iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62195

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

A Fake Products Identification by Using Blockchain

Gaurav Nagarkar[1], Utkarsha Punekar[2], Zainab Sheikh[3], Dr. Dhananjay Dumbere[4]
B. Tech, Student, Department of Computer Science and Engineering, RCERT, Chandrapur, India

Abstract: ***Counterfeiting of products is a significant challenge across various industries, leading to economic losses and risks to consumer safety. This paper proposes a novel approach to combat counterfeit products using blockchain technology. By leveraging the immutable and transparent nature of blockchain, a framework is devised to authenticate products throughout their lifecycle. The system utilizes unique identifiers assigned to each product during manufacturing, which are then recorded on a blockchain ledger. Through a decentralized network of nodes, stakeholders including manufacturers, distributors, retailers, and consumers can verify the authenticity of products in real-time. Smart contracts are employed to automate verification processes, ensuring integrity and efficiency. Additionally, the framework incorporates mechanisms for data privacy protection, ensuring sensitive information remains secure. Through empirical analysis and simulations, the effectiveness and scalability of the proposed solution are evaluated. Results demonstrate a significant reduction in counterfeit incidents and enhanced trust among stakeholders. This research contributes to the advancement of anti-counterfeiting measures, offering a robust solution to safeguard product authenticity in the digital age.***

Keywords: Blockchain technology, Smart contracts, Transparency, Counterfeit detection, Product authentication, etc.

I. INTRODUCTION

Counterfeiting is a pervasive issue across various industries, posing significant challenges to businesses, consumers, and regulatory authorities alike. The proliferation of counterfeit products not only results in substantial economic losses for legitimate businesses but also poses risks to consumer safety and brand reputation. Traditional methods of counterfeit detection have proven inadequate in combating this growing problem, highlighting the urgent need for innovative solutions. In recent years, blockchain technology has emerged as a promising tool for enhancing supply chain transparency and authenticity verification. By leveraging the inherent characteristics of blockchain, such as immutability, decentralization, and transparency, stakeholders can establish a secure and tamper-proof system for identifying fake products. Blockchain, originally developed as the underlying technology behind cryptocurrencies like Bitcoin, has evolved into a versatile platform with applications across various domains, including supply chain management, healthcare, finance, and beyond. At its core, blockchain is a distributed ledger technology that enables the secure recording of transactions in a transparent and immutable manner. Each transaction, or "block," is cryptographically linked to the previous one, forming a continuous chain of blocks. This decentralized architecture ensures that no single entity has control over the entire network, thereby enhancing security and reliability. The application of blockchain in counterfeit product identification involves the creation of a digital ledger where information about each product's origin, manufacturing process, and distribution history is recorded. Each product is assigned a unique identifier, typically in the form of a cryptographic hash, which serves as its digital fingerprint. This identifier is then associated with the product's metadata, including information such as serial number, batch number, manufacturing date, and relevant supply chain data. By recording this information on the blockchain, stakeholders can track the entire journey of a product from its point of origin to the end consumer. One of the key advantages of using blockchain for fake product identification is its immutability. Once a transaction is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity and authenticity of the data. This feature makes it extremely difficult for counterfeiters to tamper with product information or falsify records, as any unauthorized changes would be immediately detected by the network. Additionally, the decentralized nature of blockchain eliminates the need for a central authority to verify transactions, reducing the risk of fraud and manipulation. Another important feature of blockchain technology is its transparency. All transactions recorded on the blockchain are visible to all participants in the network, providing complete visibility into the supply chain. This transparency fosters trust among stakeholders and enables swift identification of counterfeit products. By simply scanning a product's unique identifier, consumers can access its entire history on the blockchain, including its journey through the supply chain and verification of its authenticity.

In this project, we propose a comprehensive framework for fake product identification using blockchain technology. We will discuss the various components of the framework, including the generation and storage of product identifiers, the implementation of smart contracts for automated verification, and the integration with existing supply chain systems. Furthermore, we will explore real-world use cases and empirical studies to evaluate the effectiveness and scalability of the proposed solution. Through this research, we aim to contribute to the advancement of anti-counterfeiting measures and foster greater trust and transparency in the global marketplace.

II. LITERATURE REVIEW

The survey focused on understanding the sources of counterfeits, impact on the society.There exist various systems of fake product detection,which use Artificial Intelligence, QR codes , Machine Learning and Blockchain.

The methods discussed by Shaik included the use of providing product with public and private keys as QR code, the app used to scan the QR should have cryptographic functionality to decrypt the QR code. The manufacturer is also supposed to run server to accept request and match the buyers name, and items code. The scanning app should have cryptographic functionality to decrypt ciphertext of the item code encoded in the QR code [9]. Benatia and Baudry et.al explains traceability-CPS based architecture for supply chain management consists of several layers that interact to form a traceability-CPS. Also, the proposed architecture allows supply chain monitoring and data analytic to enhance product. Safety and quality. The proposed algorithm con- sist on computing the most frequent item sets in the prod- uct transaction database. This item sets are then used as genuine product trajectories and can serve in detecting ab- normal product behavior[10]

Khalil and Doss et.al comes up with the solution of using RFID based system to reduce counterfeiting. This system allows consumers to query in-store the tag attached to an item to verify its legitimacy. RFID-based anti-counterfeiting and anti-theft schemes are suitable for large scale implementation in retail environments. The proposed scheme is lightweight and suitable for implementation using low-cost passive RFID tags. Tran and Hong's anti- counterfeiting protocol are used. This system is immune to DOS attacks [11]. Habib and Sardar et.al gives explanation on SCM trends. They are examined in their work process that executives' difficulties and transaction issues are problems featured in the SCM. Hence proposed a solution, SCM by considering the blockchain as a technological feature for solving them. Primary method for structuring new models should find the transaction process at a plan level [12]

Daoud and Vu et.al focuses on the architecture of AI Application. It has three main parts: the data set, detection models, and trained model. Anti- counterfeiting machine learning-based solution to detect fake products. Training models step and detecting logo step are the two steps required. Faster R-CNN achieves high accuracy and low training speed [13]. Chen and Shi et.al explains SCQI. Framework for blockchain based SCQI provides a theoretical basis to intelligent quality management of supply chains based on blockchain technology. RFID technology is used to record quality information, trans- action information. Smart contracts are used to execute quality control and improve the efficiency of the supply chain [14]. Toyoda, Kentaroh and Mathiopoulos, P Takis et.al Proposed system to detect fake product with the help of QR code. End users can scan the QR code assigned to product to get the product details and transaction history, the steps involved Product enrolment, ship product to distributor, and ship product to retailer, end user gets details about the produc [15].

In a Blockchain based system the data is stored on each node, then the nodes exchange information with each other over the network. Each node maintains all Blockchain data. The node verifies the received transactions and include them in the new block based on its own Blockchain data, and try to obtain the rights of the new block. Ethereum as the back-end Blockchain operating system. Store relevant information on product sales in Blockchain which is accessible to everyone. It is cost efficient [7]. In this blockchain technology for information sharing is proposed. Is this the information is in the control of the owner so third party interference is difficult. Users are always aware of the data that is being collected about them and how it is used. The blockchain block contains sender, amount, receiver, transaction id, product id and metadata [16]. Ethereum is a open-source Blockchain.Ethereum is a technology that's home to digital money,global payments and applications.The process is simple as to get into the portal,pick a wallet that lets you connect to Ehereum and manage your funds , Get the ETH, use applications powered by Ethereum, start building [17]

Previous studies have highlighted the limitations of traditional anti-counterfeiting methods, such as holograms, serial numbers, and RFID tags. These methods often lack transparency and traceability, making them susceptible to forgery and manipulation. In contrast, blockchain-based solutions offer a decentralized approach to product authentication, enabling stakeholders to verify the authenticity of goods in real-time. Research by Yao et al. (2019) demonstrated the potential of blockchain in combating counterfeit pharmaceuticals, where a decentralized system was utilized to track drug provenance and ensure patient safety.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Furthermore, blockchain technology facilitates the implementation of smart contracts, which are self-executing contracts with predefined conditions. Smart contracts enable automation of verification processes and enforcement of agreements without the need for intermediaries. Studies by Lu et al. (2020) and Kim et al. (2021) explored the use of smart contracts in supply chain management, demonstrating their effectiveness in enhancing transparency, efficiency, and trust among stakeholders.

Privacy and data protection are critical considerations in the implementation of blockchain-based counterfeit identification systems. While blockchain offers transparency, it also raises concerns regarding the exposure of sensitive information. Research by Kuo et al. (2020) proposed privacy-preserving techniques, such as zero-knowledge proofs and homomorphic encryption, to address these concerns while maintaining data integrity and confidentiality. Despite the promising potential of blockchain technology, challenges remain in its widespread adoption for counterfeit identification. Scalability, interoperability, and regulatory compliance are among the key issues that need to be addressed. Additionally, the success of blockchain-based solutions relies on the collaboration and participation of multiple stakeholders across the supply chain. Research by Wang et al. (2022) emphasized the importance of ecosystem collaboration in the implementation of blockchain-based anti-counterfeiting initiatives.

III. BLOCKCHAIN TECHNOLOGY

Blockchain technology has emerged as a transformative innovation with the potential to revolutionize various industries. Initially introduced as the underlying technology behind Bitcoin, blockchain has evolved into a versatile solution that extends far beyond cryptocurrencies. Its decentralized and transparent nature, combined with cryptographic security mechanisms, offers numerous advantages in terms of data integrity, trust, and efficiency. In this report, we will explore the fundamental concepts, components, and mechanisms of blockchain technology. We will also delve into its key features, applications in different sectors, and potential challenges.

A. Understanding Blockchain Technology

1) Definition and Overview

Blockchain can be defined as a distributed ledger technology that enables the secure and transparent storage and transfer of digital assets or information. It consists of a chain of blocks, where each block contains a collection of transactions. These transactions are validated, recorded, and linked together using cryptographic algorithms, ensuring the integrity and immutability of the data.

2) Components of Blockchain

a) Blocks: Blocks are containers that store a set of transactions. Each block typically includes a header containing metadata, such as a timestamp, previous block hash, and a nonce.

b) Transactions: Transactions represent the records of digital assets or information being exchanged between participants. These transactions are grouped together within a block.

c) Chain: The chain refers to the chronological sequence of blocks, forming a continuous and unbroken ledger. Each block contains a reference to the previous block's hash, creating a chain-like structure.

3) Key Features of Blockchain

a) Decentralization: Blockchain operates on a decentralized network, eliminating the need for a central authority or intermediary. This decentralized nature ensures that no single entity has control or ownership over the data.

b) Transparency: The transparency of blockchain allows all participants to view and verify the transactions and the state of the ledger. Each participant has access to a copy of the entire blockchain, ensuring transparency and accountability.

c) Immutability: Once a transaction is recorded in a block and added to the blockchain, it becomes nearly impossible to alter or tamper with. This immutability ensures the integrity and trustworthiness of the data.

d) Security: Blockchain employs cryptographic algorithms to secure the data and ensure the privacy and authenticity of transactions. Consensus mechanisms, such as proof-of-work or proof-of-stake, provide robust security against malicious activities.

B. Blockchain Architecture

1) Blockchain Networks

a) *Public Blockchains:* Public blockchains are open and permissionless networks that allow anyone to participate and validate transactions. Examples include Bitcoin and Ethereum. These networks are characterized by high transparency but may face scalability and privacy challenges.
b) *Private Blockchains:* Private blockchains are permissioned networks that restrict participation to specific entities or consortiums. These networks offer greater privacy, scalability, and control but sacrifice some degree of decentralization.

C. Consensus Mechanisms

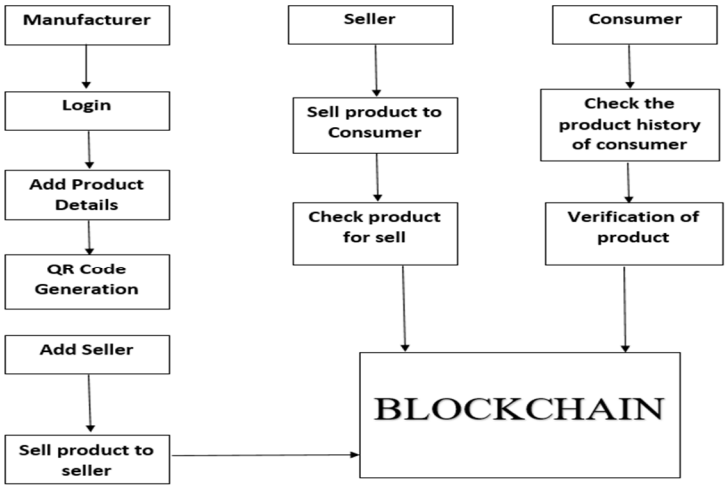
Consensus mechanisms are used in blockchain networks to agree on the validity of transactions and ensure the integrity of the ledger. Some commonly used consensus mechanisms include:

1) *Proof-of-Work (PoW):* PoW requires participants to solve complex mathematical puzzles to validate transactions. This mechanism is resource-intensive but provides a high level of security.
2) *Proof-of-Stake (PoS):* PoS assigns block validation rights based on participants' stake or ownership of the cryptocurrency. It is more energy-efficient than PoW but requires a certain level of trust among participants.

Blockchain is a distributed database with decentralised, traceable, non-tamperable, secure and reliable features. It integrates P2P (Peer-to-Peer) protocol, digital encryption technology, consensus mechanism, smart contract and other technologies together. Abandoning the maintenance mode of the traditional central node and adopting the method of mutual maintenance by multiple users to realise the information supervision among multiple parties, thereby ensuring the credibility and integrity of the data. The blockchain platform can be divided into public chain, private chain and alliance chain. All nodes in the public chain can join or withdraw freely; the private chain strictly limits the qualification of participating nodes; the alliance chain is jointly managed by several participating institutions. Bitcoin was proposed by Nakamoto in 2008, which is the most successful case of digital currency, and is also the most typical application of blockchain. In addition, the blockchain has expanded its unique application value in many aspects and has shown its potential to reshape society.

As a representative of distributed databases, blockchain stores all user transaction information on the blockchain, which has high requirements for the security performance of blockchain. Blockchain is a decentralised peer-to-peer network. Nodes do not need to trust each other and there is no central node. Therefore, transactions on the blockchain also need to ensure the security of transaction information on unsecured channels and to maintain the integrity of transactions. It can be seen that cryptography technology occupies the most central position in the blockchain. In blockchain, cryptography technology is mainly used to protect user privacy and transaction information, and ensure data consistency, etc.[2] This paper briefly introduces the cryptographic techniques such as hash algorithm, asymmetric encryption algorithm and digital signature, also elaborates the blockchain infrastructure, the blockchain structure, bitcoin address, digital currency trading and other technologies of blockchain, and also explains how cryptography technology protects privacy and transaction maintenance in the blockchain in detail.

IV. METHODOLOGY



System Architecture of project

If we describe the general architecture of the model, you will notice that it is incredibly simple to use.

A. Problem Definition and Scope Identification

Define the specific counterfeit problem faced by the target industry or product.Identify the scope of the project, including the types of products to be addressed, supply chain stakeholders involved, and geographical regions covered.

B. Requirement Analysis

Engage stakeholders, including manufacturers, distributors, retailers, and consumers, to gather requirements and understand their needs. Define the functional and non-functional requirements of the blockchain-based counterfeit detection system, considering factors such as scalability, interoperability, privacy, and regulatory compliance.

C. Blockchain Platform Selection

Evaluate various blockchain platforms (e.g., Ethereum, Hyperledger, Corda) based on their suitability for the project requirements. Consider factors such as consensus mechanism, smart contract support, scalability, security features, and developer community support.

D. System Design

Design the architecture of the blockchain-based counterfeit detection system, including the data model, smart contracts, user interfaces, and integration points with existing systems. Define the workflow for product authentication, including the generation and registration of unique product identifiers, recording transactions on the blockchain, and verification processes.

E. Prototype Development

Develop a prototype or proof-of-concept implementation of the counterfeit detection system using the selected blockchain platform. Implement smart contracts for managing product identifiers, recording transactions, and automating verification processes. Design user interfaces for stakeholders to interact with the system, including product authentication portals and administrative dashboards.

F. Testing and Validation

Conduct rigorous testing of the prototype to ensure functionality, security, and performance. Test the system under various scenarios, including simulated counterfeit attempts, network congestion, and failure conditions. Validate the effectiveness of the counterfeit detection system through empirical analysis, including metrics such as counterfeit detection rate, false positive rate, and verification speed.

G. Deployment and Integration

Deploy the blockchain-based counterfeit detection system in a production environment, ensuring scalability, reliability, and security. Integrate the system with existing supply chain management systems, ERP systems, and product databases to enable seamless data exchange and interoperability. Provide training and support to stakeholders for using the system effectively.

H. Monitoring and Maintenance

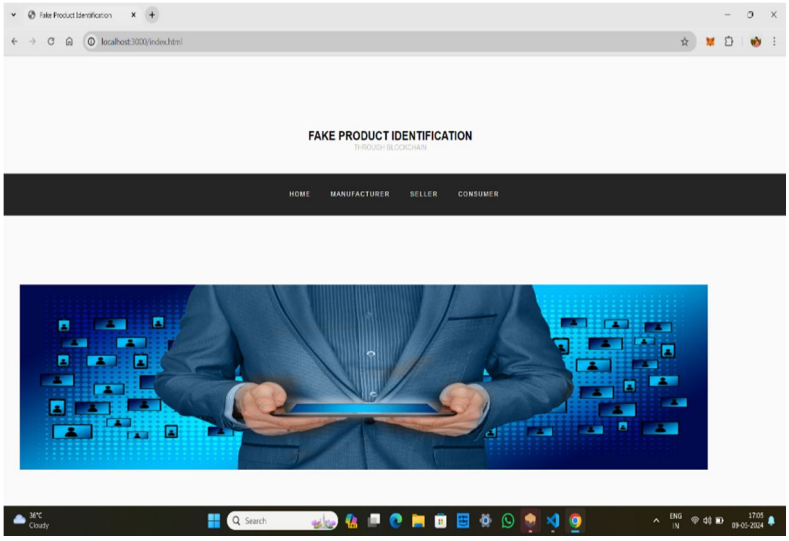
Implement monitoring tools and processes to track the performance and health of the blockchain network and counterfeit detection system. Establish protocols for handling system updates, patches, and security vulnerabilities. Continuously gather feedback from stakeholders and iterate on the system to address emerging challenges and improve functionality.

I. Modules

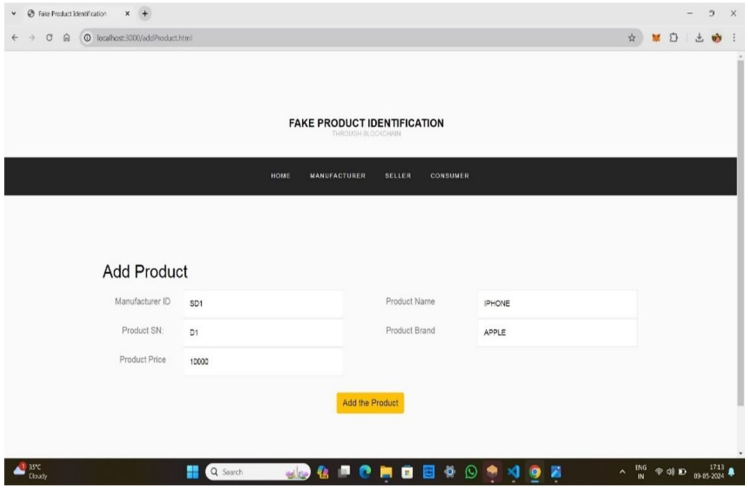
Type of Logins: Three Type of login. Manufacturer, User and Admin.
Registration: User have to register to become a part of project.
Login: User have to login themself to access in project.
Add Product : After Manufacturer Login Manufacturer can add product using java script and smart Contract in Block chain Database.
Generate Qr Code: All Product data display in admin side and admin verify that product and generate qr code of that related product using python and add in block chain database.
Scan Qr Code: User Scan that QR code using Android Application And then Display All information of product in our mobile screen.

V. OUTPUT

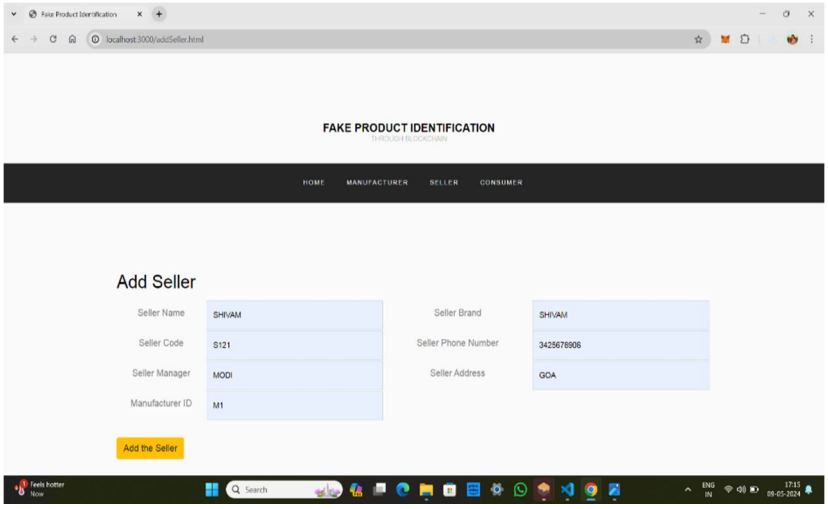
1) Graphical User Interface



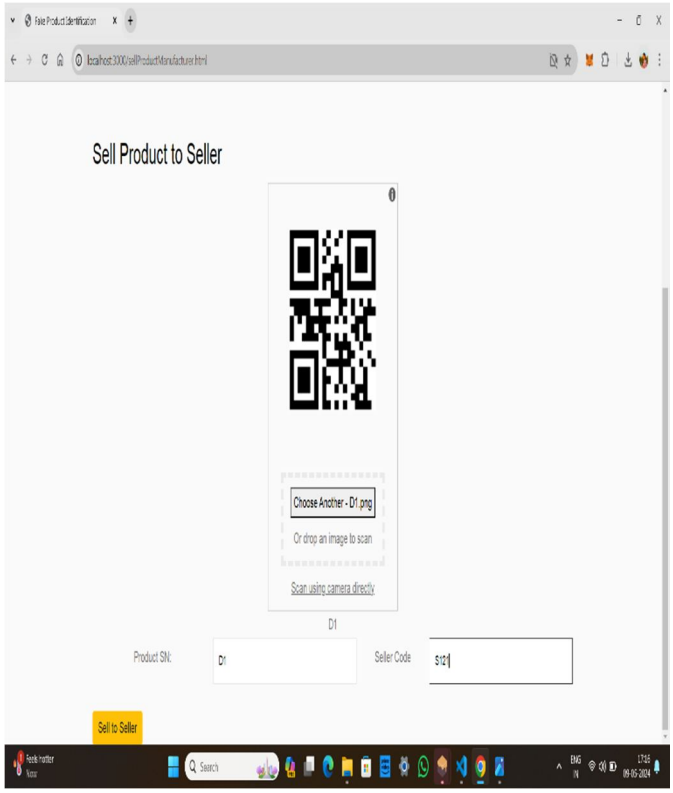
2) Add Product Details

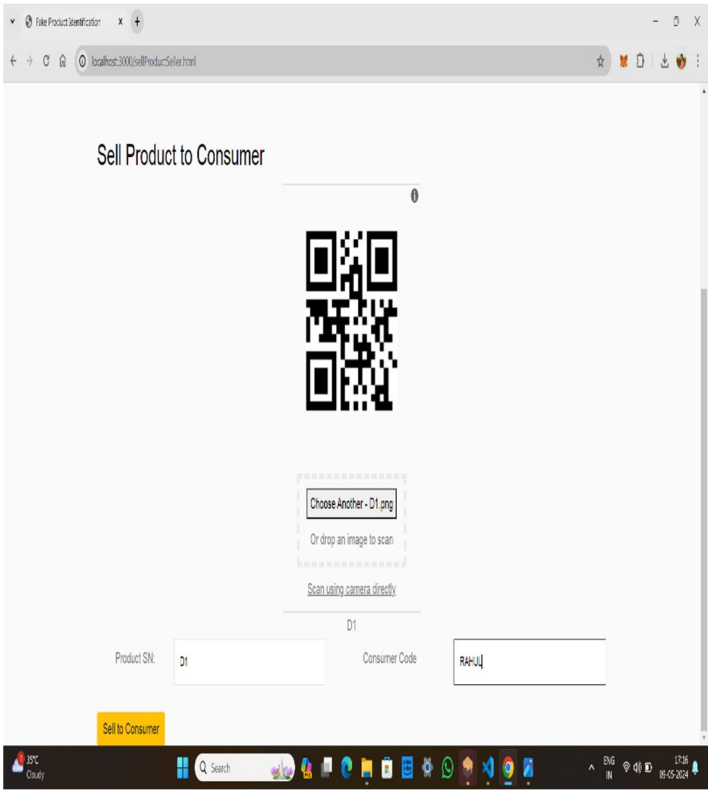


3) Add user Details

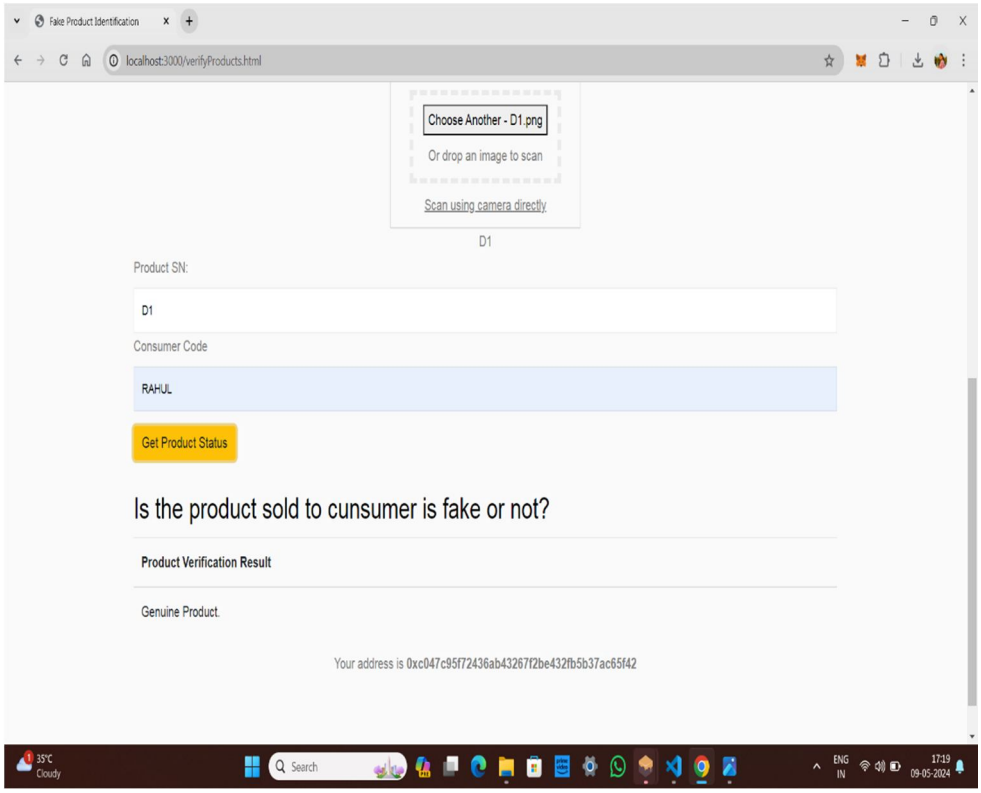


4) QR code





5) To display the Product is Fake or Not

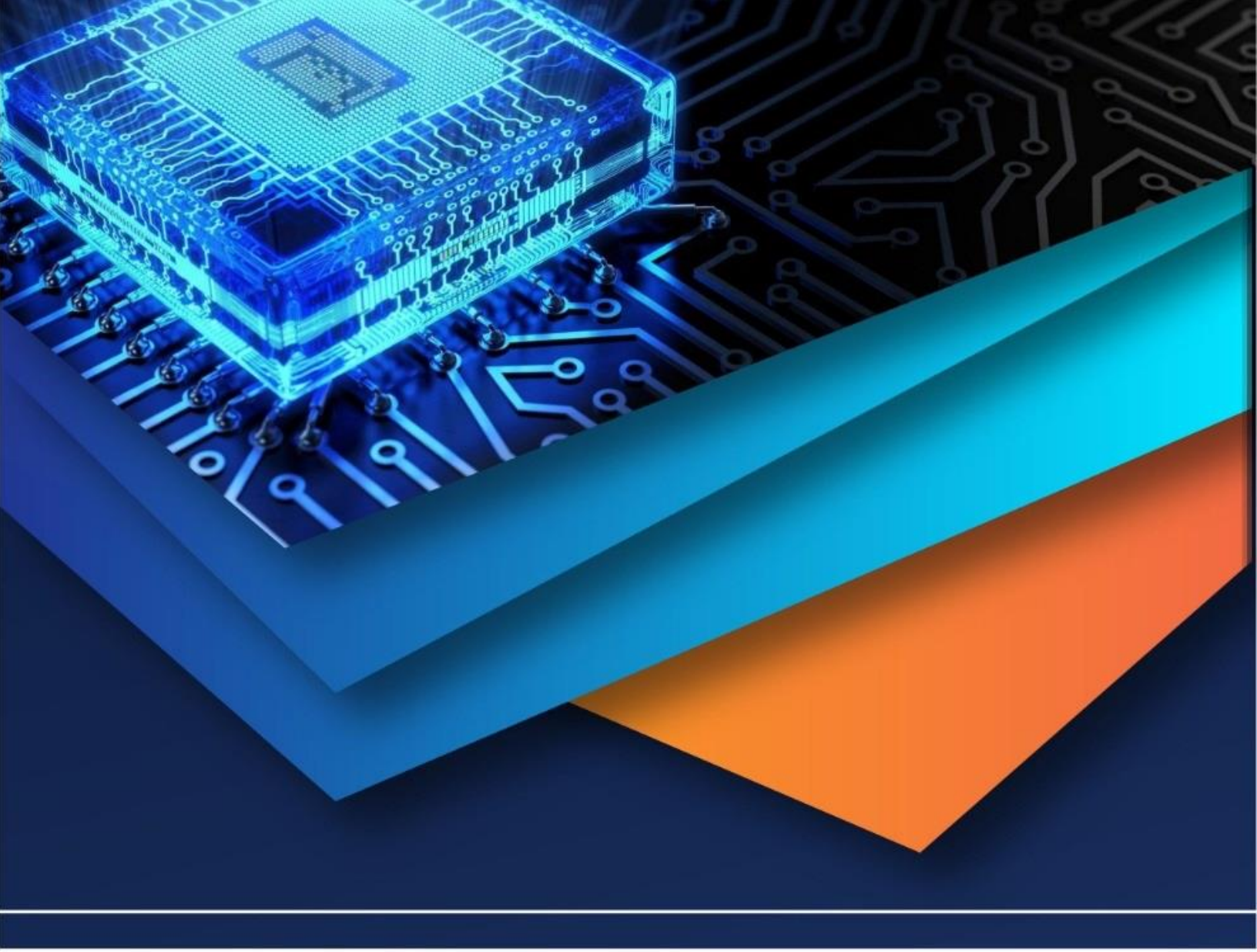


VI. CONCLUSION

The proposed system allows both manufacturers and suppliers to interact with the system to add their respective blocks containing the transaction details to the blockchain without modifying the other's block. Since the code is running on a local network ganache has been used for local testing. The contracts are then compiled and deployed using truffle. The interface is created using HTML, CSS, and JavaScript. To allow interaction with the Ethereum blockchain Web3.js library is used which is used to perform actions like reading, and writing data from smart contracts. MetaMask is installed on a browser which is a wallet to interact with the Ethereum blockchain. Accounts from ganache are imported into the MetaMask. To add supplier and manufacturer blocks they must confirm the transactions using their account MetaMask wallet which is connected using Web3.js. The end-user can then check the supply chain by scanning the QR code to check the integrity of the goods

REFERENCES

[1] G. Vidhya Lakshmi, Subbarao Gogulamudi, Bodapati Nagaeswari, Shaik Reehana, "Blockchain Based Inventory Management by QR Code Using Open CV", International Conference on Computer Communication and Informatics (ICCCI -2021) Coimbatore, INDIA, Jan. 27 – 29, 2021.
[2] Abhinav Sanghi, Aayush, Ashutosh Kata war, Anshul Arora, Aditya Kaushik, "Detecting Fake Drugs using Blockchain", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-10 Issue-1, May 2021.
[3] Miguel A. Prada-Delgado, Gero Dittmann, Ilie Circular, Jens Jelte "A blockchain- based crypto-anchor platform for interoperable product authentication", EEE International Symposium on Circuits and Systems (ISCAS),2021.
[4] Mrs. S. Thejaswini, Ranjitha K R, "Blockchain in Agriculture by using Decentralized Peer to Peer Networks", Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC 2020),2020.
[5] ASPA, The state of counterfeiting in india 2021, https : / / www.aspaglobal.com / pre_upload / nation / 1623216858-4730baa0efdb83aba174859af0a3a6a5-Report % 20The % 20State % 20of % 20Counterfeiting % 20in % 20India % 202021.pdf (2021)
[6] Y. Lu, Journal of Management Analytics 5, 1 (2018)
[7] F. Casino, T.K. Dasaklis, C. Patsakis, Telematics Informatics 36, 55 (2019)
[8] M. Peck, IEEE Spectrum 54, 26 (2017)
[9] S. Idrees, M. Nowostawski, R. Jameel, A. Mourya, Electronics 10, 951 (2021)
[10] Zignuts Technolab, How blockchain architecture works? basic understanding of blockchain and its architecture.
[11] J. Ma, S.Y. Lin, X. Chen, H.M. Sun, Y.C. Chen, H. Wang, IEEE Access 8, 77642 (2020)
[12] M.J.L.I.N.M. J.M. Bohli, N. Gruschka, IEEE 10, 9 (2013)
[13] C. Shaik, Computer Science & Engineering: An International Journal (CSEIJ) 11 (2021)
[14] M.A. Benatia, D. Baudry, A. Louis, Journal of Ambient Intelligence and Humanized Computing pp. 1–10 (2020)
[15] G. Khalil, R. Doss, M. Chowdhury, IEEE Access 8, 47952 (2020) [12] M.A. Habib, M.B. Sardar, S. Jabbar, C.N. Faisal, N. Mahmood, M. Ahmad, Blockchain-based supply chain for the automation of transaction



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY