International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X

A Blockchain-based Approach for Drug Traceability in Healthcare Supply Chain

Assistant Professor Mrs.J.Sunanthini[1], Ashina.R[2], Priskila.B[3], Pushpa Lincy.J[4], Sanju.P[5]
Stella Mary's College Of Engineering,

Abstract- Counterfeit drugs are an immense threat for the pharmaceutical industry worldwide due to limitations of supply chain. Our proposed solution can overcome many challenges as it will trace and track the drugs while in transit, give transparency along with robust security and will ensure legitimacy across the supply chain. It provides a reliable certification process as well. Fabric architecture is permissioned and private. Hyperledger is a preferred framework over Ethereum because it makes use of features like modular design, high efficiency, quality code and open-source which makes it more suitable for B2B applications with no requirement of cryptocurrency in Hyperledger Fabric. QR generation and scanning are provided as a functionality in the application instead of bar code for its easy accessibility to make it more secure and reliable. The objective of our solution is to provide substantial solutions to the supply chain stakeholders in record maintenance, drug transit monitoring and vendor side verification.

Index Terms- Counterfeit drugs, pharmaceutical industry, supply chain, trace and track, transparency, security, legitimacy, certification process, Fabric architecture, permissioned, private, Hyperledger, B2B applications

I. INTRODUCTION

Ealthcare supply chain is a complex network of several independent entities that include raw material suppliers, manufacturer, distributor, pharmacies, hospitals and patients. Tracking supplies through this network is non-trivial due to several factors including lack of information, centralized control and competing behaviour among stakeholders. Such complexity not only results in inefficiencies such as those highlighted through COVID-19 pandemic [1] but can also aggravate the challenge of mitigating against counterfeit drugs as these can easily permeate the healthcare supply chain.

Counterfeit drugs are products deliberately and fraudulently produced and/or mislabeled with respect to identity and/or source to make it appear to be a genuine product [2], [3]. Such drugs can include medications that contain no active pharmaceutical ingredient (API), an incorrect amount of API, an inferior-quality API, a wrong API, contaminants, or repack- aged expired products. Some counterfeit medications may even be incorrectly formulated and produced in substandard conditions [4].

According to the Health Research Funding Organization, up to 30% of the drugs sold in developing countries are counterfeit. Further, a recent study by World Health Organi- zation (WHO) indicated counterfeit drugs as one of the major causes of deaths in developing countries, and in most cases the victims are children [7], [8]. In addition to the adverse impact on human lives, counterfeit drugs also cause significant economic loss to the pharmaceutical industry. In this respect, the annual economic loss to the US pharmaceutical industry due to counterfeit medicine is estimated around $200 billion [9], [10].

A typical drug supply chain distribution process is illus- trated in Figure 1. An API supplier is responsible for delivering the raw materials to manufacture drugs approved by a regu- latory agency such as the US Food and Drug Administration (US FDA). The manufacturer packages the drugs into a Lot or sends it to a re-packager. The primary distributor receives several Lots of the product and is responsible for transferring them to pharmacies based on product demand or secondary distributors (in case the quantity of Lots is very large) who can transfer these Lots to the pharmacies. Finally, a pharmacy will dispense the drug to patients [11] typically based on a doctor's prescription. figure 1 depicts the Drug supply chain stakeholders and their relationships. Throughout the supply chain, the transfer of drugs is usually facilitated by third party logistic service providers such as UPS or FedEx and in some cases the distributors operate their own fleet of vehicles to transport the products.

The primary reason for counterfeit drugs to reach end-user marketplace is due to the complex structure of a healthcare supply chain. Leveraging the complexity of this distribution process, medications can easily pass through with little or no trail of information and verifiable documentation [12].

Consequently, monitoring, effective control and tracking of products in healthcare supply chain is fundamental to com- bating counterfeits.

The importance of drug traceability (track and trace) is increasingly emphasized and mandated by several countries across the world. For example, the U.S. Drug Supply Chain Security Act (DSCSA) has made it mandatory for the phar- maceutical industry to develop an electronic and interoperable system that identifies and tracks prescription drugs as they are distributed across the United States [13]. Similarly, over the last 8 years, China required all the stakeholders involved in the drugs supply chain to record information of individual pharmaceutical products in a specialized IT system whenever drugs are sent to/from their warehouses [14]. Therefore, drug traceability has become an integral part of the pharmaceutical supply chain as it establishes authenticity, and aims to track and trace chain of custody of the product across drug supply chain.

Blockchain technology has introduced a new model of application development primarily based on the successful implementation of the data structure within the Bitcoin ap- plication. The fundamental concept of the blockchain data structure is similar to a linked list i.e. it is shared among all the nodes of the network where each node keeps its local copy of all the blocks (associated with the longest chain) starting from its genesis block [15]. Recently, many real- world applications have been developed in diverse domains, such as the Internet of Things [16], e-Government [17] and e-document management [18]. These applications leverage benefits of blockchain technology due to its self-cryptographic validation structure among transactions (through hashes), and public availability of distributed ledger of transaction-records in a peer-to-peer network. Creating a chain of blocks con- nected by cryptographic constructs (hashes) makes it very difficult to tamper the records, as it would cost the rework from the genesis to the latest transaction in blocks as illustrated by [19].

Within the context of blockchain-based traceability for pharmaceutical supply chain, [20] presents one of the initial efforts. Although our solution has similarities with this effort due to the focus on pharmaceutical supply chain as well as the use of blockchains, we take a holistic view of the pharmaceu- tical supply chain, presenting an end-to-end solution for drug traceability whereas [20] only focused on a subset of these challenges. Firstly, our approach identifies and engages major stakeholders in the drug supply chain i.e. the FDA, supplier, manufacturer, distributor, pharmacy, and patient, whereas [20] is limited to the supplier, manufacturer, and wholesaler as the stakeholders. Consequently, the pharmacists are represented as an external entity which is not the case in a real drug supply chain.

Secondly, we make explicit efforts to identify and define relationships among stakeholders, on-chain resources, smart contracts, and decentralized storage systems which is lacking in [20]. Figure 1.1 depicts the Drug supply chain stakeholders and their relationships.Furthermore, in view of the significance of interactions among stakeholders, we have included precise definitions to remove any ambiguity, whereas such interactions have not been defined as part of [20]. Thirdly, we use the smart contracts technology to achieve real-time, seamless traceability with push notifications so as to minimize human intervention and therefore undesired delays. Specifically, each drug Lot is assigned a unique smart contract that generates an event whenever a change in ownership occurs and a list of events is delivered to the DApp user. However, the smart contracts in [20] are programmed for specific roles such as supplier, manufacturer, and wholesaler which requires each participant to manually confirm which drugs are received. Such approach can introduce delays and inaccuracies in the immutable data stored on the ledger. Finally, we have conducted a cost and security analysis to evaluate the performance of the proposed solution including discussion on how the proposed solution can be generalized to other supply chains.

The challenge of achieving traceability to mitigate against counterfeit drugs is well-established and several efforts have been made to address this within pharmaceutical indus- try. However, a careful review of literature presents several gaps and opportunities for a comprehensive application of blockchain technology for drug traceability. In this context, the primary contributions of this article can be summarized as follows:

- We propose a blockchain-based solution for the pharma- ceutical supply chain that provides security, traceability, immutability, and accessibility of data provenance for pharmaceutical drugs.
- We design a smart contract capable of handling various transactions among pharmaceutical supply chain stake- holders.
- We present, implement and test the smart contract that defines the working principles of our proposed solution.
- We conduct security and cost analysis to evaluate the performance of the proposed blockchain-based solution.

The reminder of this article is organized as follows. Section II presents a critical review of existing efforts with respect to traceability in the healthcare supply chain. This is followed by a description of the proposed blockchain-based track & trace system for phamaceutical products in section III. Section IV presents the implementation of the proposed system along with details of the testing and evaluation in section V. Section VI describes the efforts to evaluate the proposed system and an- alyzes the outcomes of evaluation. Section VII concludes this article summarizing contributions and highlighting avenues for further work.

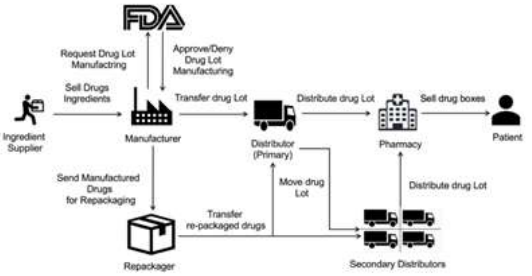

Fig .1 Drug supply chain stakeholders and their relationships

Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Structure

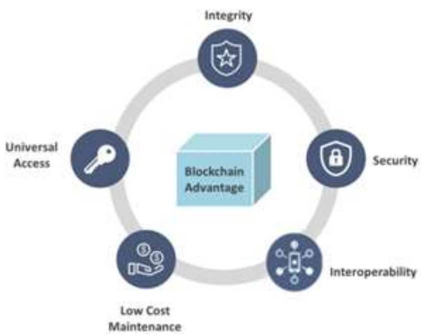

Figure 1.2 depicts the structure of a blockchain)

A blockchain is a decentralized, distributed, and often- times public, digital ledger that is used to record transac- tions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively.

A blockchain database is managed autonomously using a peer- to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long- standing problem of double spending. A blockchain has been described as a value-exchange protocol. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

Block time

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions.

II. RELATED WORKS

N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, ”Decentralized document version control using ethereum blockchain and IPFS,” Comput. Electr. Eng., vol. 76, pp. 183-197, Jun. 2019.
In this paper, we propose a blockchain-based solution and framework for document sharing and version control to facilitate multi-user collaboration and track changes in a trusted, secure, and decentralized manner, with no involvement of a centralized trusted entity or third party. This solution is based on utilizing Ethereum smart contracts to govern and regulate the document version control functions among the creators and developers of the document and its validators. Moreover, our solution leverages the benefits of IPFS (InterPlanetary File System) to store documents on a decentralized file system. The proposed solution automates necessary interactions among multiple actors comprising developers and approvers. Smart contracts have been developed using Solidity language, and their functionalities were tested using the Remix IDE (Inte- grated Development Environment). The paper demonstrates that our smart contract code is free of commonly known security vulnerabilities and attacks.

M. Muniandy. O. Gabriel, and T. Ern, ”Implementation of pharmaceutical drug traceability using blockchain technol- ogy,” Int. J., vol. 2019, p. 35, Jun. 2019.
The healthcare industry relies heavily on the use of pharmaceutical drugs to treat patients, and acquires said drugs using supply chain management. However, fraud and abuse cases in current healthcare industry are a major problem, costing the industry billions of dollars annually. Furthermore, counterfeit drugs also plague the healthcare industry, which is a major health concern to patients who consume said drugs. To solve these problems, a system is required to trace pharmaceutical drugs as they travel the supply chain, from the provider of the ingredients to produce pharmaceutical drugs, to its consumers. The proposed project will implement blockchain, an emerging technology that enables decentralized storage of data and immutable data. Blockchain stores data in a distributed ledger visible to all participants, which will create transparency in the supply chain, a much-needed change, which are presently very complex and opaque. Blockchain records the transaction details of relevant participants involved in the supply chain process as pharmaceutical drugs move through the supply chain.

B. A. Supriya and I. Djearamane, ”RFID based cloud supply chain management”, Int. J. Sci. Eng. Res., vol. 4, no. 5, pp. 2157-2159, 2013.
Radio Frequency Identification (RFID) is a key enabler for our proposed Cloud based supply chain management service. The problem area introduced here is to experiment and figure out the less expensive passive RFID in the global supply chain process using the latest cloud-based software infrastruc- ture. This paper embraces briefly the underlying principle of RFID, introduction about supply chain management process and our proposed solution RFID based cloud based SCM services. The purpose of this work is to provide clarity on how RFID can be used in supply chain management with modern cloud-based platforms by reducing cost overhead to the business. The primary target audiences are actors in the manufacturing, logistics, warehouse and retail industries who are interested in finding cost effective solution for managing their supply chain inventory management system. Most of the organization started implementing RFID, while at the same time they require the suppliers to adapt to this RFID tags with the standards like EPC standards in storing the products specific data to seamlessly integrate with their entire supply chain management systems. Successful RFID applications in logistics and supply chain management bring benefits such as rationalization of inventory management by having the data in a centralized cloud-based repository. Corporate executives use RFID and Cloud as a technological means to achieve cost savings, efficiency gains and unprecedented visibility in supply chain.

S. M. K. Jamal, A. Omer, and A. A. Salam Qureshi, ”Cloud computing solution and services for RFID based supply chain management,” Adv. Internet Things, vol. 03, no. 04, pp. 79-85, 2013.
Deploying and Implementing RFID Systems for tracking and controlling products in supply chain management is not affordable for small and midsized companies due to its complexity, cost, and difficulties pertaining data management and maintenance. Cloud computing can be used to mitigate the risks associated with the implementation and deployment of RFID based on system in supply chain management because the complex system for data filtering, management and mainte- nance can be implemented on the cloud that otherwise requires the purchase of new hardware, staff and professional services. Small and midsized companies are unable to afford the costs and risks associated with the implementation and deployment of RFID systems. Therefore, we propose a cloud computing solution so that the capital investment and the return-on- investment risks associated with the new technology of RFID can be mitigated. Cloud-base services are designed in such a way as to eliminate the hardware and software infrastructure requirements whose implementation is time consuming as well as expensive. Moreover, it provides abstraction to its users by hiding all the complex details of the system. Users can only use the provided services by interacting with applica- tion software responsible for receiving inputs and providing outputs. The inner workings are completely invisible. For organizations of all types, the ability to quickly locate and enumerate products may facilitate business value of supply chain management.

Y. Huang, J.Wu, and C. Long, ”Drugledger: A practical blockchain system for drug traceability and regulation,” in Proc. IEEE Conf. Internet Things, Jul./Aug. 2018, pp. 1137- 1144.
Drug traceability system is essentially important for pub- lic drug security and business of pharmaceutical companies, which aims to track or trace where the drug has been and where it has gone along the drug supply chain. Traditional centralized server-client technical solutions have been far from satisfying for their bad performances in data authenticity, privacy, system resilience and flexibility. In this paper, we propose a scenario-oriented blockchain system for drug traceability and regulation called Drugledger, which reconstructs the whole service architecture by separating service provider into three independent service components and ensures the authenticity and privacy of traceability data. Drugledger is more resilient than traditional solutions with its p2p architecture. Furthermore, Drugledger could efficiently prune its storage, achieving a finally stable and acceptable blockchain storage. Besides, algorithms reflecting the real drug supply chain logic (e.g., package, repackage, unpackage, etc.) are designed based on the expanded UTXO workflow in Drugledger. To our knowledge, it is the first systematic work from both a technical and practical perspective on how blockchain system could be designed for drug traceability and regulation .

F. Jamil, L. Hang, K. Kim, and D. Kim, ”A novel medical blockchain model for drug supply chain integrity management in a smart hospital,” Electronics, vol. 8, p. 505, Apr. 2019.
At present, in pharmacology one of the most serious problems is counterfeit drugs. The Health Research Funding organization reported that in developing countries, nearly 10–30% of the drugs are fake. Counterfeiting is not the main issue itself, but, rather, the fact that, as compared to traditional drugs, these counterfeit drugs produce different side effects to human health. According to WHO, around 30% of the total medicine sold in Africa, Asia, and Latin America is counterfeit. This is the major worldwide problem, and the situation is worse in developing countries, where one out of every 10 medicines are either fake or do not follow drug regulations. The rise of Internet pharmacies has made it more difficult to standardize drug safety. It is difficult to detect counterfeits because these drugs pass through different complex distributed networks, thus forming opportunities for counterfeits to enter the authentic supply chain. The safety of the pharmaceutical supply chain has become a major concern for public health, which is a collective process. In this paper, we propose a novel drug supply chain management using Hyperledger Fabric based on blockchain technology to handle secure drug supply chain records. The proposed system solves this problem by conducting drug record transactions on a blockchain to create a smart healthcare ecosystem with a drug supply chain. A smart contract is launched to give time-limited access to electronic drug records and also patient electronic health records. We also carried out a number of experiments in order to demonstrate the usability and efficiency of the designed platform. Finally, we used Hyperledger Caliper as a benchmarking tool to conduct the performance of the designed system in terms of transactions per second, transaction latency, and resource utilization .

K. M. Khan, J. Arshad, and M. M. Khan, ”Investigating performance constraints for blockchain based secure e-voting system,” Future Gener. Comput. Syst., vol. 105, pp. 13-26, Apr. 2020.
Voting is one of the fundamental pillars of modern democracy. Continuous efforts have been made to strengthen the processes and methods involved to achieve verifiable, transparent voting systems. In recent years, blockchain has been increasingly used to address multi-dimensional challenges across widespread application domains including healthcare, finance and e-voting. However, achieving an efficient solution via use of blockchain requires consideration of a range of factors such as block generation rate, transaction speed, and block size which have a profound role in determining the overall performance of the solution. Current research into this aspect of blockchain is focused on Bitcoin with the objective to achieve comparable performance as of existing online payment systems such as VISA. However, there exists a gap in literature with respect to investigating performance constraints for wider application domains. In this paper, we present our efforts to ad- dress this gap by presenting a detailed study into performance and scalability constraints for an e-voting system. Specifically, we conducted rigorous experimentation with permissioned and permissionless blockchain settings across different scenarios with respect to voting population, block size, block genera- tion rate and transaction speed. The experiments highlighted interesting observations with respect to the impact of these parameters on the overall efficiency and scalability of the e- voting model including trade-offs between different parameters as well as security and performance.

D. Ko, Y. Kwak, D. Choi, S. Song, Seokil, ”Design of cold chain application framework based on IOT and cloud,” in Proc. 8th Int. Conf. U, e-Service, Sci. Technol., 2015, pp. 11-13.
In this paper, we propose a smart cold chain application framework (SCCAF) based on Cloud and IOT (Internet of Things) techniques. The purpose of SCCAF is to provide PaaS (Platform as a Service) and IaaS (Infra as a Service) to users who want to develop and apply cold chain management systems with low cost and in short time. Also, SCCAF enables users to use any type of IOT devices such as RFID tags, WSN sensor nodes, BLE (Bluetooth Low Energy) sensor nodes and so on. We define common components by generalizing function of existing cold chain management systems, and design

International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X

SCCAF based on Hadoop and Spark to store the large amount of data stream on salable storage and process stream data to detect events and assess risks in cold chain. In this paper, we propose a smart cold chain application framework (SCCAF) based on Cloud and IoT (Internet of Things) techniques. The purpose of SCCAF is to provide PaaS (Platform as a Service) and laaS (Infra as a Service) to users who want to develop and apply cold chain management systems with low cost and in short time. Also, SCCAF enables users to use any type of lOT devices such as RFID tags, WSN sensor nodes, BLE (Bluetooth Low Energy) sensor nodes and so on. The require- ments of the proposed SCCAF are as follows. First, in order to provide PaaS for cold chain management, multitenancy should be supported. It means that SCCAF should be able to process the large amount of data stream from multiple sources in real time. Second, common components that are general functions of cold chain management systems should be provided to users, so that users use them when developing smart cold chain management systems.

GS1 DataMatrix: A Tool to Improve Patient Safety Through Visibility in the Supply Chain, May 26, 2020.
Global standards for automatic identification provide an opportunity to make the healthcare supply chain safer as well as more efficient and accurate. Healthcare regulators and trading partners have realized that a global standardized identification system from manufacturer to patient treatment is imperative to comply with the increasing need for product traceability around the world. The GS1 System, globally endorsed by the healthcare community, is the most widely used identification system worldwide with more than 5 billion transactions per day. Built on a foundation of identification keys (such as the Global Trade Item Number or GTIN) and attributes (such as a batch/lot number, expiry date, unique serial number etc.), it is uniquely suited to meet the needs of the healthcare industry. Some of these needs are being met, and will continue to be met, through the use of 'traditional' linear bar code data carriers, such as GS1-128 or GS1 DataBar. However, for applications where they are not, GS1 Healthcare has adopted the use of GS1 DataMatrix as the GS1 Data Carrier (bar code symbology) solution. The healthcare industry faces major challenges like counterfeiting, ineffective product recall, medication errors and lack of inventory costs and supply chain inefficiencies. The EU Falsified Medicines Directive (FMD) constitutes an important step in protecting patients from counterfeit medicines. As a result, European pharma- ceutical supply chain actors, amongst others EFPIA (European Federation of Pharmaceutical Industry Associations) supported by GIRP (Pharmaceutical full-line wholesalers in Europe), PGEU (Pharmaceutical Group of the European Union) and EAEPC (European Association of Euro-Pharmaceutical Com- panies) are developing systems enabling medicine packs to be verified at the point of dispensing .

Abeyratne, S. Monfared, R., "Blockchain Ready Manufac- turing Supply Chain Using Distributed Ledger," Int. J. Res. Eng. Technol. 2016, 5, 1–10.
The blockchain technology as a foundation for distributed ledgers offers an innovative platform for a new decentral- ized and transparent transaction mechanism in industries and businesses. The inherited characteristics of this technology enhance trust through transparency and traceability within any transaction of data, goods, and financial resources. Despite initial doubts about this technology, recently governments and large corporations have investigated to adopt and improve this technology in various domains of applications, from finance, social and legal industries to design, manufacturing and supply chain networks. In this article, the authors review the current status of this technology and some of its applications. The potential benefit of such technology in manufacturing supply chain is then discussed in this article and a vision for the future blockchain ready manufacturing supply chain is proposed. Manufacturing of cardboard boxes are used as an example to demonstrate how such technology can be used in a global supply chain network. Finally, the requirements and challenges to adopt this technology in the future manufacturing systems are discussed .

III. EXISTING SYSTEM

Traceability is defined as the ability to access any or all information relating to the object under consideration, throughout its life cycle, by means of recorded identifications [25]. The object under consideration is referred to as Traceable Resource Unit (TRU) which is any traceable object within the supply chain. Traceability objectives are twofold; to track the history of transactions, and to track the real-time position of the TRU [26]. Figure 4.1 depicts the block diagram of existing system. In this context, a traceability system requires access to information related to the drug which is the TRU in the supply chain by using different identification techniques to record its identity and distinguish it from other TRUs. The components of a traceability system can be broadly identified by a mechanism for identifying TRUs, a mechanism for docu- menting the connections between TRUs, and a mechanism for recording the attributes of the TRUs [27].

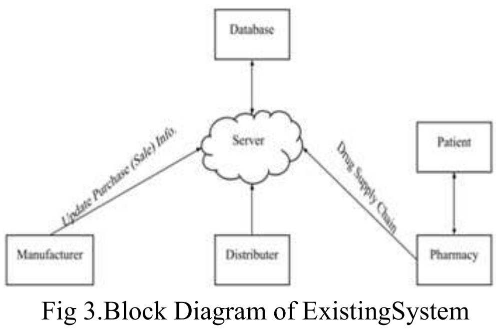

Fig 3.Block Diagram of ExistingSystem

International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X

Existing solutions within supply chain management have traditionally used barcodes and RFID tags as identification techniques, Wireless Sensor Networks (WSN) to capture data, and Electronic Product Code (EPC) to identify, capture, and share product information to facilitate tracking of goods through different stages [28]. In this context, Smart-Track utilizes GS1 standards barcodes containing unique serialized product identifier, Lot production and expiration dates [29]. The information contained in the GS1 barcode is captured across various supply chain processes and used to maintain a continuous log of ownership transfers. As each stakeholder records the possession of the product, an end user (patient) can verify authenticity through central data repository maintained as Global Data Synchronization Network (GDSN) by using a smartphone app [30]. In the downstream supply chain at the warehouse, pharmacy and hospital units can scan the barcode to verify the product and its characteristics.

Similarly, Data-Matrix tracking system creates a Data- Matrix for each drug which includes the manufacturer ID, Product ID, Unique ID of the package, the authentication code, and an optional meta-data [31]. This allows the patient to verify the origin of the drug by using the attached Data-Matrix. More recently Near Field Communication (NFC) tags have been proposed to be used to achieve visibility and authenticity across pharmaceutical supply chain [32]. In this respect, presents an effort to develop an NFC-based system which affords visibility throughout different stages of pharmaceutical supply chain [33]. Each drug is registered and authenticated by using a key value and an NFC tag is attached to it. Similar to the previous two solutions, the user or the patient can verify the authenticity or the origin of the drug by scanning the attached NFC tag using a mobile application [34].

Despite these advancements, existing systems have certain disadvantages. Even though the use of cloud computing is highly consistent and flexible, the features such as data integrity, security, immutability, transparency and decentralization are lacking in traditional pharmaceutical supply chain management systems [35].

IV. PROPOSED SYSTEM

Traditional solutions for achieving traceability within the pharmaceutical supply chain are typically centralized and lack transparency across participants, allowing central authorities to modify information without notifying other stakeholders. In contrast, blockchain-based solutions offer data security, transparency, immutability, provenance, and authenticated transaction records. Blockchain technology represents a decentralized, immutable shared ledger that can be applied to various business settings involving transaction processes[31].

While transparency and traceability are often used interchangeably, they represent different concepts. Transparency typically refers to high-level information about a supply chain, such as product components, facility locations, and supplier names, with the objective of mapping the entire supply chain. Traceability, however, relates to granular information, involving the selection of specific components to trace, determination of common standards for partner communication, implementation of methods to produce and gather accurate data, selection of platforms for data storage, and establishment of data-sharing protocols. Figure 5.1 depicts the architecture diagram of proposed model. Despite representing different con- cepts, both transparency and traceability are interdependent, as accessing granular information requires a comprehensive un- derstanding of the supply chain[32]. The proposed drug trace- ability system consists of stakeholders and their interactions with smart contracts. Stakeholders access the smart contract, decentralized storage system, and on-chain resources through software devices featuring a front-end layer, represented by a Decentralized Application (DApp). This DApp connects to the smart contract, on-chain resources, and decentralized storage system via application program interfaces (APIs) such as Infura, Web3, and Ganache. Stakeholders interact with the smart contract to initiate pre-authorized function calls and with decentralized storage systems to access data files. Their interaction with on-chain resources facilitates obtaining information such as logs, hashes, and transactions[33].

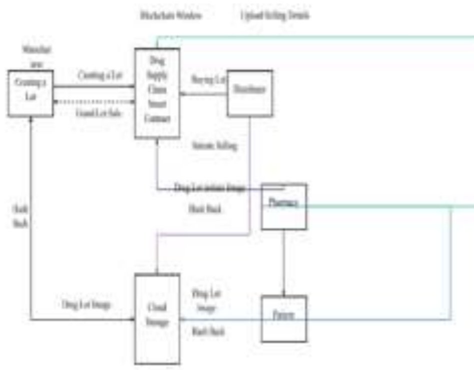

Fig.4.Architecture of Proposed Model.

System Components

Stakeholders: These include regulatory agencies such as the FDA, manufacturers, distributors, pharmacies, and patients. Stakeholders act as participants in the smart contract and are assigned specific functions based on their role in the supply chain. They have access to on-chain resources such as history and log information to track transactions in the supply chain. Additionally, they are authorized to access information stored in the storage system, such as drug lot images and information leaflets[34].

Decentralized Storage System: This provides low-cost off-chain storage to store supply chain transaction data, ensuring reliability, accessibility, and integrity of stored data. Data integrity is maintained by generating a unique hash for every uploaded file on its server. Different hashes for different uploaded files are stored on the blockchain and accessed through the smart contract, with any changes to uploaded files reflected in the associated hash[35].

Ethereum Smart Contract: This handles the deploy- ment of the supply chain. The smart contract is central to tracking transaction history and manages hashes from the decentralized storage server, allowing participants to access supply chain information. Functions of different stakeholders in the supply chain are defined within the smart contract, and access to these functions is given to authorized participants using modifiers. A modifier decorates functions by adding additional features or applying restrictions. The smart contract also handles transactions, such as selling drug lots or boxes[36].

On-chain Resources: These store logs and events cre- ated by the smart contract, enabling track and trace capabilities. A registration and identity system functions as an on-chain resource to associate Ethereum addresses of different participants with human-readable text stored in a decentralized manner[37].

The system components function in an integrated manner to track the history of drugs under consideration to verify authenticity. No real-time tracking is required because DApp users only need to verify that the drug is not counterfeit and comes from a trusted manufacturer. For real-time loca- tion tracking of drug lots, technologies such as IoT-enabled smart containers equipped with sensors can be implemented. These IoT sensors include Global Positioning System (GPS) receivers for location tracking, temperature sensors to monitor temperature, and pressure sensors to detect container opening or closing[38].

Secure Data Hashing Algorithm

The Secure Hashing Algorithm (SHA)-256 serves as the hash function and mining algorithm of the Bitcoin protocol, outputting a 256-bit value. The security of the proposed system is achieved through this Secure Hash Algorithm operating at a frequency of 256 bits. The system adapts the logic of the Secure Hash Algorithm and hashes input attributes to provide overall system security. Initially, user registration attributes are secured by collecting details from users and hashing them over the server. Similarly, each block's identity has a unique ID, which is also hashed using the Secure Hash Algorithm under 256-bit frequency, making the data maintained on the server more secure compared to other existing approaches[39].

The most significant advantage of the Secure Hash Algo- rithm is its operation based on unidirectional hashing tech- niques, meaning data hashed by this algorithm cannot be de- hashed or reverted by any logic. This provides ultimate security for the proposed system, as even service providers cannot acquire information regarding block identity or user identity[40].

Advantages of Blockchain-Based Traceability

- Prevention of data manipulation or modification by any single entity Resilience through decentralization, eliminating single points of failure
- Transparency, allowing all participants to access and view verified transactions in a trusted environment[41]

System Design and Implementation

The proposed solution leverages Ethereum blockchain tech- nology to implement smart contracts and decentralized off- chain storage for efficient product traceability in the healthcare supply chain. This approach addresses the challenge of achiev- ing traceability to mitigate counterfeit drugs, a well-established issue in the pharmaceutical industry. The smart contract handles various transactions among pharmaceutical supply chain stakeholders, guaranteeing data provenance, eliminating intermediaries, and providing a secure, immutable history of transactions to all stakeholders[42].

Development Environment: The solution is developed using the Ethereum blockchain platform, a permissionless public blockchain accessible to anyone. The smart contract is written in Solidity language and compiled and tested using React JS and Node JS. This provides an online web-based development environment for writing and executing code for smart contracts, allowing users to debug and test the Solidity code environment[43].

Process Flow: The manufacturer initially deploys the smart contract, defining and declaring details of the manufac- tured drug lot and triggering an event announced to all supply chain participants. New participants added to the network gain access to events permanently stored on the ledger, enabling them to track and trace the history of any manufactured drug lot. The manufacturer can upload images of lots to cloud storage, making them accessible to participating entities for visual inspection[44].

Before selling newly manufactured lots, they must be pack- aged. The manufacturer announces the availability of newly manufactured lots by sending an event. Participating entities interested in purchasing newly manufactured lots access a specialized function for selling lots. Once transactions are finalized, an event notifies participants, declaring the new lot owner. Manufacturers cannot deploy smart contracts for drug lots without FDA approval, although this approval is not implemented in the smart contract for simplicity[45].

International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X

Typically, manufacturers send approval requests to the FDA to initiate drug lot manufacturing processes. Upon FDA approval, manufacturers begin manufacturing and declare an event to all participants. Manufacturers upload drug lot images to cloud storage, which sends a hash to the smart contract for later access by authorized participants. Drug lots are delivered to distributors for packaging, concluding the manufacturing process.

The distribution process begins in the blockchain window, where distributors pack drug lots and upload package images to cloud storage, which sends hashes to the smart contract. Once completed, drug lot packages are delivered to pharmacies, ending the distribution phase.

The final step involves interactions between pharmacies and patients for uploading details. Pharmacies initiate drug lot box sales, declaring this to supply chain participants. Images of sold drug packages are uploaded to cloud storage, which sends hashes to the smart contract. Drug lot boxes are sold to patients, concluding the selling phase. This process ensures all transactions are stored and accessible to supply chain participants for checking product authenticity and validity in the form of event sequences.

System Modules

Creating a Lot: Functions execute only if the caller's address matches the ownerID address. Authorized callers update fields, and events update status once all fields are updated[49].

Grant Lot Sale: This function sends events alerting participants about lot availability for sale and can only be triggered by ownerID holders.

Buying Lot: This handles transactions between buyers and sellers of drug lots. It requires that buyers have dif- ferent addresses from sellers (ensuring lot owners don't buy their own lots) and that transferred amounts exactly equal lot prices. Upon fulfillment of requirements, sale amounts transfer to sellers, ownerID updates, and events announce lot sales and update new owner details.

Buying Lot Boxes: Similar to buying lots, but buy- ers must specify exact numbers of boxes within lots. Transferred amounts must equal the number of boxes multiplied by each box's price. This function differs in that it maps buyer addresses with numbers of purchased boxes, updating the mapping with each successful exe- cution.

Technical Requirements

Hardware Description:

- **System:** Pentium IV 3.5 GHz or Latest
- **Hard Disk:** 40 GB
- **Monitor:** 14' Color Monitor
- **Mouse:** Optical Mouse
- **RAM:** 1 GB

Software Description

- **Operating System:** Windows 10
- **Ethereum-based Smart Contract Development:** Solidity Programming
- **Front End:** React JS, Node JS
- **Back End:** MySQL
- **Application Development:** Ganache
- **Library:** Web 3.0
- **Software Cryptocurrency Wallet:** MetaMask

Development Technologies

Solidity Programming: Solidity is an object-oriented programming language for implementing smart contracts on various blockchain platforms, particularly Ethereum. Developed by Christian Reitwiessner, Alex Beregszaszi, and former Ethereum core contributors, Solidity programs run on the Ethereum Virtual Machine (EVM). It is a statically typed programming language designed specifically for developing smart contracts. Solidity uses ECMAScript-like syntax, making it familiar to existing web developers. Unlike ECMAScript, it features static typing and variadic return types. Solidity differs from other EVM-targeting languages such as Serpent and Mutan in several key ways. It supports complex member variables for contracts, including arbitrarily hierarchical mappings and structs, and contract inheritance, including multiple inheritance with C3 linearization. Solidity introduces an application binary interface (ABI) enabling multiple type-safe functions within single contracts, a feature later supported by Serpent. The Solidity proposal also includes "Natural Language Specifi- cation," a documentation system for specifying user-centric descriptions of method-call ramifications.

Many smart contract security properties are inherently difficult to reason about directly, and Solidity's Turing-completeness means verification of arbitrary properties cannot be decidably automated. Current automated solutions for smart contract security analysis may miss critical violations, produce false positives, and fail to achieve sufficient code coverage on realistic contracts. Solidity has been criticized for error- prone implementation of Ethereum smart contracts due to its counterintuitive nature, lack of constructs for dealing with blockchain domain-specific aspects, and lack of centralized documentation of known vulnerabilities.

In 2016, a Cornell University researcher attributed partial blame for The DAO hack to Solidity, stating that it introduced security flaws into contracts that were missed by both the com- munity and language designers. Unlike traditional program- ming languages, which allow debugging, Solidity contracts cannot be edited or fixed after deployment, as transactions cannot be reversed. Solidity follows the "Code is

Law" mantra, requiring flawless coding of smart contracts before they take effect. Notable hacking incidents include the 2016 DAO hack, resulting in a $60 million theft, and a 2021 hack causing a fork in the Ethereum system.

To prevent technical errors and mistakes, Coinbase, the largest cryptocurrency exchange in the US, introduced Solid- ify, an AI auditing system for detecting and classifying smart contract risks.

React JS: React (React.js or ReactJS) is a JavaScript library for building user interfaces, maintained by Facebook and a community of individual developers and companies. It serves as a foundation for developing single-page or mobile applications, excelling at fetching rapidly changing data re- quiring recording. However, data fetching represents only the beginning of web page activities, which is why complex React applications typically require additional libraries for state management, routing, and API interaction, such as Redux, React Router, and axios.

ReactJS is an open-source JavaScript library used for build- ing user interfaces, specifically for single-page applications. It handles the view layer for web and mobile apps and allows the creation of reusable UI components. React was created by Jordan Walke, a Facebook software engineer, and was first deployed on Facebook's newsfeed in 2011 and on Instagram.com in 2012.

React enables developers to create large web applications that can change data without page reloading. Its main purpose is to be fast, scalable, and simple, focusing solely on user interfaces in applications, corresponding to the view in the MVC template. It can be used in combination with other JavaScript libraries or frameworks, such as Angular JS in MVC.

Features of ReactJS include

JSX: Instead of using regular JavaScript for templat- ing, React uses JSX, which is simple JavaScript al- lowing HTML quoting and using HTML tag syntaxes to render subcomponents. HTML syntax is processed into JavaScript calls of the React Framework. Pure old JavaScript can also be used.

React Native: Announced by Facebook in 2015, React native libraries provide the React architecture to native applications like iOS, Android, and UPD. React-native is a mobile app building framework using only JavaScript, utilizing the same design as React and allowing the use/inclusion of rich mobile UI libraries/declarative com- ponents. It employs the same fundamental UI building blocks as regular iOS and Android apps and allows the adoption of components written in Objective-C, Java, or Swift.

Single-Way Data Flow: In React, immutable values are passed to component renderers as properties in HTML tags. Components cannot directly modify properties but can pass callback functions for modifications. This pro- cess is known as "properties flow down; actions flow up".

Virtual Document Object Model: React creates an in-memory data structure cache that computes changes and updates browsers accordingly. This feature enables programmers to code as if entire pages render on each change, while the React library only renders components that actually change.

Node JS: Node.js is an open-source, cross-platform JavaScript runtime environment that executes JavaScript code outside browsers. It allows developers to use JavaScript for command-line tools and server-side scripting, running scripts server-side to produce dynamic web page content before sending pages to users' web browsers. Consequently, Node.js represents a "JavaScript everywhere" paradigm, unifying web application development around a single programming lan- guage rather than different languages for server and client-side scripts.

Though .js is the standard filename extension for JavaScript code, "Node.js" does not refer to particular files in this context but is merely the product name. Node.js features an event- driven architecture capable of asynchronous I/O, with design choices aimed at optimizing throughput and scalability in web applications with many input/output operations, as well as real-time web applications such as real-time communication programs and browser games.

Node.js allows the creation of web servers and networking tools using JavaScript and a collection of "modules" handling various core functionalities. Modules are provided for file sys- tem I/O, networking (DNS, HTTP, TCP, TLS/SSL, or UDP), binary data (buffers), cryptography functions, data streams, and other core functions. Node.js's modules use APIs designed to reduce the complexity of writing server applications.

JavaScript is the only language Node.js supports natively, but many compile-to-JS languages are available, allowing Node.js applications to be written in CoffeeScript, Dart, Type- Script, ClojureScript, and others. Though initially based on the CommonJS module pattern, the module system has shifted toward using ECMAScript Modules in Node.js by default fol- lowing their introduction in the ECMAScript specification. Node.js is primarily used for building network programs such as web servers. The most significant difference between Node.js and PHP is that most PHP functions block until completion (commands only execute after previous commands finish), while Node.js functions are non-blocking (commands execute concurrently or in parallel and use callbacks to signalcompletion or failure).

Node.js is officially supported on Linux, macOS, and Microsoft Windows 7 and Server 2008 (and later), with tier 2 support for SmartOS and IBM AIX and experimental support for FreeBSD. OpenBSD also works, and LTS versions are available for IBM i (AS/400). The provided source code may also be built on operating systems similar to those officially supported or modified by third parties to support others such as NonStop OS and Unix servers.

MySQL Database: MySQL is an open-source relational database management system (RDBMS). Its name combines ”My,” the name of co-founder Michael Widenius's daughter, and ”SQL,” the abbreviation for Structured Query Language. MySQL is free and open-source software under the GNU General Public License and is also available under various proprietary licenses. It was owned and sponsored by the Swedish company MySQL AB, which was acquired by Sun Microsystems (now Oracle Corporation). In 2010, when Oracle acquired Sun, Widenius forked the open-source MySQL project to create MariaDB.

MySQL is a component of the LAMP web application software stack (and others), an acronym for Linux, Apache, MySQL, Perl/PHP/Python. It is used by many database-driven web applications, including Drupal, Joomla, phpBB, and WordPress, as well as popular websites like Facebook, Flickr, MediaWiki, Twitter, and YouTube.

MySQL is written in C and C++, with its SQL parser written in yacc, though it uses a home-brewed lexical analyzer. It works on many system platforms, including AIX, BSDi, FreeBSD, HP-UX, eComStation, i5/OS, IRIX, Linux, macOS, Microsoft Windows, NetBSD, Novell NetWare, OpenBSD, OpenSolaris, OS/2 Warp, QNX, Oracle Solaris, Symbian, SunOS, SCO OpenServer, SCO UnixWare, Sanos, and Tru64. A port of MySQL to OpenVMS also exists.

The MySQL server software itself and client libraries use dual-licensing distribution, offered under GPL version 2 or proprietary licenses. Support can be obtained from the official manual, with free support additionally available in different IRC channels and forums. Oracle offers paid support via its MySQL Enterprise products, which differ in scope of services and price. Additionally, third-party organizations exist to provide support and services, including MariaDB and Percona.

MySQL has received positive reviews, with reviewers noting it ”performs extremely well in the average case” and that ”developer interfaces are there, and the documentation (not to mention feedback in the real world via websites and the like) is very, very good.” It has also been tested to be a ”fast, stable, and true multi-user, multi-threaded SQL database server”.

Ganache: Ganache is part of the Truffle Suite ecosys- tem, which consists of Ganache and two additional tools: Truffle and Drizzle. Truffle is a development environment, asset pipeline, and testing framework using the Ethereum Virtual Machine (EVM), while Drizzle is a collection of frontend libraries.

Ganache is a high-end development tool used to run lo- cal blockchains for both Ethereum and Corda decentralized application (dApp) development. It assists in all parts of the development process, with the local chain allowing development, deployment, and testing of projects and smart contracts in deterministic and safe environments

There are two versions of Ganache: a desktop application called Ganache UI, supporting development for both Ethereum and Corda, and a command-line tool called ganache-CLI, sup- porting only Ethereum development. All versions of Ganache are available for Mac, Windows, and Linux.

Ganache enables the setup of blockchains, providing safe testing environments for dApps and smart contracts. Its use is motivated by cost-effectiveness and time efficiency. When uploading smart contracts to the Ethereum chain, gas fees must be paid for every transaction, which can become costly given high and unpredictable gas prices. Testing smart contracts on local chains avoids these fees, allowing developers to wait until contracts are flawless before paying transaction costs for deployment.

Furthermore, local blockchains allow instant uploads. Uploading to both main and test nets of Ethereum takes time, which can impede rapid development. With local blockchains set up using Ganache, developers avoid waiting for contracts to deploy on chains before testing them.

Web 3.0 Library: Web3 (also known as Web 3.0 and sometimes stylized as web3) represents a concept for a new iteration of the World Wide Web based on blockchain technology, incorporating decentralization and token-based economics. Some technologists and journalists contrast it with Web 2.0, wherein data and content are centralized in small groups of companies sometimes referred to as ”Big Tech.” The term ”Web3” was coined in 2014 by Ethereum co-founder Gavin Wood and gained interest in 2021 from cryptocurrency enthusiasts, large technology companies, and venture capital firms.

Some experts argue that Web3 will provide increased data security, scalability, and privacy for users and combat the influence of large technology companies. Others raise concerns about decentralized webs, citing potential for low moderation and proliferation of harmful content, centralization of wealth to small groups of investors and individuals, or loss of privacy due to more expansive data collection. Critics such as Elon Musk and Jack Dorsey argue that Web3 serves merely as a buzzword.

Specific visions for Web3 differ, and the term has been described by Bloomberg as ”hazy,” but they revolve around de- centralization and often incorporate blockchain technologies, such as cryptocurrencies and non-fungible tokens (NFTs). Bloomberg describes Web3 as an idea that ”would build finan- cial assets, in the form of tokens, into the inner workings of al- most anything you do online.” Some visions are based around decentralized autonomous organizations (DAOs). Decentral- ized finance (DeFi) is another key concept, in which users exchange currency without bank or government involvement. Self-sovereign identity allows users to identify themselves without relying on authentication systems like OAuth, where trusted parties must be reached to assess identity. Technology scholars argue that Web3 would likely run in tandem with Web 2.0 sites, with Web 2.0 sites likely adopting Web3 technologies to maintain service relevance.

MetaMask: MetaMask is a software cryptocurrency wal- let used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallets through browser ex- tensions or mobile apps, which can then be used to interact with decentralized applications. MetaMask is developed by ConsenSys Software Inc., a blockchain software company focusing on Ethereum-based tools and infrastructure.

MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryp- tocurrencies and tokens, and securely connect to decentralized applications through compatible web browsers or the mo- bile app’s built-in browser. Developers achieve connections between MetaMask and their decentralized applications by using JavaScript plugins such as Web3js or Ethers to define interactions between MetaMask and Smart Contracts.

The MetaMask application includes an integrated service for exchanging Ethereum tokens by aggregating several de- centralized exchanges (DEXs) to find the best exchange rates. This feature, branded as MetaMask Swaps, charges a service fee of 0.875% of transaction amounts.

As of November 2021, MetaMask’s browser extension had over 21 million monthly active users, according to Bloomberg. ConsenSys created MetaMask in 2016.

Prior to 2019, MetaMask had only been available as a desktop browser extension for Google Chrome and Firefox browsers. Given MetaMask’s popularity among cryptocur- rency users and its lack of an official mobile app for several years, instances of malicious software posing as MetaMask became problematic for Google in regulating its Chrome Web Store and Google Play platforms. In one instance, Google Play unintentionally removed MetaMask’s official beta app before reverting the decision a week later on January 1, 2020.

Starting in 2019, MetaMask began releasing mobile app versions for closed beta testing, followed by official public releases for iOS and Android in September 2020. In October 2020, MetaMask Swaps, a built-in DEX aggregation service, was added to the desktop extension, becoming available on mobile devices in March 2021.

While MetaMask and other ”web3” focused applications aim to decentralize control over personal data and increase user privacy, critics have pointed to the potential for Meta- Mask’s browser extension to leak identifiable information to data collection networks and web trackers as a fundamental flaw.
The blockchain-based drug traceability system presents a promising solution to the challenges of ensuring transparency and security in pharmaceutical supply chains. By leveraging decentralized technologies, smart contracts, and secure hash- ing algorithms, the system provides an immutable record of transactions and product movements throughout the supply chain. This approach significantly reduces the risk of counter- feit drugs entering the market and enhances stakeholder trust in the authenticity of pharmaceutical products.

The implementation of this system using Ethereum blockchain, Solidity programming, and supporting technolo- gies like React JS, Node JS, and MetaMask demonstrates the practical feasibility of blockchain applications in healthcare supply chains. The decentralized nature of the system elimi- nates single points of failure and prevents data manipulation by any single entity, while providing transparent access to verified transaction records for all authorized participants.

As blockchain technology continues to mature, such sys- tems are likely to become increasingly important in ensuring the integrity and safety of pharmaceutical products globally. Future research could focus on enhancing the scalability of these systems and integrating them with existing pharmaceu- tical tracking mechanisms to create comprehensive, end-to- end solutions for drug traceability.

V. CONCLUSION

Blockchain-based drug traceability has emerged as a promising solution to address challenges in the pharmaceutical supply chain, including counterfeit drugs, inefficient tracking systems, and lack of transparency. By utilizing the immutabil- ity and decentralized nature of

International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X

blockchain technology, it is possible to create a robust and transparent system for tracking drugs from manufacturing to consumption.

Drug traceability refers to the process of tracking and tracing pharmaceutical products throughout the supply chain, from manufacturing to distribution and dispensing. It involves recording and monitoring the movement of drugs, capturing relevant information, and ensuring their authenticity, integrity, and compliance with regulatory standards. Once the identity is verified, the new user is granted access permissions based on their role and responsibilities within the supply chain. These permissions define the level of access they have to view, update, or interact with the blockchain-based drug traceability system.

The inclusion of raw material suppliers is an essential aspect of ensuring transparency and accountability throughout the pharmaceutical supply chain. Package collection is an important step in the drug traceability process as it involves the collection of drugs from the manufacturer or distributor for further distribution or dispensing. When a package of drugs is collected by a transporter, it is essential to ensure that the package is properly tracked and authenticated to maintain the integrity of the drug supply chain.

When a package is delivered to the manufacturer, the delivery event is recorded on the blockchain. The creation of medicine involves the manufacturing process where various raw materials and components are transformed into finished pharmaceutical products. When a pharmacy requests products from a manufacturer, it is a crucial step in the drug supply chain. The process involves pharmacies ordering pharmaceutical products to replenish their inventory and meet the needs of their customers.

Signature creation plays a significant role in various contexts, including document authentication, digital transactions, and data integrity verification. Signature verification is the process of validating the authenticity and integrity of a digital signature using the corresponding public key. When a package is delivered to a pharmacy, it is an important step in the drug supply chain. When a patient needs medication, it typically involves a prescription submission and coordination with the pharmacy. Transferring medicine to a patient from a pharmacy involves the final step in the drug distribution process.

In conclusion, this article investigated the challenge of drug traceability within pharmaceutical supply chains, highlighting its significance especially to protect against counterfeit drugs. The blockchain-based solution leverages cryptographic fundamentals to achieve tamper-proof logs of events within the supply chain and utilizes smart contracts within Ethereum blockchain to achieve automated recording of events accessible to all participating stakeholders. The solution is cost-efficient and provides protection against malicious attempts targeting integrity, availability, and non-repudiation of transaction data, which is critical in complex multi-party settings such as the pharmaceutical supply chain.

REFERENCES

1. N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," Comput. Electr. Eng., vol. 76, pp. 183-197, Jun. 2019.
2. M. Muniandy. O. Gabriel, and T. Ern, "Implementation of pharma- ceutical drug traceability using blockchain technology," Int. J., vol. 2019, p. 35, Jun. 2019. 12) B. A. Supriya and I. Djearamane, "RFID based cloud supply chain management", Int. J. Sci. Eng. Res., vol. 4, no. 5, pp. 2157-2159, 2013.
3. S. M. K. Jamal, A. Omer, and A. A. Salam Qureshi, "Cloud computing solution and services for RFID based supply chain management," Adv. Internet Things, vol. 03, no. 04, pp. 79-85, 2013.
4. Y. Huang, J.Wu, and C. Long, "Drugledger: A practical blockchain system for drug traceability and regulation," in Proc. IEEE Conf. Internet Things, Jul./Aug. 2018, pp. 1137-1144.
5. F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," Electronics, vol. 8, p. 505, Apr. 2019.
6. K. M. Khan, J. Arshad, and M. M. Khan, "Investigating perfor- mance constraints for blockchain based secure e-voting system," Future Gener. Comput. Syst., vol. 105, pp. 13-26, Apr. 2020.
7. D. Ko, Y. Kwak, D. Choi, S. Song, Seokil, "Design of cold chain application framework based on IOT and cloud," in Proc. 8th Int. Conf. U, e-Service, Sci. Technol., 2015, pp. 11-13.
8. GS1 DataMatrix: A Tool to Improve Patient Safety Through Visibility in the Supply Chain, May 26, 2020.
9. Abeyratne, S. Monfared, R., "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger," Int. J. Res. Eng. Technol. 2016, 5, 1–10.
10. U.S. Food and Drug Administration. A Drug Supply Chain Example. Accessed: Jun. 3, 2020. [Online]. Available: https://www. fda.gov/drugs/drug-shortages/graphic-drug-supply-chain-example
11. A. Marucheck, N. Greis, C. Mena, and L. Cai, "Product safety and security in the global supply chain: Issues, challenges and research opportunities," J. Oper. Manage., vol. 29, nos. 7–8, pp. 707–720, Nov. 2011.
12. U.S. Food and Drug Administration. Drug Supply Chain Security Act. Accessed: Jun. 3, 2020. [Online]. Available: https://fda.gov

13. State Food and Drug Administration of China. (Feb. 2016). On suspension of drug electronic supervision system. Accessed: Jun. 3, 2020. [Online]. Available: http://www.sda.gov.cn/WS01/CL0051/144782.html.
14. M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "On the malleability of Bitcoin transactions," in Proc. Financial Cryptography Data Secur., 2015, pp. 1–18.
15. A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Mon- etization of IoT data using smart contracts," IET Netw., vol. 8, no. 1,pp. 32–37, Jan. 2019.
16. K. M. Khan, J. Arshad, and M. M. Khan, "Simulation of transaction malleability attack for blockchain- based E-voting," Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106583.
17. N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," Comput. Electr. Eng., vol. 76, pp. 183–197, Jun. 2019.
18. S. Nakamoto. (2009).Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Avail- able: https://metzdowd.com
19. M. Muniandy. O. Gabriel, and T. Ern, "Implementation of pharmaceutical drug traceability using blockchain technology," Int. J., vol. 2019, p. 35, Jun. 2019.
20. P. Olsen and M. Borit, "The components of a food traceability sys- tem," Trends Food Sci. Technol. vol. 77, pp. 143–149, Jul. 2018, doi:10.1016/j.tifs.2018.05.004.
21. A. Bougdira, A. Ahaitouf, and I. Akharraz, "Conceptual framework for general traceability solu- tion: Description and bases," J. Model. Manage., vol. 15, no. 2, pp. 509–530, Oct. 2019.
22. K. Al Huraimel and R. Jenkins. (2020). Smart Track. Accessed: May 26, 2020. [Online]. Available: https://smarttrack.ae/
23. GS1 DataMatrix: A Tool to Improve Patient Safety Through Visibil- ity in the Supply Chain. Accessed: May 26, 2020.
24. B. A. Supriya and I. Djearamane, "RFID based cloud supply chain man- agement," Int. J. Sci. Eng. Res., vol. 4, no. 5, pp. 2157–2159, 2013.
25. S. M. K. Jamal, A. Omer, and A. A. Salam Qureshi, "Cloud computing solution and services for RFID based supply chain management," Adv. Internet Things, vol. 03, no. 04, pp. 79–85, 2013.
26. S. Nakamoto. Bitcoin: A Peer- to-Peer Electronic Cash System. Accessed: Jun. 3, 2020. [Online]. Available: http://bitcoin.org/bitcoin.pdf
27. M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.
28. M. Pilkington, "Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations, vol. 225. London, U.K.: Edward Elgar, 2016.
29. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services, Sep. 2016, pp. 1–3.
30. J. Kurki, "Benefits and guidelines for utilizing blockchain technol- ogy in pharmaceutical supply chains: Case Bayer Pharmaceuticals," Bachelor thesis, Dept. Inf. Service Econ., Aalto Univ., Espoo, Finland, 2016.
31. Y. Huang, J. Wu, and C. Long, "Drugledger: A practical blockchain system for drug traceability and regulation," in Proc. IEEE Conf. Internet Things, Jul./Aug. 2018, pp. 1137–1144.
32. S. Delgado-Segura, C. Pe´rez- Sola`, G. Navarro-Arribas, and J. HerreraJoancomart´ı, "Analysis of the bitcoin UTXO set," in Financial Cryptography and Data Security (Lecture Notes in Computer Science), vol. 10958, A. Zohar, Ed. Berlin, Germany: Springer, 2019, pp. 78–91.
33. F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," Electronics, vol. 8, p. 505, Apr. 2019, doi: 10.3390/electron- ics8050505.
34. K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," Future Gener. Comput. Syst., vol. 105, pp. 13–26, Apr. 2020.
35. C. Hulseapple. (2015). Block Verify Uses Blockchains to End Counter- feiting and Make World More Honest. Accessed: Jun. 5, 2020. [Online]. Available: https://cointelegraph.com/news/block-verify-uses-blockchains- to- end-counterfeiting-and-make-world-more-honest
36. C. Arsene. (2019). Hyperledger Project Explores Fighting Coun- terfeit Drugs with Blockchain. Accessed: Jul. 5, 2020. [Online].
37. The MediLedger Project. Accessed: Jul. 5, 2020. [Online]. Available: