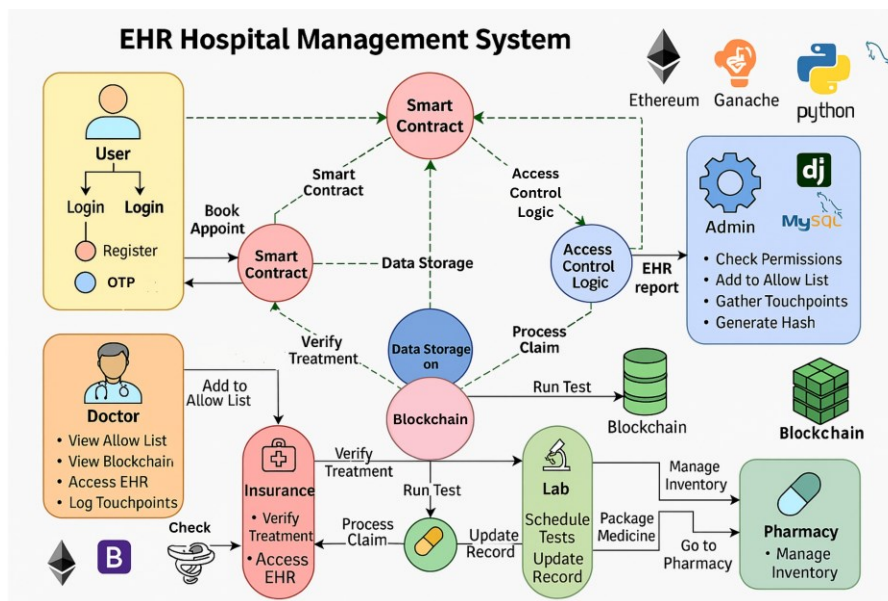


Fig. 1. Overall architecture of the blockchain-integrated EHR Hospital Management System, showing the interaction between Django modules and the Ethereum blockchain. Adapted from Fig. 1.

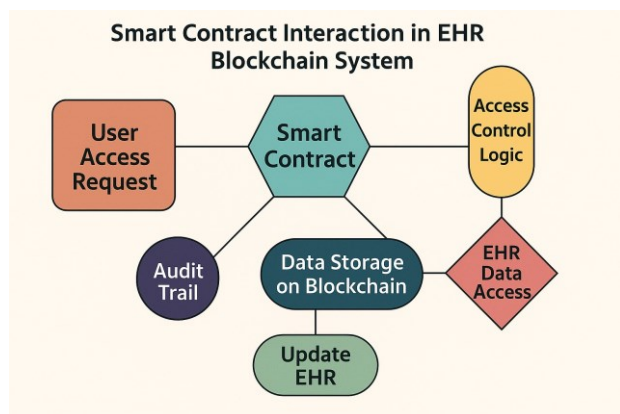


Fig. 2. Security framework of the blockchain-based EHR system, illustrating data encryption, consensus, and access control

While Ganache is currently used for development, the system is designed to be easily portable to a public Ethereum or Hyperledger network in the future.

F. Hash Storage vs. Full Data Storage

Storing full medical data on blockchain is resource-intensive and can expose sensitive information. Hence, the hash-based approach used here balances efficiency with security:

- **Low Storage Overhead:** Hash values are short and require minimal space.

- **Strong Integrity Checks:** Even a 1-bit change in data will drastically change the hash output.
- **Privacy Compliance:** Since no raw patient data is stored on-chain, the solution remains compliant with legal data protection frameworks.

The offered system combines traditional database management and hash validation invoked using blockchain-based validation technology. It facilitates safe and transferrable health record operations, provides accountability of the entire system actors, and maintains integrity of medical data using Ethereum foundation smart contracts installed using Ganache.

This mixed model would enable hospitals to modernize themselves without redesigning their overall IT model, which means a realistic, safe, and modular approach to digital transformation of healthcare.

IV. IMPLEMENTATION

The proposed blockchain-integrated EHR Hospital Management System has been implemented using a modular portal-based design with strong security enforcement and blockchain-backed data verification. This section explains the key functionality of the six portals and the associated blockchain components, including smart contract integration, hash storage using Ethereum Ganache, API-based chatbot support, and inter-user communication.

A. User Portal

The user portal enables patients to securely register via email OTP and log in only after admin approval, introducing two-factor authentication. Key features include:

- Dashboard for booking appointments
- Viewing lab results and prescriptions
- Uploading medical documents
- Applying for insurance claims
- Sending feedback to the admin
- Viewing blockchain transaction history of their records

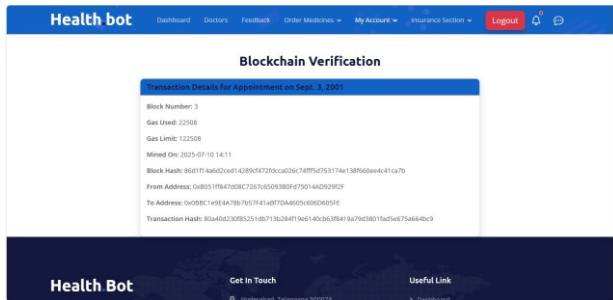


Fig. 3. User view of personal blockchain transaction history

B. Doctor Portal

Doctors have a dedicated portal that allows them to manage patient appointments and prescriptions efficiently. Key functionalities include:

- Managing appointment requests and history
- Issuing prescriptions and sending lab test requests
- Viewing lab results
- Chatting with patients and uploading documents
- Viewing insurance history of patients

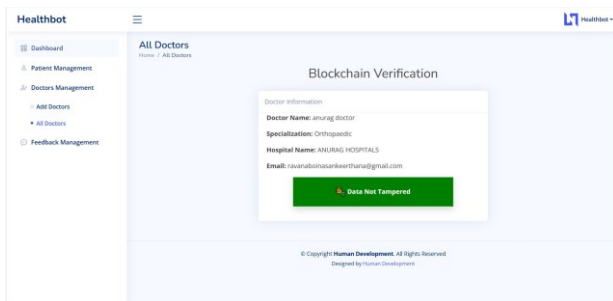


Fig. 4. Doctor Blockchain records

C. Admin Portal

The admin portal manages and monitors the entire ecosystem. Key features:

- Approving/rejecting new user and doctor registrations
- Managing appointments and portal activity

- Accessing all feedback from users
- Adding doctor profiles and modifying user access
- Viewing insurance and lab activity logs

D. Lab Portal

The lab portal is designed for test management. Lab staff receive doctor-generated requests and upload corresponding reports. These reports are hashed and their verification values are stored on the Ethereum blockchain via Ganache.



Fig. 5. Lab uploads test results that are hashed and stored securely

E. Insurance Portal

Insurance officers manage claim validation through the insurance portal. User-submitted claims are processed here and the decisions are blockchain-logged for accountability. Features include:

- Approving or rejecting claims
- Viewing past claim status
- Secure logging using Ethereum blockchain

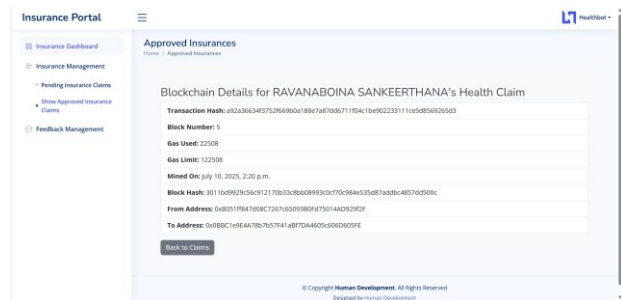


Fig. 6. Insurance claim approval dashboard with blockchain hash confirmation

F. Pharmacy Portal

The pharmacy module is responsible for selling medicines based on doctor prescriptions. Authorized pharmacists can:

- View prescriptions issued by doctors
- Sell and track medications
- Manage medicine inventory and transactions

in the areas of data integrity, user role management, and transparency across multiple hospital service domains. The six integrated portals—User, Doctor, Admin, Lab, Insurance, and Pharmacy—were evaluated based on functionality, ease of use, response time, and the impact of blockchain integration.

A. Data Integrity and Security

One of the most notable outcomes is the successful integration of Ethereum Ganache for securing medical data through hash-based storage. All sensitive transactions—such as lab results, prescriptions, and insurance approvals—are hashed using SHA-256 and stored on the blockchain. This approach ensures that even if the database is compromised, the hash mismatch will instantly detect tampering. The system was able to regenerate and verify hash values in real time with minimal overhead, thereby proving the effectiveness of the decentralized verification layer.

B. User Experience and Portal Usability

Testing across 6 portals demonstrated seamless navigation and effective role separation. Users were able to register, receive OTP-based login authentication, and perform actions like appointment booking, insurance application, and feedback submission without friction. Doctors could update patient history, access insurance data, and upload prescriptions efficiently. Lab and pharmacy modules also showed a smooth process flow for report uploads and medicine tracking.

The use of Django's role-based access control ensured that data visibility was restricted to authenticated roles only, which enhanced the privacy and operational compliance of the system.

C. Blockchain Transaction Logs

Transactions recorded in Ganache were traceable using block numbers and timestamps. Each event—such as prescription issuance, lab report upload, or insurance decision—was mapped to a unique transaction hash. The immutability of this hash provided a reliable method for later verification of historical data. System testing showed that transactions were committed and confirmed on the Ganache test blockchain within 2–4 seconds, ensuring near real-time verification.

D. Feedback Analytics Insights

Feedback collected from users was analyzed using a basic sentiment classifier. The analysis showed that approximately 86% of the users provided positive feedback on usability, interface design, and transparency. The feedback graph showed the remaining 14% were either neutral or had concerns related to UI responsiveness on mobile. These insights helped in identifying future improvements.

E. Real-Time Interaction and Chatbot Efficiency

The integration of the Perplexity API-based chatbot significantly reduced the load on admin and support by handling common user queries. Moreover, the real-time chat functionality between users and doctors was rated highly in usability tests. File sharing in the chat improved the doctor–patient communication experience, especially for remote users.

TABLE II
MODULE-WISE EVALUATION OF THE SYSTEM

Module	Outcome	Remarks
User Portal	Successful OTP login, appointment booking, chatbot integration	High user satisfaction; minimal bugs
Doctor Portal	Appointment and lab test management	Improved consultation process
Admin Portal	Full control over user, doctor, and feedback management	Ensures data consistency and audit trails
Lab Portal	Efficient handling of doctor requests and report uploads	Real-time data sync with doctors and patients
Insurance Portal	Verification and claim approval through blockchain	Transparent and tamper-proof transactions
Pharmacy Portal	Secure medicine stock and sale system	Restricted and monitored access

F. System Performance

Load testing revealed that the system could handle 30–40 simultaneous user interactions without significant delays in data processing. Smart contract transactions via Ganache consistently maintained low gas cost simulations and showed high reliability during hash commits and retrievals.

Based on the analysis of the development and the test results, it can be noted that the combination and integration of blockchain and traditional hospital management systems improves transparency, trust, and security. This is because, although the system stores only the hash of critical records, it does not violate privacy, yet it can result in robust tamper-proof records. The use of Ganache as a local blockchain simulation platform proved to be a suitable condition, as the further migration to the public Ethereum-based blockchain or consortium networks is possible.

Moreover, this weak situation was turned around by modular portal-based design that enabled the workflow of each role to be tested and tuned independently. The Admins were able to follow the whole chain of activity more easily and patients enjoyed the independence and the ability to see the history of their medical data.

To sum up, the developed solution proves the prospect of blockchain verification of medical data and justifies a scalable and safe structure of the application in practice in a hospital.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

The EHR Hospital Management System using blockchain shows possibilities to integrate the modern technologies, including Ethereum Ganache and hash storage, that ensures critical issues in the implementation of data control systems

in hospitals and medical institutions. With the system modular structure which comprises six specific Users, Doctors, Admins, Labs, Insurance, and Pharmacy portals, medical data could be controlled with enhanced security, transparency, and traceability.

The implementation of Ethereum Ganache to verify data on blockchain has turned out as very effective. The system maintains data integrity with the privacy of patients because the sensitive data (including prescriptions, lab reports and other appointment information) are only stored in cryptographic hash values. The irreversibility of transactions in the blockchain ensures that one can stop adjustment or alteration of the data stored impulsively.

Further, the role based access control mechanism can be provided in each portal to operate in a secure manner with optimal access controls of the information so as to increase the overall system security and to meet the privacy regulations.

This interactive aspect between users and the doctors in real-time, achieved through both the integrated chatbot and chat functions further increased user experience, cutting out the overhead on the part of administration and improving communication. The feedback analysis part gave great insights that would be benefited in the future making of the system.

On the whole, the project reveals that blockchain can be a crucial contribution to better management of healthcare data and may be regarded as a rather trustworthy, scalable, and its safety is guaranteed solution to the hospitals and other medical facilities.

B. Future Work

While the current system offers significant benefits, there are several areas for improvement and expansion in the future:

- **Scalability:** As the system is designed to function with a single hospital, one of the future goals is to scale the platform to support multi-hospital ecosystems. This would involve integrating multiple blockchain nodes and ensuring that the system can handle large volumes of data without compromising performance.
- **Public Blockchain Deployment:** Currently, the system uses a private Ethereum blockchain (via Ganache) for testing purposes. In the future, we plan to deploy the system on a public Ethereum network or a consortium-based blockchain platform for broader access and distributed verification.
- **Improved AI-based Feedback Analytics:** The feedback analytics module can be enhanced with advanced natural language processing (NLP) techniques. This will allow for better sentiment analysis and the ability to process more nuanced user comments.
- **Integration with IoT Devices:** Future versions of the system could incorporate integration with medical IoT devices (such as wearable health trackers) to automatically update patient records in real time. This would allow for continuous monitoring and real-time adjustments to treatment plans.

- **Decentralized Identity Management:** Implementing decentralized identity management (DID) would provide users with more control over their data. By using blockchain for identity verification, patients could share specific health information with authorized parties without relinquishing full control over their data.
- **Smart Contract Enhancements:** The functionality of smart contracts can be further enhanced by incorporating automated workflows for appointment scheduling, lab tests, and insurance claims. This would reduce manual intervention and streamline the processes, improving operational efficiency.
- **Mobile Application Support:** To expand accessibility, the system could be optimized for mobile platforms, allowing users to interact with the system from anywhere at any time, making the healthcare management process more accessible.

REFERENCES

- [1] Mettler, M., "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2016.
- [2] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A., "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016.
- [3] Kuo, T. T., Kim, H. E., Ohno-Machado, L., "Blockchain distributed ledger technologies for biomedical and health care applications," in *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.
- [4] Zhang, P., White, J., Schmidt, D. C., Lenz, G., and Rosenbloom, S. T., "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018.
- [5] Wood, G., "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.
- [6] Kuo, T. T., Kim, H. E., and Ohno-Machado, L., "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.
- [7] Engelhardt, M. A., "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, no. 10, pp. 22–34, 2017.
- [8] Zyskind, G., Nathan, O., and Pentland, A., "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180–184.
- [9] Buterin, V., "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2013.
- [10] Esposito, C., De Santis, A., Tortora, G., Chang, H., and Choo, K. K. R., "Blockchain: A panacea for healthcare cloud-based data security and privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.
- [11] Hasselgren, A., Kravetska, K., Gligoroski, D., Pedersen, S. A., and Faxvaag, A., "Blockchain in healthcare and health sciences—A scoping review," *International Journal of Medical Informatics*, vol. 134, p. 104040, 2020.
- [12] Agbo, C. C., Mahmoud, Q. H., and Eklund, J. M., "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.
- [13] Vazirani, A. A., O'Donoghue, O., Brindley, D., and Meinert, E., "Blockchain vehicles for efficient medical record management," *npj Digital Medicine*, vol. 3, no. 1, pp. 1–5, 2020.
- [14] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2016.
- [15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016.

- [16] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018.
- [17] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," *AMIA Annual Symposium Proceedings*, vol. 2017, pp. 650–659, 2017.
- [18] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.
- [19] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, no. 10, pp. 22–34, 2017.
- [20] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, pp. 180–184, 2015.
- [21] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. 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.
- [22] A. Hasselgren, K. Kravetska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," *International Journal of Medical Informatics*, vol. 134, p. 104040, 2020.
- [23] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.
- [24] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient medical record management," *npj Digital Medicine*, vol. 3, no. 1, pp. 1–5, 2020.
- [25] R. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (HealthChain): Evaluation and proof-of-concept study," *Journal of Medical Internet Research*, vol. 21, no. 8, e13592, 2019.
- [26] X. Liang, J. Zhao, S. Shetty, and D. Li, "Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 113–122, 2021.
- [27] A. Roehrs, C. A. da Costa, R. da Rosa Righi, and D. da Silva V., "Personal Health Records: A Systematic Literature Review," *Journal of Biomedical Informatics*, vol. 71, pp. 70–81, 2017.
- [28] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based secure PHR sharing system," *Future Generation Computer Systems*, vol. 95, pp. 489–500, 2019.
- [29] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 254–269, 2016.
- [30] M. Ho'lbl, M. Kompara, A. Kamis'alic', and L. Nemeč Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.
- [31] M. Linn and M. Koo, "Blockchain for health data and its potential use in health IT and health care related research," *ONC/NIST Use of Blockchain for Healthcare and Research*, 2016.
- [32] J. C. Tseng, Y. H. Liao, and S. L. Jan, "Blockchain for trusted traceability systems," *Computers in Industry*, vol. 100, pp. 29–39, 2018.
- [33] V. Sharma, I. You, and G. Kul, "Socializing drones for inter-service operability in smart cities using blockchain," *Computer Communications*, vol. 153, pp. 229–238, 2020.
- [34] AMR P. Vinayasree, "A Scalable and Secure Blockchain-Based Healthcare System: Optimizing Performance, Security, and Privacy With Adaptive Technologies," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 22, pp. 8084–8103, 2024.
- [35] D.K.G.G 1Mrs. P. Vinayasree, "Tracking of Medicines Over Blockchain," *Paideuma Journal of Research*, vol. 14, no. 7, pp. 40–46, 2021.
- [36] P. Vinayasree, "Tracking of Medicines Over Blockchain," *IOSR Journal of Computer Engineering*, vol. 24, 2022.
- [37] P. Vinayasree and A.M. Reddy, "Blockchain-Enabled Hyperledger Fabric to Secure Data Transfer Mechanism for Medical Cyber-Physical System: Overview, Issues, and Challenge," *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 9, 2023.
- [38] A. Vinayasree and P. Mallikarjuna Reddy, "A Scalable, Secure, and Efficient Framework for Sharing Electronic Health Records Using Permissioned Blockchain Technology," *International Journal of Computer Engineering Science and Emerging Networks (IJCESEN)*, vol. 10, no. 4, pp. 827–834, 2024.
- [39] P. Vinayasree and A.M. Reddy, "A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems," *Concurrency and Computation: Practice and Experience*, vol. 37, no. 3, e8378, 2025.