OPEN ACCESS Freely available online

Journal of Medical Diagnostic Methods

Review Article

Proof-of-Trust-in-Expertise (PoTE): A Consensus Mechanism for Healthcare based Consortium Block Chains

Karan Singh Bagga, Akhilesh Kasturi*, Sonaakshi Shri Kunrarasu, Beena BM

Department of Computer Science and Engineering, Amrita Viswa Vidyapeetham, Tamil Nadu, India

ABSTRACT

The growing adoption of block chain in healthcare promotes reliable patient data management. Establishing a consortium block chain network interconnecting hospitals, diagnostic laboratories and pharmaceutical entities ensures real-time tamper-evident access to patient records. This decentralized model enhances the data exchange efficiency and fortifies security through immutable audit trails. Beyond expediting emergency access to comprehensive medical histories, block chains prevent authoritative data control and commercial exploitation. Patient empowerment and trust are pivotal, prompting our paper to introduce Proof-of-Trust-in-Expertise (PoTE), a consensus mechanism leveraging medical professionals' trust and expertise, an innovative departure from Proof-of-Work (PoW) and Proof-of-Stake (PoS).

Keywords: Consortium blockchain; Healthcare; Decentralized application; Privacy; Proof-of-Trust-in-Expertise (PoTE)

INTRODUCTION

The healthcare system is complex and ever-changing. It is a blend of both socialist (public sector) and market-driven (private sector) programs, involving many different stakeholders. The goal of the system is to provide high-quality affordable care to the population. The traditional approach to healthcare data management presents several challenges, primarily in the areas of security, privacy and interoperability. These issues develop as a result of reliance on centralised databases, which are subject to cyberattacks and unauthorised access. Unfortunately, privacy incidents in healthcare, including the exposing of sensitive patient information, are not uncommon. Moreover, the fragmented nature of healthcare data across various institutions impedes effective information exchange, resulting in incomplete patient records and hindered or inaccurate diagnoses [1].

Block chain offers a viable solution to the issues that the medical sector is facing. Through the immutability and cryptographic properties, it preserves the integrity of healthcare data offering a decentralised and secure framework. This reduces the risk of tampering or unauthorized alterations. Additionally, the transparent and distributed nature of block chain enhances interoperability, enabling the seamless sharing of patient information among authorized stakeholders. By addressing these issues, the integration of block chain in healthcare aims to establish a more secure, transparent and collaborative environment for managing sensitive medical data.

Centralized approach

In the evolving landscape of healthcare information management, the conventional approach of centralized storage systems has served as a foundational model; however, its deployment is not without consequential shortcomings. As healthcare institutions increasingly grapple with the complexities of patient data management, a few challenges surface within the centralized paradigm. The pivotal drawbacks of this method are as follows:

No coordination: The main disadvantage is that a hospital may not be able to access the records of patients from a different hospital.

Security and privacy concerns: A centralized system can be a tempting target for hackers and a breach can expose the sensitive information of many patients. In addition, there is a risk that unauthorized individuals can gain access to patient records.

Vulnerability to outages: If the central system decreases, it could impact the ability of healthcare providers to access important

Correspondence to: Akhilesh Kasturi, Department of Computer Science and Engineering, Amrita Viswa Vidyapeetham, Tamil Nadu, India; E-mail: bl.en.u4cse19003@bl.students.amrita.edu

Received: 28-May-2024, Manuscript No. jmdm-24-31751; **Editor assigned:** 03-Jun-2024, PreQC No. jmdm-24-31751 (PQ); **Reviewed:** 17-Jun-2024, QC No. jmdm-24-31751; **Revised:** 14-Apr-2025, Manuscript No. jmdm-24-31751 (R); **Published:** 21-Apr-2025, DOI: 10.35248/2168-9784.25.14.510

Citation: Bagga KS, Kasturi A, Kunrarasu SS, Beena B M (2025) Proof-of-Trust-in-Expertise (PoTE): A Consensus Mechanism for Healthcare based Consortium Block Chains. J Med Diagn Meth. 14:520.

patient information. This can cause delays in care and potentially harm the patients.

Inefficiency: A centralized system can be slow and cumbersome to use because all requests for patient information must be routed through a single entity. This can lead to delays and inefficiencies in the healthcare systems [2].

An alternative to a centralized approach to storing health records is a decentralized system in which patient data are distributed across multiple locations. Some potential advantages of a decentralized approach include the following:

Better coordination of care: In a decentralized system, patient data are accessible to authorized healthcare providers from any location. This can facilitate better communication and coordination of care among healthcare providers.

Improved security and privacy: Because patient data is not kept in one place in a decentralized system, hackers have a harder time accessing it. Additionally, patients can have more control over those who have access to their personal information. Hospitals will not be able to sell the patient data.

Increased reliability: A decentralized system is less vulnerable to outages as patient data are stored in multiple locations. This means that healthcare providers can still access important patient information, even if a part of the system goes down. Block chain enables secure and transparent data sharing among numerous parties. Patient records are kept on numerous nodes in a decentralized healthcare system. This will enable authorized healthcare providers to view and update patient records in real time while ensuring the data's security and integrity [3].

LITERATURE REVIEW

Seeks to tackle the challenges and dilemmas encountered when opting for block chain technology. Given the nascent nature of block chain as an emerging technology aimed to alleviate security problems across multiple domains, there is widespread misunderstanding over the appropriate application of block chain and situations when its integration may be unnecessary. The major goal is to examine the range of applications where block chain technology is effective and conversely, to identify instances where its adoption may be unnecessary. The study's key contributions include a detailed overview of block chain technology, covering both instances that need its use and those where alternate solutions may be more appropriate.

The healthcare system, encompassing medical service providers, emergency services and health-oriented service users, faces escalating security and privacy breaches, which are particularly evident in the increasing digitization of medical care. Security breaches and unauthorized access to patient records have become pervasive, necessitating innovative solutions. By providing safe storage, limited access and adherence to data protection rules, block chain technology has emerged as a possible route for addressing these difficulties. Block chain operates as a distributed and immutable database administered by authenticated nodes, ushering in a new era in healthcare data administration. To assure data integrity and security, it employs cryptographic signatures and consensus techniques. Block chain development has advanced from cryptocurrency-focused applications to including smart contracts, with the current focus on non-financial industries like as healthcare. Block chain in healthcare addresses issues of data ownership, sharing and accessibility, giving patients more control over their health records. This technology facilitates secure, transparent and accountable management of health data, mitigating the risks associated with centralized data storage. Despite the transformative potential of block chain, its widespread adoption faces challenges related to organizational, social and implementation. Addressing issues such as security concerns, governance and awareness among stakeholders is crucial for successful block chain integration in the healthcare sector. While existing systematic literature reviews offer insights into block chain patterns and applications, there is a need for focused discussion on the implications of block chain adoption, highlighting research gaps and areas for future exploration [4].

Aims to provide a thematically organized classification of the existing literature, identify gaps and recommend areas for forthcoming research to enrich the progressing domain of block chain in healthcare.

Focuses on the development of a system that empowers patients with convenient access to their medical records, eliminating the dependence on centralized oversight. Block chain technology has emerged as a pivotal enabler, showcasing its attributes as a distributed database fortified by advanced cryptographic techniques and consensus mechanisms. By design, the block chain infrastructure offers a secure, transparent and immutable ledger for recording and validating healthcare transactions. Moreover, a Decentralized Application (DApp) strategically layered on the block chain platform has emerged as a potent solution. This DApp connects patients and healthcare professionals by enabling confidential and effective accessibility to and exchange of medical records. Within this context, paramount considerations encompass assurance of data security, privacy preservation and seamless record accessibility.

Block chain technology offers a promising avenue for the enhancement of healthcare data management, primarily addressing critical aspects of security, privacy, interoperability, accessibility, traceability and transparency, as underscored in. At its foundation, the block chain employs complex cryptographic approaches and consensus procedures to strengthen both the safety and permanence of the data it stores. Block chain's decentralised and distributed nature adds an inherent degree of resilience against unauthorised tampering and data breaches, enhancing its trustworthiness. Moreover, the utility of block chain extends to fostering the interoperability of healthcare data. This paves the way for diverse healthcare providers and systems to securely and efficiently access and exchange data, thereby contributing to the enrichment of care quality and expeditiousness. Additionally, block chain technology assumes the role of custodian for immutable transaction records, forming a robust foundation for data integrity and authenticity assurance, thereby establishing a dependable trail of data provenance [5].

In the integration of block chain technology with healthcare data security was meticulously delineated. This comprehensive

approach encompassed several stages. First, this study focuses on identifying the multifaceted challenges and opportunities intrinsic to applying block chain in healthcare data security. This initial assessment served as the foundation for subsequent stages of the research. Second, this study delves into the evaluation of the appropriate block chain platforms and technologies. This pivotal step entails a thorough examination of available options to ascertain their compatibility with the specific needs of healthcare data security. The subsequent phases of research revolve around the design and implementation of a block chain-based solution. Critical considerations span architectural elements, encompassing the data model, consensus mechanisms and security protocols. The integration of this solution into the existing healthcare systems and processes constitutes an integral part of this endeavour. To conclude, this research follows a robust methodology, culminating in the testing and evaluation of block chain-based solutions. These evaluative procedures encompass pilot studies, usability testing and rigorous security assessments to confirm that the solution aligns with the desired security and privacy requirements.

As emphasized in the integration of a database with a block chain system is critical for ensuring the efficiency and performance of the overall system. This integration should be executed with meticulous attention to detail, with the paramount objective of not adversely affecting system performance. Furthermore, this study highlights the critical need of maintaining database security during the integration process. It emphasises emphatically that the integrity and security of the database's data must not be jeopardised in any way during integration with the block chain technology. To achieve these dual imperatives, this paper suggests a set of guiding principles, such as scalability, performance, security and seamless integration with a block chain system [6].

The utilization of block chain technology has garnered significant attention for providing decentralized solutions across diverse applications and ensuring the participation of honest entities within the system. Its capacity to enable transactions in cryptocurrencies among mutually distrusting parties without the requirement of a trusted intermediary underscores its potential impact. Block chain's intrinsic feature of transparency, manifested at every level and transaction, exposes data to all involved parties, establishing a decentralized framework, but one without inherent privacy. Recognizing the complementary attributes of block chain and secure computation, the convergence of these two concepts holds promise for yielding practical solutions in decentralized distributed computing applications, seamlessly amalgamating the advantages of decentralization with enhanced data privacy.

Block chain technology has emerged from the realm of speculation in recent years, turning into a viable tool with a slew of built-in characteristics such as distributed ledgers, decentralised storage, authorization, privacy and inviolability. Its application has extended beyond conceptual frameworks to tangible implementations across various industrial sectors, with healthcare emerging as a focal point for exploration. Within the healthcare domain, where adherence to stringent authentication, interoperability and record-sharing requirements is imperative because of regulatory frameworks researchers in both academia and industry have focused on tailoring block chain applications to meet healthcare-specific demands.

Block chain, a consensus-based computing paradigm, has revolutionized transaction recording by eliminating reliance on third-party intermediaries. The application of this technology has shifted towards domains with frequent transactions. Addressed the prevailing malpractices in land registries, focusing on leveraging the ethereum platform for secure and transparent transactions. This research uses ethereum to construct a secure digital ledger for land-related transactions, establishing quick, safe and immutable contracts between reliable parties. The distributed nature of transaction tracking, which utilizes a shared database with backup facilities, guarantees a singular owner for enhanced reliability in the land registry process [7].

In healthcare institutions, the collection of sensitive patient information, underscores the critical importance of data security. Given the susceptibility of healthcare firms to cyberattacks, with phishing emails accounting for a significant portion, safeguarding patient data has become paramount. Block chain technology offers a robust solution by representing various components and their interrelationships, thereby providing a secure framework for healthcare data management. Elucidates the collaborative functioning of diverse components within the block chain framework, with the customer placed at the core of pivotal processes. The integration of the user's social security number into the profile establishes a foundation for implementing security measures such as One-Time Passwords (OTPs) or secure messages (mses). Despite being accessible from different points within the network, the system maintains centralized operation. Upon user permission, biometric data becomes instrumental, ensuring secure access to patient records. Notably, when a patient visits a hospital, their access is tailored to their specific medical history and the patient retains control over selectively sharing this information with the visited hospital. This patient-centric approach underscores the decentralized nature of block chain in healthcare, placing patients in charge of their medical records.

The paper emphasizes the significance of predicting and managing COVID-19 infections. The integration of wearable devices, block chain-based consent management and federated learning presents a holistic approach to address the privacy challenges associated with health data. The research utilized machine learning, specifically federated learning, to train models for COVID-19 prediction. Federated learning enables on-device learning without centralizing user data and addressing privacy concerns. This study aids in providing early and accurate predictions while maintaining user control over data sharing.

Because of concerns about diploma forgery and the illegal sale of counterfeit certificates, the advent of enhanced worldwide mobility and an increasing number of overseas learners has created issues in the storage and exchange of educational data. Offers unique solutions for block chain-based certificate administration systems in higher education.

Recent improvements in Internet of Things (IoT) and mobile internet technologies have had a significant impact on the growth of Vehicular Adhoc-Networks (VANETs) towards the Internet of Vehicles (IoV). The internet of automobiles introduces a paradigm in which automobiles use data obtained from other automobiles and roadside infrastructures to improve decision-making capabilities, particularly while navigating unforeseen scenarios. However, the proliferation of connected vehicles brings forth heightened security and privacy concerns, necessitating innovative solutions to prevent malicious activities such as the transmission of falsified information and tampering with critical communication data. Proposes leveraging real-time block chain to fortify the internet of vehicles that serves as a distributed ledger which ensures authentication and maintains secure communication channels between vehicles.

Architecture

The proposed decentralized architecture comprises two distinctive nodes crucial to the functioning of the healthcare block chain network: Government and hospital nodes. Acting as the central governing authority, the government node assumes the primary responsibility of overseeing the composition of the network. Its exclusive privileges encompass the addition or removal of hospitals from the network, thereby reinforcing regulatory control. In addition, government nodes play a vital role in ensuring the integrity of individual hospitals within the network, validating their compliance with predefined standards and protocols.

The distributed network, on the other hand, hosts hospital nodes, which are in charge of producing new transactions and ensuring the general reliability of the block chain. These nodes are critical to the block chain's distributed ledger. Their responsibilities extend to the continuous validation of block chain integrity, ensuring that the ledger remains untampered and cryptographic hashes align seamlessly. This collaborative architecture not only establishes a secure and decentralized data-sharing environment, but also serves as a foundation for cultivating trust and transparency within the intricate healthcare ecosystem (Figure 1).

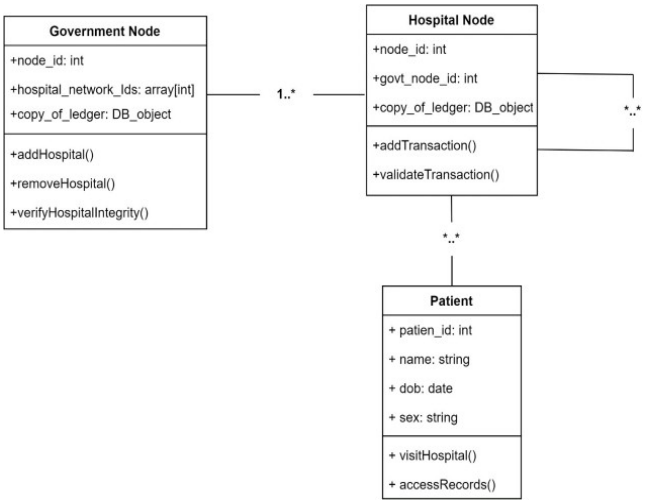

Figure 1: Blockchain architecture.

DISCUSSION

Consensus mechanism

Proof of Stake (PoS) is a block chain network consensus process used to validate and add new transactions to the block chain. It is intended to be an alternative to the Proof-of-Work (PoW) process used in cryptocurrencies such as bitcoin. PoS works differently and offers various benefits, including energy efficiency and security. The proof of stake works in the following manner:

Validators: Validators are chosen to build new blocks and confirm transactions in a PoS system based on the amount of cryptocurrency they own and are prepared to "stake" as collateral.

Staking: To become a validator, individuals or entities need to stake a certain amount of cryptocurrency in the network. The higher the stake, the higher the chance of being selected as a validator [7].

Block creation: Validators create new blocks and add transactions to the block chain in sequence. The likelihood of being selected to build a block is proportional to the stake.

Validation and rewards: Validators are incentivized to perform honestly since they risk losing their stake if they validate false transactions or attempt to scam the system. Honest validators, are rewarded for their services with transaction fees and in some cases, with newly minted cryptocurrencies.

Security: PoS is considered secure because it is expensive for malicious actors to accumulate enough stakes to control the network. In PoW, attackers need to invest in expensive mining equipment, whereas in PoS, they need to acquire a significant amount of cryptocurrency/stake.

The proof of stake mechanism relies on validators with a financial interest in the network's success in maintaining its security and integrity. It is energy efficient and has gained popularity in recent years as an eco-friendly alternative to PoW.

We propose a novel consensus protocol called Proof-of-Trust-in-Expertise (PoTE), which is a faster and more performant modification of the existing proof-of-stake mechanism, with the intent of bestowing upon its role as the consensus algorithm for the block chain solution referenced above.

Proof-of-trust-in-expertise

In our proposed consensus mechanism, Proof-of-Trust-in-Expertise (PoTE), each healthcare institution, encompassing hospitals and clinics, assumes the role of a validator within the block chain network. To ensure fair and balanced participation in the validation process, we advocate a stake quantification model that correlates with the square root of the count of actively employed medical practitioners specific to each healthcare institution, herein referred to as a hospital. This innovative approach aims to foster decentralization and prevent the concentration of stakes in larger hospitals by introducing a regulatory effect through the application of the square root function.

Furthermore, to incentivize active participation and contribution to the block chain network, we introduce a financial mechanism. Hospitals are eligible to receive tax benefits structured in accordance with an order N function, directly proportional to the quantity of medical practitioners. This strategic alignment seeks not only to acknowledge the essential role played by healthcare institutions in the network, but also to stimulate a consistent motivation for these institutions to maintain and potentially increase their medical practitioner count.

Moreover, these tax benefits are designed not merely as a means to offset the increased efforts required to uphold the integrity of the block chain, but more significantly, to actively stimulate a heightened demand for medical practitioners within the market. These benefits contribute to the enhancement of salaries for doctors by directly influencing the competitive landscape of healthcare employment and fostering a more dynamic and robust healthcare ecosystem.

Validation of the treatment prescription follows a meticulous process. Upon receiving treatment at a specific hospital, the system initiated a validation protocol. In this process, three hospitals were randomly selected from the network to independently assess and validate the diagnoses. The selection probability for each hospital is directly proportional to its stake in the network [8].

The selection of hospitals at random for validation serves several purposes. First of all, it adds a layer of decentralization and impartiality, preventing any single hospital from wielding excessive influence over the validation process. Second, it uses stake-based selection to prioritize hospitals that are more committed to the network's integrity and security.

Validation comprises a collaborative endeavor between the three hospitals chosen. For the provided diagnosis to be deemed valid and eligible for the addition of a new block to the block chain, consensus among all three hospitals is required. This stringent requirement underscores the significance of shared professional agreement on the accuracy of the diagnosis.

This approach adds a robust layer of verification to healthcare transactions recorded on the block chain. By necessitating a consensus among multiple independent healthcare institutions, the system minimizes the risk of inaccurate or maliciously provided information.

Future scope

Several critical factors emerge as we define the long-term scope of our block chain-based healthcare solution [9].

Regulatory compliance: As healthcare data are highly regulated, future work should address compliance with healthcare laws in India, such as the personal data protection bill and other relevant regulations. Developing block chain solutions that adhere to these legal requirements is essential for the Indian healthcare sector.

Security and resilience: The proposed system aims to improve security, but it should also address potential threats and vulnerabilities. Continuous research on security measures and methods to ensure the system's resilience against attacks will be necessary.

User-friendly interfaces: To encourage widespread adoption, user-friendly interfaces for both patients and healthcare professionals should be a focus. Future work can explore the development of intuitive applications and tools to access and interact with the block chain network.

Long-term sustainability: Examine the long-term sustainability of the tax benefits and incentives proposed in the PoTE consensus mechanism. Assess how they evolve over time and adapt to changing healthcare needs [10].

CONCLUSION

In conclusion, a major development in blockchain technology designed to satisfy the particular requirements of the healthcare industry is the Proof-of-Trust-in-Expertise (PoTE) consensus mechanism. Existing issues in healthcare data management, such as security, privacy and interoperability, demand the development of novel solutions. By incorporating the trust and expertise of medical professionals into the consensus process, our approach strives to establish a secure, transparent and efficient framework for healthcare data exchange, ultimately contributing to the enhancement of patient care and the overall healthcare ecosystem.

REFERENCES

1. Saeed H, Malik H, Bashir U, Ahmad A, Riaz S, Ilyas M, et al. Block chain technology in healthcare: A systematic review. PloS One. 2022;17(4):e0266462.
2. Tith D, Lee JS, Suzuki H, Wijesundara WM, Taira N, Obi T, et al. Application of block chain to maintaining patient records in electronic health record for enhanced privacy, scalability and availability. Healthc Inform Res. 2020;26(1):3-12.
3. Usman M, Qamar U. Secure electronic medical records storage and sharing using block chain technology. Procedia Comput Sci. 2020;174:321-327.
4. Khan AI, ALGhamdi AS, Alsolami FJ, Abushark YB, Almalawi A, Ali AM, et al. Integrating block chain technology into healthcare through an intelligent computing technique. Acad J Comput Mater Contin. 2022:2835.
5. Raikwar M, Gligoroski D, Velinov G. Trends in development of databases and block chain. arXiv preprint arXiv. 2020:05687.
6. Innocent AA, Prakash G. Block chain applications with privacy using efficient multiparty computation protocols. In2019 PhD colloquium on ethically driven innovation and technology for society (PhD EDITS). 2019:1-3.
7. McGhin T, Choo KK, Liu CZ, He D. Block chain in healthcare applications: Research challenges and opportunities. J Netw Comput Appl. 2019;135:62-75.
8. Ramar K, Shanmugasundaram H, Andraju BP, Baskar S. Digital healthcare using block chain. In2022 1st International Conference on Computational Science and Technology (ICCST). IEEE. 2022: 651-655.
9. Reddy TR, Beena BM. AI Integrated Blockchain Technology for Secure Health Care-Consent-Based Secured Federated Transfer Learning for Predicting COVID-19 on Wearable Devices. InInternational Conference on Innovative Computing and Communications: Proceedings of ICICC. 2022:345.

10. Rani PS, Priya SB. Trustworthy block chain based certificate distribution for the education system. In2022 International Conference on Computer, Power and Communications (ICCPC). 2022:393-397.