Computers & Industrial Engineering 190 (2024) 110021

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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

Hyperledger sawtooth based supplychain traceability system for counterfeit drugs

Anum Nawaz [a,b,*], Liguan Wang [b], Muhammad Irfan [a], Tomi Westerlund [a]

[a] Turku Intelligent and Embedded Robotic Systems Lab, Faculty of Technology, University of Turku, Finland
[b] Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai, China

ARTICLE INFO

Keywords:
Blockchain
Hyperledger sawtooth
Drugs supplychain
Drugs traceability
Quantum secure communication

ABSTRACT

Drug supply chains have been facing severe issues as counterfeit product cases are increasing exponentially. A supply chain management system that ensures transparency, reliability, and provenance of drugs would increase the trustworthiness of the whole industry. One solution to all three needs is utilizing blockchain-based distributed ledger technologies (DLTs). Even though DLTs are emerging as an ideal infrastructure for multi-stakeholder supply chain applications, they still need to be more mature to address the specific challenges specific to each use case. In this article, we propose a distributed blockchain-based framework, PHTrack, leveraging hyperledger sawtooth as a drug supply chain traceability system. Hyperledger sawtooth addresses scalability issues by offering a robust foundation to support large-scale drug supply chain operations in a modular way for it's each participating stakeholder. Furthermore, it simplifies the integration process with existing systems, even those employing different technologies, thereby facilitating a smoother transition to DLTs. The design of PHTrack is oriented towards minimizing resource consumption throughout the process, particularly within hyperledger sawtooth nodes. Additionally, it incorporates quantum secure off-chain communication for peer-to-peer (P2P) communication. A set of experiments was conducted to validate the proposed framework. Experiments have shown that PHTrack provides reliable and comprehensive drug provenance as well as real-time drug supply chain tracking.

1. Introduction

Resilient and trustworthy supply chain systems are vital in modern society to answer sudden and unexpected changes in the demand for drugs or other essential merchandise. One of the challenges is that the current global supply chain management solution is a wildly complex, interlinked network of untrusted bodies (Hassija & Vikas, 2020). Solely drug distribution has exploded in size and complexity, making it complicated to find loopholes in the systems. Therefore, building trust among the supply chain parties is essential. To underline the importance of the trustworthy supply chain, consider the process from drug discovery through development and regulatory approval to pharmacy; the process is hazardous and takes several years at minimum (Dauvergne, 2022). Thus, having a supply chain system which ensures that a customer is receiving a genuine product developed by a legitimate manufacturer rather than a counterfeit one cannot be undermined.

There are several supply chain management platforms for the pharmaceutical industry. Yet, they are outdated, incapable of allowing manufacturers and regulatory agencies to control drug distribution, and withstand modern cyber-security threats (Melnyk, 2022). When a pharmaceutical company's supply chain is breached, fraud and counterfeit drugs are more likely to happen. Even a slight doubt is serious because counterfeit drugs may include harmful ingredients, incorrect proportions of ingredients, substandard composition, correct ingredients with wrong packaging, fake brand names, or expired products (Moosivand, Ghatari, & Rasekh, 2019). Even if the drugs are excellent, doubt cannot be removed because drug regulatory authorities do not supervise production and distribution.

To give an insight into the size of the problem, the European Union Intellectual Property Office's (EUIPO) report estimates that counterfeit drugs are causing pharmaceutical companies to lose over EUR 16.5 billion in sales and affect more than 80 thousand jobs in the

* Corresponding author at: Turku Intelligent and Embedded Robotic Systems Lab, Faculty of Technology, University of Turku, Finland.
E-mail addresses: anunaw@utu.fi, 18110720163@fudan.edu.cn (A. Nawaz), 17110240019@fudan.edu.cn (L. Wang), muhammad.m.irfan@utu.fi (M. Irfan), tovewe@utu.fi (T. Westerlund).
URL: https://tiers.utu.fi/team (A. Nawaz).

https://doi.org/10.1016/j.cie.2024.110021
Received 26 September 2023; Received in revised form 15 January 2024; Accepted 26 February 2024
Available online 27 February 2024

pharmaceuticals sector and other sectors that sell goods and services to it (Pharmaceutical sector - observatory, 2016). According to the World Health Organization (WHO), a trade worth 73 billion euros in counterfeit medicines is taking place annually (Kaiser-Kershaw, 2022). WHO also reports that counterfeit medical products increased by 47% from 2020 to 2021 (Ziavrou, Noguera, & Boumba, 2022). The case of third-world countries is much more severe than that of developed countries, and the news reflects its intensity regularly. Further, the report indicated that fake drugs causing pneumonia cause 72,000 deaths in children, and 69,000 people die of malaria each year, which is considered one of the significant causes of death.

1.1. Challenges and loopholes in existing systems

The presence of falsified drugs in the pharmaceutical supply chain is one of the fundamental threats to public health (Abdallah & Nizamuddin, 2023; Saraji, Rahbar, Chenarlogh, & Streimikiene, 2023). Developing and deploying an efficient traceability channel has become a need of the hour around the globe. These tracing and tracking requirements need an authenticity system throughout the life cycle of a drug. It starts by tracking the origin of all pharmaceutical ingredients through production, packaging, and transportation to wholesale dealers and pharmaceutical stores (Sylim, Liu, Marcelo, & Fontelo, 2018). In a bigger picture, along with counterfeit and falsified drugs, the pharmaceutical industry is facing several issues in conventional systems (Ali & Kannan, 2022; Dasaklis, Voutsinas, Tsoulfas, & Casino, 2022; Nguyen, Lamouri, Pellerin, Tamayo, & Lekens, 2022):

- Unavailability of the system for real-time verification of provenance for medicines.
- Artificially created market shortage of medicines in epidemic situations.
- Uncontrollable situation of drug prices.
- Disruption in manufacturing and falsified usage details of import Active Pharmaceutical Ingredients (APIs).
- Wrong reporting of adverse drug reactions (ADR) for genuine medicines caused by the consumption of counterfeit drugs.

Loopholes in centralized cloud systems turned the interest towards decentralized and distributed blockchain systems (Malik & Alkhatib, 2021). The tracing capabilities of blockchain represent a novel manifestation of supply chain tracking solutions. It constitutes a temporally sequenced series of blocks systematically arranged by the computational entities of diverse participants (Azevedo & Gomes, 2023). Within the blockchain framework, the immutability of blocks containing the transactional history among nodes in a P2P network is ensured by applying hash functions (Altaf, 2023; Wang, Duan, & Zhu, 2018).

Blockchain technology can be integrated as an embedded web layer to facilitate various functionalities, including but not limited to payment processing, currency exchange, token reception and distribution, digital asset transfers, and the execution of smart contracts (Wang, 2022). In particular, distributed ledger technologies provide improved control of data by providing increased supply chain transparency using blockchain Saberi, Kouhizadeh, Sarkis, and Shen (2019), privacy by utilizing distributed technologies (Nawaz et al., 2019), ownership incorporation by enabling blockchain-based solutions (Nawaz et al., 2020), and leveraging blockchain as a security measure (Killer, Rodrigues, & Stiller, 2019).

Thus, Blockchain technologies can counter falsified drugs and all illegal activities through increased traceability of goods (Kordestani, Oghazi, & Mostaghel, 2023). However, distributed-based solutions encounter challenges related to high variability in structural requirements for each entity involved in supply chain solutions (Karuppiah, Sankaranarayanan, & Ali, 2023). Scalability and reliability issues due to complex requirements and large-scale implementations (Pandey et al., 2023), integration with existing conventional solutions based on dispersed technologies and interoperability challenges.

1.2. Our contribution

The main motivation of our proposed system is to answer the above-mentioned challenges in conventional and blockchain-based supply chain solutions. Based on the findings, we propose *a modular distributed blockchain-based solution utilizing hyperledger sawtooth framework "PHTrack"* to address the multifaceted above-mentioned challenges encountered in distributed supply chain solutions. Its highly modular structure enhances supply chain operations while accommodating the unique requirements of each participating stakeholder.

- PHTrack addresses the solutions that stem from the substantial divergence in structural and industrial requirements among the various entities participating in the drug supply chain traceability systems.
- It addresses interoperability challenges by fostering a cohesive and collaborative environment among the diverse stakeholders in the drug supply chain ecosystem.
- It resolves scalability issues by providing a robust foundation capable of supporting large-scale industrial supply chain operations by utilizing a highly modular structure, hyperledger sawtooth.
- It eases the integration process with pre-existing systems, often employing different technologies, enabling a smoother transition to blockchain-based solutions.
- The design of PHTrack is geared towards minimizing resource consumption throughout the process, notably within the blockchain hyperledger sawtooth node, while ensuring the privacy and security of participating entities.
- It incorporates quantum secure off-chain communication for P2P communication.

To ensure the feasibility and usability of the proposed PHTrack system, We put it in a real-time testbed environment. To safeguard transaction execution against post-quantum attacks, we employ post-quantum-based data sharing and authentication schemes using TLS-based secure communication. Based on the author's understanding, the proposed framework represents one of the first comprehensive solutions utilizing hyperledger sawtooth, offering real-time provenance capabilities.

2. Background and related work

Regulatory bodies like the FDA have introduced rules like the Drug Supply Chain Security Act (DSCSA), a law to tackle the problem of counterfeit drugs (Commissioner, 2023). They aim to create a transparent supply chain to prevent counterfeit drugs from entering the market. The DSCSA, enacted in 2013, was a response to a nationwide fungal outbreak caused by contaminated steroidal injections. It mandates that all entities involved in the pharmaceutical supply chain, including manufacturers, distributors, repackagers, and pharmacies, must provide detailed transaction histories and statements, known as T3 information, to the next party in the chain. This information helps verify the authenticity of the product and ensures that it has been handled by authorized trading partners. It must be retained for at least six years after the product is received.

2.1. Non-distributed ledger technologies

Several non-distributed methodologies were presented in different studies to counter drug counterfeit problems. Authors in King and Zhang (2007), Onieva et al. (2015), proposed RFID-based architecture to create a drug supply chain resistant to counterfeit drugs. They also present a method for finding RFID events more efficiently and discuss the requirements needed to ensure the authenticity of a product using RFID technology. The proposed components communicate using technologies such as Bluetooth and Wi-Fi to provide real-time tracking and tracing, along with incident reporting. NFC tags-based systems were presented by Alzahrani and Bulusu (2016) that can only be

Table 1
Perspective mapping of Blockchain as an Entity for supply chain solutions tracking and counterfeit detection.

Sr. No	Entity	Relation	Entity	Perspective
1	Blockchain	*consists of*	Blocks	Distributed Ledger
2	Blocks	*contain*	Header	Chain Records
3	Blocks	*contain*	Body	Transactional Records
4	Blocks	*contain*	Reference	Distributed Trust
5	Blockchain	*maintains*	Historical Record	Timestamped Blocks
6	Historical Records	*preserves*	Irreversibility of Record	Provenance
7	Irreversibility of Record	*maintains*	Transparency	Reliability
8	Transparency	*uses*	Pseudonymity	Anonymity
9	Blockchain	*includes*	Shared Database	Distributed Trust
10	Shared Database	*secures*	P2P Transmission	Validity
11	P2P Transmission	*includes*	Encrypted Transmission	Integrity

scanned once, thus preventing the duplication of these tags and the introduction of counterfeit drugs. Authors in Meng, Liang, Xu, and Li (2022) combine NFC tags with a lightweight authentication protocol. This protocol allows for the updating of NFC tags. Once a tag is authenticated by the anti-counterfeiting server, the user receives the actual drug data.

Recently, authors in Valizadeh et al. (2023), present a solution for improving the vaccine supply chain to overcome obstacles in the public vaccination program based on government and organizational concerns. To achieve this, a strong two-level optimization model is suggested. Findings of the hybrid model discussed in Khan, Gupta, Gunasekaran, Mubarik, and Lawal (2023) can help decision-makers and managers in the healthcare sector develop strategies to improve their supply chain performance. Authors in Aytekin, Görçün, Ecer, Pamucar, and Karamaşa (2023) present fermatean fuzzy sets-based optimal selection criteria of pharmaceutical supply chains by the healthcare industry. Decision-makers can use the proposed model as a guide to evaluate their capabilities and improve their skills. The sensitivity analysis results show that the proposed fuzzy fuzzy-weighted anticipatory System (FF-WASPAS) approach is a robust and practical framework.

Despite the benefits of this semi-centralized or centralized architecture, which improved the efficiency of drug supply chains, there are still challenges to address. Integrating this with existing systems is difficult, and all trade partners must also subscribe to this system. Centralized authorities are more susceptible to security threats and data manipulation. With an increase in the number of requests, the system's response time is severely affected (Nguyen et al., 2022). Information fragmentation is also a significant issue, as it does not provide transparency into the supply chain, leading to many discrepancies. Auditing such systems is also challenging, and the cost of deployment and maintenance is high. Therefore, more alternatives that take advantage of the latest technological advancements, such as distributed ledger technologies (DLTs), should be explored.

2.2. Distributed ledger technologies

The first successful DLT application was Bitcoin, which manages digital assets to solve problems of double spending and anonymity issues (Nakamoto, 2008). Blockchain-enabled solutions leverage different DLT frameworks, and some of them are designed for specific domains. Some frameworks are good for applications requiring permissionless architectures, and a few are specifically designed for permissioned networks. Permissionless blockchain solutions are publicly available for everyone to join, which creates scalability and performance issues (Liu, Wu, & Xu, 2019). For example, the transaction rate of bitcoin is limited to 7 transactions per second, which makes it incompetent to handle high-frequency trades. Furthermore, in permissionless networks, the transaction confirmation rate increases exponentially as the network expands. Along with the performance, it creates transaction cost issues. Due to the above-mentioned issues, many observers believe permissionless networks are unsuitable for large-scale non-financial applications such as supply chain solutions (Wamba & Queiroz, 2020).

In contrast to permissionless networks, permissioned blockchain networks identify each node, and administrator nodes are capable of removing malicious nodes (Helliar, Crawford, Rocca, Teodori, & Veneziani, 2020). These network models improve performance throughput by using more adaptive consensus protocols like Practical Byzantine Fault Tolerance (Xu et al., 2021), side chains (Singh et al., 2020), and blockchain-based edge-computing solutions (Nguyen Gia, Nawaz, Peña Querata, Tenhunen, & Westerlund, 2019). In recent years, researchers proposed various permissioned blockchain frameworks such as ethereum (Buterin et al., 2013), EOS (Grigg, 2017), hyperledger (Androulaki et al., 2018), and ripple (Benji & Sindhu, 2019). Permissioned blockchain networks are highly suitable for supply chain solutions and can be customized according to business needs and requirements. They support transactional-level privacy and network-level transparency. In Table 1 perspective mapping of blockchain as an entity for supply chain solution is presented. However, it is worth noting that each framework may have its strengths and weaknesses according to drug supply chain solutions. For instance, ethereum is focusing on Layer 2 rollups, a technique that can support many transactions per second. In Musamih et al. (2021), ethereum blockchain is utilized along with off-chain storage to make tracking products easier in the pharmaceutical supply chain. The proposed method ensures the origin of data, removes the need for middlemen, and provides a secure, unchangeable history of transactions for everyone involved. Dwivedi, Amin, and Vollala (2020) proposed and developed a smart contract algorithm using directed graphs with six states and six actions. In addition to performing strong key management in smart contracts, it also achieves reasonable performance in terms of computation and communication overheads. The proposed protocol was robust and achieved reasonable performance regarding smart contract performance. Authors in Agrawal and Angelis (2022) proposed a framework and smart contracts to ensure data accuracy and authenticity within supply chains requiring highly accurate and authentic data. The proposed framework has yet to be tested in an industrial setting. Transaction and maintenance costs were not analyzed on the blockchain network. In Abdellatif and Al-Marridi (2020), authors optimize data sharing among participating stakeholders using restricted blockchain using edge computing concept. They proposed a blockchain-based architecture and enabled a flexible configuration to securely share and access medical data between healthcare organizations, enabling the detection of probable epidemics, remote monitoring of patients and quick response times.

2.3. Modular distributed ledger technologies

Wang, Ye, Meng, and Xu (2020) undertook an examination of the four predominant blockchain platforms, namely Ethereum, Fabric, Sawtooth, and Fisco-Bcos. Their findings indicated that in terms of performance metrics such as latency and throughput, hyperledger sawtooth exhibits superior performance compared to other platforms. The architectural attributes of hyperledger sawtooth were highlighted, emphasizing its simplicity, modularity, and considerable flexibility for customization.

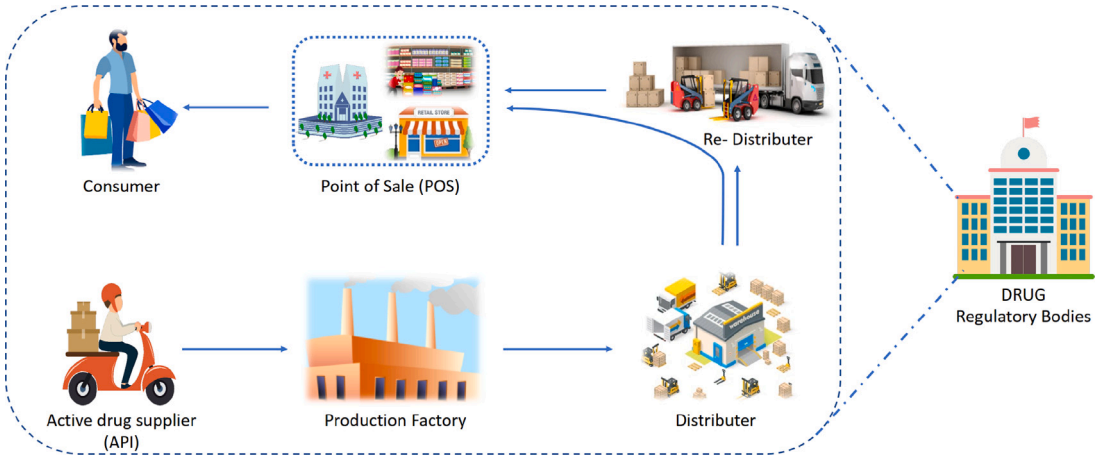


Fig. 1. Drug distribution supply chain and its stakeholders.

Hyperledger frameworks, on the other hand, offer a modular design, allowing for extensive customization. Authors in Sharma and Rohilla (2023) present hyperledger fabric-based application for drug discovery. The proposed application allows organizations to upload, update, view, and verify their contributions. Each contribution is given a unique identifier using a secure hash algorithm, and the design also allows regulatory authorities to issue certificates confirming the ownership of contributions. Uddin (2021) investigated the challenges faced by pharmaceutical supply chains and proposed hyperledger fabric-based solution, but their proposed solution lacks any kind of implementation test-beds which leads to the feasibility of the proposed framework. Work of Vijay and Priya (2022) proposed hyperledger fabric-based agricultural supply chain to enhance the trust between the end consumer and the product they are purchasing, proposed solution *"grainchain"* enables the tracking of the grain from the farmer to the retailer.

Authors in Wisessing and Vichaidis (2022) present an IoT-based seafood supply chain by leveraging hyperledger sawtooth framework. Consumers can track seafood and notify drivers through a seafood supply chain when the container temperature exceeds a specified level. The authors recorded the shipment log as a blockchain transaction by connecting the application, the devices, and the blockchain database. Another study is proposed (Mohit, Kaur, & Singh, 2022) as generic ownership and traceability of products using hyperledger sawtooth. The proposed system can prevent counterfeit goods from entering the supply chain.

Compared to other permissioned frameworks in Table 2, hyperledger sawtooth's event system can potentially lead to more efficient and effective operations in a drug supply chain context. Broadcasting and relaying events across the network enables real-time updates and actions, which are crucial in supply chain management for timely and accurate tracking of goods. Due to its modularity, each participating stakeholder can define its own business logic and interact through transaction families. Transaction families work similarly, such as smart contracts in ethereum. However, unlike ethereum and other distributed networks, each node or application handles and defines its own transaction family rather than using the business logic of a complete system. Transaction states share updates between untrusted stakeholders and are regulated through consensus protocols.

3. Hyperledger sawtooth based pharmaceutical supply chain

As discussed, drug transparency from the point of origin of active ingredients (supplier) to distributors and then to end-users (consumers) requires a complete network framework. In the next section, we introduce all the entities in our proposed system: pharmaceutical supply chain stakeholders, the hyperledger sawtooth framework and its functionalities, REST APIs, and a consensus protocol to validate transactional blocks. Fig. 1 illustrates all stakeholders and their relationships in the pharmaceutical supply chain. and Table 3 describes the role of each participating stakeholder.

3.1. Hyperledger sawtooth framework

Under the broad spectrum of open-source hyperldeger frameworks, hyperledger sawtooth is a private permissioned network proposed and built by the Linux foundation (Dhillon, Metcalf, & Hooper, 2017). Intel designed this distributed ledger specifically for highly modular business logic where governance bodies must customize rules and regulations in a run-time environment while maintaining immutability and privacy. Its modularity separates its core system and the application domain. Therefore, each participating entity can define a set of rules according to its requirements without knowing the underlying business logic of the core system.

In sawtooth, business decisions take place on the transaction processing layer, where transaction families work as models to handle low-level functions like sets of permissions, policies, and storing block states and logs. Transactions are explained by the "transaction family" through which a transaction state changes. Corresponding transaction processors are bonded to the transaction's execution by each entity. This modular structure can handle several consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) (Xu et al., 2021), RAFT (Ongaro & Ousterhout, 2015), Proof of Elapsed Time (PoET) and PoET simulator (Corso, 2019). Core Modules of hyperledger sawtooth are described in detail:

3.2. Consensus protocol

A procedure in which all participating nodes of a network endorse or reject some transactional state is known as a consensus protocol. Several options with different attributes like throughput, finality, size, latency, threat model, censorship resistance, and failure model are available. Distributed technologies build trust among untrusted members through these algorithms. After facing many drawbacks in Proof-of-X protocols, PBFT, RAFT and PoET consensus protocols are proposed with hyperledger sawtooth. The PBFT consensus engine is preferable to maintain fault tolerance and resolve issues in the original chain. Raft is a leader-based consensus protocol that is preferable for a small number of participating nodes. Intel has presented Proof of Elapsed Time (PoET) (Corso, 2019), a promising, novel consensus protocol, and their SGX hardware as a trusted environment. Nevertheless, PoET can also be used without Intel hardware support by using the

Table 2
Comparison of hyperledger sawtooth with hyperledger fabric, iroha, and burrow.

Feature	Hyperledger sawtooth	Hyperledger fabric	Hyperledger iroha	Hyperledger burrow
Ledger Type	Permissioned	Permissioned	Permissioned	Permissioned
Smart Contract Functionality	Transaction Processors	Chaincode	Smart Contracts	Ethereum VM
Consensus Algorithm	Pluggable Framework	Pluggable Framework	YAC	Raft
Governance	Linux Foundation	Linux Foundation	Hyperledger	Not specified
Key Features	Parallel transaction processing, Compatible with Ethereum by Seth, Secure private permissioned network, Pluggable consensus mechanism	Modular framework, Pluggable consensus mechanism	User-friendly interfaces, Modular design, Custom smart contract logic	Ethereum compatible

Table 3
Drug supply chain stakeholders and their roles.

Stakeholder	Role in drug supply chains
Drug Regulatory Bodies:	The World Health Organization (WHO) defines the drug regulatory bodies role as monitoring, protecting, and enhancing pharmaceutical products' safety, efficacy, and consistency. Additionally, they supervise the production, delivery, and storage of prescription drugs to identify and sanction illegal drug production and trafficking.
Active Pharmaceutical Ingredient (API) Supplier:	APIs supply raw materials and other active ingredients to the manufacturer. Various information about the ingredients will be logged on the ledger so that, if a recall occurs, stakeholders can identify the source of raw materials, such as the name, unique code, quantity supplied, and date of supply.
Manufacturer:	To produce prescription medications, pharmaceutical suppliers provide traceable identifiers to suppliers. The manufacturer is responsible for encoding the information related to the drug using coding standards such as EAN/UCC-13, since the manufacturer owns the drug.
Wholesale distributor:	Wholesale distributors ensure that all stakeholders in the supply chain of drugs can purchase drugs efficiently, transparently, reliably, and uninterruptedly. Besides offering wholesale distribution of drugs, they also offer packing, repackaging of drugs, and online ordering services.
Re-distributor:	Distributors manage a complex supply chain, harnessing innovative technologies to ensure safe, secure, and efficient delivery. The next step is initiating the distribution process after wholesale distributors. The distributor will pack and transfer the drug lots to the concerned retailers.
Retailers:	Pharmacies work as retailers, and according to estimates, pharmacies monitor about 70% of the prescription drug industry. They buy drugs in bulk from wholesalers and resell them to end-users (patients). The relationship between pharmacies and patients is close. Based on the point-of-sale requirements, these pharmacies may be self-governing or franchise-based.
Consumers:	Consumers are also included in this supply chain as they buy drugs from pharmacies. Consumers are those actors in the proposed solution who have the right to query the ledger. Consumers can scan QR codes from their mobile phones and see the complete history of transactions and events for the specified drug.

PoET simulator with hyperledger sawtooth. This protocol stands out for many reasons. It is considered one of the most robust implementations of the Proof-of-X protocol and comes as a part of the sawtooth project. Furthermore, it is highly parameterizable, unlike the bitcoin protocol. It is also a currency-independent protocol, which makes it best suited for use cases without financial transactions. As it comes as a suit with a sawtooth, its working environment follows the sawtooth structure:

- Validator node requests for a waiting time from an enclave (trusted module).
- Enclave assigns waiting time randomly to each validator.
- Leader is elected by checking the validator with the shortest wait time "CreateTimer" function creates a timer which guarantees the creation of transaction blocks by an enclave.
- Validator can claim leadership after finishing the allocated waiting time.

3.3. Data model

The architectural design of the data model incorporates a sequentially arranged collection of transactions, logs for transactional activities, and a distributed framework for data storage to maintain the resultant states. The management of transaction serialization is facilitated by deploying a Radix Merkle Tree structure (de Ocáriz Borde, 2022). Each participating node is equipped with a transaction processor and is allocated a discrete namespace for implementing its proprietary business logic. Within a sawtooth ecosystem, a transaction processor functions analogously to smart contracts within the ethereum platform. The serialization schema offers considerable adaptability and can leverage decentralized storage mechanisms, both on-chain and off-chain, to preserve batches of committed transactions chronologically. Each data batch comprises multiple transactions, a timestamp, the index hash of the previous batch, and a Merkle root to authenticate the integrity of the batch data. The aggregation of transactions into a single data batch occurs at arbitrary intervals. Upon the amalgamation of several data batches, a data block is constructed, with the timing parameters being determined by the business logic. Each participating entity is free to select any decentralized storage system, such as Firebase (Paul, 2023), Filecoin (Vakilinia, Wang, & Xin, 2023), or the Interplanetary File System (IPFS), based on their specific business requirements.

Every stakeholder has the option to integrate their individual off-chain storage solution. Sawtooth's utilization of off-chain storage systems offers distinct benefits, provides cost-effective scalability and efficient data processing for less sensitive information. This bifurcation

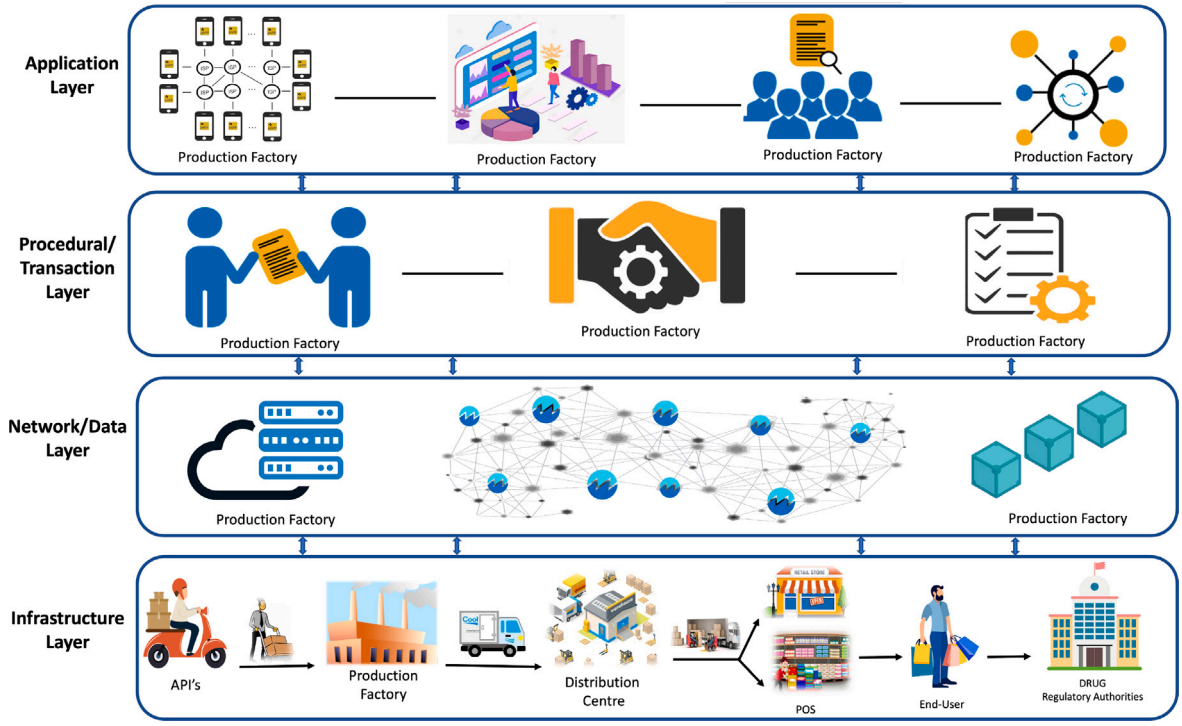


Fig. 2. Layered structure of sawtooth based Supplychain traceability framework PHTrack.

allows for the secure submission and validation of requests, maintaining the confidentiality of transactional data while catering to the specific needs of various stakeholders. Moreover, the approach aids in adhering to sawtooth's business rules functionality, ensuring a robust, scalable and flexible solution.

3.4. Execution model

The highly flexible structure of hyperledger sawtooth supports the running and compilation of code as docker images. Docker images are simply chain codes which can interact hyperledger's back-end via predefined interfaces. It supports parallel executions of chain codes and transactions in each node. The transaction processor must verify each state and transaction before adding it to the data batch. Moreover, each participating node can connect to other miners, validators, and light nodes via some RPC-like mechanisms. Third-party interfaces and applications are built on top of the chain and can connect the application domain to the core-level module and vice versa. The REST API allows the client to communicate with the core system module "Validator" using HTTP/JSON standards. This pragmatic RESTful API provides a simple, language-neutral interface to submit transactions and read/write requests. It works as a lightweight layer on top of sawtooth's internal ZMQ communication, so it does not require any authentication and passes the message requests to the validator for signature verification. It uses the validator component as a black box, which can only send requests and get the required result without knowing the internal system logic.

4. PHTrack: Hyperledger sawtooth based pharmaceutical supply chain

In this section, we described our proposed system, PHTrack, in detail by highlighting its architecture, system flow, and deployment to enable telemetry of the pharmaceutical supply chain and provenance of drugs.

4.1. PHTrack: System architecture

PHTrack leverages hyperldeger sawtooth technology to provide on-chain governance to the drug regulatory authorities. It provides central authoritative controls and offers better scalability, transaction efficiency, immutability, interoperability, highly modular, fine-grained traceability, and run-time upgradation of the consensus protocol. It provides on-chain governance by using dynamic consensus protocols and provides permissioning features. Each stakeholder possesses its transaction processor and can run its business logic via chain codes, side-chain decentralized storage, and consensus protocol. The PHTrack framework prefers the PoET consensus protocol. It offers the solution to the Byzantine Generals' Problem by using a trusted environment. PoET is unlike the traditional lottery-based protocol, where the chances of winning are proportional to the amount of computational work. Instead of spinning the computational load, it uses the element of randomness to control the block commitment. PoET elects the individual nodes to execute requests at a prescribed target rate. It is similar to Proof of Work but replaces huge computation with a cheap random wait.

To create a trusted network, we use a peer-to-peer network of nodes as a validator, which provides journal block management and identity management system services. It manages *User_ID* and authenticates all participating nodes (modules) by issuing *registration_certificate*. The high-level architectural diagram of the proposed framework PHTrack is depicted in Fig. 4 and layered structure of proposed system is defined in Fig. 2, highlighting all the major system modules involved. Each node represents one complete module (stakeholder) of a system. The number of compulsory and optional components involved in the constitution of each node. Compulsory items are P2P sawtooth environment, transaction processor, consensus engine, validator, and REST API services to interact with the system. Optional items include side chains, storage systems, client applications and their inter-communication protocols. A highly modular structure consists of all stakeholders involved in the pharmaceutical supply chain, a sawtooth core system module, an application domain, a distributed storage system, and clients. The REST API

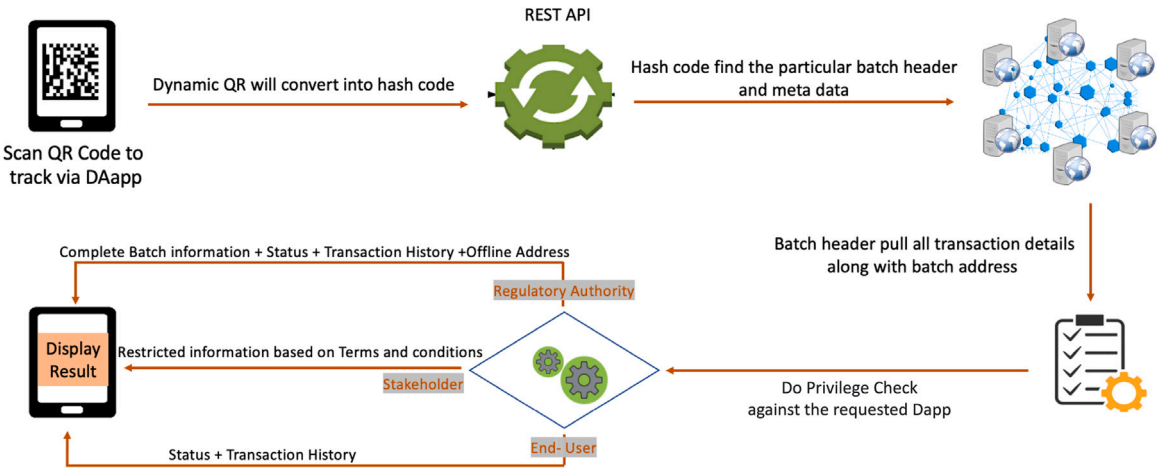


Fig. 3. Process to Track backward using dynamic QR code.

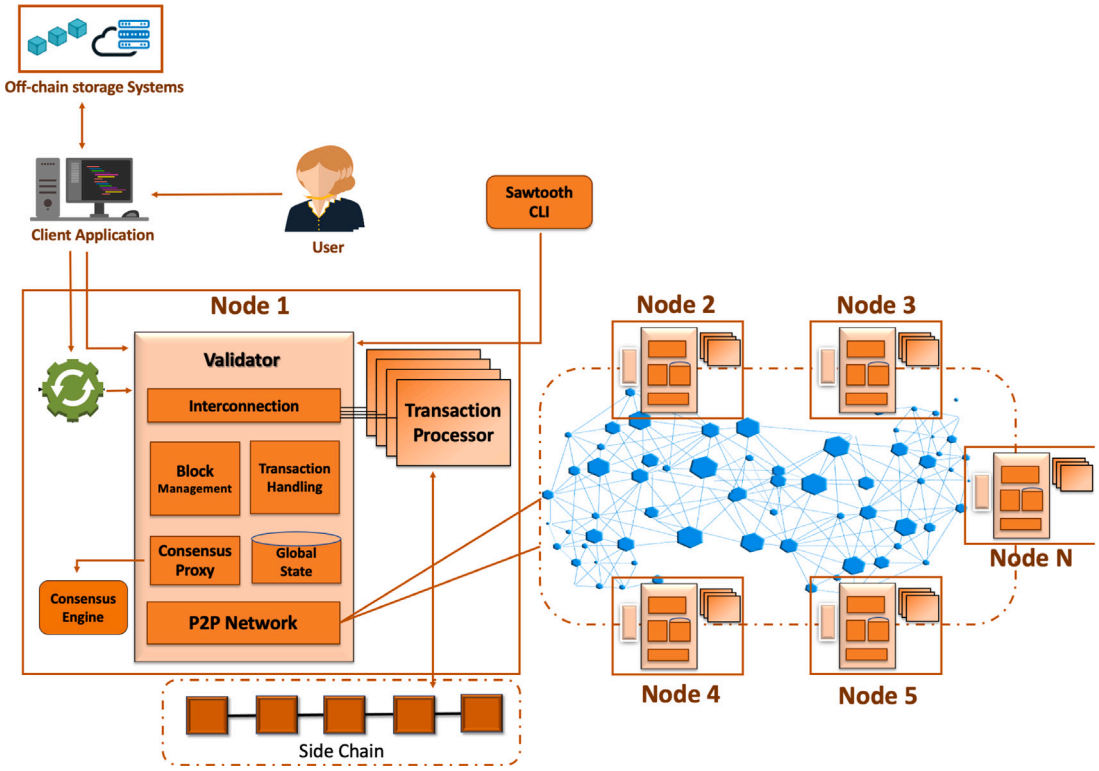


Fig. 4. A high-level architecture for the proposed PHTRACK sawtooth-based system for Drug supply chain.

develops communication between core system modules and application domains. Fig. 3 shows how clients use it to submit transactions and read/write requests to the validator and its associated components. Each stakeholder node represents some sort of node category:

- Validator node: Each stakeholder is represented as a validator node. It is responsible for authorizing transaction requests related to it after getting approval from the transaction processor. It does not need to participate in other network transactions (other stakeholders' transactions).
- Leader node: The leader node is responsible for committing a batch of authorized transactions after random time interval *t*.
- Client node: Clients can submit read requests. Customers can track drug information from the origin to the point of sale by scanning dynamic QR codes.

Chain codes handle and deploy regulations, business logic, and transactions. These are the central and essential components for handling peer-to-peer networks and managing the complete system flow. Moreover, accessibility roles are different for each stakeholder, defined and executed via chain codes. Dynamic QR codes are used to track drug lots. When creating a QR code for each drug lot, all of the drug lot's transactional history is saved in the QR code, which updates all of the event information to their side chain and broadcasts the hash and metadata of the saved block in the network. Each participating stakeholder can request access to the information saved in the block. The drug regulatory bodies and the owner of the data block own the validating rights.

4.1.1. Core system module

The core system module consists of a validator node, which includes a single validator, a REST API service, a consensus engine, a state

database, a peer-to-peer network, and one or more transaction processors. The transaction handling module is inside the validator node, which handles messages, transaction batches and blocks, validation, and publishing after getting approval from the specified transaction processor. One data batch consists of a random number of transactions, and one datablock consists of databatches created at a specified time T. Multiple transactions work as an atomic unit in a batch. The validator rejects the complete transaction batch by rolling it back to the previous state, even if a single transaction failed to complete the validation process. Transaction batches are wrapped in batch lists. It allows parallel transaction execution and validation. Each pharmaceutical supply chain stakeholder works as a network's validator node. Furthermore, the validator is also responsible for peer-to-peer communication with other validator nodes (stakeholders) on the network. REST API services are used to communicate with transaction processors and clients.

4.1.2. Application domain

The client is responsible for creating and signing transactions, combining them into batches and blocks, and submitting them to the validator through the REST-API module. The client application uses node.js based application, which provides a web user interface for the user to interact with. Transaction families are used to write business logic and policies. Transaction families separate the transaction rules and content of core functionalities. A transaction family can be a simple set of rules to change the state of a system or a complete set of logic defined by the stakeholder. These are smart contracts written in any supported programming language, used to automate the entire system. We use python3 and Go to write transactions. The transaction processor and client use the same data model, serialization, and addressing scheme. Setting transaction families enables participants to agree on prescribed network policies. Transaction families authorize the transaction requests by other validator nodes and the clients. A client creates a transaction and submits it to the validator. The validator then authorizes it after getting approval from the transaction processor. Each node is assigned one authorized key, which is used by the validator to authorize each requested transaction. After getting consensus approval, any validator node can act as a leader to approve a transaction batch.

4.2. PHTrack: System flow

To track and trace counterfeit drugs, our proposed system flow is described in two ways: track forward and backwards. Each stakeholder works as a validator node, which defines its working policies independently without leaning on the core system. To join a network, every stakeholder must implement online system requirements and write transaction policies based on their business logic. A stakeholder can start their validator node and associated components after getting approval from the drug regulatory bodies (Leader). To achieve traceability, it is essential to have two separate and asynchronous transaction flows. Transaction flow describes the physical movement of the original drug and the associated information flow going from one stakeholder to another. 'Track backward' is the primary workflow, which allows tracing the origin of active ingredients, manufacturer, wholesale distributor, and retailer, as well as the location of the drugs on the PHTrack. Drug tracking refers to tracking the drug's current location in the supply chain and its related information in the current transaction process until the drug reaches its end-user (patient).

4.2.1. Track backward

Using Track backward flow, participants can access the transaction record at any time, ensuring the process's accuracy, integrity, and transparency. To track backwards, rules and regulations are defined for each stakeholder, depending on the proportionality of information revealed. Access control transaction rules are implemented to regularize them throughout the system. Decentralized applications (DApps) are deployed at point-of-sale units. Consumers can scan QR codes to track back all the information about the required drug. The complete tracking process is depicted in Fig. 3. In this process, Sources of active ingredients (supplier), manufacturers (owners of drugs), a chain of transfers (transfer activities), wholesale distributors, re-distributers and POS units are included in the transparency of details. The sold status of the drug appears as the QR code scanned at retail pharmacies at the time of the transaction, and the transaction details are uploaded along with the location data.

4.2.2. Track forward

Track forward-protocol is implemented to track all the transaction details of the drug by all stakeholders. Access control methods define the attributes of drug transparency for each stakeholder in a system. Transaction families are used to implement access control methods via smart contracts managed by leader nodes. Transaction rules are implemented in a modular approach based on the nature of tasks they will handle and initialize, such as registration, transactions, tracing, and tracking. Procurement of dynamic QR codes is available on a timely basis for each drug manufacturer. End-users or regulatory bodies can trackback any drug they need. An end-user can scan a QR code to display all the transactions performed on this drug during its complete life cycle. Specific access control methods, defined for each stakeholder, add additional layers of privacy and security to a system.

1. **Drug Regulatory Bodies:** Drug regulatory bodies work as administrator nodes, which can govern the whole system.
2. **Active Pharmaceutical Ingredient Suppliers (APIs):** Each API supplier has its validator node and associated components such as transaction processors. It can only track its orders, manage transactions with the manufacturers, and request additional details from the drug regulatory bodies. It can use off-chain distributed storage for additional storage requirements.
3. **Manufacturers:** Manufacturers work as independent validator nodes. They can access the statistics of APIs and associated distributors by defining the set of transaction families. They need authorization from other collaborative nodes.
4. **Wholesale distributors:** Wholesale distributors can only access the drug details of drugs they will distribute and those already distributed.
5. **Re-distributors:** Re-distributors can track the ongoing deliveries booked by them and their transaction status.
6. **Point-of-sale Unit:** Point-of-sale units have client applications with access to writing a sale transaction. They are required to scan a QR code to update the status of the drug as sold, along with the details of the POS unit, date, and time.
7. **End-Users:** End-users can check a drug's status, including its date of manufacturing, expiration date, and manufacturer, by simply scanning its QR code.

5. Implementation and performance analysis

In this section, we introduce our research problem in the context of service optimization. PHTrack, represents a drug traceability system which comprises α^x individual participating nodes. The number of parallel transactions generated by each participating node will be blocked together in databatches (db), and the size of databatch is denoted as $S_{txn}(db)$. Each transaction within a blockchain databatch encompasses multiple attributes that collectively determine its size and can be expressed as follows:

$$S_{\text{txn}}\ (db) = \gamma_{\text{flag}}\ + \Sigma_{t=t_{\text{initial}}}^{t_{\text{elapsed}}}\ \left(cnt_{\text{in}}\ + cnt_{\text{out}}\ \right)$$

$$+t_{\text{elapsed}}\ + \alpha$$

where α is network id of registered entity node, γ_{flag} is flags data, t_{initial} is initial time, cnt $_{\text{in}}$ is initial count of input values, cnt $_{\text{out}}$

is output count list, and t_{elapsed} is total elapsed time. If the number of transactions in a databatch db are $n_{txn}(db)$, then the total size of transaction data in a databatch can be given as:

$$S_{txn}(db) = n_{txn}(db) \cdot S_{txn}(db)$$

Each databatch, in addition to the transaction data, also carries some metadata. This metadata includes elements like a databatch header, the network id of the registered entity node, a random wait time, elapsed time, merkle tree, and a time stamp. As such, the size of a databatch can be determined based on these factors.

$$S_{\text{hdr}}\ (db) = h(previousblock) + h(\alpha) + h(merkletree)$$

$$+h(totalelapsedtime) + h(randomwaittime) + h(timestamp)$$

In this context, h symbolizes the hash function employed in the hyperledger sawtooth framework. The term 'previous databatch' pertains to the hash value of the databatch preceding the current one in the network. 'Merkle tree' signifies the hash value encapsulating all the transactions in the databatch. The 'target formula' is applied to compute the target value required for mining a fresh databatch. 'Nonce' is an acronym for 'Number Only Used Once', while 'timestamp' marks the precise time the databatch was generated. Consequently, the comprehensive size of the metadata for databatch db can be defined as:

$$S_{md}(db) = S_{hdr}(db) + S_{ctr}(db),$$

where $S_{cnt}(db)$ signifies the size of transaction counts. Every databatch in a network encompasses both transaction data and its corresponding metadata. Hence, by utilizing the previous four equations, the cumulative size of the databatch db for the network β_i can be expressed as:

$$S(db, \beta_i) = S_{txn}(db) + S_{md}(db),$$

As previously explained, a databatch is composed of numerous transactions. The duration required for a network to achieve consensus on a specific databatch is contingent on the complexity of the consensus along with network latencies. Where a databatch db is published, it undergoes a propagation period within the β_i. Consequently, the propagation delay for transmitting a databatch db on network β_i can be characterized by:

$$t_p(db, \beta_i) = t_c(db, \beta_i) + t_{pr}(db, \beta_i) + t_q(db, \beta_i)$$

Where, $t_c(db, \beta_i)$ = network delay, $t_{pr}(db, \beta_i)$ = execution delay, and $t_q(db, \beta_i)$ = wait delay. In addition to the turnaround delay, the total elapsed time taken for a databatch to complete includes propagation delay time, contributing to the overall delay before confirmation. This turnaround delay, $t_s(db, \beta_i)$, can be represented by:

$$t_s(db, \beta_i) = t_{cs}(db, \beta_i) + t_{ot}(db, \beta_i).$$

Where $t_{cs}(db, \beta_i)$ denotes the encryption plus consensus processing time, and $t_{ot}(db, \beta_i)$ represents other potential delays, such as synchronization delay or network delay. Consequently, employing the equations mentioned above, the comprehensive network latency $T(db, \beta_i)$ required for the generation of a data batch can be formulated as follows:

Where, $t_{cs}(db, \beta_i)$ denotes the encryption plus consensus processing time, and $t_{ot}(db, B_i)$ represents other potential delays, such as synchronization delay or network delay. Consequently, employing the equations mentioned above, the comprehensive network latency $T(db, \beta_i)$, for a databatch to be generated can be given by:

$$T(db, \beta_i) = t_p(db, \beta_i) + t_s(db, \beta_i).$$

Consequently, to attain optimal performance within a network, the mathematical representation of the optimization problem can be expressed as follows:

$$\min T(db, \beta_i)\ \&\ \max S(db, \beta_i)$$

Table 4
Hardware and software specifications.

Component	Description
Framework	Hyperledger Sawtooth
Operating System	Ubuntu 18.04.6 LTS x64
Server Specification PC	Core i5-6300U @ 2.5 GHz
AWS Server specs	EC2 instance: t2.Large
Client Application	Nodejs Server
Runtime Environment	Docker-compose v.1.29.2

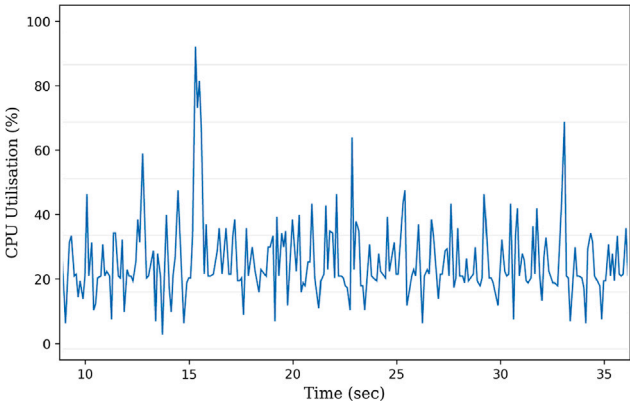


Fig. 5. CPU Utilization in terms of CPU percentage.

Thus, this optimization problem provides a mathematical foundation for determining the most efficient combination of databatch size, transactions per second (tps), resource utilization and network resources while ensuring the reliability of transaction commitment. To evaluate the platform performance, two separate testnets of the proposed PHTrack framework were designed and deployed with the specifications written in Table 4. Permissionless PoET consensus engine in dev modes is used. A Client App was used to implement the application layer. Nodejs was used as the client-side execution engine and docker containers for the server side.

In our testnets, the complete hyperledger sawtooth system was installed and initiated on a Linux-Ubuntu operation system as a local host communication. An EC2 instance of AWS was used for separate server communications. Each component of sawtooth, including transaction processors, events, chain codes, and different nodes, was launched as docker containers. Sawtooth is implemented using Python embedded in docker images. Each node is only responsible for validating transactions related to it and committing them in batches after validation by the validator. In addition to the REST API, transaction processor, validator, and data from blocks and states, every validator node has several containers.

Each stakeholder application has a different interface, which depends on the rights it owns, and leader nodes can access every module and update the entire system. Each validator node can prescribe its own set of rules and define roles for its sub-system modules and off-chain settings. Interfaces can add transactions, accept inputs, retrieve transactions, and log information. Transaction processors are server-side programs that store operations and process transaction submissions according to business logic. Validators run all the validation processes that happen in a node. They manage everything from business logic validation by the transaction processor to consensus validation by the consensus manager. A genesis batch, the first block of the chain, was created by the first validator node. Upcoming data batches append this chain by adding new batches. Any validator node can start the genesis node if it does not acquire any extra authority. All authoritative protocols, terms, and conditions can be added later at any time during the running system via chain codes.

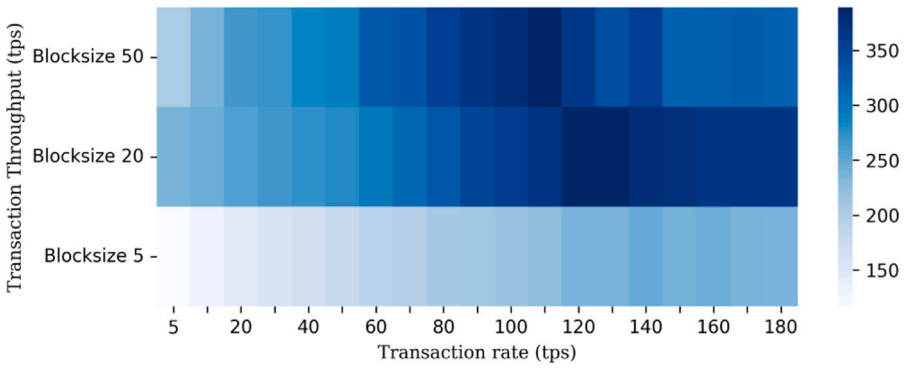
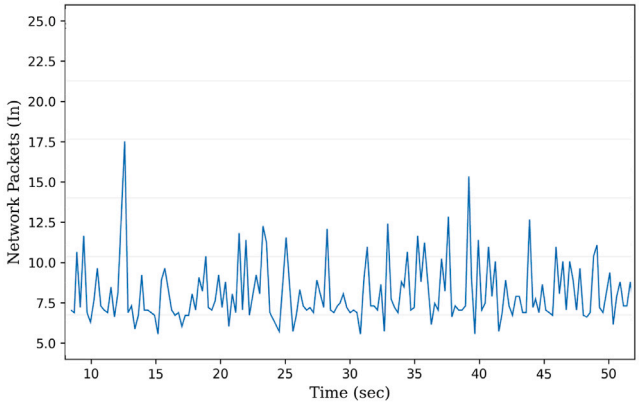
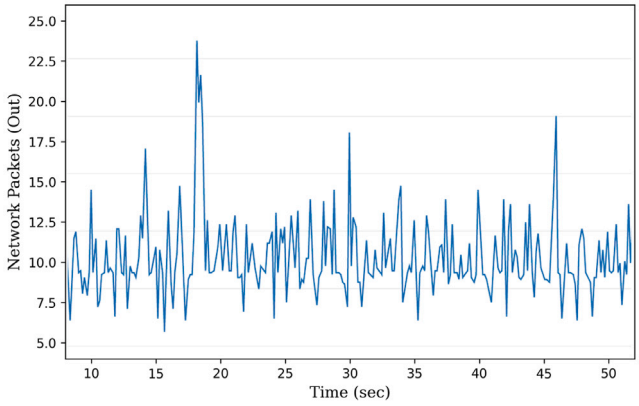


Fig. 6. Impact of blocksize and transaction rate on throughput.



(a) Received number of Network Packet count



(b) Outgoing Network traffic Packet count

Fig. 7. Incoming and outgoing Network traffic Packets.

To determine the business logic for the Traceability System, two transaction processors (TPs) were used, namely stakeholder-registration-TP and transaction-request-TP, and the PoET development mode consensus was used. Successful transaction requests are combined into data batches as shown in Fig. 10. Multiple transaction batches are combined to make one block.

5.1. Impact of TPS and blocksize on latency

Firstly, we evaluated the impact of blocksize by varying the transaction rate (transaction per second, tps) in terms of transaction latency. Transaction rate refers to the number of transactions processed by the sawtooth network within a specific time period T. Latency is defined as the time gap between the transaction submission and completion. The latency L_t is calculated as follows.

$$Lt = \frac{1}{n}\sum_{i=1}^{n}\left(t_{xi} - t_{yi}\right)\frac{1}{T_i}$$

Here, t_{xi} and t_{yi} represent the transaction completion and submission times, respectively, of the ith experiment and Ti denotes the total number of transactions submitted for the ith experiment. It measures the rate at which transactions are submitted to and executed by the network. Transaction latency decreased linearly by decreasing the parallel number of transactions, which can be seen clearly in Fig. 8.

With a low transaction rate, it is easier for the network to process and confirm transactions quickly. Latency tends to be lower in such cases, as there is less competition for block space, and transactions can be included in blocks sooner. However, a high transaction rate means many transactions are being submitted simultaneously. This can lead to increased competition for block space, potentially causing delays in transaction confirmation. Higher transaction rates may result in higher latency due to the time it takes to accumulate and validate transactions for block inclusion.

Proper network optimization and scaling can help mitigate the latency impact of varying block sizes and transaction rates. Techniques such as load balancing, parallel processing, and optimized consensus algorithms can help maintain lower latency even as the blockchain network faces increased traffic. The availability of network resources, such as computing power, memory, and bandwidth, plays a role in determining how well a sawtooth network can handle different block sizes and transaction rates. Networks with abundant resources can handle larger blocks and higher transaction rates more efficiently, resulting in lower latency. We need dynamic adjustment of block size and other network parameters. This adaptability can help balance the trade-off between throughput, block size and latency in response to changing network conditions.

5.2. Impact of transaction rate on throughput

The transaction rate directly and significantly impacts throughput in sawtooth network. Throughput measures the system's ability to process a certain number of transactions within a specified time period. To validate our proposed model, we create three categories of blocksizes and run parallel transactions per second. Fig. 6 depicts that transaction throughput increases rapidly by increasing the transaction rate until it reaches 120–130 tps while using blocksize-20, at which point it stops increasing significantly, and only a slight difference can be seen. These results indicate that bigger blocksizes show better performance throughput until they reach their maximum throughput per block size.

As an average, transaction throughput is higher in blocksize-20 than in 5 and 50, which shows that the more often the consensus algorithm

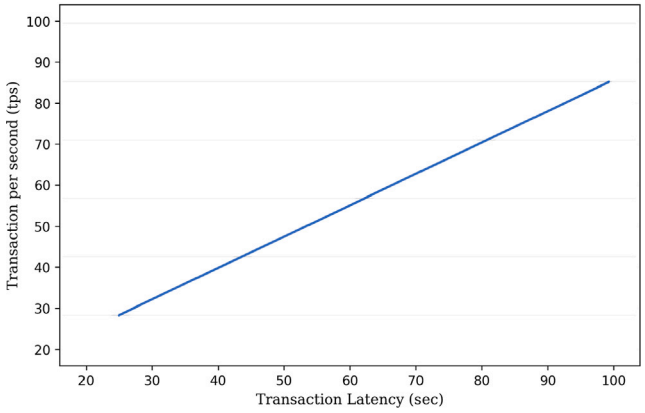


Fig. 8. Transaction latency (sec) increases linearly by increasing transactions per second (tps).

```
----------------------------------------------------------------------
Ran 15 tests in 0.769s

OK
Name                                                    Stmts   Miss  Cover
---------------------------------------------------------------------------
cli/sawtooth_cli/__init__.py                                1      0   100%
cli/sawtooth_cli/admin_command/__init__.py                  1      0   100%
cli/sawtooth_cli/admin_command/config.py                   28     12    57%
cli/sawtooth_cli/admin_command/genesis.py                  66      4    94%
cli/sawtooth_cli/admin_command/keygen.py                   58      7    88%
cli/sawtooth_cli/exceptions.py                              4      0   100%
cli/sawtooth_cli/network_command/__init__.py                1      0   100%
cli/sawtooth_cli/network_command/compare.py               293     57    81%
cli/sawtooth_cli/network_command/fork_graph.py             44      2    95%
cli/sawtooth_cli/network_command/parent_parsers.py         23     18    22%
cli/sawtooth_cli/protobuf/__init__.py                       0      0   100%
cli/sawtooth_cli/protobuf/batch_pb2.py                     25      0   100%
cli/sawtooth_cli/protobuf/genesis_pb2.py                   16      0   100%
cli/sawtooth_cli/protobuf/settings_pb2.py                  45      0   100%
cli/sawtooth_cli/protobuf/transaction_pb2.py               23      0   100%
cli/sawtooth_cli/rest_client.py                            99     74    25%
cli/tests/test_admin_keygen.py                             56      5    91%
cli/tests/test_config.py                                   33      0   100%
cli/tests/test_genesis.py                                 112      0   100%
cli/tests/test_network.py                                  75      0   100%
---------------------------------------------------------------------------
TOTAL                                                    1003    179    82%
```

Fig. 9. Total number of successful commits.

runs, the more often it decreases the overall efficiency of the system but we need to set the limit dynamically according to the availability of the resources. The impact on throughput also depends on the available network resources, such as bandwidth. If limited, increasing the transaction rate may not significantly increase throughput. The transaction rate increases significantly when we move towards 5 to 100 transactions per second and then increases in a non-significant style. Latency can also be decreased by increasing the number of transactions per block. In the case of blocksize-5, the average transaction rate was 306.89 ms, which increased to 270.47 ms by increasing the blocksize to 20 transactions per block. The transaction latency decreases further by increasing the size to 50 transactions per block, the transaction rate comes to 198.68 ms average. The experimental results of

5.3. Network reliability analysis

More than 1000 parallel statements were initialized and tracked to test the system's reliability; as shown in Fig. 9, the system could handle 82 percent of the statements and miss only 179 requests with limited computational resources. These sets of statements include different kinds of commands and events, but missed statements are network-bound only.

Node.js based client was responsible for initiating and deploying a different number of transactions by using *Int-key* transaction processor. These transactions are then sent to the validator through the REST-API module. Peer-to-peer nodes, as well as client applications, use RESt-API to communicate between them. RESt-API uses google protocol buffers to make communication easier, and curl sends data from HTTP to RESt-API. Int-key transaction processor was also used to sign each transaction and combine these transactions into batches. The number of batches is combined to publish one block on the network. CPU and network utilization performance test marks were recorded and analyzed for Amazon AWS instances and personal computer systems. Hardware specifications are described in detail in Table 4. To collect the matrices of PC, cAdvisor (Container Advisor) is used, and a running daemon is used to collect the analytics against each running container separately. 11 virtual cores were used to start the network.

To track the performance metrics of AWS cloud instances, Cloud-Watch was used. We aggregate these performance parameters of running containers and their impact on CPU and network consumption in charts. Fig. 5 describes the CPU utilization in terms of CPU percentage, which shows sudden spikes over time during the parallel number of transaction commits. sawtooth is mainly a network-bound protocol, Fig. 7(a) and 7(b) show the network packet count used during transaction requests and event handling using AWS EC2 instance. Sudden spikes show the network usage during transactions and event handling. The following analysis demonstrates that the suggested system effectively maintains privacy, without introducing any disturbances in the areas of traceability and ownership. Moreover, the integration of privacy measures does not significantly influence the system's performance.

5.4. On and off-chain secure communication

The serialization model of sawtooth demonstrates remarkable flexibility, as it can seamlessly leverage both on-chain and off-chain decentralized storage systems. For on-chain communication, sawtooth's internal ZMQ based communication model does not require any authentication and passes the message requests to the validator for signature verification. In the context of drug supply chain traceability, where numerous industrial entities participate on a large scale, there arises a need for direct communication between two or more entities without involving the entire network. For instance, some participating entities may seek to enhance their functionality by gaining additional insights from others, such as real-time data-driven recommendation systems. These entities have the capability to independently send and receive data within the network through the use of chain codes. Moreover, participating entities can autonomously update their terms and conditions without requiring the involvement of other network members.

To facilitate this off-chain communication within the network, we propose the implementation of a secure communication infrastructure based on Transport Layer Security (TLS) for encrypted data sharing. This approach incorporates post-quantum essential encapsulation methods to ensure the security of private keys and employs digital signature algorithms for authentication purposes. Kyber 768 is utilized as a key encapsulation method for sharing crypto keys over the network and dilithium3 for digital signatures. One of the NIST finalists, Kyber is a family of post-quantum key exchange algorithms. It is designed to establish secure communication channels by exchanging cryptographic keys that are resistant to attacks by quantum computers. Kyber standardized three security levels of 515,768, and 1024. Kyber768 provide NIST security level 3, which is equal to AES 192. This network utilizes kyber768 for key encapsulation before the off-chain key-sharing process. Dilithium signatures help guarantee data integrity by providing a way to detect any unauthorized modifications to the content of a message. This is particularly important in critical applications where even small changes to data can have serious consequences. In industrial and legal contexts, digital signatures are also required to meet regulatory compliance and legal standards. Dilithium provides a secure and legally recognized means of signing digital documents and communications, making it valuable in these settings. Dilithium is employed in communication to ensure messages' confidentiality, authenticity, and

```
{
 - data: [
    -{
     - header: {
          signer_public_key: "0382hed971ws109h87h0bh491dgfe0578fd08ews97c489s34k841deaj1gr480ae",
       -transaction_ids: [
            "83hf0735ow74926cbsj736scg3920al109deh261dbw0ok32bc103cjsoebb863mdn284bhs39fhe0osm283clenwoek30dhr57sbza0917sx0olqwn172owndsl
         ]
       },
    header_signature:"4oeh3764bdkw483gmaq0183hfeoncow901k183uqw3bem65041e5abcfad29306462c1f8d2bc2bb980b0ab1ae5bc04d39457e95abfb60a7e645d
    09d4d592f97f6ee538b1".
     trace: false,
    - transaction: [
        - {
         - header: {
              batcher_public_key: "0382hed971ws109h87h0bh491dgfe0578fd08ews97c489s34k841deaj1gr480ae",
              dependencies: [ ],
              family_name:  "transaction_request"
         input:  [
            "6a0cd88919ee9e9305c5fc7ef277bf805195cf8fc583deb428a32f7f3d6883b76ea4b7255f7dd998cef79518d016eb",
             nonce:  "0x1.73dowu09niq12d478op23+30",
         outputs:  [
                "6a0cd88919ee9e9305c5fc7ef277bf805195cf8fc583deb428a32f7f3d6883b76ea4b7255f7dd998cef79518d016eb"
         ],
           payload_sha512:"2208940ab214e0d4543fa1c087a46015081d067af87eb5be86f359da92a6e608798812582c2606a4853ac6a63ccb6c24a91161f8b390c4a
           1d3e4b89f78b78b8f50fdb7efe53e",
            signer_public_key: "0382hed971ws109h87h0bh491dgfe0578fd08ews97c489s34k841deaj1gr480ae"
       },
```


Fig. 10. Data batches created after transaction.

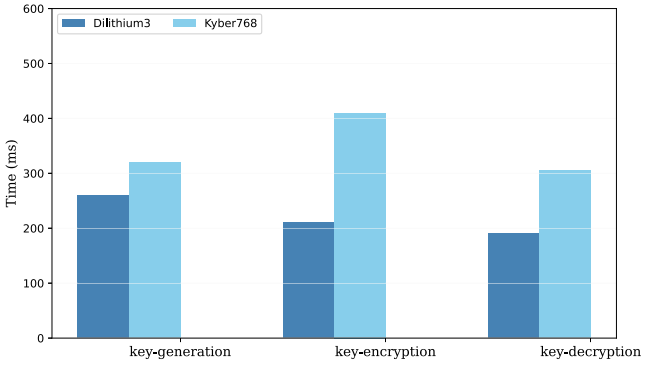


Fig. 11. Latency in (ms) for kyber76 and dilithium3 process.

integrity, especially in a world where the threat of quantum computing looms. Its post-quantum security properties make it a critical choice to secure sensitive and important communications against future quantum attacks. Fig. 11, shows the latencies (ms) we got using kyber678 and Dilithium3 using TLS-based secure communication over wi-fi. In the off-chain communication paradigm, the involved parties will assume responsibility for confirming a transaction (the actual execution) and certifying the agreement. This chain of communication can be executed instantly in comparison to on-chain transactions.

5.5. Security and privacy analysis

Sawtooth's security framework inherits the utilization of policies and roles within the identity transaction family. Policies, represented by sets of key rules, are assessed sequentially, while roles grant specific authorizations for operations and data access. Transaction key permissions further enhance granularity, with roles controlling client access based on the signing public key, extending permissions to specific transaction families (TFs) or entire batches. Additionally, Sawtooth employs challenge-response authorization, requiring nodes to prove their identity through signed nonces, and supports encryption for various aspects, securing data in transit through ZeroMQ with CurveZMQ.

For off-chain communication and storage in distributed places, Kyber key encapsulation algorithm (KEM) with the Kyber public-key encryption algorithm is implemented. 32-octet *cpaseed* is used as input for the key generation process. $cpaPublicKey$, $cpaPrivateKey$, h, and z are variables representing the components needed to derive the private key. The publicKey is derived directly from $cpaPublicKey$, while the privateKey is derived from a combination of $cpaPrivateKey$, $cpaPublicKey$, h, and z. In terms of resource utilization, the performance of post-quantum Key Encapsulation Mechanisms (KEMs) can be compared against elliptic curves implemented in the $OpenSSL$ cryptography library. The results show that, in general, the elliptic curves perform similarly to the post-quantum KEMs, indicating the need for further optimizations to make them more suitable for devices with low resources. However, the performance study can be extended to include all currently competing KEMs, including those with higher security settings and code-based KEMs. Various type of attacks such as multi-certificate attacks, double spending, 51% Attacks, phising, sybil and quantum Computing Threats have been eliminated by leveraging sawtooth transaction processors, PoET consensus and post-quantum cryptography.

On the privacy front, PoET is utilized to ensure permissioning capabilities enable the creation of private networks with distinct access controls, safeguarding sensitive transaction patterns and confidential information from unauthorized exposure. Core transaction families, including identity transaction family, facilitate identity management and on-chain permissioning. The platform's modular design enables the configuration and extension of these security and privacy features, providing a robust foundation for secure permissioned blockchain networks tailored to enterprise needs.

6. Discussion

The practice of counterfeiting drugs is widespread, which undermines the confidence of end-users in the drug industry. In addition to being time-consuming, costly, and cumbersome, legacy drug verification systems pose many security risks. In this article, we investigated the challenge of drug traceability within drug supply chains and demonstrated its importance in preventing counterfeit drugs. To track and trace drugs in a decentralized way, we have developed and evaluated PHTrack, a distributed ledger-based solution leveraging hyperledger sawtooth for the drug supply chain. By using cryptographic principles embedded in permissioned blockchain technology, we achieve tamper-proof logs of events within the supply chain and

automate the recording of events in the hyperledger sawtooth environment for access by all participating stakeholders. The highly modular sawtooth structure enables each stakeholder to define their system specifications based on their requirements. PHTrack provides system transparency, immutability, and reliability, and enables trust in multiple stakeholder systems by eliminating third-party services. Enabling traceability and tracking all transactions in the drug supply chain lifecycle can provide a complete picture of each transaction, including the date, time, location, and stakeholders involved in the operation.

6.1. Theoretical contributions

Integrating Hyperledger sawtooth in the drug supply chain brings about several theoretical implications. Firstly, the decentralized nature of hyperledger sawtooth ensures that no single entity controls the entire supply chain, fostering increased trust among participants. This decentralization aligns with theoretical perspectives on decentralized systems and trust within supply chain management. Using the unique PoET consensus algorithm in sawtooth enhances the security and efficiency of transaction validation, a critical aspect in maintaining the integrity of transactions within the drug supply chain. Additionally, the immutable ledger of sawtooth ensures transparent and traceable records of all transactions, crucial for verifying the authenticity of pharmaceutical products and preventing the infiltration of counterfeit goods into the supply chain.

Furthermore, smart contracts within sawtooth enable automating and enforcing predefined business rules, aligning with theories emphasizing automation and efficiency in supply chain management. The blockchain technology underlying sawtooth also contributes to security and immutability, creating a tamper-resistant system that reduces the risk of counterfeit drugs. The theoretical underpinning of a DLT system involves ensuring data consistency and synchronization across multiple participants, reducing discrepancies and potential errors in the pharmaceutical supply chain. These theoretical implications highlight the potential for enhanced transparency, security, and efficiency in the pharmaceutical supply chain by adopting hyperledger sawtooth.

6.2. Managerial implications

Adopting blockchain technology, specifically hyperledger sawtooth, has significant managerial implications for each participating stakeholder in drug supply chain. Utilizing hyperledger sawtooth can lead to substantial cost savings for consumers by removing intermediaries, thus reducing administrative expenses. Faster payment processes and minimized errors also contribute to economic efficiency at various levels, including API suppliers, manufacturers, re-distributers, and retailers. Operational efficiency can be greatly improved by automating transaction recording and verification, freeing staff to focus on strategic tasks. The transparency and traceability provide detailed recording and tracking of transactions, which enhances risk management by facilitating the early detection of irregularities for regulatory bodies.

Hyperledger sawtooth's ability to provide an immutable record of transactions is particularly beneficial for industries with stringent regulations, like pharmaceuticals, aiding compliance efforts. Managerially, the reduction in time and costs associated with traditional supply chain management, such as paperwork processing, is significant. The system's automated verification processes ensure that pharmaceutical batches meet necessary conditions before moving through the supply chain, increasing efficiency and ensuring adherence to quality standards and regulatory requirements. Real-time monitoring capabilities of hyperledger sawtooth allow for better tracking of drug movement from manufacturing to delivery, improving inventory management and allowing for prompt responses to potential issues.

6.3. Conclusion and future work

Our proposed system consists of a private permissioned hyperledger sawtooth framework which provides the complete system flow. The proposed network is divided into core system modules and application modules. Stakeholders play a key role in the sawtooth network as participants, and their roles within the supply chain determine their roles. Additionally, they can access on-chain resources such as logging and history information to track transactions. Furthermore, they can access decentralized data such as images and complete information logs. In addition, it offers low-cost off-chain storage to ensure scalability and immutability by storing supply chain transactions in hashed form. It is important to keep the integrity of data, so for each uploaded file, the server hashes it and stores the hashes on the blockchain. Chain codes can be used to get the hashes from the blockchain. We employ smart contracts and chaincodes to streamline the verification and validation of PHTrack transactions, covering the entire journey from the initial acquisition to the delivery process. This guarantees the seamless exchange of transaction information among all participating stakeholders, adhering to the protocols established within the Hyperledger Sawtooth framework.

We demonstrated the performance of the proposed framework by testing various significant parameters, which include the impact of blocksize on latency by varying the transaction rate per second and the impact of blocksize and transaction rate on throughput. Experimental results show that transaction latency decreases linearly by increasing the blocksize and transaction rate (tps). Parallel transactions increase the system's overall performance metrics by decreasing latency and increasing transaction throughput. After reaching its maximum transaction throughput, it does not show a significant rise and then starts decreasing gradually. Network bandwidth and CPU consumption per core were also observed by using cAdvisor and AWS cloudwatch. CPU utilization metrics show that there is not much change during transaction handling or in idle conditions. However, sudden spikes in network packet count have been observed during transaction processing, and idle state systems do not require significant bandwidth, making sawtooth network protocol network-bound rather than CPU bound. To make quantum secure off-chain communication, we utilized kyber768 and dilithium3 algorithms.

The experimental results demonstrated that PHTrack offers a reliable, all-encompassing drug provenance system and real-time supply chain traceability capabilities. Our proposed system provides profound theoretical and managerial implications for drug supply chains, with benefits ranging from improved transparency and regulatory compliance to cost savings, increased operational efficiency, and enhanced risk management.

We gathered information on our model's performance through the benchmarking tools, which can be used as a basis for future discussions. As part of our ongoing efforts to enhance the efficiency of drug supply chains, we will incorporate case study-based research on generating increased value for stakeholders by incorporating automated transaction processors for each core module.

CRediT authorship contribution statement

Anum Nawaz: Conceptualization, Data curation, Methodology, Writing – original draft. **Liguan Wang:** Methodology. **Muhammad Irfan:** Writing – review & editing. **Tomi Westerlund:** Conceptualization, Supervision, Writing – review & editing.

Data availability

Data will be made available on request.

References

Abdallah, S., & Nizamuddin, N. (2023). Blockchain-based solution for pharma supply chain industry. *Computers & Industrial Engineering*, *177*, Article 108997.

Abdellatif, A. A., & Al-Marridi (2020). Sshealth: Toward secure, blockchain-enabled healthcare systems. *IEEE Network*, *34*(4), 312–319. http://dx.doi.org/10.1109/MNET.011.1900553.

Agrawal, T. K., & Angelis (2022). Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. *International Journal of Production Research*, 1–20.

Ali, I., & Kannan, D. (2022). Mapping research on healthcare operations and supply chain management: a topic modelling-based literature review. *Annals of Operations Research*, *315*(1), 29–55.

Altaf, A. (2023). A survey of blockchain technology: Architecture, applied domains, platforms, and security threats. *Social Science Computer Review*, *41*(5), 1941–1962.

Alzahrani, N., & Bulusu, N. (2016). Securing pharmaceutical and high-value products against tag reapplication attacks using nfc tags. In *2016 IEEE international conference on smart computing* (pp. 1–6). IEEE.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth euroSys conference* (pp. 1–15).

Aytekin, A., Görçün, Ö. F., Ecer, F., Pamucar, D., & Karamaşa, Ç. (2023). Evaluation of the pharmaceutical distribution and warehousing companies through an integrated Fermatean fuzzy entropy-WASPAS approach. *Kybernetes*, *52*(11), 5561–5592.

Azevedo, & Gomes (2023). Supply chain traceability using blockchain. *Operations Management Research*, [ISSN: 1936-9743] *16*(3), 1359–1381. http://dx.doi.org/10.1007/s12063-023-00359-y.

Benji, M., & Sindhu, M. (2019). A study on the corda and ripple blockchain platforms. In *Advances in big data and cloud computing* (pp. 179–187). Springer.

Buterin, V., et al. (2013). Ethereum white paper. *GitHub Repository*, *1*, 22–23.

Commissioner (2023). FDA protects patients from harmful drugs through the DSCSA, URL https://www.fda.gov/news-events/fda-voices/fda-protects-patients-harmful-drugs-through-drug-supply-chain-security-act.

Corso, A. (2019). *Performance analysis of proof-of-elapsed-time (poet) consensus in the sawtooth blockchain framework* (Ph.D. thesis), University of Oregon.

Dasaklis, T. K., Voutsinas, T. G., Tsoulfas, G. T., & Casino, F. (2022). A systematic literature review of blockchain-enabled supply chain traceability implementations. *Sustainability*, *14*(4), 2439.

Dauvergne, P. (2022). Is artificial intelligence greening global supply chains? Exposing the political economy of environmental costs. *Review of International Political Economy*, *29*(3), 696–718.

de Ocáriz Borde, H. S. (2022). An overview of trees in blockchain technology: Merkle trees and Merkle patricia tries.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). The hyperledger project. In *Blockchain enabled applications* (pp. 139–149). Springer.

Dwivedi, S. K., Amin, R., & Vollala, S. (2020). Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications*, [ISSN: 2214-2126] *54*, Article 102554. http://dx.doi.org/10.1016/j.jisa.2020.102554, URL https://www.sciencedirect.com/science/article/pii/S2214212620301484.

Grigg, I. (2017). Eos-an introduction. *White paper*, https://whitepaperdatabase.com/eos-whitepaper.

Hassija, & Vikas (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, *8*(8), 6222–6246.

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, *54*, Article 102136.

Kaiser-Kershaw, S. (2022). Helping pharma help people: New NFC Tags Boost Safety and adherence, URL https://www.nxp.com/company/blog/helping-pharma-help-people-new-nfc-tags-boost-safety-adherence:BL-HELPING-PHARMA.

Karuppiah, K., Sankaranarayanan, B., & Ali, S. M. (2023). A decision-aid model for evaluating challenges to blockchain adoption in supply chains. *International Journal of Logistics Research and Applications*, *26*(3), 257–278.

Khan, S. A., Gupta, H., Gunasekaran, A., Mubarik, M. S., & Lawal, J. (2023). A hybrid multi-criteria decision-making approach to evaluate interrelationships and impacts of supply chain performance factors on pharmaceutical industry. *Journal of Multi-Criteria Decision Analysis*, *30*(1–2), 62–90.

Killer, C., Rodrigues, B., & Stiller, B. (2019). Security management and visualization in a blockchain-based collaborative defense. In *2019 IEEE international conference on blockchain and cryptocurrency* (pp. 108–111). IEEE.

King, B., & Zhang, X. (2007). Securing the pharmaceutical supply chain using RFID. In *2007 international conference on multimedia and ubiquitous engineering* (pp. 23–28). IEEE.

Kordestani, A., Oghazi, P., & Mostaghel, R. (2023). Smart contract diffusion in the pharmaceutical blockchain: the battle of counterfeit drugs. *Journal of Business Research*, *158*, Article 113646.

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing*, *13*(2), A19–A29.

Malik, N., & Alkhatib (2021). A comprehensive review of blockchain applications in industrial Internet of Things and supply chain systems. *Applied Stochastic Models in Business and Industry*, *37*(3), 391–412.

Melnyk, S. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162–183.

Meng, X., Liang, W., Xu, Z., & Li, K.-C. (2022). A lightweight authentication protocol for NFC-enabled drug anti-counterfeiting system. In *2022 IEEE 24th int conf on high performance computing & communications; 8th int conf on data science & systems; 20th int conf on smart city; 8th int conf on dependability in sensor, cloud & big data systems & application (HPCC/DSS/smartCity/dependSys)* (pp. 516–522). IEEE.

Mohit, M., Kaur, S., & Singh, M. (2022). Design and implementation of transaction privacy by virtue of ownership and traceability in blockchain based supply chain. *Cluster Computing*, *25*(3), 2223–2240.

Moosivand, A., Ghatari, A. R., & Rasekh, H. R. (2019). Supply chain challenges in pharmaceutical manufacturing companies: using qualitative system dynamics methodology. *Iranian Journal of Pharmaceutical Research: IJPR*, *18*(2), 1103.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., et al. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access*, *9*, 9728–9743.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*.

Nawaz, et al. (2019). Edge AI and blockchain for privacy-critical and data-sensitive applications. In *2019 twelfth international conference on mobile computing and ubiquitous network* (pp. 1–2). http://dx.doi.org/10.23919/ICMU48249.2019.9006635.

Nawaz, et al. (2020). Edge computing to secure iot data ownership and trade with the ethereum blockchain. *Sensors*, *20*(14), 3965.

Nguyen, A., Lamouri, S., Pellerin, R., Tamayo, S., & Lekens, B. (2022). Data analytics in pharmaceutical supply chains: state of the art, opportunities, and challenges. *International Journal of Production Research*, *60*(22), 6888–6907.

Nguyen Gia, T., Nawaz, A., Peña Querata, J., Tenhunen, H., & Westerlund, T. (2019). Artificial intelligence at the edge in the blockchain of things. In *International conference on wireless mobile communication and healthcare* (pp. 267–280). Springer.

Ongaro, D., & Ousterhout, J. (2015). The raft consensus algorithm. *Lecture Notes CS*, *190*, 2022.

Onieva, E., Osaba, E., Angulo, I., Moreno, A., Bahillo, A., & Perallos, A. (2015). Improvement of drug delivery routes through the adoption of multi-operator evolutionary algorithms and intelligent vans capable of reporting real-time incidents. *IEEE Transactions on Automation Science and Engineering*, *14*(2), 1009–1019.

Pandey, M., Velmurugan, M., Sathi, G., Abbas, A. R., Zebo, N., & Sathish, T. (2023). Blockchain technology: Applications and challenges in computer science. *Vol. 399*, In *E3S web of conferences* (p. 04035). EDP Sciences.

Paul, M. B. (2023). Concept of firebase. *Intelligent Electrical Systems*, 44.

(2016). Pharmaceutical sector - observatory, URL https://euipo.europa.eu/ohimportal/en/web/observatory/ipr-infringement-pharmaceutical-sector.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135.

Saraji, M. K., Rahbar, E., Chenarlogh, A. G., & Streimikiene, D. (2023). A spherical fuzzy assessment framework for evaluating the challenges to LARG supply chain adoption in pharmaceutical companies. *Journal of Cleaner Production*, *409*, Article 137260.

Sharma, N., & Rohilla, R. (2023). A novel Hyperledger blockchain-enabled decentralized application for drug discovery chain management. *Computers & Industrial Engineering*, *183*, Article 109501.

Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K.-K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, *149*, Article 102471.

Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR Research Protocols*, *7*(9), Article e10163.

Uddin, M. (2021). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics*, *597*, Article 120235.

Vakilinia, I., Wang, W., & Xin, J. (2023). An incentive-compatible mechanism for decentralized storage network. *IEEE Transactions on Network Science and Engineering*.

Valizadeh, J., Boloukifar, S., Soltani, S., Hookerd, E. J., Fouladi, F., Rushchtc, A. A., et al. (2023). Designing an optimization model for the vaccine supply chain during the COVID-19 pandemic. *Expert Systems with Applications*, *214*, Article 119009.

Vijay, & Priya (2022). Grainchain–agricultural supply chain traceability and management technique for farmers sustainability using blockchain hyper ledger. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(3), 141–146.

Wamba, S. F., & Queiroz, M. M. (2020). Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities. *International Journal of Information Management*, *52*, Article 102064.

Wang, Q. (2022). Exploring web3 from the view of blockchain. arXiv preprint arXiv:2206.08821.

Wang, M., Duan, M., & Zhu, J. (2018). Research on the security criteria of hash functions in the blockchain. In *Proceedings of the 2nd ACM workshop on blockchains, cryptocurrencies, and contracts* (pp. 47–55).

Wang, R., Ye, K., Meng, T., & Xu, C.-Z. (2020). Performance evaluation on blockchain systems: a case study on Ethereum, Fabric, Sawtooth and Fisco-Bcos. In *Services computing–SCC 2020: 17th international conference, held as part of the services conference federation, SCF 2020, honolulu, HI, USA, September 18–20, 2020, proceedings 17* (pp. 120–134). Springer.

Wisessing, K., & Vichaidis, N. (2022). IoT based cold chain logistics with blockchain for food monitoring application. In *2022 7th international conference on business and industrial research* (pp. 359–363). IEEE.

Xu, X., Zhu, D., Yang, X., Wang, S., Qi, L., & Dou, W. (2021). Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain. *ACM Transactions on Internet Technology (TOIT)*, *21*(1), 1–17.

Ziavrou, K. S., Noguera, S., & Boumba, V. A. (2022). Trends in counterfeit drugs and pharmaceuticals before and during COVID-19 pandemic. *Forensic Science International*, Article 111382.