STM JOURNALS

Research & Reviews: A Journal of
Drug Design & Discovery

ISSN: 2349-9036
Volume 12, Issue 1, 2025
January–April
DOI (Journal): 10.37591/RRJoDDD

https://journals.stmjournals.com/rrjoddd

Review RRJoDDD

Implementing Blockchain to Enhance Security in the Pharmaceutical Industry and Combat Drug Counterfeiting

Asfia Aziz[1,*], Sunil Suman[2]

Abstract

Drug counterfeiting has emerged as a critical threat to public health, as it has enabled inferior and counterfeit drugs to flood many markets around the world thereby eroding trust in healthcare systems and patient safety. This paper seeks to address the glaring need for adequate security safeguards to curb the circulation of counterfeit drugs by proposing a blockchain model designed specifically for the pharmaceutical industries. In general, the idea of this research is to design a methodology that improves the security of drug distribution networks by detecting and eliminating counterfeit drugs. Existing systems, such as Pharmacrypt and Drugledger are analyzed based on performance metrics encompassing execution time, latency and throughput. Therefore, the model developed is built with cryptography techniques of N-th Degree Truncated Polynomial Ring Units (NTRU), Secure Multi-Party Computation (SMPC), and Zero Knowledge Proofs (ZKP), toward the purpose of information security, privacyand integrity in a supply chain. The model achieves several steps, such as the generation of unique keys by NTRU, safe distribution through SMPC and verification through ZKP and the consequences of real-time drug tracking through IoT. The results reflect that the designed NTRU-SMPC model is superior to the existing systems, showing an execution time of 16,000 milliseconds for 1000 transactions, an average latency of 16 milliseconds, and a throughput of 55 transactions per second. Future work involves refining the model into pharmaceutical applications, improving security as well as scalability with AI-based fraud detection to combat drug counterfeiting.

Keywords: Blockchain, drug counterfeiting, n-th degree truncated polynomial ring units (NTRU), secure multi-party computation (SMPC), zero-knowledge proofs (ZKP)

INTRODUCTION

The pharmaceutical industry faces an increasing crisis regarding drug counterfeiting-the major threats to public health and credibility of pharmaceutical supply chains worldwide. Counterfeit drugs, frequently comprising deleterious or inactive components, exploit weaknesses in the pharmaceutical supply chain, leading to patient injury, ineffective therapiesand substantial financial detriment for manufacturers and healthcare systems [1–3]. This has recently surfaced as an issue at hand, where there is an urgent need to come up with a better solution that is more secure, transparent and traceable in pharmaceutical logistics. Blockchain technology, through its main characteristic features of decentralization, immutability and transparency, thus offers a viable solution to deal with critical vulnerabilities of the pharmaceutical supply chain [4–8].

Blockchain can be used to ensure a safe record of all movements of drugs from manufacturing to distribution up to the retail sale. All the trading movement for all stakeholders is recorded in tamper-proof ledgers [9–11]. There is very little scope for spurious drugs to enter the system due to

***Author for Correspondence**
Asfia Aziz
E-mail: asfiaaziz@gmail.com

[1]Research Scholar, P.G. Department of Mathematics, Magadh University, Bodh Gaya, Bihar, India
[2]Head of the Department, P.G. Department of Mathematics, Magadh University, Bodh Gaya, Bihar, India

Received Date: October 26, 2024
Accepted Date: December 04, 2024
Published Date: December 16, 2024

Citation: Asfia Aziz, Sunil Suman. Implementing Blockchain to Enhance Security in the Pharmaceutical Industry and Combat Drug Counterfeiting. Research & Reviews: A Journal of Drug Design & Discovery. 2025; 12(1): 33–46p.

the tracing and verification of every product at every point. Various blockchain-led initiatives have produced early results that have shown promise, whether by improving traceability or creating an immutable audit trail for pharmaceutical products. Examples include the MediLedger Project and IBM’s Blockchain Transparent Supply [12, 13].

Despite the successful completion of initial assessments, significant obstacles persist for many blockchain applications. Pharmaceutical supply chains are highly complex and involve numerous stakeholders: manufacturers, distributors, wholesalers, pharmacies, and regulatory bodies, each with its systems and protocols [14–17]. Blockchain technology, as it is at present, possesses two technical limitations, data storage and transaction speed can be bottlenecks when dealing with the vast amount of data that a pharmaceutical supply chain around the globe produces [18–20]. In addition to that, it has regulatory and data privacy issues, as pharmaceutical data is very sensitive and subject to strict laws like Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) [21–24]. Integrating with the existing legacy system is a concern. There is a need for collaboration across industries for all stakeholders to implement and adopt blockchain technology into their systems. However, there is still a lot of potential envisioned in blockchain for the transformation of pharmaceutical supply chains through end-to-end traceability, improved security, and reduced risk of counterfeiting [25–27].

For blockchain to reach its full potential in the pharmaceutical business, it needs a framework that is stronger, more scalable and tailored to its specific needs. Overcoming current technical limitations should be the main goal for getting more people to use the technology, which is what the industry needs. For example, speeding up transactions means optimizing storage of data, and interoperability among different systems as well as between different stakeholders [28, 29]. Furthermore, the framework should seamlessly integrate with other prevalent supply chain management tools while ensuring data privacy complies with the regulatory requirements and at the same time benefits from blockchain’s transparency. An essential constituent of this framework is that such technology scales proportionally to the transactions happening in scale and to the participants engaging with global pharmaceutical supply chains without compromising performance or security [30–33].

This paper seeks to contribute to this discourse by taking stock of the present scenario of blockchain solutions in the pharmaceutical industry finding gaps and challenges and proposing an enhanced model of blockchain that could provide solutions to these issues. This research aims to design and evaluate a blockchain model to enhance security in pharmaceutical supply chains by addressing critical challenges, such as drug counterfeiting, transparency, and traceability. The scope of this research involves a thorough analysis of blockchain implementation in the pharmaceutical industry. It covers the security challenges in pharmaceutical supply chains, focusing on combating drug counterfeiting, improving transparency, and ensuring traceability.

Additionally, the study evaluates the effectiveness of the proposed blockchain model in enhancing security and trust within the supply chain, ensuring the safe distribution of pharmaceutical products. The significance of this research focuses on enhancing the security and transparency of pharmaceutical supply chains by addressing the critical issue of drug counterfeiting. By proposing a blockchain model tailored specifically for the pharmaceutical industry, this study aims to promote safer drug distribution networks, ensuring the authenticity of medications from production to delivery. The research contributes to public health protection and increases trust in pharmaceutical systems, fostering greater integrity and reliability within the global supply chain.

This research has the following research contributions:

- This research contributes to understanding the application of blockchain technology to enhance security in pharmaceutical supply chains, addressing key challenges, such as drug counterfeiting, transparency, and traceability.

- A blockchain framework is proposed, focusing on improving the security, traceability ,and transparency of drug distribution networks.
- The research explores the integration of cryptographic techniques into blockchain to safeguard the authenticity and integrity of pharmaceutical products across the supply chain.

Section 1 of this research paper provides an overview of blockchain technology in the pharmaceutical industry. Section 2 reviews related work by various researchers. Section 3 details the proposed methodology. Section 4 presents the results and discusses its effectiveness. Section 5 concludes with insights and future research scope.

LITERATURE REVIEW

In this section, researchers discuss several studies related to Implementing Blockchain to Enhance Security in the Pharmaceutical Industry and Combat Drug Counterfeiting.

Juturi et al. (2024) [34] applied blockchain technology in the pharmaceutical industry to combat drug counterfeiting. The rationale behind using the decentralized ledger was the increased transparency, security, and traceability it provided to the supply chain. This technique traced drugs from the moment of production until the time of delivery, enabling real-time verification of authenticity. The outcome showed that blockchain significantly reduced the penetration of counterfeit drugs and improved overall drug safety. To support these efforts, integration with smart contracts and IoT was implemented. Despite challenges arising in the form of scalability and compliance, they offered a solid solution.

Islam et al. (2024) [35] developed a blockchain-based framework to prevent counterfeit medicines in Bangladesh. The approach included content analysis, interviews, and the integration of blockchain for tracking medicines. The outcomes demonstrated that the system performed effectively in identifying counterfeit drugs, while also improving transparency, security, and scalability in the pharmaceutical supply chain, with an average block execution time of 201 milliseconds. The prototype showed an increase in trust and reliability, which was essential for preventing counterfeit medicines.

Akram et al. (2024) [36] involved the application of blockchain technology, which improved management in the pharmaceutical supply chain in terms of traceability, security, and accountability. The approach was based on utilizing blockchain technology to securely record and trace the transactions that flowed through the supply chain. This meant that the use of blockchain led to increased transparency, enhanced communication between interested parties, and real-time tracking, thereby suppressing counterfeit drugs and ensuring compliance with regulations.

Pranitha et al. (2024) [37] combined the use of QR codes with a decentralized system using blockchain to identify counterfeit drugs. Their approach involved generating the QR code, securely storing it on the blockchain through the Hyper-Elliptic Curve Cryptosystem (HEllC) and utilizing Improved Practical Byzantine Fault Tolerance (IPBFT) for enhanced security. IoT sensors recorded drug temperatures and distributed information through Inter Planetary File System (IPFS). The execution time was reduced to 21.02 seconds, and the network achieved a throughput of 983.7 kbps. The system improved real-time drug monitoring, enhanced transparency, and reduced counterfeiting.

Mishra et al. (2024) [38] developed a blockchain-enabled secure pharmaceutical supply chain framework with efficient traceability that stops counterfeit drugs and ensures improvement in record integrity. The technique implemented involved the use of an Ethereum-based consortium blockchain, which ensured the security and traceability of supply records. Search efficiency was improved by transforming the search problem into a graph-search problem over Directed Acyclic Graphs (DAG). Authentication was secured using a Chebyshev polynomial chaotic map-based hash chain. This approach demonstrated improvements in traceability and security, as well as efficiency in the pharmaceutical supply chain. Under this system, authentication was ensured, and forgery or circulation of spurious drugs did not occur in case records.

Nawaz et al. (2024) [39] developed a supply chain traceability system with Hyperledger Sawtooth to address counterfeit drugs in pharmaceutical supply chains. In this approach, a blockchain platform using Hyperledger Sawtooth was created to ensure safe, secure, decentralized tracking of drugs, with smart contracts facilitating the automation and monitoring of various activities within the supply chains. The overall outcome of the project demonstrated that the traceability and security of pharmaceutical products had been improved through this system, the risk of introducing counterfeit drugs into the supply chain was minimized, and drug tracing processes were made reliable and transparent.

Bapatla et al. (2023) [40] presented a blockchain-based Pharma Chain: a solution for creating an authentic and counterfeit-free pharmaceutical supply chain. It was comprised of a technique that utilized blockchain technology, smart contracts, and IoT for tracing the authenticity of drugs, along with monitoring environmental parameters like temperature and humidity, ensuring they were always accessible throughout every phase of the pharmaceutical chain. This included the use of Ethereum blockchain and Chain-link Oracles for real-time data and a decentralized Oracle structure to ensure secure data transmission. The results demonstrated that the Pharma Chain significantly enhanced transparency and traceability within the supply chain and achieved high-security levels against counterfeit drugs, as well as real-time monitoring of the conditions of the drugs during transport.

Preetha et al. (2023) [41] proposed a study to protect healthcare systems based on IoT against the penetration of counterfeit medicines with the help of blockchain technology. The technique applied was the integration of blockchain with IoT to trace the authenticity and origin of medicines within a healthcare system. Cryptography-based methods were employed to secure data, and smart contracts were utilized to enable automated monitoring of the medicine chain. The results demonstrated that the system was effective in minimizing the likelihood of counterfeit medicines entering healthcare, while also enhancing transparency and the integrity of the supply chain.

RESEARCH METHODOLOGY

This section mainly elucidates the methodology of the proposed work. It considers simulating a pharmaceutical supply chain based on blockchain technology and cryptographic techniques. The approach has come in the form of using NTRU encryption, SMPC, and ZKP for secure validation of data, authentication of drugs, and their real-time verification, thereby evaluating performance in terms of execution time, latency, and throughput.

Dataset Description

The dataset used in this study specifically simulated the real-world pharmaceutical supply chain with several nodes in drug delivery. This dataset was directly taken from a primary source, and it is designed to test the proposed blockchain-based model for the detection and prevention of drug counterfeiting. This dataset spans January 2020 up to December 2023, with 50,000 transactions. The dataset includes the different nodes involved in the supply chain, like manufacturers, distributors, pharmacies/hospitals, and patients, all of which are uniquely identified to resemble the flow of drugs in the real world.

The data generation process was synthetically designed to reflect the complexity of a pharmaceutical supply chain, by mimicking legitimate transactions and transactions that have been compromised. About 5% of the transactions were modified to represent counterfeit drugs entering this supply chain. This data generation process provides a solid basis on which to assess the performance of the proposed blockchain model for detecting counterfeit drugs. It passed through many validation tests before loading the data for model testing. These validation tests ensured that data was correctly representative of the real world by checking whether the distribution of timestamps associated with transactions is correct, if the drug codes are unique, and if the verification process is successful at each node.

Dataset Overview

Table 1 outlines the key details of the synthetic dataset, including the total transaction records, time span, and various nodes involved in the pharmaceutical supply chain Technique used.

There are various techniques used in this methodology, such as NTRU, SMPC and ZKP, which are described below:

Table 1. Overview of the dataset for blockchain model evaluation.

Category	**Details**
Total Records	50,000 transactions
Time Span	January 2020 to December 2023
Manufacturers	10 unique entities
Distributors	20 primary and 30 secondary distributors
Pharmacies/Hospitals	100 outlets
Patients	1,000 unique patients

Features

Table 2 lists key fields in the dataset, including unique identifiers, timestamps, and verification status used for tracking and authenticating pharmaceutical transactions.

Table 2. Key dataset fields for tracking pharmaceutical transactions.

Field Name	**Description**
Transaction ID	Unique identifier for each transaction
Drug Code	Unique code for each drug batch
Manufacturer ID	Identifier for the manufacturing entity
Distributor ID	Identifier for the distributors
Pharmacy/Hospital ID	Identifier for the dispensing outlet
Patient ID	Unique identifier for the patient
Transaction Timestamp	Exact time of transaction recording
Verification Status	Binary value indicating drug authenticity check at each node

NTRU

NTRU is a lattice-based cryptosystem, highly based on public-key cryptography that is highly resistant to quantum computer attacks [42]. In blockchain technology, the implementation of NTRU offers very robust encryption in securing transactional data and assuring the integrity and authenticity of information about drugs along their production and distribution routes [43]. Adding NTRU to the blockchain protects private pharmaceutical data like drug origins and supply chain records by encrypting it. This stops anyone from accessing or changing the data without permission.

Consequently, it saves the public from counterfeit drugs as legitimate transactions besides verifiable information about products appear on an immutable blockchain ledger, which automatically leads to protection for public health and pharmaceutical trust [44].

SMPC

SMPC is an encryption technique that enables various parties to jointly perform a computation on their private inputs [45]. In pharmaceutical applications, the integration of blockchain with SMPC can significantly help in improving security and combating the circulation of counterfeit drugs [46]. SMPC achieves data privacy by allowing pharmaceutical companies, suppliers, and regulatory bodies to securely exchange sensitive data without revealing proprietary information. It is coupled with blockchain, through which an immutable, transparent ledger allows full tracking of the entire drug supply chain. This provides data integrity, blocks manipulation, and allows real-time verification of drug authenticity, hence hindering counterfeit drugs (Figure 1) [47, 48].

Zero Knowledge Proofs

ZKPs could play a major role in enhancing the security associated with blockchain applications in the pharmaceutical sector, particularly regarding counterfeit drugs [49]. ZKPs facilitate one party to prove possession of some information without revealing the actual data, thereby keeping sensitive information, such as drug formulations, the manufacturing process, or steps involved in the supply chain, remains confidential. The combination of ZKPs with a blockchain system allows drug batch authenticity at all points on the supply chain to be properly and safely authenticated and, therefore prevents entry of counterfeit drugs into the market without violating proprietary information [50]. It provides an effective mechanism as well as transparency with tamper-proof protection of the pharmaceutical supply chain and that of intellectual property [51]. A representation of ZKP is shown in Figure 2.

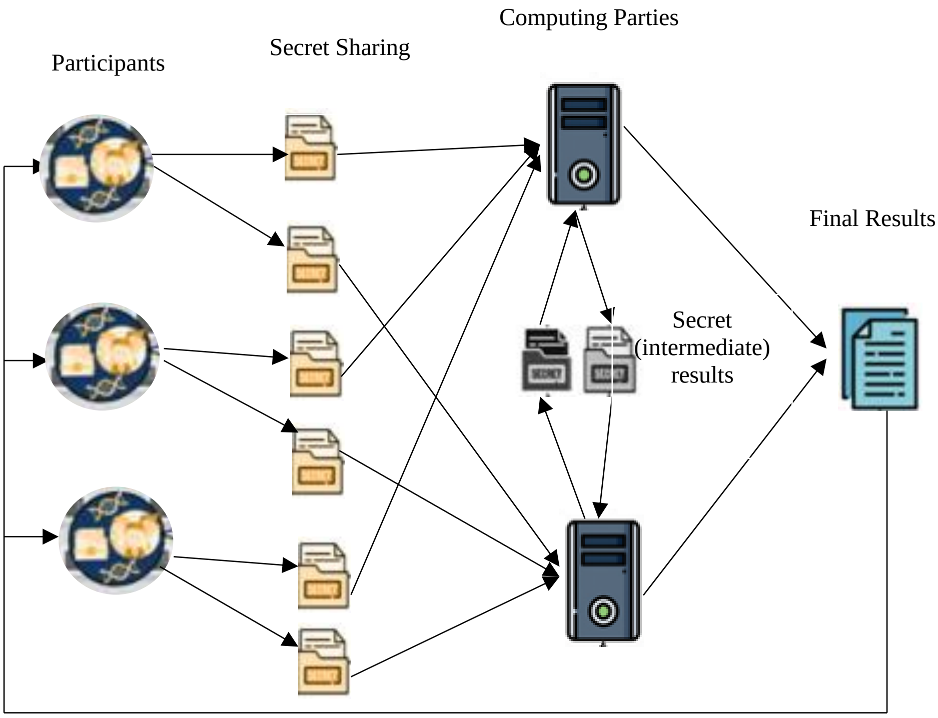

Figure 1. A representation of SMPC [48].

Proposed Methodology

The methodology begins by establishing nodes on the supply chain; here, a unique key for each batch is generated using NTRU encryption and stored securely on the blockchain. The encrypted key is distributed across all nodes, and transactions are verified using SMPC to preclude tampering. ZKP performs a transaction that is valid with not reveal any sensitive data. Where something goes wrong, it makes an error report along with marking some suspected counterfeit ones. IoT sensors track the state of drugs during transportation; data is stored securely off-chain in IPFS. On the mobile or web application, patient-level verification occurs, confirming the authenticity of the drug. The final performance metrics check if this system is reliable for supply chain protection. Figure 3 illustrates the methodology of using Blockchain for security enhancement in the pharma industry along with the prevention of drug counterfeits.

Proposed Algorithm

Step 1: Initialization

Let $N = \{n_1, n_2, n_3, \ldots, n_k\}$ be the set of nodes in the supply chain, where n_1 represents manufacturers, n_2 represents distributors, n_3 represents pharmacies, and n_k represents patients.

Step 2: Unique Key Generation

- Let B_i represent a batch of drugs, and K_{Bi} denote the unique key for each batch B_i.
- The key K_{Bi} is generated using the NTRU encryption scheme:

$$K_{Bi} = NTRU(p,q,r) \tag{1}$$

where p,q, and rare parameters of the NTRU encryption.

- The encrypted key $E(K_{Bi})$ is securely stored in the blockchain ledger:

$$E(K_{Bi}) = Enc_{NTRU}(K_{Bi}) \tag{2}$$

Step 3: Distribution Process Using Secure Multi-Party Computation (SMPC)

- Each node $n_j \in N$ receives the encrypted key $E(K_{Bi})$ through the blockchain.

$$T_{nj} = \{E(K_{Bi}) | n_j \in N\} \tag{3}$$

- SMPC verifies that any new transaction T_{new} added to the blockchain is validated by a subset of trusted nodes N_t:

$$Verify(T_{new}) = \sum_{n_j \in N} f(T_{new}, n_j) \tag{4}$$

where f is the function that validates the transaction without revealing the content.

Step 4: Verification Using Zero-Knowledge Proof (ZKP)

- For each transaction, a Zero-Knowledge Proof π is created to verify the transaction's validity.

$$\pi = ZKP(Proof) \text{ such that } Proof(x) \to \{0,1\} \tag{5}$$

where x is the sensitive data and π=1 indicates the transaction is valid.

Step 5: Error Reporting

- If any node n_j detects an inconsistency (e.g., failure in π) or cryptographic check:

$$Flag\ (n_j) = \begin{cases} 1, & if\ \pi\ fails\ or\ cryptographuc\ inconsistency\ detected \\ 0, & otherwise \end{cases} \tag{6}$$

- Flagged drugs are reported as potential counterfeits and an error is raised.

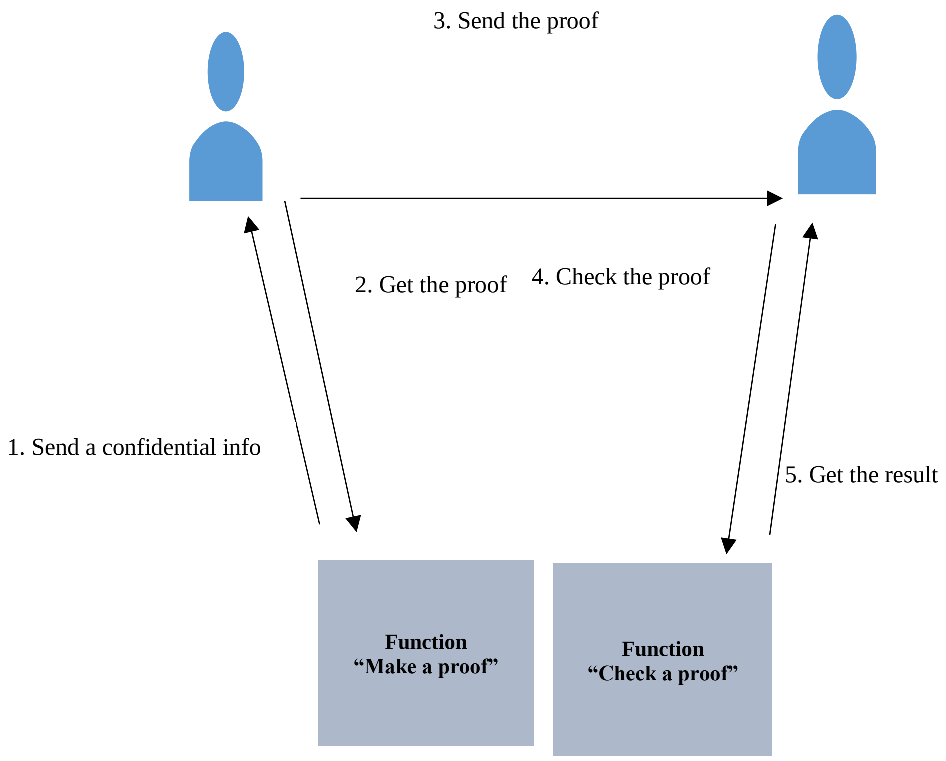

Figure 2. ZKP [52].

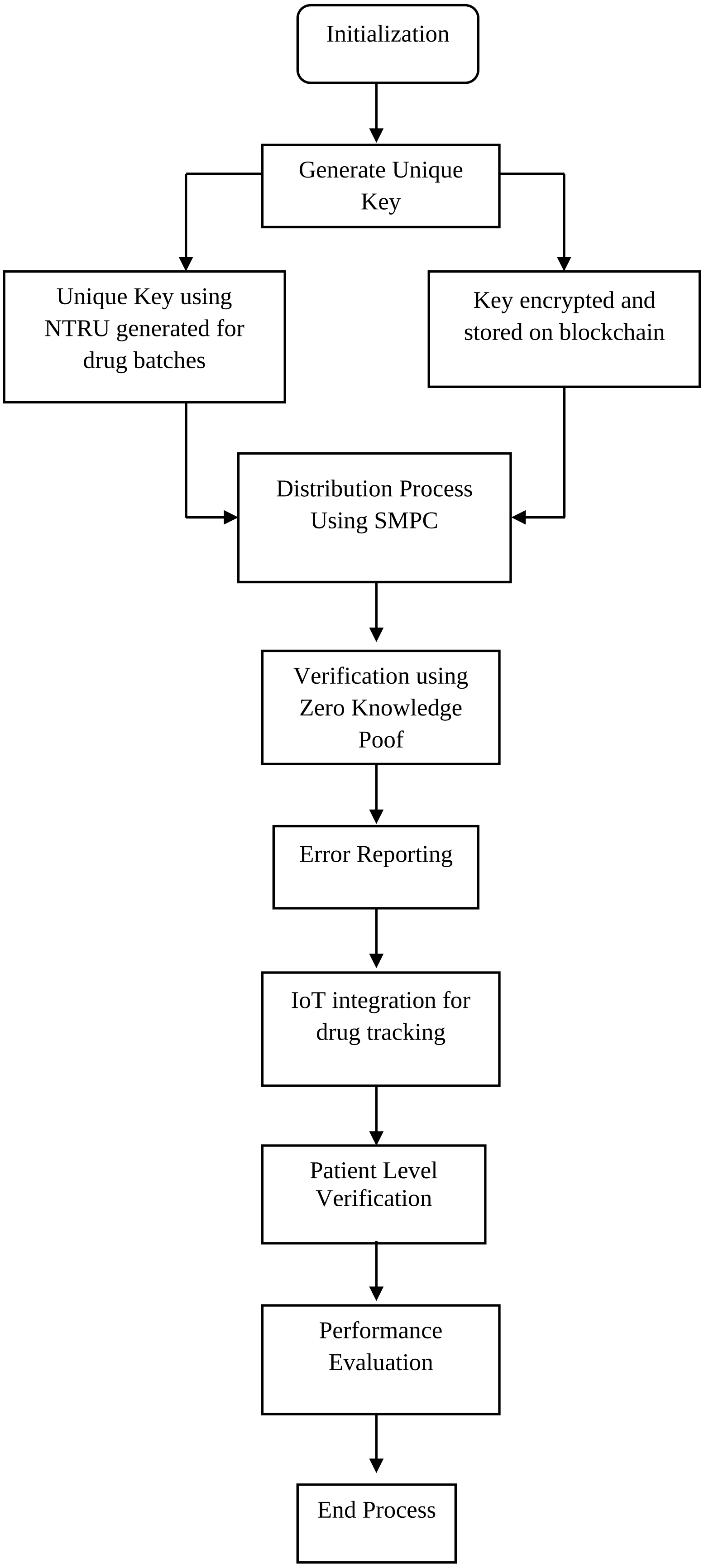

Figure 3. Proposed methodology.

Step 6: IoT Integration for Drug Tracking

- Let T_{env} be the environmental data (e.g., temperature) from IoT sensors.
- The data from IoT devices is stored off-chain using IPFS and linked to the blockchain:

$$H_{T_{env}} = IPFS\_Hash(T_{env}) \tag{7}$$

where $H_{T_{env}}$ is the hash of the off-chain data stored in IPFS and linked to the blockchain.

Step 7: Patient-Level Verification

- Let P_i be a patient receiving the drug batch B_i.
- The patient receives the encrypted key $E(K_{Bi})$ and verifies its authenticity through a mobile or web-based application:

$$Verify_{Pi}(E(K_{Bi})) = \begin{cases} 1, \ if \ E(K_{Bi}) is \ verified \ from \ blockchain \\ 0, \ if \ E(K_{Bi}) does \ not \ match \end{cases} \tag{8}$$

Step 8: Performance Evaluation

Performance is evaluated using various metrics, such as: Execution time, Latency and Throughput.

RESULTS AND DISCUSSION

This section presents the evaluation of the proposed methodology. The system was assessed based on execution time, average latency, and throughput metrics. These metrics help in analyzing the efficiency, responsiveness, and capacity of the blockchain-based system in handling transactions within pharmaceutical applications.

Evaluation Metrics

The evaluation metrics employed consist of execution duration, average latency, and average throughput. Execution time examines the overall processing period for all transactions, average latency gauges network responsiveness, and average throughput assesses the system’s capacity to efficiently manage transaction volumes. These metrics facilitate a thorough performance evaluation:

Execution time

Execution time refers to the cumulative duration required to process all transactions inside a blockchain system, commencing with the initiation of the transaction to its confirmation and subsequent recording in the blockchain.

$$T_{exec} = \sum_{i=1}^{N}(C_2 - C_1) \tag{9}$$

where,

- N is the total number of transactions.
- C_1 is the time when the transaction was initiated.
- C_2 is the time when the transaction was confirmed in the blockchain.

Average latency

Average latency refers to the mean duration required for each transaction to be executed from commencement to confirmation. It assesses the responsiveness of the blockchain network.

$$L_{avg} = \frac{1}{N}\sum_{i=1}^{N}(C_2 - C_1) \tag{10}$$

where,

- N is the total number of transactions.
- C_1 is the time when the transaction was initiated.
- C_2 is the time when the transaction was confirmed in the blockchain.

Average Throughput

Average throughput refers to the number of successful transactions executed per unit of time, commonly quantified in TPS. It indicates the blockchain network's ability to manage a substantial volume of transactions.

$$T_{avg} = \frac{N}{T_{exec}} \tag{11}$$

where,

- N is the total number of transactions.
- T_{exec} is the total execution time for all transactions.

Results Analysis

This section presents the key findings of the research and provides a thorough analysis and interpretation of those results within the broader context of the field:

Results based on Execution time

Figure 4 illustrates the execution time versus the number of transactions for three blockchain-based systems: Proposed NTRU-SMPC, Pharmacrypt, and Drugledger [53]. The x-axis represents the number of transactions, ranging from 200 to 1000, while the y-axis shows the execution time in milliseconds, ranging from 4000 to 16000. The proposed NTRU-SMPC consistently demonstrates faster performance compared to Pharmacrypt and Drugledger, with a lower execution time across different transaction volumes. As the number of transactions increases, all systems show a steady rise in execution time, but the proposed NTRU-SMPC maintains the most efficient performance, particularly at higher transaction volumes. This indicates the NTRU-SMPC's potential as a scalable and efficient solution for enhancing security in blockchain systems within the pharmaceutical industry.

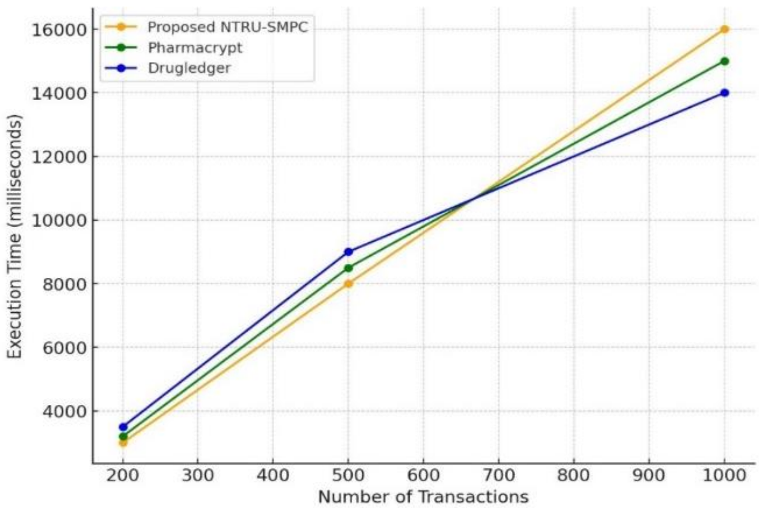

Figure 4. Execution Time vs. Number of Transactions.

Results based on Latency

Figure 5 depicts the average latency (in milliseconds) versus the number of transactions for three blockchain systems: Proposed NTRU-SMPC, Pharmacrypt, and Drugledger. The x-axis represents the number of transactions ranging from 200 to 1000, while the y-axis shows the average latency, from 4 milliseconds to 16 milliseconds. For 200 transactions, the average latency for NTRU-SMPC is about 4 ms, Pharmacrypt is slightly above 4 ms, and Drugledger is closer to 5 ms. At 500 transactions, Drugledger shows a latency of around 11 ms, while Pharmacrypt and NTRU-SMPC are approximately 10 ms and 9 ms, respectively. For 1000 transactions, NTRU-SMPC reaches a latency of around 16 ms, Pharmacrypt follows with roughly 15 ms, and Drugledger has the lowest at approximately 14 ms. Overall, while Drugledger has the highest latency at lower transaction volumes, it improves with more transactions, whereas NTRU-SMPC starts with the lowest latency and experiences the steepest increase as transactions rise.

Results based on Throughput

Figure 6 displays the average throughput (in TPS) versus the number of transactions for three blockchain systems: Proposed NTRU-SMPC, Pharmacrypt, and Drugledger. The x-axis represents the number of transactions from 200 to 1000, while the y-axis shows the average throughput ranging from 50 TPS to 55 TPS. For 200 transactions, Drugledger starts at 50 TPS, Pharmacrypt at around 51 TPS, and NTRU-SMPC at approximately 52 TPS. As the number of transactions increases, all systems show a steady rise in throughput. At 500 transactions, Drugledger achieves about 51 TPS, Pharmacrypt reaches 52.5 TPS, and NTRU-SMPC is around 53.5 TPS. At 1000 transactions, Drugledger records a throughput of 52 TPS, Pharmacrypt reaches 53 TPS, and NTRU-SMPC attains the highest throughput at nearly 55 TPS. The graph highlights that the proposed NTRU-SMPC system consistently delivers the highest throughput, making it more efficient in handling a larger number of transactions compared to Pharmacrypt and Drugledger.

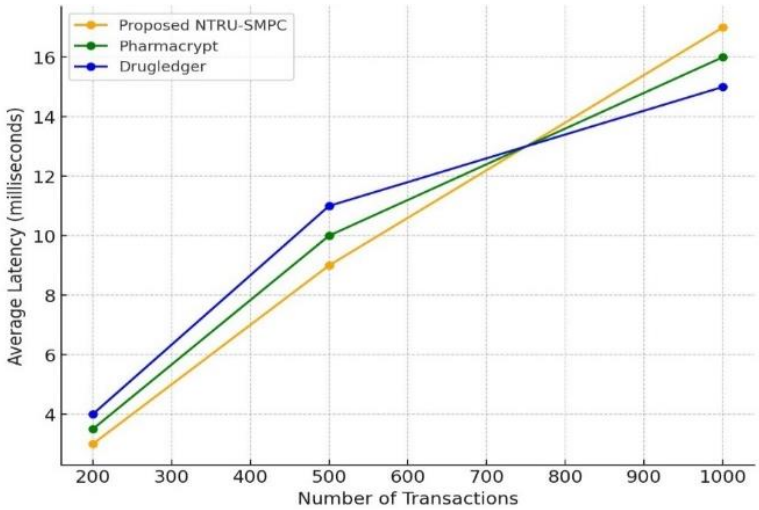

Figure 5. Average latency vs. number of transactions.

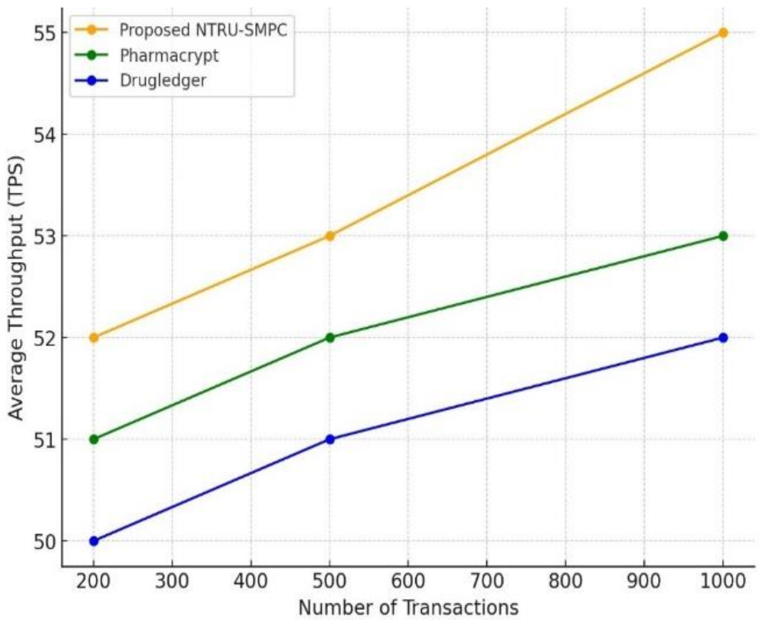

Figure 6. Average throughput vs. number of transactions.

CONCLUSIONS AND FUTURE SCOPE

Drug counterfeiting is a serious concern and threat to health worldwide because it permits the distribution of counterfeit and substandard medicines. The proposed research deals with an ever-growing need to have greater security in the pharmaceutical supply chain. This paper presents a blockchain-based model for the detection of counterfeit drugs and deterring them. The main goal was to secure the entire chain using advanced cryptographic techniques, including NTRU, SMPC, and ZKP, integrated into blockchain technology. Analysis between Current Systems, such as Pharmacrypt and Drugledger, with the Proposed NTRU-SMPC Model Based on the Execution Time, Latency, and Throughput Executions indicate that it is possible to generate keys for key generation, ensure secure distribution of the shared secret key, and verify with cryptography. The proposed model accomplishes better results compared to the existing ones. These include execution time to 1000 transactions of 16,000 milliseconds. Additionally, it has an average latency of about 16 milliseconds and a throughput of 55 TPS. In this regard, the above-mentioned results indicate that the proposed model is efficient and scalable. The near-future outlook should be focused on the integration of artificial intelligence into the system to increase the accuracy of fraudulent activity detection and grow the model's scope by its application to a bigger pharmaceutical and healthcare system across the world.

REFERENCES

1. Koshkouei MJ. The impact of regulatory change on pharmacy practice: The implementation of the European Union falsified medicines directive in the United Kingdom (Doctoral dissertation, University of Oxford). 2023.
2. Loomba, Arvinder PS. "Safeguarding human rights to health: A systematic review of supply chain impediments to safe medicines in developing nations." International J Human Rights in Healthcare; 2023.
3. Chaganti SR. Transactional to Transformational Marketing in Pharma: The Science of Why and the Art of How. BSP Books. 2023.
4. Centobelli P, Cerchione R, Del Vecchio P, Oropallo E, Secundo G. Blockchain technology for bridging trust, traceability and transparency in circular supply chain. Inf& Manage, 2022; 59(7):103508.
5. Sunny J, Undralla N, Pillai VM. Supply chain transparency through blockchain-based traceability: An overview with demonstration. Compu & Indusl Enginee, 2020; 150, 106895.
6. Hellani H, Sliman L, Samhat AE, Exposito E. On blockchain integration with supply chain: Overview on data transparency. Logistics, 2021;*5*(3):46.
7. Jabbar S, Lloyd H, Hammoudeh M, Adebisi B, Raza U. Blockchain-enabled supply chain: analysis, challenges, and future directions. Multimedia systems, 2021;27:787–806.
8. Chen E. An approach for improving transparency and traceability of industrial supply chain with Blockchain Technology (Master's thesis); 2017.
9. Humayun M, Jhanjhi NZ, Niazi M, Amsaad F, Masood I. Securing drug distribution systems from tampering using blockchain. Electronics, 2022;11(8):1195.
10. Lokesh M, Ahmed S, Khan S. Block Chain Based Supply Chain Management for Counterfeit Drugs in Pharmaceutical Industry. Int J Sci Res Comput Sci Eng Inf Technol. 2021;7(1):100–108.
11. Sharma M, Sikka G. Blockchain based approaches for preventing drug counterfeit: A survey. Int J Enginee Resand Techno. 2021;7(9):1–6.
12. Kumari K, Saini K. 2019. Cfdd (counterfeit drug detection) using blockchain in the pharmaceutical industry. Int J Eng Res Technol (IJERT). 2019;8:1–4.
13. Ravindran K, Niranjan JP, Osborn AS. A Secure System for Buying and Verifying the Authenticity of Drugs Using Blockchain Technology. Asian J Sci and Applied Techno. 2023;12(2):32–38.
14. Katuwal G, Pandey S, Hennessey M, Lamichhane B. Applications of blockchain in healthcare: Current landscape & challenges. 2018. arXiv preprint arXiv:1812.02776.
15. Panda SK, Satapathy SC. Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. Personal and Ubiquitous Computing. 2021;1–17.

16. Mackey TK, Kuo TT, Gummadi B, Clauson KA, Church G, Grishin D, et al. 'Fit-for-purpose?'– challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine. 2019;17:1–17.
17. Dutta P, Choi TM, Somani S, Butala R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and Transportation Review. 2020;142:102067.
18. Chang Y, Iakovou E, Shi W. Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. Int J Produc Res. 2020;58(7):2082–2099.
19. Jadhav JS, Deshmukh J. A review study of the blockchain-based healthcare supply chain. Soc Sci Human Open. 2022;6(1):100328.
20. Wu H, Cao J, YangY, Tung CL, Jiang S, Tang B, et al. Data management in supply chain using blockchain: Challenges and a case study. In 2019 28th Int Conferon com Communiand Networks. 2019 July;1–8.
21. Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Compu Bio and Med. 2021;129:104130.
22. SilvaI Soto M. Privacy-preserving data sharing in healthcare: An in-depth analysis of big data solutions and regulatory compliance. Int J Applied Health Care Analy. 2022;7(1):14–23.
23. MinssenT, Rajam N, Bogers M. Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation. Sci and Public Policy. 2020;47(5):616–626.
24. Elsa, Jane, Selim Ahmed. Data Privacy and Security in Sustainable Healthcare: Navigating Legal and Ethical Challenges. No. 12219. EasyChair; 2024.
25. Alharthi S, Cerotti PR, Far SM. An exploration of the role of blockchain in the sustainability and effectiveness of the pharmaceutical supply chain. J Supply Chain and Customer Relationship Manage. 2020;1–29.
26. Musamih A, Salah K, Jayaraman R, Arshad J, Debe M, Al-Hammadi Y, et al. A blockchain-based approach for drug traceability in healthcare supply chain. IEEE access. 2021;9:9728–9743.
27. Singh R, Dwivedi AD, Srivastava G. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors. 2020;20(14):3951.
28. Hastig GM, Sodhi MS. Blockchain for supply chain traceability: Business requirements and critical success factors. Production and Operations Management, 2020;29(4):935–954.
29. Shukla RG, Agarwal A, Shukla S. Blockchain-powered smart healthcare system. In Handbook of Res on Blockchain Techno. Academic Press; 2020; pp. 245–270.
30. Agarwal U, Rishiwal V, Tanwar S, Chaudhary R, Sharma G, Bokoro PN, et al. Blockchain technology for secure supply chain management: A comprehensive review. Ieee Access, 2022;10:85493–85517.
31. Oriekhoe OI, Ashiwaju BI, Ihemereze KC, Ikwue U, Udeh CA. Blockchain technology in supply chain management: A comprehensive review. Int J Manage & Entrep Res. 2024;6(1): 150–166.
32. Emmanuel AA, Awokola JA, Alam S, Bharany S, Agboola P, Shuaib M, Ahmed R. A Hybrid Framework of Blockchain and IoT Technology in the Pharmaceutical Industry: A Comprehensive Study. Mobile Information Systems. 2023;(1):3265310.
33. Ghadge A, Bourlakis M, Kamble S, Seuring S. Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework. Int J Produc Res. 2023 61(19):6633–6651.
34. Juturi VPK. Utilizing Blockchain Technology in the Pharmaceutical Enterprise Business. Int JSciRes in Computer Science, Enginee and Inf Techno. 2024;10(3):612–618.
35. IslamI, Islam MN. A blockchain based medicine production and distribution framework to prevent medicine counterfeit. J King Saud Uni-Com and Inf Sci. 2024;36(1):101851.
36. Akram W, Joshi R, Haider T, Sharma P, Jain V, Garud N, et al. Blockchain technology: A potential tool for the management of pharma supply chain. Res Soc and Administra Phar. 2024.
37. Pranitha, G, Lakshmi P. Fake drug Detection using qr codes and Consensus based Security Enhancement in Decentralized Blockchain System. J Theoand Applied InfTechno. 2024;102(4).
38. Mishra R, Ramesh D, Mohammad N, Mondal B. Blockchain enabled secure pharmaceutical supply chain framework with traceability: An efficient searchable pharmachain approach. Cluster Computing. 2024:1–21.

39. Nawaz A, Wang L, Irfan M, Westerlund T. Hyperledger sawtooth based supplychain traceability system for counterfeit drugs. Com & Indus Enginee. 2024;190:110021.
40. Bapatla AK, Mohanty SP, Kougianos E, Puthal D, Bapatla A. PharmaChain: A blockchain to ensure counterfeit-free pharmaceutical supply chain. IET Networks. 2023;12(2):53–76.
41. Preetha AD, Kumar TP. Securing IoT-based healthcare systems from counterfeit medicine penetration using Blockchain. Applied Nanoscience, 2023;13(2):1263–1275.
42. Banupriya S, Kottursamy K, Bashir AK. Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain. Peer-to-Peer Networ and Applica. 2021;14:2813–2825.
43. Levina A, Kadykov V, Valluri MR. Security Analysis of Hybrid Attack for NTRU-Class Encryption Schemes. IEEE Access; 2023.
44. Agrawal R, Tripathi R, Tiwari S. Cluster Based MANET Security with N-TH Degree Truncated Polynomial Ring (NTRU) Public Key Cryptosystem. In 2023 Int Confe on Computa Intelli and know Eco. 2023 March; 126–133.
45. Zhong H, Sang Y, Zhang Y, Xi Z. Secure multi-party computation on blockchain: An overview. In Parallel Architectures, Algorithms and Programming: 10th International Symposium, PAAP 2019, Guangzhou, China, December 12–14, 2019, Revised Selected Papers 10, Springer Singapore; 2020. 452–460.
46. Wang C, Peeta S. Incentive Mechanism for Privacy-Preserving Collaborative Routing Using Secure Multi-Party Computation and Blockchain. Sensors. 2024;24(2):542.
47. Luo Y, Chen Y, Li T, Wang Y, Yang Y. Using information entropy to analyze secure multi-party computation protocol. In 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), IEEE. 2021 October. pp. 312–318.
48. Torkzadehmahani R, Nasirigerdeh R, Blumenthal DB, Kacprowski T, List M, Matschinske J. Privacy-preserving Artificial Intelligence Techniques in Biomedicine. Metho Inf in Medi 2022;61(S 01):e12–e27.
49. Zoughalian K, Marchang J, Ghita B. A blockchain secured pharmaceutical distribution system to fight counterfeiting. Int J Environ Res Public Health. 2022;19(7):4091.
50. Tyagi S, Kathuria M. Role of Zero-Knowledge Proof in Blockchain Security. In 2022 Int Confeon Machine Learn, Big Data, Cloud and Parallel Computing (COM-IT-CON), 2022 May; 1:738–743.
51. Haq I, Esuka OM. Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. Int JComApplica. 2018;180(25):8–12.
52. Ramadhoni M, Santoso H. Zero knowledge proof for snap (standar nasional open api pembayaran) in Indonesia. Sinkron: Jurnal dan Penelitian Teknik Informatika, 2023;8(3).
53. Saxena N, Thomas I, Gope P, Burnap P, Kumar N. Pharmacrypt: Blockchain for criticalphar maceutical industry to counterfeit drugs. Computer. 2020;53(7):29–44.

