International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Technology to Improve Security in Healthcare Data Breaches

[1]D. Praveena Anjelin, [2]Dr. S.Ganesh Kumar

Submitted:23/03/2023 **Revised:**26/05/2023 **Accepted:**11/06/2023

Abstract: The modernization of healthcare is now a top issue in the quickly changing technological world. Healthcare data systems now have vulnerabilities due to their centralised design, making them more prone to single points of failure, especially in the event of natural catastrophes. Blockchain technology has emerged as a highly respected answer among the wide range of technological developments that show promise in resolving data management issues in the healthcare industry. Blockchain technology is gaining popularity as a way to guarantee the confidentiality and dependability of healthcare data. The promise of blockchain technology to address a number of issues is being acknowledged, despite the fact that its use in healthcare big data management is still relatively limitedBeyond dealing with patient consents, data ownership, management of information, data inspection, security, confidentiality, tracking, indestructibility, flexible access, and resolving conflicting changes from numerous sources, blockchain technology offers a variety of advantages. Healthcare organisations can improve data management procedures and create a more stable and secure healthcare environment by implementing blockchain technology.

Keywords: *modernization, implementing, environment, ownership, procedures*

1. Introduction:

Concerns about the existing system of patient information gathering have been raised in light of the increase in security breaches that jeopardise people's privacy [2]. The idea of using a distributed ledger has showed promise in securing this sensitive information and was inspired by the concepts behind bitcoin and blockchain technology. A sizeable amount of private data is currently processed in digital formats as the healthcare sector experiences increasing digitization [3, 12, 19].

The complex task of handling various healthcare data from multiple sources, particularly the significant volume of medical data created by Internet of Things (IoT) devices, is faced by healthcare data analysts and researchers worldwide [12, 17, 21]. Healthcare data providers simultaneously face resistance when it comes to disclosing private medical information, which makes it difficult to provide individualised patient care and do in-depth data analysis [1].

Effective collaboration and communication among key stakeholders, including patients, payers, suppliers, and analysts, is essential in the field of healthcare big data. These four parties—patients, payers, suppliers, and analysts—play important roles in the healthcare sector but are also linked to security and privacy breaches. Through wearable technology or healthcare records, patients provide useful data [1]. Payers include insurance companies and other for-profit organisations that contribute money towards a patient's medical expenses. The medical records are received and stored by medical record providers, including hospitals, clinics, medical facilities, and blood banks. The data produced by these numerous sources is used by researchers and analysts. The dispersion of medical data among numerous healthcare facilities, however, has made it more difficult to keep health information securely.

Numerous centralised healthcare systems have vulnerabilities that put patients at risk of data breaches and system failure as a result of the rising frequency of cybersecurity attacks [4]. Personal and sensitive patient data loss or compromise might have serious repercussions. Additionally, the administration of patient data in current healthcare systems frequently lacks adequate security safeguards, immutability, trustworthy traceability, auditability, and transparency [5]. Blockchain technology appears as a possible remedy to these issues [6, 7, 8, 9].

2. Literature Survey:

By introducing new elements to its operations, blockchain technology has the ability to totally transform the healthcare industry. It provides opportunities to

[1]*Research Scholar. Department of DSBS, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai. Email : pd6231@srmist.edu.in*
[2]*Professor, Department of DSBS, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai. Email : ganeshk1@srmist.edu.in*

formalise and standardise data access agreements, give privacy issues top priority, and accelerate the processing of big data in healthcare. Additionally, blockchain technology increases data efficiency and promotes trust within the healthcare ecosystem [10, 11, 12, 13, 14, 15]. Blockchain is especially well-suited for managing massive data in healthcare while also reducing administrative expenses due to its intrinsic qualities, such as decentralised storage, transparency, immutability, authentication, flexible data access, interconnection, and encryption [16, 17].

Blockchain technology does away with the need for middlemen between network participants [18, 19]. Determining roles and keeping track of task completion can be difficult when handling patient medical records, which sometimes require complex data storage routines. Each procedure in a blockchain system is given a timestamp and an identity, and copies are sent to all active nodes in the network. This guarantees process transparency and traceability from beginning to end.

Because of this, any modifications or updates made to one node are instantly and equitably sent to all the others, giving worldwide accessible from any place. Without the help of humans, blockchain technology protects data integrity between endpoints. Numerous benefits result from its adoption, including greater data auditing, lower data processing costs, better data accuracy, facilitated worldwide data exchange, and increased security of data transactions. Figure 1 depicts the idea as a flow diagram, presenting a clear portrayal of the workflow, to provide a visual understanding of the process.

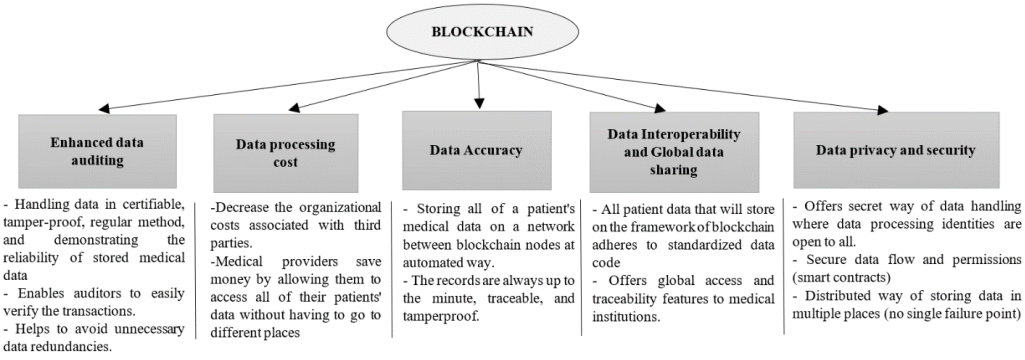

Fig 1: Attributes of blockchain

Numerous research investigating the use of blockchain technology in the healthcare sector have been conducted [6, 20–22]. However, no study has directly addressed the use of blockchain in managing massive data in healthcare. By evaluating important aspects of blockchain technology in relation to big data management in the healthcare sector, this study seeks to expand our understanding of those topics. It tries to address important aspects, implementation possibilities, challenges, and concerns with acceptance in the healthcare sector that may not have gotten enough attention in earlier research initiatives.

Numerous studies have emphasised the many advantages that blockchain technology brings to the healthcare industry, successfully tackling numerous issues. The accompanying picture provides a visual representation of how blockchain technology is being used in healthcare. Additionally, studies show that blockchain is expected to have a considerable impact on the healthcare sector by 2025, offering a workable option to reduce the dangers related to data breaches.

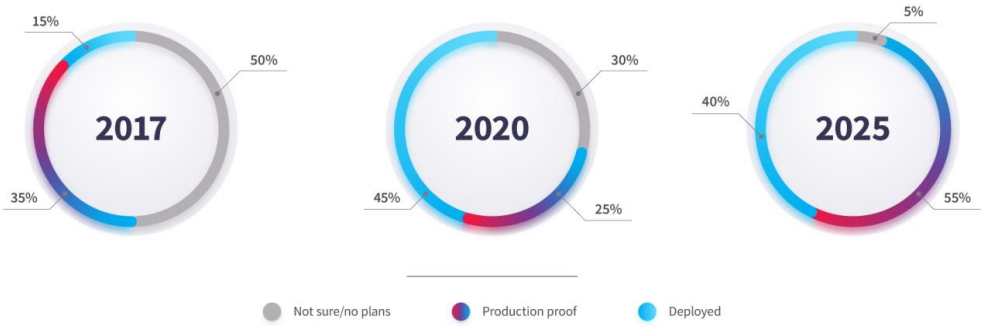

Fig 2: By 2025, blockchain

3. Installation of System:

Figure 3 below illustrates the blockchain configuration..

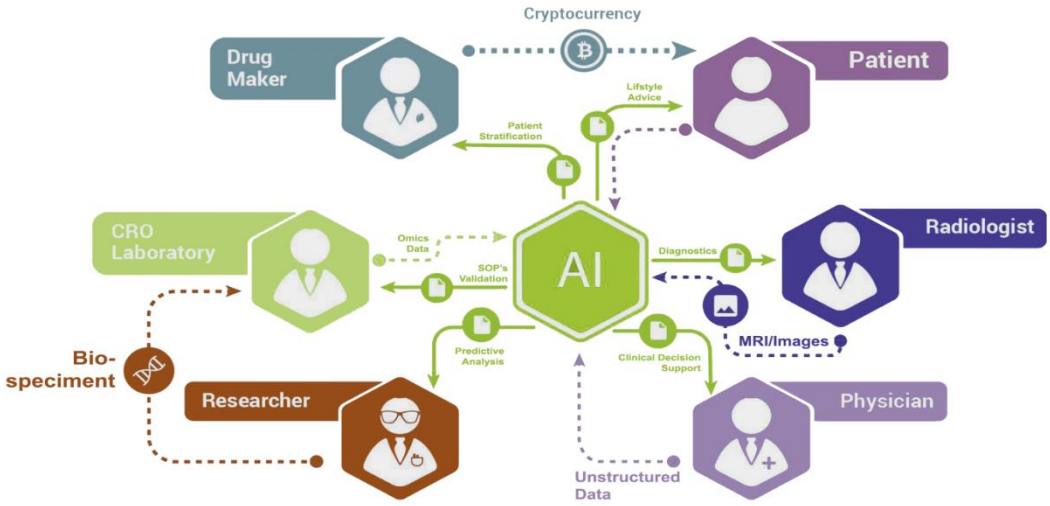

Fig 3: Structure of blockchain

Figure 3 provides a thorough picture of how blockchain technology has affected the healthcare sector, highlighting its many uses across numerous areas. Blockchain helps medical researchers decode genetic information by enabling safe medical record transfers for patients. Additionally, it is essential for controlling the drug supply chain and guaranteeing the safe transfer of patient details. Despite the fact that ALM algorithms have already been used to encrypt patient data, the possibility of data breaches still exists. The use of blockchain technology is suggested as a solution to these problems in order to stop data leaks. The arrangement shown is shown in the accompanying picture and includes a number of users, including patients, radiologists, doctors, researchers, CRO labs, medication manufacturers, and other pertinent entities. Blockchain technology makes it possible for these organisations to transact in a safe manner, improving data security and privacy.

Figure 4 shows various reasons why healthcare data breaches happen. The report reveals that the most frequent reasons for healthcare data breaches are hacking and IT incidents. Next to this, unauthorised access is a factor in healthcare data breaches.

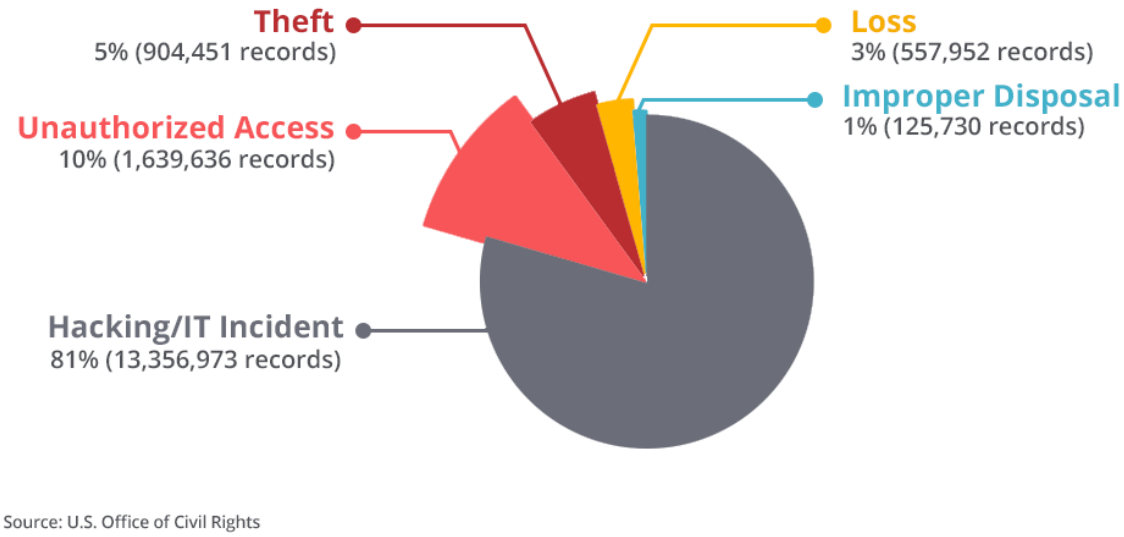

Fig 4: Numerous sources of data leaks

Thus, implementing blockchain will aid the current system in substantially reducing data leaks.

4. Application and Outcomes:

Numerous benefits are brought about by the suggested system's fusion of big data and blockchain technologies. Aware of the significance of blockchain as a crucial tool for monitoring financial transactions, decentralising patient data, and assuring security and immutability, healthcare organisations are aggressively investigating its possibilities. Transactions are securely recorded in blocks under the proposed system, prohibiting any unauthorised alteration or change. A solid framework for secure data sharing is established by the use of cryptographic algorithms. The use of cloud computing streamlines the management of patient data and makes it possible to save recorded data effectively. Smart contracts also improve data access management, enabling patients to efficiently manage their own data.

As can be seen in Figure 5 below, blockchain technology has been developed to increase security. As seen in Figure 5, blockchain layers have been developed.

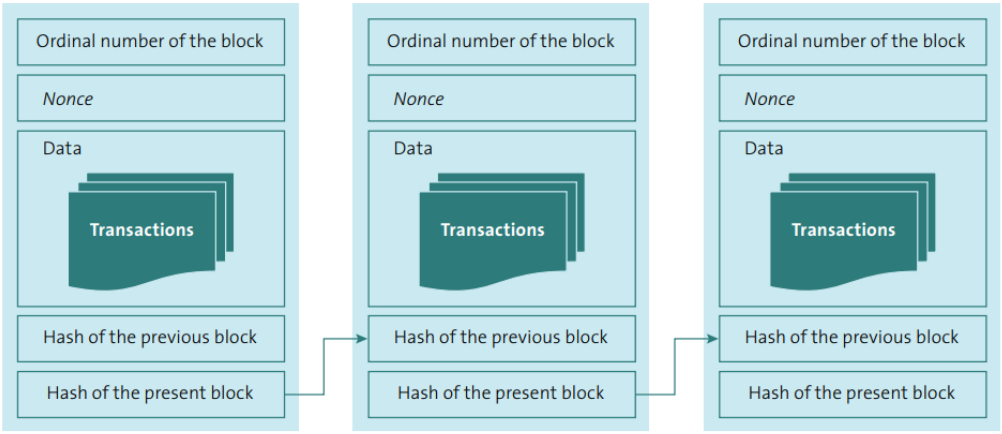

Fig 5: Levels for a proposed blockchain

The channels were then found, as demonstrated in Figure 6. The blockchain presents a total of 3 channels, including 1 global channel. The diagram is shown for the three healthcare sectors. Up to n healthcare sectors may be included in this.

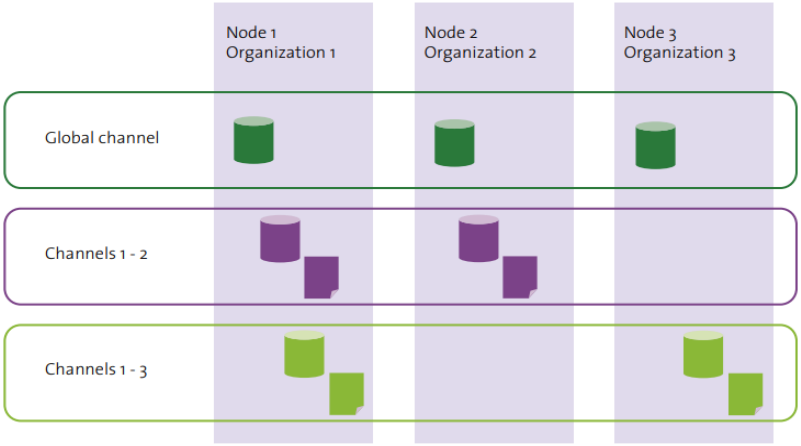

Fig 6: Blockchain channel representation

We will receive a global channel after organising the channels, and the corresponding nodes will be passed along with the planned transactions. The channels are then put into blocks, as Figure 7 below illustrates.

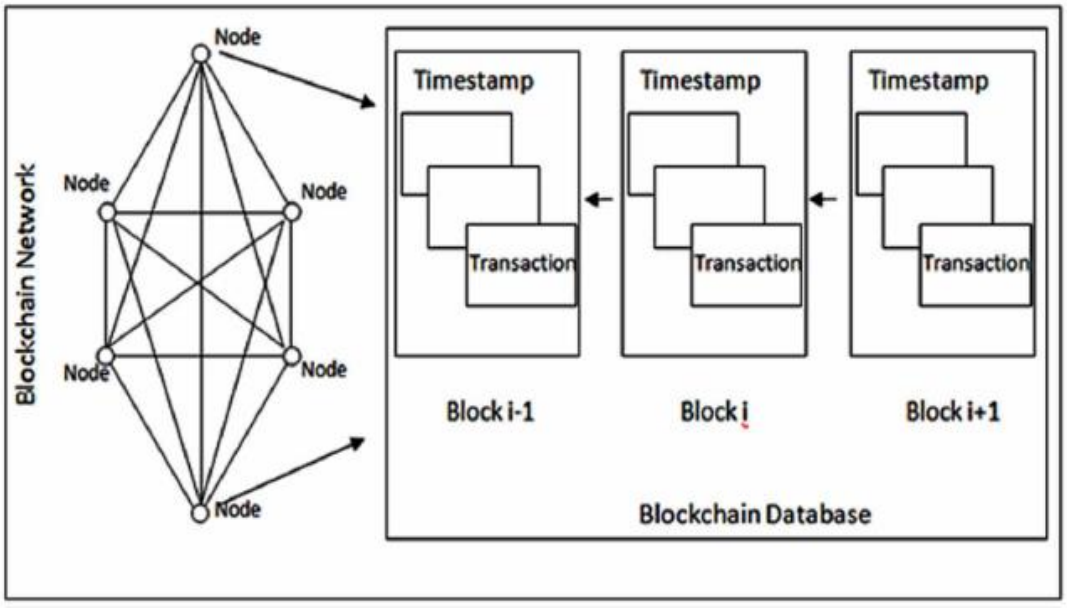

Fig 7: eEach block has a timestamp

Pharmaceutical companies may address supply chain difficulties with the help of businesses like Vibrant, built on blockchain technology. Their applications are suitable with the supply chain of the medical business and are specifically created to enable effective tracing [10]. Collaboration and monitoring may be improved with the use of this technology, saving time and resources in the process. Utilising big data analytics also makes it easier to examine how patients are treated, how they respond, and how they use their medications. These insights aid in the creation of accessible treatment alternatives and useful tools for the general populace. Figure 8 provides an illustration of the method and a sample of the code used to create blockchain for better understanding.

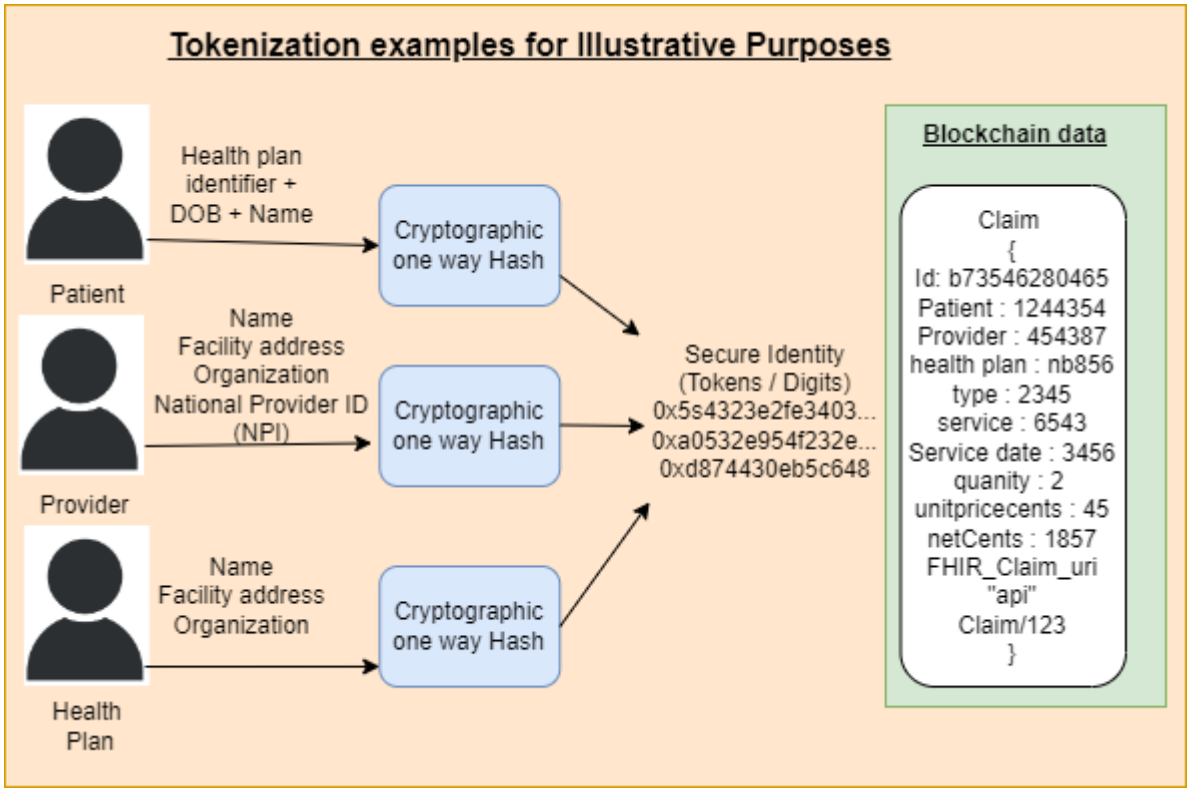

Fig 8: Process illustration for suggested blockchain-based big data solution in healthcare

The architecture of the suggested framework incorporates blockchain technology and evaluates the level of data security achieved in comparison to other blockchain algorithms. Proof of work (POW), proof of stake (POS), ripple protocol consensus algorithm (RPCA), delegated proof of stake (dPOS), stellar consensus protocol (SCP), and proof of importance (POI) are consensus methods that are frequently employed in blockchain technology. The performance of this proposed algorithm's proof of work (POW) implementation is compared to that of the POS and dPOS algorithms.

The following snippet of code for the implementation of the block chain is provided for understanding:

```
30      @property
31      def last_block(self):
32
33          return self.chain[-1]
34
35
36      def new_transaction(self, sender, recipient, amount):
37          transaction = {
38              'sender': sender,
39              'recipient': recipient,
40              'amount': amount
41          }
42          self.pending_transactions.append(transaction)
43          return self.last_block['index'] + 1
44
```

The consensus algorithm (proof of work) employed here to generate the blockchain has been compared to all other algorithms, and the findings showed that the suggested approach performs well. The outcomes are displayed in figure 9.

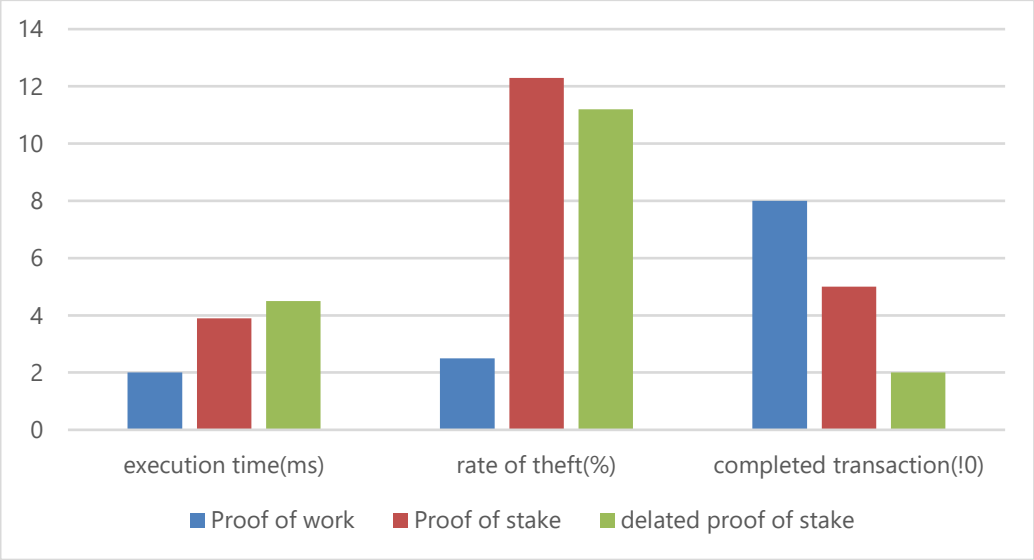

Fig 9: Comparison of the proposed algorithm's performance

The comparison between several parameters, including Execution Time, Theft Rate, and Completed Transactions over a specific time period is shown in the following graph. It has been determined that the suggested algorithm performs admirably across the board.

5. Conclusion:

The revolutionary technology known as blockchain has the potential to transform established industries. This paper's goal is to give readers a thorough grasp of blockchain and how it relates to bitcoin, with an emphasis on how bitcoin served as blockchain's inspiration. Examining the foundational ideas and architecture of blockchain is done with an emphasis on addressing security issues. Data protection accuracy of 95% or greater has been established using the suggested method deployed on the blockchain, outperforming current consensus algorithms in this area.

References:

[1] Chalaemwongwan, N., & Kurutach, W. (2018). State of the art and challenges facing consensus protocols on blockchain. International Conference on Information Networking (ICOIN), 957-962. 10.1109/ICOIN.2018.8343266

[2] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: AData Processing View of Blockchain Systems. IEEE Transactions on Knowledge and Data Engineering,30(7), 1366–1385. doi:10.1109/TKDE.2017.2781227

[3] Ishan, P. B., & Rai, G. (2018). Analysis of Cryptographic Hash in Blockchain for Bitcoin Mining Process. International Conference on Advances in Computing and Communication Engineering (ICACCE),105-110. 10.1109/ICACCE.2018.8441688

[4] Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain — Literature survey. 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2145-2148. 84

[5] A Brief Analysis of Blockchain Algorithms and Its Challenges Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2567-2572. 10.1109/SMC.2017.8123011

[6] Ogiela, M. R., & Majcher, M. (2018). Security of Distributed Ledger Solutions Based on Blockchain Technologies. IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 1089-1095. 10.1109/AINA.2018.00156

[7] Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2016). Security Services Using Blockchains: A State-of-the-Art Survey. IEEE Communications Surveys and Tutorials.

[8] Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 1-5. 10.1109/ICACCS.2017.8014672

[9] Salman Al-Nuaimi, M. A. ., & Abdu Ibrahim, A. . (2023). Analyzing and Detecting the De-Authentication Attack by Creating an Automated Scanner using Scapy. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 131–137. https://doi.org/10.17762/ijritcc.v11i2.6137

[10] Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. 2nd International Conference on Contemporary Computing and Informatics (IC3I), 463-467. 10.1109/IC3I.2016.7918009

[11] Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. International Conference on Information Networking (ICOIN), 473-475.

[12] Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. (2017). Consensus protocols for blockchain-based data provenance: Challenges and opportunities. IEEE 8th Annual Ubiquitous Computing,Electronics and Mobile Communication Conference (UEMCON), 469-474.

[13] Wang, Y., Cai, S., Lin, C., Chen, Z., Wang, T., Gao, Z., & Zhou, C. (2019). Study of Blockchains's Consensus Mechanism Based on Credit. IEEE Access: Practical Innovations, Open Solutions, 7, 10224–10231. doi:10.1109/ACCESS.2019.2891065

[14] Yuan, Y., & Wang, F. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. IEEE Transactions on Systems, Man, and Cybernetics. Systems, 48(9), 1421–1428. doi:10.1109/TSMC.2018.2854904

[15] Singh, M. ., Angurala, D. M. ., & Bala, D. M. . (2020). Bone Tumour detection Using Feature Extraction with Classification by Deep Learning Techniques. Research Journal of Computer Systems and Engineering, 1(1), 23–27. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/21

[16] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data (BigData Congress), 557-564.

[17] Yu, G., Zha, X., Wang, X., Ni, W., Yu, K., Yu, P., ... & Guo, Y. J.(2020). Enabling attribute revocation for fine-grained access control in blockchain-IoT systems. IEEE Transactions on Engineering Management, 67(4), 1213-1230.

[18] Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J.M., & Hayajneh, T. (2018). Secured data collection with hardwarebased ciphers for IoT-based healthcare. IEEE Internet of Things Journal, 6(1), 410-420.

[19] Ali, F., El-Sappagh, S., Islam, S. R., Kwak, D., Ali, A., Imran, M., & Kwak, K. S. (2020). A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion.Information Fusion, 63, 208-222.

[20] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, 102481.

[21] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 1-8.

[22] Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 95, 420-429.

[23] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.

[24] Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and futureopportunities. Computer Communications, 154, 223-235. .2021.9515747