Computers & Industrial Engineering 177 (2023) 108997

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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

Blockchain-based solution for Pharma Supply Chain Industry

Salam Abdallah [a], Nishara Nizamuddin [b]

[a] College of Business, Abu Dhabi University, Abu Dhabi, United Arab Emirates
[b] College of Interdisciplinary Studies, Zayed University, Dubai, United Arab Emirates

ARTICLE INFO

Keywords:
Pharma supply chain management
Blockchain
IoT
Ethereum
Smart contracts

ABSTRACT

Modern pharma supply chain systems are complicated, involving manufacturers, suppliers, and consumers that span across continents. To date, there is a considerable lack of transparency in the movement and sale of pharmaceutical products sold online. Lack of transparency, mistrust in collaboration, and unwillingness to share data can be huge challenges for this global industry. In this paper, we propose a blockchain-based framework for the online sale of pharma products, in a decentralized manner with no intermeies such as hospitals or pharmacies. The proposed solution is based on utilizing Ethereum smart contracts, to monitor the interaction between participants, trigger events that are logged to help the participants to keep track and be informed about sale transactions, and ensure payment dispersal securely. In addition, smart contracts regulate the interaction between sellers and consumers by monitoring the status of IoT containers, including pharmaceuticals, and fully notifying consumers. Our smart contracts handle special cases related to consumer refunds in case of breach of contract terms to ensure the safe delivery of medicines.

1. Introduction

Pharma companies manage complex supply chains as it involves interacting with many numbers of suppliers contributing ingredients and components for drug production. The Pharma supply chain industry needs to ensure the utmost safety precautions to transport goods, as any negligence of safety measures may lead to a fatal outcome. Pharma companies played a major role during the Covid19 pandemic, by supporting the requirements of healthcare providers, and patient needs, and facilitating access to medicine (McKinsey & Company, 2020). There is an increased need to meet challenges to comply with new serialization regulations (Brechtelsbauer et al., 2016) that require inventory to be auditable as it moves through the supply chain (Waters, 2019). With the supply chain industry spanning globally across continents, its operation being shifted from an intra-functional to an inter-organizational structure, a substantial number of defects enter the pharma supply chain system, which makes it a difficult task to trace any deterioration of quality or safety standards (Ballou et al., 2000). Digitalization and online sale of pharmaceutical products have opened doors to the production of counterfeit drugs, diminished quality, untraced transport of drugs, and customers' absence in the entire supply chain process. Currently, there is no efficient decentralized application or system to record and trace the production and movement of consumer products such as pharma products, and agriculture products throughout the supply chain (Toyoda et al., 2017); (Majdalawieh et al., 2021). The reason for the diminished quality of drugs is discovered at a very later stage in a supply chain process, which results in a product or financial loss for the entities within the supply chain. Furthermore, lack of transparency and cross-supply chain communication failure increases the problems faced which forces every single operating entity in the supply chain to work using information from a localized point of view.

1.1. Problem Statement

There is a considerable lack of transparency and trust in the production, sales, and movement of pharmaceutical products (in terms of quality and constituents). Today's supply chains are diverse and global, and that means it's easy for things to wrong. Even the slightest problem deep in the pharma supply chain, such as an incorrect pharmaceutical component used by a supplier's supplier can become a massive issue after the product has been rolled down the assembly line to another finished product (Barry, 2014). Typically, as products move from one organization to another, organizations have accounting review invoices and reconcile shipments. Refunds are initiated in case of a temperature or quality breach during the process of transportation of goods and payments are made once the products have arrived. This conventional process is time-consuming, costly, and prone to delay and

Abbreviations: IoT, Internet of Things.

E-mail addresses: salam.abdallah@adu.ac.ae (S. Abdallah), nishara.nizam@gmail.com, nishara.nizamuddin@zu.ac.ae (N. Nizamuddin).

https://doi.org/10.1016/j.cie.2023.108997

Available online 12 January 2023

errors. This typically slows down the business process and the customers are directly impacted as poor-quality medicines may be delivered to the end consumers which might sometimes lead to a detrimental outcome. Further, consumers have always had very little influence on the supply chain as they were not fully aware of what it was and any of its processes (Mackey and Nayyar; WHO,2021). A consumer who ordered an item would have no idea where the item was made, who made the item, under what conditions, or when to expect delivery. On the other hand, it's hard for healthcare organizations around the world to know if the incoming shipments of medicines are real (Mackey and Nayyar, 2017; Barry, 2014).

Fig. 1 illustrates a typical scenario of production, distribution, and provision of pharma drugs to end-users (consumer/patient) via pharmacy or hospital. In this case, the customers are unaware of the production, and shipment of the drugs due to a lack of transparency. The World Health Organization's (WHO) report claims (WHO,2021) that up to 2 billion people around the world lack access to necessary vaccines, medical supplies, and medicines, which creates a void that is too often filled by substandard products. And when medicines are in high demand, there is an increased introduction of counterfeit and expired drugs into the supply chain (WHO,2021; Interpol, 2021). WHO also claims that the problem of substandard medicines is growing as global supply chains have become more complex spanning across continents, meaning products being manufactured in one country may be packaged in another country and sold to consumers in a third country. Further, the growth of e-commerce contributes to this trend as it makes it easier to purchase medicines online, often from unverified sources (WHO,2021). The production, transport, and sales of pharmaceutical drugs are not transparent or accessible to all the participants in the supply chain. Transactional events are recorded either in a localized or centralized manner and are vulnerable to tampering (Toyoda et al., 2017); Swan, 2015).

Though several techniques such as using RFID (Radio Frequency Identification) for the efficient and effective dispatch of products in the healthcare supply chain business applications have been adopted to enhance trust, the cost of implementing the current RFID technology is high for a globally spanned healthcare supply chain (Yue et al., 2008; Abugabah et al., 2020) and that consumer is mostly left out or has minimal knowledge in terms of accessing the RFID data (Federal Trade Commission (FTC), 2005). A robust, decentralized, and complete solution with transparent, traceable, and credible sales and transactions are still lacking. RFID (Radio Frequency Identification) enables businesses to provide every product with a unique digital identity that can store data and connect to the blockchain to improve transparency throughout the supply chain (Berry et al., 2019).

In this paper, we present a blockchain-based solution that can protect the end-consumer by providing secure delivery of pharma goods and providing a verifiable decentralized ledger that is traceable by all stakeholders across the supply chain. Blockchain provides a decentralized, distributed, peer-to-peer network with an immutable ledger eliminating centralized authority for verification of transactions which creates secure records that cannot be tampered with (Toyoda et al., 2017); (Majdalawieh et al., 2021); Swan, 2015). While the most prominent use of blockchain is in the cryptocurrency, Bitcoin, the reality is that blockchain—essentially a distributed, digital ledger—has many applications and can be used for any exchange, agreements/contracts, tracking, and, payment. Since every transaction is recorded on a block and across multiple copies of the ledger that are distributed over many nodes (computers), it is highly transparent. It's also highly secure since every block links to the one before it and after it. There is no one central authority over the blockchain, and it's extremely efficient and scalable. Conclusively, blockchain can improve the efficiency and transparency of the supply chain and categorically impact the entire business cycle from warehousing to delivery to payment. The smart contract is a prevalent concept with blockchain as its underlying technology, which digitally facilitates, verifies, and monitors the events of a transaction. It ensures trustworthy transactions without third parties which are verifiable and irrevocable. Ethereum is an open-source, public, irreversible decentralized computing platform that supports smart contract execution (Wood, 2014; Dannen, 2017). The smart contract code is written in Solidity, which runs on the EVM (Ethereum Virtual Machine). The blockchain is publicly available to everyone in the network who is authorized to view the transactions; all the events are made visible to all operative participants within the chain (Wood, 2014; Dannen, 2017).

The combination of blockchain ledger technology and IoT device technology is revolutionizing the pharmaceutical industry's supply chain management process, as well as the customer purchasing paradigm, as consumers are now more informed than ever before deciding. The main outcome of utilizing blockchain technology will eliminate the trust issues among the members of the pandemic structure of the supply chain as all the transactions are time-stamped in sequential order and broadcast the events to all authorized parties including the consumer.

Motivated by the importance of having a transparent and decentralized pharma supply chain management solution, we propose a framework that uses blockchain in supply chain management along with the Internet of Things (IoT). The containers that carry the pharmaceutical products can be fitted with sensors that will collect data and blockchain will guarantee quality, authenticity, and identifying defective products (Majdalawieh et al., 2021). For some specific cases, containers' temperature can be very critical to avoid quality degradation and contamination of the shipment (Mackey and Nayyar, 2017). Smart contracts can be used to write code to automate efforts that benefit supply chain management, eliminating the presence of malicious

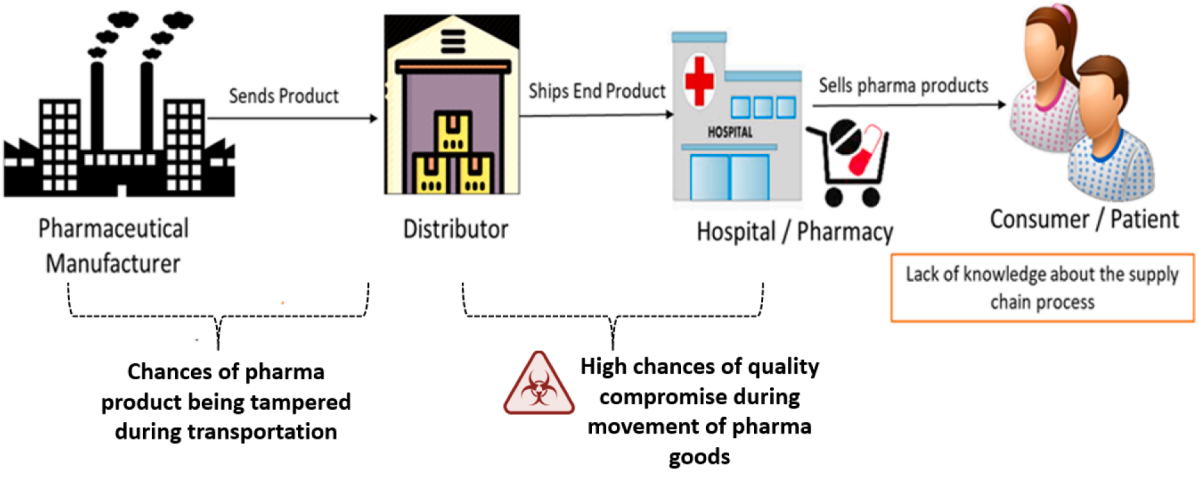

Fig. 1. Existing – Traditional Flow in Online Pharma Supply Chain (WHO,2021; Interpol, 2021; Barry, 2014).

entities, and thereby improving the efficiency of supply chain management by recording every event. (Christidis and Devetsikiotis, 2016, (Majdalawieh et al., 2021). Following the shipment of goods, smart contracts can be executed to certify the predefined contractual terms which can be verified by all the stakeholders at any time (Zhou et al., 2015). The features that smart contracts and blockchain provide can effectively regulate the interaction between multiple parties, protecting and guaranteeing authentic and high-quality pharma goods for the end consumers. The purpose of the paper is threefold:

- To illustrate a solution that eliminates the need for a trusted third-party authenticator to verify the genuineness of transactions and quality of products while in the supply chain.
- To provide a novel smart contract-based supply chain management solution that guarantees the rights of the manufacturer, distributor, and consumer.
- To present a system that utilizes sensors in IoT shipment containers detects violations, and logs the events in the smart contract.
- To highlight the overall architecture, system design, and major events among the participants in the supply chain process. The paper is generic enough to be extended for any type of supply chain network management using blockchain technology.

This paper starts with a short overview of related works and the theoretical background of blockchain technology, followed by a brief introduction to the used DSR (Design Science Research) approach. We then describe the proposed framework and evaluate it. Finally, we discuss its implications, give an outlook and investigate the limitations of our work. The remainder of this paper is organized as follows. In Section 2, we have summarized the related work. In Section 3, our proposed solution for pharma supply chain management is presented. In Section 4, key aspects of implementation and testing details of the smart contract are detailed. In Section 5, we have presented the discussion. In Section 6, the conclusion is presented.

2. Literature review

In this section, we summarize efforts, initiatives, publications, and articles found in the literature related to the blockchain and pharma supply chain industry. It is worth noting that most of the related articles are high-level with no implementation details, as this blockchain technology is emerging.

The ongoing covid-19 pandemic crisis has taught several important lessons. One of them is the need for effective organization and safe deployment of primary healthcare to ensure the continuity of care within our communities. The timely delivery of pharmaceutical products and medical supplies has been an indispensable element of the Covid-19 response. Starting from delivering products with high quality, timely delivery, and international standards, several factors might affect the nature of the pharma products delivered. Rabah (2017) emphasizes that the structure of the pharma supply chain is complex, starting from the stage of manufacturing a drug until it reaches the end-user. The author has argued in the paper how blockchain can prove to be very effective across the pharma supply chain industry due to its various promising features such as immutability, tamper-proof digital ledger, and accessibility by all authentic participants. The paper highlights how blockchain technology can be disruptive in improving the efficiency of the overall healthcare sector, improving data security for safeguarding Electronic Health Records (EHR), and managing privacy in patient care. Clauson et al. (2018) discuss the various challenges and opportunities associated with the adoption and implementation of blockchain technology concepts for the pharmaceutical supply chain industry, medical equipment supplies, and the Internet of Healthy Things (IoHT). An extensive literature study on exploring blockchain-based solutions for the healthcare supply chain industry and its characteristics was conducted and potential use cases to combat counterfeit drugs, pharmaceutical falsifications, and drug recall management were identified. Further, the authors (Clauson et al., 2018) highlight how the utility of smart contracts to automate the entire process, improve the transparency of transactions, and reduce costs with the help of blockchain technology. Though both papers (Rabah, 2017; Clauson et al., 2018) are of a prominent level in nature, do not provide details about solution implementation or the use of immutable smart contracts to prove that the end consumer or patient is receiving an authentic pharma product.

The emerging p2p distributed immutable ledger technologies, applications, and the impact of blockchain technology for biomedical and healthcare applications are discussed by (Kuo et al., 2017). The authors have compared and contrasted various existing distributed databases and blockchain technology for improving healthcare and biomedical applications. Further, the authors discuss data provenance as one of the key benefits of blockchain-based distributed ledger for the pharma online supply chain to ensure the transfer of pharmaceutical products starting from manufacturer to end consumer using blockchain technology. The authors argue that the transport of a pharma product can be traced from beginning to end and the entire supply chain process is made transparent to all active participants in the chain. Commonly found problems in the supply chain process are identified such as substandard quality, and counterfeit product issues, and resolved with the help of the immutable nature of the distributed ledger. The pharma supply chain model in this paper is of a high level in nature from a research point of view but has no actual implementation. The various key objectives of supply chain management such as cost, sustainability, speed, and flexibility are discussed (Kshetri, 2018). The author discusses various case studies of blockchain-based projects in supply chain industries which improves transparency and liability spanning diverse industries. IoT incorporation into blockchain-based solutions and the implementation of blockchain concepts to validate the identities of assets and individuals in the network are discussed (Kshetri, 2018). US-based Blockchain start-up Chronicled and life sciences supply chain consultancy is a unique supply chain consulting group founded to provide life science companies guidance and support to meet worldwide serialization. The launch of a "*track and trace*" pilot project for the pharmaceutical industry whose projected growth was $1.12 trillion as declared by *Linklab* (Chronicled, 2017). The protocol launched was a blockchain-based compliance protocol to satisfy the Drug Supply Chain Security Act (DSCSA). The proposed solution is aimed to contribute to the pharma industry with a lower cost and secure access to satisfy the existing regulatory requirements. Further the project's objective is to develop GS1 standards and to highlight data privacy. This model is still in the development process with no actual implementation.

It is important to design a system that ensures the safe packaging, transport, and secure delivery of pharmaceutical drugs. Shipping of pharmaceutical products can be extremely challenging as it involves long complex shipping that requires temperature-controlled surroundings, storage temperature variations, unpredicted delays in shipment, and packaging damages in the logistics market (Markarian, 2015). Any compromise in terms of the quality of packaging, shipment, and delivery may lead to a fatal outcome as it involves human lives. A Swiss start-up combined with the University of Zurich designed a system to ensure secure transport and delivery of pharmaceutical drugs with the help of the immutable and robust nature of blockchain technology (Modum, 2016). The combined benefits of IoT sensors and blockchain for monitoring the temperature and quality of transactions are aimed at improving the trust of valuable consumers by increasing transparency in terms of regulations and quality requirements. Modum.io, a fast-growing start-up, which provides innovative digital supply chain solutions with global partners, focuses on categories of temperature ranging from $-25\ ^{\circ}C$ to 8°. In such cases, the sensors in the truck would monitor the temperature of the products and report any sudden change in storage temperature. Once the shipment arrives at the destination, the data is transferred to a blockchain-based smart contract framework, which

confirms the integrity of the delivered products. Based on the data collected and events generated by the contract, the product delivery or automated payment process is initiated. This proves to be cost-effective and efficient for monitoring the environmental conditions of a freight containing pharma drugs.

The intersection between IoT devices and distributed ledger technology can provide several benefits which can resolve the issues associated with the IoT centralized architecture as proposed by Atlam and Wills (2019). IoT-based systems aim to improve the quality of life by enhanced digitization of services and by sharing data over the Internet. Moreover, cloud computing has gained acumen in the field of healthcare for publishing sensitive medical transactions data by using data anonymization techniques (Nizamuddin and Pandey, 2015), and also by providing the IoT system with the required functionalities to analyze and process the information and convert them into the real-time application. But, the existing IoT architecture depends on the centralized server which leads to a lack of trust and confidence in the system. The centralized server involves a third-party service provider/authenticator to monitor and control the data collection process across various IoT devices. This setup acts as a black box due to which the network participants lack a vision of where and how their data is being utilized (Fabiano, 2017).

The existing IoT centralized architecture faces many issues concerning security and scalability (Atlam and Wills, 2019). Further, the authors propose an innovative idea, by combining blockchain and IoT devices. The P2P communication model can be used to process billions of transactions between IoT devices which drastically reduces the cost of installing and maintaining large centralized datacenters storage units. Fig. 2 shows a decentralized IoT system after integrating blockchain with IoT. The decentralized feature of blockchain will eliminate the unavailability of the network in case of failure of any of the nodes (Ferraro et al., 2018).

The authors (Atlam and Wills, 2019) discuss various benefits and features such as decentralization, improved transparency, identity management, security, immutability, and anonymity that results as an outcome of integrating blockchain with IoT. Thus, IoT and blockchain technologies can work together, creating a symbiotic relationship where blockchain becomes prevalent and IoT becomes autonomous. This paper highlights an interesting research area and the Distributed Ledger Technology (DLT) -based system solutions presented are of significant importance for the development of distributed IoT services soon.

An idea to integrate the Internet of Things (IoT) devices with a

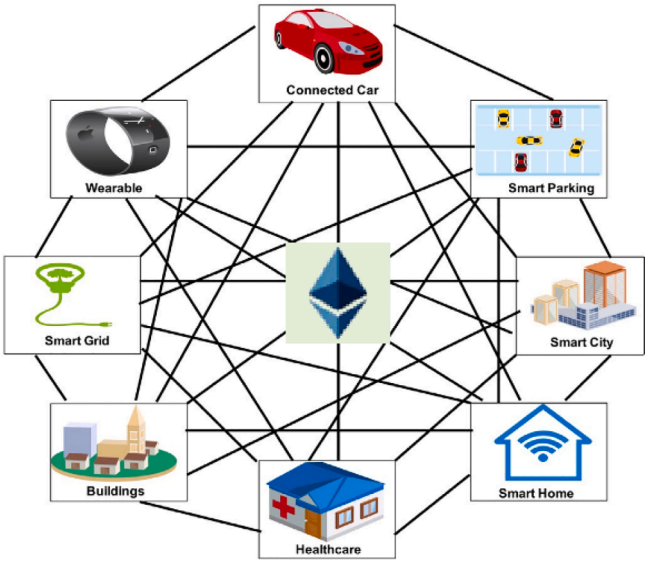

Fig. 2. Decentralized IoT architecture by integrating blockchain with IoT [Atlam and Wills, 2019].

blockchain-based decentralized application based on the Ethereum platform is presented by Ahmad (2017). The proposed blockchain-based application consists of a front-end application that can be deployed on any web server and a smart contract that will be deployed on a private blockchain network which is comprised of P2P IoT devices acting as a full Ethereum node. This application follows the digital transport ticketing system, where a ticket is considered an asset that can be purchased by the user, and payment can be made in the form of ether from their Ethereum account on the blockchain. Upon purchase, the transaction is mined, which is then propagated across the network to all the peer nodes. This ticket is then locally accessible and safe because of the decentralized nature of the blockchain. The author further presents a scenario for integrating IoT devices via a DApp (Decentralized Application), which can be used for purchasing transport tickets using ether and validating the ticket on any node in the network without the need for a centralized server. The system is designed in 3 layers such as the blockchain layer (which represents all the blockchain nodes), the account management layer (which consist of account management tools that enable to perform transactions or calls on the blockchain), and the presentation layer (web-based Graphical User Interface (GUI) for interaction with blockchain). The DApp utilizes all these three layers, by making the system interactive, decentralized, and secure. This thesis (Ahmad, 2017) is of high quality and gives insight into governing the storage problem of IoT devices without giving away the decentralized nature of the system.

Jüttner et al. (2003) explore perceptions of risk and management strategies in the supply chain industry. The authors discovered four important aspects of the management concept: (1) determining the sources of the risk (2) elucidating the supply chain risk concept (3) identifying the risk drivers (4) subduing risks for the supply chain. The analysis showed an effectual need for more empirically grounded research on supply chain management. In a complex supply chain system, it is very difficult to have an overall picture of all transactions within the chains. This information is typically stored in multiple locations and is accessible to certain system entities. The distributed ledger technology is explored by multiple industries due to its immutability and robust nature. Clark and Burstall (2018) reinstate that blockchain can be a ground-breaking transformation in safeguarding the intellectual property of consumer-centric industries, especially those faced with counterfeit goods, such as the luxury, consumer goods, and pharmaceutical industries. A recent study by PricewaterCoopers (PricewaterhouseCoopers, 2017), states that fake pharma drug markets are about €188 billion (US$200 billion) annual business, turning out to be the largest of all counterfeit goods. The World Health Organization (WHO) claims that about 50% of the drugs on sale on the Internet are fake (Clark and Burstall, 2018; PricewaterhouseCoopers, 2017). Fake pharmaceutical drugs may lead to fatal effects because of harmful ingredients or the absence of active ingredients. Blockchain unless like systems that safeguard using QR codes, uses digital decentralized ledgers that are tamper-free and record all the events in a transparent record by allowing multiple parties to verify a transaction and finally add the verified transaction to the chain of blocks. With the digital ledger, the pharma goods' movement in the chain can be recorded, and lost or misplaced goods can be identified. With this approach, fake goods can also be easily identified.

Tseng et al (Tseng et al., 2018) suggest a Gcoin blockchain model creates a lucid record of drug transaction data. The Gcoin blockchain double-spending prevention is highlighted to prevent the counterfeit-drug problem. The authors have highlighted that blockchain technology can be a solution to establish trust between identities and parties involved in the network by using the consortium proof-of-work approach. This aimed at resolving the double-spending issue in the blockchain pharma industry (Tseng et al., 2018). Each authorized entity can be assigned a role such as miners, and coin issuers, including end consumers or patients. Gcoin blockchain was designed to track every pill for drug identification by using the serial or batch number to identify it

in the drug supply chain. The complete drug information can be utilized to be used for the generation of public keys (or hashes) which in turn generates a QR code as identification for drugs. The participants in this system are identified as producers, wholesalers, retailers, pharmacies, and consumers (Tseng et al., 2018). This system also suggests that government entities should take part to monitor transactions and drug information in the form of an alliance member in the Gcoin blockchain system. The drug producer is granted the role of coin issuer and the miners are suggested to be large manufacturers and government agencies. Other entities such as wholesalers and retailers are considered to be backup storage entities of transactions. Consumers are considered to be wallets who can implement the transactions. The authors further suggest using the Gcoin blockchain multi-signature design, which is approved by successfully applying in the "Nanyang Technological University (NTU) Help Centre". As far as the functioning of the system is considered, manufacturers pass the transaction data (such as location, name, etc.) to sellers directly which is recorded in the Gcoin blockchain which is verified on the chain which is hashed to be recorded on the Gcoin blockchain. In case, if an illegal distributor tries to sell fake drugs to buyers, the transaction will become invalid because of the presence of fraudulent information about unspent transaction outputs (UTXO) stored in the Gcoin blockchain and due to a lack of authentic private keys (Tseng et al., 2018). This makes the buyer and seller aware of aberrations within the transactions. This paper is a highly innovative approach in the field of blockchain-based health care systems that concentrates on the prevention of counterfeit goods from entering the legitimate supply chain and not more on the automation of the entire supply chain management cycle.

The benefits of blockchain for biomedical/healthcare applications are reviewed by Toyoda et al (Toyoda et al., 2017). The authors put forward the idea that using blockchain will trace the origin of the pharma product and track its movement in the supply chain process. By adopting blockchain technology, counterfeit, and quality degraded goods can be easily identified and discarded. Further, the improvement of system robustness can be achieved for counterfeit drug prevention in the pharmaceutical supply chain, by modifying the existing solutions with blockchain-enabled anti-tampering features during the manufacturing, supply, and dispatch process. Counterfeit medicines are a major public health problem and pharmaceutical companies have started looking for and implementing various solutions to curb substandard goods in drug supply chain management (Glass, 2014). It is estimated that fake drugs cost the European Union pharmaceutical industry around €10.2 billion or 4.4% of sales each year and result in a direct loss of around 40,000 jobs (Wajsman et al., 2016). Blockchain-based systems could be implemented to record the movement of pharmaceuticals and their authentication throughout the supply chain. Making the market participants aware of the decentralized ledger technology to verify the product authenticity can be a major step in dealing with the issues of counterfeit drugs (Radanović and Likić, 2018, SupplyDemandChain, 2018). However, the technology is still in its infancy and needs to overcome several obstacles such as building up a robust regulatory framework and data access controls to operate to its full potential in the healthcare industry.

To sum up, the supply chain industry has been facing increasing challenges to create, maintain and regulate transparent, decentralized, and effective supply chain methods. Complicated customer service, operating cost, freight cost when dealing with a greater number of global customers, the credibility of delivered products, protection of intellectual property, supplier-partner relationship management, and trustworthy technology for monitoring the complete supply chain process, have been identified as the most common problems in today's era of supply chain management. Hence, there is a compelling need to design a system, which is trustworthy, distributed, transparent, and robust. As blockchain has been gaining importance for its decentralized and tamper-proof characteristics across several industries, in this paper, we propose a smart contracts-powered blockchain-based solution for pharma supply chain management.

3. Proposed solution

In this section, we propose and describe our solution that utilizes the Ethereum blockchain, smart contracts, and IoT containers to monitor, track and carry out the dispatch of pharma products from the manufacturer to the customers. Our solution eliminates the need for a trusted third-party authenticator and improves integrity, reliability, and security among the stakeholders in the supply chain industry.

3.1. Research methodology: Design science research approach

The definition of research can be given as the activity that contributes to the understanding of a particular phenomenon. Design science research is typically applied to categories that include algorithms, design methodologies (including process models), HCI (Human-Computer Interfaces), and languages. This method's application is notable in Engineering and Computer Science disciplines and is widely found across many disciplines and fields. This methodology is a sequence of activities that lead to the production of an innovative end product. Further, this method includes a complete understanding of the problem, and research gap and improves the design quality of the solution by re-evaluating the process. Considering our proposed solution, the research gap in the online pharma supply chain is identified to be a lack of transparency in the movement of goods and data across the chain and automated payment settlement to various parties. The built-and–evaluate loop is iterated several times before the final design is generated. In this approach, the focus is on field-tested and grounded technological rules to improve the relevance of academic management research (Peffers et al., 2012; Peirce, 1974).

The methodology can be classified into mode 1 which is purely academic and mono-disciplinary and mode 2 is multidisciplinary for solving complex field problems. Fig. 3 explains the Cognition in the Design Science Research Cycle and demonstrates the cognition that takes place during a design science research cycle. The design science research (Takeda et al., 1990) uses the abduction, deduction, and circumscription approach, but there is a difference in how these cognitive processes are used. Fig. 3 demonstrates the flow of effort through the types of new knowledge that arise from design science research activities. The figure shows the cognition in the design science research cycle.

In this paper, we have adopted the design science research model in which the research begins with the knowledge about the problem and is also called "*Improvement Research*" as this method involves problem-solving – performance improving nature of the activity (Peffers et al., 2012). One of the major problems in the pharma supply chain industry is the lack of transparency to monitor and regulate the entire process that may be tampered with as it involves several entities across the world.

This gave rise to the idea of having a tamper-proof, trustworthy, transparent, and decentralized solution. Suggestions for a solution can be drawn abductively from the existing knowledge base or theories for the problem area (Peirce, 1974).

In Fig. 3, ***Abduction*** refers to a form of logical inference that starts with an observation or set of observations and then seeks to find the simplest and most likely explanation for the observations. ***The deduction*** is the process of reasoning from one or more statements (premises) to reach a logically certain conclusion. ***Reflection*** and ***Abstraction*** play a major role in the process of the knowledge-building process (Peffers et al., 2012). However, in a research model, these suggestions result in inadequacy. Using the existing knowledge, an attempt is made to solve the problem. A tentative design is made to implement the problem solution in the development phase of the process steps as shown in Fig. 3. The successful implementations either partial or full are evaluated according to the functional specifications and are done during the Evaluation stage. ***Circumscription*** is the formal-logical method that assumes

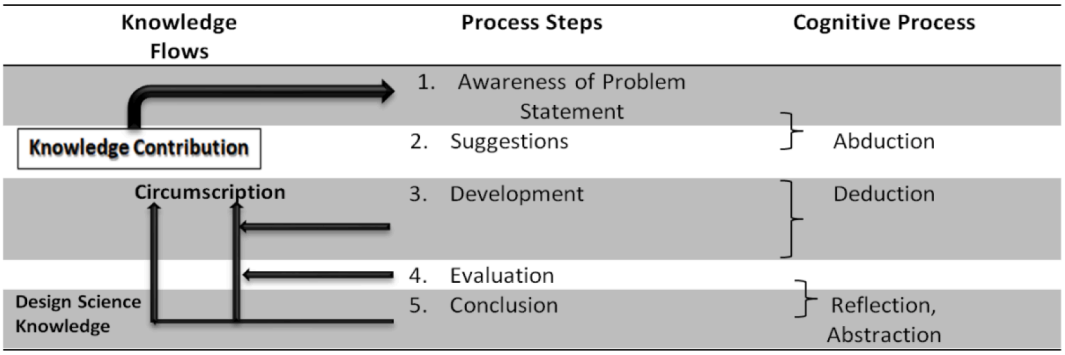

Fig. 3. Design Science Research Cycle (Peffers et al., 2012; Takeda et al., 1990).

that every fragment of knowledge is valid only when the discovery of constraint knowledge about theories is gained through the detection and analysis of contradictions. This results in exposing new problems at the end of the awareness cycle (Peffers et al., 2012). In our solution, we developed smart contracts on a decentralized platform, explicitly tested our implementation the on Remix platform, evaluated the results, and presented the outcome by following the DSR approach.

There are several other DSR models in terms of descriptions of the DSR process (Peffers et al., 2008); Purao, 2013; Gregor and Hevner, 2013; March and Smith, 1995; Nunamaker et al., 1990) and are similar to the above-described model. The authors (Peffers et al., 2008) synthesize selected prior literature on the topic. This model, in comparison to the model shown in Fig. 2, breaks the Awareness of Problem phase into two phases: Identification of problem and definition of solution; merging the suggestions and development phases into a single phase, design & development; breaks the evaluation phase into two phases, demonstration and evaluation; and finally renames the conclusion phase as communication (Peffers et al., 2008). Our proposed solution was evaluated by testing the necessary functionalities of the various parties involved. Purao (2013) presents the fact that invention, improvement, and adaptation can be types of knowledge contribution in DSR. Also, a single research project can make more than one type of knowledge contribution (Purao, 2013). Conventional design cannot be used as applying known solutions for known problems leads to no new contribution. We adopt the methodology of Cognition in the Design Science Research Cycle and have sound knowledge of the Messaging Protocol, Ethereum platform, IoT, and smart contracts. In this paper, we adopt the DSR approach by proposing smart contracts for online pharma supply chain management by identifying the research problem, further dividing the approach into system design and implementation phase, followed by a results section and conclusion that includes a future research agenda.

3.2. System overview and design

In this section, we present the system overview and design which focuses on utilizing smart contracts for a decentralized and transparent supply chain management process. Automated alerts are sent to both seller and consumer in case of any events or any violations that may occur during the transportation and dispatch of the pharma freight. As shown in Fig. 4, MQTT (Messaging Queuing Telemetry Transport), a publish-subscribe-based messaging protocol that works on top of TCP /IP protocol is used in our proposal to exchange data between clients and the server.

An MQTT system consists of clients communicating with a server, which is usually termed a “broker”. Every client present in the system can connect to the broker and MQTT is the most commonly used protocol in IoT-based projects. Violation is identified by the rule-based engine at the Raspberry Pi. Specific rules are considered for each sensor reading and any deviation from the set of rules specified will be considered a violation. Message Queue Telemetry Transport (MQTT) server hosted in the cloud to store, and publish all sensor data generated from the IoT sensors installed within the shipment. Processing interfaces and communication components in IoT-enabled container, cloud-hosted MQTT server, sensors, Raspberry Pi, and the contract through the Ethereum blockchain are shown in Fig. 5. Message Queue Telemetry Transport *(MQTT)* server hosted in the cloud to store, and publish all sensor data generated from the IoT sensors installed within the shipment. Processing interfaces and communication components in IoT-enabled containers cloud-hosted MQTT servers, sensors, Raspberry Pi, and the contract through the Ethereum blockchain are shown in Fig. 5 (Majdalawieh et al., 2021). During a violation, the readings will be sent to the smart contract which would be then communicated to the seller and the consumer.

For testing purposes, we have the temperature to be between 15◦ and 25◦ C, the accelerator between 0 and 5, where 0 to 3 would be a normal movement, and a value more than 3 would be considered a jerk. Pressure change should be 0 to be normal and 1 will represent a big pressure change. All the specifications and rules can be set after an agreement between stakeholders. Apart from this, periodic readings about every 10 min (which can be modified as per requirement) will be sent to the

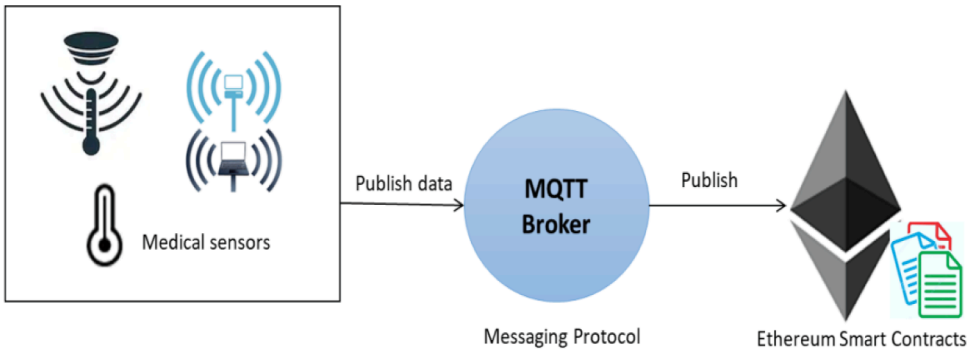

Fig. 4. Smart contracts and Messaging Protocol interactions.

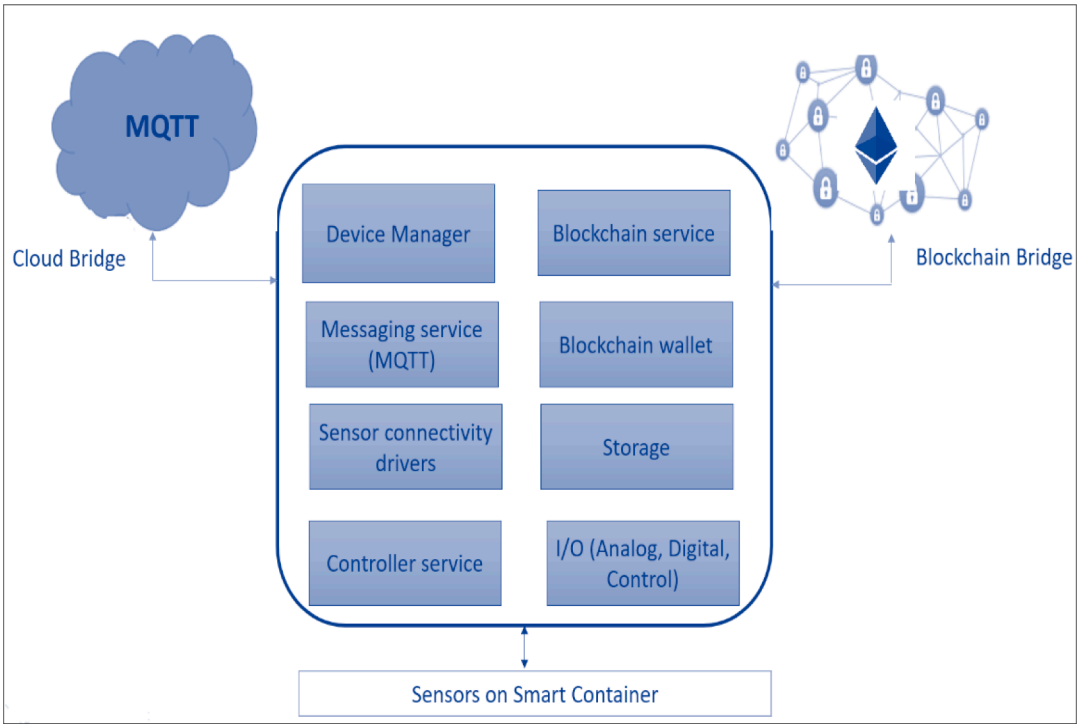

Fig. 5. MQTT server for blockchain-based food safety use case. (Majdalawieh et al., 2021).

MQTT server. The container's Raspberry Pi the tiny computer publishes the state topic that contains the reading of the pressure change, temperature, and jerk. Publishing and subscribing will follow QoS0 (Quality of service – a service level that guarantees a best-effort delivery) as the container's state data are sent periodically. The MQTT gives the resilience to subscribe to the topic and monitor the readings.

Fig. 6 presents a general system diagram of the proposed pharma blockchain-based supply chain management (PBSCM) solution highlighting different components and participants who interact with the smart contract. Each of these participants has an Ethereum account with an address, public key, and private key. The main participants/ components can be summarized as follows:

- ***Seller***: The seller is the entity that creates and initiates the smart contract, following the IoT container's package check to ensure that the freight is in good condition.
- ***Consumer***: Consumer deposits payment (in ether) and the payment are made to the seller only if the freight reaches the consumer without any damage or violation. The delivery of the pharma package to the legitimate consumer, by providing a *keccak256* hash of a pass-phrase to the smart contract by the consumer upon depositing the payment. At the time of delivery, the same passphrase must be provided by the consumer, which would be matched with the original hash value and if it matches then the authenticity of the consumer is confirmed and the IoT container will open.

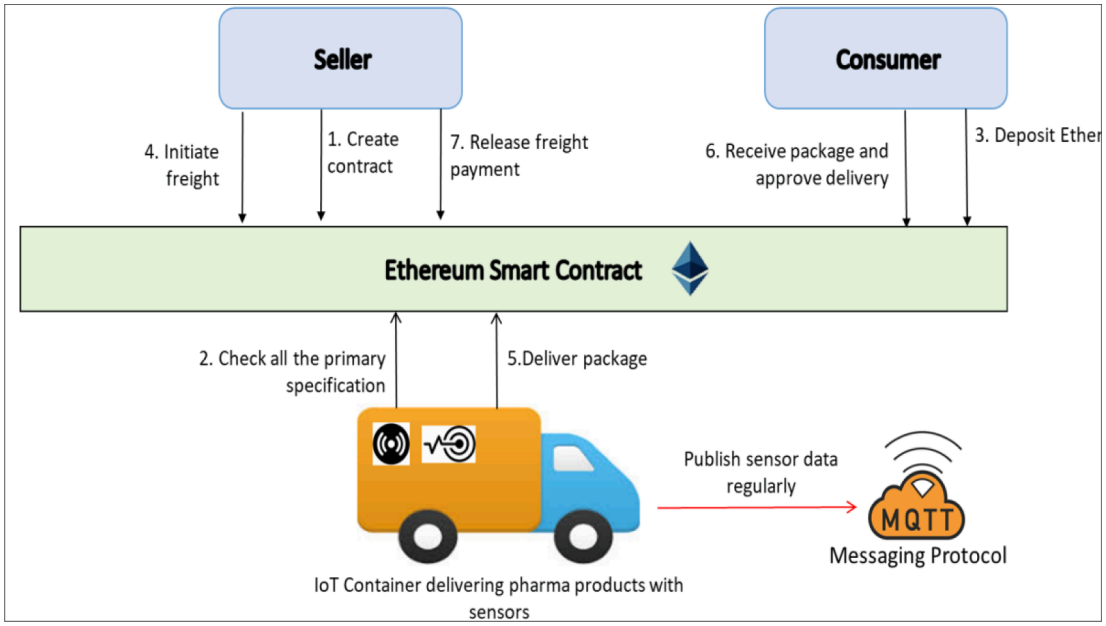

Fig. 6. Blockchain-based solution for Online Pharma Supply Chain.

- ***IoT Container***: The IoT container is a part of the Ethereum blockchain and is identified with an Ethereum address in the network. It is equipped with IoT sensors to track and trace the shipment between the seller and the consumer. The IoT sensors track the temperature of the pharmaceutical freight, pressure sensors check the pressure differences that may be caused due to accidental jerk or opening of the container, and GPS devices trace the location of the shipment. All the sensors are connected to a Raspberry Pi that is placed inside the container. Wi-Fi connectivity is essential for communicating the data to other system components.

This proposed framework proves to be robust enough to maintain, monitor, and verify the temperature maintained during the transit of medicines. Also, it reports any violation of temperature in the smart contract thereby alerting all the participants quality of medicines or vaccines as it uses IoT sensor technology thereby eliminating the risk of any contamination during the transit of goods. Further, the use of a smart contract will ensure a tamper-proof record of all transactions when within the supply chain.

The proposed solution makes use of Ethereum smart contracts which comprise algorithms and logic that administer the sale among the parties involved by executing code and triggering events to keep track of transaction details (Christidis and Devetsikiotis, 2016). In addition, smart contracts govern the fair payment distribution across the Ethereum network, to various parties involved in the chain. The smart contract contains the following entities:

- **Events**: Events help to keep track of any state changes or occurrences in the network. In case of any state changes, the event is logged and broadcasted by the smart contract to all the active participants in the system.
- **Modifiers**: They are used to modify a function's behavior and used to check or specify a condition before the execution of a function. For example, the cost of shipment must be fixed and accepted before the consumer deposits the amount which is specified using the modifier amounts to(). If the modifier condition is not met, then the contract returns to its initial state. Other modifiers used in the smart contract code are OnlyContainer(), OnlySeller(), and OnlyConsumer() which determine which entity in the network has to initiate the transaction or invoke a function.
- **Variables**: Variables used in the smart contract are values that depend upon conditions to execute or change. In this smart contract, receivedAfter, startDate, and freightTariff are some of the important variables.
- To ensure the safe delivery of the pharmaceutical package, as shown in Fig. 6, the seller creates the smart contract and places the freight in the smart container. The container then performs a package check to ensure that the specifications to carry the dispatch of pharma goods have been strictly adhered to. Depending upon the result of the package check, the freight is either continued or gets terminated to fix the containers' issues, which assures that the freight can be trusted by both seller and consumer as per their specific requirements. Upon successful package-check completion, an event is triggered by the smart contract following which the consumer deposits the amount for a purchase to be done and receives the secret hash. The hash provided acts as a secret code to determine the legitimacy of the end consumer who receives the freight. Upon the freight arrives at the destination, the consumer needs to submit the correct secret code for the container to unlock and dispatch the freight.

If a wrong code is provided by the consumer at the time of dispatch, the smart contract offers a time frame of 72 h to provide the correct secret code. If the end consumer fails to provide the right code within 72 h, half of the freight price deposited would be refunded to the consumer, and the shipment is terminated. In the event of a consumer defaulting to provide the correct code, the smart contract releases half of the payment to the seller that is pre-decided between the parties, to make sure that the parties do not suffer any monetary loss.

4. Implementation and testing

Our smart contract was implemented and tested using Remix IDE (Integrated Development Environment) – http://remix.ethereum.org. The code was written in Solidity using the web browser-based IDE, Remix, which offers a lot of features that make it possible to test and debug the smart contracts before deploying them. It has a JavaScript EVM (Ethereum Virtual Machine) as a default environment, to run and deploy the contracts locally. Fig. 7 shows a flowchart for the proposed solution for the pharma blockchain supply chain process using smart contract technology. In this section, we provide the main implementation details and focus predominantly on testing the proper interaction among system participants and the smart contract functionality.

4.1. Implementation details

The code is written in Solidity programming using the web browser-based IDE, Remix. Three entities are participating in the contract are seller, the smart container, and the consumer. Each of the entities is identified in the network with an Ethereum address and can participate by calling functions within the smart contract at certain time stamps. Fig. 8 illustrates the sequence flow for a scenario of successful delivery of the pharma package. The seller or manufacturer creates the contract with certain details such as freight tariff, freight's initial state, and the time taken to provide the secret code. Following the package check carried out by the smart container, the smart contract assures both the seller and consumer that the supply chain process carried out can be trusted once the check is successful by the container else the contract terminates and sends out an event to the seller to fix the container issues and also sends a notification to the consumer about the freight status in the form of an event.

As discussed earlier, upon a successful check, the customer is allowed to deposit the shipment purchase price and is provided with a hash. The hash provided acts as a standard that will determine that this is the legitimate receiver of the freight when the shipment arrives at the destination. Once the customer deposits the specified amount in the contract, an event to start the shipment is broadcasted by the smart contract. The container reports to the contract upon reaching the destination and requests the consumer to provide the secret code to unlock the pharma package. The customer provides the secret code, and upon successful authentication, the container unlocks and the freight is delivered to the authorized consumer. An event is transmitted across the network about the successful delivery, triggering to release of shipping payment to the seller. Once the payment process is completed successfully to shut down the current process, the smart contracts call the self-destruct function from within it to signify the closure of the process. This process also sends all of the current smart contract balance to a destination address.

Fig. 9 illustrates the message sequence diagram which discusses two major cases, where the first case is when a hash provided by the consumer at the time of dispatch is not matched but has no breach of contract terms, and the second case is an occurrence of the breach in the contract terms related to shipments such as pressure, temperature violation or delayed delivery due to wrong routes by the container. All these would be sent to the smart contract via the sensors from the smart containers. The contract provides a time frame of 72 h to provide the correct secret code. If the consumer fails to provide it, then 50% of the freight would be refunded to the consumer and the shipment will be terminated permanently. Fig. 8 also illustrates a breach in terms of accidental breakage of the container during transport and in such cases, the smart contract recompenses.

Next, we present the essential code snippets of the smart contract.

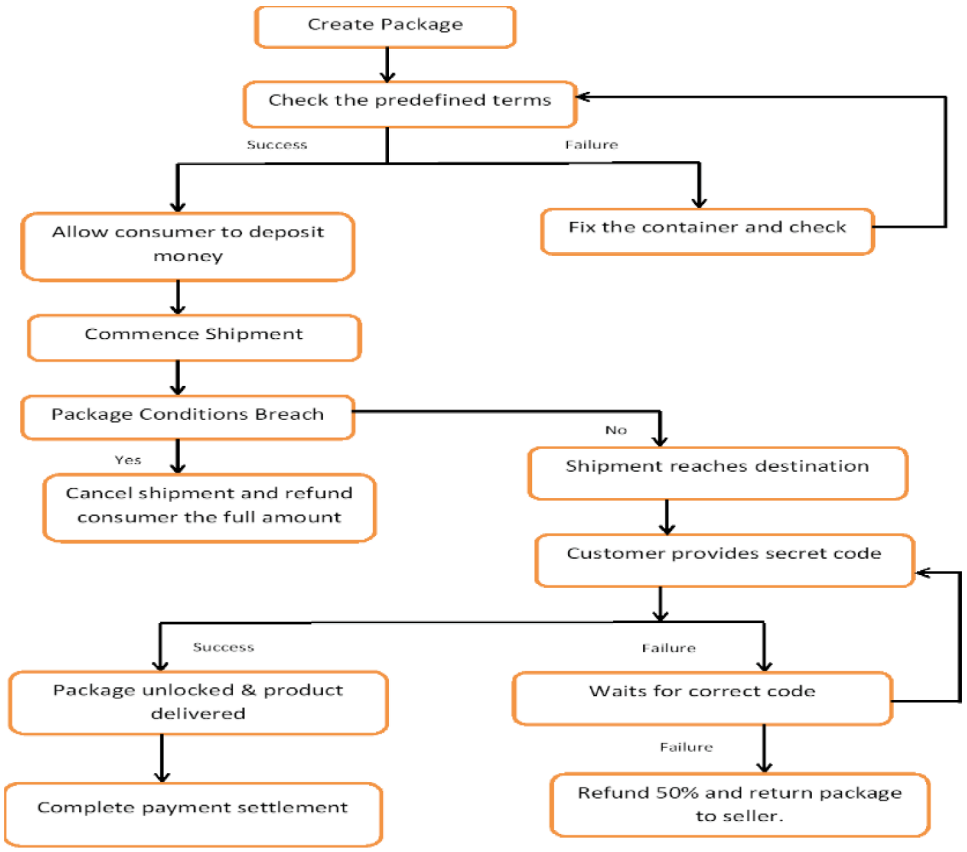

Fig. 7. Flow chart for pharma blockchain supply chain.

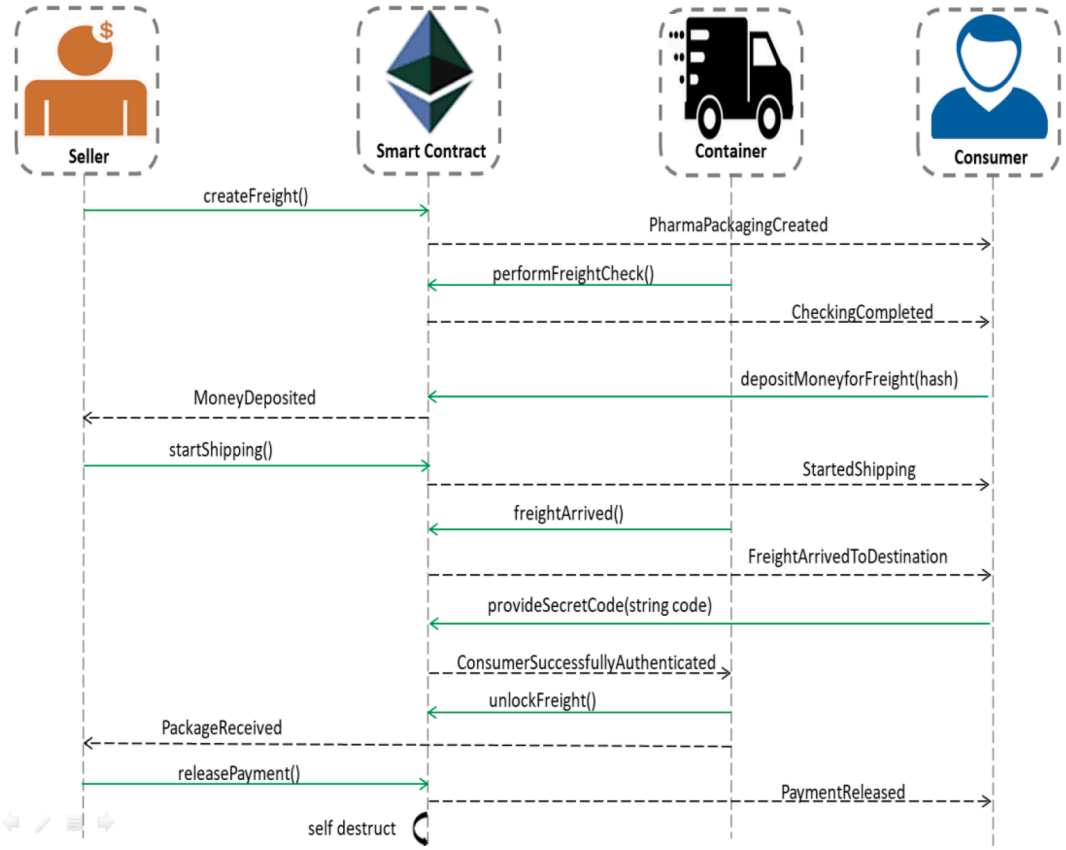

Fig. 8. Message sequee diagram for successful freight delivery.

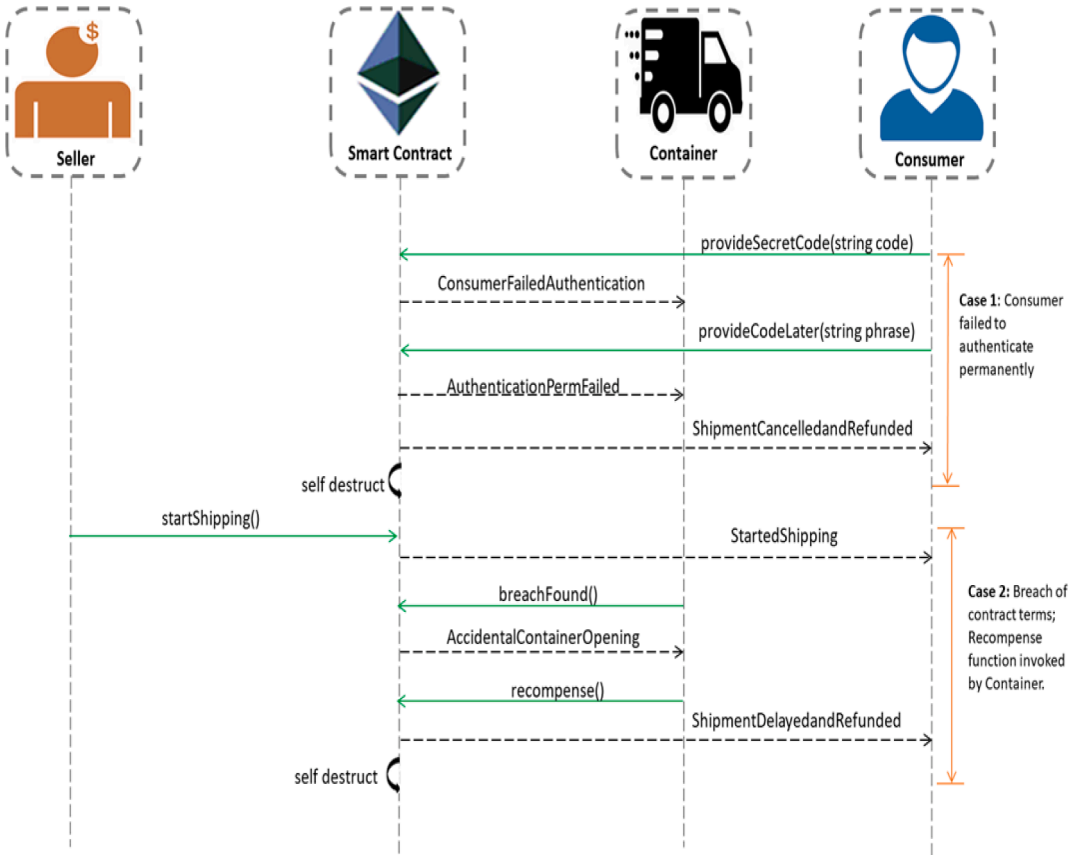

Fig. 9. Message sequence diagram showing a failed consumer authentication [Case 1] and a Breach of shipment specifications [Case 2].

The full code is available at https://github.com/OnlineBookPublishing/Pharma-Supply-Chain. Fig. 10 shows the constructor of the smart contract `PharmaPackage()` which initializes variables such as `batchNumber`, `startDate`, `receivedAfter`, `freightTariff`, and `freightstate`. The state of the freight is `NotReady` and the tariff rate is fixed at 10 ether. For testing purpose, the address of the smart container and consumer are fixed.

The contract state changes to `PharmaPackageReady` once the seller receives an order and executes the `createFreight ()` function. The event `FreightCreated` is sent out to show the completion of package creation. Now the smart container performs the package check; if the result is successful the state of the freight changes to `Freight-Ready` and the event `CheckingCompleted` is broadcasted. The smart contract has one 'payable' function `depositMoneyforFreight()` which is shown in Fig. 11, that allows consumers to deposit ether for a purchase. `MoneyDeposited` is a trigger event that notifies that the customer has deposited money and has been provided with the secret hash.

To improve the security of the proposed solution, a cryptographic hashing technique is applied to the verification of the hash provided by the contract. To verify the legitimacy of a consumer digitally, a secret hash is sent to the consumer who deposited the amount for the freight. When the consumer/ patient receives the pharma package can provide the hash upon delivery, and the smart contract compares and verifies if the hash provided during the amount deposit and the hash provided by the end consumer match. If it matches, the pharma package delivered can be claimed to be in the custody of the legitimate consumer. Fig. 12 demonstrates the code for the `provideSecretCode()` function which is executed by the consumer. It is clear from the figure that the freight state changes to `AuthenticatedByConsumer` if the consumer

```
function PharmaPackage(){
 batchNumber= "Xrdpf";
 startDate = block.timestamp;
 receivedAfter = 3; //3 days maximum for providing
                    another secret code
 pharmacrate = "This package contains pharmaceutical product";
 freightTariff = 10 ether;
 container = 0x583031d1113ad414f02576bd6afabfb302140225;
 seller = msg.sender; //address of sender
 consumer = 0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db;
 freightstate = freightState.NotReady;
 result = 0;
   }
```

Fig. 10. Constructor function[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

```
function depositMoneyforFreight(bytes32 hash)  payable
OnlyConsumer amountsto {
        require(freightstate == freightState.FreightReady);
        //this indicates that check is OK
           freightstate = freightState.MoneyDeposited;
           secrtcode = hash;
       MoneyDeposited("Money deposited and secret
       hash provided", msg.sender); //trigger event
   }
```

Fig. 11. Smart contract function for depositing freight amount[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

```
function provideSecretCode(string code) OnlyConsumer {
require((freightstate == freightState.WaitingforSecretCode ||
freightstate ==  freightState.WaitingForCorrectCode)
&& breach == breachType.None);
  acquiredCodeToBehashed = code;
if(secrtcode == keccak256(acquiredCodeToBehashed)){//authenticated
freightstate = freightState.AuthenticatedByConsumer;
ConsumerSuccessfullyAuthenticated("SUCCESS:Secretcode
                                      matched", msg.sender);
} else {
freightstate = freightState.WaitingForCorrectCode;
ConsumerFailedAuthentication("You have 72 hours to provide the
                    correct code", msg.sender);
          }
     }
```

Fig. 12. Smart contract function for providing the secret code.[1] ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

provides the correct hash or `WaitingForCorrectCode` if the hash does not match. It is important to note that the terms of breach or violation are None in this case.

The container unlocks only when the customer provides the correct hash otherwise the container waits for 3 days for the consumer to provide the correct code. Fig. 13 shows the function `provideCodeLater()` which executes the `ProvideSecretCode` function in case a consumer provides the secret code. In case the consumer does not respond within 3 days or provides a wrong code then the `AuthenticationPermFailed` event is invoked, the shipment is canceled and the consumer is refunded half of the freight tariff.

Upon successful provision of the secret code by the customer, the `unlockFreight()` function is executed by the container, and freight state changes from `AuthenticatedByConsumer` to `FreightReceived`, and the event `PackageReceived` is triggered. Fig. 14 shows the `releasePayment()` function which is executed by the seller to complete the payment for the purchase made. The proposed solution ensures beneficial and agreed on payment of incentives to all participants.

```
function releasePayment() OnlySeller{
  require(freightstate == freightState.FreightReceived);
  //transfer the money to the seller
  seller.transfer(freightTariff);
  PaymentReleased(msg.sender, "Payment made to Seller");
  selfdestruct(msg.sender);
    }
```

Fig. 14. `releasePayment()` function code[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

4.2. Testing

In this section, we focus on testing the precise interaction among the system participants with the help of the Ethereum smart contract. For testing purposes, we consider the Ethereum address of the smart container to be `0x583031d1113ad414f02576bd6afabfb302140225`, the address of consumer / patient, who orders for a pharma package after accepting to pay the predetermined amount of 10 ether, is `0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db` and

```
function provideCodeLater(string phrase) OnlyConsumer {
  if (block.timestamp <= startDate + receivedAfter * 1 days) {
  provideSecretCode(phrase);
  }
  else//it will be more than 3 days
  {
   freightstate = freightState.AuthenticationFailureAborted;
   AuthenticationPermFailed("Failure to provide the correct
                passcode within 72 hours", msg.sender);
   consumer.transfer(freightTariff/2);// half refunded
   ShipmentCancelledandRefunded(msg.sender);
   selfdestruct(msg.sender);
     }
  }
```

Fig. 13. Function for providing secret code later[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

the address of the seller is `0xca35b7d915458ef540ade6068dfe2-f44e8fa733c`. In this section we discuss three scenarios of (1) a Successful purchase; i.e., the customer provides the correct secret code (2) Failed authentication i.e., the customer provides the wrong secret code and is asked to submit the correct code within 3 days (3) Breach occurred during shipment of the freight. In Remix, each entity has 100 Ethers to test the smart contract code. All the functions are executed in sequential order as per the state of the freight. For example, if the transaction fails, if the consumer tries to deposit the freight tariff by executing the `depositMoneyforFreight ()` function before the freight check is performed, an error occurs and the transaction aborts as shown in Fig. 15, and returns to the initial state.

Scenario 1: Successful purchase.

1) Firstly, we test the smart contract for the freight check scenario. Fig. 16 shows the container's success results in checking the predetermined terms. This indicates that the pharma shipment can be initiated as all the predefined rules are met. This console assures the customer that a deposit can be made as the pharma packaging in the container is secure to be sent.

Secondly, we test the contract for a successful deposition of freight money and purchase of a pharma package. Fig. 17 demonstrates the consumer depositing money and receiving a secret hash during the purchase scenario. For testing purpose, we used the secret hash to be "Hello I am Receiver A" whose keccak256hash is '`0xe9dd4-fa294a0dde282d8f232151fc5d9f12b363bb62 f61d6074d2422f1d8e529`' and enter this as an array of one byte ["0xe9","0xdd","0x4f","0xa2","0x94","0xa0","0xdd","0xe2","0x82", "0xd8","0xf2","0x32","0x15","0x1f","0xc5","0xd9","0xf1","0x2b", "0x36","0x3b","0xb6","0x2f","0x61","0xd6","0x07","0x4d","0x24", "0x22","0xf1","0xd8","0xe5","0x29"].

Fig. 18 shows the console of Remix that shows the execution of `depositMoneyforFreight ()` where the consumer deposits 10 ether and provide the bytes32 hash in the form of a one-byte array.

2) Following successful payment by the consumer, the seller initiates the `startShipping()` function and the container announces with an event `FreightArrivedToDestination` when the shipment reaches the consumer. Now the consumer needs to validate its legitimacy by providing the secret code as shown in Fig. 19. The event `ConsumerSuccessfullyAuthenticated` is broadcasted and a log message `SUCCESS: Secretcode` matched is published in the network.

Upon successful authentication, the shipment is unlocked and the consignment is handed over to the consumer. The seller is made aware by invoking the event `PackageReceived` and the state of freight changes to `FreightReceived`. This will enable the seller to execute the `releasePayment()` function as shown in Fig. 20 to complete the payment for the shipment.

Scenario 2: Wrong secret code submitted by the consumer, without any other breach.

This scenario explains the consumer providing the wrong secret code at the time of receiving the pharma package from the container. At this point, the contract provides an option for the consumer to provide the correct code within a specific amount of time (i.e., 3 days in this case). Fig. 21 shows the execution of the `provideCodeLater()` function when the consumer provides the wrong string code (i.e., "hello" instead of the code provided at the time of depositing money for freight). On providing the correct code within 3 days, the container unlocks and the freight is handed over to the consumer; else if the authentication fails, the shipment is terminated and half of the deposit done by the consumer is refunded.

Fig. 22 shows the smart contract state in case of a breach. The type of breach shown in the below figure is about the container taking a wrong route which is recorded via the sensor and reported in the contract during freight. During times of breach, the smart contract is designed to abort the dispatch and refund the deposit made by the consumer.

4.2.1. *Performance analysis of the smart contract in terms of cost*

This subsection discusses the performance of smart contracts in terms of the cost of functions and gas spent for each transaction. When a transaction is committed, it requires a minimum spend on a nominal amount of gas to load it on the Ethereum blockchain to execute the command. Remix IDE environment offers a convenient platform for providing the gas cost of each transaction in the output console. Fig. 22 presents the execution and transactional cost against the smart contract functions of the code. The red line in Fig. 23 is execution costs, "that are based on the cost of computational operations which are executed as a result of the transaction ". The blue line in Fig. 22 represents transaction cost, "*the costs for sending the smart contract code to the Ethereum blockchain, and they depend on the size of the contract*".

5. Discussion

To our knowledge, this is a novel study that has explored the utilization of blockchain technologies in influencing the pharma supply chain industry management principles. Several barriers and risk factors were identified that are consistent with past research (Markarian, 2015; Jüttner et al., 2003, PricewaterhouseCoopers, 2017). These include shipment delivery and accuracy, physical security, and social and economic factors. Cost remains a huge obstacle to achieving dynamic change. While there is huge pressure on pharma companies to deliver through their R&D budget, recent research suggests that only half of them are adopting the right digital tools to achieve this. There is also a lack of integration behind many supply chain components. Today's drug

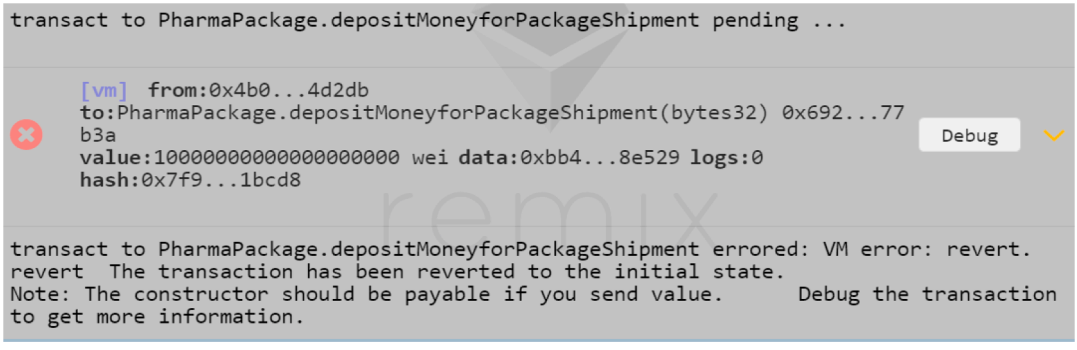

Fig. 15. Logs showing error: when consumer deposits amount before package-check function[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

Fig. 16. Logs showing successful freight check[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

Fig. 17. Logs showing freight amount deposit[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

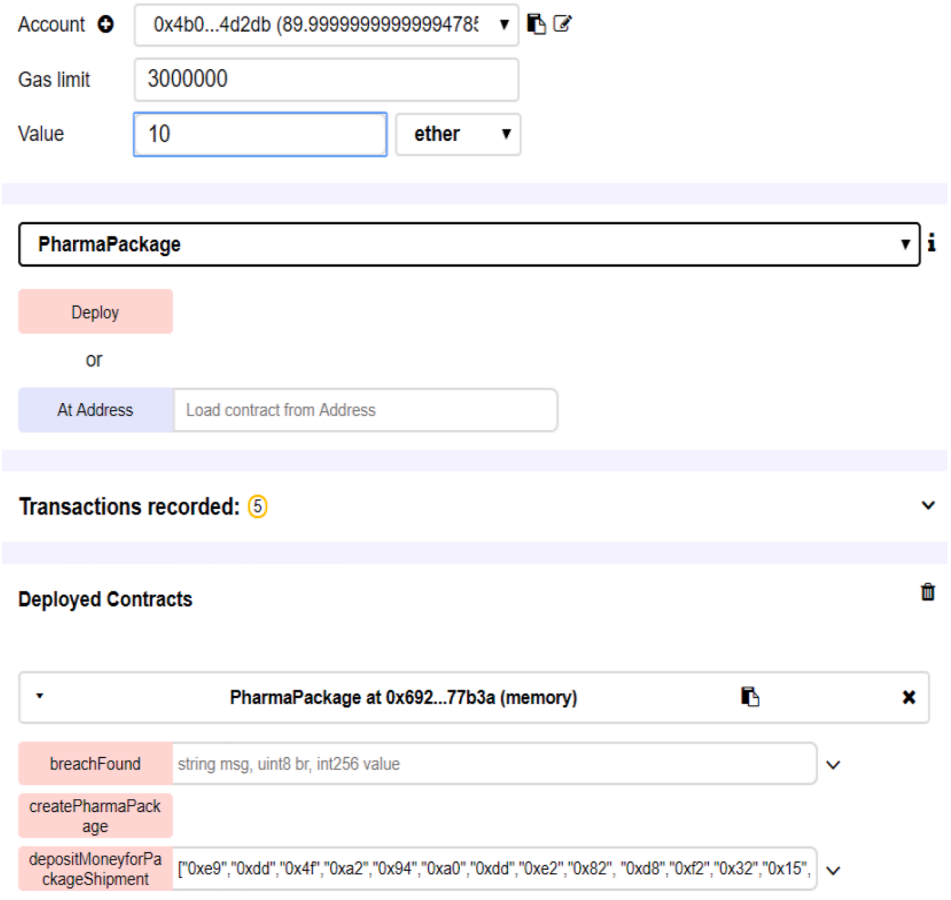

Fig. 18. Logs showing `depositMoneyforFreight()` function[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

makers are clustered and are made up of many divisions spanning multiple geographic regions and operating in complex ecosystems (Fawcett and Magnan, 2002). Inevitably, data flow is complex and prone to delays and networks are open to vulnerabilities, and compliance culture is often mismatched. Patient significance is a new directive for many life sciences companies. The implications are quite prevalent and

Fig. 19. Successful authentication by consumer[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

Fig. 20. Payment made to manufacturer[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

Fig. 21. Consumer submitting a wrong secret code at the time of dispatch[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

influence many of the factors described above. If the industry is to become truly outcome-oriented, then the security of data in digital supply chains must be managed in a robust and scalable way. This is equally true in both emerging as well as more advanced economies.

Blockchain is one of the currently adopted disrupting technologies to improve the traditional structure of various industries due to its features such as transparency, efficiency, and versatility (Abugabah et al., 2020; Allen, 2017; (Nizamuddin and Abugabah, 2021; Abdallah et al., 2019; Ferraro et al., 2018; (Sanka et al., 2021); Katuwal et al., 2018; Kuo et al., 2017). Our findings contribute to utilizing the advantage of decentralized blockchain technology to solve the major issues that are affecting the supply chain industry. The noteworthy feature of our contribution is that we deployed the smart contracts on the open-source Ethereum platform and executed our framework which proved to eliminate the need for a trusted third party in the supply chain management process and automate the payment process. Also, Abugabah et al. (2020) highlight the employment of blockchain in telehealth and telemedicine systems, to deliver remote healthcare services which can be very useful in mitigating the recent spread of the Covid-19 pandemic. Bocek et al (2017) in their research have highlighted modum.io a startup

```
logs
[
        {
                "from": "0x692a70d2e424a56d2c6c27aa97d1a8639587
7b3a",
                "topic": "0x12de8f30aca55284a6ee0af48fa60f4ac7c
fb0c8d3578faf22d0acd1423e7a1e",
                "event": "OutofTrack",
                "args": {
                        "0": "Wrong Track",
                        "1": true,
                        "2": "1",
                        "msg": "Wrong Track",
                        "r": true,
                        "br": "1",
                        "length": 3
                }
        },
        {
                "from": "0x692a70d2e424a56d2c6c27aa97d1a8639587
7b3a",
                "topic": "0x3a17555898451944bdb1842d01d9a01aacd
391d94ad488bbc9085342d64b66cb",
                "event": "ShipmentDelayedandRefunded",
                "args": {
                        "0": "0x583031D1113aD414F02576BD6afaBfb
302140225",
                        "container": "0x583031D1113aD414F02576B
D6afaBfb302140225",
                        "length": 1
```


Fig. 22. Logs showing a breach condition[1]. ([1]Code available at: https://github.com/nisharan/OnlineSupplyChainManagement).

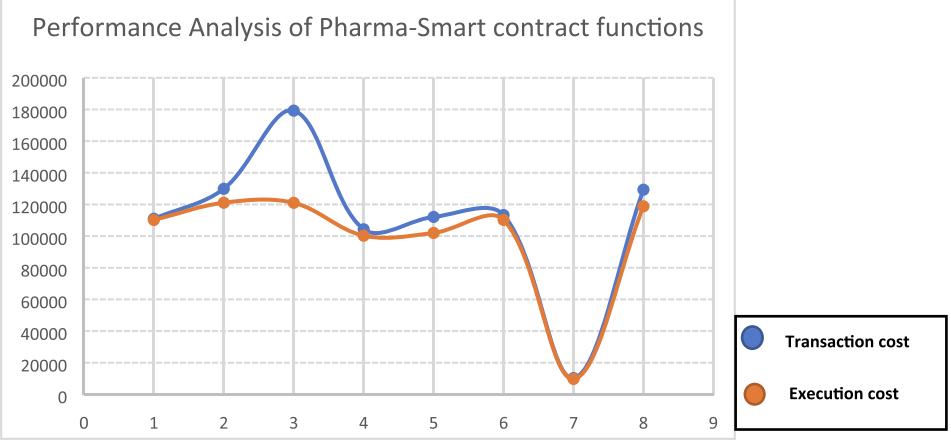

Fig. 23. Performance analysis of Pharma-smart contract functions.

that uses IoT sensors to monitor the records and reduce the cost of the pharmaceutical supply chain. Since the medical industry has many complexes and strict regulatory compliance over the shipment and dispatch of medical products, the use of IoT devices can ensure rigorous quality control and regulations.

Smart contracts are employed to assess and govern the pharma freights' attributes such as temperature, number of days to deliver the product, and pressure mentioned in the dispatch agreements between stakeholders involved. Many logistics industries such as DHL and Accenture have started adopting and trailing using blockchain technology to eliminate counterfeit products and ensure that delivery of the goods is not tampered with (SupplyDemandChain, 2018). These organizations have built a working prototype that tracks the pharma products from point of origin until it reaches the consumer, preventing tampering and any dispatch errors but have not implemented a fully functional system. Multi-tier, highly disjointed, and geographically spread are some of the characteristics of today's supply chain (Jüttner et al., 2003; Oracle NetSuite, 2022; Oracle, 2018). All these common grounds constitute complexity in probing incidents and tracing or tracking events in case of abrupt disruptions. The end-to-end transactions starting from manufacturer to end consumer are usually opaque which makes the supply chain management more complicated. There is an alarming need for this chain to be transparent which can now be made possible with the help of blockchain. Blockchain can be also useful in tackling certain sustainable development issues (Lund et al., 2019), as discussed in Table 1. Integrating blockchain into business application systems such as enterprise resource planning (ERP), customer relationship management (CRM), warehouse management system (WMS), and manufacturing execution systems (MES), will enhance the profit and help the customers to achieve success as proposed by Infosys (Infosys, 2018). Further, the benefits of integrating the ERP systems and blockchain discussed in this report are:

- The entire process of manufacturing, tracking, sales, and purchase and its integration with blockchain will hold an immutable and tamper-proof copy of transactions to be used as a reference at any time by authentic participants.
- The financial transactions generated by ERP systems can be made transparent and reliable by integrating with blockchain.
- Blockchain, when integrated with ERP, WMS, and MES systems, can reduce feuds over invoices, purchases, shipments, and returns. All these are recommendations and high-level business ideologies with no practical implementation.

Finlync (2003), a pioneer in leading innovation for financial institutions and businesses in ERPhasve developed a plug–and–play integration for SAP, Ethereum, and Hyperledger blockchains for managing a business in the digital era. It offers more services such as integration of SAP with other blockchains and extending services in finance, HR, and supply chain. It is highlighted that three potential areas in the supply

Table 1
Blockchain-based solutions for sustainability issues in the supply chain (Lund et al., 2019; Alharthi et al., 2020).

Sustainability Problems	Blockchain-based solutions
Economic-related	Permits disintermediation where lower tiers assist to minimize the cost of time and transaction, thereby reducing minimal waste.
Environmental	Tracking substandard products; Enhances transparency and traceability of smart contracts resulting in increased sustainability of the environment.
Access to High-Quality Data for Everyone	All parties involved in a transaction will have accurate, timely, consistent, and complete data to make a well-informed decision.
Unethical Suppliers and Counterfeit Products	Proactive supply chain sustainability can be achieved using blockchain as the data it offers can help identify and correct contract violations, redundancies, and bottlenecks in the flow of goods.
Social	Increased transparency between stakeholders of the supply chain industry across the globe, leading to social sustainability. Helps government to track government policy adherence corresponding to the working hours of employees.
Improved Visibility	Visibility, identifying all parties involved in a transaction, the state, quality, and price of the products as well as the date and location of the transaction is recorded in an immutable fashion and becomes evident.

chain domain can be improved. Firstly, it is the emergence of middleware technologies such as Microsoft Dynamics NAV, AX, and CRM. The second is the identification of use cases in the supply chain that can benefit from the blockchain network and the third is blockchain as a service (BaaS). Many mid-size organizations are now adopting ERP systems on a larger scale.

The cardinal feature of ERP systems is a shared database that supports all the functions across different business units defined (Oracle, 2018). Parties across different business divisions, for example, accounting, sales, and logistics can rely on and operate upon the same information for carrying out business operations. Technology-based solutions such as Cloud-based solutions - Software-as-a-Service can help to implement such a system that makes the ERP software affordable, easier to implement and manage, and empowers employees by presenting real-time business intelligence reports. Organizations need to understand the capabilities of IoT and blockchain to identify and address the supply chain industry's challenges. Oracle and Delloite (Oracle, 2018) have come together to identify the core use cases to apply blockchain functionality to the supply chain process. The report comprises 5 use cases:

- Tracking of the product throughout the supply chain process including the origin and product journey tracking.
- Digitization and auto verification of all supply chain documents.
- Monitoring and exceptional handling of quality attributes such as temperature, volume, and weight.
- Handling Settlements or reverse logistics.
- Automated monetary settlements without intermediaries.

By adopting a blockchain and IoT-based approach, parties involved can embark on an innovative and secure journey by adopting a value-driven approach. Traditional business structures may not be effective for such decentralized ecosystems due to their dynamic nature. To utilize the benefits of innovative technologies and implement the system successfully, robust risk management strategies and governance frameworks need to be constructed. The report emphasizes the importance of robust system architecture, communication architecture, and security paradigms to consider, setting up regulations and standards, and definite security practices.

Oracle (Oracle NetSuite, 2022; Oracle, 2018) has also highlighted that a transparent and secure supply chain can be made possible by integrating blockchain with the ERP systems for a value-driven approach. It is suggested that by integrating parties across diverse business divisions and by operating on a unique set of information, the integrity of the business can be well improved by keeping the middlemen at bay. Employing cloud technologies such as IoT can help all partners within the business chain to keep well informed about the movement of the products in the supply chain, any violation or breach that may occur during the transportation of goods, and ensure end-consumer satisfaction. Further, by inculcating blockchain technology, auto verification of all supply chain agreements and contracts signed between business collaborators can be governed and monitored by all proprietors involved. Table 3 presents the comparative analysis of the cost between the traditional approaches and the blockchain-based approach for carrying out supply chain projects.

Though blockchain has gained importance across many platforms and industries, there are several research questions still to be addressed. Although the business activities carried out vary between organizations, the operational issues in the pharmaceutical supply chain continue to prevail (Yli-Huumo et al., 2016); (Reyna et al., 2018). The most common shortcomings are:

- ***Gaining industry adoption:*** Most industries are still in the process of adopting digital tools and upcoming technologies. There is always a certain amount of reluctance in embracing new technologies into business as the outcome is unknown and there is a measurable percentage of the opinion of the stakeholders and partners involved in making new business decisions.
- ***Setting standards and regulations:*** The primary challenge for blockchain adoption is regulation. The regulatory standard has not caught up to innovation and is slow in many cases in the adoption of new technologies. More products, technologies, and services can be utilized by mainstream consumers only when there is a robust regulatory framework, though in many cases consumers are not aware of the changes taking place in the business world.
- ***Scalability:*** Mass adoption across industries is not possible if blockchain can't scale related to latency and throughput, as slower applications can't be adopted for the sake of decentralization. EOS (EOS.IO is the system architecture) (Reyna et al., 2018) is one of the projects trying to solve the scalability issues for decentralized applications. This project uses the Delegated proof of stake consensus algorithm and has adopted parallel processing technology which enables Decentralized Applications (DApps) and transactions to be processed simultaneously without doubling the load on the network which can be made possible by adding processing power and machines to the resource pool.
- ***Integrating with IoT:*** Bitcoin has been recently used to provide security in p2p systems (Reyna et al., 2018). However, blockchains are computationally expensive and involve high bandwidth delays and overheads, which is not suitable for IoT devices. In a typical IoT deployment, limited resource devices are used for forwarding sensor data to upper layers. When integrating with blockchain, end nodes need a cryptographic functionality to be provided to IoT devices. When implementing on a large scale, these factors are important to be considered.

The DAO (Distributed Autonomous Organization) attack is one of the major attacks that ever happened in the Bitcoin industry, in which the hacker drained 3.6 M ether, forcing the Ethereum founders to take radical measures and create a hard fork to salvage the lost funds. However, with stable programming practices, the attacks on smart

contracts can be warded off effectively. On the other hand, when it comes to real-world implementation by utilizing sensors, hardware plays a key role in determining the accuracy of data, which is assured by the quality control team of the manufacturer. To verify that, we need to hit the hardware commands from User Interface - through the sensor attached to the controller. However, we are yet to implement it practically for our blockchain-based application. Also, the storage of data collected from sensors needs to be stored on a decentralized file system named IPFS (Interplanetary file system) as blockchain is not capable of storing a large quantity of data. IPFS is one of the most trusted file systems for handling data storage for blockchain. It uses hash keys. We have planned to implement this as a part of future work. A stable and robust framework can only be designed if the challenges are addressed. Besides, the article aims to assimilate the payment processing features into the existing design, in which automatic payments can be made possible with cryptocurrency transactions.

6. Conclusion

In this paper, we have adopted the design science research model, to propose a solution for the pharma supply chain industry. The proposed framework will guarantee the delivery of credible pharmaceutical products to the end consumer using IoT sensor technology and blockchain technology powered by smart contracts. Our proposed framework focuses on the pharmaceutical supply chain, but our solution framework and smart contract code and algorithms are generic enough to be extended and applied to other supply chain frameworks that transport perishable goods. We implemented the functionality of the smart contract code using Remix IDE and focused on cases related to the trustworthiness in the delivery of the pharmaceutical package, detection of breaches during transportation, and refunds. In future work, we plan to deploy smart contracts on the Hyperledger platform and develop Decentralized Applications (DApps) with various other real-world entities such as drug manufacturers, distributors, and patients.

CRediT authorship contribution statement

Salam Abdallah: Conceptualization, Supervision, Validation, Visualization. **Nishara Nizamuddin:** Conceptualization, Methodology, Writing – original draft, Software, Investigation, Visualization.

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.

Acknowledgment

We would like to thank Abu Dhabi University management for the support in carrying out this research work. We would also like to thank the reviewers and editorial team for their valuable insights.

References

Abdallah, S., Nizamuddin, N., & Khalil, A. (2019). Blockchain for improved safety of smart buildings. In *International Conference Connected Smart Cities 2019, Portugal*.

Abugabah, A., Nizamuddin, N., & Alzubi, A. A. (2020). Decentralized telemedicine framework for a smart healthcare ecosystem. *IEEE Access, 8*, 166575–166588.

Abugabah, A., Nizamuddin, N., & Abuqabbeh, A. (2020). A review of challenges and barriers to implementing RFID technology in the Healthcare sector. *Procedia Computer Science, 170*, 1003-1010.

Alharthi, S., Cerotti, P. R., & Far, S. M. (2020). An exploration of the role of blockchain in the sustainability and effectiveness of the pharmaceutical supply chain. *Journal of Supply Chain and Customer Relationship Management, 20*(1), 1–29.

Ahmad, A. (2017). *Integration of IoT devices via a blockchain-based decentralized application* (Master's thesis).

Allen, M. (2017) How blockchain could soon affect everyday lives. http://www.swissinfo.ch/eng/joining-the-blocks_how-blockchain-could-soon-affect-everyday-lives/43003266. Accessed 28 Jan 2022.

Atlam, H. F., & Wills, G. B. (2019). Intersections between IoT and distributed ledger. In *Advances in Computers* (Vol. 115, pp. 73–113). Elsevier.

Ballou, R. H., Gilbert, S. M., & Mukherjee, A. (2000). New managerial challenges from supply chain opportunities. *Industrial Marketing Management, 29*(1), 7–18.

Barry, J. (2014). Fake medicines: a global threat. *Nursing Management (Harrow, London, England: 1994)* 21(8), 17-17.

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere-a use-case of blockchains in the pharma supply chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)* (pp. 772–777). IEEE.

Berry, B., Donato, L., and McCarthy, W., Blumshapiro. (2019). Blockchain and RFID: In Pursuit of the Internet of Things. Available [online]: http://us-tech.com/RelId/2116163/ISvars/default/Blockchain_and_RFID_In_Pursuit_of_the_Internet_of_Things.htm, Accessed 25 Feb 2022.

Brechtelsbauer, E. D., Pennell, B., Durham, M., Hertig, J. B., & Weber, R. J. (2016). Review of the 2015 drug supply chain security act. *Hospital Pharmacy, 51*(6), 493–500.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303.

Chronicled (2017). Pharma companies tap start-ups to develop the protocol for tracking and verifying prescription drugs using blockchain. http://www.prnewswire.com/news-releases/pharma-companies-tap-startups-to-develop-protocol-for-tracking-and-verifying-prescription-drugs-using-blockchain-300428313.html. Accessed 18 Jan 2022.

Clark, B., & Burstall, R. (2018). Blockchain, IP, and the pharma industry—how distributed ledger technologies can help secure the pharma supply chain. *Journal of Intellectual Property Law & Practice, 13*(7), 531–533.

Clauson, K. A., Breeden, E. A., Davidson, C., and Mackey, T. K. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare. Blockchain in Healthcare Today. Available [online]: https://blockchainhealthcaretoday.com/index.php/journal/article/view/20. Accessed 27 May 2020.

Dannen, C. (2017). *Introducing Ethereum and solidity* (Vol. 1,, 159–160.

Fabiano, N. (2017). The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. In *2017 International Conference on Internet of Things for the Global Community (IoTGC)* (pp. 1–7). IEEE.

Fawcett, S. E., & Magnan, G. M. (2002). The rhetoric and reality of supply chain integration. *International Journal of Physical Distribution & Logistics Management*.

Federal Trade Commission (FTC) (2005) Workshop on RFID: Applications and Implications for consumers. Available [online]: https://www.ftc.gov/sites/default/files/documents/reports/rfid-radio-frequency-identification-applications-and-implications-consumers-workshop-report-staff/050308rfidrpt.pdf. Accessed 20 Jan 2022.

Ferraro, P., King, C., & Shorten, R. (2018). Distributed ledger technology for smart cities, the sharing economy, and social compliance. *IEEE Access, 6*, 62728–62746.

Finlync (2003). Available [online]: https://www.finlync.com/. Accessed 18 Feb 2022.

Glass, B. D. (2014). Counterfeit drugs and medical devices in developing countries. *Research and Reports in Tropical Medicine, 5*, 11.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 337–355.

Infosys. Perspective: Integrating Blockchain with ERP for a Transparent Supply Chain. Whitepaper. Available [online]: https://www.infosys.com/Oracle/white-papers/Documents/integrating-blockchain-erp.pdf. Accessed 18 Jan 2022.

Interpol. Fake Medicines. Available [online]: https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Fake-medicines. Accessed 25 Feb 2022.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics: Research and Applications, 6*(4), 197–210.

Katuwal, G. J., Pandey, S., Hennessey, M., & Lamichhane, B. (2018). Applications of blockchain in healthcare: current landscape & challenges. *arXiv preprint arXiv: 1812.02776*.

Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220.

Lund, E. H., Jaccheri, L., Li, J., Cico, O., & Bai, X. (2019, May). Blockchain and sustainability: A systematic mapping study. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)* (pp. 16-23). IEEE.

Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert opinion on Drug Safety, 16*(5), 587–602.

Majdalawieh, M., Nizamuddin, N., Alaraj, M., Khan, S., & Bani-Hani, A. (2021). Blockchain-based solution for Secure and Transparent Food Supply Chain Network. *Peer-to-Peer Networking and Applications, 14*(6), 3831–3850.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251–266.

Markarian, J. (2015). Understanding Risks in Pharmaceutical Shipping. *Pharmaceutical Technology, 39*(8), 52–54.

McKinsey & Company. (April 2020). COVID-19 and commercial pharma: Navigating an uneven recovery. Available [online]: https://www.mckinsey.com/~/media/McKinsey/Industries/Pharmaceuticals%20and%20Medical%20Products/Our%20Insights/COVID%2019%20and%20commercial%20pharma%20Navigating%20an%20une

ven%20recovery/COVID-19-and-commercial-pharma-navigating-an-uneven-recovery-vF.pdf, Accessed 23 Feb 2022.
Modum. Next-Generation Supply Chain Automation and Intelligence. [Online] Available at https://modum.io/. Accessed 8 Feb 2022.
Nizamuddin, N., & Abugabah, A. (2021). Blockchain for automotive: An insight towards the IPFS blockchain-based auto insurance sector. *International Journal of Electrical & Computer Engineering* (2088-8708), 11(3).
Nizamuddin, N., & Pandey, R. (2015). Enhancing Security in Public Clouds using Data Anonymization Techniques. *International Journal of Computer Applications, 975*, 8887.
Nunamaker, J. F., Jr, Chen, M., & Purdin, T. D. (1990). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89–106.
Oracle. Enhancing Supply Chains with the Transparency and Security of Distributed Ledger Technology- Value Driven Supply Chain powered by Blockchain and IoT. Aug 2018. https://www.oracle.com/a/ocom/docs/deloitte-oracle-blockchain-supply-chain-pov-vf.pdf Accessed 8 Jan 2022.
Oracle Netsuite. What is ERP? Enterprise Resource Planning Systems Transform. Integrate and Scale Businesses, (January 5, 2022). Available [online]: http://www.netsuite.com/portal/resource/articles/erp/what-is-erp.shtml. Accessed 8 Jan 2022.
Peffers, K., Rothenberger, M., Kuechler, B. (2012) Design Science Research in Information Systems. Advances in Theory and Practice (Lecture notes in computer science, 7286).
Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45–77.
Peirce, C. S. (1974). *Collected papers of charles sanders peirce* (Vol. 5). Harvard University Press.
PricewaterhouseCoopers, Fighting counterfeit pharmaceuticals, (2017). Available [online]: https://www.strategyand.pwc.com/gx/en/insights/2017/fighting-counterfeit-pharmaceuticals/fighting-counterfeit-pharmaceuticals.pdf, Accessed on 14th February 2022.
Purao, S. (2013). Truth or dare: The ontology question in design science research. *Journal of Database Management (JDM), 24*(3), 51–66.
Rabah, K. (2017). Challenges & opportunities for blockchain powered healthcare systems: A review. *Mara Research Journal of Medicine & Health Sciences*, *1*(1), 45-52.
Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy, 16*(5), 583–590.
Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190.
Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications, 169*, 179–201.
Supply&DemandChain. DHL Trials Blockchain in Pharma Supply Chain. (March 13, 2018). Available [online]: https://www.sdcexec.com/software-technology/news/20996111/dhl-trials-blockchain-in-pharma-supply-chain. Accessed 17 Feb 2022.
Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling design process. *AI magazine, 11*(4), 37–48.
Toyoda, K., Mathiopoulos, P. T., Sasase, I., & Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access, 5*, 17465–17477.
Tseng, J. H., Liao, Y. C., Chong, B., & Liao, S. W. (2018). Governance on the drug supply chain via gcoin blockchain. *International Journal of Environmental Research and Public Health, 15*(6), 1055.
Wajsman, N., AriasBurgos, C., & Davies, C. (2016) EUIPO. The economic cost of IPR infringement in the pharmaceutical industry. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study9/pharmaceutical_sector_en.pdf. Accessed 28 Jan 2022.
Waters, D. (2019). *Supply chain management: An introduction to logistics*. Bloomsbury Publishing.
World Health Organization. Substandard and falsified medical products. Available [online]: https://www.who.int/health-topics/substandard-and-falsified-medical-products#tab=tab_1, Accessed 25 Feb 2022.
Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper, 151*(2014), 1–32.
Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? — a systematic review. *PloS one, 11*(10), e0163477.
Yue, D., Wu, X., & Bai, J. (2008, October). RFID application framework for pharmaceutical supply chain. In *2008 IEEE International Conference on Service Operations and Logistics, and Informatics* (Vol. 1, pp. 1125-1130). IEEE.
Zhou, L., Chong, A. Y., & Ngai, W. T. (2015). Supply chain management in the era of the internet of things. *International Journal of Production Economics, 159*, 1–3.