Proceedings of the 2nd International Conference on Environmental Geoscience and Earth Ecology
DOI: 10.54254/2753-8818/37/20240207

Enhancing transparency and security in blood donation management through blockchain technology

Yiyang Wu

Southwest Jiaotong University, Chengdu, Sichuan, China, 611730

2021112632@ swjtu.edu.cn

Abstract. In the context of the increasing importance of digitalization and cybersecurity, exploring the application of blockchain and smart contract technologies in blood donation management aims to enhance data transparency and privacy protection, addressing challenges in current healthcare systems. This paper explores the transformative potential of blockchain and smart contract technologies in digitalizing the blood donation process. By leveraging the Ethereum platform and employing a Browser/Server (B/S) architecture integrated with Solidity programming and web development practices, this paper proposes a novel framework designed to enhance the transparency, digitalization, and shared accessibility of blood donation data. The implementation of this system within a healthcare context promises to streamline the donation process, ensuring the integrity and confidentiality of donor data, thereby fostering trust among all stakeholders involved. The findings indicate that the application of blockchain technology not only facilitates a more efficient and secure management of blood donation records but also sets a precedent for future healthcare innovations.

Keywords: Blockchain, Blood Donation, Digitalization, Ethereum, Healthcare Innovation

1. Introduction

The management and coordination of blood donation processes stand at the crux of modern healthcare systems, ensuring the life-saving transfusion of blood to patients in need [1]. Despite its critical importance, this process often grapples with challenges such as inefficient data management, lack of transparency in the tracking and allocation of blood supplies, and concerns over donor and patient data privacy. The traditional systems, while functional, are marred by fragmented data silos and an overarching lack of interoperability between various stakeholders, including hospitals, blood banks, and donation centers. These limitations not only hinder the efficacy of blood donation campaigns but also pose significant barriers to timely and secure access to blood supplies.

In this context, blockchain technology emerges as a beacon of innovation, offering a paradigm shift in how data can be securely managed and shared across the healthcare ecosystem. Known for its robust security, decentralization, and immutable record-keeping capabilities, blockchain technology promises to address the perennial issues plaguing the blood donation process. By leveraging blockchain, it can be designed a system where blood donation records are encrypted, stored immutably, and made transparently available to all authorized parties involved, from the initial donor registration through to the final transfusion.

DOI: 10.54254/2753-8818/37/20240207

This paper explores the implementation of a blockchain-based solution aimed at digitizing the blood donation process, thereby making it more transparent and secure. This paper proposes a comprehensive framework that not only outlines the technical architecture of such a system but also delves into its potential to revolutionize the management of blood donation records [2]. Through this innovative approach, the system aims to enhance the overall efficiency of blood donation campaigns, ensure the integrity and privacy of donor and patient data, and ultimately foster a more trustful and reliable blood donation ecosystem.

The implications of this research are far-reaching, suggesting that further exploration into optimizing blockchain infrastructure and developing user-friendly interfaces is essential for advancing global healthcare systems.

2. Blockchain Technology

Blockchain technology, often heralded as a cornerstone of the modern digital era, is a distributed ledger technology (DLT) that allows data to be stored across a network of computers around the world.

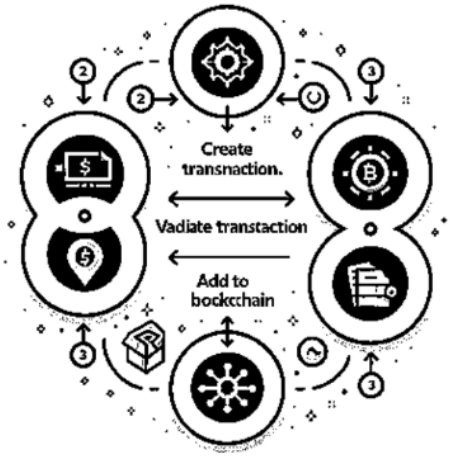

Figure 1. Blockchain

As shown in Figure 1, this technology underpins cryptocurrencies like Bitcoin, but its applications span far beyond, touching sectors such as healthcare, finance, supply chain management, and more.

It has some characteristics:

Decentralization: Blockchain is a decentralised database [3]. It connects all nodes through a network in the form of a distributed ledger, allowing each node to have its own identity and to freely exchange data, assets and information. As a result, blockchain does not require a third-party institution to implement transactions but rather enables point-to-point transfers, so that there is no concept of "centre" in the management of information throughout the network.

Immutability: Blockchain uses cryptographic techniques to secure the information on the blockchain and prevent it from being tampered with, the main techniques used are hash functions in cryptography and asymmetric encryption.

Consensus Mechanisms: Consensus mechanisms are the heart of blockchain technology, enabling agreement on the state of the blockchain among distributed nodes, even in the absence of trust. There are two main ways to realise this mechanism:

Proof of Work (PoW): Used by Bitcoin, PoW requires nodes (miners) to solve complex mathematical puzzles to validate transactions and create new blocks.

Proof of Stake (PoS): A more energy-efficient alternative, PoS selects validators to create a new block based on the number of coins they hold and are willing to "stake" as collateral. This reduces the computational energy required, as the chance to validate transactions and create new blocks is proportional to ownership.

DOI: 10.54254/2753-8818/37/20240207

3. Project Methodology

3.1. System Design

Leveraging the Ethereum smart contract architecture, our goal is to establish a decentralized "Digital Blood Donation Data System" [4]. The functionalities of this system include, but are not limited to, the encryption of blood donation records, their immutable storage, and the transparent access to these records by all relevant authorized parties from the initial donor registration to the final transfusion. Building on these functionalities, once a donor has made a donation, their blood type, blood quality, and other pertinent information will be shared with global blood donation agencies, thereby facilitating information sharing and transparency [5]. This will expediently aid matchers in locating suitable blood sources. The personal information of the donors will be stored within each block of the system and secured via hash encryption.

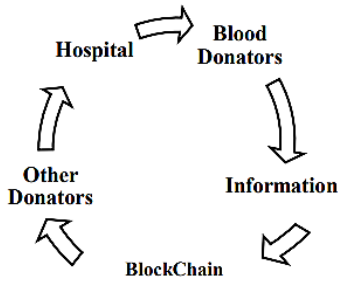

Figure 2. Process of Blood Donation

Figure 2 depicts the process of blood donation leveraging blockchain technology. Hospitals and blood donors interact, with donors providing vital information which is then recorded on the blockchain. This information is also accessible to other donors. The use of blockchain ensures that all the data in this process is secure, transparent, and immutable.

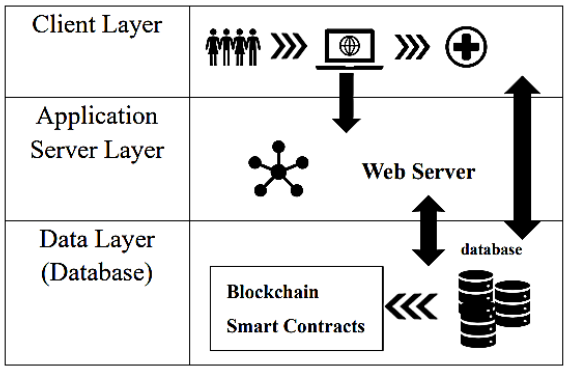

Figure 3. B/S Architecture for Handling Blood Data

Figure 3 illustrates a three-tiered Browser/Server (B/S) architecture for handling blood donor data using blockchain technology and smart contracts, presumably on the Ethereum platform.

Client Layer: The topmost layer is the client layer, where end-users (like blood donors and hospital staff) interact with the system. It symbolizes the user interface—here, users can input data (like blood type and donation records), request information, and perform other interactions through a web application viewed in a browser.

Application Server Layer [6]: The middle tier represents the application server layer, depicted by a centralized node network symbol. This layer contains the application's business logic. It processes requests received from the client layer, like querying blood donor data or adding new records. The logic within this layer interacts with the web server to retrieve or store data as needed.

DOI: 10.54254/2753-8818/37/20240207

Data Layer (Database): The bottom tier is the data layer, which includes a database for storing blood donor data and a separate component for blockchain and smart contracts. This is where all the data is securely stored. The blockchain component suggests that records are not just stored in a traditional database; they are also recorded on a blockchain, ensuring data integrity and immutability [7]. Smart contracts automate tasks and enforce rules, such as verifying the eligibility of blood donors or managing access to data. The web server, which is central to the application server layer, handles HTTP requests from the client layer and serves the appropriate responses. It acts as an intermediary that communicates between the client and the data layer, processing client requests by executing application server logic and interacting with the data layer.

The diagram indicates a distinct blockchain component within the data layer, emphasized by the ledger-like icon and the smart contract symbol. Blockchain securely logs transactions, maintaining a permanent and tamper-evident record of all blood donations. Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code, ensuring that certain conditions, once met, are fulfilled automatically. The arrows between the layers depict the flow of information and data. From the client layer, user inputs travel down to the application server, where they are processed. Validated requests are sent to the data layer, where they are stored in the database and recorded on the blockchain through smart contracts, ensuring data reliability and security. The bidirectional arrows suggest a continuous and interactive flow of data, allowing for real-time updates and retrieval of information.

In the outlined system, hospitals transmit the hash and storage location of electronic medical records from their proprietary blockchain to a consortium blockchain accessible to other medical entities. Upon verification of legitimate identity and authorization from the data owner, a user with requisite access rights can decrypt the data with their private key, which was re-encrypted by an intermediary for their use [8]. This intermediary, tasked with transforming the original encrypted data into a re-encrypted format decipherable by the user, is a miner node designated by the Delegated Proof of Stake (DPoS) consensus protocol. Within this framework, blockchain participants are responsible for electing a set of 101 representatives, each sequentially accountable for validating and generating designated blocks. The DPoS mechanism offers a more decentralized and computationally efficient alternative to the Proof of Work (PoW) and Proof of Stake (PoS) models. Although the improved Practical Byzantine Fault Tolerance (PBFT) algorithm enhances efficiency, it requires a precise number of nodes, which may be insufficient for the expansive bookkeeping demands outlined in this scenario, potentially compromising network performance due to excessive node counts.

This architecture ensures that the blood donation process is streamlined and secure, leveraging the strengths of blockchain for data integrity and smart contracts for automation and compliance.

3.2. Data Privacy and Security

Ethereum smart contract technology implements data privacy and security measures in blood donation processes through a combination of on-chain and off-chain strategies.

Off-Chain Data Handling within the context of Ethereum smart contracts refers to the practice of managing and storing data outside the Ethereum blockchain. Given the public and immutable nature of the blockchain, not all types of data are suitable to be stored on-chain, especially sensitive information that requires privacy, such as personal details in a blood donation system [9]. When data needs to be verified, a cryptographic hash of the data can be computed off-chain and then compared with the on-chain hash to ensure data integrity.

Smart contracts can use these hashes to confirm transactions or validate data without revealing the actual data on-chain. Oracles are used as bridges between the off-chain data storage systems and the Ethereum blockchain. Oracles can fetch data from off-chain, perform necessary computations, and then trigger smart contract functions with the results. By handling data off-chain, the smart contract can operate more efficiently because it reduces the amount of data stored on the blockchain, which can be expensive and slow due to gas costs and network congestion.

DOI: 10.54254/2753-8818/37/20240207

Off-chain systems can be scaled independently from the blockchain, providing more flexibility in managing large or complex datasets. When off-chain data is updated, corresponding on-chain records, such as hashes or metadata, can also be updated to maintain synchronization between the on-chain and off-chain states.

Hash algorithms play a pivotal role in maintaining data privacy within blockchain technology [10]. By transforming input data into a fixed-size string of characters, which is typically a unique set of numbers and letters, hash functions create a digital fingerprint of data. Hashing anonymizes data, which means that the original information cannot be derived from the hash output, preserving the privacy of the data.

The integrity of transaction data is maintained because any alteration to the input data results in a completely different hash, making tampering evident. In some blockchain implementations, hash functions are used in zero-knowledge proofs to allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself.

4. Challenges

However, implementing a blockchain system in a medical blood donation project can encounter several potential technical barriers.

Blockchain networks, particularly those utilizing Proof of Work (PoW) consensus mechanisms, can face significant scalability issues due to the inherent design choices that prioritize security and decentralization. These challenges are magnified in applications requiring high transaction throughput and real-time data access, such as managing a national or global blood donation and distribution network. Most public blockchains can process only a limited number of transactions per second.

For a blood donation system, this could mean delays in recording donations, accessing donor records, or updating inventory, potentially affecting the timeliness and efficiency of blood distribution. Blockchain is not optimized for large-scale data storage. Storing extensive medical records, donor information, and transaction histories directly on-chain can quickly become impractical and expensive. Additionally, high demand on the network, either through increased donations or queries, can lead to congestion, resulting in slower transaction validation times and higher costs for data storage and access.

The decentralized nature of blockchain can lead to latency issues, as every transaction must be validated by multiple nodes across the network. In emergencies where immediate access to blood types or donor information is crucial, any delay, however minimal, could have serious consequences.

Solutions such as state channels or plasma can help offload transactions from the main blockchain, improving throughput and reducing latency.

User adoption presents a significant challenge in integrating blockchain technology into blood donation systems. The success of such a system heavily relies on its acceptance by various stakeholders, including donors, healthcare providers, and regulatory bodies. Blockchain technology can be complex and intimidating for users unfamiliar with its concepts [10]. The perceived difficulty in understanding how the system works can deter potential users. What's more, individuals and organizations accustomed to traditional blood donation systems may resist transitioning to a new, blockchain-based system due to comfort with existing processes or skepticism about new technology.

Not all users have equal access to the technology required to participate in a blockchain-based blood donation system, potentially excluding certain demographics. Rural areas often suffer from limited internet connectivity and lack the necessary technological infrastructure, which is critical for accessing blockchain-based systems.

5. Conclusion

In conclusion, the digitalization of the blood donation process can be effectively achieved through the utilization of blockchain and smart contract technologies. By leveraging the Ethereum platform, employing a Browser/Server (B/S) architecture, and utilizing the Solidity programming language in conjunction with web development practices, this paper has outlined a robust framework for enhancing the transparency, digitalization, and shared accessibility of blood donation data. This approach not only

DOI: 10.54254/2753-8818/37/20240207

streamlines the donation process but also ensures that data integrity and privacy are maintained, thereby increasing trust among donors, recipients, and medical institutions alike [11]. The implementation of this system addresses critical challenges in the current blood donation infrastructure by providing a decentralized, secure, and efficient method of managing and sharing blood donation records. Continued efforts must be made to refine these technologies and expand their adoption, ensuring that the benefits of digitalization in the blood donation process are realized globally. This study underscores the transformative potential of blockchain and smart contract technologies in revolutionizing healthcare processes, setting a precedent for future innovations in the medical field.

The implications of this research for future studies are profound and multifaceted. Firstly, it establishes a foundational blueprint for integrating blockchain technology within healthcare processes beyond blood donation, such as organ donation systems and patient health records management. The successful application of blockchain and smart contracts for blood donation digitalization paves the way for broader exploration into how these technologies can further enhance privacy, efficiency, and transparency in healthcare.

Moreover, this paper opens avenues for technical advancements in blockchain technology itself, particularly in addressing scalability, interoperability, and user adoption challenges within healthcare contexts. Future research could focus on optimizing blockchain infrastructure to support high-volume, real-time medical data transactions, or developing more intuitive interfaces to increase technology accessibility among healthcare professionals and patients.

Acknowledgement

I extend my sincerest gratitude to everyone who played a pivotal role in the realization of this project. First and foremost, I wish to express my profound appreciation to my academic supervisor, Prof. Franchitti, whose expertise, insightful guidance, and unwavering support were invaluable throughout this research journey. Their dedication and mentorship have been fundamental to my personal growth and the success of this study.

My heartfelt thanks go to Southwest Jiaotong University, for providing the necessary resources and an intellectually stimulating environment that facilitated my research. Special acknowledgement is due to the technical and administrative staff whose assistance was crucial at various stages of the project.

References

[1] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc. 2018 Apr 16;2017:650-659. PMID: 29854130; PMCID: PMC5977675.

[2] Remolina-Medina C. Beneficios y limitaciones del Blockchain en contratos inteligentes en el sector salud. Una revisión de la literatura. Revista científica anfibios 2022;5(2):57

[3] Cui B, Hu Y. BSELA: A Blockchain Simulator with Event-Layered Architecture. Future Generation Computer Systems 2024;151:182

[4] Xie Y, Zhang J, Wang H, Liu P, Liu S, Huo T, Duan Y, Dong Z, Lu L, Ye Z.Applications of Blockchain in the Medical Field: Narrative Review J Med Internet Res 2021;23(10):e28613

[5] XIA Weihao, ZHAO Zhenjiang, CAO Jialu, WU Minamatafei, ZHANG Lili. Medical information sharing platform based on blockchain[J]. Shanxi Electronic Technology,2024(1):91-94

[6] ZHAI Sheping, WANG Yijing, CHEN Siji. Research on the application of blockchain technology in the sharing of electronic medical records[J]. Journal of Xidian University, 2020, 47(5): 103-112.

[7] Chen HS, Jarrell JT, Carpenter KA, Cohen DS, Huang X. Blockchain in Healthcare: A Patient-Centered Model. Biomed J Sci Tech Res. 2019;20(3):15017-15022. Epub 2019 Aug 8. PMID: 31565696; PMCID: PMC6764776.

DOI: 10.54254/2753-8818/37/20240207

[8] Mamoshina P, Ojomoko L, Yanovich Y, et al. (2018) Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 2018; 9: 5665–5690.
[9] Firdaus A, Anuar NB, Razak MFA, Hashem Ibrahim Abaker Targio, Bachok Syafiq, et al. (2018) Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management.
[10] Yue X, Wang H, Jin D, Mingqiang Li, Jiang Wei (2016) Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst 40: 218.
[11] Zhou L, Wang L and Sun Y (2018) MIStore: a Blockchain-Based Medical Insurance Storage System. J Med Syst 42: 149.