MedBlock: Blockchain-based data storage system

Prathamesh Ramtirthkar[1], Chinmay Kotecha[2], Kushal Patel[3], Utkarsh Rai[4], Supriya Balote[5]
[1,2,3,4]*Students,* [5]*Professor*
[1,2,3,4,5]*Dept. of Artificial Intelligence & Data Science,*
[1,2,3,4,5]*PES's Modern College of Engineering, Pune, India*

***Abstract*—With the evolving nature of healthcare, the need for secure and efficient data management systems has become the order of the day. Traditional data storage solutions are riddled with significant challenges, including vulnerability to data breaches and poor levels of transparency in transactions between healthcare stakeholders. This research proposes a blockchain-based data storage system designed for the healthcare industry, using Ethereum as the blockchain platform and Solidity as the programming language for smart contracts. The proposed system enhances data integrity and patient trust by allowing secure, tamper-proof, and transparent transactions between doctors and patients. The system architecture includes decentralized storage, smart contracts for permission and transaction management automatically, and an easy-to-use interface for interaction. This research indicates the revolutionary potential of blockchain technology in transforming healthcare data management and, in the process, addressing scalability, interoperability, and regulatory compliance issues. Future research will be focused on enhancing the system and expanding applications to the healthcare ecosystem.**

***Index Terms*—Ethereum Blockchain, Smart contracts, Data storage solutions, Doctor-Patient interaction, Digital health records.**

I. INTRODUCTION

The healthcare industry is facing a growing demand for secure, effective, and reliable data management systems. With exponentially increasing amounts of patient data, the traditional centralized storage model is faced with unprecedented challenges of data breaches, unauthorized access, and ineffective sharing among institutions. Blockchain technology, being decentralized and tamper-proof, is the ideal solution to such an issue. In this paper, we present a blockchain-based storage system for the healthcare industry. Utilizing distributed ledger technology, the proposed system offers secure, transparent, and tamper-proof storage of patient records. It enhances data privacy and integrity, enabling healthcare providers and patients to securely exchange medical information without a central authority. Furthermore, the use of smart contracts enables automated processes such as patient consent management and controlled access to the data. This not only provides security but also adheres to regulatory requirements. The system can revolutionize healthcare data management through the provision of a scalable, secure, and decentralized solution and improved overall healthcare delivery.

II. LITERATURE REVIEW

X. Zhang and Y. Wang. [1] points to the development of an intelligent medical big data system with Hadoop and blockchain technology integration. The article focuses on the issue of managing and securing the huge quantity of medical data produced by healthcare systems. Hadoop, as a distributed big data platform, is employed to manage the storage, processing, and analysis of large data sets efficiently. In the meantime, blockchain technology is incorporated to protect and secure medical records because it is decentralized and tamper-proof. Through the integration of these technologies, the proposed system improves the ability of healthcare organizations to manage data, with accelerated processing and safe sharing of sensitive medical information. The authors emphasize the significance of upholding the integrity and confidentiality of medical data, which is commonly vulnerable to breaches in conventional systems. The research proves that the system can enhance the reliability and efficiency of healthcare services, with real-time data sharing, and minimize the risk of data manipulation. Furthermore, intelligent algorithms used facilitate predictive analytics, which improves clinical decision-making processes. The article concludes by pointing to the potential of the system to transform the

healthcare industry through enhanced data security and operational efficiency.

N.Z. Benisi, M. Aminian, and B. Javadi [2] present a comprehensive survey on blockchain-based decentralized storage networks (DSNs). The study explains how blockchain technology has the potential to transform traditional storage systems by decentralizing data storage, improving security, and enhancing privacy. Traditional centralized storage systems are prone to single points of failure, data leakage, and little control by users over their data. Blockchain, being decentralized and immutable, offers a suitable solution to break through these obstacles by spreading data across multiple nodes, thus preserving data integrity and availability. The survey categorizes various blockchain-based DSN architectures, highlighting their structure, underlying technology, and consensus mechanism. It highlights key features such as enhanced security due to cryptographic mechanisms, enhanced data ownership, and cost-effectiveness due to the absence of middlemen. The study also surveys existing projects and platforms that have utilized blockchain for decentralized storage, including IPFS and Filecoin, and their strengths, weaknesses, and potential applications. In conclusion, the authors argue that while blockchain-based DSNs have much to offer in terms of security and decentralization, they are constrained by scalability, network performance, and power consumption. The paper calls for further research to overcome these drawbacks and enhance the practical application of blockchain in decentralized storage.

Y. Xu's [3] research paper presents "Section-blockchain," a new blockchain protocol for minimizing storage needs without compromising decentralized storage architecture feasibility. The research addresses a major flaw of conventional blockchain systems: the constantly growing size of the blockchain, which becomes a storage burden and a scalability bottleneck. The Section-blockchain protocol presents a mechanism that segments the blockchain into sections, enabling efficient data management by storing only necessary data in some sections and keeping the whole chain safe and intact. The method minimizes the overall storage burden without sacrificing the decentralized nature or security aspects inherent in blockchain technology. The protocol provides the basis for an "autotrophic decentralized storage architecture," which controls its storage autonomously while ensuring scalability and redundancy of data. By optimizing the blockchain's storage structure, the system becomes more responsive to real-world applications where data growth is an issue. The research also explains how Section-blockchain can improve in terms of energy efficiency and performance, especially in scale-out distributed networks. Xu concludes that the proposed protocol can greatly improve the efficiency of blockchain-based systems, making them more sustainable and feasible for a wide range of decentralized storage applications.

X. Liu, Y. Hong, and J. Sun [4] present a blockchain-based platform for safe storage and sharing of medical data. To address the increasing data privacy, security, and interoperability challenges in healthcare, the authors propose using blockchain technology as a remedy for these issues. The system is designed to prohibit tampering or manipulation by unauthorized parties and ensure that the medical data is stored in a decentralized manner to enhance data integrity. Blockchain technology's immutability and transparency are best suited to the management of sensitive medical records and ensuring that the control over their data is maintained by the patients. The paper explains the mechanism of the system for secure, efficient sharing of medical data among healthcare providers, patients, and third parties like insurance providers without the loss of their privacy. Data access control is automated and enforced through smart contracts, which provide access to specific medical records to only authorized stakeholders. The authors also address future scalability challenges and propose optimizations in processing large amounts of medical data. Overall, the study concludes that the vast potential of blockchain to enhancing data security, patient confidentiality, and efficiency in healthcare service with a more stable and transparent mechanism for data sharing.

X. Wang [5] discusses the use of data storage management systems in blockchain-based technology for improved data processing and security in different industries. The study aims to develop a scalable and efficient data storage management system that leverages blockchain's decentralized and tamper-proof nature. The system is supposed to solve data integrity, security, and access control problems typically faced by traditional storage systems. With the use of blockchain, the authors make sure that data not only receives secure storage but is also processed efficiently, and transparency and traceability are

feasible throughout the storage network. The technical architecture of the proposed system is discussed in the paper, including important blockchain features such as distributed ledgers, consensus mechanisms, and smart contracts to increase the level of security and flexibility in data storage. The study also discusses the feasibility of the system in finance, healthcare, and supply chain management industries, where secure and fault-free data management is important. The authors highlight the advantages of this system in terms of increased data redundancy, minimized risk of data breaches, and increased control by users over their data. In short, the study proves the efficiency of blockchain-based data storage management systems in changing data security and efficiency across a wide range of industries.

P. R. Nair and D. R. Dorai [6] compare and evaluate the performance and security of two of the most widely used consensus algorithms employed in blockchain, i.e., Proof of Work (PoW) and Proof of Stake (PoS). Both algorithms are crucial in maintaining the integrity and security of blockchain networks. Proof of Work, employed in widely used blockchains like Bitcoin, requires participants (miners) to solve a complicated math puzzle, securing the network at the cost of high energy consumption and slow transaction speed. Proof of Stake, on the other hand, selects validators based on how much cryptocurrency they hold and are willing to "stake" as collateral, presenting an energy-efficient alternative with quicker transaction processing. The paper discusses the trade-offs of PoW and PoS in a systematic manner, specifically regarding scalability, energy efficiency, transaction throughput, and resistance against different types of attacks like double-spending. It states the fact that while PoW is more mature and robust as regards security, PoS presents a cleaner and more scalable solution towards future uses of blockchain, most prominently the reduction of the carbon footprint. The study concludes on the lines of mentioning that PoS has huge potential to be the consensus method of choice for its improved performance and energy efficiency, although it grapples with issues related to risks of centralization.

A. Abuhashim and C. C. Tan [7] describe the design and implementation of smart contracts on blockchain platforms, noting their revolutionary capabilities in automating and securing transactions across a variety of industries. Smart contracts are self-executing contracts whose terms are embedded directly into code. Smart contracts automate and enforce terms automatically without intermediaries, hence enhancing trust, reducing transaction costs, and eradicating the risk of human error or forgery. The article describes a variety of smart contract designs for various applications, including financial transactions, supply chain management, and healthcare data exchange. The authors note the challenge of designing effective and secure smart contracts, particularly in dealing with complex conditions, enabling scalability, and protecting against exposures such as bugs and hacking. The article also notes the limitations of existing blockchain platforms such as Ethereum in supporting high-volume transactions of smart contracts and describes possible solutions to improve performance, including sharding and off-chain computation. The authors highlight the importance of formal verification methods in ensuring the correctness of smart contracts, noting that any flaw can lead to heavy financial or data losses. Generally, the article captures the widespread use of smart contracts and the need for extensive design to reap maximum potential in blockchain applications.,

III. PROPOSED SYSTEM

A distributed web-based health system that makes use of blockchain technology, i.e., Ethereum and MetaMask, a widely used digital wallet, and interoperates with it using MetaMask to securely authenticate and manage their identities. MetaMask manages the generation and storage of private keys, enabling users to sign up and safely log in to the system. The private key plays a critical role in signing transactions on the Ethereum blockchain to ensure secure and tamper-evident communication. When a physician registers through MetaMask, their private key is associated with an Ethereum account that communicates with the blockchain. The Ethereum blockchain acts as a decentralized ledger, ensuring transparency, security, and immutability of all healthcare transactions and medical records. The API of the system provides interactions between the user and the blockchain, allowing secure execution of smart contracts or handling of health data. With the successful completion of the transaction, the Ethereum blockchain confirms the exchange, providing for the security and transparency of every action within the system. With this decentralized scheme, patient data privacy and security are increased, and the dependence

on centralized intermediaries is removed, building trust among patients and healthcare providers.

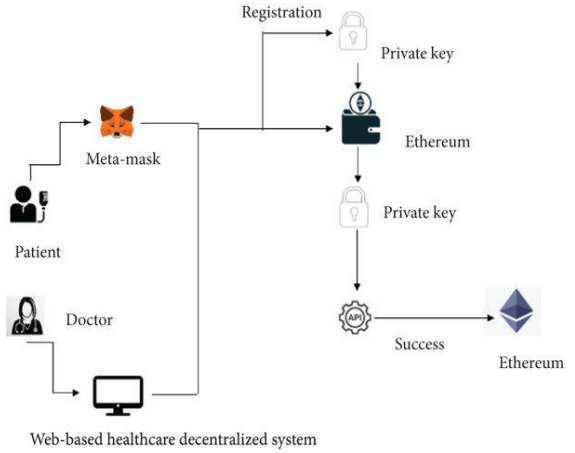
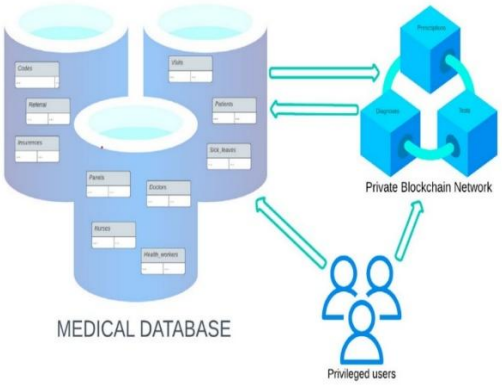


Fig. 1. Proposed Methodology

A hybrid health data management system combining a conventional medical database with a private blockchain network. The medical database retains general healthcare data, such as patient visits, referrals, insurance, and healthcare staff information, while the private blockchain protects more sensitive information like prescriptions, diagnoses, and test results. The blockchain provides privacy, immutability, and security, blocking unauthorized access or tampering. Authorized users, like physicians, nurses, and medical administrators, get access to the information through the blockchain, which has all activity logged and checked securely. The system provides a clear audit record, making management accountable for maintaining patient data. The system demarcates the day-to-day information from urgent medical records and uses blockchain's decentralized nature to secure data better. In doing so, it enables healthcare professionals to safeguard confidential patient data while ensuring effective access to less sensitive administrative information via the medical database. This design facilitates both data privacy and operational effectiveness in healthcare.



IV. RESULTS AND DISCUSSION

We successfully validated MEDBLOCK using data from 25 patients and 10 doctors. The system securely managed and shared medical records via blockchain, ensuring accurate, transparent access for all participants. It proved reliable, user-friendly, and effective in maintaining data integrity and confidentiality. This validation marks a key milestone, highlighting MEDBLOCK's readiness for real-world use in delivering secure, efficient, and decentralized medical record management within healthcare environments.

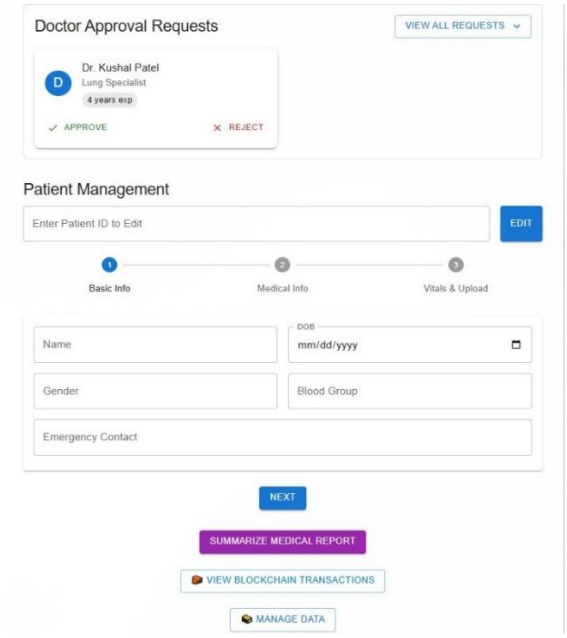


Fig. 2. Admin Dashboard

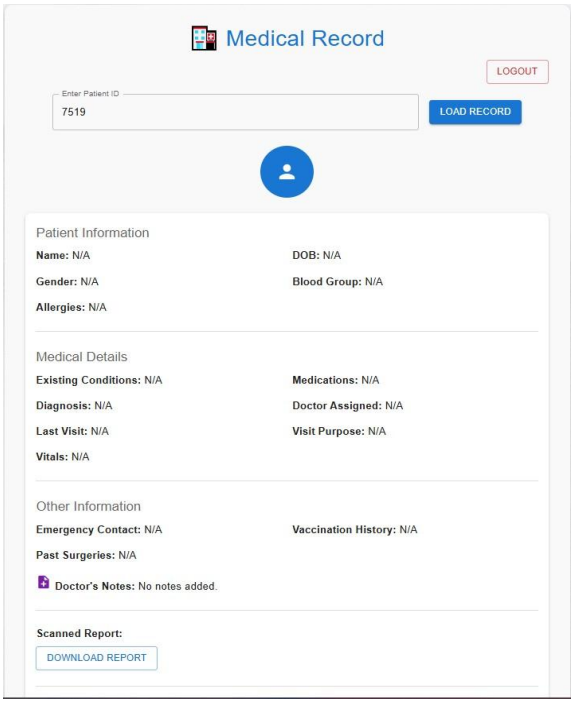


Fig. 3. Doctor login

We successfully validated MEDBLOCK using data from 25 patients and 10 doctors. The system securely managed and shared medical records via blockchain, ensuring accurate, transparent access for all participants. It proved reliable, user-friendly, and effective in maintaining data integrity and confidentiality. This validation marks a key milestone, highlighting MEDBLOCK's readiness for real-world use in delivering secure, efficient, and decentralized medical record management within healthcare environments.

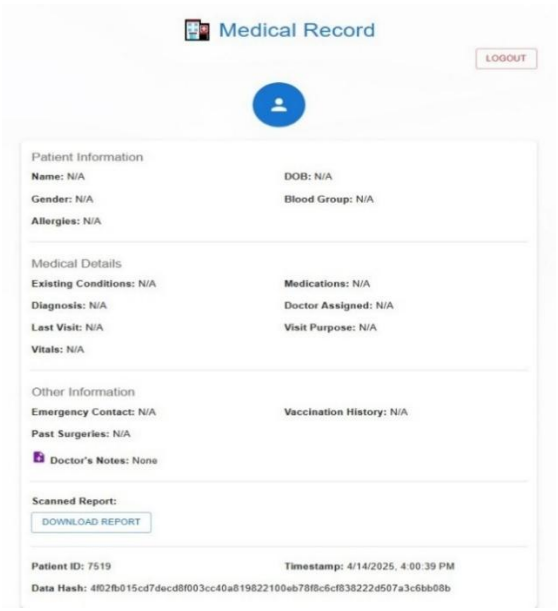


Fig. 4. Patient Login

The system is designed to be highly scalable and efficient, making it adaptable to various healthcare environments. It allows for the quick input and retrieval of medical records, ensuring a smooth experience for both doctors and patients. Different forms of medical data, including text-based records, images, CT scans, and X-rays, can be securely stored and accessed. Its underlying architecture supports seamless expansion, enabling the addition of more users without affecting performance or speed. By combining fast processing, secure data handling, and support for diverse medical formats, the platform provides a reliable solution for managing comprehensive healthcare information.

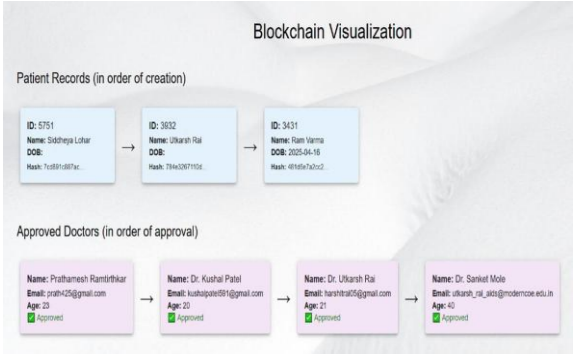


Fig. 5. Block Generation

V. CONCLUSION

In summary, the use of blockchain technology for medical data storage is a revolutionary step in the healthcare industry. Utilizing its natural attributes—decentralization, immutability, increased security, and patient ownership of data—blockchain solves the paramount issues related to conventional data storage systems. The nature of medical records as sensitive information, combined with the rising number of data breaches and privacy issues, calls for a strong solution that blockchain easily offers.

The decentralized architecture of blockchain eliminates the risks inherent in centralized databases by ensuring that patient data is safe and impenetrable. Moreover, the immutability of blockchain data ensures the integrity of medical data, building confidence among healthcare professionals and patients alike. Giving control to patients over their medical data not only boosts privacy but also promotes active involvement in their health journey.

Additionally, the ability of smart contracts to automate processes like consent management simplifies operations and minimizes administrative tasks, enabling healthcare providers to concentrate on providing quality care. With continued interoperability, blockchain can enable easy data sharing across platforms, encouraging improved care coordination and holistic patient management.

REFERENCES

[1] X. Zhang and Y. Wang, A study on integrating Hadoop and blockchain technologies for intelligent handling of medical big data, EURASIP Journal on Wireless Communications and Networking, Special Section 2021, pp. 1–21, 2021. Available: https://jwcneurasipjournals.springeropen.com/articles/10.1186/s13638-021-01999-1

[2] N. Z. Benisi, M. Aminian, and B. Javadi, An overview of decentralized storage solutions using blockchain infrastructure, Journal of Network and Computer Applications, vol. 162, July 2020. Available: https://www.sciencedirect.com/science/article/abs/pii/S1084804520301302?via%3Dihub

[3] Y. Xu, Section-blockchain: A low-storage blockchain protocol forming the base of an autonomous decentralized storage model, in Proc. 23rd Int. Conf. on Engineering of Complex Computer Systems (ICECCS), Dec. 2018. Available: https://ieeexplore.ieee.org/document/8644745

[4] X.. Liu, Y. Hong, and J. Sun, A medical data management and sharing system using blockchain, 2022 IEEE Int. Conf. on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2022. Available: https://ieeexplore.ieee.org/document/9983744

[5] X. Wang et al., Implementing a data storage management approach in blockchain technologies, 2023 IEEE 2nd Int. Conf. on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 2023. Available: https://ieeexplore.ieee.org/document/10111326.

[6] P. R. Nair and D. R. Dorai, A comparative analysis of blockchain consensus methods: Proof of Work vs. Proof of Stake, 2021.

[7] A. Abuhashim and C. C. Tan, Design approaches for smart contracts in blockchain-based applications, 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020..

[8] Z. Yuan, J. Wu, J. Gong, Y. Liu, G. Tian, and J. Wang, Self-auditing mechanism with batch verification for decentralized blockchain storage, Wireless Communications and Mobile Computing, vol. 2022.

[9] V. A. Kanade, A blockchain-powered distributed network architecture addressing modern data storage challenges, 2021.

[10] S. S. Fateminasab, S. Memarian, S. R. K. Tabbakh, and M. C. Romero-Ternero, Survey on open data storage and retrieval in blockchain ecosystems, 2024 10th Int. Conf. on Web Research (ICWR), Tehran, Iran, 2024.

[11] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, A blockchain framework to support secure health data exchange, 2018

[12] F. Wang, J.-t. Zhou, H. Wang, and X. Guo, Blockchain-enabled method for ensuring consistent storage across multi-cloud platforms, 2022.

[13] D. Xia, P. Yao, J. Liang, and W. Chen, RemoteBlock: A scalable storage model enhancing Ethereum via blockchain, 2024 IEEE

4th Int. Conf. on Power, Electronics and Computer Applications (ICPECA), Shenyang, China, 2024.

[14] A. Rustemi, V. Atanasovski, and A. Risteski, Survey on privacy-preserving techniques and blockchain-based storage, 2022.

[15] J. S. Gazsi, S. Zafreen, G. G. Dagher, and M. Long, VAULT: Secure and collaborative access protocol for scalable blockchain data, 2021.

[16] M. Shaikh, C. Shibu, E. Angeles, and D. Pavithran, Blockchain-based architecture for IoT data storage, 2021

[17] H. G. Do and W. K. Ng, A blockchain-oriented secure data storage system with private keyword search, 2017 IEEE World Congress on Services (SERVICES), Honolulu, HI, USA, 2017.

[18] Z. Wang, Q. Chen, and L. Liu, Secure and private data sharing protocol based on permissioned blockchain, IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10698–10707, June 15, 2023.

[19] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, BlockIPFS: Integrating blockchain with IPFS for trustworthy and traceable forensic data, 2019.

[20] L. R. Soares, J. C. Nobre, and G. Kerschner, Secure storage architecture for resource-limited healthcare environments via blockchain, 2023 IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 2023.