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

Sakshi Dahake[1], Sharayu Nalawade[2], Priya Nigade[3] , Tanvi Shinde[4], Varsha Rasal[5]

[1] *Student, Computer Department, NBN Sinhgad College of Engineering, Pune, Maharashtra, India*
[2] *Student, Computer Department, NBN Sinhgad College of Engineering, Pune, Maharashtra, India*
[3] *Student, Computer Department, NBN Sinhgad College of Engineering, Pune, Maharashtra, India*
[4] *Student, Computer Department, NBN Sinhgad College of Engineering, Pune, Maharashtra, India*
[5] *Guide, Computer Department, NBN Sinhgad College of Engineering, Pune, Maharashtra, India*

ABSTRACT

Drug traceability system is essentially important for public 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 centralised server-client technical solutions have proved unsatisfactory due to poor data integrity, privacy, system resilience, and adapt-ability.Counterfeit medications are becoming a more serious problem in the healthcare industry, posing serious hazards to society. The challenge of tracing medications throughout the pharmaceutical supply chain is tough. The management and sharing of health records is another important challenge in the fight against counterfeit medications in healthcare systems. E-health records' security is a major concern since they are vulnerable to threats to confidentiality and integrity.In this paper, we offer an Ethereumblock chain-based approach for efficient product tracing in the healthcare supply chain that uses smart contracts and decentralized off-chain storage. The smart contract ensures data provenance, eliminates the need for middlemen, and provides all parties with a safe, immutable transaction history. We offer the system architecture as well as the detailed algorithms that regulate our proposed solution's functioning principles.

Keyword :- *Blockchain, drug counterfeiting, traceability, healthcare, supply chain, trust, security.*

1. INTRODUCTION

Drug traceability is critical for the health and well-being of patients, businesses, and the government. Patients and other parties involved in the drug supply chain could easily track the location of their medication if it had a dependable traceability mechanism. In fact, governments all around the world are increasingly making drug tracking a requirement. Prescription medications must be identified and tracked elec-tronically and interoperably as part of the U.S. Drug Supply Chain Security Act (DSCSA), enacted on November 27, 2013, to ensure their safety in the country's supply chain. About eight years ago in China, the above-mentioned stakeholders were compelled to input the drug information of individual pharmaceutical goods into the official authorised IT system whenever pharmaceuticals entered or exited their warehouses.

An effective drug traceability system should be able to maintain track of or trace drug transactions as they move through various supply chain participants. It should provide stakeholders and patients with trustworthy

information about the flow, particularly regarding the origin of medicine produc-tion for anti counter feiting purposes. In some cases, it could be utilised as a means of tying the hands of the relevant parties.
in the control of drug security. There must also be a high level of privacy for traceability data, especially that pertaining to statistical information on drugs that have passed through the stakeholder's hands (such as productivity, sales volume, and so on). For the first time, a blockchain system for drug traceability and regulation is presented in this study. As time goes on, it rebuilds the entire service architecture, ensuring the authenticity and privacy of traceability data, while at the same time, achieving a finally stable blockchain storage There have also been presented algorithms that mirror the practical workflow of the medication supply chain.

A. Motivation

- Healthcare supply chain is a complex network of several independent entities that include raw material suppliers, manufacturer, distributor, pharmacies, hospitals and pa-tients.
- Tracking supplies through this network is non-trivial due to several factors including lack of information, central-ized control and competing behaviour among stakehold-ers.
- Such complexity not only results in inefficiencies such as those highlighted through COVID-19 pandemic but can also aggravate the challenge of mitigating against coun-terfeit drugs as these can easily permeate the healthcare supply chain

B. Objectives

- 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 dense the working principles of our proposed solution.
- We conduct security and cost analysis to evaluate the performance of the proposed blockchain-based solution.

2. REVIEW OF LITERATURE

Suliman, Z. Husain,et.al., proposed work based on 'Monetization of IoT data using smart contracts.In this article , We have given a system design, architecture, and implementation of a blockchain-based solution using Ethereum smart contracts for the automated monetization of IoT data with no intermediary . We put it into action. Ethereum smart contracts written in the Solidity programming language. We described the system's interactions with participants and used Remix IDE to test the system's numerous functionalities.

K. M. Khan, J. Arshad, et.al., proposed work based on Simulation of transaction malleability attack for blockchain-based E-voting. The transaction malleability attack was discussed in this work in the context of a specific application area, namely blockchain-based e-voting. The suggested system demonstrated how a transaction malleability attack might result in an inconsistent blockchain, allowing attackers to take advantage of the situation for a number of malevolent purposes. We are continuing our research by evaluating the approach described utilising a real-life test-bed.

N. Nizamuddinet.al., proposed work based on 'Decentralized document version control using ethereum blockchain and IPFS. In this paper, for document version management and sharing, we presented a decentralised architecture and solution. The benefits and features of Blockchain, smart contracts, and the IPFS file system are all utilised in our

solution. The Remix IDE was used to implement and test the functionalities of our solution. We also used prominent security analysis tools, such as ChainSecurity and Oyente, to validate and illustrate the built smart contract's robustness and security against well-known attacks.

M. Muniandy. O. Gabriel et.al., proposed based on Implementation of pharmaceutical drug traceability using blockchain technology. In this study, The system that was created is functional and meets the project's goals. Despite this, there is potential for development in terms of features and functions. The designed system must be deployed and tested in real time.

P. Olsen et.al., proposed based on the components of a food traceability system. In this paper The primary goal of this article is to identify, define, and differentiate the various components of a traceability system. To distinguish between the mechanisms in a traceability system that assign identities and record transformations, and the TRU properties that we want access to. This distinction has not always been made in past papers, studies, and other materials about food, traceability, and this absence has resulted in ambiguous or inadequate assessments and conclusions in certain cases. The designed system must be deployed and tested in real time.

A. Bougdira, et.al., proposed based on Conceptual framework for general traceability solution: Description and bases. In this paper, the framework consists of a number of components that serve as the foundation for a traceability solution. Logical linkages are used to connect the framework's components. As a result, the framework's application provides traceability solution bases that are likely to be useful and applicable to a variety of traceability applications. The foundations walk a user through the process of developing and deploying a traceability system.

Y. Huang, J. et.al., proposed based on Drugledger: A practical blockchain system for drug traceability and regulation. Drugledger, a realistic blockchain system for drug tracking and regulation, is proposed in this study. Drugledger rebuilds the entire service architecture by separating service providers, ensuring the authenticity and privacy of traceable data while ensuring service delivery. A healthy and sustainable business ecosystem is formed by service providers (CSP, ASP, and QSP), stakeholders, and patients as a whole. The enhanced UTXO data structure, particularly that of package, repackage, and unpackage, is used by Drugledger to complete its workflow.

F. Jamil, et.al., proposed based on A novel medical blockchain model for drug supply chain integrity management in a smart hospital. In this study, they explain the design, implementation, and performance evaluation of a proposed Hyperledger Fabric-based drug supply chain integrity management in a smart hospital. A series of experiments were conducted in order to validate the proposed system's performance analysis in terms of transaction response time, throughput, latency, and resource utilisation. Our findings show that implementing blockchain technology improves the proposed system's throughput while also lowering latency and reducing resource use.

K. M. Khan, et.al., proposed based on Investigating performance constraints for blockchain based secure e-voting system. In this study, they have detailed our efforts to close this gap in this paper by undertaking an in-depth examination of criteria that play a significant role in establishing scalable blockchain solutions. We look into the impact of block production rate, block size, transaction processing rate, and transaction size on the scalability of blockchain-based solutions in particular. The results of our experiments reveal a trade-off between these variables and point to areas for future investigation.

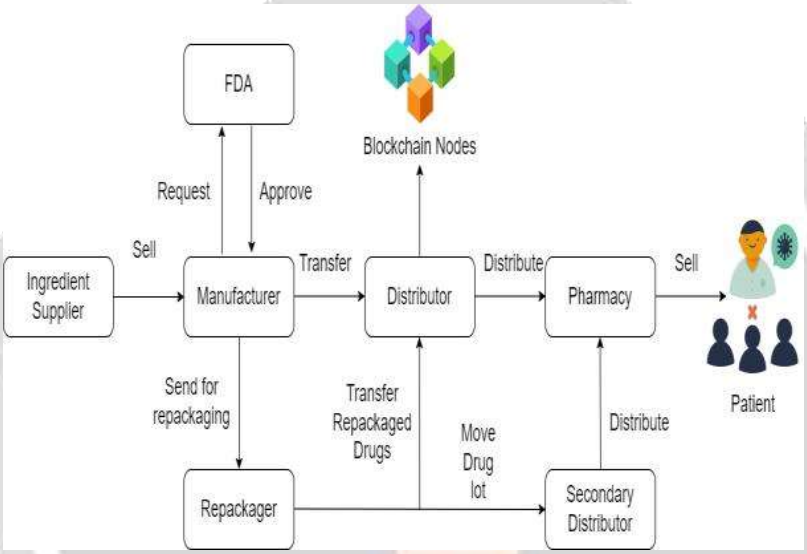
D. Vujicic, et.al., proposed based on Blockchain technology, bitcoin, and Ethereum: A brief overview. In this paper, The most popular and valuable cryptocurrencies are Bitcoin and Ethereum. They are built on blockchain technology,

which is designed to promote a peer-to-peer network's trust mechanism by relying on the majority of nodes' consensus. In this article, we provide a brief historical overview of the early stages of digital currency implementation, as well as the foundations of blockchain technology and its most promising (or popular) implementations, Bitcoin and Ethereum.

3.PROPOSED METHODOLOGY

3.1 Architecture

- Our method identifies and involves significant stakehold-ers in the medication supply chain, such as the FDA, suppliers, manufacturers, distributors, pharmacies, and patients, whereas the FDA, suppliers, manufacturers, and wholesalers are the only ones involved.



• We make a concerted effort to identify and disentangle linkages between stakeholders, on-chain resources, smart contracts, and decentralised storage systems, which is currently lacking.

• We use smart contracts technology to achieve real-time, seamless traceability with push alerts, reducing the need for human intervention and, as a result, unnecessary delays.

• Each drug Lot is given its own smart contract, which gen-erates an event whenever there is a change in ownership and sends a list of events to the app user

3.2 Algorithm

ECC Algorithm:

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

Few terms that will be used,
E -¿ Elliptic Curve
P -¿ Point on the curve
n -¿ Maximum limit (This should be a prime number)

Key Generation

Key generation is an important part of which both public and private key are to be produced. The transmitter encrypts the letter by using the public key of the recipient, and the recipient decrypts his private key.
Now, we have to select a number 'd' within the range of 'n'. Using the following equation we can generate the public key

$$Q = d * p$$

d = the random number that we have selected within the range of (1 to n-1). P is the point on the curve. 'Q' is the public key and 'd' is the private key.

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details.
Conside 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)]. Two cipher texts will be generated let it be C1 and C2.

$C_1 = k * p$

$C_2 = M + k * Q$

C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

$$M = C_2 - d * C_1$$

M is the original message that we have send.
How does we get back the message?

$$M = C_2 - d * C_1$$

M can be represented as

$$'C_2 - d * C_1$$

$C_2 - d * C_1 = (M + k * Q) - d * (k * p) (C_2 = M + k * Q and C_1 = k * p)$

$$= M + k * d * P - d * k * P$$

$$= M(OriginalData)$$

4.RESULT AND ANALYSIS

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System

runs these experiments on a window machine with an Intel processor 2.30GHz processor and 8GB memory.

All these experiments use Java programming language with the various encryption algorithms such as ECC (Proposed system -yellow color), AES (Existing System-blue color).

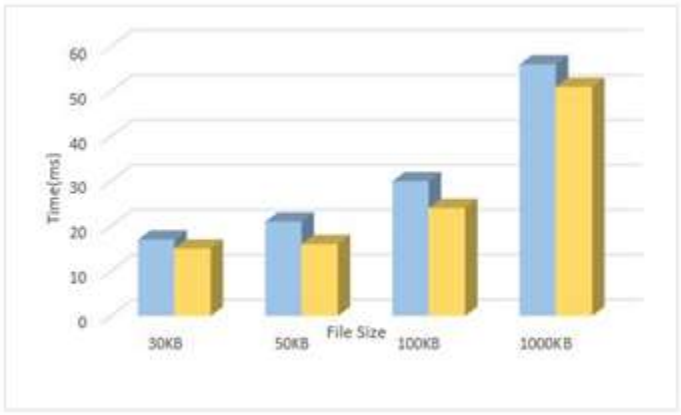


Fig. 2. Shows file size on x axis and Encryption Time on Y-axis

File Size	AES	ECC
100 KB	35ms	32ms
150 KB	36ms	31ms
500 KB	63ms	58ms
1000 KB	113ms	97ms

Table 1: Show File Size and Encryption Time

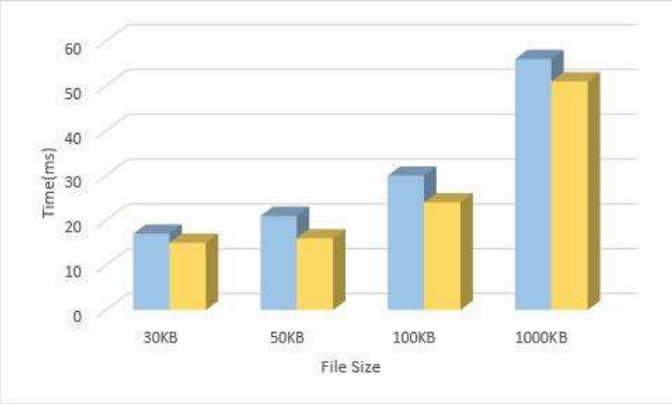


Fig. 3. Shows file size on x axis and Decryption Time on Y-axis

File Size	AES	ECC
100 KB	12ms	9ms
150 KB	16ms	12ms
500 KB	26ms	21ms
1000 KB	52ms	46ms

Table 2: Show File Size and Decryption Time

V.CONCLUSION

In this paper, we looked into the problem of drug traceability in pharmaceutical supply chains, emphasizing its with the various encryption algorithms such as ECC importance in protecting against counterfeit drugs. We test and validate the system, as well as give a cost and security analysis, in order to assess its usefulness in improving traceability within pharmaceutical supply chains.To track and trace pharmaceuticals in a decentralised manner, we built and evaluated a blockchain-based system for the pharmaceutical supply chain.As part of our ongoing efforts to improve the efficiency of pharmaceutical supply chains; we plan to expand the suggested system to achieve end-to-end transparency and verifiability of drug usage in the future.

REFERENCES

[1] A. Suliman, Z. Husain, M. Abououf, M. Alblooshi, and K. Salah, "Monetization of IoT data using smart contracts," IET Netw., vol. 8, no. 1, pp. 32–37, Jan. 2019
[2] 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

[3] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereumblockchain and IPFS," Comput. Electr. Eng., vol. 76, pp. 183–197, Jun. 2019
[4] M. Muniandy. O. Gabriel, and T. Ern, "Implementation of pharmaceutical drug traceability using blockchain technology," Int. J., vol. 2019, p. 35, Jun. 2019
[5] 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.
[6] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and Ethereum: A brief overview," in Proc. 17th Int. Symp. InfotehJahorina (INFOTEH), East Sarajevo, Srpska, Mar. 2018, pp. 1–6, doi: 10.1109/INFOTEH.2018.8345547.
[7] 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
[8] A. Bougdira, A. Ahaitouf, and I. Akharraz, "Conceptual framework for general traceability solution: Description and bases," J. Model. Manage., vol. 15, no. 2, pp. 509–530, Oct. 2019.
[9] 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.
[10] 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/electronics8050505
.