Journal of Inventive and Scientific Research Studies (JISRS)
www.jisrs.com Vol: II, Issue: 2 December 2024 ISSN: 2584-0630 (Online)

BLOCKCHAIN: BALANCING PRIVACY AND ACCESSIBILITY IN EHR DATA: A REVOLUTIONARY APPROACH IN HEALTH DATA MANAGEMENT

K. MANIKANDAN
Assistant Professor, Department of Information Technology
G. Venkataswamy Naidu College (Autonomous), Kovilpatti
E-mail: kmanikandan901@gmail.com

Received: July 06, 2024, **Accepted**: October 28, 2024, **Online Published**: December 15, 2024

ABSTRACT

A blockchain-powered health information ecosystem offers a promising solution to the often-discussed issue of lifelong patient health data management. This challenge involves balancing patient privacy with the increasing demand for data from research and policy-making institutions. While the availability of such data is crucial in emergencies and significantly supports research, population health management, and development activities, its misuse can lead to serious social and ethical issues by malicious actors. Currently, privacy regulations for health data vary globally, but the core principles consistently emphasize protecting patient privacy over general availability. This protective stance often leads health system developers to adopt a defensive approach to avoid violating privacy laws, resulting in restricted data access. Consequently, policymakers and developers, especially in the pharmaceutical sector, face ethical and political challenges in utilizing this data. This article investigates how blockchain technology can secure data while maintaining accessibility. Our method follows the principles of the US HIPAA statute, which sets criteria for public access to health information, while local restrictions may differ. Blockchain's decentralization, absence of intermediaries, and cryptographic security provide a novel solution to securely storing medical data. It also improves the efficiency of electronic health records (EHR) by providing public access via peer-to-peer connectivity.

Keywords: Health data storage, patient privacy, blockchain, EHR, cryptographically secure data storage, multi-signature data access.

Introduction

Blockchain is a secure, unchangeable data structure that organizes information into blocks, linking them with cryptographic keys. As a decentralized system, it allows multiple participants in a network to manage and verify data collaboratively without a central authority overseeing the process. In a peer-to-peer setup, independent participants work together to keep the blockchain data consistent and synchronized, relying on a consensus mechanism to validate information. In open, permissionless blockchains, no single entity controls the consensus rules, as a network of independent peers maintains them. This structure eliminates the need for intermediaries, creating a system where trust is built directly through the network. Known as the “technology of trust,” blockchain's complex, costly consensus process ensures that data and transactions, once added, are practically irreversible.

II. Centralized Electronic Health Record (EHR) systems face several challenges

A. Current Healthcare Infrastructure

Currently, a wide range of separate health information systems store individual patient data in large, isolated silos. These systems are structured differently based on the unique objectives of each healthcare provider's business. Whether it's a diagnostic center or a general practitioner, data is organized in distinct ways. In any case, both types of providers rely on (name, value) pairs to convey encounter results, which are then incorporated into EHR records through various structuring methods. These pairs are accompanied by key attributes, with the timing of events being particularly important.

It requires a set of interfaces to be developed and maintained for years in order to amalgamate these data sources that are kept separately. Numerous protocols have been created to solve the problem of connecting disparate health data systems. Nevertheless, the lack of a standardized protocol is still hindering widespread access to data exchange.

At the same time, there is a move from procedure and profession-based healthcare provision to comprehensive care - this requires more data about patients being available for health providers. This transition to a more accessible incorporated EHR format. This is combined with the pursuit of better care outcomes, and there are also myriad research initiatives or supplementary health providers (e.g., pharmaceutical companies or service sectors) who, too, would like to get the data from individual patients. This was an added layer due to space for personal fitness tracking gadgets deployed.

B. Simplified Working Model of Patient-Provider Relations

Before you can thoroughly assess a patient, it is critical that you first understand

their details. Although the manner of operation varies in healthcare systems worldwide, one constant throughout is that Primary Care providers must ensure cooperation between various healthcare professionals and entities such as labs or pharmacies. This typically involves a central figure, such as the primary care provider (PCP) or designated physician of record, having services coordinated through them and generating critical information from any auxiliary providers.

These methods can be effective for specific care scenarios, whether focused on a particular condition or level of care. During emergencies, centralized data storage systems hold the potential to offer critical, life-saving information. While centralized systems can efficiently provide requested data, the main concern lies in the centralization itself. Overly concentrated authorization in central bodies can lead to a convoluted permission structure, increasing the risks of data breaches and information disclosure.

C. Aligning Care Delivery and Payment

In healthcare systems, where how care is provided impacts providers' earnings, manipulating data can pose challenges. Introducing a blockchain-based, secure patient record system can address inconsistencies and uphold data reliability.

D. Patient Data Accessibility

In healthcare systems where provider earnings are influenced by care provision, the manipulation of data can pose challenges. Implementing a blockchain-based system for immutable patient records can help prevent inconsistencies and preserve the reliability of data.

III. A Regulation to Begin With - HIPAA

Given the variation in national regulations, we will begin by applying the standards set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This paper does not aim to offer an exhaustive summary of pertinent regulations; instead, we will rely on fundamental principles common to most national jurisdictions.

The essential part of the HIPAA rules is summarized as: "All individually identifiable health information held or transmitted by a covered entity or its business associates in any form or media, whether electronic, paper, or oral," constitutes private patient health information. De-identified health information is defined as: "Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information." The use restrictions for de-identified data are summarized as follows: "There are no restrictions on the use or disclosure of de-

identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual." The line between identifiable data and de-identified data is determined by any details that could limit the potential number of individuals linked to a set of information to a specific proportion of the total population. This proportion is subjective and may vary based on local circumstances.

IV. Tools used for encryption and intelligent contracts

It seems like you're outlining the foundational cryptographic tools and concepts that are crucial for blockchain-based systems in healthcare. Here's a summary of each:

A. **Public-key cryptography (PKI)**: This is essential for secure identification and transactions within blockchain systems, utilizing private-public key pairs.

B. **Digital signatures**: Ensures the integrity and authenticity of data by confirming its source using cryptographic verification.

C. **Blind signature**: Allows signing of messages without revealing their content, useful for protecting sensitive patient information in healthcare systems.

D. **Multi-signature**: Requires multiple parties to sign a transaction, enhancing security and decentralization in blockchain networks.

E. **Smart contracts**: Automated, self-executing contracts with predefined rules, integral to blockchain ecosystems like Ethereum, enabling decentralized applications (dApps) and complex transactional logic.

These tools collectively provide a robust foundation for secure, privacy-preserving, and efficient healthcare information systems based on blockchain technology.

V. Electronic Health Record Application Model

Blockchain technology offers transformative benefits to healthcare's Electronic Health Record (EHR) systems, addressing challenges inherent in centralized data management. By decentralizing data storage, blockchain enhances security, relying on consensus mechanisms like mining and cryptographic tools, such as blind signatures and multi-signatures, to protect data privacy. It also expands data sources beyond traditional providers to include IoT-based wearables, implants, and home devices, which enrich data reliability. Access to sensitive information is tightly controlled through encryption, allowing only authorized users access and avoiding centralized data gatekeeping. The technology also reduces operational costs by minimizing database maintenance expenses while supporting interoperability through a secure, immutable platform that eliminates complex data reconciliation processes. To balance security and accessibility, EHR systems can

operate in both permissioned and permissionless settings. Permissioned subsystems restrict sensitive data access to authorized entities and ensure compliance with regulations like GDPR and HIPAA, while permissionless subsystems handle decentralized storage of non-sensitive or anonymized data, facilitating research, public health analysis, and system interoperability without risking privacy. Incentive models in these blockchain networks vary: permissioned systems may reward participants through centralized governance rules, while permissionless systems often rely on native tokens within a decentralized governance structure to incentivize network participation and maintain security. By integrating both models, blockchain-based EHR systems promote secure, decentralized, and compliant healthcare data ecosystems that support both patient privacy and broader data-sharing needs, enabling an adaptable and resilient healthcare information infrastructure.

VI. Summary

This paper introduces an integrated health information model based on blockchain technology. It solves data access problems without compromising personal privacy. The decentralized and cryptographically secured network supports new service providers and automatic personal monitoring devices, advancing healthcare delivery.

References

[1] Adam Back. Hashcash - A Denial of Service Counter-Measure, Online, 2002.

[2] Andrew Poelstra. "Distributed Consensus from Proof of Stake is Impossible" (PDF).

[3] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder: Bitcoin and Cryptocurrency Technologies with a preface by Jeremy Clark - Draft — Feb 9, 2016

[4] Centers for Disease Control Prevention. “HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services.” In: (2003.)

[5] Rosenberg (ed.) Handbook of Financial Cryptography and Security. CRC Press, 2011.

[6] Chaum, A. Fiat, M. Naor. Untraceable electronic cash. CRYPTO 1998.

[7] Digital Assets on Public Blockchains - White Paper - BitFury Group - Mar 15, 2016

[8] HHS.gov. “H. H. S. O. of the Secretary Summary of the HIPAA Privacy Rule.”In:(2013).url:www.hhs.gov/hipaa/forprofessionals/privacy/lawsregulations/index.html.

[9] Incentive Mechanisms for Securing the Bitcoin Blockchain - White Paper - BitFury Group -Dec 07, 2015

[10] Joseph Poon, Thaddeus Dryja: The Bitcoin Lightning Network: Scalable O-Chain Instant Payments - January 14, 2016 - DRAFT Version 0.5.9.2

[11] Katz, Jonathan, and Yehuda Lindell. Introduction to Modern Cryptography, Second Edition. CRC Press, 2014.

[12] Leslie Lamport. Time, Clocks, and the Ordering of Events in a Distributed System. Communications of the ACM, 21(7):558{565, Jul 1978.

[13] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. (2008)

[14] Nick Szabo. Formalizing and Securing Relationships on Public Networks. http://szabo.best.vwh.net/formalize.html , Sep 1997.

[15] Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast: Patientory: A Healthcare Peer-to-Peer EMR https: //patientory.com/patientory_whitepaper. pdf, May, 2017

[16] Peter Todd. Near-zero fee transactions with hub-and-spoke micropayments. http://sourceforge.net/p/bitcoin/mailman /message/33144746/, Dec 2014.

[17] Pieter Wuille. BIP 0032: Hierarchical Deterministic Wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, Feb 2012.

[18] Proof of Stake versus Proof of Work - White Paper - BitFury Group - Sep 13, 2015

[19] R. Anderson. Security Engineering (2nd ed). Wiley, 2008.

[20] S. Haber, W. S. Stornetta. Secure names for bitstrings. CCS, 1997.

[21] Vitalik Buterin. "On Stake". "Hard Problems of Cryptocurrencies". Retrieved 23 January 2016. one thing has become clear: proof of stake is non-trivial

[22] Wood, Gavin. "Ethereum: A Secure Decentralised Generalised Transaction Ledger" (PDF). Retrieved 23 January 2016. Ethash is the planned PoW algorithm for Ethereum 1.0