**Journal of Information Systems Engineering and Management**
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Enhanced Traceability and Transparency in Medical Supply Chain Management Using Blockchain-Based Customized Smart Contracts

Nitin Shivale[1], Dr. Pratap Singh Patwal[2], Dr. Parikshit Mahalle[3]
*[1]Research Scholar (Computer Science Engineering), Nirwan University, Jaipur Rajasthan, India*
*shivalenitin23@gmail.com*
*[2]School of Engineering & Technology Nirwan University, Jaipur Rajasthan, India*
*Pratappatwal@gmail.com*
*[3]Dean & Director of Research, VIT Autonomous Institute, Pune Maharashtra, India*
*parikshit.mahalle@viit.ac.in*

**ARTICLE INFO**

Received: 06 Nov 2024

Revised: 24 Dec 2024

Accepted: 05 Jan 2025

**ABSTRACT**

The medical supply chain faces challenges like counterfeit drugs, lack of transparency, and inefficient traceability. Blockchain technology, with its decentralized and secure architecture, offers a promising solution. By implementing customized smart contracts, stakeholders can ensure data integrity, improve trust, and streamline supply chain operations, enhancing overall efficiency and reliability. Counterfeit medicines and limited visibility across the medical supply chain pose significant risks to patient safety and public health. Traditional systems lack robust mechanisms to verify authenticity or ensure transparency. The need for a secure, efficient, and scalable system to trace and validate medicines in real-time has become crucial. A blockchain-based framework was developed using customized smart contracts for traceability. Each medicine is registered with unique identifiers stored on the blockchain. QR codes link physical products to the digital ledger, enabling real-time tracking and user verification. The system uses consensus mechanisms to validate transactions and ensure authenticity. Proof of Work (PoW) ensures robust security by requiring significant computational effort for transaction validation, deterring malicious activities. Proof of Stake (PoS) enhances scalability and energy efficiency, validating transactions based on a node's stake in the network. Together, these algorithms provide a balance of security, speed, and sustainability. The proposed system significantly improves traceability and transparency in the medical supply chain. Counterfeit detection rates increased, and transaction validation times decreased due to optimized algorithms. User feedback confirmed enhanced trust and reliability. The solution demonstrates scalability and adaptability for broader applications in healthcare and beyond.

**Keywords:** Traceability, Medical Supply Chain, Blockchain Technology, Smart Contracts, Transparency, PoW, PoS

## Introduction

The supply chain is an complex process due to involvement of various entities such as product manufacturer, providers, distributors and legal authorities etc [1-3]. However, this network is often plagued by inefficiencies, lack of visibility, counterfeit products, and inadequate regulatory compliance, leading to risks that jeopardize patient safety and overall healthcare outcomes. The pandemic further exposed susceptibilities in the comprehensive supply chain, underscoring the urgent need for innovative solutions to improve its resilience, traceability, and transparency. Blockchain technology, with its decentralized, secure, and tamper-proof nature, has emerged as a transformative tool for addressing these challenges [3]. When coupled with customized smart contracts, blockchain can significantly enhance the management of medical supply chains by automating processes, ensuring data integrity, and fostering trust among stakeholders Enhanced traceability ensures that each operation and movement of medical products—from raw material procurement to final distribution is recorded on an immutable blockchain ledger. This feature combats the persistent issue of counterfeit medicines, allowing stakeholders to verify the authenticity of products at every stage [4]. Blockchain's real-time tracking capabilities also improve supply chain visibility, enabling stakeholders to monitor inventory levels, forecast demand accurately, and reduce waste caused by overproduction or underutilization. Customized smart contracts further enhance the functionality of blockchain by automating critical processes such as order placement, payment settlements, and compliance checks. These self-executing contracts ensure that pre-defined conditions, such as quality checks or regulatory approvals, are met before transactions are completed, thereby reducing delays, errors, and fraud [8-10].

This integration of blockchain and smart contracts not only addresses operational inefficiencies but also builds trust by providing stakeholders with a transparent, tamper-proof record of supply chain activities. Patients and healthcare providers can verify the authenticity of medicines using QR codes linked to blockchain records, ensuring safety and accountability. Furthermore, regulatory agencies gain access to reliable data for monitoring compliance and investigating supply chain anomalies. While challenges such as high implementation costs, scalability, and regulatory uncertainties exist, the potential benefits of customized smart contracts in enhancing traceability and transparency far outweigh these barriers. By addressing critical pain points, this technology offers a robust framework for a more resilient, efficient, and trustworthy medical supply chain [10-15], eventually causative to enhanced outcomes and public health.

## Literature Survey

Omar, R. et al. [1] explores the potential of blockchain-based smart contracts to automate procurement processes in the healthcare supply chain. It focuses on addressing inefficiencies and trust-related issues prevalent in traditional procurement systems. The authors introduce a framework leveraging blockchain to ensure transparency, immutability, and efficiency in contract management. By integrating smart contracts, the framework automates payment triggers, delivery confirmations, and compliance checks. The study highlights the importance of decentralized decision-making and real-time data sharing to reduce delays and operational risks. The research evaluates the scalability of blockchain algorithms and consensus mechanisms suitable for the healthcare domain, emphasizing Ethereum's potential. Additionally, it demonstrates the reduction in administrative costs and human error due to automation. The paper includes a case study that showcases blockchain's capability to prevent fraud and enhance supplier-buyer relationships. Challenges such as initial implementation costs, interoperability issues, and regulatory compliance are discussed, with suggestions for addressing these barriers. The findings illustrate blockchain's transformative impact on procurement in healthcare supply chains.

Musamih, K. et al. [2] proposes a blockchain-based framework for ensuring drug traceability throughout the healthcare supply chain. The authors address the pressing issue of counterfeit drugs by introducing a system where all stakeholders, including manufacturers, distributors, and consumers, can verify the authenticity of pharmaceutical products. The framework employs a tamper-proof blockchain ledger combined with QR codes for real-time tracking and verification. This decentralized approach enhances transparency, data integrity, and trust across the supply chain. Smart contracts facilitate automated record-keeping and enforce compliance with predefined standards. The study showcases how blockchain can streamline the drug recall process by providing end-to-end visibility. Additionally, the authors conduct a performance analysis, demonstrating the framework's scalability and security under different blockchain protocols. Challenges such as data privacy concerns, system adoption barriers, and the need for stakeholder collaboration are examined. The proposed solution underscores blockchain's potential in combating counterfeit drugs and improving patient safety globally.

Subramanian, G. et al. [3] introduces a hybrid blockchain technology to address challenges in the pharmaceutical SC. The authors highlight issues like counterfeit medicines, inefficiencies, and lack of transparency. The proposed system leverages a combination of public and private blockchain networks to achieve a balance between transparency and data privacy. The integration of smart contracts automates various processes such as order placements and inventory updates. The framework employs cryptographic techniques to ensure data integrity and secure transactions. A case study is presented, demonstrating the system's ability to identify and eliminate counterfeit drugs. Additionally, the paper discusses the scalability and energy efficiency of hybrid blockchain compared to fully public systems. The authors emphasize the significance of user-friendly interfaces and interoperability with existing supply chain infrastructure. Challenges such as adoption resistance, regulatory alignment, and technical complexity are acknowledged. The study concludes by reinforcing the possible of hybrid blockchain to revolutionize pharmaceutical SCM ensuring drug safety and patient trust.

Reyes, P. M. et al. [4] examines the impact of blockchain technology on the operational and managerial processes within global supply chains. The authors focus on how blockchain enables enhanced visibility, trust, and efficiency among supply chain participants. The study identifies key operational benefits, such as real-time tracking, automated verification, and reduced reliance on intermediaries. From a managerial perspective, blockchain facilitates informed decision-making through reliable and immutable data. The authors present a framework outlining how blockchain integrates with supply chain activities such as procurement, production, logistics, and customer relations. Use cases in industries like retail, automotive, and healthcare are explored to illustrate blockchain's adaptability across various domains. The paper highlights the significance of smart contracts in reducing transactional bottlenecks and ensuring compliance with contractual terms. Challenges such as high implementation costs, lack of technical expertise, and the need for regulatory clarity are discussed. The authors conclude by emphasizing blockchain's transformative potential in reshaping global supply chain operations, though adoption requires strategic planning and stakeholder collaboration.

Pattanayak, S. et [5] explores the blockchain integrated SCM theory which demonstrated secure, reliable and transparent. Key capabilities include improved visibility, real-time tracking, and enhanced information sharing across the supply chain. The authors outline how blockchain can help manage supply-demand mismatches, reduce fraud, and ensure regulatory compliance. Using case studies, the paper demonstrates blockchain's application in mitigating risks and enhancing recovery speed after disruptions. Smart contracts are highlighted as a tool for automating transactions and ensuring adherence to supplier agreements. Challenges such as integration with legacy systems, cost of implementation, and data privacy concerns are acknowledged. The paper concludes by proposing a framework for organizations to evaluate blockchain’s potential based on their unique supply chain needs, emphasizing its role in building resilient and agile supply chains.

Musamih, I. et al. [6] introduces a novel application of secure token generation for authentication in healthcare supply chain management. The authors propose using NFTs to represent unique products, ensuring their authenticity, traceability, and ownership. The study demonstrates how NFTs can enable secure digital certification for pharmaceutical products, mitigating counterfeit risks. The framework incorporates blockchain technology to create a tamper-proof ledger, facilitating secure trading and delivery of healthcare items. By combining NFTs with smart contracts, the system automates compliance checks, payment processes, and inventory management. The authors also address scalability challenges and propose solutions for integrating the system into existing supply chain infrastructures. The paper highlights how this approach enhances transparency and trust among stakeholders, ultimately improving patient safety and operational efficiency. Challenges related to cost, interoperability, and regulatory compliance are discussed, with suggestions for overcoming these barriers. The study concludes by emphasizing the potential of NFTs in revolutionizing product management within healthcare supply chains.

Rasi, R. Z. et al. [7] categorize risks into technological, organizational, and environmental factors. Key technological risks include scalability, interoperability, and security vulnerabilities. Organizational challenges involve resistance to change, lack of technical expertise, and high implementation costs. Environmental factors include regulatory uncertainties and varying global standards. The paper discusses how blockchain can mitigate traditional supply chain risks, such as fraud and lack of transparency, while also introducing new risks related to its implementation. The authors propose a risk management framework to help organizations assess and address these challenges. They emphasize the need for stakeholder collaboration, regulatory support, and continued research to enhance blockchain's adoption in supply chain management. The study concludes by outlining future research directions to address gaps in understanding blockchain-related risks.

Agarwal, U. et al. [8] p explore how blockchain enhances transparent as well as traceable in supply chain operations. Key areas of application include product authentication, fraud prevention, and efficient data sharing. The study categorizes blockchain use cases into manufacturing, logistics, and retail, highlighting how it addresses specific challenges in each domain. It also examines different consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), and their suitability for supply chain applications. The authors discuss implementation challenges, including scalability, energy consumption, and integration with legacy systems. The paper emphasizes the importance of collaboration between technology providers and supply chain stakeholders for successful adoption. Future research directions are proposed, focusing on improving blockchain’s efficiency and exploring its integration with incipient technologies like IoT and AI. This approach conclude by reaffirming blockchain's transformative potential in securing global supply chains.

Gai, K. et al. [9] explores how blockchain technology can optimize services in a supply chain digital twin environment. The digital twin concept involves creating virtual models of physical supply chains for enhanced simulation and decision-making. The authors propose integrating blockchain to address issues such as data integrity, security, and real-time visibility. Blockchain provides an immutable ledger for recording transactions, enabling trusted communication between stakeholders. Smart contracts automate processes such as order validation, payment settlements, and compliance checks. The study highlights blockchain’s role in improving supply chain coordination, reducing inefficiencies, and mitigating risks associated with data tampering. Use cases in industries like manufacturing and logistics demonstrate the framework's potential to enhance operational efficiency. Challenges such as high computational costs, regulatory hurdles, and the need for system interoperability are discussed. The authors conclude that blockchain-enabled digital twins can transform supply chain management by delivering accurate, real-time insights and fostering trust among participants.

Madhwal, Y. et al. [10] presents a blockchain-based proof-of-delivery (PoD) system to enhance performance measurement in supply chains. The proposed solution uses smart contracts to automate the validation of deliveries and payments. Blockchain's tamper-proof nature enhances trust and accountability among supply chain participants. The authors evaluate the system's performance in terms of scalability, data integrity, and operational efficiency. By replacing manual verification processes, the PoD system reduces errors, delays, and associated costs. The paper highlights its application in sectors such as e-commerce and logistics, where timely and accurate deliveries are critical. Challenges such as integrating the solution with legacy systems and addressing privacy concerns are discussed. The authors suggest that adopting blockchain-based PoD systems can significantly improve supply chain performance by increasing transparency and reducing disputes.

Omar, A. et al. [11] proposes a inventory sharing among supply chain participants. The system ensures transparency and real-time visibility of inventory levels. The framework facilitates collaboration among stakeholders, enabling efficient resource utilization and reducing waste. Smart contracts automate inventory updates, order placements, and payment settlements, minimizing human intervention and errors. The authors conduct a case study to demonstrate the framework's ability to optimize inventory management and reduce costs. Blockchain's immutability ensures trust and prevents fraudulent activities, while its decentralized nature eliminates the need for intermediaries. Challenges such as scalability, adoption resistance, and compliance with regulations are acknowledged.

Hawashin, D. et al. [12] addresses the issue of resource imbalance in medical supply chains using a blockchain-based solution. The system that leverages blockchain's transparency and traceability to mitigate overproduction and underconsumption. The solution includes a decentralized ledger for real-time tracking of medical supplies and smart contracts to automate inventory management and redistribution processes. The system ensures accurate demand forecasting and minimizes wastage by facilitating collaboration among stakeholders. A performance evaluation demonstrates the framework's ability to improve efficiency for suppliers. The paper also highlights challenges such as integration with existing systems, data privacy concerns, and initial implementation costs. The authors conclude this method can significantly enhance the sustainability and efficiency of medical supply chains.

Hasan R. et al. [13] investigates a blockchain enabled framework for ensuring the trustworthiness of IoT data streams by integrating the InterPlanetary File System (IPFS). The authors propose using blockchain to record immutable hashes of IoT data, while the actual data is stored in IPFS to optimize storage and access efficiency. The approach enhances data integrity, authenticity, and transparency in IoT applications, addressing challenges like data tampering and centralized storage vulnerabilities. Smart contracts automate access permissions and enforce security policies can access data. The framework is tested for its scalability and performance, demonstrating its suitability for large-scale IoT ecosystems. The study highlights potential use cases in healthcare, logistics, and smart cities, where secure real-time data streaming is critical. Challenges such as latency, energy consumption, and integration with existing systems are acknowledged. The authors conclude that combining blockchain with IPFS is a promising solution for enhancing the security and reliability of IoT data.

Guo, S. et al. [14] focus the challenge on challenges connected to operational transparency, ethical sourcing, and environmental impact in SCM. By using blockchain, stakeholders can trace the lifecycle of fashion products, from raw material sourcing to end-of-life disposal. Smart contracts are employed to ensure compliance with sustainability standards and automate transactions. The authors highlight the role of blockchain in promoting ethical practices, reducing waste, and encouraging circular economy models. Use cases demonstrate blockchain's ability to enhance trust among consumers by providing verifiable information on product origins and environmental efforts. Challenges such as high implementation costs, data standardization, and resistance from traditional supply chain actors are discussed. The paper concludes by emphasizing blockchain's potential to drive sustainability in fashion supply chains and suggests future research to address existing barriers.

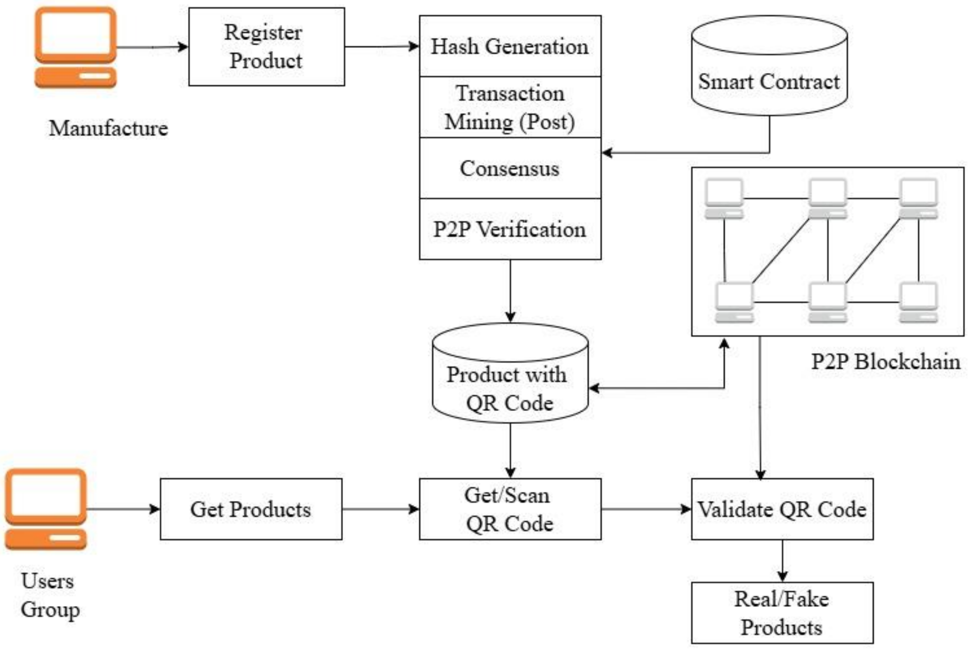
Garcia, R. D. et al. [15] propose using blockchain to create a decentralized and tamper-proof ledger for data transactions while preserving stakeholder privacy. This method describes various secure cryptographic techniques that enhances the security as well as priacy. It is particularly applicable to industries such as healthcare and supply chain management, where data sharing is critical but must comply with strict privacy regulations. The paper highlights blockchain's role in enabling transparent and accountable data governance while preventing unauthorized access. Challenges such as computational overhead and scalability are addressed, with suggestions for improving the framework's efficiency. The authors conclude that blockchain technology, combined with advanced privacy-preserving methods, can revolutionize data governance in collaborative environments.

## Research Methodology

The combination of blockchain framework in the medicine supply chain enhances transparency, security, and trust describes in below Figure 1. A Medicine Registration Module ensures the authenticity of each medicine, with details stored immutably on the blockchain. Unique QR codes are generated for every registered medicine, enabling tracking and verification through user-friendly scanning. Blockchain algorithms such as PoW and PoS secure the information, ensuring data integrity. A consensus algorithm further validates the authenticity of medicines, empowering users to differentiate between genuine and counterfeit products, thus combating fraudulent practices and ensuring patient safety.

**1. Medicine Registration Module:** The Medicine Registration Module ensures the secure and transparent onboarding of medicines into the blockchain system. Pharmaceutical manufacturers are required to register their products with critical details such as the drug's name, composition, manufacturing date, expiry date, batch number, and manufacturer information. This data is securely recorded on the blockchain, ensuring immutability and traceability. To avoid counterfeit products, each medicine is assigned a unique identifier linked to the blockchain ledger. This unique identifier creates an immutable record, making it impossible for unauthorized entities to tamper with or duplicate product information. The authenticated manufacturer can add their product in the blockchain, reducing the risk of fraudulent entries. This module also ensures compliance with regulatory standards and audits by providing verifiable records for each registered product. The system includes role-based access for stakeholders such as manufacturers, distributors, and regulators, allowing them to access and manage only their assigned areas. Blockchain's decentralized structure ensures that all data remains tamper-proof, creating a robust framework for medicine registration.

**2. Generate QR Code and Add Medicine Info in Blockchain :** This module involves the creation of a unique QR code for every registered medicine batch. The QR code encodes essential information, such as the unique blockchain identifier, batch number, manufacturing and expiry dates, and the manufacturer's digital signature. Once the QR code is generated, it is integrated with the blockchain system using cryptographic hashing to ensure security and authenticity. The module leverages blockchain algorithms such as SHA-256 for digital signatures, and Merkle Trees for data integrity. These algorithms ensure that medicine information is securely stored and verified. The QR code, when scanned, retrieves the product's blockchain-stored information, allowing seamless and accurate verification. By incorporating smart contracts, the system ensures that any updates to the medicine's status, such as shipment or recall, are automatically recorded on the blockchain. This module ensures transparency, allowing all stakeholders to track a medicine's journey from manufacturer to end-user.



**3. Verify Medicine Using QR Code Scanning by User :** The verification module allows users, such as patients and pharmacists, to scan a medicine's QR code using a smartphone or dedicated scanner. Upon scanning, the QR code links directly to the blockchain to retrieve real-time information about the medicine. This includes the manufacturer, batch number, production and expiration dates, and the supply chain history. The verification process confirms whether the medicine is genuine or counterfeit by cross-checking the blockchain data. If the scanned information matches the immutable record on the blockchain, the medicine is marked as authentic. In cases where the data is missing or tampered with, the system alerts the user about potential fraud. This module empowers end-users to make informed decisions while purchasing medicines. It also strengthens trust by ensuring that the medicine they consume meets quality standards. Blockchain technology ensures the integrity of this verification process, making it impossible for counterfeit medicines to infiltrate the system unnoticed.

**4. Consensus Algorithm for Medicine Validation:** The consensus algorithm plays a critical role in determining whether a medicine is authentic. This module implements blockchain consensus mechanisms, such as Proof of Stake (PoS) to validate transactions within the supply chain. Every medicine’s data is verified by a network of nodes before being added to the blockchain ledger. When a new medicine is registered or verified, nodes in the network validate the data using the consensus algorithm. For example, PoS assigns validator nodes based on their stake in the network, ensuring decentralization and preventing manipulation. Alternatively, PoS achieves consensus by requiring agreement from a majority of nodes, making it highly efficient for private blockchain networks used in supply chains. This validation ensures that only genuine medicines with verified details are accepted into the system. Counterfeit products attempting to enter the supply chain are flagged and rejected. The consensus algorithm ensures transparency, secure among all participants in the medicine SC.

## Algorithm Design

In the proposed we used set of algorithms during the execution, these algorithms describe in detail in this section. Initially the smart contract generation algorithm is a process used to create, verify, and deploy self-executing contracts on a blockchain. It begins by encoding predefined rules and logic into a digital contract, typically written in a programming language like Solidity. The contract logic is hashed using a cryptographic function, ensuring its integrity and immutability.

### 1. Smart Contract Generation

Smart contracts are predefined sets of rules. Their generation involves cryptographic principles and logical computation.

**Hashing Functions for Rules:**

$$H = Hash\big(f(x)\big)$$

$f(x)$: The smart contract logic.

$H$: The cryptographic hash of the contract logic, ensuring immutability.

**Digital Signature:**

$$S{=}D_{priv}\ (H)$$

$D_{priv}$: The private key of the creator.

$S$: Digital signature proving authenticity.

**Transaction Incorporation:**

$$T = (H, S)$$

The hash and signature are packaged into a transaction that is added in blockchain. To verify the authenticity of the smart contract, the users private key is used to create a digital sign ($S$), which is then appended to the contract hash. This signature proves ownership and prevents unauthorized tampering. The smart contract, along with its hash and signature, is packaged into a transaction ($T$) and submitted to the blockchain network. Once submitted, the contract undergoes validation by network nodes (miners or validators), ensuring it adheres to network protocols and consensus rules.

### 2. Genesis Block

It is an first block in the blockchain and is hardcoded. It typically contains no reference to a previous block.

**Block Hash:**

$$B_{gen}=Hash(T1+T2+\cdots+Tn)$$

*T1,T2,...,Tn*: Transactions included in the genesis block.

$B_{gen}$: Hash of the genesis block.

**Nonce (Proof of Work for Genesis Block):**

$$B_{gen}=Hash(Data//Nonce)$$

The **Genesis Block algorithm** refers to the creation of the first block in a blockchain, which serves as the foundation of the entire chain. Its creation involves several key steps:

All initial data, such as predefined transactions or metadata, is compiled. These transactions are typically hardcoded into the blockchain's implementation. A cryptographic hash function is used to combine the transaction data into a single unique value. If multiple transactions exist, a Merkle root is generated to summarize them.

$$B_{gen}=Hash(T1+T2+\cdots+Tn)$$

To ensure security, a valid hash must meet a difficulty target. The algorithm incrementally adjusts the nonce (a random number) and recalculates the hash until the condition $H(Block+Nonce) < Target$ is satisfied. Once the genesis block is mined, its hash serves as the reference for all future blocks, making it immutable. The genesis block is critical as it establishes the blockchain's cryptographic and structural foundation, ensuring integrity and trustworthiness in the decentralized network.

### 3. Hash Generation

Hash generation is critical for block integrity. The formula for generating a block hash:

**Merkle Root:**

$$M=Hash(Hash(T1)+Hash(T2))$$

*M:* Merkle root of all transactions *T*.

The process begins with the Merkle Tree, a structure used to efficiently and securely verify transactions. All transactions *(T1,T2,...,Tn)* in the block are hashed, and these hashes are combined pairwise to create a Merkle Root:

**Block Hash:** The block headers contains metadata such as the previous hash and timestamp with Merkle Root, is concatenated with a Nonce (a random number used for mining). The resulting data is hashed:

$$H=Hash(Header+M+Nonce)$$

*Header*: Metadata (timestamp, previous block hash, etc.).

*Nonce*: Proof of Work value.

The generated hash serves as the block's unique identifier and must meet the blockchain's difficulty level to be valid. This mechanism ensures that blocks are securely linked, prevents tampering, and establishes the foundation for consensus algorithms such as PoW and PoST.

### 4. Proof of Work (PoW)

It is an type of consensus approach that ensure the security and integrity of the system. It requires participants solve the difficulty as puzzle to validate and add a new block to the blockchain. The algorithm involves hashing the block data combined with a variable called the *nonce*. Miners repeatedly adjust the nonce to produce a hash that meets the network's difficulty target, which is typically a hash value with a specific number of leading zeros. The process is computationally intensive, as miners must perform numerous hash calculations to find a valid solution. The key formula is:

$$H(Block+Nonce) < Target$$

*Block*: Block data.

*Nonce*: Iterative number added to adjust the hash.

*Target*: Difficulty threshold.

**Hash Rate (Performance Measure):**

$$R = \frac{n}{t}$$

$R$: Hash rate.

$n$: Total hashes calculated.

$t$: Time taken.

where $H$ is the secure hash function, $Block$ is the block's data, $Nonce$ is the adjustable number, and $Target$ represents the difficulty level. The difficulty is periodically adjusted to maintain a constant block generation rate. PoW ensures decentralization and security but it consumes high computational power and heavy energy consumption. It is used in networks like Bitcoin and Ethereum (pre-2.0).

### 5. Proof of Stake (PoS)

Proof of Stake (PoS) is an advanced consensus algorithm that builds upon the traditional PoS by incorporating the factor of time into the block selection process. PoS enhances this by rewarding participants not only based on their stake but also on how long they have held it. This encourages long-term commitment and discourages rapid stake turnover. The probability of a node being selected to mine the next block is calculated as**:**.

$$P = \frac{S_i \cdot T_i}{\sum_{j=1}^{N} S_j T_j}$$

$T_i$: Time for which stake $S_i$ is held.

Here, $S_i$ is the stake of a participant, $T_i$ is the time they've held it, and the denominator represents the total weighted stake across all participants. By factoring in time, PoST provides a fairer and more distributed block creation mechanism.

### 6. Majority Voting (Consensus Mechanism)

The algorithm begins by broadcasting the proposed block to all nodes which is associated in the network. The every node independently verifies the block's validity by checking its contents, such as transactions and cryptographic proofs. Once verified, each node casts its vote (e.g., 1 for valid, 0 for invalid). The network aggregates these votes, and a majority threshold—typically greater than 50%—must be met for the block to be accepted. In weighted majority voting, nodes' votes are influenced by factors like their stake, reputation, or computational power. The final consensus is calculated using:

$$C = \frac{n_{agree}}{n_{total}} > 0.5$$

$n_{agree}$ : Number of nodes agreeing on the block.

$n_{total}$ : Total number of nodes.

**Weighted Voting:**

$$\mathbf{V} = \sum_{i=1}^{n} w_i \cdot v_i$$

$w_i$: Weight of vote from node iii.

$v_i$: Vote value (0 or 1).

The above both methods maintain decentralization, ensures consistency across the blockchain, and guards against malicious actors attempting to disrupt the network.

## Results and Discussion

The implementation was conducted in an open-source Java environment using a 3.0 GHz CPU and 16 GB RAM, specifically within JDK 1.8. A custom blockchain solution was proposed, leveraging a distributed approach to create virtual nodes, ranging from 4 to 100. Experimental results from this setup are thoroughly analyzed. Visual aids, such as tables and figures, are utilized to present data effectively, enhancing the comprehension of the results. These graphical elements play a critical role in academic research by simplifying complex information and supporting a clear interpretation of findings from the investigation. The detailed outcomes are summarized below.

Exp 1: Hash generation with different data size with various hash generation methods

| Data Size | SHA-1 | SHA-2 | SHA-256 | SHA-512 |
|---|---|---|---|---|
| 1 KB | 2.2 | 2.1 | 2 | 2 |
| 2 KB | 2.9 | 2.5 | 2.4 | 2.3 |
| 3 KB | 3.2 | 2.9 | 2.7 | 2.6 |
| 4 KB | 3.8 | 3.2 | 3.1 | 2.9 |
| 5 KB | 4.1 | 3.8 | 3.4 | 3.0 |
| 10 KB | 4.3 | 4.1 | 3.9 | 3.3 |
| 20 KB | 7.9 | 7.1 | 6.6 | 5.8 |
| 50 KB | 15.6 | 14.8 | 12.2 | 11.4 |

Table 1 compares hash generation times (in milliseconds) for hashing algorithms—SHA-1, SHA-2, SHA-256, and SHA-512—across data sizes from 1 KB to 50 KB, showcasing their computational efficiency. Figure 2 emphasizes the balance between hashing speed and algorithm complexity. SHA-1 is the fastest for small data, while SHA-512 excels in handling larger data sizes, offering both security and versatility for modern cryptographic applications.

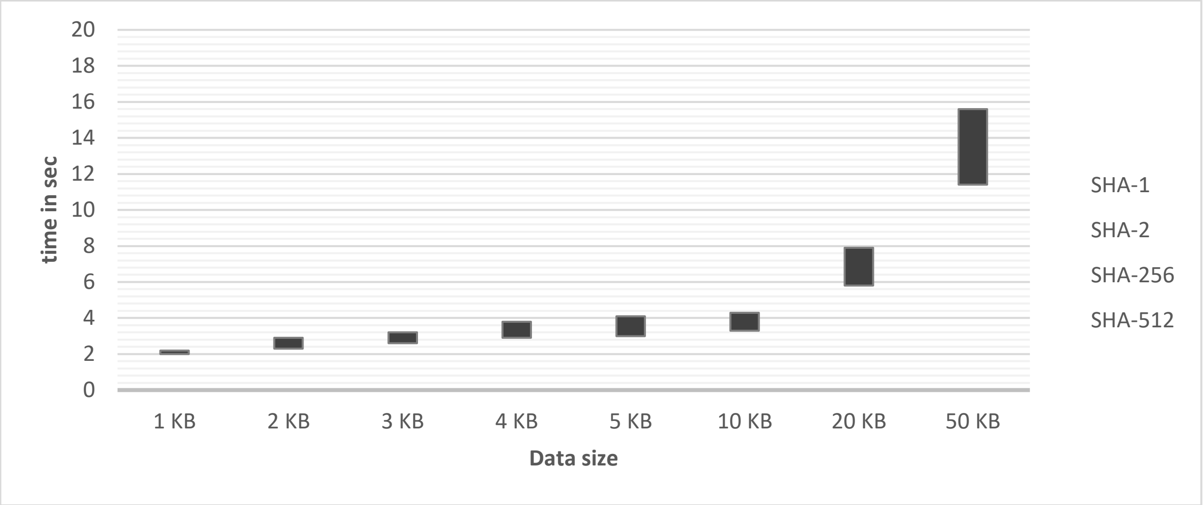


Figure 2: Transaction mining analysis (Gigabyte NVIDIA GeForce GT 710 2 GB DDR3 Graphics Card) time in seconds

For smaller data sizes (1–5 KB), all four algorithms—SHA-1, SHA-2, SHA-256, and SHA-512—perform similarly, with SHA-1 being the fastest. At 1 KB, SHA-1 processes in 2.2 ms, while SHA-512 takes 2 ms—a negligible difference. At 5 KB, SHA-1 leads with 4.1 ms, followed by SHA-2 (3.8 ms), SHA-256 (3.4 ms), and SHA-512 (3.0 ms). However, as data sizes exceed 10 KB, SHA-512 demonstrates better scalability. For instance, with 50 KB, SHA-512 outperforms SHA-1 by 4.2 ms.

This performance disparity stems from algorithmic design. SHA-1, an older standard, excels with smaller data but lacks robustness. SHA-2 and SHA-512, designed for enhanced security, handle larger datasets more efficiently. SHA-512 is ideal for applications requiring scalability and high security, while SHA-1 or SHA-2 suffice for smaller data with lower security demands.

Table 2 : comparison between PoW and PoST algorithm

| **Data size** | **PoST** | | | |
|---|---|---|---|---|
| | **1GB** | **2GB** | **5GB** | **10 GB** |
| **1 KB** | 3.0 | 3.0 | 1.7 | 1.0 |
| **2 KB** | 3.8 | 3.2 | 2.8 | 1.2 |
| **3 KB** | 4.0 | 3.4 | 3.2 | 2.4 |
| **4 KB** | 4.9 | 4.3 | 3.4 | 3.0 |
| **5 KB** | 6.0 | 5.4 | 5.0 | 4.2 |
| **10 KB** | 10.1 | 9.3 | 7.1 | 5.1 |

Table 2 showcases the performance metrics of a system processing varying data sizes, highlighting its efficiency across file sizes from 1 KB to 10 KB and datasets ranging from 1 GB to 10 GB. Each metric represents a performance indicator, such as processing time (in seconds) or throughput (in MB/s), demonstrating the system's adaptability to different workloads. The data illustrates how the system maintains consistent performance and scalability, ensuring effective handling of diverse data scenarios. These metrics provide valuable insights into the system's ability to manage increasing data loads while maintaining optimal processing efficiency and reliability.

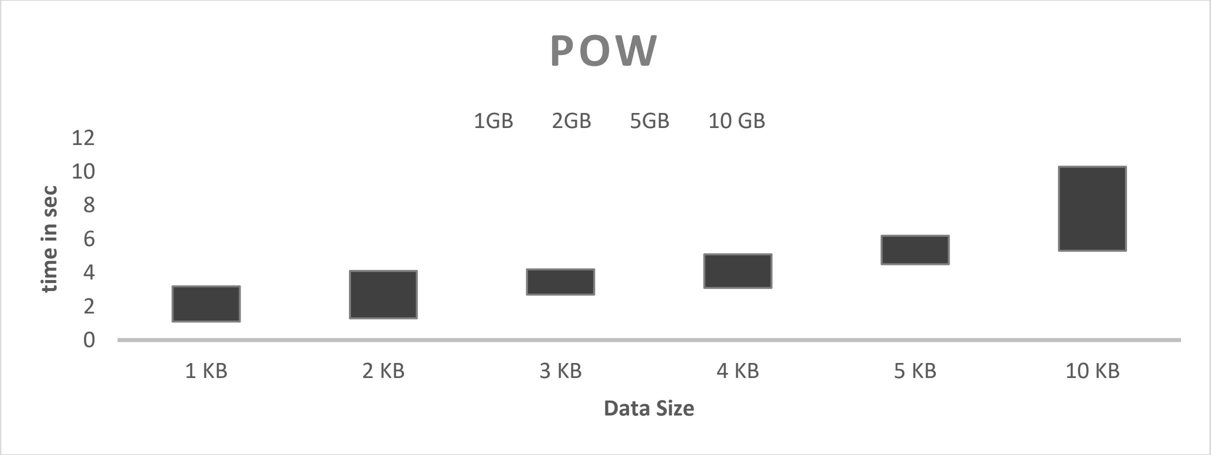


Figure 3 : performance evaluation PoW mining algorithm

Figure 3 highlights the performance impact of increasing file sizes (1 KB to 10 KB) across datasets of varying sizes. For smaller datasets like 1 GB and 2 GB, performance degradation is minimal. For instance, in the 1 GB dataset, processing a 1 KB file takes 3.2 units, while a 10 KB file requires 10.3 units, showing linear scaling. Similarly, the 2 GB dataset ranges from 3.0 to 9.8 units. However, larger datasets like 5 GB and 10 GB exhibit significant performance drops. In the 10 GB dataset, processing a 1 KB file takes 1.1 units, but a 10 KB file increases to 5.3 units, indicating exponential degradation. This reflects potential system bottlenecks in capacity, memory, or I/O bandwidth. Smaller datasets manage large files efficiently, while larger datasets struggle. Figure 3 emphasizes the need to optimize system configurations to maintain consistent performance when handling larger datasets and file sizes.

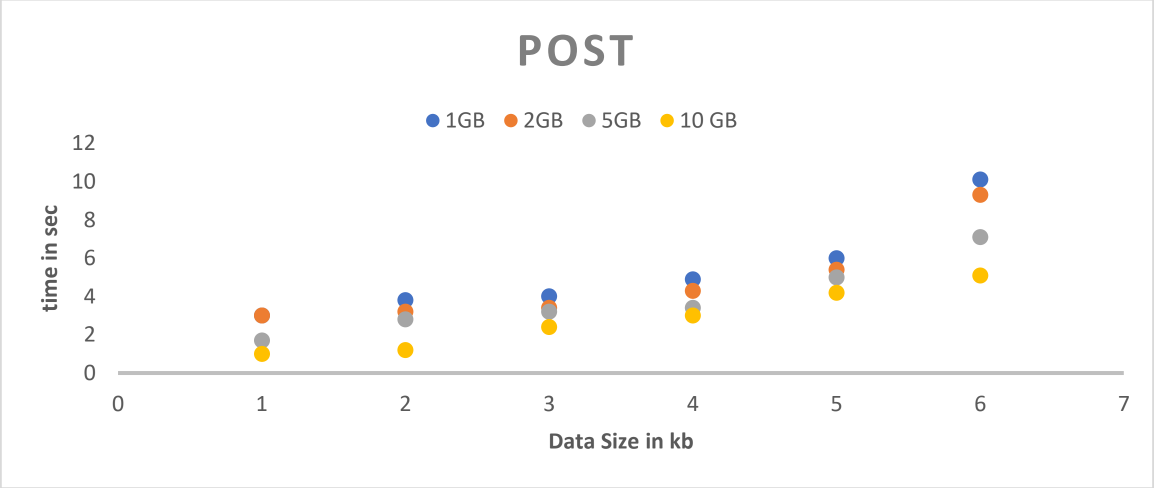


Figure 4 : performance evaluation PoW mining algorithm

Figure 4 highlights performance trends for varying file sizes and dataset sizes. For smaller file sizes, such as 1 KB, performance remains stable at 3.0 units for datasets of 1 GB and 2 GB but drops significantly for larger datasets, reaching 1.7 units for 5 GB and 1.0 unit for 10 GB. This indicates higher overhead when processing larger datasets with smaller files. As file sizes increase to 2 KB and 3 KB, a similar pattern emerges, though the performance declines more gradually, suggesting reduced processing overhead compared to smaller files. For 4 KB and 5 KB file sizes, performance decreases are less pronounced, reflecting a better balance between file size and efficiency. The highest efficiency is observed with 10 KB files, where performance remains relatively strong despite dataset growth. Overall, the analysis underscores the need to optimize file sizes to improve scalability and efficiency, especially for large-scale data processing systems.

## Conclusion

The proposed research has described SCM using customized blockchain, integrated with customized smart contracts, provides an effective solution to eliminate challenges by enhancing traceability and transparency. The proposed blockchain-based framework enables the secure registration of medicines with unique identifiers, ensuring real-time tracking and verification through QR codes linked to the digital ledger. By employing consensus algorithms PoW and PoS for scalability and energy efficiency, the system achieves an optimal balance of speed, security, and sustainability. The results indicate substantial improvements in counterfeit detection rates and transaction validation times, addressing critical vulnerabilities in the supply chain. Additionally, user feedback highlights the increased trust and reliability of the system, fostering greater confidence among stakeholders. Beyond its impact on medical supply chains, the framework demonstrates scalability and adaptability, offering potential for broader application across various industries requiring secure and transparent supply chain management. In conclusion, blockchain technology, enhanced by customized smart contracts, presents a transformative approach to addressing pressing issues in the medical supply chain, improving safety, efficiency, and trust across the healthcare ecosystem.

## References

[1] Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob, and M. Omar, “Automating procurement contracts in the healthcare supply chain using blockchain smart contracts,” IEEE Access, vol. 9, pp. 37397–37409, 2021, doi: 10.1109/ACCESS.2021.3062471.

[2] Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi and S. Ellahham, “A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain,” in IEEE Access, vol. 9, pp. 9728-9743, 2021, doi: 10.1109/ACCESS.2021.3049920.

[3] G. Subramanian, A. S. Thampy, N. V. Ugwuoke and B. Ramnani, “Crypto Pharmacy – Digital Medicine: A Mobile Application Integrated With Hybrid Blockchain to Tackle the Issues in Pharma Supply Chain,” in IEEE Open Journal of the Computer Society, vol. 2, pp. 26-37, 1 Jan. 2021, doi: 10.1109/OJCS.2021.3049330.

[4] P. M. Reyes, M. J. Gravier, P. Jaska and J. K. Visich, “Blockchain Impacts on Global Supply Chain Operational and Managerial Business Value Processes,” in IEEE Engineering Management Review, vol. 50, no. 3, pp. 123-140, 01 thirdquarter,Sept. 2022, doi: 10.1109/EMR.2022.3187729.

[5] S. Pattanayak, R. M. Arputham, M. Goswali and N. P. Rana, “Blockchain Technology and Its Relationship With Supply Chain Resilience: A Dynamic Capability Perspective,” in IEEE Transactions on Engineering Management, vol. PP, no. 99, pp. 1-15, 19 Jan. 2023, doi: 10.1109/TEM.2023.10021963

[6] Musamih, I. Yaqoob, K. Salah, R. Jayaraman, M. Omar and S. Ellahham, “Using NFTs for Product Management, Digital Certification, Trading, and Delivery in the Healthcare Supply Chain,” in IEEE Transactions on Engineering Management, vol. PP, no. 99, pp. 1-22, 02 Nov. 2022, doi: 10.1109/TEM.2022.3192166.

[7] R. Z. Rasi, U. S. Bin Rakiman, R. Z. Raja Mohd. Radzi, N. R. Masrom and V. P. Kaliani Sundram, “A Literature Review on Blockchain Technology: Risk in Supply Chain Management,” in IEEE Engineering Management Review, vol. 50, no. 1, pp. 186-200, 01 Firstquarter,march 2022, doi: 10.1109/EMR.2021.3133447.

[8] U. Agarwal, V. Rishwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro and R. Sharma, “Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review,” in IEEE Access, vol. 10, pp. 85493-85517, 2022, doi: 10.1109/ACCESS.2022.3194319.

[9] K. Gai, Y. Zhang, M. Qiu and B. Thuraisingham, “Blockchain-Enabled Service Optimizations in Supply Chain Digital Twin,” in IEEE Transactions on Services Computing, vol. 16, no. 3, pp. 1673-1685, May-June 2023, doi: 10.1109/TSC.2022.3192166.

[10] Y. Madhwal, Y. Borbon-Galvez, N. Etemadi, Y. Yanovich and A. Creazza, “Proof of Delivery Smart Contract for Performance Measurements,” in IEEE Access, vol. 10, pp. 69147-69159, 2022, doi: 10.1109/ACCESS.2022.31856

[11] A. Omar, R. Jayaraman, M. S. Debe, H. R. Hasan, K. Salah and M. Omar, “Supply Chain Inventory Sharing Using Ethereum Blockchain and Smart Contracts,” in IEEE Access, vol. 10, pp. 2345-2356, 2021, doi: 10.1109/ACCESS.2021.3139829.

[12] D. Hawashin, K. Salah, R. Jayaraman, I. Yaqoob and A. Musamih, “A Blockchain-Based Solution for Mitigating Overproduction and Underconsumption of Medical Supplies,” in IEEE Access, vol. 10, pp. 71669-71682, 2022, doi: 10.1109/ACCESS.2022.3188778.

[13] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic and M. Omar, “Trustworthy IoT Data Streaming Using Blockchain and IPFS,” in IEEE Access, vol. 10, pp. 17707-17721, 2022, doi: 10.1109/ACCESS.2022.3149312.

[14] S. Guo, X. Sun and H. K. S. Lam, “Applications of Blockchain Technology in Sustainable Fashion Supply Chains: Operational Transparency and Environmental Efforts,” in IEEE Transactions on Engineering Management, vol. 70, no. 4, pp. 1312-1328, April 2023, doi: 10.1109/TEM.2020.3034216.

[15] R. D. Garcia, G. S. Ramachandran, R. Jurdak and J. Ueyama, “Blockchain-Aided and Privacy-Preserving Data Governance in Multi-Stakeholder Applications,” in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 3781-3793, Dec. 2022, doi: 10.1109/TNSM.2022.3225254.