Decision Analytics Journal 17 (2025) 100620

Contents lists available at ScienceDirect

Decision Analytics Journal

journal homepage: www.elsevier.com/locate/dajour

PharmChain: A data-driven scenario-based drug traceability and regulation blockchain framework

Amrendra Singh Yadav [a], Vincent Charles [b,*], Tatiana Gherman [c], Vinay Kumar [d], Vijayant Pawar [e], Nishchay Chaudhary [f]

[a] Atal Bihari Vajpayee Indian Institute of Information Technology and Management, Gwalior, India
[b] Queen's Business School, Queen's University Belfast, Belfast BT9 5EE, United Kingdom
[c] Faculty of Business and Law, University of Northampton, Northampton NN1 5PH, United Kingdom
[d] Department of Computer Science and Engineering, National Institute of Technology Delhi, Delhi, India
[e] School of Computer Science, Engineering, and Technology, Bennett University, Greater Noida, India
[f] IQVIA, India

ARTICLE INFO

Keywords:
Blockchain
Smart contract
Drug traceability
Merkle direct acyclic graph
Pharmaceutical supply chain
Data-driven scenario-based

ABSTRACT

The manufacturing and distribution of counterfeit tablets, especially in developing countries, is an urgent and increasingly critical global problem. Falsified medicinal products may contain incorrect ingredients and doses. One of the reasons for drug counterfeiting is the imperfect supply chain system in the pharmaceutical industry. Medicinal products are moved between manufacturers, suppliers, wholesalers, retailers, and pharmaceutical firms before meeting consumers. This study proposes PharmChain, a scenario-oriented drug traceability and regulation blockchain framework that reconstructs the entire service infrastructure by splitting the service provider into three separate service components and ensuring the authenticity and privacy of traceability details. PharmChain can track medication development via patient supply in the pharmaceutical industry. An Ethereum-based blockchain stores the transactions, and only trusted parties can access the data through the chain. We create and test our smart contract code in the Remix environment. We present detailed cost and security analyses incurred by supply chain stakeholders. We also use cost analysis to assess the performance of the proposed solution and demonstrate its affordability.

1. Introduction

Trust serves as a cornerstone of the pharmaceutical industry, underpinning the safe, effective, and reliable delivery of medicines across the supply chain. However, this trust is increasingly jeopardised by the growing circulation of counterfeit medicinal products, a concern that has gained prominence in recent studies, highlighting both financial and humanitarian risks [1–3]. These counterfeit drugs not only cause substantial economic damage but also pose serious threats to public health, particularly in low-regulation environments with limited oversight. As Ghadge et al. [1] further pointed out, such risks escalate during global health crises, such as pandemics, where falsified medications can undermine treatment efficacy and severely erode public confidence in healthcare systems. According to the World Health Organisation [4], an estimated one in ten medical products in developing countries is substandard or falsified, failing to meet established safety and efficacy standards. The World Health Organisation [5] further highlights that counterfeit pharmaceuticals contribute to treatment failures, drug resistance, and severe health complications, with critical medications such as antibiotics, cardiovascular drugs, and cancer treatments being particularly affected. The ability of counterfeiters to mimic legitimate pharmaceutical packaging exacerbates the issue, making detection increasingly challenging for regulatory authorities and consumers alike.

Despite continued advancements in pharmaceutical research and development, ensuring the delivery of authentic medications to end users remains a critical challenge, primarily due to persistent vulnerabilities in the supply chain. As Gaynor et al. [6] emphasised, these vulnerabilities continue to undermine drug safety and traceability despite technological progress. The increasingly globalised nature of pharmaceutical manufacturing, with numerous intermediaries such as manufacturers, suppliers, wholesalers, retailers, and healthcare providers, introduces multiple points of entry for counterfeit drugs

[*] Correspondence to: Queen's Business School, Queen's University Belfast, 185 Stranmillis Road, Belfast, Northern Ireland, BT9 5EE, United Kingdom.
E-mail addresses: asy@iiitm.ac.in (A.S. Yadav), c.vincent@qub.ac.uk (V. Charles), tatiana.gherman@northampton.ac.uk (T. Gherman), vinayvats@nitdelhi.ac.in (V. Kumar), vijayant.pawar@bennett.edu.in (V. Pawar), Nishchay.chaudhary@iqvia.com (N. Chaudhary).

https://doi.org/10.1016/j.dajour.2025.100620
Received 19 June 2024; Received in revised form 22 June 2025; Accepted 9 August 2025
Available online 13 August 2025

[7]. This complexity, combined with limited transparency, outdated infrastructure, and fragmented regulatory oversight, enables illicit actors to exploit systemic gaps and introduce fraudulent products into legitimate distribution networks. To address these challenges, innovative technological solutions are required. Blockchain technology, initially introduced by Nakamoto [8], has emerged as a promising tool for enhancing transparency, security, and traceability in supply chain management [9–12]. Those interested in a general overview of blockchain's historical background and underlying principles may refer to Tripathi et al. [13], while a more specific review of its applications in supply chain management can be found in Agarwal et al. [14].

Blockchain technology offers a decentralised and tamper-proof ledger that ensures pharmaceutical transactions are secure and verifiable at every stage of the supply chain, a capability increasingly recognised in recent studies [15–17]. These studies highlight how the integration of smart contracts can automate compliance protocols, enforce regulatory standards, and enable real-time auditing of drug distribution activities. Such capabilities not only streamline supply chain operations but also play a critical role in mitigating the risks of counterfeiting and fraud, thereby reinforcing trust among manufacturers, distributors, regulators, and end users. Recognising the limitations of existing systems, this research proposes PharmChain, a blockchain-based pharmaceutical supply chain tracking system that adopts an off-chain storage model using Swarm, a decentralised network where large files are stored externally and only cryptographic references are retained on-chain. PharmChain aims to address key weaknesses in current traceability and regulatory frameworks by: (1) ensuring data authenticity and security through decentralised verification mechanisms; (2) facilitating private and permissioned access to sensitive supply chain data; (3) introducing a structured approach to handling drug transactions, including packaging, repackaging, and order cancellations; and (4) enhancing affordability and performance through Ethereum-based smart contracts and cost analysis.

This paper makes the following key contributions:

- Develops PharmChain, a blockchain-based tracking system that leverages smart contracts and decentralised storage to securely track pharmaceutical products throughout the supply chain.
- Analyses traditional supply chain vulnerabilities and compares existing blockchain-based solutions, identifying key limitations that PharmChain aims to overcome.
- Implements and validates PharmChain's smart contracts within a Remix testing environment, ensuring system functionality and performance.
- Conducts cost and security analysis, demonstrating the affordability and effectiveness of the proposed approach.
- Integrates Swarm, a decentralised file system, to address blockchain storage limitations, allowing for efficient storage of drug-related data.

The remainder of this paper is structured as follows: Section 2 reviews related research in pharmaceutical supply chains and blockchain applications, while Section 3 discusses traditional pharmaceutical supply chain models and their limitations. Section 4 presents the technological foundations of the system, followed by Section 5, which outlines PharmChain's architecture and workflow. Section 6 describes the implementation and validation of the system, and Section 7 provides a comparative analysis and performance evaluation. Section 8 examines the managerial implications of the proposed system for the pharmaceutical industry, and finally, Section 9 presents concluding remarks and future research directions.

2. Related works

This section reviews existing research on blockchain applications in pharmaceutical supply chains, highlighting key developments, limitations, and open challenges. While several studies have explored blockchain-based drug traceability and regulatory compliance, many remain theoretical, or face issues related to scalability, interoperability, and data privacy. By analysing prior work, this review identifies critical gaps and establishes the foundation for PharmChain, demonstrating how it addresses these limitations through a structured, scenario-based approach.

O'Hagan and Garlington [18] highlighted how the internet and the dark web have facilitated the counterfeit drug trade, offering anonymity to manufacturers, distributors, and consumers. The authors emphasised that while online pharmacies serve legitimate medical purposes, they also pose serious risks by harbouring counterfeit products. The challenges in detecting falsified medicines, such as complex packaging replication and hidden trade routes, expose vulnerabilities in existing regulatory frameworks. Despite global initiatives to combat counterfeit drugs, most proposed solutions remain theoretical, lacking practical implementation strategies. This demonstrates the need for robust technological frameworks to enhance drug traceability and regulatory enforcement.

Mettler [19] explored the applicability of blockchain in healthcare, particularly for drug traceability and patient-centric research. While blockchain's decentralisation and transparency offer trust and security, the study remains purely theoretical, lacking practical demonstrations or case studies to validate its feasibility in large-scale pharmaceutical supply chains.

Xia et al. [20] proposed a hybrid blockchain-cloud model for medical data sharing, which enhances data privacy and auditing capabilities. However, the absence of a defined access control mechanism introduces potential security risks, limiting its effectiveness in regulating pharmaceutical supply chains. Similarly, Cheng et al. [21] developed a blockchain-based patient identification system to improve scalability and efficiency in health record management. Although the model enhances patient tracking, its reliance on extensive stakeholder collaboration and technical complexity makes large-scale implementation difficult, highlighting the need for simplified decentralised health systems.

Huang et al. [22] introduced Drugledger, a blockchain-based framework for drug traceability and regulation. The system ensures data authenticity and privacy, but its application is limited to small-scale scenarios, raising concerns about scalability and real-world implementation. Similarly, Haq and Esuka [23] proposed a blockchain system for drug traceability, enabling patients to verify drug authenticity. However, their study provides only an application layout, lacking technical depth or comprehensive deployment analysis, leaving uncertainties regarding performance, security, and regulatory adoption.

Shahid et al. [24] and Hasan et al. [25] examined the use of blockchain and the Interplanetary File System (IPFS) for secure pharmaceutical supply chains. While these models incorporate detailed algorithms and performance evaluations, their reliance on private blockchain solutions raises concerns about efficiency versus decentralisation. A key challenge in blockchain adoption is balancing security, scalability, and decentralisation, as private blockchains increase efficiency but deviate from blockchain's trustless principles, making them less suitable for global pharmaceutical applications.

Recent research has increasingly highlighted the potential of blockchain technology to enhance healthcare logistics and sustainability. For instance, Yousefi and Tosarkani [26] explored how blockchain can support sustainable supply chain practices, while Beaulieu et al. [27] identified key digitisation vulnerabilities in healthcare logistics, particularly within home care services. Complementing these findings, Benevento et al. [28] examined the broader integration of digital technologies into healthcare supply chains, and Kholaif et al. [29] investigated blockchain's contribution to green and sustainable healthcare systems. Collectively, these studies underscore blockchain's relevance to healthcare applications. However, they also reveal a persistent gap in tailoring these solutions to meet the specific demands of cross-border pharmaceutical trade, regulatory compliance, and patient data privacy, areas where our proposed PharmChain framework seeks to make a targeted contribution.

This review highlights several critical knowledge gaps in existing research. Firstly, scalability remains a major concern, as many blockchain models struggle with high transaction costs and slow processing speeds, limiting their viability for large-scale pharmaceutical supply chains. Secondly, while some studies propose private blockchains for efficiency, they contradict decentralisation principles, raising questions about data integrity and stakeholder trust. Thirdly, interoperability with regulatory frameworks is largely unexplored, creating barriers to seamless compliance. Finally, secure yet scalable storage solutions for large pharmaceutical datasets remain underdeveloped, with on-chain storage being cost-prohibitive and off-chain alternatives lacking standardisation.

To address these gaps, this study proposes PharmChain, a blockchain-based pharmaceutical supply chain framework that integrates decentralised storage and smart contracts to enhance transparency, data integrity, and supply chain security. By leveraging Ethereum's Proof of Stake (PoS) model, PharmChain offers higher transaction throughput and cost efficiency, making blockchain adoption feasible for large-scale pharmaceutical applications. Additionally, interoperability with existing regulatory frameworks is ensured through widely adopted standards such as ERC-20 and ERC-721, facilitating secure data sharing and compliance tracking. This study aims to provide a practical, scalable, and privacy-preserving blockchain solution tailored to the unique demands of the pharmaceutical industry, bridging the gap between theoretical proposals and real-world implementation.

Table 1 compares previous research studies based on technologies used, advantages, and limitations. The analysis highlights that while blockchain architecture is widely applied, many models lack additional technologies to improve security, interoperability, and efficiency. Technological advancements over the years have introduced more sophisticated models, yet challenges in scalability, decentralisation, and regulatory compliance persist.

Table 2 presents a comparison of blockchain technologies across different studies, considering validation methods, blockchain types, application areas, authority distribution, access mechanisms, and additional incorporated technologies. These factors determine the adoption feasibility of blockchain in supply chains and underscore the need for solutions that balance decentralisation, security, and regulatory compliance.

3. Limitations of the traditional system

To identify vulnerabilities in the pharmaceutical supply chain, we analysed traditional supply chain processes and found that transactions typically occur in four stages. The points at which counterfeiting can occur are outlined below:

Stage 1 (Raw material sourcing): The supply chain begins with the supplier providing raw materials, which presents the first potential risk. Suppliers may introduce adulterated, obsolete, low-cost, or substitute ingredients, compromising the quality and safety of medications.

Stage 2 (Manufacturing): The next stage involves drug production by manufacturers. This is a critical point where falsified medicines or substandard components can enter the supply chain. Counterfeit drugs may contain incorrect ingredients, have altered packaging, or even be placebos instead of genuine medication. Counterfeit manufacturers often replicate the appearance of authentic drugs but operate without proper quality control.

Stage 3 (Distribution and wholesale): At this stage, wholesalers and distributors handle drug distribution. Fraudulent actors can exploit this link by infiltrating legitimate networks with falsified medicines, leveraging weak security measures or engaging in barcode fraud to bypass mass scanning systems. While some counterfeit drug distribution operations are highly sophisticated, others rely on simple loopholes in transportation and logistics.

Stage 4 (Retail and consumer access): Pharmacies, hospitals, and online retailers represent the final stage of the supply chain, where counterfeit drugs can reach consumers. Even large pharmacies may unknowingly distribute falsified medications. Many consumers opt for online prescription purchases due to lower costs; however, these products often originate from different countries with varying regulations, increasing the risk of receiving counterfeit or mislabelled drugs. Illicit online pharmacies frequently re-emerge even after government crackdowns, capitalising on the high-profit margins of counterfeit pharmaceuticals.

Through our analysis of the pharmaceutical supply chain, we identified several existing strategies aimed at mitigating counterfeit drug infiltration. Some of these industry solutions are discussed below:

Advanced packaging technologies: Many pharmaceutical companies have adopted complex packaging strategies to deter counterfeiting. One such approach is holographic technology, where holograms on product packaging serve as authentication markers. The assumption is that consumers can verify a product's authenticity by checking for a hologram. A major advantage of this method is that each product can be uniquely personalised. However, implementing holographic packaging can be expensive, especially for large-scale production. Additionally, counterfeiters can replicate holograms, undermining the security of this approach. Another limitation is that holograms alone do not provide real-time tracking or traceability when counterfeit products enter the supply chain.

Product serialisation: Mass serialisation leverages radio frequency (RF) technology to track and record pharmaceutical products across the supply chain. Radio Frequency Identification (RFID) tags are assigned to individual packages, allowing chip readers to collect data at various checkpoints. This method enhances traceability by ensuring that only authorised products reach the consumer. However, RFID enforcement is costly due to the high price of RFID tags and the infrastructure needed to support them [30]. Additionally, different RFID systems may require varying types of readers and tags, leading to compatibility issues that complicate large-scale implementation.

Encryption-based authentication: In the pharmaceutical sector, encryption techniques have been proposed as a means to safeguard against counterfeit drugs. This approach involves encoding pharmaceutical data using mass encryption software, ensuring that only authorised users can decode the digital information [31]. While encryption enhances security, it requires large-scale database servers to store encrypted data, making implementation resource-intensive.

The EU Falsified Medicines Directive: The European Union Falsified Medicines Directive (EU FMD) is a regulatory initiative designed to protect the pharmaceutical supply chain by integrating unique identification features into drug packaging [32]. Under this directive, each pharmaceutical product is assigned a barcode containing a unique identifier, which is verified at multiple checkpoints as the product moves through the supply chain. The unique identifier includes essential details such as product code, name, dosage form, package size, serial number, batch number, and expiry date. While this directive enhances security, it primarily serves as a defencive mechanism rather than an active tracking solution.

4. Preliminaries

4.1. Blockchain data structure

Since the launch of Bitcoin by Satoshi Nakamoto, blockchain technology has gained widespread popularity, significantly influencing the digital payment system. Its applications are expected to revolutionise not only the financial services industry but also various non-financial sectors. The Bitcoin blockchain functions as a decentralised ledger that records all transactions in a chronological sequence. Transactions are grouped into blocks, and approximately every ten minutes, a new block is added to the chain. This decentralised structure ensures that no

Table 1
Comparison of related works.

Reference	Technology used	Advantages	Disadvantages
Mettler [19]	Blockchain, Digital Health	The paper analyses the different state-of-the-art technologies used in health care.	The paper's primarily theoretical evaluation could be demonstrated more efficiently and supplemented with practical analysis in the article.
Xia et al. [20]	Access Control, Blockchain, Electronic Medical Records	The authors incorporated blockchain with cloud computing technology for wider access.	Access to the network is not illustrated in the system, which means privacy protection is challenging.
Cheng et al. [21]	EHR, Unique Patient Identifier	Patient identification and health record system is developed, which does a good job when tracking a travelling patient.	The system is too complex to implement. It requires different stakeholders like hospitals and labs to work together for system development.
O'Hagan and Garlington [18]	Communication, Collaboration, and Regulation	The system focuses on dismantling the counterfeit industry.	The proposed system is purely theoretical, and its practical implementation is too complex.
Huang et al. [22]	Supply chain, Blockchain	The authors proposed a drug traceability and regulation framework called Drugledger.	The system is not implemented for large-scale scenarios.
Haq and Esuka [23]	Blockchain	The authors constructed a supply chain for the pharmaceutical industry where patients can also verify if the drug is authentic or not.	The authors provided only an application layout in the paper; most of the information about the system is not presented or is theoretical.
Shahid et al. [24]	Blockchain, Supply Chain, IPFS	The authors proposed a complete solution for the agriculture supply chain. The code implementation of the system is available on Github for further research and analysis.	The implementation of IPFS in the paper is given, but it is not clearly illustrated how files and data flow over the database.
Hasan et al. [25]	Blockchain, Smart Contract, IPFS	The system proposed by the authors targets the mechanical spare parts delivery problem. The authors incorporated a futuristic distributed file system scheme.	The system uses a private blockchain for the development of the system, which increases the efficiency of the system. However, it fails to follow the blockchain fundamentals of a public database.

Table 2
Comparison of technologies in investigated research.

Reference	Validation	Blockchain type	Area of application	Distribution of authority	Access mechanism	Additional incorporated technology
Mettler [19]	DPos	Private	Medical	Centralised	Permissioned	None
Cheng et al. [21]	Cryptographic Keys	Private	Medical	Decentralised	Permissioned	Cloud Computing
Huang et al. [22]	Ethereum	Public	Medical	Decentralised	Permissionless	None
Haq and Esuka [23]	Ethereum	Public	Food Industry	Centralised	Permissioned	IPFS
Shahid et al. [24]	Ethereum	Private	Mechanical Industry	Centralised	Permissioned	IPFS
Hasan et al. [25]	Ethereum	Public	Medical	Decentralised	Permissionless	None
Yousefi and Tosarkani [26]	Ethereum	Public	Supply Chain	Decentralised	Permissioned	None
Beaulieu et al. [27]	Authentication	Public	Medical Supply Chain	Decentralised	Permissionless	None
Benevento et al. [28]	Cryptographic Keys	Private	Supply chain integration	Decentralised	Permissioned	None

central authority governs the system; instead, it relies on a network of distributed nodes to achieve consensus and maintain trust. The core data structure of blockchain relies on cryptographic hashing, where each block stores a cryptographic hash reference to the previous block, forming an immutable chain (Fig. 1). This cryptographic linkage ensures that any modification to a previous block would require altering all subsequent blocks, making the system tamper-resistant and highly secure. In a blockchain network, each node acts as both a host and a server, participating in data distribution and network consensus. Transactions are validated through a decentralised consensus mechanism, ensuring consistency across all nodes and preventing fraudulent modifications. This architecture serves as the foundation for the future of decentralised, open-source technologies and has extended its use beyond digital payments to sectors such as healthcare, supply chain management, and digital identity verification.

4.2. Merkle DAG

A Merkle Directed Acyclic Graph (Merkle DAG) is a type of Direct Acyclic Graph (DAG) similar to a Merkle tree, but with additional flexibility. Unlike traditional Merkle trees, where each node has a fixed structure, Merkle DAGs allow more flexible node structures, where even non-leaf nodes can store data and the graph does not need to be strictly hierarchical or balanced. A Merkle tree is a structured way of organising data in a hierarchical, tree-like format, making it efficient for data verification and integrity checks. The foundation of Merkle trees relies on cryptographic hashing, a mathematical process

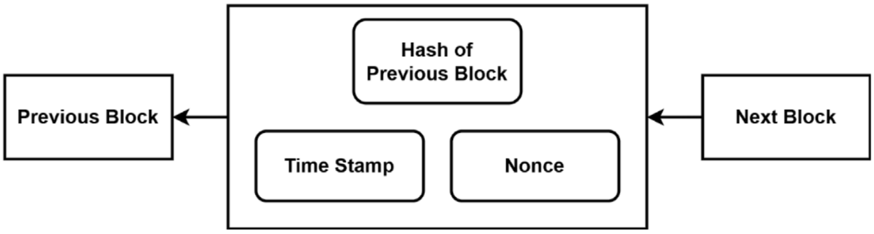


Fig. 1. Blockchain block structure.

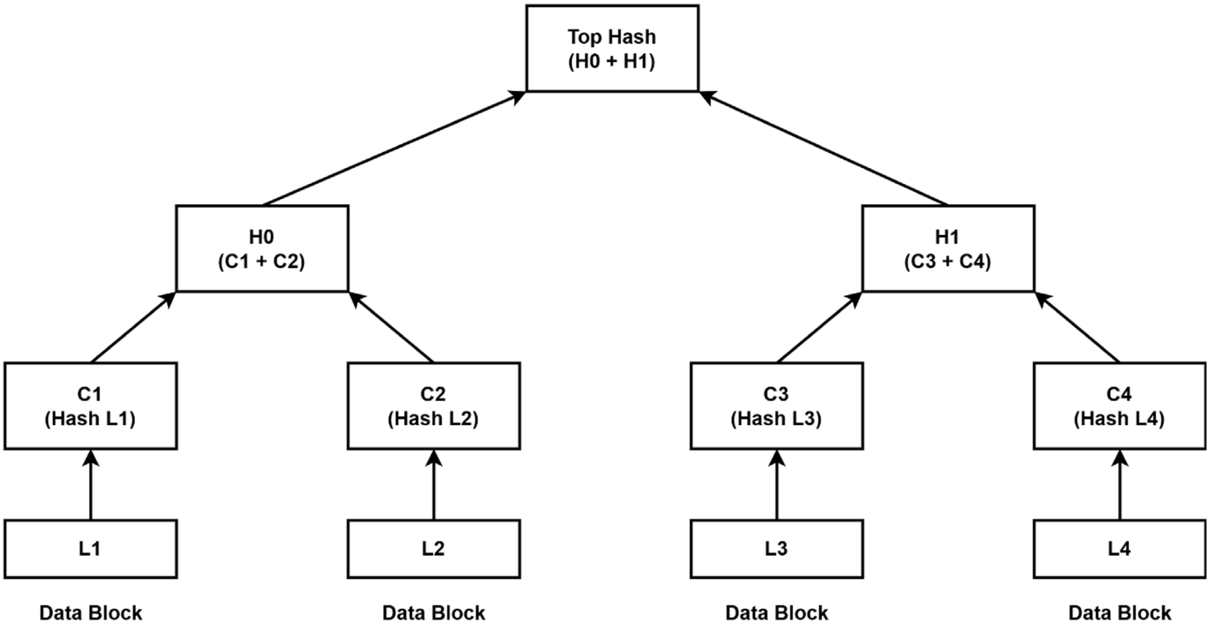


Fig. 2. Merkle tree illustration.

that generates a unique hash for each data block. Each leaf node in a Merkle tree contains the cryptographic hash of a data block, while each non-leaf node stores the hash of its child nodes, as illustrated in Fig. 2. Merkle trees (also referred to as hash trees) are widely used in cryptographic applications to securely summarise and verify large data structures. One key advantage is that verification requires only a logarithmic number of hash computations, rather than processing the entire dataset. This makes Merkle trees more efficient than hash lists, where the number of required hash operations increases proportionally with the dataset size.

Unlike traditional Merkle Trees, Merkle DAGs improve storage efficiency and data deduplication by allowing nodes to have multiple parents, making them particularly suited for handling redundant or shared pharmaceutical data. This structure enables efficient traceability by linking related transactions without unnecessary duplication while ensuring immutability. Additionally, Merkle DAGs allow for more flexible updates without requiring a full reconstruction of the tree, enhancing scalability and adaptability in complex supply chain environments.

4.3. Smart contract

A smart contract [33] is a self-executing piece of code deployed on the blockchain to perform specific tasks automatically when predefined internal or external conditions are met. Smart contracts offer a cost-effective and efficient method for establishing digital agreements between two parties, ensuring secure and automated execution without the need for intermediaries. These contracts contain a set of predefined rules agreed upon by both parties, and once the specified conditions are satisfied, the contract executes the corresponding actions. Running directly on the blockchain, smart contracts are tamper-proof, secure from misuse, and resistant to modification. Aligned with the cryptographic principles of blockchain technology, they eliminate the risks of manual errors or unauthorised alterations. Additionally, the outcomes generated by a smart contract are permanently recorded within a blockchain block, ensuring transparency, consistency, and verifiability. Solidity is the most widely used programming language for writing smart contracts. In the context of PharmChain, a new smart contract is deployed for each shipment, ensuring compliance with the various data requirements associated with pharmaceutical transactions. A basic illustration of this process is shown in Fig. 3.

4.4. Ethereum

Ethereum is a publicly distributed blockchain network that provides the necessary environment for running decentralised applications and smart contracts. Initially, Ethereum employed the Proof of Work (PoW) consensus mechanism, which required extensive computational power for transaction validation. However, Ethereum has transitioned to Proof of Stake (PoS), which enhances network scalability and reduces energy consumption while maintaining decentralisation and security.

In the PoS consensus model, validators are selected to propose and verify new blocks based on the amount of cryptocurrency they commit (or 'stake') to the network, rather than solving complex cryptographic puzzles. This shift significantly lowers computational costs and mitigates the environmental impact associated with traditional mining. For PharmChain, adopting Ethereum with PoS ensures energy efficiency, high transaction throughput, and reduced operational costs, making it a viable solution for supply chain management.

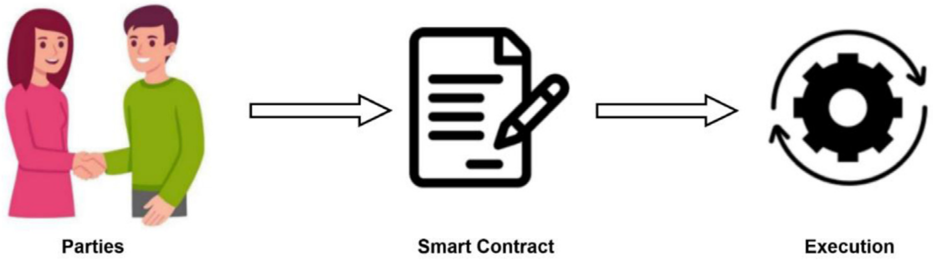


Fig. 3. Smart contract mechanism.

Ethereum supports over 1,900 tokens and coins, with 47 among the top 100 market-capitalised cryptocurrencies. The Ethereum Virtual Machine (EVM) enables smart contract execution in a decentralised environment, ensuring transparency and security. Unlike traditional centralised databases, Ethereum's immutable ledger guarantees that transactions recorded in the blockchain remain tamper-proof. Additionally, Ethereum integrates with Swarm, a decentralised storage solution that PharmChain utilises to store large volumes of off-chain data securely.

While various blockchain platforms could support PharmChain, Ethereum was chosen for its unique combination of scalability, decentralisation, interoperability, and security. Unlike Hyperledger, which operates as a permissioned blockchain suited for centralised enterprise systems, Ethereum's public and decentralised nature ensures trust among competing stakeholders. This feature is essential for cross-border pharmaceutical supply chains, where multiple independent entities (including manufacturers, regulators, and distributors) need to interact without relying on a central authority. Ethereum's transition to PoS has significantly improved its scalability and transaction throughput, making it better suited for handling high-volume pharmaceutical transactions. In contrast, Polkadot's parachain model, while promising for customised blockchain scalability, introduces additional complexity and requires specialised governance mechanisms, making it less practical for immediate deployment in pharmaceutical supply chains. Additionally, Ethereum supports widely adopted interoperability standards, including ERC-20 and ERC-721, which facilitate smooth integration with external regulatory databases, compliance frameworks, and pharmaceutical supply chain management platforms. While Polkadot offers cross-chain interaction capabilities, its ecosystem is still evolving, whereas Ethereum has an established, battle-tested infrastructure for enterprise adoption.

By utilising Ethereum's well-established network, security model, and developer ecosystem, PharmChain benefits from a robust, scalable, and widely compatible blockchain infrastructure, making it the optimal choice for securing and enhancing the pharmaceutical supply chain.

4.5. Swarm

Swarm is a decentralised peer-to-peer (P2P) network that provides infrastructure for distributed storage, message routing, and data processing. As a core component of Ethereum's ecosystem, Swarm functions as a cloud-native base layer for decentralised applications, offering secure and redundant storage for blockchain-related data. It enables participants to economically pool storage and bandwidth resources, ensuring the efficient and distributed delivery of digital services.

The Swarm network functions as an integral component of PharmChain, allowing for the secure storage of large pharmaceutical datasets such as drug packaging images, regulatory documents, and transaction records. Given the cost-prohibitive nature of storing large volumes of data directly on-chain, Swarm provides a scalable and cost-effective alternative. Data stored within Swarm is referenced on-chain through cryptographic hashes, ensuring verifiability without increasing blockchain storage requirements.

Swarm incorporates two primary incentive models: Bandwidth Incentives (rewarding nodes for relaying data efficiently across the network) and Storage Incentives (ensuring data persistence through financial compensation for storage providers). These incentives are essential for ensuring reliable decentralised data availability in a fully operational mainnet environment. However, the current implementation of PharmChain operates on the Swarm testnet, where an incentive model is not required, as data persistence is ensured through voluntary node participation. Additionally, redundant storage mechanisms and trusted nodes within the test environment enhance data reliability and availability, ensuring that pharmaceutical records remain accessible.

The Swarm client is implemented in Golang and stored in the Golang repository within the Ethereum Stack. While PharmChain currently utilises Swarm's testnet, it is important to note that uploaded content does not persist indefinitely until economic incentives and storage security mechanisms are fully established. As such, Swarm may not yet offer guaranteed long-term persistence in its testnet implementation; full production reliability will depend on the integration of the incentivised mainnet model. Moving forward, future iterations of PharmChain will explore integrating Swarm's incentivised mainnet, ensuring fully decentralised, long-term data persistence for real-world pharmaceutical supply chain applications.

5. PharmChain system architecture

When a factory manufactures a new product, it generates and assigns a unique cryptographic hash to the product. The product is then registered on the blockchain with a hash (unique ID). It becomes a digital network asset, and its hash is used to track it throughout the supply chain. Depending on the retailer's preference, additional product details may be stored either on-chain or off-chain. When referencing off-chain data on-chain, a specific identification mechanism (typically a cryptographic hash) links the on-chain record to its corresponding off-chain file. In most blockchain-based applications, off-chain data is typically hashed, and the corresponding hash is stored on-chain to ensure verifiability and integrity.

Once the manufacturer has registered the product on the blockchain, the ownership can be quickly transferred to another participant via a user-friendly mobile app. For instance, if a wholesaler purchases a drug from a seller, the physical transfer of the drug is accompanied by a blockchain transaction, ensuring real-time updates to the ledger. The wholesaler follows a similar process when transporting medications to a pharmaceutical business.

Fig. 4 illustrates this architecture and transaction flow across stakeholders. Events such as product dispatch, arrival, and delivery trigger smart contract transactions (TX) on-chain, while supporting files (e.g., packaging images or regulatory documents) are stored off-chain in Swarm for efficiency and traceability. The entities involved in the system are as follows.

Manufacturer

The manufacturer's role in the supply chain is to ensure that its stock is ready for sale to wholesalers. Manufacturers collect orders from

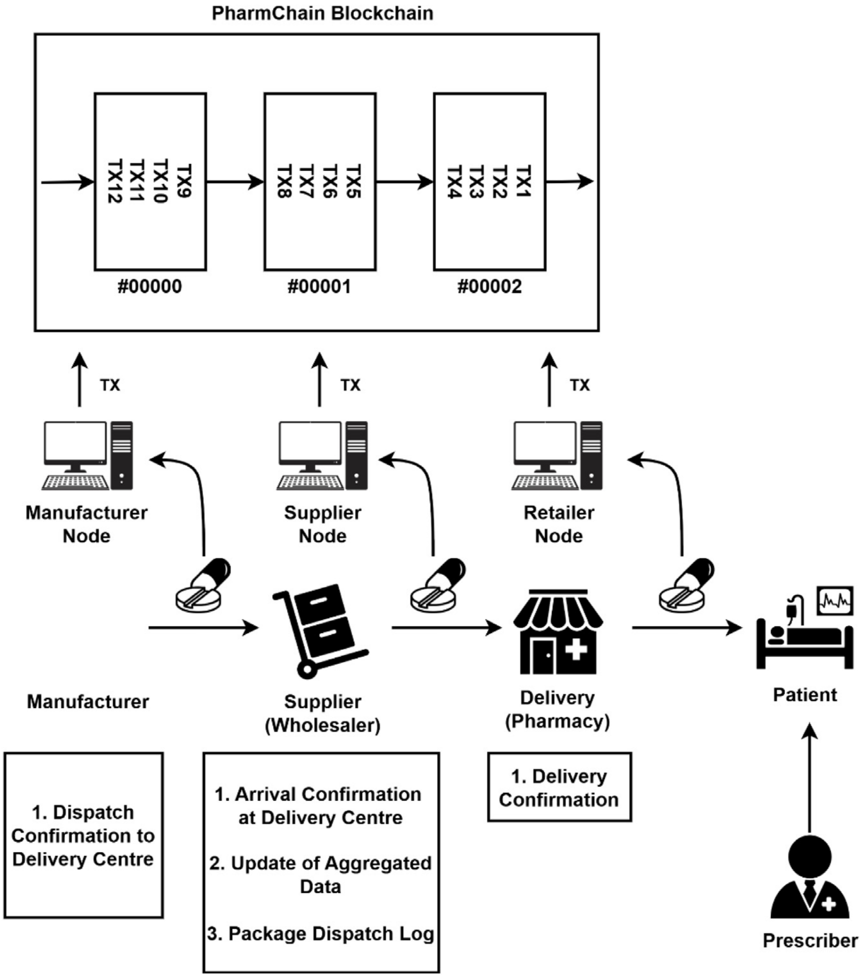


Fig. 4. PharmChain system architecture and basic flow.

distributors or buyers and dispatch the goods accordingly. Additionally, distributors issue inventory data reports to suppliers to maintain transparency and accountability within the system.

Wholesaler

Wholesalers are responsible for facilitating and optimising the process of purchasing pharmaceuticals. They serve thousands of pharmacies and dispensers, preventing manufacturers from directly exporting drugs to hospitals. Wholesalers can offer a variety of services, including drug delivery logistics, order processing and fulfilment, and inventory restocking.

Pharmacist

Pharmacies and hospitals are the final points of sale in the supply chain. About 75% of prescription drugs are sold through pharmacies, while the remaining 25% serve non-retail businesses, such as hospitals. Medicines are purchased from wholesalers and dispensed to patients.

The Working of the Swarm File System

Swarm is an integral component of PharmChain. It stores all photographs of drug packaging, purchasing quotes (PQ) from manufacturers, and other regulatory documents. Since storing large datasets directly on-chain can be extremely expensive, Swarm offers a cost-effective and scalable alternative for data storage. Swarm facilitates interaction between the blockchain network and front-end users, enabling the creation and modification of smart contracts, secure data storage and retrieval in the database, and efficient management of off-chain data. The Swarm network operates as a P2P system and utilises a data structure known as a Swarm object, which organises and links stored data within the network, as shown in Fig. 5. The data stored in Swarm is binary and unstructured, forming an array-based relationship. The protocol functions as follows:

- Each file stored in the network is assigned a unique cryptographic hash.
- Duplicate files do not exist on the network, ensuring data integrity and optimisation.
- Each network node stores both the actual data (content) and indexing information to facilitate efficient retrieval and verification.

Usage Scenario of the System

The information flow shown in Fig. 6 represents the basic structure of a blockchain-based pharmaceutical supply chain. The system involves multiple stakeholders, each with distinct responsibilities. The process begins with a Super Admin deploying the smart contract and having administrative control over system functionalities. The Super Admin then adds verified Admins, who register users (Manufacturers, Suppliers, and Retailers), enabling them to interact and conduct transactions. A Manufacturer produces a medicine and broadcasts the product details on the blockchain, along with a quotation for other users to review. Verified users can approve, reject, or request a requote, which the Manufacturer can update accordingly. If a Supplier approves the quotation, ownership transfers from the Manufacturer to the Supplier, and the Manufacturer ships the goods to the Supplier's delivery centre. The Supplier then broadcasts a medicine quotation for Retailers, allowing them to place an order upon approval. The Supplier transfers ownership to the Retailer using the "Sell" function and is responsible for shipping the product. The Retailer then updates the

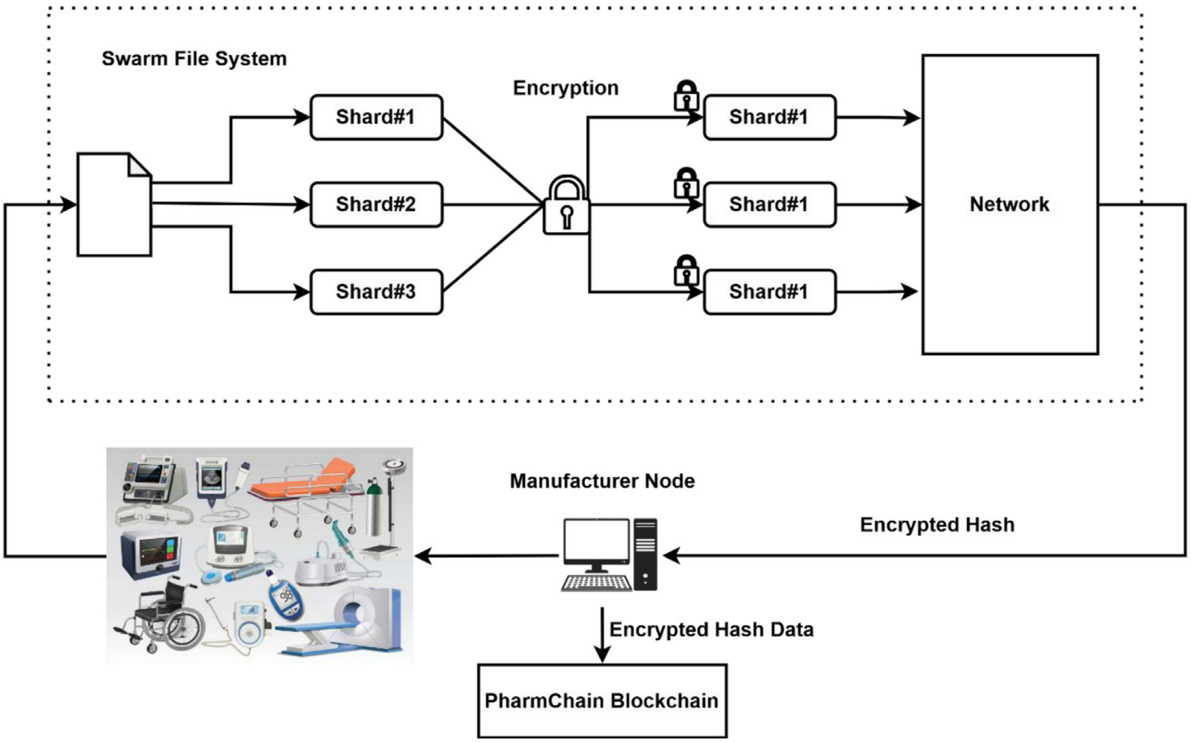


Fig. 5. Swarm file storage mechanism.

delivery confirmation on the blockchain. Finally, patients can purchase the medication from the Retailer, such as a pharmacy or hospital. The sequence flow of this process is depicted in Fig. 7.

Privacy and Data Confidentiality in PharmChain

PharmChain ensures privacy and data confidentiality through cryptographic techniques and selective data exposure. Rather than storing sensitive pharmaceutical data directly on the public ledger, only cryptographic references to off-chain encrypted data are recorded, ensuring that information remains secure yet verifiable. The system adopts a hybrid on-chain/off-chain storage model, where critical transaction metadata remains on-chain, while larger datasets, such as drug packaging images and regulatory documents, are securely stored off-chain using Swarm decentralised storage. This model prevents unnecessary blockchain bloat and excessive transaction costs while ensuring that sensitive pharmaceutical data is protected from unauthorised access. Furthermore, access control mechanisms within smart contracts enforce role-based permissions, ensuring that only authorised stakeholders, such as manufacturers, wholesalers, and regulators, can retrieve specific data. These measures collectively enable PharmChain to maintain both security and privacy while leveraging blockchain's transparency and immutability.

6. System implementation

This section provides a detailed description of the smart contract design and explains the roles and functionalities of each entity. Fig. 4 illustrates the user interaction methods and the system workflow. The back end of the system is implemented using NodeJS and web3.js. Web3.js is a JavaScript library that enables communication with the Ethereum blockchain. Using NodeJS, data is encrypted before being stored on the Ethereum Blockchain. Larger files are stored off-chain using Swarm and referenced via cryptographic hashes.

In Ethereum, a transaction is a communication between external entities and the Ethereum network. External users can use transactions to update records or modify stored information on the blockchain. The key elements of an Ethereum transaction are:

From : The message sender, identified by a 20-byte address.

To : The message recipient, also identified by a 20-byte address.

Value : The amount of Ether transferred from the sender to the recipient (measured in Wei).

Data (optional) : Includes an optional message or function call.

Gas : The computational fee required to process the transaction.

Gas Price : The cost per unit of gas, set by the sender.

Gas Limit : The maximum gas the sender is willing to pay for the transaction.

6.1. Transactions

Contract Deployment: Only the super administrator of the system can deploy a contract on the network. The Super Admin has exclusive permissions to appoint and approve other Admins in the system.

Rejection or Approval of Admins/ Users: The system supports three user roles: Manufacturer, Supplier (Wholesaler), and Retailer. Admins can create, approve, or reject users in the system (Algorithm 1).

Create Admin/ User: Creating an admin or user in the system is an Admin's functionality. An admin can also accept or reject Admin requests (Algorithm 2).

Rejection or Approval of Quotes/ Products: A quote is a digitally signed transaction request containing product details, price, and quantity, submitted by a user for approval on the blockchain. Quotes must be approved or rejected before processing.

Create Quote/ Product: Both Admins and Users can create quotes or add new products (Algorithm 3).

Requote: If a user rejects a quotation, the Manufacturer can update and resubmit the quote (Algorithm 4).

Sell to Retailer (Pharmacist): This function allows Suppliers to sell products to Retailers, who then distribute them to patients (Algorithm 5).

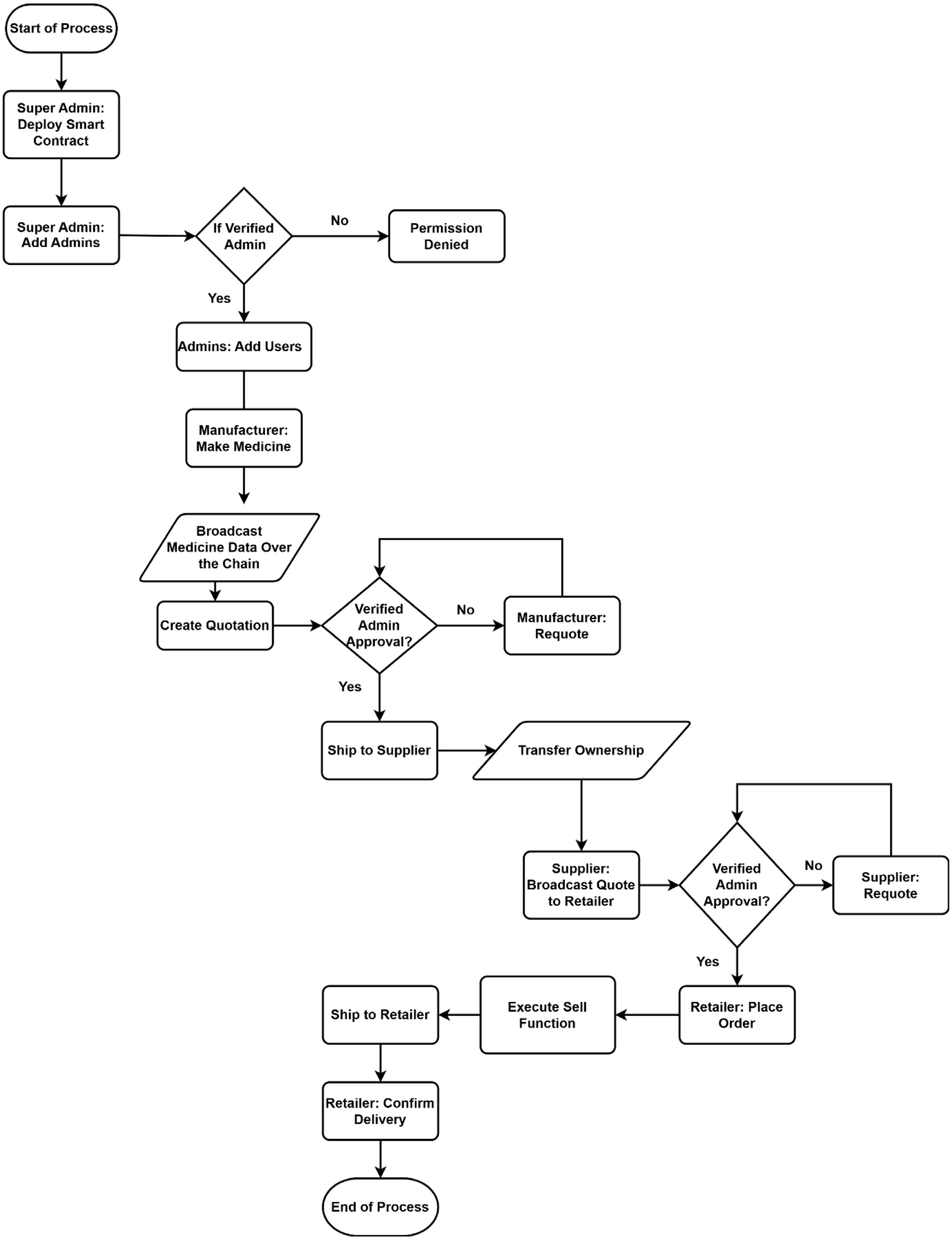


Fig. 6. Information flow in the PharmChain system.

7. System analysis

The implementation configuration requires an Intel(R) Core i7 5th Gen CPU @ 4.2 GHz, 8 GB RAM, a 64-bit operating system, and an x64-based processor. The smart contracts were written using Solidity, while the front-end graphical user interface was developed using Bootstrap 4.0 and JavaScript.

The system was implemented using the Truffle Framework [34], a development and testing environment for distributed applications (DApps). For smart contract deployment, we used Ganache, a pri-

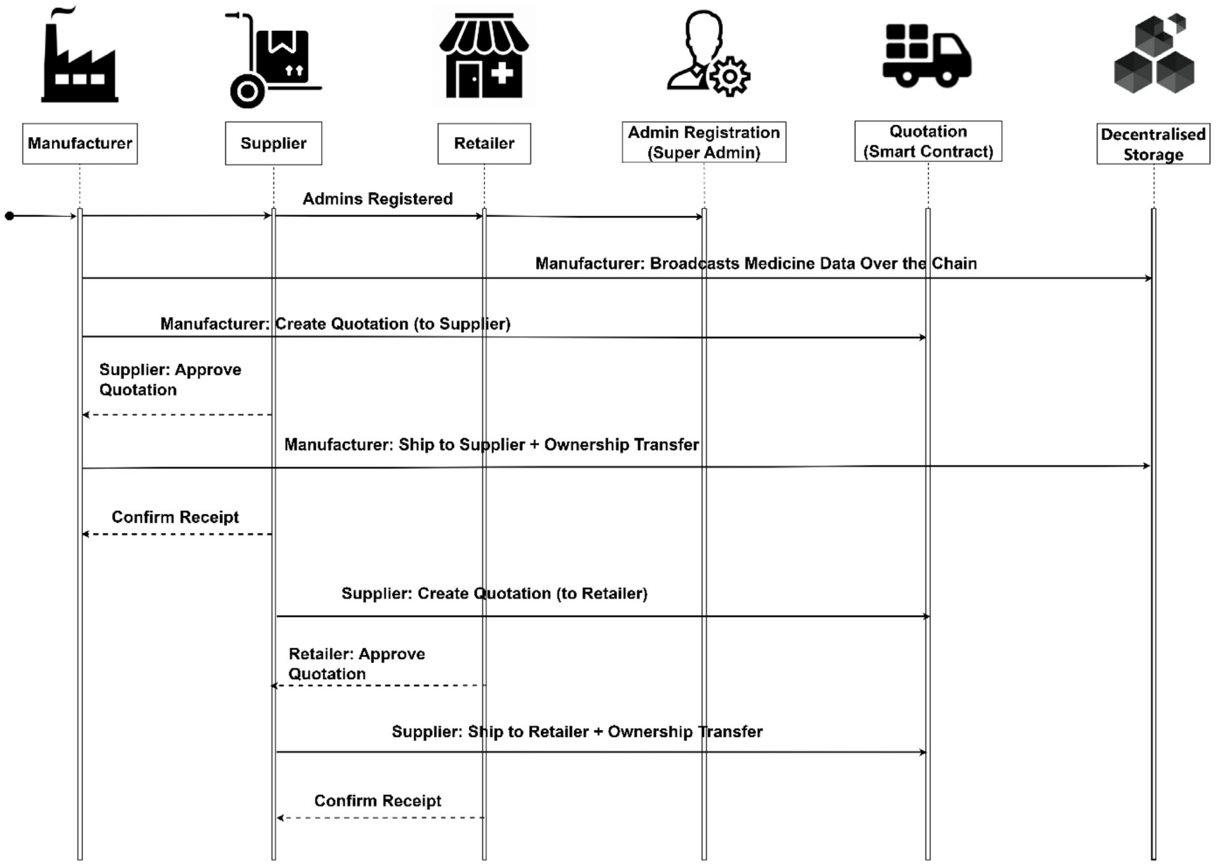

Manufacturer
Supplier
Retailer
Admin Registration (Super Admin)
Quotation (Smart Contract)
Decentralised Storage
Admins Registered
Manufacturer: Broadcasts Medicine Data Over the Chain
Manufacturer: Create Quotation (to Supplier)
Supplier: Approve Quotation
Manufacturer: Ship to Supplier + Ownership Transfer
Confirm Receipt
Supplier: Create Quotation (to Retailer)
Retailer: Approve Quotation
Supplier: Ship to Retailer + Ownership Transfer
Confirm Receipt

Fig. 7. Sequence diagram of the PharmChain system.

Algorithm 1: Approve Admin

Purpose: Authorises a new administrator and ensures no duplicates are added.

Input:

`newAdminAddress`: The address of the new admin to be approved.

Output:

`bool`: Returns `true` if the admin is successfully approved, otherwise `false`.

Procedure:

1. **Authorisation Check** (Role-Based Access Control):
   Use a modifier or `require` to ensure that `msg.sender` is a `SuperAdmin`. If not, terminate execution (`require(superAdmins[msg.sender], "Not a SuperAdmin");`).
2. **Duplicate Check** (Security with `require)`:
   Check if `newAdminAddress` is already in the `admins` list. If it is, revert with a message to prevent duplicate admins (`require(!admins[newAdminAddress], "Admin already exists");`).
3. **Add Admin (**State Modification):
   Add `newAdminAddress` to the `admins` list: `admins[newAdminAddress] = true;`.
4. **Event Emission (**Transparency):
   Emit an event `AdminApproved` to notify off-chain listeners of the new admin: `emit AdminApproved(newAdminAddress);`.
5. **Return Success**:
   Return `true` to indicate the operation was successful (`return true;`).

Algorithm 2: Add New Admin

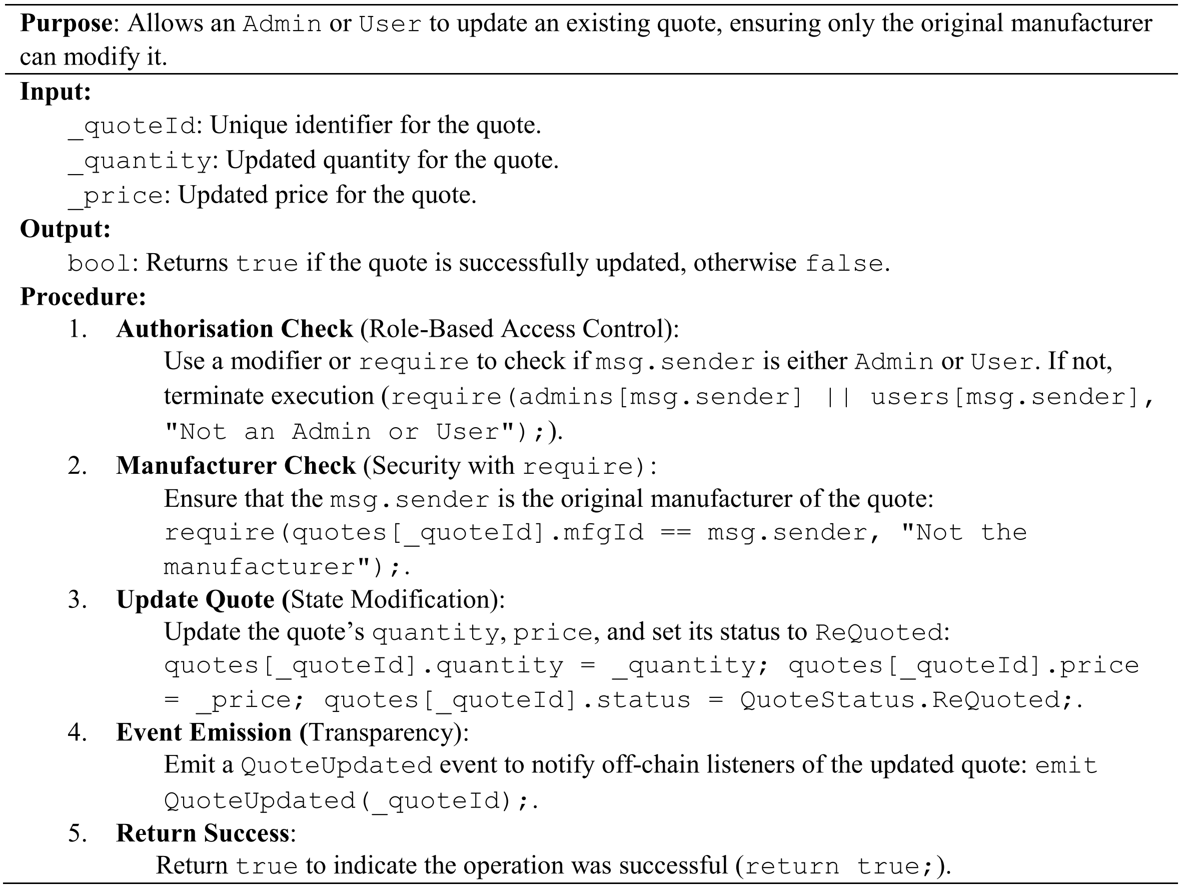
```
Purpose: Allows SuperAdmin or Admin to add a new administrator while preventing duplicates.
Input:
        newAdminAddress: The address of the new admin to be added.
Output:

        bool: Returns true if the admin is successfully added, otherwise false.
Procedure:
    1.  Authorisation Check (Role-Based Access Control):
            Use a modifier or require to ensure msg.sender is either a SuperAdmin or Admin. If
            not, terminate execution (require(admins[msg.sender] ||
            superAdmins[msg.sender], "Not an Admin or SuperAdmin");).
    2.  Duplicate Check (Security with require):
            Check if newAdminAddress already exists in admins. If it does, revert with a message
            (require(!admins[newAdminAddress], "Admin already exists");).
    3.  Add Admin (State Modification):
            Add newAdminAddress to the admins list: admins[newAdminAddress] =
        true;.
    4.  Event Emission (Transparency):
            Emit an event NewAdminAdded to notify off-chain listeners of the new admin addition:
            emit NewAdminAdded(newAdminAddress);.
    5.  Return Success:
            Return true to indicate the operation was successful (return true;).
```

Algorithm 3: Add Product

```
Purpose: Allows an Admin or User to add a new product, ensuring no duplicate products are added.
Input:
    _productid: Unique identifier for a product stored on-chain.
    _productName: Name of the product.
    _mfgdDate: Manufacturing date of the product.
    _swarmId: Reference to off-chain product data stored in Swarm.
Output:
    bool: Returns true if the product is successfully added, otherwise false.
Procedure:
    1.  Authorisation Check (Role-Based Access Control):
            Use a modifier or require to check if msg.sender is either an Admin or User. If not,
            terminate execution (require(admins[msg.sender] ||
            users[msg.sender], "Not an Admin or User");).
    2.  Duplicate Check (Security with require):
            Check if the product with _productid already exists in productVerfs. If it does,
            revert with a message (require(productVerfs[_productid].productId ==
            0, "Product already exists");).
    3.  Add Product (State Modification):
            Add the product to the productVerfs mapping, initialising its details, and setting the
            status to Pending.
    4.  Event Emission (Transparency):
            Emit a ProductAdded event to notify off-chain listeners of the new product addition:
            emit ProductAdded(_productid);.
    5.  Return Success:
            Return true to indicate the operation was successful (return true;).
```

Algorithm 4: Requote



Purpose: Allows an `Admin` or `User` to update an existing quote, ensuring only the original manufacturer can modify it.

Input:

`_quoteId`: Unique identifier for the quote.
`_quantity`: Updated quantity for the quote.
`_price`: Updated price for the quote.

Output:

`bool`: Returns `true` if the quote is successfully updated, otherwise `false`.

Procedure:

1. **Authorisation Check** (Role-Based Access Control):
   Use a modifier or `require` to check if `msg.sender` is either `Admin` or `User`. If not, terminate execution (`require(admins[msg.sender] || users[msg.sender], "Not an Admin or User");`).
2. **Manufacturer Check** (Security with `require)`:
   Ensure that the `msg.sender` is the original manufacturer of the quote: `require(quotes[_quoteId].mfgId == msg.sender, "Not the manufacturer");.`
3. **Update Quote (**State Modification):
   Update the quote's `quantity`, `price`, and set its status to `ReQuoted`: `quotes[_quoteId].quantity = _quantity; quotes[_quoteId].price = _price; quotes[_quoteId].status = QuoteStatus.ReQuoted;.`
4. **Event Emission (**Transparency):
   Emit a `QuoteUpdated` event to notify off-chain listeners of the updated quote: `emit QuoteUpdated(_quoteId);.`
5. **Return Success**:
   Return `true` to indicate the operation was successful (`return true;`).

vate Ethereum blockchain that allows local testing before deployment on a public network. Ganache provides multiple pre-funded accounts with virtual Ether, enabling the execution of test transactions [35]. To facilitate Ethereum node interactions, we used MetaMask (n/a), a browser extension that provides a secure interface for connecting to the Ethereum blockchain and executing transactions within a decentralised network.

7.1. Experiments and results

To evaluate the performance and cost-effectiveness of the PharmChain system, we tested it under three representative operational scenarios. Each scenario corresponds to specific smart contract algorithms described in Section 6.1 and reflects a typical transaction process within the pharmaceutical supply chain.

Scenario 1 (User and Product Creation): This scenario involves the execution of smart contract functions for creating users (Admins, Manufacturers, Suppliers, Retailers) and for adding new products to the blockchain. These actions correspond to Algorithms 1, 2, and 3 outlined in Section 6.1.

Scenario 2 (Quotation and Requote Management): This scenario addresses the generation of quotes and the handling of quote rejections and requotes. It reflects the workflow defined in Algorithm 4, where Manufacturers can modify and resubmit rejected quotes.

Scenario 3 (Approval, Rejection, and Final Transactions): The final scenario evaluates the processes of approving or rejecting users, products, and quotes, as well as completing transactions from Supplier to Retailer. These actions correspond to Algorithm 5 and illustrate the full transaction lifecycle, from initial registration to product delivery.

7.1.1. Performance evaluation of transactions

Every Ethereum transaction contains a payload of data, which consumes gas for execution. This data payload is embedded in transactions that invoke smart contract functions. The gas price determines transaction speed; higher gas costs result in faster transaction processing and vice versa.

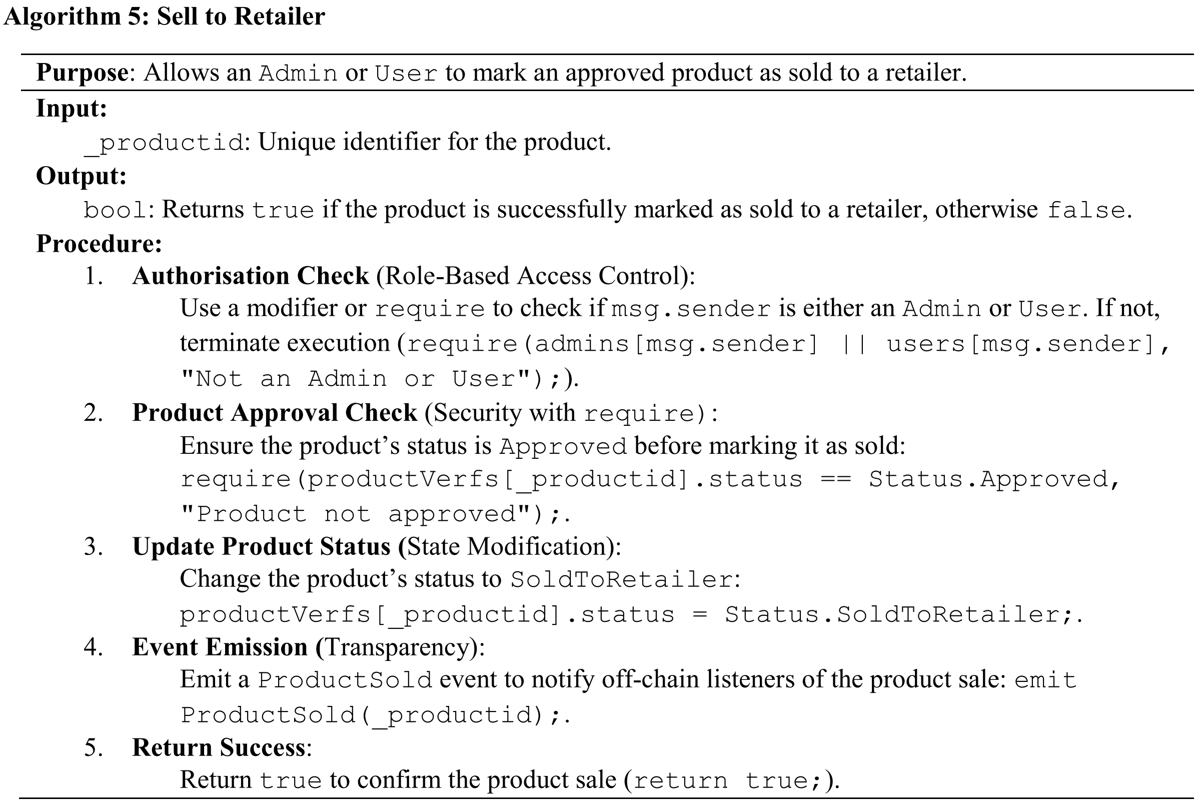
At the time of implementation, the gas price was 50 Gwei, but for the purpose of analysis, we assigned a constant value of 10 Gwei for smart contract deployment. In the Ethereum network, gas prices play a crucial role in determining transaction priority. The higher the gas price, the sooner the transaction is included in the block. By fixing the gas price at 10 Gwei, transactions were ensured to be processed within a maximum of 15 min.

For cost evaluation, we assume the value of 1 Ether to be $380, with the Gas required for Contract Deployment set at 0.0616067 ETH. Then, the Ether Cost is computed as Gas Usage * Gas Price/ 1,000,000,000. To analyse cost fluctuations, functions are categorised into three groups: Mfg (Manufacturer), Sup (Supplier/Wholesaler), and Ret (Retailer/Pharmacy/Hospital). The following tables compare creation, rejection, and approval costs for various functions.

Table 3 illustrates gas consumption and cost for different creation functions. The Requote function is included as it also involves the creation of a new quotation when an earlier one is rejected.

Table 4 compares the gas usage and cost for various rejection functions in Ether and dollars.

Table 5 presents gas usage and cost for approval functions, which facilitate user approvals, quotation approvals, and product confirmations. Additionally, to reduce on-chain gas costs, PharmChain leverages off-chain storage using Swarm. Large files such as drug packaging images and regulatory documents are stored in Swarm, while only



Algorithm 5: Sell to Retailer

```
Purpose: Allows an Admin or User to mark an approved product as sold to a retailer.
Input:
    _productid: Unique identifier for the product.
Output:
    bool: Returns true if the product is successfully marked as sold to a retailer, otherwise false.
Procedure:
    1. Authorisation Check (Role-Based Access Control):
           Use a modifier or require to check if msg.sender is either an Admin or User. If not,
           terminate execution (require(admins[msg.sender] || users[msg.sender],
           "Not an Admin or User");).
    2. Product Approval Check (Security with require):
           Ensure the product's status is Approved before marking it as sold:
           require(productVerfs[_productid].status == Status.Approved,
           "Product not approved");.
    3. Update Product Status (State Modification):
           Change the product's status to SoldToRetailer:
           productVerfs[_productid].status = Status.SoldToRetailer;.
    4. Event Emission (Transparency):
           Emit a ProductSold event to notify off-chain listeners of the product sale: emit
           ProductSold(_productid);.
    5. Return Success:
           Return true to confirm the product sale (return true;).
```

Table 3
Creation function costs on different parameters.

Function	Gas	Cost (ETH)	Cost ($)
Create Admin	111 125	0.0011113	0.422294
Create User: Mfg	135 531	0.0013553	0.515014
Create User: Sup	135 430	0.0013543	0.514634
Create User: Ret	136 930	0.0013693	0.520334
Create Product	111 638	0.0011164	0.424232
Create Quote	215 441	0.0021544	0.818672
Requote	41 221	0.0004122	0.156636

Table 4
Rejection function costs on different parameters.

Function	Gas	Cost (ETH)	Cost ($)
Reject Admin	30 970	0.0003097	0.117686
Reject User: Mfg	30 638	0.0003064	0.116432
Reject User: Sup	30 637	0.0003064	0.116432
Reject User: Ret	30 715	0.0003072	0.116736
Reject Product	29 816	0.0002982	0.113316
Reject Quote	29 794	0.0002979	0.113202

Table 5
Approval function costs on different parameters.

Function	Gas	Cost (ETH)	Cost ($)
Approve Admin	30 904	0.0003090	0.117420
Approve User: Mfg	30 638	0.0003064	0.116432
Approve User: Sup	30 595	0.0003059	0.116242
Approve User: Ret	30 600	0.0003060	0.116280
Approve Product	29 795	0.0002980	0.113240
Approve Quote	29 793	0.0002979	0.113202
SelltoRetailer	29 774	0.0002977	0.113126

their cryptographic hashes are recorded on-chain. This hybrid model significantly reduces gas consumption and improves scalability.

Fig. 8 compares the costs of different system functions. It is evident that creation functions involve significantly higher gas costs than rejection and approval functions. However, once a user is registered and granted permissions, the cost of subsequent operations is low and manageable.

7.1.2. Performance assessment

Average Latency

Latency refers to the delay or time difference between when a request is sent by one system component and when another system component produces a response. It is measured as the time difference between these two actions. Using JMeter, we evaluated the average latency of the proposed system, as shown in Fig. 9. JMeter was used to simulate multiple users during the latency testing phase. In JMeter, latency is measured in milliseconds.

7.2. Discussion and analysis

The pharmaceutical industry requires a modernised supply chain structure to address the issues discussed in Section 1. The proposed PharmChain framework leverages blockchain technology to enhance drug traceability and supply chain security. In situations where both privacy and data access are needed simultaneously, blockchain technology offers the best solution. By registering each transaction on the blockchain, a permanent product history is created, ensuring that every time a product changes hands, the transaction is recorded from production to final sale. Over time, this will significantly reduce costs and minimise human errors in transactions. The key characteristics and benefits of the SCM framework using blockchain in the pharmaceutical industry are summarised in Table 6:

Accountability: Producers and customers can track pharmaceutical products throughout the supply chain, building trust between them. Manufacturers must ensure that only authorised customers access the

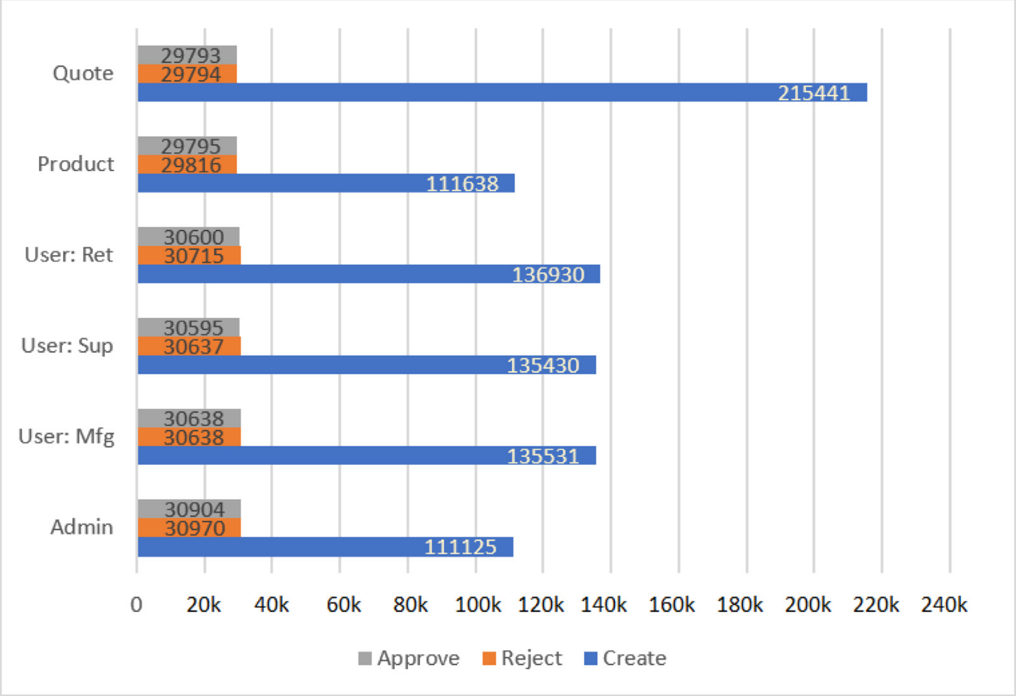


Fig. 8. Gas usage comparison for create, reject, and approve functions.

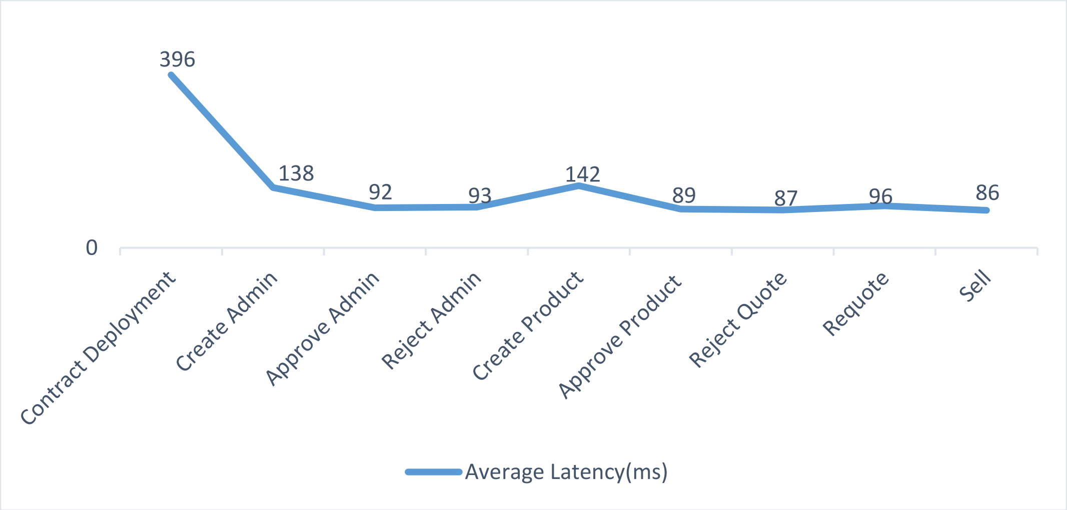


Fig. 9. Average latency comparison for different operations.

products they produce, while customers must be able to verify the authenticity of medicines before purchase.

Traceability: Once a product is manufactured, it is recorded and authenticated on the blockchain. As ownership changes hands, the ownership transfer is simultaneously updated on the blockchain network. Drug producers, manufacturers, suppliers, and distributors can track products at any stage in real time.

Credibility: Blockchain ensures that publicly available data is genuine and verifiable, while protecting private and sensitive information. Pharmaceutical products can be authenticated within a supply chain environment without exposing proprietary manufacturing techniques. Similarly, patients' medical records can be accessed by different stakeholders without revealing personal information.

Extended Safety: Blockchain is one of the most secure ledger networks in the world. The information stored on the blockchain is immutable, meaning it cannot be removed or modified. The PharmChain framework builds on the public Ethereum blockchain while implementing access-controlled smart contracts and off-chain data references. This ensures high security and trust among authorised participants without sacrificing decentralisation. The enhanced security model provides high-precision solutions while facilitating secure communication between users, vendors, regulatory bodies, and industry stakeholders.

Decentralisation: Blockchain's decentralised nature eliminates the need for a central database to secure user transactions. With multiple copies of transactions distributed across the network, there is no single point of failure. For any modification to occur, an attacker would

Table 6
Comparison with related works.

Factors	Acc	Tra	Cre	ES	Dec
O'Hagan and Garlington [18]	No	No	No	Yes	No
Xia et al. [20]	Yes	No	No	Yes	Yes
Huang et al. [22]	No	Yes	Yes	No	Yes
Shahid et al. [24]	Yes	Yes	Yes	No	Yes
Yousefi and Tosarkani [26]	Yes	Yes	No	No	Yes
Beaulieu et al. [27]	No	Yes	Yes	No	Yes
Benevento et al. [28]	Yes	Yes	No	No	Yes
PharmChain	Yes	Yes	Yes	Yes	Yes

Note: Acc = Accountability, Tra = Traceability, Cre = Credibility, ES = Extended Safety, and Dec = Decentralisation.

need to simultaneously alter all copies and bypass consensus protocols, making fraudulent activities extremely difficult.

8. Managerial implications

The adoption of a blockchain-based secure system for tracking pharmaceutical supply chains has significant managerial implications for pharmaceutical companies. This system ensures both authenticity and privacy in drug traceability, addressing key challenges in the pharmaceutical industry. PharmChain provides a practical and innovative solution by leveraging blockchain technology to restructure the service infrastructure into three key components: enhancing transparency, ensuring authenticity, and strengthening security across the drug traceability process. The Ethereum-based blockchain guarantees the immutability of transactions, while access to critical traceability information is restricted to trusted parties, safeguarding sensitive pharmaceutical data from unauthorised access and tampering.

This paper demonstrates the viability of the proposed solution through the implementation and testing of smart contract code in the Remix environment. Additionally, comprehensive cost and security analyses have been conducted for various supply chain stakeholders, providing valuable insights into the feasibility, effectiveness, and economic impact of implementing PharmChain. The managerial relevance of this study lies in its potential to revolutionise pharmaceutical supply chain management. By addressing counterfeit drug infiltration, improving traceability, and enhancing supply chain security, PharmChain offers a practical, scalable, and cost-effective solution. This has far-reaching benefits for patient safety, regulatory compliance, and the overall integrity of the pharmaceutical industry.

In conclusion, the adoption of PharmChain as a blockchain-based pharmaceutical supply chain tracking system holds significant promise for managerial practice in the pharmaceutical industry. By enhancing security, transparency, regulatory compliance, and operational efficiency, PharmChain empowers pharmaceutical managers to address industry challenges effectively, ultimately leading to improved patient safety, reduced risks, and enhanced operational excellence.

9. Conclusions

PharmChain is developed as a response to the widespread issue of counterfeit drugs within the pharmaceutical supply chain. By leveraging the Ethereum blockchain and the decentralised storage platform Swarm, PharmChain enhances traceability, transparency, and data integrity across all supply chain stages. To conclude, we summarise the key contributions, limitations, and future directions of this work:

Key Contributions: This study proposes PharmChain, a blockchain-based framework designed to improve drug traceability and regulatory compliance through secure, decentralised transaction tracking. The system utilises Ethereum smart contracts to automate processes and maintain data integrity, while integrating Swarm to address the limitations of on-chain data storage. The framework was implemented and validated in the Remix development environment, confirming both its functional viability and deployment feasibility. Additionally, comparative analysis with traditional and existing blockchain models demonstrates PharmChain's advantages in terms of performance, cost-effectiveness, and security.

Limitations: Despite its strengths, PharmChain has some limitations. It does not currently incorporate Layer 2 scalability solutions such as Optimism or Arbitrum, which may limit performance under high transaction volumes. Furthermore, while the system supports strong traceability in domestic contexts, integration with cross-border and multi-jurisdictional regulatory frameworks remains an open challenge.

Future Work: Future development will focus on enhancing system scalability and interoperability. Planned extensions include incorporating agent-based simulations to test system resilience in complex, real-world scenarios such as drug recalls and regulatory audits. We also intend to explore cross-chain interoperability to facilitate compliance and collaboration across national boundaries. To further strengthen data privacy while maintaining verifiability, we aim to implement advanced privacy-preserving techniques such as Zero-Knowledge Proofs (ZKPs), homomorphic encryption, and differential privacy.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to thank the Editor-in-Chief, the Associate Editor, and the anonymous reviewers for their valuable feedback on the previous version of this manuscript.

Data availability

Data will be made available on request.

References

[1] A. Ghadge, M. Bourlakis, S. Kamble, S. Seuring, Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework, Int. J. Prod. Res. 61 (19) (2023) 6633–6651.

[2] H. Malik, T. Anees, M. Faheem, M.U. Chaudhry, A. Ali, M.N. Asghar, Blockchain and internet of things in smart cities and drug supply management: Open issues, opportunities, and future directions, Internet Things 23 (2023) 100860.

[3] C. Yang, S. Lan, Z. Zhao, M. Zhang, W. Wu, G.Q. Huang, Edge-cloud blockchain and IoE-enabled quality management platform for perishable supply chain logistics, IEEE Internet Things J. 10 (4) (2023) 3264–3275.

[4] World Health Organisation, 1 in 10 Medical Products in Developing Countries Is Substandard or Falsified: WHO Urges Governments to Take Action, World Health Organisation, Geneva, Switzerland, 2017, Available online at http://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.

[5] World Health Organisation, A Study on the Public Health and Socioeconomic Impact of Substandard and Falsified Medical Products, World Health Organisation, Geneva, Switzerland, 2020, Available online at https://www.who.int/publications/i/item/9789241513432.

[6] M. Gaynor, K. Gillespie, A. Roe, E. Crannage, J.E. Tuttle-Newhall, Blockchain applications in the pharmaceutical industry, Blockchain Heal. Today 7 (1) (2024) 1–10.

[7] S. Abdallah, N. Nizamuddin, Blockchain-based solution for pharma supply chain industry, Comput. Ind. Eng. 177 (2023) 108997.

[8] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, Available at https://bitcoin.org/bitcoin.pdf.

[9] V. Charles, A. Emrouznejad, T. Gherman, A critical analysis of the integration of blockchain and artificial intelligence for supply chain, Ann. Oper. Res. 327 (2023) 7–47.

[10] A. Emrouznejad, V. Charles, Big Data and Blockchain for Service Operations Management, Springer, Cham, 2022.

[11] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management, Int. J. Prod. Res. 57 (7) (2019) 2117–2135.

[12] A.S. Yadav, V. Charles, D.K. Pandey, S. Gupta, T. Gherman, D.S. Kushwaha, Blockchain-based secure privacy-preserving vehicle accident and insurance registration, Expert Syst. Appl. 230 (2023) 120651.

[13] G. Tripathi, M.A. Ahad, G. Casalino, A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges, Decis. Anal. J. 9 (2023) 100344.

[14] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P.N. Bokoro, R. Sharma, Blockchain technology for secure supply chain management: A comprehensive review, IEEE Access 10 (2022) 85493–85517.

[15] W.A.H. Ahmed, B.L. MacCarthy, Blockchain-enabled supply chain traceability – How wide? How deep? Int. J. Prod. Econ. 263 (2023) 108963.

[16] D. Biswas, H. Jalali, A.H. Ansaripoor, P. De Giovanni, Traceability vs. sustainability in supply chains: The implications of blockchain, Eur. J. Oper. Res. 305 (1) (2023) 128–147.

[17] A.K. Yadav, Shweta, D. Kumar, Blockchain technology and vaccine supply chain: Exploration and analysis of the adoption barriers in the Indian context, Int. J. Prod. Econ. 255 (2023) 108716.

[18] A. O'Hagan, A. Garlington, Counterfeit drugs and the online pharmaceutical trade, a threat to public safety, Forensic Res. Criminol. Int. J. 6 (3) (2018) 151–158.

[19] M. Mettler, Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), IEEE, Munich, Germany, 2016, pp. 1–3.

[20] Q.I. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: Trustless medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.

[21] E.C. Cheng, Y. Le, J. Zhou, Y. Lu, Healthcare services across China–on implementing an extensible universally unique patient identifier system, Int. J. Heal. Manag. 11 (3) (2018) 210–216.

[22] Y. Huang, J. Wu, C. Long, Drugledger: A practical blockchain system for drug traceability and regulation, in: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, IEEE, Halifax, Canada, 2018, pp. 1137–1144.

[23] I. Haq, O.M. Esuka, Blockchain technology in pharmaceutical industry to prevent counterfeit drugs, Int. J. Comput. Appl. 180 (25) (2018) 8–12.

[24] A. Shahid, A. Almogren, N. Javaid, F.A. Al-Zahrani, M. Zuair, M. Alam, Blockchain-based agri-food supply chain: A complete solution, IEEE Access 8 (2020) 69230–69243.

[25] H.R. Hasan, K. Salah, R. Jayaraman, R.W. Ahmad, I. Yaqoob, M. Omar, Blockchain-based solution for the traceability of spare parts in manufacturing, IEEE Access 8 (2020) 100308-100322.

[26] S. Yousefi, B.M. Tosarkani, Exploring the role of blockchain technology in improving sustainable supply chain performance: A system-analysis-based approach, IEEE Trans. Eng. Manage. (2023) 1–17.

[27] M. Beaulieu, O. Bentahar, S. Benzidia, A. Gunasekaran, Digitalization initiatives of home care medical supply chain: A case-study-based approach, IEEE Trans. Eng. Manage. (2023) 1–14.

[28] E. Benevento, A. Stefanini, D. Aloini, R. Dulmin, V. Mininno, Beyond digital technologies: Investigating the barriers to supply chain integration of healthcare organizations, IEEE Trans. Eng. Manage. (2023) 1–13.

[29] M.M.N.H.K. Kholaif, M. Xiao, X. Tang, Opportunities presented by COVID-19 for healthcare green supply chain management and sustainability performance: The moderating effect of social media usage, IEEE Trans. Eng. Manage. (2023) 1–14.

[30] S. Mondal, K.P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, P. Chahal, Blockchain inspired RFID-based information architecture for food supply chain, IEEE Internet Things J. 6 (3) (2019) 5803–5813.

[31] P. Behner, M.-L. Hecht, F. Wahl, Fighting counterfeit pharmaceuticals. New defenses for an underestimated – and growing – menace, Strategy (2017) 1–24, [Online]. Retrieved from https://www.strategyand.pwc.com/gx/en/insights/2017/fighting-counterfeit-pharmaceuticals/fighting-counterfeit-pharmaceuticals.pdf.

[32] S. Dechand, A. Naiakshina, A. Danilova, M. Smith, In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception, in: 4th IEEE European Symposium on Security and Privacy (EuroS & P 2019), IEEE, Stockholm, Sweden, 2019, pp. 401–415.

[33] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, in: Ethereum Project Yellow Paper, vol. 151, 2014, pp. 1–32, Available online at https://ethereum.github.io/yellowpaper/paper.pdf.

[34] trufflesuite.com. (2019) [online] Available: https://www.trufflesuite.com/truffle..

[35] W.M. Lee, Testing smart contracts using ganache, in: W.M. Lee (Ed.), Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript, A Press, Berkeley, CA, 2019, pp. 147–167.