Research article

PharmaChain: Blockchain-based drug supply chain provenance verification system

Sarmistha Sarna Gomasta [a,*], Aditi Dhali [a], Tahlil Tahlil [b], Md. Musfique Anwar [a], A.B. M Shawkat Ali [c]

[a] *Department of Computer Science and Engineering, Jahangirnagar University, Bangladesh*
[b] *Institute of information technology, University of Dhaka, Bangladesh*
[c] *JU Data Mining Research Lab, Dhaka, Bangladesh*

ARTICLE INFO

ABSTRACT

Over the last decade, pharmaceutical businesses have battled to standardize product traceability across the supply chain process, enabling counterfeiters to enter the market with counterfeit pharmaceuticals. As a result, an end-to-end product tracking system is crucial for ensuring product safety and eliminating counterfeit products across the pharmaceutical supply chain. In this paper, we introduce PharmaChain, a decentralized hyperledger fabric framework that leverages confidentiality, accountability, and interoperability. This system enables on-chain and off-chain storage for secured, rapid transactions, along with smart contracts establishing data provenance. To demonstrate security, we have provided double signing through the elliptic curve digital signature algorithm, hash data encryption, and 33% node attack. The purpose of this suggested framework is to engage particular governance disciplines to assess its effectiveness in improving drug traceability across the pharmaceutical supply chain to preserve public health by preventing counterfeit pharmaceuticals.

1. Introduction

The main aim of pharmaceutical companies is to maintain their distribution to improve the quality of various channels and protect patients from faults or malfunctions that arise during repackaging or relabeling. The pharmaceutical supply chain involves multiple stakeholders, including manufacturers, wholesale distributors, and pharmacy managers, and encompasses clinical research, development, manufacturing, distribution, and a wide range of healthcare services. Due to the intense scrutiny from authorities, industry, and consumers, the pharmaceutical and healthcare industries are highly complicated. Not only does this complexity result in cold-chain shipping, increased prescription drug prices, and supply shortages, but it also exacerbates the challenge of reducing counterfeit drugs. Pharmaceutical items that have been purposefully and fraudulently manufactured and mislabeled concerning the identity and source such that they appear genuine are known as counterfeit pharmaceuticals [1]. Counterfeit medications may also be manufactured under inadequate standards and with inappropriate formulations, including insufficient or no active pharmaceutical ingredient (API), contaminants, or repackaged expired drugs [2].

Due to the growing variety of medications and advancements in technology, new pharmaceuticals are being introduced onto the market under various names, increasing the likelihood of drug counterfeiting. According to estimates, the pharmaceutical industry in the United States suffers an estimated yearly loss of around $82.0 billion and $353.3 billion causing around three million job vacancies due to medicine counterfeiting [3]. About 30% fraudulent pharmaceuticals are suppressed by underdeveloped nations [4,5] which leads to tens of thousands of deaths annually, with a disproportionate number of casualties being children. Bangladesh, surprisingly, controls approximately 70.9% of generic medications marketed in the world's 48 developing countries [6]. As a source of concern, the drug regulator authorities estimate over 70,000 illegal drugstores in Bangladesh [7]. Pharmaceutical companies estimate that counterfeit medicines worth 600 crores of Bangladeshi Taka (BDT) are traded each year, resulting in a significant loss for the country's medicine market [8]. The pandemic of COVID-19 has exposed a lack of coordination, and equal access to personal protective equipment throughout the world, including Bangladesh [9].

To ensure the safety of people's health, many healthcare organizations emphasize drug traceability to prevent drug counterfeiting using cutting-edge technologies. The Drug Supply Chain Security Act (DSCSA) mandates that the pharmaceutical industry develop an electronic and extensible system for detecting and tracking prescription medications as they are delivered across the U.S. [10]. Similarly, China has enforced that all stakeholders contribute to tracking individual details in the medicine supply chain whenever pharmaceutical items are stored in a specific Internet Technology (IT) system and inventory transaction [11]. However, the most difficult challenge is establishing a national standard for deploying and serializing pharmaceutical track and trace technologies. For example, the Food and Drug Administration (FDA) has urged the healthcare sector to establish a uniform framework for identifying and tracing all pharmaceuticals [12]. According to an analysis of the current 250 healthcare vendors, the worldwide market is predicted to exceed $500 million by 2022, and health insurance or pharmaceutical businesses are among the first to engage in industrial market collaboration with cutting-edge technology [13]. Since internet technology has spawned another ground-breaking evolution known as the blockchain, many healthcare businesses have adopted the blockchain for decentralization, transparency, and anonymization, as well as interoperability [14]. Blockchain provides a self-cryptographic verification structure among transactions (by hashes) and the public availability of a peer-to-peer database of transaction records. The creation of a chain of blocks linked by cryptographic concepts (hashes) makes tampering with the records extremely difficult, as it would require modification from the genesis block to the most recent transaction in blocks [15].

This manuscript presents an end-to-end solution for secure drug supply chain management based on Hyperledger fabric to monitor and track the distribution process to prevent drug counterfeiting. Our proposed approach, PharmaChain, in particular, leverages cryptographic fundamentals to create tamper-proof logs of supply chain events and smart contracts to automate the recording of events. To commence, we identify and involve key stakeholders in the pharmaceutical supply chain of Bangladesh, such as the Directorate General of Drug Administration (DGDA), hospitals, manufacturers, transporters, central distributors, etc. Secondly, we concertedly identify and describe interactions between stakeholders, on-chain and off-chain resources, intelligent contracts, and decentralized storage systems. We also leverage smart contract technology to execute real-time, seamless drug tracking with push alerts, reducing the need for human interaction and, as a result, unnecessary delays. To guarantee successful network operations, incentives, compliance, and support services with related risks and security costs, we have established three categories: network membership, technological infrastructure, and business network level of governance. Finally, we included a security analysis in determining the effectiveness of the provided approach. As a consequence, the following provides an overview of our contributions:

- We develop a novel architectural design for Bangladesh's pharmaceutical supply chain based on a hyperledger fabric that guarantees security, traceability, immutability, and accessibility of data provenance.
- We ensure off-chain and on-chain mechanisms for storage allocation and specify read-write control access.
- We create a smart contract that deals with various transactions between parties in the pharmaceutical supply chain.
- Using the hash algorithms and elliptic curve digital signature algorithm, we introduce a three-step security analysis for security concerns.
- To assess the efficacy of the suggested blockchain-based solution, we conduct a risk and cost analysis.
- To guarantee optimal network operations, incentives, compliance, and support services, we have established three governance categories.

The remaining paper is structured as follows: Section 2 represents a literature overview of different approaches to resolving the problem of drug counterfeiting. Section 3 describes the product flow of Bangladesh's existing system and the methodology of our proposed solution. Section 4 details the technical architecture, data architecture, smart contract, and three modules of governance to represent our drug traceability system properly. Section 5 and Section 6 include security methods to evaluate the system and discussion of value generation and security analysis of PharmaChain, respectively. We conclude this research article with future directions in Section 7.

2. Literature review for drug counterfeit

Health information technology (HIT) has played a significant role in improving clinical data. For example, many HIT companies are choosing to outsource their data repositories to the cloud for further improvement. Some technologies also prefer the Internet of Things (IoT) to ease drug traceability and mine patient profiles. In this section, we have discussed some of those approaches, categorizing them into traditional, blockchain-based, and combined systems.

2.1. Traditional approaches

Goodarzian et al. have developed a sustainable, integer, and linear programming-based model named Sustainable Medical Supply Chain Network (SMSCN) to locate the distribution centers, manage the inventory, optimize the total cost of the supply chain, and organize the allocation centers during the pandemic situation [16]. In the same manner, Khan et al. have focused on identifying the significant impacts of COVID-19 on the supply chain, which will eventually assist the policy planner in coming up with improvised policies to deal with the pandemic at the functional level [17].

2.2. Artificial intelligence based approaches for drug counterfeit

The Internet of Technology, cloud computing, and artificial intelligence have opened a new doorway of possibility in the medical supply chain. Korpela et al. have investigated company-specific data to find the importance of interoperability and integration in the digital supply chain for various organizations and systems [18].

One of those ways of proving the efficiency of artificial intelligence in the healthcare field is by using mobile applications to verify and trace every capsule using 3D fluorescent QR codes. These Android applications often allow consumers to check the product's authenticity by verifying the local government. There is also a framework that utilizes a data matrix to resolve the current vulnerabilities of present solutions [19–21]. Using RFID and data mining algorithms, fake medicine detection becomes more convenient [22], [23]. Other than these, image processing-based techniques can identify fake drugs. With the help of a heat map, a support vector machine and other classifiers can successfully classify relevant regions [24].

However, the offered solutions may lack interoperability and scalability due to the usage of various centralized databases.

2.3. Blockchain-based approaches

Existing approaches for ensuring drug supply chain traceability are often centralized and lack transparency among supply chain participants, permitting centralized power to modify information without notifying other stakeholders. Alternatively, a blockchain-based system offers data security, transparency, immutability, provenance, and validated transaction records. In an online survey, the authors noticed that most customers viewed this new blockchain technology very positively [25] for the medical supply chain.

In this respect, Casado-Vara et al. has proposed a new version of the circular economy, a multi-agent system model using blockchain to ensure data security and interoperability [26]. Abeyratne et al. [27] have proposed a blockchain-ready manufacturing supply chain template for the future. Gcoin blockchain has been proposed by Tseng et al. to ensure transparent data flow in drug transactions [28]. A time-worthy discussion on the opportunities, obstacles, and future scopes of blockchain in the medical supply chain can be found in the article of Wamba et al. [29]. K. Mackey, in his work, emphasizes blockchain technology for solving security and integrity issues of health supply chain [30].

Encrypted QR(quick response) code security via blockchain is offered to identify counterfeit drugs [31]. Chang et al. have proposed a ledger that can ease secured information sharing and miscellaneous participation among supply chain units [32]. The proposed framework of Haq et al. can track the drug supply chain and record the effect of the medicine [33]. Slim et al. have developed a pharmacy surveillance blockchain to share drug-related information in a distributed network [34]. In another paper, Sahoo et al. suggest blockchain countering these loopholes and making the drug supply chain more traceable, visible, and secure. Uddin et al. have proposed a blockchain-based system where immutable Medledger is linked with decentralized file systems [35]. In the U.S., the MediLedger Project has been built to put a stop to drug counterfeiting [36]. Additionally, it also follows the DSCSA regulations to provide interoperability between organizations. Raj et al. have developed a permissioned blockchain to prevent this drug replica chain and add more security and transparency to the drug supply chain [37]. A start-up, Modum.io AG has built an intelligent contract to store temperature-related data and utilize it whenever necessary [38].

2.4. Combined approaches

There are also some approaches where the traditional approach and blockchain work hand in hand to develop and ease a transparent medical supply chain to prevent drug counterfeiting. To increase security in the drug supply chain, Schöner et al. have suggested a blockchain-based application [39] that can trace each medicine item from its trade history to its distribution. They have attached a unique identity tag to the items of medicine to track their ownership virtually and physically, eventually verified by smart contracts. In the same way, to track drug supply platforms, Liu et al. have proposed a framework combining blockchain and IoT [40]. They use off-chain and on-chain mechanisms to store data and smart contracts to ensure traceability.

3. Problem formulation and proposed framework

3.1. Product flow in current drug supply chain

Bangladesh's pharmaceutical supply chain is complicated, impacting effective regulatory control, acceptable use, and medication quality. The Directorate General of Drug Administration (DGDA) governs all five forms of medicine (allopathic, ayurvedic, homeopathy, herbal, and unani) to preserve the quality of medicines, set prices, inspect all facilities, and conduct post-marketing surveillance.
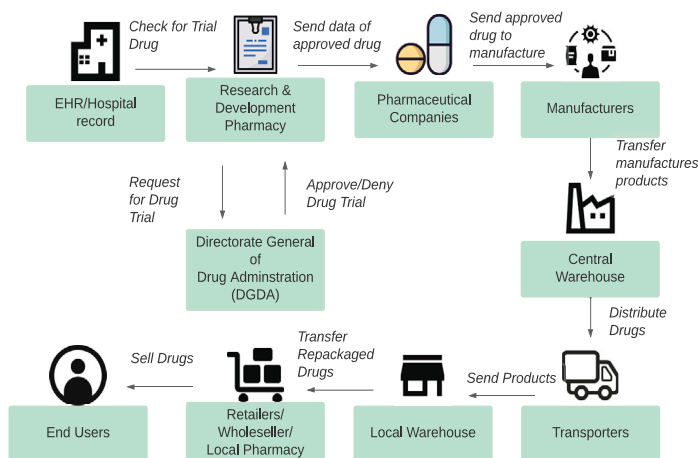
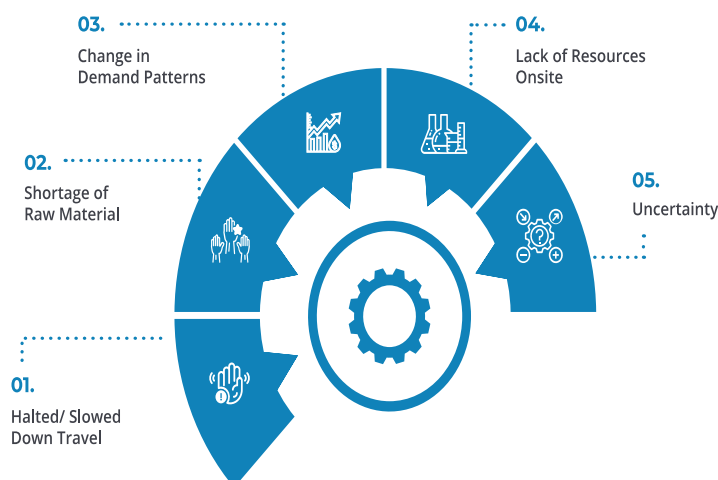**Fig. 1.** Sequence of Operations in Current System.

Fig. 2. Pharmaceutical Supply Chain Challenges.

This seems to be critical in light of the World Health Organization's (WHO) finding that low-quality medicines are inclined to proliferate in circumstances with limited regulatory capacity, high demand for medicines, low cost, and availability, as well as the impact of moderate medicines [41]. Following is a summary of the product flow in the existing drug traceability system, which is illustrated in Fig. 1.

- To begin, a clinical research lab collects data from medical records and uses it to initiate a drug trial.
- The trialed drug is then approved or rejected by the country's drug regulatory agency (DGDA).
- Pharmaceutical companies, in turn, send approved drug products to manufacturers.
- After that, the finished goods are delivered to a central warehouse, separated into packages, and distributed to local warehouses.
- The repackaged drugs will be handled by retail pharmacies, wholesalers, and other types of local pharmacies.
- Finally, to deliver the drugs to the final customers, the local vendors will process the new negotiated price.

Unfortunately, unethical people, unlicensed vendors, and enterprises interested in cutting corners (and ignoring product efficacy challenges) to earn a profit abound in this stock market. The situation is dire, with crooked wholesalers and intermediaries ready to purchase stolen goods, falsify pedigree records, and sell the product at the total market price to unwitting pharmacies.

3.2. Key challenges of current system

Pharmaceutical supply chain issues have recently been a critical source of concern for the business, as shown in Fig. 2.[1] The issues are still very much present because of the complicated relationships among stakeholders. Besides that, this pandemic had a profound socioeconomic influence on the world and disrupted whereas almost every aspect of the industry. The following are some of the primary obstacles in combating the issue of counterfeit drugs:

- **Lack of Transparency**: One of the most frequently encountered concerns is the difficulty of determining the source of a problem. Whenever drugs arrive in an unfit state for human consumption, when a counterfeit drug is included in the shipment, or when costs increase for no apparent reason, transparency is compromised.
- **Regulations and Compliance**: The pharmaceutical distribution system is already required to follow the most recent Quality System Practices. Regulations, on the other hand, are constantly changing. Enterprises will gradually be required to improve their internal control and management of customs and supply chains to comply with a new level.
- **Raw Material Scarcity**: The failure to plan efficiently during a pandemic might result in a slew of problems when it comes to obtaining raw materials. Without a guiding document, figuring out production time and exact inventory levels can take a long time as they try to generalize data and comprehend the supply schedule.
- **Rapid Drug Delivery**: Historically, bringing medications to market has been a race against the clock. Pharmaceutical processes and supply chain management handling must be as efficient to ensure fewer bottlenecks and probable errors during these testing intervals.
- **Inventory Management**: Another problem is keeping inventory under control so that it does not fluctuate.
- **Technological bottlenecks are Frequent**: The pharmaceutical sector has historically been reluctant and conservative when it comes to adopting innovation. While significant progress has been made in the recent decade, there are still several obstacles to achieving the full potential of technological advancements.

3.3. Methodology of PharmaChain

Our solution's primary technological architecture is built on Hyperledger Fabric, which offers authentication security, scalability, and critical data separation capability. Developers may construct plug-in components using Fabric's modular architecture. Then, in terms of channels, ordering services, peers, and certificate authority, we have detailed the network architecture of the indicated platform, which is split into pharmaceutical companies, the Drug Regulator Authority, and local vendors such as hospitals, pharmacies, etc. On-chain Resources are utilized to record the logs and events generated by the smart contract, enabling tracking and tracing. Moreover, a registration and identity system is applied as an off-chain resource to integrate the decentralized storage of the identification addresses of multiple stakeholders. In addition, we have introduced three modules of governance, including network membership, technical infrastructure, and business networks, in order to maintain coordination among stakeholders, including the formalization and decentralization of rules, improved surveillance, and automatization of process.

For result analysis, we generate data in the .json format of a single product and then store it in a shared ledger in CouchDB. For security purposes, we have produced the hash value of every piece of data using the SHA-256 algorithm. To encrypt the hash value; we have generated two pairs of elliptic keys, including private and public keys for the pharmaceutical company and the drug regulator authority, using the elliptic curve digital signature algorithm. We have chosen the private keys generated by the elliptic curve cryptography (ECC) for these two stakeholders and then formed a signed document for them. Finally, hash values can be verified by decrypting the signed document using the pharmaceutical business's or regulatory authority's public key. To verify the clarity of this regenerated hash, it can be compared to the original hash in the global chain.

Fig. 3 depicts the proposed drug traceability system's high-level architecture, including the participants and their actions with the smart contract. Through web APIs, stakeholders will access intelligent contracts and decentralized storage (on-chain and off-chain) resources. Logs, hashed data, and transactions will be generated based on interactions with on-chain and off-chain resources.

4. Technical architecture

4.1. Hyperledger fabric overview

Practical Byzantine Fault Tolerance (PBFT) is the consensus mechanism to verify transactions and create blocks. The critical technical architecture of our solution is implemented in Hyperledger Fabric [42,43]. Peer nodes, ordering nodes, channels, application programs, etc., are the main components of the Hyperledger Fabric architecture, which are described below and depicted in Fig. 4.[2]

- **Channel:** A configuration block-defined channel is a permissioned blockchain middleware that enables data security and confidentiality.
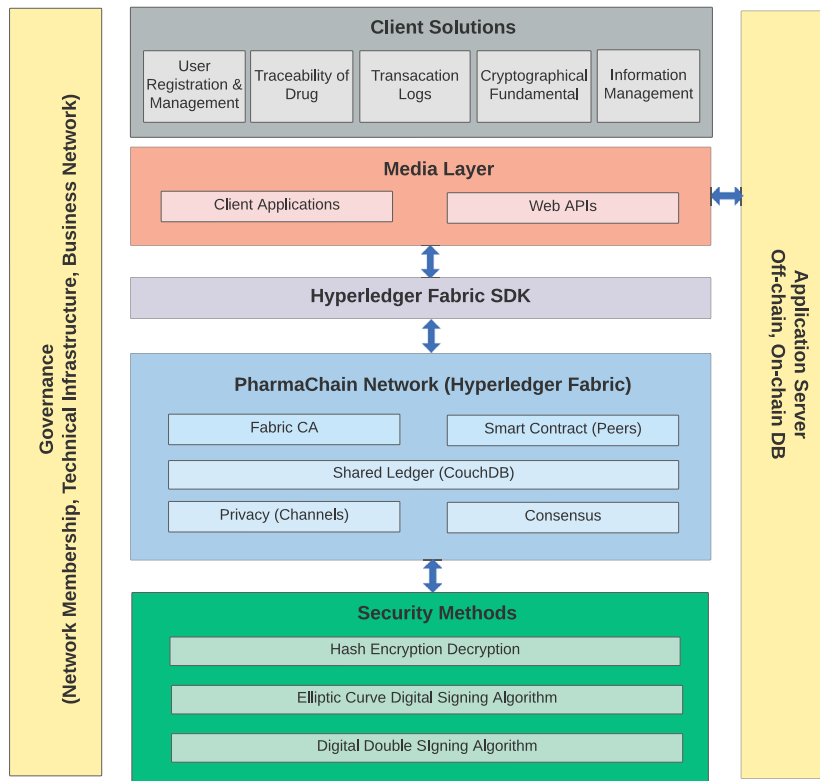

Fig. 3. High level architecture of PharmaChain.

- **Node:** In a specialized device, nodes are the framework's interaction entities. The hyperledger fabric platform supports various node types, including peer nodes, orderers, anchor nodes, and leading nodes [42].
  - **Peer Node:** The primary purpose of a peer node is to perpetrate transactions and maintain a state and a duplicate of the Ledger along with the smart contracts.
  - **Ordering Service node (Orderer):** This node ensures delivery service which can be centralized or decentralized by establishing a standard connection between clients and peers.
  - **Anchor Node:** Each participant in a channel is assigned an anchor peer, allowing peers from individual Participants to explore all other participants on the channel.
  - **Leading Node:** One of these peers continues to serve as the channel's leading peer, communicating with the network ordering service on the member's behalf.
- **Certificate Authority:** The Certificate Authority (CA) is primarily responsible for formulating credentials for stakeholders for network-wide identity management.
- **Ledger**: The Ledger is a hash-linked log of transactions.
- **Chaincode:** The Chaincode is the set of innovative contracts computer programs hosted on each peer node in a secured docker container.

4.2. Technical architecture of PharmaChain

We have outlined the network topology as depicted in Fig. 5. The technical architecture of the proposed system is divided into three entities: pharmaceutical companies (C1, C2), the Drug Regulator Authority (D1), and hospitals or pharmacies (X, Y, Z). Each company is subdivided into four segments: a research lab, a manufacturer, a supplier, and a distributor, all grouped into a single channel. Additionally, these three departments have agreed to develop a network policy for establishing and initializing a blockchain network. Each division has its own shared ledger ($L1$, $L2$), peer nodes ($P1$, $P2$,...... PN), and ordering nodes ($O1$, $O2$,...... ON). The ordering service's responsibility is to create channels and enable other nodes to participate. Each entity has its anchoring node for communication and a global certificate authority for identity management and interconnection. For example, companies C1 and C2 are connected to D1 via CA1's connections to CA2 and CA3. The certificate authority creates the scope of joining as a new stakeholder in a specific local and global channel. The process is in two steps: first, public key infrastructure (PKI) is set up for the user, and second, the user calls a smart contract method from the chain code to register into the system.
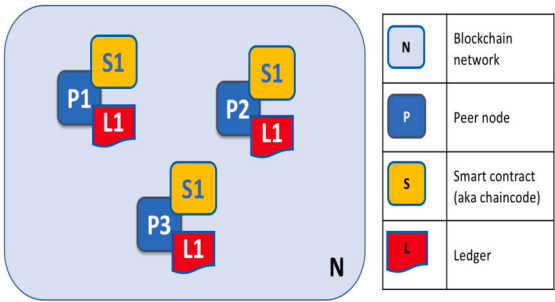
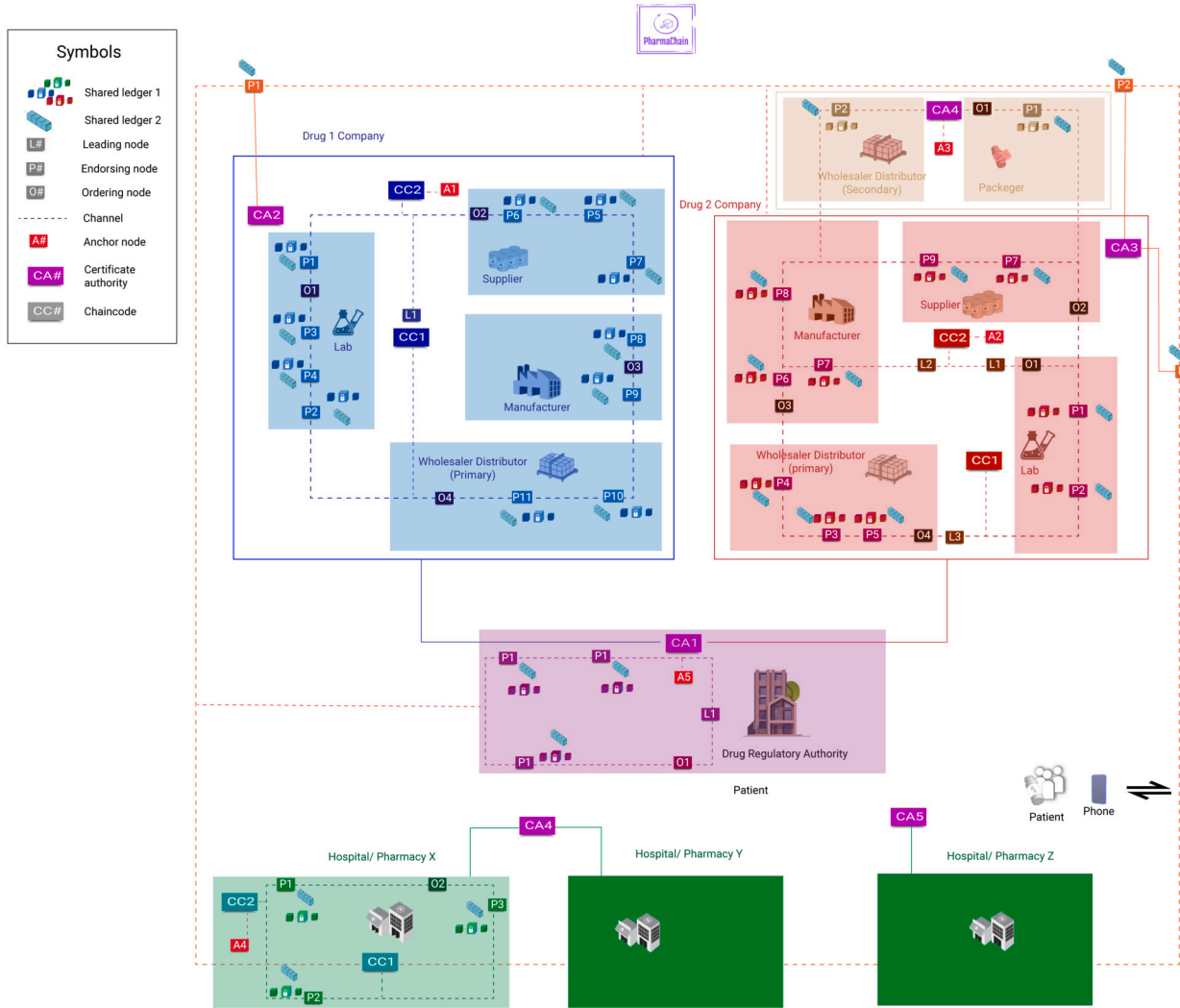**Fig. 4.** General Architecture of Hyperledger Fabric.

Fig. 5. PharmaChain's Network Topology Architecture on Hyperledger Fabric.

4.3. Data architecture

4.3.1. On-chain and off-chain transactional mechanism

To minimize network traffic while ensuring high levels of security, immutability, and a transaction validated by active stakeholders, to secure transactional data and non-transactional data, on-chain and off-chain read control matrix are listed in Table 1 Table 2 respectively.

Table 1
On-Chain Read Access Control Matrix Chart.

Stakeholders	Entity					
	Electrical Medical Record	Prescription Status	Clinical Research Repository	Trial Drug Status	Manufacturer Order Replacement	Warehouse
Pharmaceutical Company	If involved	If involved	If involved	If involved	Yes	If involved
Doctor	Yes	Yes	If involved	With Restriction	No	No
Patient	Yes	Yes	No	No	No	No
DGDA	If involved	If involved	With Restriction	Yes	No	No
Pharmaceutical R&D	If involved	If involved	Yes	With Restriction	No	No
Manufacturer	No	No	No	No	Yes	Yes
Transporter	No	No	No	No	If involved	If involved
Central Warehouse	No	No	No	If involved	If involved	Yes
Secondary Warehouse	No	No	No	No	No	No
Local Vendors	No	No	No	No	No	No
Hospitals	Yes	Yes	If involved	If involved	No	No

Table 2
Off-Chain Read Access Control Matrix Chart.

Stakeholders	Entity (Identification Repository)					
	Pharmaceutical Co.	Clinical Researcher	Regulatory Administrator	Manufacturer	Transporter	Local Vendors
Pharmaceutical Company	Own	Yes	With Restriction	If involved	If involved	No
Doctor	Global data	No	No	No	No	No
Patient	Global Data	No	No	No	No	No
DGDA	Yes	With Restriction	Own	No	No	No
Pharmaceutical R&D	Yes	Own	With Restriction	No	No	No
Manufacturer	If involved	No	No	Own	If Involved	No
Transporter	No	No	No	If involved	Own	No
Local Vendors	No	No	No	No	No	Yes
Hospitals	With Restriction	No	No	Global data	No	No

4.4. Smart contract design of PharmaChain

Fig. 6 illustrates how the proposed system will conduct ledger inquiries and upgrades via the chain code. The functions of smart contracts are written below.

- **Registration Contract:** Here, each stakeholder's registration smart contract (RegisterStakeholders (License no)) will be stored in the blockchain, and a unique identifier will be provided to them. The inputs of the smart contracts are license no, name, contact address, etc. Some functions are:
  - *RegisterManuf()*: Confirm the manufacturer registration by paying an application fee.
  - *RegisterCDist()*: Confirm the central distributer's registration by paying service charge.
  - *RegisterLDist()*: Confirm the local distributer's registration by paying an admin payment.
  - *RegisterLV()*: Confirm the local vendors, such as retailers, and wholesalers, registration by paying an additional amount.
- **Shipment Contract:** Further placement of drugs is covered by the agreement between the pharmaceutical company, manufacturer, and distributer.
  - *VerifyTrialDrug()*: By making a payment, the pharmaceutical clinical research lab will enquire the DGDA to verify the results.
  - *ConfirmTrialDrug()*: DGDA Confirm Trial drug requested by the lab authority.
  - *PalceOrderRequest()*: Here, the pharma company orders the manufacturer to arrange necessary medical supplies.
  - *ConfirmOrderManu()*: The manufacturer confirms order placement by assessing the available medical equipment.
  - *NotificationRequestedOrder()*: The company will be notified of the current confirmation of the order.
  - *AssignPrimaryDistributer():* A central warehouse will be a primary distributor between manufacturers and end-users.
  - *ShipmentRequest()*: The central warehouse will place a shipment request to the local warehouse through registered transporter.
  - *ConfirmShipmentSecondaryDistributer()*: The transporter confirms its availability and stores time and location on the server.
  - *ConfirmDrugRecive():* The local warehouse or secondary distributor notifies the central warehouse of the received products.
- **Negotiate purchase order contract:** These transactions are between the pharmaceutical company, local vendors, and secondary distributors.
  - *NewPriceContract()*: Secondary distributer initiates new price to the local vendors.
  - *NegotiateContract()*: Stakeholders will be notified and they will negotiate.
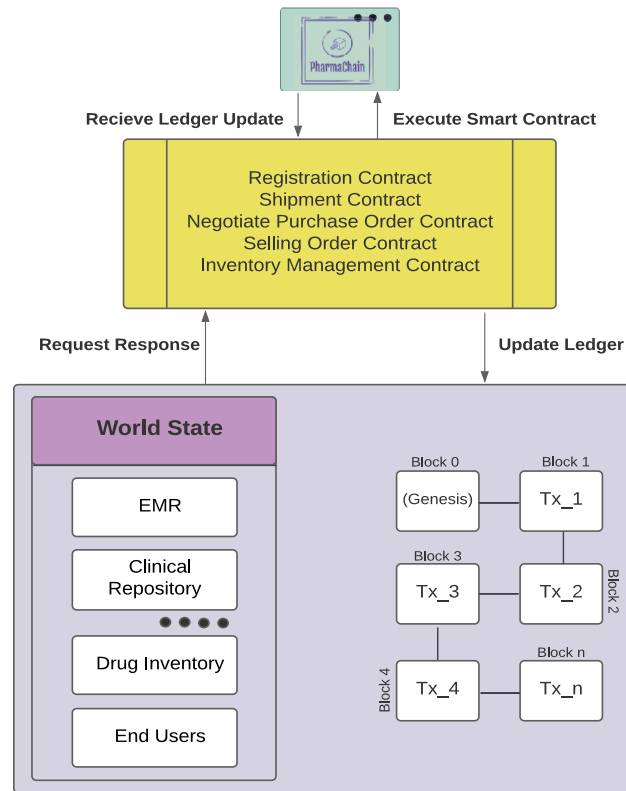
Fig. 6. Operations of Ledger Using a Smart Contract.

- – *ContractStatus()*: Confirmation or rejection of new price by local distributor.
- – *ConfirmNewContract()*: The stakeholders will be notified about the agreed-upon negotiated price.
- • **Selling Order Contract:** The transactions occur between the customer and supplier of the pharmaceutical product.
  - – *SubmitOrderLocalVendors()*: Local distributors will provide the drugs with a new price list to various registered local vendors.
  - – *OrderConfirmationLocalVendors()*: Order confirmation of drugs by local vendors.
  - – *SubmitPurchaseOrder()*: End users will provide purchase orders to the respective local vendors.
  - – *DeliveryStatus()*: Provide the delivery status to the stakeholders.
- • **Inventory Management Contract:**
  - – *UpdateInventory()*: To assure that the drugs available in the local vendor's store can fulfill the requirements of the end users.
  - – *TransferOwnership()*: The inventory authority can be changed from one entity to another.

4.5. Governance structure

Digital innovations progressively influence the everyday operations and interactions of stakeholders, enterprises, and governments. Traditional governance fails to recognize the shift in power dynamics caused by new actors, activities, and interactions in blockchain technology. Our research established three governance approaches to examine emerging power dynamics in the pharmaceutical supply chain, summarized below.

- • **Network Membership Governance:** It supports efficient network operations, including participant onboarding and offboarding, permission, support services, risks, and equitable cost distribution depending on participants' actions.
- • **Technology Infrastructure Governance:** This discipline's checklists concentrate on IT infrastructure, resources, performance, and technology evaluation via the lens of security, cost structures, and associated risks.
- • **Business Network Governance:** This combination of disciplines provides the foundation for an industry or user-specific multi-organizational operation structure, including a business strategy, external resources, charges, incentives, compliance, and laws.

Using the public key pairs kept in the global chain, end users, including the government, can monitor and trace pharmaceuticals in the supply chain without accessing factories, warehouses, or pharmacies. If any transaction is not in conformity with the governance standards, the smart contract might trigger an alert signal, and the PharmaChain blockchain system would invalidate the possible unlawful trade of counterfeit medications (Fig. 7).
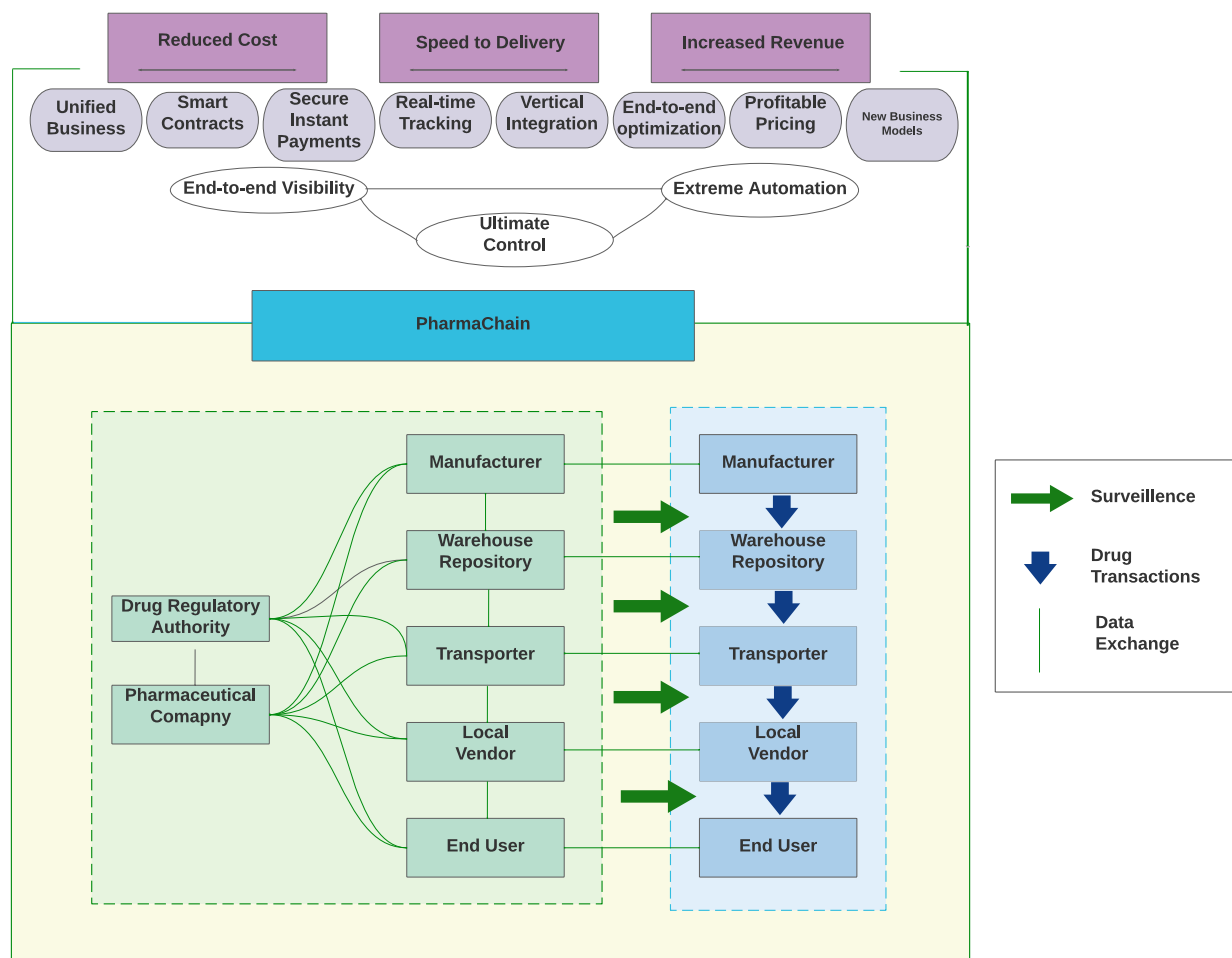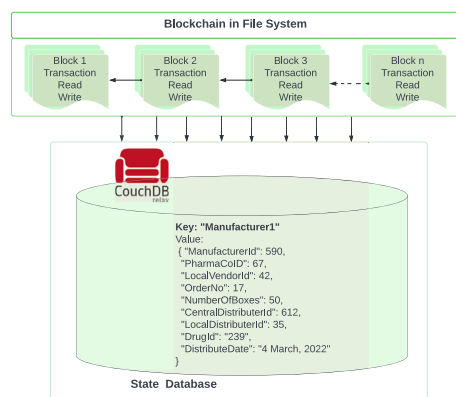
Fig. 7. Governance Structure of PharmaChain.

5. Experimental evaluation

All the experimental works in this chapter have been carried out on with an Intel(R) Core(TM) i5-8500M 3.00 GHz processor Windows 10 PC with 8 GB RAM.

- **Data Generation:** We have created some .json files such as drug-related information, medical history, doctor details, manufacturing details, transport system, personal information, etc., for a single product.
- **Distributed Ledger Storage for Corresponding Data:** CouchDB is an optional intermediary state database that enables complex queries when chain code statistical measures are specified in .json format. The world state of one file's data and dashboard is depicted in Fig. 8[a-b]. Here, manufacturer1 is a key-value pair that is kept in CouchDB. These transactions are then converted into encrypted data connected cryptographically to build a chain-like structure in the next step. This chain structure is used to record transactions chronologically on the ledger.
- **Hash Data Creation:** Encryption ensures data integrity by converting data into an unreadable form that can only be deciphered with the correct key. Multiple techniques, including SHA1, SHA256, and SHA512, can be used to create hash data. SHA256 has been used in our proposed framework. SHA-256 is a trademarked cryptographic algorithm that generates a 256-bit-long value. For example, this algorithm reduces a 512-bit data sequence to a 256-bit data sequence. Fig. 9 illustrates the hash value of the manufacturing entity using the SHA-256 algorithm. Using elliptic curve cryptography generates confidentiality between key pairs for public-key encrypted communications.
- **Elliptic Key Pair Generation:** A practical alternative to RSA's elliptic curve cryptography (ECC) is available. RSA attains comparable results using prime numbers rather than elliptic curves, but ECC has gained recent momentum due to the smaller key size and better security. Drug regulators and pharmaceutical companies each have their elliptic key, which we have developed separately. The public and private keys of two entities, a pharmaceutical company, and a drug regulatory authority, are depicted in Fig. 10 and Fig. 11, respectively. We choose ECC, which utilizes the secp256k1 curve and has a 32-bytes private key (a random value) and a 64-bytes public key.

(a) World view of one .json file

(b) Dashboard of CouchDB Database

Fig. 8. PharmaChain's Distributed Ledger.

Fig. 9. Hash Data Generation Using SHA256 Algorithm.

Fig. 10. Elliptic Key Pair Generation for Pharmaceutical Company.

- **Double Signing Procedure:** Digital signatures are computational techniques that verify the accuracy and integrity of a message, software, or electronic document. It aims to prevent tampering and imitation in digital communications by providing more inherent security. We have implemented a double digital signing algorithm to validate the hash values of drug regulators and pharmaceutical companies. We have selected the private keys generated by ECC for these two stakeholders and then created a signature for that entity. Here, Fig. 12 [a-b] demonstrates the encrypted contents created by forming the digital signature using the company's and regulator authority's elliptic private keys.

Public Key (Drug Regulatory Authority)	EC-Private Key (Drug Regulatory Authority)
-----BEGIN PUBLIC KEY----- MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAErpUlzNstM k5PEAtiamDe/3wQYWSTSAt9DVaNfSiRGgix9mgfYTenH6 Ovv3h8IxjtDE632kHtkaHw21StjQEMgQ== -----END PUBLIC KEY-----	-----BEGIN EC PRIVATE KEY----- MHQCAQEEIEu8J1DjiODAX/xu8MtA5KZaI8w+IYC+QFD +5OSMDA3LoAcGBSuBBAAKoUQDQgAErpUlzNstMk5P EAtiamDe/3wQYWSTSAt9DVaNfSiRGgix9mgfYTenH6Ov v3h8IxjtDE632kHtkaHw21StjQEMgQ== -----END EC PRIVATE KEY-----

Fig. 11. Elliptic Key Pair Generation for Drug Regulator Authority.

(a) Pharmaceutical Company   (b) Drug Regulator Authority

Fig. 12. Digital Signature Creation of Hash Value Using Elliptic Keys.

Fig. 13. Verification of Pharmaceutical Company's Signed Document.

- **Hash Decryption and Verification:** The user decrypts the signed document using the pharma company's or drug regulatory's public key. After decryption, the user can retrieve the specific hash value and compare it to the original hash values stored in the global chain. For the sake of consistency, the comparison must be the same. The successful verification of the company's and regulator authority's signed documents is displayed in Fig. 13 and Fig. 14 respectively.

Fig. 14. Verification of Drug Regulator Authority's Signed Document.

Table 3
Comparative Analysis of PharmaChain and Other Blockchain Solutions.

Features	PharmaChain	A. Musamih et al.	DrugLedger	Faisal et al.
Consensus Process	Permissioned	Permissionless	Permissionless	Permissioned
Blockchain Platform	Hyperledger Fabric	Ethereum	Bitcoin	Hyperledger Fabric
Storage Mechanism	Off-chain and On-chain	Off-chain and On-chain	On-chain	On-chain
Programmable Module	Smart Contract	Smart Contract	None	Docker Container
Currency	None	Ether	BTC	None
Governance	Three specialized modes	None	None	None
Cryptographic Algorithm	ECDSA	None	None	None

5.1. Performance evaluation

For the proposed traceable pharmaceutical supply chain approach, a comparative assessment of relevant existing systems' features are presented in Table 3. However, we have created three distinct governance and cryptographic techniques to facilitate counterfeit drug detection. Our proposed solution, PharmaChain, utilizes the Hyperledger fabric because of its multi-chain code and multi-channel capabilities, while IPFS based solution proposed by A. Musamih et al. [44] and DrugLedger [11] utilize the public permissioned model. They both employ bitcoin and ether as currencies.

6. Discussion

For our proposed approach to address counterfeit medications, we've detailed our security analysis and certain critical objectives including integrity, scalability and reliability in this part.

6.1. Value generation

In this part, we briefly cover the security analysis and other added value of the proposed blockchain-based solution for the healthcare supply chain, where major security objectives include integrity, accountability, scalability, and non-repudiation.

- **Integrity:** The proposed system maintains its integrity since all events and records are stored in the immutable blockchain ledger. As a consequence, every transaction in the healthcare supply chain will be able to be tracked and monitored.
- **Data Privacy and Reliability:** Only authorized parties are allowed to perform important operations in the smart contract. This guarantees that the data is protected from unauthorized access and that no undesirable entities are able to use it.
- **Scalability:** Our proposed solution, tackles the scalability issue by controlling specific data access by using both off-chain and on-chain transaction methods so that it can handle larger transactions. We design our technical architecture in such a way that when a new entity happens, we can add it easily to the global chain, and it can also be added to the local chain via certified authority.
- **Accountability:** Each function execution in this framework is recorded on the blockchain, making it easy to track down the function caller at any time. As a result, all participants are accountable for their conduct.

However, our platform doesn't ensure case-specific ledgers that can be replicated among multiple locations with a local chaining system. For research mining while preserving individuals' privacy, k-anonymity usable privacy needs to be applied with the scope of lower overhead in mining.

6.2. Security analysis of proposed framework

The security evaluation of PharmaChain is briefly discussed in this subsection, with integrity, transparency, authorization, accessibility, and non-repudiation as key security goals. We have introduced three levels of protection to resolve some critical flaws that can be utilized for malicious purposes, which are pointed out below:

- **Hash Data Encryption:** For privacy, we used a digital signature algorithm on the hash data of JSON files. The hash code or key cannot be converted back to the original data. It can only be identified, and the hash code is checked to see if it is equivalent; otherwise, the data is not identical.
- **Digital Signature with Two Private Keys:** We have implemented a double signing algorithm with the company's private key and the regulator's private key. The SHA-256 algorithm converts the data in each transaction block into hash values. All encrypted data is concatenated during the distribution phase and signed with the company's and regulator's respective private keys. If an intruder tries to change data, he or she will need to know two private keys. This feature is critical for healthcare supply chain applications because it ensures data security and integrity.
- **33% Node Attack:** An external entity must control more than 33% of the chain's nodes in order to control the channel's transaction addition capabilities, or hash leverage ratio. In addition, the attacker would need to go through the screening process of certificate authority, making it almost impossible to alter and hack this network.

7. Conclusion and future work

Blockchain has already manifested its scope to change the conventional supply chain business into a safe, automated, permanent, audible, anonymous, and decentralized supply chain. In this paper, we have proposed a hyperledger fabric-based system named PharmaChain that ensures data provenance in the pharmaceutical supply chain. To be more specific, PharmaChain leverages the cryptographic fundamentals of distributed ledger technology to create tamper-proof logs of supply chain events and deploys smart contracts embedded in the hyperledger fabric for the automation of events to be accessible to all stakeholders. Transactional logs enable patients, nurses, physicians, researchers, and pharmacists to securely store, retrieve, and communicate personal medical information. Additionally, PharmaChain protects against malicious efforts to compromise the security, accessibility, transparency, and non-repudiation of transaction data, which is crucial in a comprehensive and multi-environment like the pharmaceutical supply chain. Our model ensures three-step data security using SHA-256, elliptic curve cryptography, and the double signature encryption method. It successfully generates a system that cannot be vulnerable until the 33% node attack, which is quite a success compared to existing models. As part of our efforts to build a secure and transparent drug supply chain, we've selected three governance models to help optimize the flow of information between the drug regulatory authority and organizations.

In the future, we will continue to work on improving the system's performance and proving its viability via deployment in a real-world scenario for additional supply chain systems.

CRediT authorship contribution statement

Sarmistha Sarna Gomasta: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools, or data; Wrote the paper.
Aditi Dhali; Tahlil Tahlil: Contributed reagents, materials, analysis tools or data; Wrote the paper.
Md. Musfique Anwar; A. B. M. Shawkat Ali: Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data.

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.

References

[1] Walter G. Chambliss, Wesley A. Carroll, Daniel Kennedy, Donald Levine, Michael A. Moné, L. Douglas Ried, Marv Shepherd, Mukund Yelvigi, Role of the pharmacist in preventing distribution of counterfeit medications, J. Am. Pharm. Assoc. 52 (2) (2012) 195–199.
[2] Ronald J. Ziance, Roles for pharmacy in combatting counterfeit drugs, J. Am. Pharm. Assoc. 48 (4) (2008) e71–e91.
[3] Henry I. Miller, Wayne Winegarden, Fraud in Your Pill Bottle: The Unacceptable Cost of Counterfeit Medicines, Center for Medical Economics and Innovation Issue Brief. Pacific Research Institute, 2020.
[4] Faisal Jamil, Lei Hang, KyuHyung Kim, DoHyeun Kim, A novel medical blockchain model for drug supply chain integrity management in a smart hospital, Electronics 8 (5) (2019) 505.
[5] T Guardian, 10% of drugs in poor countries are fake, says who, Accessed: Jun, 3:2020, 2017.
[6] Mohammad Saidul Islam, A review on the policy and practices of therapeutic drug uses in Bangladesh, Calicut. Med. J. 4 (4) (2006) e2.
[7] Mujahid Mohiuddin Babu, Factors contributing to the purchase of over the counter (otc) drugs in Bangladesh: an empirical study, Internet J. Third World Med. 6 (2) (2008) 9–24.
[8] Alaul Alam, Combating Fake Drug Menace - Op-ed, Sep 2021 [Online; accessed 29-May-2022].
[9] Talha Burki, Global shortage of personal protective equipment, Lancet Infect. Dis. 20 (7) (2020) 785–786.

[10] Drug Supply Chain Security Act, Sep 2021 [Online; accessed 29-March-2022].
[11] Yan Huang, Jing Wu, Chengnian Long Drugledger, A practical blockchain system for drug traceability and regulation, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1137–1144.
[12] Benefits of Pharmaceutical Track-and-Trace, Sep 2021 [Online; accessed 29-May-2021].
[13] Frost & Sullivan, Global Blockchain Technology Market in the Healthcare Industry, https://www.marketresearch.com/Frost-Sullivan-v383/Global-Blockchain-Technology-Healthcare-12732534/, 2019. (Accessed 29 May 2021).
[14] Satoshi Nakamoto Bitcoin, A Peer-to-Peer Electronic Cash System, Decentralized Business Review, 2008, 21260.
[15] M. Niranjanamurthy, B.N. Nithya, S.J.C.C. Jagannatha, Analysis of blockchain technology: pros, cons and swot, Clust. Comput. 22 (6) (2019) 14743–14757.
[16] Fariba Goodarzian, Ata Allah Taleizadeh, Peiman Ghasemi, Ajith Abraham, An integrated sustainable medical supply chain network during covid-19, Eng. Appl. Artif. Intell. 100 (2021) 104188.
[17] Shahbaz Khan, Abid Haleem, S.G. Deshmukh, Mohd Javaid, Exploring the impact of covid-19 pandemic on medical supply chain disruption, J. Indust. Integr. Manag. (2021).
[18] Kari Korpela, Jukka Hallikas, Tomi Dahlberg, Digital supply chain transformation toward blockchain integration, in: Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.
[19] Saif ur Rehman, Raihan Ur Rasool, M. Sohaib Ayub, Saeed Ullah, Aatif Kamal, Qasim M. Rajpoot, Zahid Anwar, Reliable identification of counterfeit medicine using camera equipped mobile phones, in: 8th International Conference on High-Capacity Optical Networks and Emerging Technologies, IEEE, 2011, pp. 273–279.
[20] Minli You, Junjie Zhong, Yuan Hong, Zhenfeng Duan, Min Lin, Feng Xu, Inkjet printing of upconversion nanoparticles for anti-counterfeit applications, Nanoscale 7 (10) (2015) 4423–4431.
[21] Naimah Mat Isa, Shuria Saaidin, Norakmar Arbain Sulaiman, Azwati Azmin, Nur Shazarina Atiqah, Azhar Shah, Pharmaceutical product information based on android platform, in: 2014 2nd International Conference on Electrical, Electronics and System Engineering (ICEESE), IEEE, 2014, pp. 66–70.
[22] Ho Sung Lee, Hyo Chan Bang, Detecting counterfeit products using supply chain event mining, in: 2013 15th International Conference on Advanced Communications Technology (ICACT), IEEE, 2013, pp. 744–748.
[23] Tim K. Mackey, Gaurvika Nayyar, A review of existing and emerging digital technologies to combat the global trade in fake medicines, Exp. Opin. Drug Saf. 16 (5) (2017) 587–602.
[24] Fábio do Prado Puglia, Michel José Anzanello, Jacob Scharcanski, Juliana de Abreu Fontes, João Batista Gonçalves de Brito, Rafael Scorsatto Ortiz, Kristiane Mariotti, Identifying the most relevant tablet regions in the image detection of counterfeit medicines, J. Pharm. Biomed. Anal. 205 (2021) 114336.
[25] Niels Hackius, Moritz Petersen, Blockchain in logistics and supply chain: trick or treat?, in: Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), vol. 23, epubli GmbH, Berlin, 2017, pp. 3–18.
[26] Roberto Casado-Vara, Javier Prieto, Fernando De la Prieta, Juan M. Corchado, How blockchain improves the supply chain: case study alimentary supply chain, Proc. Comput. Sci. 134 (2018) 393–398.
[27] Saveen A. Abeyratne, Radmehr P. Monfared, Blockchain ready manufacturing supply chain using distributed ledger, Int. J. Res. Eng. Technol. 5 (9) (2016) 1–10.
[28] Jen-Hung Tseng, Yen-Chih Liao, Bin Chong, Shih-wei Liao, Governance on the drug supply chain via gcoin blockchain, Int. J. Environ. Res. Public Health 15 (6) (2018) 1055.
[29] Samuel Fosso Wamba, Maciel M. Queiroz, Blockchain in the Operations and Supply Chain Management: Benefits, Challenges and Future Research Opportunities, 2020.
[30] Kevin A. Clauson, Elizabeth A. Breeden, Cameron Davidson, Timothy K. Mackey, Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: an Exploration of Challenges and Opportunities in the Health Supply Chain, Blockchain in Healthcare Today, 2018.
[31] Randhir Kumar, Rakesh Tripathi, Traceability of counterfeit medicine supply chain through blockchain, in: 2019 11th International Conference on Communication Systems & Networks (COMSNETS), IEEE, 2019, pp. 568–570.
[32] Shuchih Ernest Chang, Yi-Chian Chen, Ming-Fang Lu, Supply chain re-engineering using blockchain technology: a case of smart contract based tracking process, Technol. Forecast. Soc. Change 144 (2019) 1–11.
[33] Ijazul Haq, Olivier Muselemu Esuka, Blockchain technology in pharmaceutical industry to prevent counterfeit drugs, Int. J. Comput. Appl. 180 (25) (2018) 8–12.
[34] Patrick Sylim, Fang Liu, Alvin Marcelo, Paul Fontelo, Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention, JMIR Res. Protoc. 7 (9) (2018) e10163.
[35] Mueen Uddin, Blockchain medledger: hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry, Int. J. Pharm. 597 (2021) 120235.
[36] Jens Mattke, Axel Hund, Christian Maier, Tim Weitzel, How an enterprise blockchain application in the us pharmaceuticals supply chain is saving lives, MIS Q. Exec. 18 (4) (2019).
[37] Rohit Raj, Nandini Rai, Sonali Agarwal, Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 1572–1577.
[38] Thomas Bocek, Bruno B. Rodrigues, Tim Strasser, Burkhard Stiller, Blockchains everywhere-a use-case of blockchains in the pharma supply-chain, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), IEEE, 2017, pp. 772–777.
[39] Manuela M. Schöner, Dimitris Kourouklis, Philipp Sandner, Erick Gonzalez, Jonas Förster, Blockchain Technology in the Pharmaceutical Industry, Frankfurt School Blockchain Center, Frankfurt, Germany, 2017.
[40] Xinlai Liu, Ali Vatankhah Barenji, Zhi Li, Benoit Montreuil, George Q. Huang, Blockchain-based smart tracking and tracing platform for drug supply chain, Comput. Ind. Eng. 161 (2021) 107669.
[41] Express tf. bangladesh exports medicines to 151 countries, 2018 [Online; accessed 31-March-2022].
[42] Hyperledger fabric v1.0 project, 2020 [Online; accessed 30-March-2022].
[43] Hyperledger fabric v0.6 project, 2020 [Online; accessed 30-March-2022].
[44] Ahmad Musamih, Khaled Salah, Raja Jayaraman, Junaid Arshad, Mazin Debe, Yousof Al-Hammadi, Samer Ellahham, A blockchain-based approach for drug traceability in healthcare supply chain, IEEE Access 9 (2021) 9728–9743.