International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-14 Issue-2, May 2024

Counterfeit Medicine Detection using Blockchain

Shreyas Zagare, Manish Khodaskar, Yash Sonawane, Harish Verma

Abstract: ***The healthcare industry has grappled with the challenge of monitoring genuine medicines while counterfeit drugs continue to proliferate, posing significant risks to patient safety. These fraudulent pharmaceuticals not only have detrimental effects on health but also result in substantial financial losses, with reports indicating annual losses of approximately 200 billion dollars for US pharmaceutical companies. Particularly concerning is the World Health Organization's revelation that in underdeveloped nations, one in every ten medicines consumed by patients is counterfeit and of low quality. To address this critical issue, we use blockchain technology to track the supply chain, from the manufacturing stage to the end- user. Leveraging blockchain technology, our system enhances reliability, transparency, and security in healthcare data. This paper focuses on bolstering transaction security, safeguarding medicine quality, and fortifying data protection through the utilization of blockchain technology.***

Index Terms: Counterfeit, Blockchain, Smart contracts, Fake Medicines

I. INTRODUCTION

The proliferation of counterfeit medicines poses a severe threat to public health and cre- ates substantial challenges for pharmaceutical companies worldwide. The consequences of counterfeit drugs extend beyond financial losses to these companies, impacting patient well-being and potentially caus- ing life-threatening complications. With an estimated annual global market of $650 billion in counterfeit products, it becomes imperative to address this pressing issue. Various techniques, including barcoding and RFID (Radio-Frequency Identification), have been implemented in the pharmaceutical supply chain to trace counterfeit drugs. However, these so- lutions are not without their limitations, such as high imple- mentation costs and lack of transparency. This research paper aims to introduce a transformative solution in the form of a blockchain-based system for medicine traceability and regula- tion. The pharmaceutical supply chain is intricate, involving numerous entities like suppliers, manufacturers, trans- porters, wholesalers, distributors, and retailers. Maintaining trans- parency and traceabil- ity throughout this extensive network is a formidable challenge.

Manuscript received on 01 May 2024 | Revised Manuscript received on 14 April 2024 | Manuscript Accepted on 15 May 2024 | Manuscript published on 30 May 2024.
*****Correspondence Author(s)*
Shreyas Zagare, Department of Information Technology SCTR's Pune Institute of Computer, Pune (M.H.), India. E-mail: sbzagare@gmail.com
Prof. Manish Khodaskar, Department of Information Technology SCTR's Pune Institute of Computer, Pune (M.H.), India. E-mail: mrkhodaskar@pict.edu
Yash Sonawane, Department of Information Technology SCTR's Pune Institute of Computer, Pune (M.H.), India. E-mail: yash493031@gmail.com
Harish Verma*, Department of Information Technology SCTR's Pune Institute of Computer, Pune (M.H.), India. E-mail: vermarharish@gmail.com, ORCID ID: 0009-0004-7448-1342

Counterfeit medicines infiltrate the market, particularly affecting developing countries, where the percentage of fake drugs can range from 10financial losses but also jeopardize human health by causing adverse side effects. The existing supply chain faces inherent inefficiencies, primarily due to a lack of transparency, making it challeng- ing for customers and buyers to ascertain the true value of products. It becomes even more challenging to investigate suspected unethical or illegal practices within the supply chain. This paper advocates the use of blockchain technology as a game-changing solution to address these issues. Blockchain offers a decentralized, immutable ledger with no central au- thority, ensuring transparency and trust among various supply chain entities. The use of smart contracts enables secure and transparent transactions between manufacturers, distributors, suppliers, and end-users, leading to improved customer experi- ences and heightened customer satisfaction. The amalgamation of blockchain technology and other innovative approaches promises to revolutionize the pharmaceutical industry, ensur- ing the safety, quality, and authenticity of medicines while prioritizing the well-being of patients.

II. LITERATURE SURVEY

In recent years, blockchain technology has garnered sig- nificant attention for its potential to revolutionize various industries, including healthcare. Ahmad et al. [1][9][10] explores the application of blockchain in securing COVID-19 man- agement within the supply chain, emphasizing the importance of transparency and efficiency in handling medical supplies and patient data. Building on this, the systematic review conducted by Khan et al. [2] provides insights into blockchain- based solutions in healthcare, shedding light on their potential benefits and challenges across different domains, including pharmaceutical authentication and supply chain management. In particular, the pharmaceutical supply chain has been a focus of attention for blockchain applications due to the need for enhanced transparency and traceability to combat coun- terfeit drugs. Zhang and Li [3] offer insights into the use of blockchain technology to secure pharmaceutical supply chains, highlighting its role in ensuring the authenticity of medicines and mitigating the risks associated with counterfeit products. Similarly, the bibliometric analysis conducted by Wang et al. [3] examines trends in blockchain research in healthcare, revealing a growing interest in supply chain management, patient data security, and pharmaceutical authentication. Further supporting the exploration of blockchain in health-care, Nakamoto et al. [4] present a systematic review that delves into various applications of blockchain technology, including pharmaceutical traceability and supply chain man-agement.

This review underscores the potential of blockchain to address critical challenges in healthcare, such as interoperability and data security.

Amidst these advancements, the detection of counterfeit medicines remains a pressing concern. While not directly addressing this issue, the decentralized blockchain-based solution proposed by Smith et al. [5][7][8][11] aims to automate the forward supply chain processes for COVID-19 medical equipment, emphasizing the importance of transparency and reliability in managing medical supplies and waste. However, the broader implications of blockchain technology for detecting fake medicines are evident in the literature, with authors like Wang and Liu [6] discussing its potential to enhance traceability and authenticity within pharmaceutical supply chains.

Overall, the literature survey reveals a growing interest in blockchain technology as a solution to various challenges in healthcare, including the detection of counterfeit medicines. While significant progress has been made in exploring blockchain applications in supply chain management and data security, further research is needed to fully realize its potential in ensuring the authenticity and safety of pharmaceutical products.

III. SYSTEM ARCHITECTURE

A. System Overview

As shown in Fig. 1, The system architecture of the counterfeit medicine detection project is designed to ensure robustness, security, and scalability. It comprises several layers and components working together seamlessly to achieve the project's objectives. Below is an overview of the system architecture:

1) Frontend Layer:

- User Interface (UI) developed using React.js: This layer provides the interface for users to interact with the system. It includes various screens and components for product registration, tracking, and counterfeit detection. The UI communicates with the backend through RESTful APIs.

2) Backend Layer:

- Node.js and Express.js: The backend layer consists of server-side logic responsible for handling re- quests from the frontend, processing business logic, and communicating with the blockchain network.
- RESTful APIs: These APIs facilitate communica- tion between the frontend and backend, enabling seamless data exchange and user interactions.

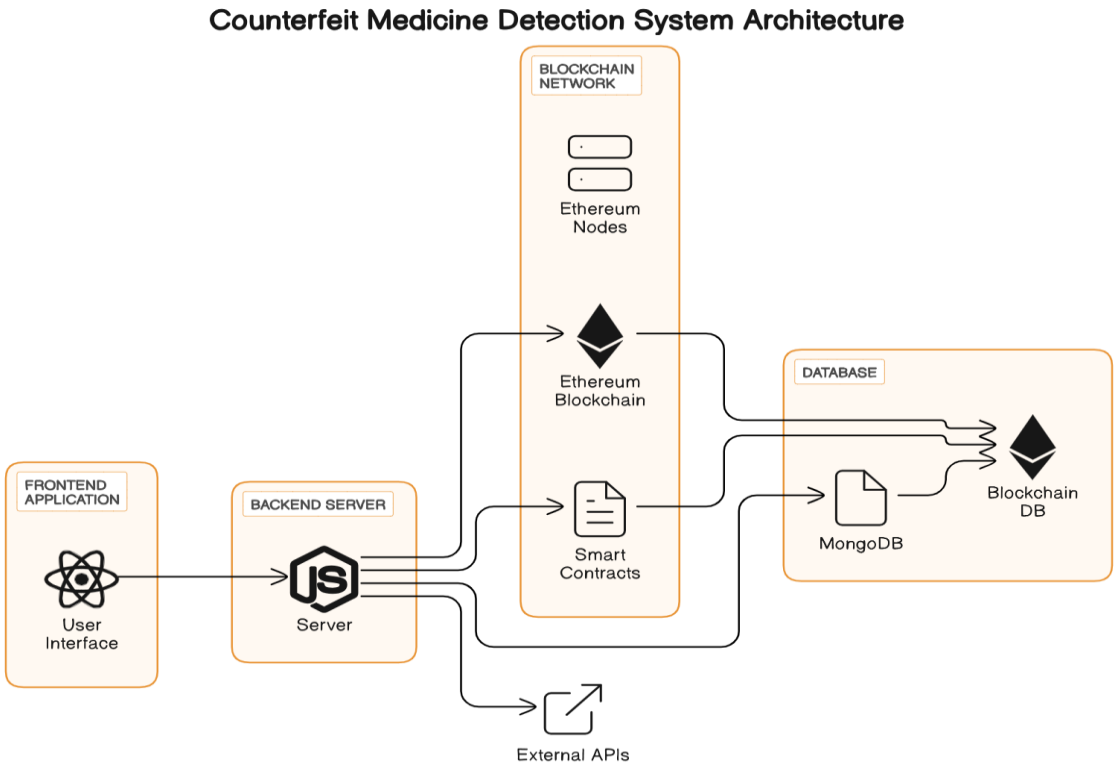

Fig. 1. System Architecture

3) Blockchain Layer:

- Ethereum Blockchain: The core of the system is built on the Ethereum blockchain, which serves as a decentralized and immutable ledger for storing information related to medicine products. Smart contracts are deployed on the Ethereum network to manage product registration, tracking, and counter- feit detection.
- Smart Contracts: These self-executing contracts govern the rules and interactions within the system. They enforce transparency, security, and trust by automating processes such as product registration, ownership transfer, and verification.

Retrieval Number: 100.1/ijsce.C363414030724
DOI: 10.35940/ijsce.C3634.14020524
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

4) Database Layer:
- MongoDB: The system utilizes MongoDB as the database layer for storing non-blockchain-related data, such as user profiles, authentication tokens, and application settings. MongoDB provides flex- ibility, scalability, and performance for managing structured and unstructured data.

5) Integration Layer:
- Integration with External Systems: The system may integrate with external databases, APIs, or services for additional functionality, such as regulatory com- pliance checks or supply chain integration.

6) Security Layer:
- Encryption and Authentication: Security measures such as data encryption and user authentication mechanisms are implemented to safeguard sensitive information and prevent unauthorized access.
- Smart Contract Auditing: Smart contracts undergo thorough auditing and testing to identify and miti- gate vulnerabilities, ensuring the integrity and secu- rity of the system.

7) Scalability and Performance:
- Load Balancing and Scaling: The architecture sup- ports horizontal scaling and load balancing to ac- commodate increasing user traffic and data volumes.
- Performance Optimization: Techniques such as caching, query optimization, and asynchronous pro- cessing are employed to enhance system perfor- mance and responsiveness.

By leveraging these architectural components and prin- ciples, the counterfeit medicine detection system provides a reliable, secure, and efficient solution for combating the proliferation of counterfeit drugs.

B. Smart Contract Design

a. Supply Chain Contract:

This contract is deployed by the Owner of the chain. It consists of many entities associated with the supply chain, i.e., Owner, Supplier, Transporter, Manufacturer, Wholesaler, Distributor, Customer. It also consists of various Solidity events used to communicate with the front end in real-time. Each function in the contract can only be accessed by its respective role assigned to it. This is done with the help of ”modifiers” in Solidity. Thus, no entity without a particular role can access a specific function. This helps to increase the security and accessibility of data stored or queried from the blockchain.

b. Raw Material Contract:

A respective Supplier deploys the Raw Material Contract. Once a raw material is created physically, it is then added to the chain by the supplier that created the raw material. While creating a raw material to be added to the chain, data such as EA (Ethereum Address) of the Supplier, DateTime, EA of Transporter, Transaction Contract Address, etc. are requested from the supplier. It also contains events that can compute the whereabouts of the package in real-time. The EA of Receiver (Manufacturer) is later updated based on the event request- response mechanism. It also stores the current status of the medicine, i.e., which entity currently has the raw material.

c. Medicine Contract:

The respective manufacturer deploys the Medicine Contract. Once a medicine is created physically, it is then added to the chain by the manufacturer that created the medicine. While creating medicine to be added to the chain, data such as EA (Ethereum Address) of Raw Material used to create medicine, DateTime, EA of Transporter, Transaction Contract Address, etc., is requested from the manufacturer. It also contains events that can compute the whereabouts of the package in real- time. The EA of Wholesaler, EA of Distributor, and EA of Customer are updated later based on the event request- response mechanism. It also stores the current status of the medicine, i.e., which entity currently has the package.

d. Transaction Contract:

The Transaction Contract is deployed automatically by the Raw Material and Medicine smart contracts whenever created. The contract takes data such as DateTime, sender EA, receiver EA, location, transaction hash, and the hash of the previous transaction. The transaction hash is 32 bytes. The previous transaction hash is stored for entities to verify the source of products in the chain—an example of transaction data in the smart Transaction contract.

IV. PROPOSED METHODOLOGY

The proposed methodology for detecting counterfeit medicines leverages the integration of blockchain technol- ogy, smart contracts, and QR codes to establish a robust authentication framework. At its core, blockchain serves as the underlying infrastructure, providing a decentralized and immutable ledger to record all transactions and events related to medicine production, distribution, and authentication. This distributed ledger ensures transparency, integrity, and security, mitigating the risk of counterfeit medicines infiltrating the supply chain.

Smart contracts play a pivotal role in the proposed method- ology, encoding authentication rules and protocols to automate the verification process. These self-executing contracts enforce authentication criteria based on QR codes affixed to medicine packaging, validating each transaction on the blockchain in real-time. By embedding authentication logic directly into the blockchain, smart contracts enhance efficiency, accuracy, and transparency in counterfeit detection processes.

The integration of QR codes adds an additional layer of security and traceability to the authentication process. Each medicine package is equipped with a unique QR code con- taining encrypted information about its origin, batch number, and authenticity status. When scanned, the QR code triggers a transaction on the blockchain, prompting smart contracts to validate the medicine’s authenticity against predefined criteria. Any discrepancy or anomaly detected during this process is immediately recorded on the blockchain, enabling stakeholders to take swift and decisive action to mitigate risks and protect public health.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Furthermore, the proposed methodology includes the devel- opment of a user-friendly interface, leveraging technologies such as React.js and Node.js for seamless interaction with the blockchain-based authentication system. This interface facili- tates easy scanning of QR codes by consumers, pharmacists, and regulatory authorities, providing instant feedback on the authenticity of medicines.

Overall, the proposed methodology offers a comprehensive solution to combat the proliferation of counterfeit medicines, safeguarding patient safety and public health through the seamless integration of blockchain, smart contracts, QR codes, and user-friendly interfaces.

A. Medicine Supply Chain Data Storage in Blockchain

The model establishes a supply chain involving drug ad- ministration, manufacturers, distributors, and pharmacies. The verification authority, which is the drug administration, authen- ticates various participants within the blockchain network. The data storage system in the designed framework closely resem- bles the storage of transaction data in Bitcoin. Each participant within this network possesses a public key. Transactions that occur between these participants involve the sharing of public keys, the hash value from the previous transaction, and an encrypted QR code provided by the manufacturer. Also, Smart Contracts are Designed for the supply chain, for raw materials, and for each transaction.

Manufacturers assign QR codes to medicines, encrypting them with hash values generated through a hash function. These QR codes contain comprehensive information regarding the medicine, including details of the manufacturer, ingre- dients, manufacturing and expiry dates, and quantity. This information is processed using CRC-32. To ensure that each medicine possesses a unique QR code and to prevent any potential reuse by the manufacturer, a hash function is em- ployed. Transactions within this supply chain are characterized by robust security and tamper resistance, thanks to intricate algorithms. This design effectively verifies the sender's cryp- tographic signature, ensuring the data's integrity. Unauthorized access to the data storage is effectively thwarted by the combination of public keys, sender-verified digital signatures, and encrypted QR codes, which collectively prevent medicine duplication.

B. Methodology for the Prototype Work

In Fig.3 the process of agreeing on the delivery and receipt of goods by both parties of the transaction is shown using the event request-response mechanism [2].

The process begins with the buyer initiating a purchase request. This action triggers the"buyEvent()" event within the Supply Chain contract. This event provides crucial information, including the Ethereum addresses of the buyer and seller (referred to as Buyer EA and Seller EA), the specific address of the raw material or medicine to be purchased, a signature generated using the buyer's private key, and a timestamp indicating when the request was made. Importantly, the inclusion of these signatures confirms the identity of both parties and the authenticity of the request. The seller's addresses are indexed to enable each seller to access their records based on their unique Ethereum Address.

Subsequently, the seller retrieves log records relevant to their Ethereum address and proceeds to verify the signature within the events. Successful verification results in the triggering of the "respondEvent()" event, allowing the seller to respond to the buyer's request. This response includes a signature created using the seller's private key.

Once this step is completed, the seller arranges for the product to be shipped to the buyer through a transporter. This shipment event is recorded through the "sendEvent()" event, which documents essential details such as the Ethereum addresses of the seller and buyer (Seller EA and Buyer EA),

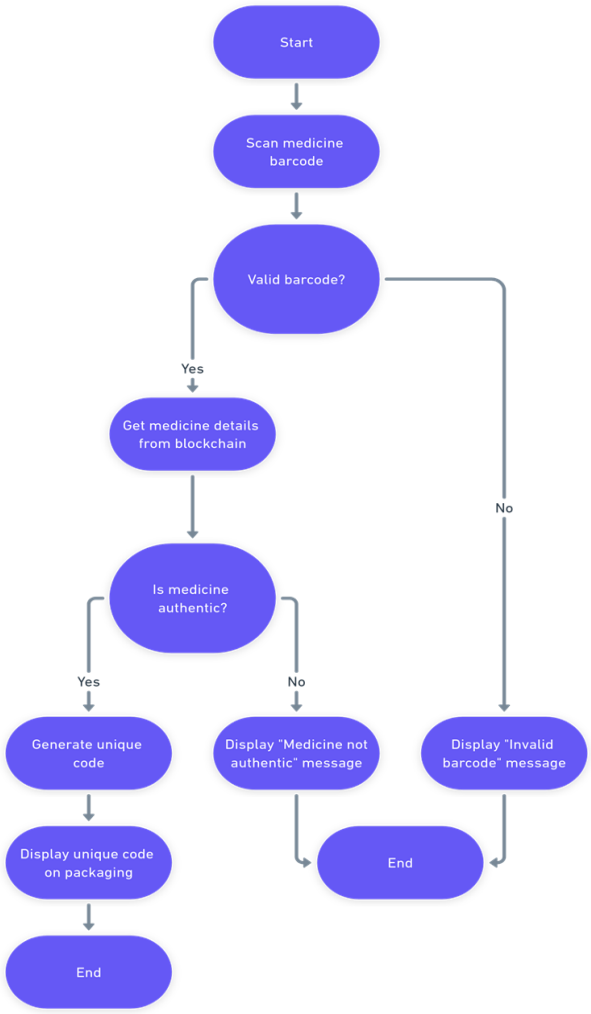

Fig. 2. Qr Code Scanning Flowchart

the product's address, a signature signed with the seller's private key, and a timestamp reflecting when the product was transferred.

Finally, upon receiving the goods, the buyer triggers the "receivedEvent()" event to officially acknowledge the receipt of the products. For instance, in a scenario where a manu- facturer needs raw materials for producing new medicines, the manufacturer takes on the role of the buyer, while the supplier, providing the required raw materials, acts as the seller. Upon successful completion of the described process, the supplier updates transaction information based on the product address in the corresponding Transaction contract, and the new recipient of the raw material is recorded in the Raw Material contract.

Retrieval Number: 100.1/ijsce.C363414030724
DOI: 10.35940/ijsce.C3634.14020524
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

It is essential that only after both transaction parties have genuinely activated the events mentioned above will the transaction details be modified. This system operation ensures that the source of the product is deemed trustworthy.

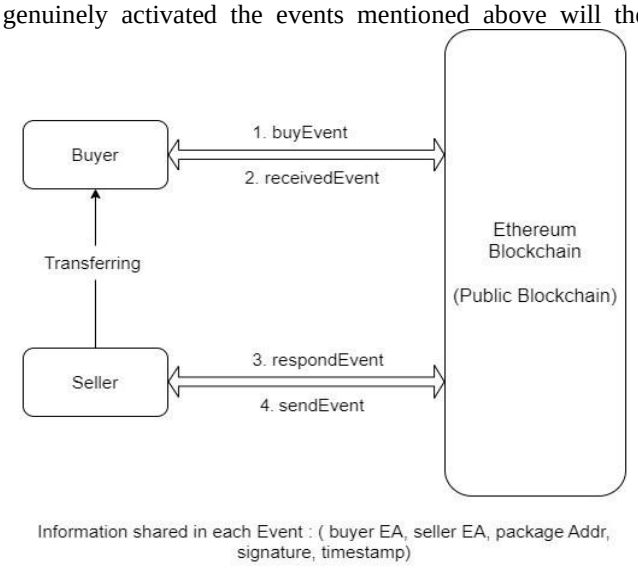

Fig. 3. Event Request-Response Mechanism

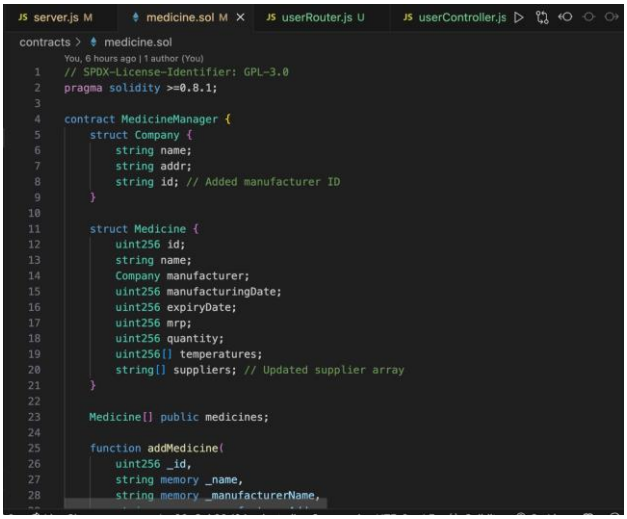

Fig. 4. Smart Contract Development

V. IMPLEMENTATION

A. Softwares & Version

Table I SOFTWARE USED

Software	Version
Solidity	0.8.4
Ganache	2.5.4
Hardhat	2.6.0
Metamask	10.3.0
Web3	1.3.5
React.js	17.0.2
Node.js	14.17.0
MongoDB	4.4.6

B. Setting Up Server with Ngrok

The first step was to set up a server using Ngrok, which provides a secure tunnel to localhost. This allowed for external access to the server and its functionalities.

C. Smart Contract Development

Smart contracts were developed using Solidity, the program- ming language for Ethereum smart contracts. These contracts were designed to manage various aspects of the counterfeit medicine detection system, such as product registration, track- ing, and verification.

D. Integration with Ngrok

The developed smart contracts were integrated with the Ngrok server to enable interaction with the blockchain network. This integration ensured that the server could communicate with the blockchain and execute transactions securely.

E. Utilizing Ganache for Public Blockchain

Ganache, a local blockchain network, was utilized to simulate the Ethereum network environment. It provided a sandboxed environment for testing smart contracts and handling gas fees without incurring actual costs.

F. Connecting MongoDB for Data Storage

MongoDB, a NoSQL database, was connected to the server to store user data securely. This included information about registered products, user accounts, transaction history, and other relevant data needed for the system's operation.

G. QR Code Integration

An API for generating QR codes was integrated into the system. QR codes were generated for each registered product, containing unique identifiers and relevant information. This allowed consumers to scan the QR codes to verify the authen- ticity of the medicines.

VI. RESULT

A. Experimental Results of Smart Contract

Table II Smart Contract Deployment Cost

Contract	Gas Cost	Actual Cost (Ether)
Supply Chain contract	5055356	0.10110712 ETH
Raw Material contract	1015651	0.00142702 ETH
Medicine contract	1405550	0.0023604 ETH
Transaction contract	574042	0.0012762 ETH

B. Performance Analysis

To assess the system's performance deployed on the Ethereum blockchain and accessed through Ganache, the capacity is calculated using Transaction Per Second (TPS).

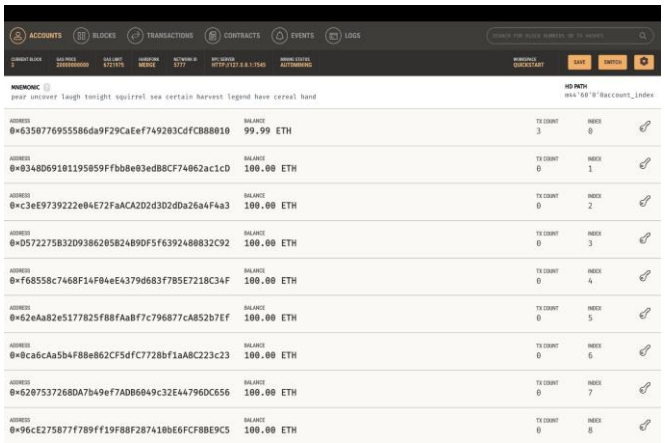

Fig. 5. Ganache Transactions

1) Capacity Calculation Formula:

$$TPS = Capacity = \frac{BlockSize * BlockTime}{Number\ of\ Concurrent\ Average\ Values}$$

Where:

- Block Size and Block Time are determined by the blockchain network.
- Number of Concurrent Average Values refers to the transactions processed simultaneously.

The average TPS for the proposed system ranges between 0.01 to 0.209.

2) Latency Rate: The network's average latency rate, also known as block time, indicates the time required to generate the next block of transactions in the chain. It represents the waiting time for users after executing a transaction. The average latency for the proposed system is measured to be between 0.01 seconds to 1.07 seconds.

3) Deployment Environment: The smart contracts are de- ployed on a local blockchain provided by Ganache, a part of the Truffle suite. The frontend client application interacts with the blockchain using Web3.js.

C. Interface Workflow

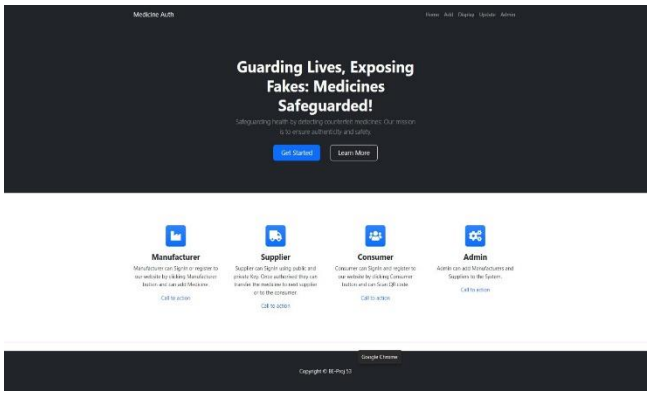

Fig. 6. Website Interface

1) Admin Workflow:

Add Users:

- Admin adds users to the system.
- Users can be suppliers, consumers, or manufactur- ers.

2) Manufacturer Workflow:

Add Medicines:

- Manufacturer logs in and adds medicines to the system.
- Medicines include details like name, batch number, expiry date, etc.

Dispatch Medicines:

- Manufacturer dispatches medicines to the supplier.
- Dispatched medicines are assigned a unique identi- fier or QR code.

3) Supplier Workflow:

Receive Medicines:

- Supplier receives medicines from the manufacturer.
- The supplier logs the received medicines into the system.

Dispatch Medicines:

- Supplier dispatches medicines to other suppliers or directly to consumers.
- Dispatched medicines are logged into the system with relevant details.

4) Consumer Workflow:

Scan QR Code:

- Consumer scans the QR code on the medicine packaging.
- The system fetches and displays detailed informa- tion about the medicine.

Purchase Medicines:

- Consumer purchases medicines directly from the supplier or through a pharmacy.
- Purchase details are recorded in the system for tracking and verification purposes.

VII. FUTURE SCOPE

The future scope of the counterfeit medicine detection project is vast and holds the potential for further enhance- ments and expansions to address evolving challenges in the pharmaceutical industry. Several avenues can be explored to augment the capabilities and impact of the system.

Firstly, the integration of advanced technologies such as machine learning and artificial intelligence (AI) can signif- icantly enhance the accuracy and efficiency of counterfeit detection algorithms. By leveraging machine learning mod- els, the system can continuously learn from incoming data and adapt its detection mechanisms to identify increasingly sophisticated counterfeit patterns and anomalies. AI- powered image recognition algorithms can also be employed to analyze product packaging and identify counterfeit products based on visual cues.

Furthermore, expanding the scope of the project to encom- pass the entire pharmaceutical supply chain offers immense potential for enhancing transparency, traceability, and account- ability. By integrating blockchain technology beyond the point of sale to include manufacturing, distribution, and regulatory oversight, stakeholders can gain real-time visibility into the entire lifecycle of pharmaceutical products. This end-to-end traceability enables proactive risk management, rapid response to quality issues, and enhanced regulatory compliance.

Moreover, the project can explore collaboration opportu- nities with regulatory agencies, industry associations, and international organizations to establish standardized protocols and interoperable systems for counterfeit medicine detection and supply chain integrity. By fostering collaboration and information sharing among stakeholders, the project can con- tribute to the development of a global ecosystem for combating counterfeit drugs and ensuring patient safety on a broader scale.

Additionally, the adoption of decentralized identity solu- tions, such as self-sovereign identity (SSI) frameworks, can strengthen the authentication and verification process for phar- maceutical products. By leveraging decentralized identifiers (DIDs) and verifiable credentials, the system can provide tamper-proof digital identities for products, enabling seamless verification of authenticity across disparate systems and stake- holders.

Retrieval Number: 100.1/ijsce.C363414030724
DOI: 10.35940/ijsce.C3634.14020524
Journal Website: www.ijsce.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Furthermore, the project can explore the potential of integrating Internet of Things (IoT) devices and sensors into the pharmaceutical supply chain to enable real-time monitoring of product conditions and integrity. IoT-enabled smart packaging and tracking devices can transmit vital information such as temperature, humidity, and location, allowing stakeholders to detect and mitigate potential quality issues or tampering incidents in transit.

Overall, the future scope of the counterfeit medicine detection project is characterized by innovation, collaboration, and continuous improvement. By embracing emerging technologies, forging strategic partnerships, and advocating for regula- tory reforms, the project can contribute to the advancement of patient safety, public health, and trust in the pharmaceutical supply chain ecosystem.

VIII. CONCLUSION

In conclusion, the project presents a robust solution for counterfeit medicine detection leveraging blockchain technol- ogy. By enhancing supply chain transparency and enabling stakeholders to track medicine movement, it offers an efficient method for identifying counterfeit products. While challenges like data collection and scalability exist, the project provides a solid groundwork for future research. Future work could include exploring IoT integration and addressing regulatory compliance to further bolster the system's effectiveness in safeguarding public health.

DECLARATION STATEMENT

Funding	No, I did not receive it.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. N. Alam, M. R. Hasan Tanvir, S. A. Shanto, F. Israt, A. Rahman and S. Momotaj, "Blockchain Based Counterfeit Medicine Authentication System," 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 2021, pp. 214-217, doi: https://doi.org/10.1109/ISCAIE51753.2021.9431789
2. D'souza, S.; Nazareth, D.; Vaz, C.; Shetty, M. Blockchain and AI in Pharmaceutical Supply Chain. SSRN Electron. J. 2021. https://doi.org/10.2139/ssrn.3852034
3. Prof. A. G. Said1 , Triveni Gawali , Mayuri Chavan , Sheetal Bendgude, Rutuja Hande, "Fake Drug Detection Using Blockchain Technology", International Journal Of Scientific & Technology Research Volume 11 Issue V May 2023, issn 2321-9653. https://doi.org/10.22214/ijraset.2023.52290
4. M. Wazid, A. K. Das, M. K. Khan, A. A. -D. Al-Ghaiheb, N. Kumar and A. V. Vasilakos," Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1634-1646, Oct. 2017, doi:. https://doi.org/10.1109/JIOT.2017.2706752
5. G. Subramanian, A. S. Thampy, N. V. Ugwuoke and B. Ramnani," Crypto Pharmacy – Digital Medicine: A Mobile Application Integrated With Hybrid Blockchain to Tackle the Issues in Pharma Supply Chain," in IEEE Open Journal of the Computer Society, vol. 2, pp. 26-37, 2021, doi: https://doi.org/10.1109/OJCS.2021.3049330
6. M. Dashtizadeh, F. Meskaran and D. Tan,"A Secure Blockchain-based Pharmaceutical Supply Chain Management System: Traceability and Detection of Counterfeit Covid-19 Vaccines," 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 2022, pp. 1-5, doi: https://doi.org/10.1109/MysuruCon55714.2022.9972646
7. C. Zhang, L. Zhu, C. Xu, K. Sharif, R. Lu and Y. Chen, "APPB: Anti-Counterfeiting and Privacy-Preserving Blockchain-Based Vehicle Supply Chains," in IEEE Transactions on Vehicular Technology, vol. 71, no. 12, pp. 13152-13164, Dec. 2022, doi: https://doi.org/10.1109/TVT.2022.3196051
8. Surjandy, Meyliana, Fernando, E., & Oktriono, K. (2019). Benefit and Challenge of Blockchain Technology in Pharmaceutical Supply Chain Management. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 4, pp. 8309–8313). https://doi.org/10.35940/ijrte.d8986.118419
9. Tribis, Y., Bouchti, A. E., & Bouayad, H. (2021). Blockchain Technology based Supply Chain State of the art and Future Prospects. In International Journal of Innovative Technology and Exploring Engineering (Vol. 10, Issue 3, pp. 125–136). https://doi.org/10.35940/ijitee.c8384.0110321
10. Zagare, S., Khodaskar, Prof. M., Sonawane, Y., & Verma, H. (2024). Study of Fake Medicine Detection using Blockchain. In International Journal of Inventive Engineering and Sciences (Vol. 11, Issue 4, pp. 1–4). https://doi.org/10.35940/ijies.f8017.11040424
11. Kumar, Mr. S. A., & Chakraborty, A. (2019). Medical Applications using Blockchain and Machine Learning. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 2, pp. 3928–3932). https://doi.org/10.35940/ijeat.b2666.129219
12. Kuriakose, N., & Midhunchakkaravarthy, Dr. D. (2022). A Review on IoT Blockchain Technology. In Indian Journal of Data Communication and Networking (Vol. 3, Issue 1, pp. 1–5). https://doi.org/10.54105/ijdcn.f3719.123122