Special article

Potential and limitations of blockchain technology in blood quality tracking and verification: approaches for blood bank systems

Attapong Sinkitjasub and Patchanika Hengtrakool
Faculty of Science and Technology, Bansomdejchaopraya Rajabhat University

Introduction

Blockchain technology, first developed by Nakamoto in 2008[1], laid the foundation for the digital currency system known as Bitcoin. Bitcoin emerged as the world's first decentralized cryptocurrency, designed as a peer-to-peer electronic cash system. This innovative approach allows transactions to occur directly between users, bypassing traditional financial institutions or banks entirely. Consequently, it significantly lowers transaction costs and removes geographical limitations for both domestic and international transfers.

Currently, Bitcoin and other cryptocurrencies have gained substantial popularity as digital assets and valuable tools for exchanging value, primarily due to their speed and cost-effectiveness. Although cryptocurrencies exist merely as digital data on the internet, they are widely recognized and valued by users as equivalent to conventional assets. Therefore, ensuring the security and trust in holding these digital assets is paramount. Owners require a robust system to protect their funds from loss or fraudulent activities and to guarantee that transactions can be traced accurately. It is precisely these fundamental needs for security and reliability that propelled the development of blockchain technology.

The concept of blockchain originated in 1991 with Haber and Stornetta[2], who aimed to create a digital document recording system that would be unalterable. Consequently, blockchain has become crucial for digital finance and other transactions. This is because it is a technology capable of safeguarding assets and information through sequential cryptographic encryption. This process ensures high security for each transaction, allowing financial activities to be traced precisely and securely. Critically, data recorded on a blockchain cannot be altered retroactively (immutable), a core feature that establishes the system's inherent trustworthiness and transparency.[2]

As a decentralized data storage system, blockchain offers high levels of security and transparency. Every transaction is recorded as a block, chronologically linked to the previous one, which enables verification and prevents data falsification. Its utility is particularly amplified when integrated with various electronic devices connected via the Internet of Things (IoT).[3]

Understanding blockchain transaction security

The infographic below (Figure 1), titled "Transaction Segmentation, Password Coding & Blockchain Activity Encryption" shows how a secure blockchain deal relies on several protective layers that activate the moment a user hits send. When users decided to move funds or hand over a token, the first thing to do is prove that they have the right to make that change, either by tapping your private key directly or by entering a password that unlocks that key. That first validation is the bedrock of trust for everything that follows. After that authorization, the deal stops being viewed as one solid block of data. Instead, it gets sliced into smaller pieces: inputs that show where the money is coming from, outputs that say where it is going, and bits of meta info needed to tie it all together. Each of these segments then contains specific details, such as the

Correspondence should be addressed to Patchanika Hengtrakool, Faculty of Science and Technology, Bansomdejchaopraya Rajabhat University, Bangkok 10600 E-mail : ann_patchanika999@hotmail.com, attapong.si@bsru.ac.th

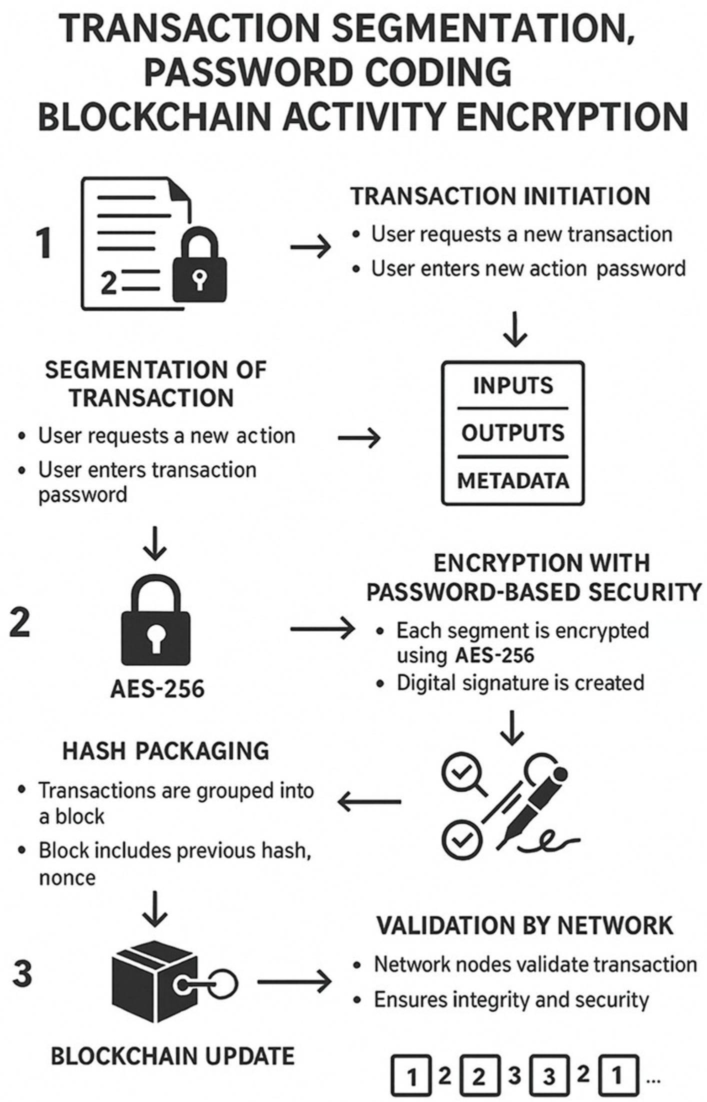

Figure 1 The Infographic of transaction segmentation, password coding & blockchain activity encryption

intended recipient, the amount involved, and the precise timestamp of the transaction. A critical security measure follows, involving the use of cryptographic keys derived from a user's password or master seed for signing. Although anyone can see the transaction details on the blockchain for independent verification, a user's true control over their fund's hinges on the privacy and safety of the corresponding private key. Most wallets shield that key with a locally stored password using standard stretching methods like PBKDF2 or SCRYPT, so only the person who remembers the correct passphrase can unlock it and sign new payments. To reinforce overall security and guard against accidental tampering, every part of the transaction that remains public is passed through a hashing function-SHA-256, in most cases-which turns all the data into a short, fixed-size string that acts like a unique fingerprint for that entry. Concurrently, the sender's private key is used to create a digital signature. This signature serves as irrefutable proof of the sender's identity and confirms that the transaction hasn't been tampered with since it was signed. These securely prepared transactions are then bundled together with other transactions into a block. Once processed, the block carries the fingerprint of its predecessor, effectively locking the new data into the history. It also includes a nonce-a random, trial-and-error number the network's miners adjust repeatedly during proof-of-work-to produce a hash that satisfies network's current difficulty.[2,3]

Given the sophisticated technology used to ensure the security of financial transaction data, its application to managing other critical information, such as in healthcare and public health, or even in blood banking and transfusion services, presents significant challenges.

The following succinctly describes how blockchain functions in this situation:

1. Secure data management

Blockchain protects data with cryptography. Each block containing transaction data has a distinct hash value that is produced using the data in the block and the hash of the block before it. This makes data falsification very challenging because the hash value changes if any block's data is altered. Furthermore, each network node keeps an identical copy of the data due to distributed ledger storage. Any unauthorized changes are detected and rejected by the system[2].

2. Historical data retrieval

Due to blockchain's structure that links each block through hash values, tracking and verifying the history of data or transactions becomes straightforward. Every change is recorded and verifiable, which proves highly beneficial in systems requiring transparency, such as product tracking or transaction history verification.[2,3]

3. Creating subsequent data

When new transactions are created, the data is packaged into a new block. Other network nodes must concur with this process, and it must pass verification checks. After confirmation, the new block is appended to the chain, using its hash value to refer to the previous block. This process ensures data continuity and prevents retroactive modifications[1].

4. Encryption for data analysis

Both symmetric and asymmetric encryption are used by blockchain to safeguard data. Asymmetric-key cryptography uses pairs of public and private keys, whereas symmetric-key cryptography uses the same password for both encryption and decryption. Only the matching private key can decrypt data that has been encrypted with a public key. These encryption techniques guarantee that information sent or stored on the blockchain stays safe and that only authorized users can access it[4].

Because of these features, blockchain technology has a lot of potential for use in blood bank systems. It can help with donor information verification, blood quality tracking, and access control to vital data, which lowers the risk of falsification and boosts operational effectiveness. Technical requirements and legal restrictions are two obstacles that must be taken into account when putting this technology into practice.[5]

5. Applications of blockchain technology in blood banking

Blockchain technology offers significant potential for application within blood bank systems. It can effectively facilitate blood quality tracking, donor information verification, and secure data access control, thereby minimize the risks of falsification and enhance overall operational efficiency.

5.1 Blood quality tracking and verification: blockchain enables the recording of comprehensive data pertaining to blood donation and storage processes, including storage duration and conditions. This capability allows for the accurate and secure traceability of the blood's quality at any point.[4]

5.2 Donor information management: blockchain also facilitates the secure management of blood donor information. By utilizing Smart Contracts–digital agreements that automatically execute predefined conditions–the system can control data access and safeguard donor privacy, ultimately improving the system's efficiency and security.[6]

5.3 Historical data retrieval and future data creation: a key advantage of blockchain is its inherent ability to securely retrieve historical data and generate securely interconnected new data. Every recorded transaction undergoes verification through cryptographic mechanisms, integrated into an immutable chain structure. This ensures that data evolution across the entire blood donation and storage process can be meticulously monitored.[7]

5.4 Enhanced security in IoT-based data analysis: blockchain technology can be integrated with the Internet of Things (IoT), a network connecting various computing and communication devices, to enhance data security in analytical processes. For example, when IoT sensors monitor blood temperature and status, the blockchain allows this data to be precisely and immutably recorded, thus mitigating risks of falsification or potential errors[8].

5.5 Reducing data falsification issues: given its inherent transparency and immutability, data recorded on a blockchain cannot be easily altered. This characteristic effectively reduces issues related to the falsification of information concerning blood and donors.[3,9]

6. Case studies of blockchain implementation in blood banks

The application of blockchain technology in medical systems and blood banks is increasingly evident across numerous countries, underscoring its potential to significantly enhance efficiency and security. The following case studies illustrate these developments:

6.1 Vietnam: in Vietnam, a blood management model has been developed utilizing the Hyperledger Fabric platform.[10] This is a permissioned blockchain platform, often referred to as a private or consortium blockchain, specifically designed for enterprise and institutional use where controlled access is essential. The adoption of Hyperledger Fabric has enabled Vietnam's blood bank system to achieve enhanced data transparency across the entire blood supply chain, from collection and testing to processing, storage, and eventual delivery to patients. Furthermore, it strengthens the security of both donor and blood data, ensuring data integrity and preventing falsification, while allowing precise traceability of every step to optimize blood management efficiency and reliability.

6.2 United Arab Emirates: in the United Arab Emirates, the Ethereum platform has been implemented for managing blood donations.[11] Ethereum, a public blockchain, is notable for its robust support for Smart Contracts–self-executing digital agreements that automate processes based on predefined conditions. These Smart Contracts contribute to more transparent and efficient blood donation processes, such as automating donor qualification verification, recording donation details, and managing donor incentives. Additionally, the Inter-Planetary File System (IPFS), a decentralized file storage system, is used concurrently for storing large blood donation-related data, like laboratory results or medical records. The blockchain (Ethereum) itself stores only the cryptographic "hash" of these files, ensuring the integrity and security of these larger datasets without imposing excessive storage burden on the main blockchain.

6.3 Pakistan: Similarly, Pakistan has utilized Hyperledger Fabric to develop a platform aimed at enhancing the efficiency of blood transfers between different blood banks.[12] This application of blockchain facilitates swift, secure, and seamless communication and data sharing regarding blood stock, required types, and transportation details among various blood banks. This significantly reduces delays in logistics, minimizes errors associated with manual documentation, and improves responsiveness to emergency blood demands, ultimately leading to more efficient and secure overall operations.

6.4 Spain: Spain has adopted IBM Hyperledger Fabric blockchain technology for biobanking applications.[13] Biobanking involves the secure storage of biological samples, such as blood and tissue, for medical research purposes. The use of blockchain in this context ensures the data integrity and security of stored biological samples throughout their entire lifecycle, encompassing collection, processing, storage, access, and utilization for research. Recording every step on the blockchain creates an immutable audit trail, which is crucially important for ensuring the accuracy of research data, protecting donor personal information, and adhering to strict regulatory requirements in both research and medical fields.

Conclusion

Data security, transparency, and dependability could all be improved in blood banks by implementing blockchain technology. Limitations must be taken into account, though, such as infrastructure, user acceptance, and legal requirements, all of which call for more research and development.

In blood banking systems, blockchain technology provides a number of noteworthy benefits. Blockchain's immutable ledger structure improves data security and transparency while lowering the possibility of errors and falsification, which can be crucial in medical settings. Assuring accurate chain-of-custody documentation for every blood unit, blood banks gain from simpler information tracking and verification throughout the donation-to-transfusion pipeline. Additionally, blockchain enables smooth integration with IoT devices for real-time data management, enabling ongoing storage condition monitoring and prompt identification of possible problems before they jeopardize blood quality. The infographic below (Figure 2), illustrates the application of blockchain technology in blood banking. It highlights key functions like blood quality tracking, secure data management, and donor information management, emphasizing transparency, traceability, and data integrity.

Despite these advantages, there are a number of significant obstacles to blockchain adoption in blood banking. Many healthcare facilities, especially those in developing nations, might not have the necessary infrastructure and strong support networks to implement the technology. Adoption is also severely hampered by the potentially high expenses of system development, deployment, and continuing maintenance. There are still legal and regulatory obstacles to overcome, as different jurisdictions have different data privacy laws that make standardization difficult and may restrict cross-border information exchange.

In the future, a number of exciting development opportunities may hasten the adoption of blockchain technology in blood banking. Standardized procedures and information exchange between institutions globally would be made easier by the creation of open blockchain platforms tailored for international blood bank cooperation. Blockchain integration may offer revolutionary potential for predictive analysis of blood supply needs and efficient resource allocation during shortages or emergencies, when combined with laboratory information management systems (LIMS), artificial intelligence (AI), deep learning (DL), machine learning (ML), and the internet of things (IoT). Lastly, establishing blockchain as a workable,

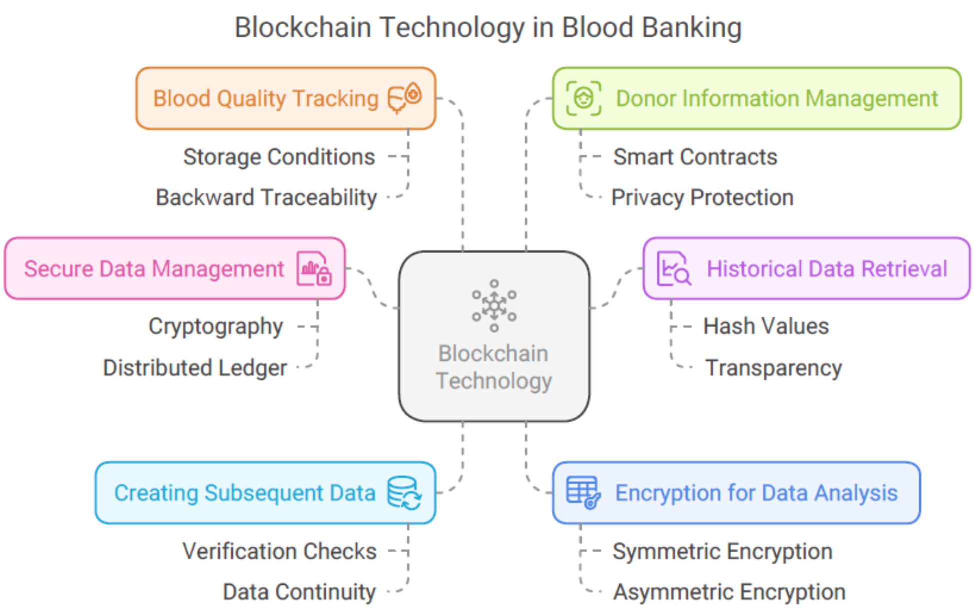

Figure 2 The infographic of blockchain for blood banking

widely-accepted method for blood banking management will require advancing international standards through agencies like the World Health Organization (WHO), Centers for Disease Control and Prevention (CDC), and blood banking associations. This could completely transform the way this essential healthcare resource is tracked and distributed throughout the world.

References

1. *Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Internet]. 2008 [cited 2025 Jul 2]. Available from: https://bitcoin.org/bitcoin.pdf.*
2. *Haber S, Stornetta WS. How to time stamp a digital document. J Cryptol. 1991;3:99-111.*
3. *Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world [Internet]. New York: Portfolio; 2016 [cited 2025 Jul 2]. Available from: https://www.penguinrandomhouse.com/books/537733/blockchain-revolution-by-don-tapscott-and-alex-tapscott/*
4. *Kshetri S. Can blockchain revolutionize developing country economies? J Dev Stud. 2018;54:457-71.*
5. *Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Comput Surv. 2019;52:1-34.*
6. *Nazir T, Ahmed RH, Hussain M, Zahid S. Transforming blood donation processes with blockchain and IoT integration: an augmented approach to secure and efficient healthcare practices. In: Proceedings of the 2023 International Conference on IT and Industrial Technologies (ICIT); 2023; Chiniot, Pakistan. p. 1-8.*
7. *Ozdayi MS, Kantarcioglu M, Malin B. Leveraging blockchain for immutable logging and querying across multiple sites. BMC Med Genomics. 2020;13(Suppl 7):82.*
8. *Kamangar F, Singh A, Khan S. Blockchain-enhanced IoT ecosystem for healthcare: transformative potentials, applications, challenges, solutions, and future perspectives. Comput Electr Eng. 2024;108659.*
9. *Wu Z, Ji M. Blockchain technology and applications. Int J Inf Manag. 2021;45:44-55.*
10. *Le Van H, Le Quoc K, Vo HK, Huong LH, Nguyen TA. Blockchain technology-based management of blood and its products: a case study in Vietnam. In: Sakurai K, Su C, editors. Science of cyber security: SciSec 2022 workshops. Singapore: Springer; 2022. p. 97-111.*
11. *Hawashin D, Mahboobeh DAJ, Salah K, Jayaraman R, Yaqoob I, Debe M, et al. Blockchain-based management of blood donation. IEEE Access. 2021; 9:163016-32.*
12. *Zafar MH, Khan I, Rehman SU, Iqbal W, Raza S. Secure and efficient blood donation system using blockchain technology. EAI Endors Trans Smart Cities. 2022;6(18):e3.*
13. *Ortiz-Lizcano MI, Arias-Antunez E, Hernández Bravo Á, Caminero MB, Rojo Guillen T, Nam Cha SH. Increasing the security and traceability of biological samples in biobanks by blockchain technology. Comput Biol Med. 2023;163:107379.*