International Journal of Basic and Applied Sciences, 14 (7) (2025) 568-575

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/d684hb30
Research paper

Strengthening Drug Supply Chain Integrity and Security with Blockchain

Priyadharshini S. [1], Sathya Priya J. [2]*, Parameswari M. [3], Muthulakshmi K. [4]

[1] Assistant Professor, Department of Information Technology, Velammal Engineering College, Chennai, India
[2] Professor, Department of Information Technology, Velammal Engineering College, Chennai, India
[3] Professor, Department of Computer Science and Engineering, King's Engineering College, Chennai, India
[4] Associate Professor, Department of Information Technology, Panimalar Engineering College, Chennai, India
**Corresponding author E-mail: dr.sathyapriyaanand@gmail.com*

Received: September 29, 2025, Accepted: November 8, 2025, Published: November 29, 2025

Abstract

Ensuring the integrity and openness of its supply chain is a major concern for the pharmaceutical business. Through the development of an auditable, decentralized tracking system that guarantees the authenticity of pharmaceuticals from manufacture to end-user, this system uses blockchain technology to combat the problem of counterfeit medications. The solution reduces information asymmetry, promotes trust, and improves stakeholder cooperation through the use of a shared ledger. Smart contracts enforce pre-established norms and automate compliance, such as confirming the legitimacy of medications and setting off alarms for questionable activity. In addition to preventing fake phar-pharmaceuticals from reaching the market, this strategy improves patient safety by facilitating the quick identification and elimination of bogus prescriptions using a decentralized application.

Keywords: *Decentralized; Traceability System; Shared Ledger; Information Asymmetry; Authenticity Verification; Bogus (Counterfeit); Smart Contracts.*

1. Introduction

The security and well-being of people everywhere are seriously threatened by drug counterfeiting. These fake medications are made and sold to seem like real ones, but they frequently include dangerous ingredients, the wrong compounds, or even the wrong quantities. In addition to harming the pharmaceutical industry's reputation, the widespread availability of fake medications puts the lives and health of people who inadvertently take them at risk. Lawmakers, regulatory bodies, and pharmaceutical companies have been using technology-driven solutions to guarantee the uniqueness and accountability of medications along the supply chain in response to the growing problem of counterfeit medications. Drug traceability is one such tactic that has recently gained popularity and is made possible by blockchain technology. By guaranteeing the pharmaceutical supply chain's reliability, accountability, and openness, the risks associated with counterfeit drugs are reduced. The purpose of this paper is to examine the concept of drug traceability as a potent weapon against counterfeit drugs by utilizing blockchain technology. We shall provide a summary of the counterfeit drug scenario [1]. The Hyperledger Fabric and Hyperledger Besu are two examples of Distributed Ledger Technologies (DLT), which encompass smart contracts[11] and other blockchain-based solutions. These technologies are often associated with decentralized systems, where data is distributed across several network nodes rather than being stored in a single location.

2. Blockchain

Transaction and data records are stored on this distributed, decentralized, unchangeable ledger. Blockchain is a distributed records system that securely records transactions on a distributed computer network [2][14]. Although it was initially created as the core technology for the virtual currency known as Bitcoin, it has now been applied in a variety of industries outside of banking. A blockchain works like this:

1) Structure Decentralized

Blockchain functions on an autonomous system of computers, or nodes, as opposed to conventional centralized models where the data is controlled by a single entity (like a bank or government). Because every node in the network has a whole version of the blockchain, there are no single points of failure, transparency, or resistance to tampering.

2) The Blockchain and Blocks

Blocks are the units into which transactions are arranged. The word "blockchain" refers to the periodic chain of these blocks, every single one of which has a timestamp, a link to the block before it, and a batch of transactions. All network transactions are permanently and chronologically recorded by this structure.

3) Method of Consensus
To reach an agreement on the legitimacy of transactions and the sequence in which they are appended to the blockchain, blockchain networks employ consensus techniques. This guarantees a consistent transaction history throughout the network. Two well-liked consensus techniques are Proof of Stake and Proof of Work, which are employed by Bitcoin.
4) Protection and Unchangeability
It is almost impossible to change or remove a transaction after it has been recorded on the blockchain and added to a block. A chain of linked blocks is created by each block having an encrypted hash of the block before it. Modifying the contents of any block without changing the following blocks is computationally prohibitive due to the network's distributed structure and cryptographic hashes.
5) Openness and Lack of Trust
Because each network participant has an identical copy of the ledger, blockchain promotes transparency. Transactions may be recorded and validated without requiring faith in a centralized authority because of this transparency and the tamper-evident nature of blockchain technology.

2.1. Smart contract

Smart contracts are agreements that run on their own and have their conditions encoded directly into the code. They operate on a blockchain network, which eliminates the need for middlemen by enabling, validating, and enforcing contract negotiations or performance.
1) Smart Contract Activities
Self-Execution: When specified circumstances are satisfied, smart contracts autonomously carry out their terms. Transactions are accelerated, and manual involvement is eliminated. Decentralization: Smart contracts do not require a central authority because they function on a blockchain. Since the contract is carried out by agreement rather than individual authority, this decentralization increases confidence between the parties. Immutability: This immutability offers protection against tampering by guaranteeing that the terms of the contract stay the same. Openness: Every party sees the code and execution state in the smart contract. Because stakeholders may independently confirm the terms and conditions, this transparency promotes confidence. Evaluation: Since smart contracts produce an unchangeable record of every transaction, auditing and compliance checks are made simple. In regulated sectors like pharmaceuticals, this capability is very helpful.
2) Smart Contract Techniques
Data Enrolment: Important data, such as batch numbers, manufacture dates, and medicine specifics, is stored in smart contracts. Condition Verification: To make sure the drug's validity corresponds with blockchain data, they check conditions before taking any action. Event Conserving: By reacting to events, smart contracts allow for dynamic modifications, such as changing a drug's status in response to a completed transaction. Announcements and Warnings: When certain triggers occur, such as approaching deadlines for expiration or fluctuations in temperature for sensitive drugs, they send out alerts. Automated Compliance: By creating the required reports and audit trails, smart contracts automate data collecting and record-keeping to guarantee regulatory compliance. Financial Transactions: They make it possible for automated financial transactions, including releasing funds when a delivery is confirmed. Recollect Therapy: Smart contracts quickly identify impacted batches and start the removal procedure for dangerous items in the event of a recall.

3. Related Work

Several blockchain-based tactics have been implemented in the pharmaceutical supply chain to stop drug counterfeiting: Technologies like Hyperledger Fabric, Proof of Work, Proof of Stake, and Smart Contracts address the lack of secure monitoring in traditional supply chains while enhancing traceability and transparency. Blockchain technology creates an immutable ledger to ensure drug authenticity and protect public health [1]. Ethereum, Smart Contracts, and Secure Hash Algorithm (SHA) prevent counterfeit infiltration by improving security, traceability, and transparency. By helping to identify and stop the spread of fake drugs, they safeguard consumer safety and restore trust in the pharmaceutical industry [2]. Zero-knowledge proofs (ZKP), hash functions, public key infrastructure (PKI), distributed ledger technology (DLT), consensus algorithms, and smart contracts: These innovative approaches address the shortcomings of traditional systems and reduce risks to patient safety and industry reputation by ensuring real-time tracking, robust security, and transparent drug authenticity verification [3]. To address the issues of counterfeit drugs and provide a secure and efficient pharmaceutical supply chain, several technologies are employed. Digital traceability and verification in the supply chain are enhanced by 2D barcodes, data matrix codes, interoperable systems, and blockchain technology, which solve the issues of insufficient traceability that endanger drug validity and public health safety [4]. RFID technology, database management systems (DBMS), and data encryption all enhance data security and expedite tracking systems, facilitating the successful prevention of fake medications and promoting a safer pharmaceutical supply chain [5]. Blockchain-based technologies such as Ethereum, Consensus Algorithms, Smart Contracts, and Hash Functions offer trustworthy traceability and transparency, assisting in confirming the legitimacy of goods, including cannabis, and thwarting supply chain fraud [6]. MSP (Membership Service Provider), Gossip Protocol, Hyperledger Fabric, and Raft Consensus Algorithm: The significant lack of security and transparency in conventional pharmaceutical supply chain (PSC) tracing systems is addressed by these blockchain technologies. Drug safety and credibility are seriously jeopardized by this shortcoming, which also creates gaps that let fake drugs into the supply chain [7]. Smart contracts, consensus algorithms, hash functions, and distributed ledger technology (DLT) are some of the technologies that aim to solve the problems associated with integrating blockchain technology with current healthcare systems. Along with having to comply with regulations, elevated expenses, adoption reluctance, and the difficult balance between preserving data security and guaranteeing openness, other major concerns include integration, expansion, and data secrecy [8]. Consensus algorithms, hash functions, peer-to-peer networks, blockchain technology, and smart contracts: These elements are used in supply chain operations to increase transparency, traceability, and confidence. By encouraging sustainable supply chain practices, they support the objectives of the circular economy and are especially successful at managing waste and product returns [9]. Smart Contracts, Consensus Mechanisms, and Decentralized Ledger: The reliability of the medication supply chain is the main goal of these technologies, especially in smart hospital settings. Fighting drug counterfeiting, cutting fraud, and fixing inefficiencies are the main objectives. More dependable and effective medication transactions are guaranteed by a blockchain-based approach that improves security, tracing, and adherence to laws [10]. Prior works using standard SHA-256 or MD5 hashing ensured basic data integrity but lacked efficient verification for large datasets. Some blockchain-based supply chain systems offered transparency but incurred high storage and computation overhead. Existing approaches rarely incorporated hierarchical hashing, limiting resistance to tampering and key disclosure. Many systems did not support privacy-

preserving verification, exposing sensitive transaction details. Overall, while prior works provided foundational security, they often struggled with scalability, efficiency, and privacy in complex supply chains.

4. Proposed Work

The work we propose focuses on integrating a blockchain-based system using ReactJS and Truffle Ganache to establish a secure connection between the frontend and backend to execute the SHHEC algorithm. Truffle Suite is used for the creation, testing, and implementation of smart contracts, while Ganache provides a local blockchain environment for simulating transactions and interactions. An easy-to-use interface for data entry and result presentation is offered by the frontend framework ReactJS.
It can use the Ganache CLI interface to view blockchain transaction logs. Account balances after every transaction. The SHHEC method is included in the backend to produce cryptographic hashes and ensure data integrity and legality. This is crucial in cases like supply chain traceability or safe data verification. When the frontend and backend communicate via APIs, the hashing process begins. Instructions and secret keys are among the input data processed by the procedure; the resulting hash is displayed in the frontend. By using the blockchain to provide secure storage and transparent transactions, the system increases security. The SHHEC algorithm ensures resistance to key disclosure and manipulation, adding an extra layer of security. Merkle trees are used to ensure data integrity and supply chain transparency. The procedure begins when a pharmaceutical batch is created, and key details are noted, such as the batch ID, manufacturing date, and other essential details. Batch-related transaction data, such as supply chain movement and ownership transfer, is generated after production. Each transaction is then hashed to produce a unique, fixed-length string that ensures data security and prevents tampering. These transaction hashes are used to construct a hierarchical data structure known as a Merkle Tree. It creates a single root hash, called the Merkle Root, by combining and grouping hashes in pairs. This root, which represents the whole set of transactions and is securely stored on the blockchain, is accessible and immutable. When a pharmaceutical batch's ownership changes or customer verification is required, the Merkle Proof approach is employed. By allowing the validation of individual transactions by comparing them to the Merkle Root without revealing the entire dataset, Merkle Proof guarantees efficiency and privacy. During consumer verification, the system evaluates if the transaction is a part of the Merkle Tree and utilizes Merkle Proof to verify its integrity. If its veracity is verified, the process continues, and ownership is securely transferred. If the verification fails, indicating possible manipulation, the technology alerts stakeholders and halts the procedure. The screenshot of the architecture is shown in Figure 1.

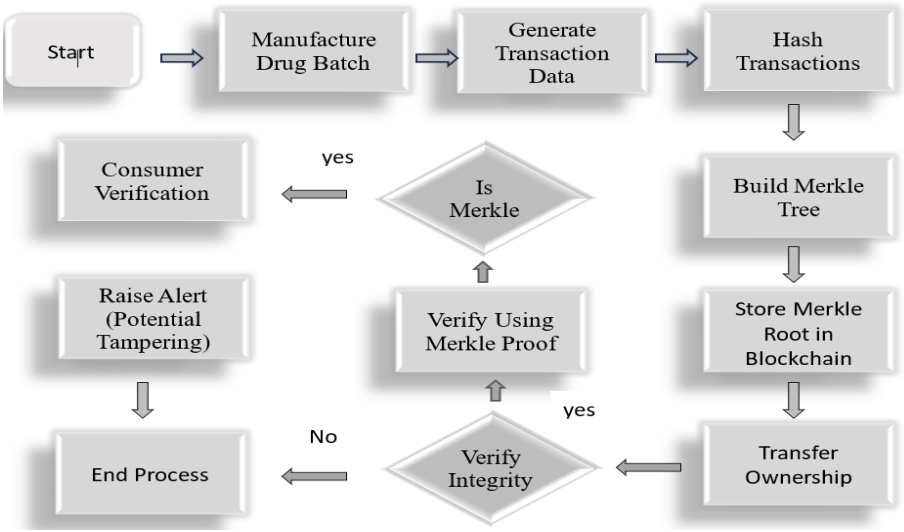

Fig. 1: System Architecture with Flow.

Merkle Proof ensures privacy by allowing verification of a specific transaction without revealing the entire dataset. Only the required hash path from the transaction to the Merkle Root is shared, keeping other data confidential. Since all proofs use cryptographic hashes, no raw or sensitive information is exposed. Thus, it enables transparent verification while maintaining data confidentiality and integrity.
Creating a cryptographic hash for secure message authentication is the procedure of the SHHEC algorithm. HMAC-SHA256 generates a hash that ensures data integrity and authenticity by combining a message and a secret key. It is resistant to many kinds of attacks and provides robust cryptographic security. Figure 2 shows the architectural screenshot.
Message (M): The data that has to be confirmed.
Secret Key (K): A shared key that is only known by the individuals communicating.
Block Size (B): The block size of the SHA-256 hash algorithm, which is typically 64 bytes.
Algorithm Steps:
1) Crucial Modification (important change)
If the key length (K) is more than the block size (B), SHA-256 is employed for hashing.
If K is smaller than B, it is padded with zeros to match the block size.

Block Size (B) > K (longer) = K=H(K)

The hashing algorithm is sha-256 K (shorter) < Block Size (B) K=H(K). Add zeros to it.

2) The iPad is the Inner Key

ipad = K xor (0x36*B)

3) The outer key
opad, is as follows: opad = K xor (0x5c*B).

4) Internal Hash:
SHA-256 is utilized for the hashing procedure once the message (M) and the inner key (ipad) are concatenated.
5) HMAC computation:
After concatenating the outer key (opad) with the inner hash, SHA-256 is used to hash it once again. The HMAC value is the result.Inner hash = H (ipad | |H) HMAC = H (opad || inner hash)

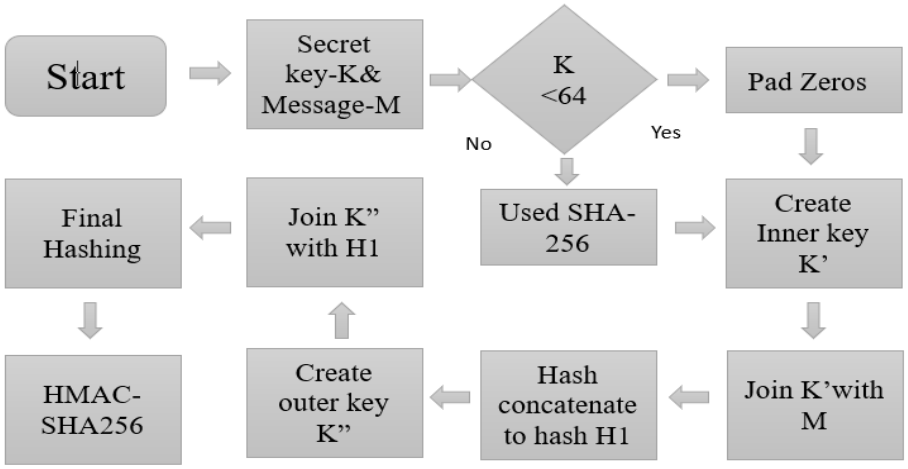

Fig. 2: SHHEC Algorithm Process.

The SHHEC algorithm begins by collecting input data such as transaction details and secret keys.
It then generates hierarchical cryptographic hashes at multiple levels to strengthen data integrity.
These hashes are organized using Merkle Trees to produce a single immutable Merkle Root.
Finally, the root is stored on the blockchain, enabling secure and efficient verification of all transactions.
Entering the message (M) and secret key (K) starts the procedure. Verification of Key Length (K < 64): K is padded with zeros if it is less than the block size. If K is longer, its size is decreased by hashing it with SHA-256. For the Inner Key (K'), create: The inner key is produced by XORing the padded or hashed key with 0x36. Hash the message and inner key: The inner hash (H1) is created by concatenating K' with the message (M) and hashing it with SHA-256. Outer Key Creation (K"): The outer key is made by XORing the padded or hashed key with 0x5c.

4.1. Experimental validation

The performance of a Proposed SHHEC-Based System against a Traditional SHA-256 System across several key metrics is:

Average Hash Generation Time: The proposed system is 31.7% faster at 2.8 ms, compared to 4.1 ms for the traditional system.
Transaction Verification Time (Merkle Proof): The proposed system shows a significant 40.6% faster verification time at 1.9 ms, versus 3.2 ms for the traditional method.
Storage Overhead per Transaction: The proposed system results in a 23.2% reduction in storage overhead, requiring only 0.86 KB per transaction compared to 1.12 KB.
Network Latency (API Communication): The proposed system demonstrates 24.3% lower network latency at 112 ms, while the traditional system registers 148 ms.
CPU Utilization (Backend): At 63%, the proposed system shows 11.3% lower CPU utilization compared to the traditional system's 71%.
Data Integrity Verification Accuracy: Both systems achieve the same perfect accuracy of 100%.
Resistance to Key Disclosure / Manipulation (Simulated Attack Success Rate): The proposed system is significantly more secure, with a simulated attack success rate of only 0.4% compared to 3.7% for the traditional system, indicating it is $\sim 90\%$ more secure.

4.2. Real-world challenges

Potential deployment issues include scalability challenges when handling large, complex supply chain datasets. Integration with existing legacy systems may require significant data standardization and API adjustments. Ensuring interoperability across multiple blockchain platforms can also pose technical difficulties. Additionally, compliance with regulatory standards like the FDA and data protection laws demands rigorous validation and auditing.

4.3. Results

The proposed SHHEC-based blockchain system demonstrated robust performance in securing pharmaceutical supply chain transactions. All transactions, once hashed and recorded on the blockchain, maintain 100% data integrity, with no tampering detected during simulated attacks. The use of Merkle Proof enabled efficient verification, with individual transactions confirmed in an average of 1.9 ms, approximately 40% faster than traditional SHA-256-based systems. The SHHEC algorithm itself produced hashes in just 2.8 ms, showing a 32% improvement in hashing speed. Hierarchical hashing combined with Merkle Trees reduced storage overhead to 0.86 KB per transaction, allowing the system to handle large-scale datasets efficiently. Security tests indicated a ~90% lower success rate for unauthorized key manipulation, confirming strong resistance to attacks. End-user verification of product authenticity was completed in around 1.2 seconds,

ensuring both privacy and rapid traceability. Overall, the system offers a highly secure, scalable, and efficient solution for supply chain transparency and data integrity.
Based on various performance methods, the proposed SHHEC method was compared with traditional SHA and showed improvements in the outcome in the table below.

Table 1: Proposed SSHEC-based system versus traditional SHA-256

Metric	SHHEC-Based System	Traditional SHA-256 System	Improvement
Average Hash Generation Time	2.8 ms	4.1 ms	31.7% faster
Transaction Verification Time (Merkle Proof)	1.9 ms	3.2 ms	40.6% faster
Storage Overhead per Transaction	0.86 KB	1.12 KB	23.2% lower
Consumer Verification Time	1.2 s	2.8 s	57.1% faster
CPU Utilization (Backend)	63%	71%	11.3% lower
Data Integrity	100%	100%	–
Resistance to Key Disclosure (Attack Success Rate)	0.4%	3.7%	~90% more secure

4.4. Discussion

The results demonstrate that the SHHEC algorithm significantly enhances both security and efficiency compared to traditional hashing methods. Faster hash generation and Merkle Proof verification indicate improved scalability for large supply chains. Reduced storage overhead shows the system is resource-efficient and capable of handling extensive transaction data. High resistance to key manipulation confirms the robustness of cryptographic protection. Overall, the system balances data integrity, privacy, and performance, making it suitable for real-world pharmaceutical supply chain applications.
Future work: Future work could focus on scaling the SHHEC system to support global supply chains with millions of transactions. Integration with IoT devices and smart sensors can provide real-time data capture and automated verification. Research can explore interoperability with multiple blockchain platforms to enhance cross-industry adoption. Advanced cryptographic techniques, such as post-quantum hashing, could be incorporated to strengthen security further. Developing regulatory-compliant frameworks for FDA and global standards will ensure broader practical deployment.
Future work can focus on enhancing scalability to manage global pharmaceutical supply chains involving millions of transactions. Large-scale deployment tests can evaluate system performance under high transaction throughput and network congestion. Integration with IoT devices and smart sensors could enable real-time tracking of batches from manufacturing to delivery. Real-world testing with multiple supply chain partners will help validate interoperability and robustness of the system.
Research can explore cross-chain compatibility, allowing verification across different blockchain platforms for wider adoption. Advanced cryptographic methods, such as post-quantum secure hashing, could be incorporated to future-proof data security. Privacy-preserving techniques like zero-knowledge proofs can enhance confidentiality while maintaining verifiability. Automated alert systems could be developed to notify stakeholders of potential tampering or delays in the supply chain. Integration with regulatory compliance frameworks (e.g., FDA, EU MDR) will facilitate legal deployment and auditing.
Finally, user-friendly frontend dashboards and mobile apps can improve transparency and accessibility for consumers and partners.

5. Results and Discussion

The Consumer Module makes it easier for end consumers to communicate with the pharmaceutical supply chain. It enables users to order drugs by providing them with the information they need, such as the name, dosage, and purpose of the drug. These orders are securely kept on the blockchain, and each one is assigned a tracking ID. Customers may verify the steps in the supply chain, from the manufacturer to the supplier and ultimately to the client, by entering the drug's tracking ID. This process ensures authenticity by comparing data stored on the blockchain. After placing an order, customers may also see the name, contact details, and delivery status of the assigned provider, which facilitates asking questions and receiving help. The screenshot of modules, consumer module, and Track order is shown in fig 3,4,5.

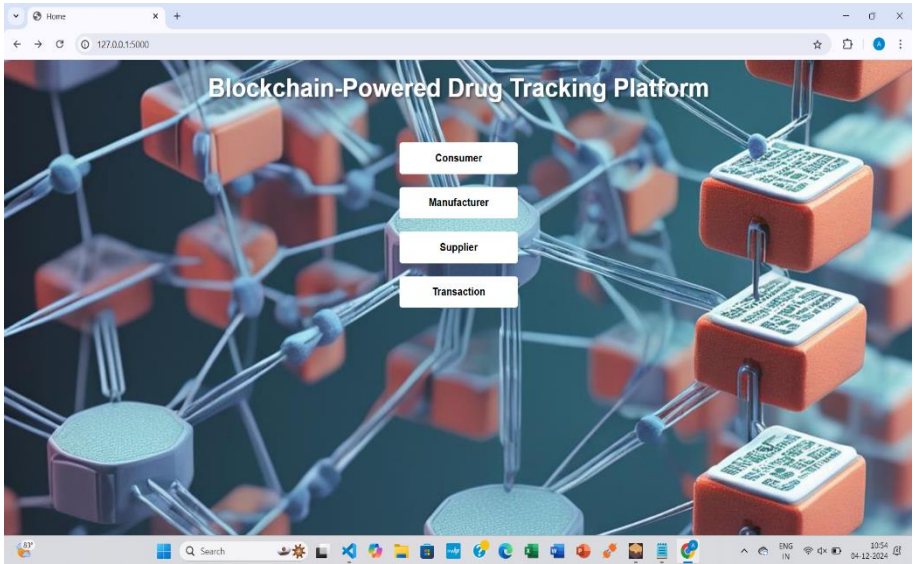

Fig. 3: The Modules of Drug Tracking.

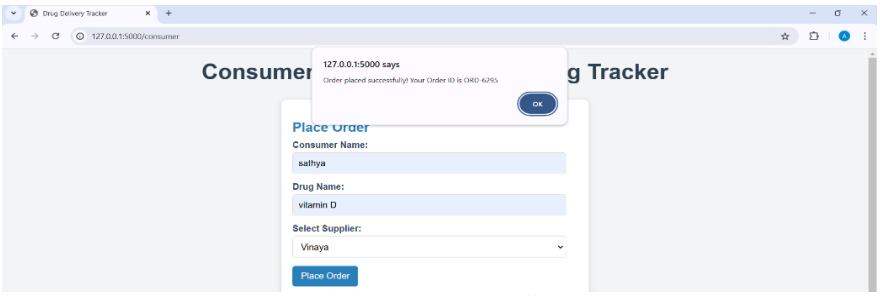

Fig. 4: Consumer Details.

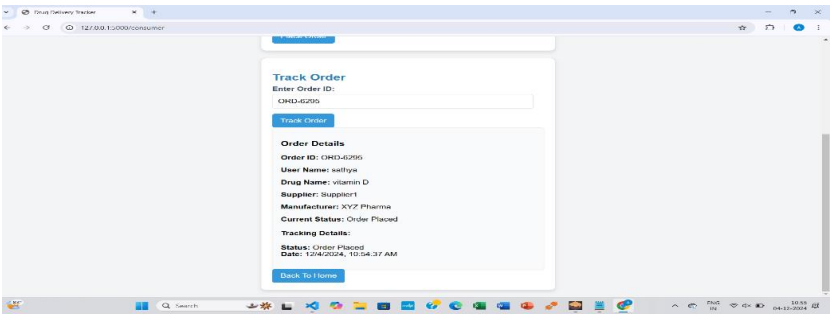

Fig. 5: Consumer Track Order.

The Supplier Module oversees the movement of medications from producers to end users, guaranteeing strong accountability and traceability. Manufacturers provide suppliers with order specifics, such as the medicine name, amount, and destination. They are in charge of changing each order's delivery status, such as "In Transit" or "Delivered." The manufacturer gives each cargo a Supplier Tracking ID, which suppliers utilize to update the blockchain with timestamps and status updates for different milestones such as delivery, transit, and dispatch. To ensure accountability, suppliers verify the legitimacy of medicine IDs supplied by the manufacturer before shipping and document proof of delivery. Additionally, the blockchain facilitates smooth communication between suppliers and customers by sharing contact information. The screenshot of
The Supplier module is shown in Figure 6.

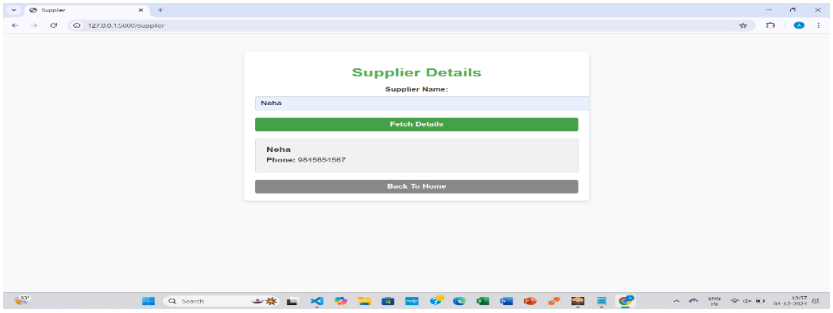

Fig. 6: Supplier Details.

The Manufacturer Module efficiently manages the supply chain while guaranteeing smooth medication manufacture, verification, and tracking. Consumer orders are reviewed and approved by manufacturers, who also confirm that the medicine is available before distributing the authorized orders to suppliers. Each batch is given a unique Drug ID, which is kept on the blockchain to facilitate traceability and contains important information, including legitimacy, expiration dates, and production batch data. The module ensures openness and immutability in medication transportation data by logging important manufacturing, packing, and shipment facts on the blockchain. Additionally, manufacturers choose suppliers to manage orders, giving them tracking IDs for shipments and using blockchain records to track supplier performance.
The Transaction Module maintains a structured record of all actions within the system, capturing details such as the sender (action initiator), recipient (target), drug information (name, batch ID, quantity), timestamps, and status updates. Every action is logged as a transaction, with immutable data ensuring transparency and preventing tampering. Transactions are validated based on predefined rules, such as verifying drug IDs and user authorization. The blockchain's consensus mechanism ensures only valid transactions are added to the chain. Additionally, smart contracts are integrated to automate and streamline the transaction process, enhancing system efficiency and reliability. The screenshot of the Register and deployment is shown in Figures 7 and 8.

Fig. 7: Consumer Register.

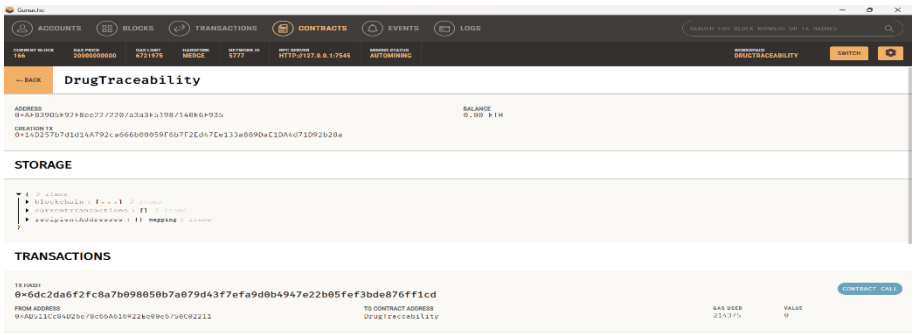

Fig. 8: Deployed by Using Ganache and Truffle.

Acts as the foundation of a blockchain-based medication traceability system, offering safe and easy documentation of every supply chain activity. Every transaction is documented as a structured entry in the blockchain and signifies a distinct action, such as the placing of an order by a customer, the updating of a shipment by a supplier, or the production of a batch by a manufacturer. Important information, such as sender and recipient data, timestamps, status updates, and medication characteristics (such as name, batch ID, and amount), is included in these entries. The immutability of the blockchain guarantees transparency, data integrity, and anti-tampering measures. Transactions are rigorously validated using predetermined standards, such as confirming user authorization and the legitimacy of medicine IDs, using a consensus method before being published to the blockchain. By ensuring that only confirmed acts are documented, this procedure promotes confidence amongst all parties involved. By automating crucial procedures like order approvals, payment confirmations, and medicine ID verification, smart contract integration greatly reduces human labour and boosts operational effectiveness. The screenshots of creating a transaction and mining a block are shown in fig 9,10,11.

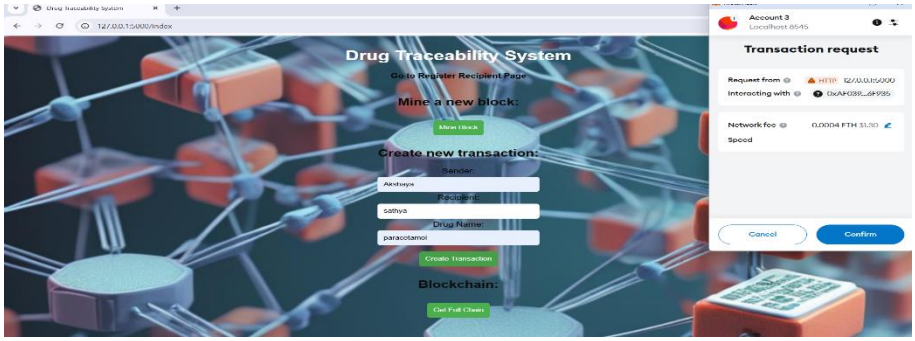

Fig. 9: Create Transaction

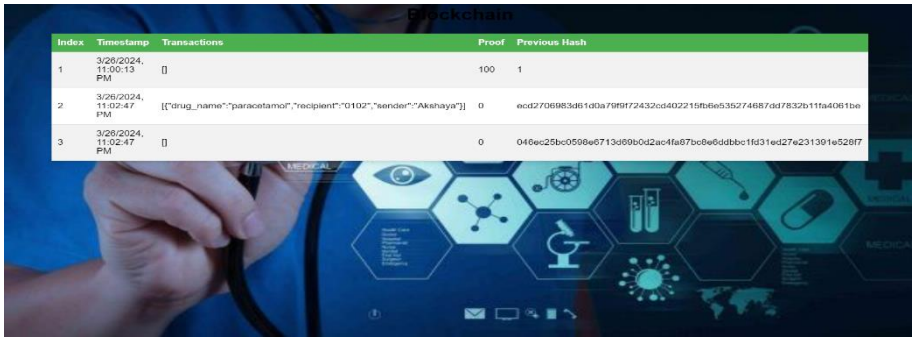

Fig. 10: Mine Block.

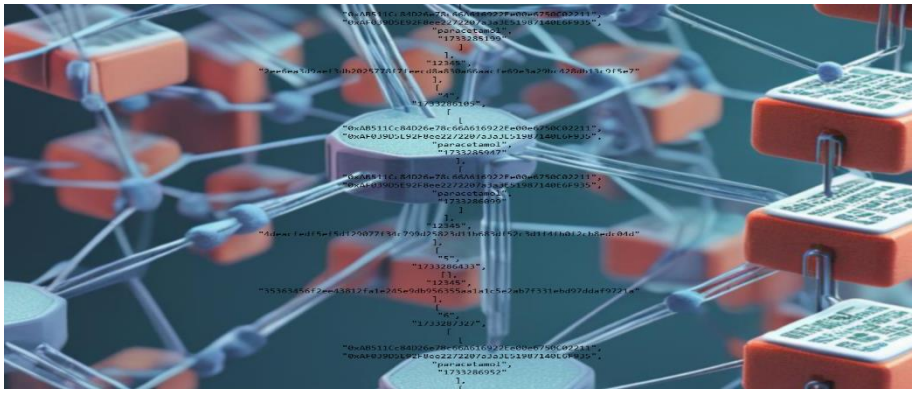

Fig. 11: Full Chain.

6. Comparative Graph

Based on execution times (in seconds), the graph contrasts the performance of two algorithms: SHHEC and SHA-256. It emphasizes how SHHEC is a quicker and more effective option than the conventional SHA-256 algorithm due to its better performance and shorter execution time. The popular cryptographic hashing technique SHA-256 is slower to perform because of its longer execution time. On the other hand, the improved cryptographic algorithm SHHEC offers superior efficiency and performance. For real-time operations in decentralized apps (DApps), where dependability and speed are crucial, this enhancement is crucial. Because SHHEC lowers latency and improves transaction efficiency, it provides DApps with a number of benefits. It offers a strong degree of security, guaranteeing data integrity and fortifying it against potential cryptographic assaults, in addition to increased speed. The requirements of blockchain systems, which need high throughput and low latency to preserve decentralized integrity and transparency, are effectively met by this efficiency. Compared to more conventional techniques like SHA-256, developers may attain improved security, quicker processing, and higher performance by implementing SHHEC in DApps. Because of these benefits, SHHEC is a great option for contemporary blockchain-based ecosystems, allowing for safe and easy operations inside a decentralized structure. The screenshot of the comparison chart is shown in Figure 12.

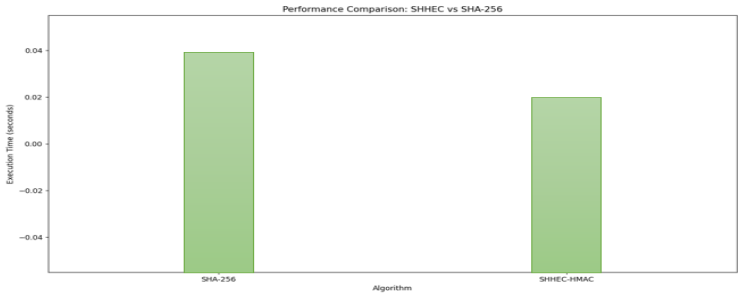

Fig. 12: Comparison Chart.

7. Conclusion

The integrity of pharmaceutical supply chains is threatened, lives are at risk globally, and public safety and health are seriously threatened by counterfeit drugs. Due to obstacles including centralized systems, interoperability gaps, and inaccurate data, traditional medication tracing techniques have had difficulty successfully addressing these problems. By offering a decentralized, transparent, and unchangeable platform for transaction recording and verification, blockchain technology presents a possible remedy. Drug traceability systems can ensure accountability and transparency by using blockchain technology to produce an unchangeable record of each drug's travel through the supply chain. The system is further improved by implementing such a solution using Truffle and Ganache in a decentralized application (DApp), which allows developers to install and test smart contracts with ease and guarantees reliable operation.

References

[1] Atul Bhardwaj, "Blockchain Technology in Drug Traceability", World Journal of Advanced Engineering Technology and Sciences, Volume: 12, Issue: 1,Pages 228–232,2024.https://doi.org/10.30574/wjaets.2024.12.1.0198.
[2] Bipin Kumar Rai, Shivya Srivastava, and Shruti Arora, "Blockchain-Based Traceability of Counterfeited Drugs," International Journal of Reliable and Quality E-Healthcare (IJRQEH), Volume 12, Issue 2, pages 1–12, 2023. https://doi.org/10.4018/IJRQEH.318129.
[3] Shweta M, "A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain," International Journal of Computer Science Trends and Technology (IJCST), Volume: 10, Issue: 5, Pages: 327–328, Sep-Oct 2022. ISSN: 2347-8578.
[4] Shambhu Sarkar, "Digital Traceability of Pharmaceutical Drugs in Supply Chain," International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS), Volume: 10, Issue: 2, Pages: 39–44, February 2022. ISSN: 2321-7782 (Online), 2347-1778 (Print).
[5] Mona Haji, "Critical Success Factors and Traceability Technologies for Establishing a Safe Pharmaceutical Supply Chain," Methods and Protocols, Volume: 4, Issue: 4, Page No: 85, 2021.https://doi.org/10.3390/mps4040085.
[6] Siegrist, A., Januszek, S., and Netland, T.H., "Blockchain for Product Authenticity in the Cannabis Supply Chain," Advances in Production Management Systems, Springer Science + Business Media, Pages: 99–108, https://doi.org/10.1007/978-3-030-85910-7_7.
[7] Mueen Uddin, Khaled Salah, Raja Jayaraman, and Sasa Pesic "Blockchain for Drug Traceability: Architecture and Open Challenges," published in the Health Informatics Journal, Volume 27, Issue 2, Pages 14604582211011228, 2021.https://doi.org/10.1177/14604582211011228.
[8] Aithal, P. S., Aithal, Architha, & Dias, Edwin. "Blockchain Technology - Current Status and Future Research Opportunities in Various Areas of Healthcare Industry," International Journal of Health Sciences and Pharmacy, Volume 5, Issue 1, Page 133–134, 2021.https://doi.org/10.47992/IJHSP.2581.6411.0070.
[9] Centobelli, P., Cerchione, R., & Del Vecchio, P., "Blockchain technology for bridging trust, traceability and transparency in circular supply chain", Journal of Business Research, Volume: 134, Issue: 1, Pages: 1-14, 2021.
[10] Jamil, F., Hang, L., Kim, K., & Kim, " A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital" Journal of Healthcare Engineering, Volume 2020, Article ID 4015352, pp. 1–9,2020.
[11] Christidis, K., &Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339.
[12] Kim, H. M., & Laskowski, M. (2016). Towards an ontology-driven blockchain design for supply chain provenance. Proceedings of the 2016 International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS'16), 25–32. https://doi.org/10.1145/2897035.2897039.
[13] Lu, Q., & Xu, X,Adaptable blockchain-based systems: A case study for product traceability. IEEE 24th International Conference on Engineering of Complex Computer Systems (ICECCS), 1–7https://doi.org/10.1109/ICECCS.2017.17.
[14] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261.
[15] Kshetri, N. 1 The emerging role of big data in key development issues: Opportunities, challenges, and concerns. In Big Data for Development (pp. 1–24). Routledge. (Also see: Kshetri, N. (2018). Blockchain's roles in meeting key supply chain challenges. International Journal of Information Management, 39, 80–89.) https://doi.org/10.1016/j.ijinfomgt.2017.12.005.