Blockchain Technology in Healthcare, Logistics, and Transportation: An Investigation of Applications, Frameworks and Challenges

Shisheng Zheng*

Faculty of Science and Technology, Beijing Normal University-Hong Kong Baptist University United International College, 519088 Zhuhai, China

Abstract. Today, blockchain technology is no longer confined to the financial sector for which it was originally designed, but has been integrated across diverse fields, achieving noteworthy advancements. Researchers have endeavored to demonstrate the feasibility and potential of blockchain applications beyond finance. This paper introduces the characteristics and workflow of blockchain technology. It provides an overview of the current state of blockchain applications in healthcare, logistics management, and transportation, analyzing several specific examples and presenting their corresponding simplified frameworks. These frameworks are conductive to traditional sectors by offering additional functionalities. In healthcare, blockchain is utilized to enhance the security and integrity of the sensitive health data records, as well as to facilitate remote patient monitoring. In logistics management, blockchain is employed to effectively enhance data security and ensure cold chain traceability, thereby improving the transparency and reliability of supply chain operations. In transportation, blockchain supports the development of intelligent transportation systems. Due to the inherent limitations of blockchain technology, such as issues with scalability, and the specific deficiencies of certain proposed frameworks, including the inaccuracies of Body Area Sensor Networks (BSN) and the drawbacks associated with Rivest-Shamir-Adleman (RSA) encryption, these integration efforts continue to face challenges. Various approaches, such as sharding, have been proposed to address these drawbacks and improve the efficacy of blockchain implementations in these domains. Despite these challenges, the ongoing research and development efforts indicate a promising future for blockchain technology in a wide array of applications.

1 Introduction

Since its inception by Satoshi Nakamoto in 2009, blockchain technology, as a nascent innovation, has fundamentally reshaped the paradigm of transactions and revolutionized the digital world [1]. Basically, Blockchain technology was made popular mainly for its following key properties. Decentralization: Refers to in a decentralized network, transactions

* Corresponding author: s230026220@mail.uic.edu.cn

are executed exclusively between two participating nodes at a given moment, obviating the necessity for third-party validation. This peer-to-peer structure ensures that blockchain technology operates autonomously, without reliance on centralized authorities for oversight. As a result, nodes in the network effectively have equal voting rights, which the consensus algorithm uses to determine how the Blockchain is constructed [2, 3]. Anonymity: Refers to users in blockchain system can create one or more virtual addresses to protect their identity from attacks by adversaries or malicious individuals. However, only very few blockchains provide full anonymity(such as Monero [4]), most blockchain applications are pseudonymous(such as Ethereum). Immutability: Refers to each transaction must be validated by a trusted miner and every block is connected to other blocks compactly. Only when hackers control more than 51% of the nodes can the records be changed [5]. Therefore, it is almost impossible to tamper with or delete the records in blockchain since these operations would destroy the consistency of blockchain system. Auditability: Refers to since timestamps play a critical role in enhancing the transparency of the blockchain system, Auditors can easily use a time stamp to determine the exact time of each transaction or to verify previous transaction records, which provides transparency and convenience to the entire system.

Of the previously mentioned properties, decentralization is the most important one and it largely depends on the robustness of Distributed Ledger Technology (DLT). In order for a blockchain network to operate effectively, its participants must reach a consensus on the current state of the distributed ledger and the method for organizing data into blocks. This agreement, known as a distributed consensus protocol [6], ensures the validation of the sequence of transactions in the correct chronological order [7]. Numerous consensus protocols have been introduced to enhance the performance of blockchain networks or to address the specific requirements of various applications [8]. There are several commonly used protocols, such as Proof of Work (PoW), Proof of Stake (PoS) and Proof of Burn (PoB).

Despite blockchain's initial emphasis on financial purposes,these characteristics of blockchain encouraged its wider adoption in several non-financial areas, including supply chain management, healthcare [9], Internet of Things(IoT) [10] as well as other domains. To date, Researchers have conducted numerous studies on blockchain-related applications and have made notable progress.

In the healthcare sector, it relies on a trusted third party to store and verify the sensitive or personal health records of patients at present. However, the use of blockchain in healthcare appears promising. Currently, its primary uses are in data exchange, health records, and access control; it is still hardly employed in other contexts, such as medication prescription management. In fact, a great deal of blockchain's potential remains untapped [11]. During the business 4.0 era, the logistics management sector garnered significant attention and produced some valuable applications. For example, in recent years, companies like Walmart intended to enhance last-mile deliveries by leveraging blockchain technology to manage drone deliveries [12]. And it has already adopted blockchain to increase transparency in their food supply chains. Once food safety incidents occur, tracking the sources becomes efficient. And Walmart intends to enhance last-mile deliveries by leveraging blockchain technology to manage drone deliveries. Blockchain technology is also seen as productive and influential in the transportation sector. With the booming development of blochchain, an emergent part of transportation, intelligent transportation systems (ITS) have gone through remarkable refinement. Both entertainment services and a reduction in the incidence of traffic accidents are provided by ITS. It generally gains the acceptance of general public.

The aim of this study is to analyze and assess how blockchain is applied in three promising sectors: healthcare, logistics management, and transportation. The structure of the remaining part of this paper is organized as follows: First, this paper will analyze three promising sectors: health, logistics management and transportation. Second, it will present discussions on the

findings of these fields. Finally, this paper summarizes the above chapters and presents conclusions.

2 Methodology

In general, blockchain is structured as a sequential chain of blocks, each securely linked to the previous one using encryption algorithms [13]. Each block contains a cryptographic hash that references the preceding block, ensuring security and integrity. Fraud can be effectively deterred because hash values are unique, and any alteration to a block in the chain would instantly modify its corresponding hash value [14]. After being recognized by adistributed consensus protocol, the qualified block will be added to the global blockchain, and the corresponding transaction will also be broadcast throughout the whole internet. A timestamp is also used to indicate the exact time of a certain transaction. A simplified workflow for better understanding is shown in Fig. 1.

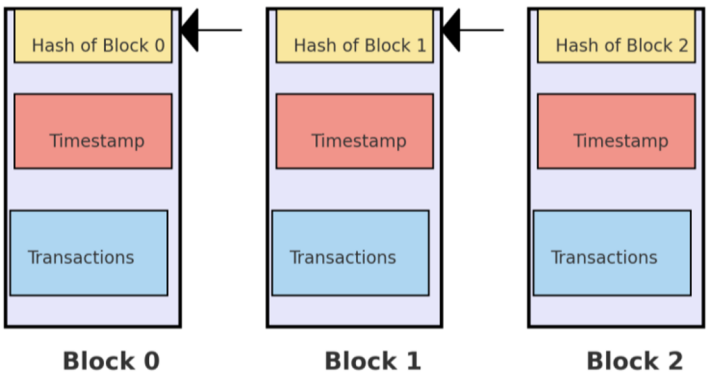

Fig. 1. The workflow of blockchain (Photo/Picture credit: Original).

2.1 Healthcare

2.1.1 Health records

Researchers have made significant progress in ensuring the privacy of sensitive health data through the use of blockchain technology. For instance, Shahnaz et al. [15] developed a framework based on Ethereum, which comprises three modules: user layer, blockchain layer, and system implementation. The user layer enables patients, doctors and administrative staff of a certain hospital to access and manage health records. Additionally, it functions as DApp browser which contains a Graphical User Interface (GUI) to facilitate interaction with the blockchain layer. The blockchain layer is situated centrally, connecting the other two modules. It consists of three components: blockchain assets, network, and governance rules. Notably, a peer-to-peer network is employed to establish a distributed platform rather than a centralized one, thereby promoting decentralization. Furthermore, the system adheres to a distributed consensus protocol, such as PoW, to establish a secure and reliable environment. When the system functions optimally, an ideal scenario involves patients or healthcare providers requesting permission from the system to modify health records. Upon receiving approval, they can proceed with the respective modifications. The updated data is subsequently stored within the blockchain layer by the system.

2.1.2 Remote patient monitoring

Remote Patient Monitoring (RPM) has emerged as a primary approach to addressing healthcare challenges. Due to the inherent complexity of RPM, various innovations have been introduced to create a more accessible framework. Uddin et al. [16] proposed a continuous remote patient monitoring system, building upon the foundation of RPM. This architecture comprises several elements, including Body Area Sensor Network (BSN), Sensor Data Provider (SDP), Patient Centric Agent (PCA), Blockchain, Healthcare Provider Agent (HPA) and Healthcare Provider's Wallet (HPW). Multiple communication channels enable seamless end-to-end connectivity within the architecture. In a blockchain context, the secret key is essential for information encryption and decryption. The SDP, BSN and PCA collaboratively generate a symmetric secret key to mitigate the risk of attacks from hackers. Subsequently, based on the information previously generated by the PCA, each component undergoes identity verification. Then, according to a trusted model, the PCA then selects a reliable miner to execute the PoW protocol. Finally, the PCA determines which data should be added to the blockchain and establishes the connection between the patient's BSN and the blockchain.

2.2 Logistics management

2.2.1 Data security

Ugochukwu et al. [17] developed a blockchain-based logistics management system employing RSA(Rivest-Shamir-Adleman) encryption. The system comprises several stakeholders (manufacturers, suppliers, and transporters) and customers. The process begins with stakeholders creating accounts and acquiring customer identification through a client application. Customers generate asymmetric keys for secure data sharing using RSA method, which are then validated and stored on a decentralized server. Upon successful authentication, stakeholders are able to log in and initiate transactions such as adding products, making purchases, updating product statuses, or transferring product ownership. All transactions are encrypted, validated via smart contracts, and recorded on the blockchain. Then, the information is broadcast across the peer-to-peer network to maintain synchronization among all stakeholders. Transporters are responsible for product delivery, utilizing encrypted information and updating delivery statuses on the blockchain. The entire process heavily relies on the robustness of five algorithms: 1) RSA encryption ensures secure sharing of customer information due to its inherent mathematical complexity. 2) Use smart contracts to create transactions. 3) Stakeholders perform validation checks to verify transaction authenticity. 4) Retrieve asymmetric keys from the server. 5) Transactions, including product purchases, ownership transfers, and deliveries.

2.2.2 Cold chain traceability

Zhang et al. [18]. proposed a comprehensive framework for tracing the cold chain of agricultural products. The process is initiated with data collection at each node, such as production, logistics and sales, utilizing technologies such as RFID, barcodes and sensors. Once the data is entered, the node generates a summary of the collected data using the SHA-3 hashing algorithm. This summary is then transmitted to the blockchain network. Within the blockchain, the participating nodes validate the information through a consensus mechanism, ensuring that all nodes agree on the accuracy of the data before it is officially recorded. After consensus is reached, the summary data is added to a new block on the blockchain. The system generates a hash value for this block, which is then stored in the relational database. This hash serves as a reference for retrieving the corresponding complete data set from the

database when needed. As the product moves through subsequent nodes of the supply chain, this process is repeated at each node, with new data being collected, summarized, validated, and recorded. The full data set continues to be updated in the relational database, while the blockchain stores the secure summaries. The architecture for tracing agricultural cold chains is organized into six layers: Operation, Data Acquisition, Data, Consensus and Network, Presentation, and User Layers. These layers collect, process, store, and validate data using blockchain and databases, ensuring secure, real-time traceability.

2.3 Transportation

2.3.1 Intelligent transportation system

Cocîrlea et al. [19] proposed a blockchain-based framework for securing data storage such as traffic events and user reputation in vehicular networks, utilizing user nodes, region nodes and a master node to manage and validate traffic event data. Traffic reports are submitted through user nodes and forwarded to region nodes for validation via a consensus algorithm that incorporates user reputation. This validation process employs a consensus algorithm that integrates the reputation of the reporting user. The framework relies on two key algorithms. The most critical one, the Speed Alerts Consensus Algorithm, calculates average speed in a specific direction by weighing user reports based on reputation. Reports falling within a predetermined tolerance range are validated, recorded in the regional blockchain, and forwarded to the master node. The master node aggregates data from multiple region nodes, ensuring integrity and accuracy across regions by storing it in a central blockchain. Additionally, a Reputation Update Algorithm dynamically adjusts user reputations based on the accuracy of their reports. Reports are classified as correct or incorrect, and user reputations are updated accordingly. This mechanism is expected to strengthen the reliability of system by rewarding consistently accurate users with greater influence, while reducing the impact of less reliable users' reports.

3 Discussion

Although significant progress has been made in this area, however, there are several challenges and limitations associated with the mentioned framework or solutions. For instance, the framework proposed by Ugochukwu et al. [17] presents notable challenges, particularly regarding the functionality of RSA encryption, which significantly impacts the overall security of the system. While RSA encryption provides a robust level of security, it also has inherent limitations: due to its reliance on complex mathematical calculations, such as exponentiation with large numbers and modulo operations, the computational burden is considerable, and it takes a relatively long time. Moreover, secure data transmission with RSA requires keys typically as large as 2048 bits, which also increases the demand for both computational power and storage resources. Similarly, the effectiveness of the continuous remote patient monitoring system developed by Uddin et al. [16] is closely tied to the accuracy of the components within this architecture. For instance, the data collected from Body Area Sensor Network (BSN) is susceptible to interference due to various factors, such as fluctuations in temperature. These inevitable factors collectively contribute to a reduction in data reliability and accuracy. Furthermore, BSN generates substantial volumes of data, but often lacks sufficient computational power to process raw data effectively, which can lead to significant latency in the system's performance.

There are claims that blockchain will be an influential force in the technological ecosystem. However, aside from cryptocurrencies, it has yet to see significant growth and

impact [20]. This is primarily due to the scalability of blockchain which severely hinders the implementation of blockchain in various areas. The requirement for each transaction to be verified by network nodes before being broadcast introduces significant inefficiencies, particularly because the commonly used consensus protocols are often computationally demanding. This inefficiency not only increases the verification time but also results in substantial consumption of computational resources. Moreover, as the blockchain grows in size, the execution time is further extended, leading to additional challenges in storage and system maintenance. Another critical limitation is the low throughput; current blockchain systems are constrained to an upper limit of 7 Transactions Per Second (TPS), whereas VISA, for instance, can theoretically process up to 4000 TPS [21]. Additionally, blockchain system often suffers from high latency. If there are a large number of transactions on the network, transactions may have to wait for a long time to be confirmed. These limitations significantly hinder the potential for blockchain technology to be widely adopted across various practical applications, especially in scenarios where large-scale transactions are required. The current practice of node exploration by miners is largely driven by profitability. However, as the number of nodes in a blockchain network increases, the profitability for miners diminishes due to a corresponding decrease in rewards. This situation is exacerbated when the rewards received are insufficient to offset the computational costs incurred. Consequently, many miners may choose to withdraw from the mining process. Such a reduction in active mining participation could critically undermine the network's overall computational power. As a result, the blockchain system becomes more vulnerable to security threats, including the 51% attack, double-spending attacks, and Distributed Denial-of-Service (DDoS) attacks. This degradation in computing power directly compromises the integrity and security of the blockchain network. These disadvantages are not easily surmountable, thus hinder the further development and widespread application.

However, researchers have proposed some strategies to overcome these challenging drawbacks. For example, to enhance the efficiency of RSA encryption, Großschädl et al. [22] introduced an effective hardware multiplier utilizing the RSAγ crypto chip to optimize the algorithms involved, particularly for modular arithmetic. This approach significantly facilitates the processing of long integers, thereby reducing the time complexity from n^3 to n^2 for n-bit numbers. Furthermore, in the Chinese Remainder Theorem (CRT) mode, the computational resources required for decryption are substantially diminished and the decryption rate is increased to 2 Mbit/s. Consequently, the throughput of RSA encryption increases proportionately. In addition, to address the scalability challenge faced by blockchain systems, researchers have offered several profound insights. For example, Zamani et al. [23] proposed a model which is promising to improve the capacity of throughput and lower latency by employing sharding techniques within blockchain. Sharding partitions network into numerous relatively small and independent blocks, which allows each block to be executed simultaneously, thereby improving overall network efficiency. Moreover, refined consensus protocols, such as Proof of Authority (PoA) and PoS, have been proved to have potential to increase efficiency compared with previous consensus protocols. Furthermore, the restructuring of blockchain architecture has been identified as a viable approach, however, research in this domain remains limited, highlighting the necessity for further in-depth investigation and development.

4 Conclusion

The paper provides an analytical review of the fundamental properties and the workflow of blockchain technology. It is suggested that the application of blockchain extends beyond the financial sector, demonstrating its versatility across diverse industries. The paper presents an overview of blockchain applications within healthcare, logistics and transportation, detailing

how it has been integrated into these sectors. This integration is illustrated by summarizing some of the existing proposals and frameworks developed by various researchers. Basically, blockchain technology has the potential to significantly enhance both data security and accessibility within the domains of healthcare and logistics management. It serves as a pivotal element in enabling remote patient monitoring, thereby facilitating healthcare professionals in their patient care duties and fostering a safer environment for patients. Furthermore, the transparent framework of blockchain technology enhances traceability within cold chain logistics. Additionally, it plays a crucial role in the transportation sector by aiding in the establishment of intelligent transportation systems, which secure data storage and improve traffic conditions. However, due to the inherent limitations of blockchain and the constraints of current implementation methods, the widespread adoption of blockchain faces several challenges. These obstacles indicate a need for further refinement and optimization to achieve broader acceptance and usability. Fortunately, despite many unresolved issues, substantial studies have been conducted to address these shortcomings, resulting in significant progress toward improving their deficiencies, thus providing a strong foundation for more effective and promising methods in the near future.

References

1. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba. Blockchain technology innovations. In: 2017 IEEE Technology & Engineering Management Conference (TEMSCON), IEEE, pp. 137-141 (2017)
2. J. Zarrin, H. Wen Phang, L. Babu Saheer, B. Zarrin. Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Computing, 24, 2841-2866 (2021)
3. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun. A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, pp. 2567-2572 (2017)
4. T. Zhang. Privacy evaluation of blockchain based privacy cryptocurrencies: A comparative analysis of dash, monero, verge, zcash and grin. IEEE Transactions on Sustainable Computing (2023)
5. D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, C. Yang. The blockchain as a decentralized security framework [future directions]. IEEE Consumer Electronics Magazine, 7, 18-21 (2018)
6. S. Shetty, C. A. Kamhoua, L. L. Njilla. Blockchain for distributed systems security. John Wiley & Sons (2019)
7. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, pp. 557-564 (2017)
8. Y. Xiao, N. Zhang, W. Lou, Y. T. Hou. A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22, 1432-1465 (2020)
9. B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, M. Abid. HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500 (2021)
10. T. Frikha, F. Chaabane, N. Aouinti, O. Cheikhrouhou, N. Ben Amor, A. Kerrouche. Implementation of blockchain consensus algorithm on embedded architecture. Security and Communication Networks, 2021, 9918697 (2021)

11. M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas. A systematic review of the use of blockchain in healthcare. Symmetry, 10, 470 (2018)
12. E. Tijan, S. Aksentijević, K. Ivanić, M. Jardas. Blockchain technology implementation in logistics. Sustainability, 11, 1185 (2019)
13. J. Al-Jaroodi, N. Mohamed. Blockchain in industries: A survey. IEEE Access, 7, 36500-36515 (2019)
14. M. Nofer, P. Gomber, O. Hinz, D. Schiereck. Blockchain. Business & Information Systems Engineering, 59, 183-187 (2017)
15. A. Shahnaz, U. Qamar, A. Khalid. Using blockchain for electronic health records. IEEE Access, 7, 147782-147795 (2019)
16. M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian. Continuous patient monitoring with a patient-centric agent: A block architecture. IEEE Access, 6, 32700-32726 (2018)
17. N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. Islam, J. He, M. Aslam. An innovative blockchain-based secured logistics management architecture: utilizing an RSA asymmetric encryption method. Mathematics, 10, 4670 (2022)
18. X. Zhang, Y. Sun, Y. Sun. Research on cold chain logistics traceability system of fresh agricultural products based on blockchain. Computational Intelligence and Neuroscience, 2022, 1957957 (2022)
19. D. Cocîrlea, C. Dobre, L. A. Hîrţan, R. Purnichescu-Purtan. Blockchain in intelligent transportation systems. Electronics, 9, 1682 (2020)
20. D. Khan, L. T. Jung, M. A. Hashmani. Systematic literature review of challenges in blockchain scalability. Applied Sciences, 11, 9372 (2021)
21. Q. Zhou, H. Huang, Z. Zheng, J. Bian. Solutions to scalability of blockchain: A survey. IEEE Access, 8, 16440-16455 (2020)
22. J. Großschädl. High-speed RSA hardware based on Barret's modular reduction method. In: International Workshop on Cryptographic Hardware and Embedded Systems, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 191-203 (2000)
23. M. Zamani, M. Movahedi, M. Raykova. Rapidchain: Scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931-948 (2018)