Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
https://irojournals.com/iroismac/

Fake Product Identification in E-Commerce Platform using Blockchain Technology

SANTHIYA. G[1], LOKESH.G[2]

[1]Assistant professor, Department of Information Technology, SRM Valliammai Engineering College, Kattankulathur.

[2]Student Department of Information Technology, SRM Valliammai Engineering College, Kattankulathur.

Email: [1]santhiyag.it@srmvalliammai.ac.in, [2]lokesh.gna2020@gmail.com

Abstract

The proposed fake product identification system employs blockchain technology to address the escalating issues of counterfeit goods. Utilizing a decentralized ledger, each product is assigned a unique identifier recorded on the blockchain, which includes important manufacturing details and origin information. Smart contracts streamline the verification process by executing predefined rules to confirm product authenticity. Integration with supply chain systems ensures real-time tracking, enabling consumers to trace a product's journey from production to sale. Utilizing QR codes consumers gain direct access to blockchain records, empowering them to make informed purchasing decisions. The system's decentralized nature ensures information immutability, providing a tamper proof solution for product authentication. Collaboration among stakeholders within the blockchain network creates a united front against counterfeiters, fostering a shared responsibility for maintaining supply chain integrity. This globally accessibly solution transcends borders, enhancing international cooperation in combatting counterfeit products and preserving brand credibility.

Keywords: Blockchain, Fake product, QR code, Decentralized Nature, Supply Chain.

DOI: https://doi.org/10.36548/jismac.2024.2.005
Received: 08.04.2024, received in revised form: 30.04.2024, accepted: 14.05.2024, published: 24.05.2024

1. Introduction

Fake product identification through blockchain technology is a revolutionary approach to tackle the pervasive issue of counterfeit goods in the global market. Blockchain, a decentralized and distributed ledger, provides a secure and transparent system for tracking and verifying the authenticity of products throughout their entire supply chain. This creates an immutable and transparent history, making it virtually impossible for malicious actors to introduce fake products into the supply chain without detection. Consumers and other stakeholders can easily access this information using blockchain-powered apps or scanning devices. By checking the product's unique identifier against the blockchain records, they can verify its authenticity and ensure that it has not been tampered with or substituted along the way. To design and develop the user interface for a blockchain-based application, we use React for building dynamic and responsive UIs, and Web3.js and Ethers.js for interacting with Ethereum and other blockchain networks, in order to integrate smart contract functionality. For scalable and flexible data storage, MongoDB can be used to handle metadata and IPFS can be used to handle decentralized data, respectively. Visual Studio Code provides an efficient and robust development environment with extensive extensions for JavaScript and blockchain development. Additionally, Truffle and Ganache are valuable tools for deploying and testing smart contracts in a personal blockchain environment.

2. Related Works

Leveraging blockchain technology eliminates the necessity for consumers to place trust in external entities when seeking information about the origin of their purchased products securely. This paper introduces a novel approach to detect counterfeit products by utilizing a barcode reader, connecting the product's barcode to a Blockchain-Based Management (BCBM) system. The proposed system serves as a repository for storing comprehensive product details and the corresponding unique codes as individual blocks within the blockchain database. When a customer provides the unique code, the system cross-references it with the entries in the blockchain database. In the event of a match, a notification is promptly sent to the customer, ensuring a secure and reliable validation process for product authenticity [1].

This comprehensive survey paper delves into the architectures of cryptocurrencies, smart contracts, and various applications based on Blockchain technology. It offers an insightful perspective on elucidating Blockchain architectures in connection with

cryptocurrencies, smart contracts, and diverse applications. The paper underscores research progress in consensus mechanisms, shedding light on pivotal advancements and application frameworks. Furthermore, it engages in an in-depth exploration of future prospects and open research avenues, providing a roadmap for researchers to navigate the challenging aspects in the evolving landscape of Blockchain technology [2].

While conventional Supply Chain Management (SCM) systems are extensively utilized in the current market, blockchain represents a relatively new paradigm that is yet to witness widespread adoption in the industry. The prevalence of current SCM systems is attributed to their ease of implementation on a large scale and cost-effectiveness. However, despite their extensive use, these systems exhibit inherent flaws that have persisted throughout their existence. Notably, the existing systems are characterized by opaqueness and susceptibility to various fraudulent activities due to inadequate transaction record maintenance. The lack of transparency fosters a significant trust deficit among participating entities, a challenge that remains unresolved. Customer trust in the system is compromised by the failure to deliver quality-assured products, a critical factor influencing business growth. Despite these shortcomings, major market players continue to deploy these systems, exploiting product prices without necessarily establishing credibility [3].

This well-conceived paper introduces a framework for Supply Chain Quality Intelligence (SCQI) based on blockchain technology. The proposed framework not only establishes a theoretical foundation for intelligent quality management within the supply chain but also serves as a cornerstone for advancing theories related to the management of information resources in distributed, virtual organizations. Specifically, it contributes to the development of theories concerning the management of information resources in scenarios characterized by distribution, cross-organizational collaboration, and decentralized management. The framework's application extends beyond intelligent quality management, providing a valuable contribution to the broader field of organizational management theories in the context of distributed and decentralized structures [4].

This paper addresses the escalating issue of counterfeit products proliferating in both online markets and the illicit black market. The prevalence of counterfeit goods poses a significant challenge to supply chains, prompting governmental efforts to combat the problem

through the enactment of laws and regulations. Despite these initiatives, controlling counterfeit products remains a formidable task for the government. Consequently, there is a pressing need for an effective approach to detect counterfeit products and implement security measures that can alert both manufacturers and consumers within the supply chain [5].

In this specific paper, manufacturers are presented with the opportunity to utilize a system for storing pertinent information about product sales on the accessible Blockchain. Transparency is ensured as the system reveals the total sales capacity of a seller and the current inventory available. Users can seamlessly engage in vendor-side verification using the system's provided functions. Identity verification is strengthened through the implementation of digital signatures, and the security of the private key is upheld, barring any accidental leaks by the key owner. In the system analysis, the cost-effectiveness is evident, with the initial product record contract incurring a minimal cost of 1.2893394289 US dollars, and each subsequent product sale process being economically viable at 0.17415436749 US dollars [6].

This study focuses on applying the Blockchain concept to enhance the transparency and validity of agricultural supply chains and their processes. The production of food and raw materials has undergone rapid changes in the recent past, prompting the need for an efficient method to connect farmers producing commodities with end customers. The paper explores the implementation of a Blockchain-based architecture and its concepts to instill trustworthiness and transparency within users and their transactions. A notable concern addressed in this study is the potential drawback where farmers may lack awareness of product traceability once they are registered [7].

Blockchain technology is recognized as a potential solution to enhance traceability in the agri-food supply chain and provide stakeholders with crucial information on food quality, safety, and nutrition. However, the lack of expertise in designing the user interface for traceability applications may result in usability challenges. In a move toward creating more user-friendly blockchain-based agri-food traceability applications, this paper conducts a review of existing literature, specifically focusing on the user interface aspects [8].

The detection of counterfeit products, emphasizing the substantial growth of such illicit goods in online and black markets. The escalating prevalence of counterfeit items necessitates a robust response to tackle the challenges associated with their detection. Consequently, there is a pressing demand for developing advanced technologies to enhance the accuracy of

counterfeit product detection, marking it as a dynamic and actively researched domain in the contemporary world. The paper extensively explores different methodologies and techniques aimed at effectively identifying counterfeit products [9].

Blockchain-based Supply Chain Quality Management. The proposed framework serves as a theoretical foundation for implementing intelligent quality management within the supply chain using blockchain technology. Additionally, it establishes a basis for advancing theories related to the management of information resources in distributed and virtual organizations [10].

3. Proposed System

This innovative approach aims to enhance authenticity verification and combat the proliferation of fake products in the market. By utilizing the decentralized and tamper-resistant nature of blockchain, the proposed system provides a robust solution for tracing and confirming the legitimacy of products throughout the supply chain. Each genuine product is assigned a unique identifier, such as a QR code or RFID tag, linked to a blockchain-based ledger. The ledger contains immutable records of the product's journey, including manufacturing details, origin, and transaction history. Smart contracts, self-executing programs with predefined rules, are integrated into the blockchain to automate various processes. These contracts facilitate secure and transparent transactions, contributing to a trustworthy ecosystem. To empower consumers, a user-friendly interface, possibly through a mobile app, allows for easy product verification. By scanning the unique identifier, users can access real-time information stored on the blockchain, confirming the authenticity of the product. Furthermore, the proposed system includes mechanisms for reporting and handling suspicious activities. If a discrepancy is identified or a counterfeit product is suspected, users can report it through the system. Smart contracts and automated alerts can then trigger appropriate actions, ensuring a swift response to potential threats.

3.1. Architecture Diagram

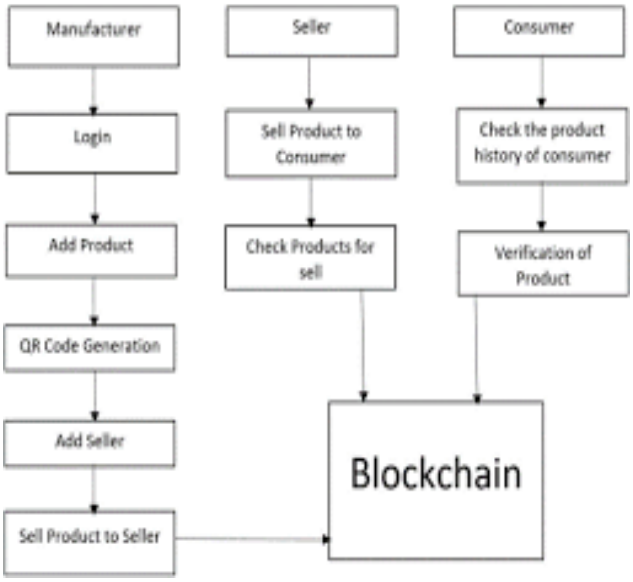

Figure 3.1 Architecture Diagram of Proposed Diagram

3.2. Implementation

In a blockchain-based e-commerce platform, each transaction typically takes place in the following steps with the help of blockchain technology.

1. Initiation: The transaction is initiated when a user (buyer or seller) performs an action on the e-commerce platform, such as placing an order, making a payment, or updating product information.

2. Transaction Data: The details of the transaction, such as the product ID, quantity, price, buyer's address, and payment method, are collected and formatted into a transaction data package.

3. Smart Contract Execution: If smart contracts are used (common in blockchain-based platforms), the transaction data is sent to the relevant smart contract. The smart contract code contains predefined rules and logic for processing transactions automatically without the need for intermediaries.

4. Validation: The transaction data is validated by the nodes (computers) in the blockchain network. This validation ensures that the transaction meets all the predefined conditions, such as available funds for payment, valid product ID, and correct delivery address.

5. Consensus: After validation, the transaction data is included in a new block. The nodes in the network reach a consensus on adding this block to the blockchain. This process ensures that all nodes agree on the validity of the transaction and its sequence in the blockchain's history.

6. Block Addition: Once a consensus is reached, the new block containing the validated transaction data is added to the blockchain. This block becomes part of the immutable ledger, ensuring that the transaction record cannot be altered or deleted.

7. Confirmation: The transaction is confirmed and visible to all participants in the blockchain network. Participants can verify the transaction's details, timestamp, and other relevant information.

8. Notification: Both parties involved in the transaction (buyer and seller) receive notifications or updates regarding the transaction status. This communication can be facilitated through the e-commerce platform's user interface or via email/SMS notifications.

9. Completion: Depending on the type of transaction (e.g., purchase, payment, shipment), the process is completed once all relevant actions, such as product delivery or payment confirmation, are executed as per the smart contract rules.

By leveraging blockchain technology, each transaction in the e-commerce platform benefits from transparency, immutability, and security, reducing the risk of fraud, disputes, and data manipulation.

3.2.1. Manufacturer Module

The Manufacturer Module (MM) primarily serves two functions: (i) registering the manufacturer's details in the blockchain and (ii) verifying authorship for manufacturers seeking to enroll a product's Electronic Product Code (EPC). The pseudo-code for the "enroll Manufacturer ()" function is outlined in algorithm, which captures the process of registering the necessary information when a manufacturer's product is stored in the blockchain.

Adhering to our Product Ownership Management System (POMS) guidelines, only a designated administrator, such as GS1, is permitted to enroll manufacturer information. This condition is assessed in the first step of the algorithm. If validated, the administrator proceeds to enroll the manufacturer's information in the Manufacturers Manager (MM) blockchain.

MM, is responsible for managing manufacturers' information, facilitates functions like registering a company prefix through GS1 and recording the manufacturer's address. Conversely, the Products Manager (PM) is operated independently by each manufacturer, offering functionalities for managing product information, such as enrolling new products and transferring ownership.

Unlike PM, MM operates with the assumption of an administrator tasked with managing manufacturers' information. To mitigate the risk of impersonation, only administrators possess the authority to modify any manufacturer's details. One such administrative candidate is GS1, given its role in overseeing company prefixes.

3.2.2. Distributer Module

In contrast to the Manufacturer Manager ( ), the Decentralized Contract Manager (DM) is individually created by each manufacturer and encompasses four main functions:

1.enrollProduct(): This function is invoked when a manufacturer, denoted as M, initially enrolls its product, specified by a unique Electronic Product Code (EPC), and claims its initial ownership.

2.shipProduct(): Activated when the current owner of a product decides to part with it, specifying the recipient of the product.

3.receiveProduct(): This function is invoked by the new owner to confirm the successful transfer of ownership upon receiving the product.

4.receiveProduct() Description: This function ensures the receiver confirms the product's arrival. It verifies that the claimed EPC is specified by the current owner and that the EPC's status is "Shipped." If validated, ownership is successfully transferred to the message sender's address. Additionally, the product's manufacturer provides an incentive, such as some ETH, as a reward for adhering to the protocol.

Due to Ethereum's transaction execution fees, current owners may hesitate to issue a "shipProduct()" transaction when sending a product to the recipient. To address this, a procedure is introduced. Upon successful ownership transfer, a financial reward, termed "transferReward," is paid back to the previous owner by the product's manufacturer. This reward serves to incentivize cooperation and helps in detecting and identifying counterfeits. It's important to note that the manufacturer's investment in implementing the Product Ownership Management System (POMS) influences the values chosen for "transferReward" and "MAXTRANSFER." However, these considerations are beyond the scope of the current research and will not be explored further.

3.2.3. Retailer Module

Upon completion of the registration process, retailers gain access to product details, including information about the manufacturer, retrieved through a scanning procedure. In the backend, the execution unfolds as all products undergo scanning, and the respective storage locations are transmitted for product verification. This verification process occurs within a hub where a plethora of information is stored. Subsequently, a new blockchain is generated, encapsulating the product's verified details, rendering it ready for sale. The product is then distributed to consumers, marking the completion of the transaction.

3.2.4. Consumer Module

Upon completing the registration, consumers proceed to register themselves, initiating a scanning process for specific products. This process involves the identification of the storage location within the hub, facilitating the verification of the product. Upon successful verification, the product is conclusively identified, marking a pivotal step in the overall process.

3.2.5. QR Code Generation Process

Data Collection: When a product is registered on the e-commerce platform or a transaction is initiated, relevant data such as product details (name, ID, description), transaction ID, timestamp, and any other necessary information are collected. This data is crucial for creating a QR code that links to the corresponding blockchain records.

QR Code Generation: Using a QR code generation library or tool, the collected data is encoded into a QR code format. The QR code can contain various types of information, such as a simple text string, a URL, or structured data in a specific format (e.g., JSON).

Blockchain Record Linking: Before or after generating the QR code, the relevant blockchain records related to the product or transaction are created or updated. This typically involves interacting with smart contracts on the blockchain to store or update the necessary data.

Embedding QR Code Data: The generated QR code is embedded or associated with the blockchain records. This linkage can be achieved by storing the QR code data (e.g., text or URL) in the blockchain along with other transaction details.

Display and Use: The QR code is then made accessible to users, either by displaying it on the product packaging, order confirmation page, or through downloadable/printable options. Users can scan the QR code using a mobile device or QR code scanner application.

Blockchain Verification: When a user scans the QR code, the application retrieves the encoded data. This data is then used to query the blockchain records associated with the QR code. The blockchain verification process ensures that the data in the QR code matches the corresponding records stored on the blockchain.

Transaction Confirmation: Upon successful verification, the user receives confirmation that the product is genuine or that the transaction details are valid. This confirmation is based on the integrity and immutability of the blockchain records linked to the QR code.

3.3. Algorithm

3.3.1 PoW Algorithm

The node diligently monitors the entire network's data records, temporarily storing those that successfully pass basic legality verification.

Once a suitable random number is identified, the node proceeds to generate block information by initially inputting block header details, followed by the inclusion of the verified data record information.

The freshly generated block is disseminated to external nodes upon receiving the necessary authorization. Subsequently, after undergoing verification by other nodes, the block seamlessly integrates into the blockchain, causing an increment in the main chain's height. Consequently, all nodes seamlessly transition to the new block, resuming the execution of workload proof and subsequent block production.

The effectiveness of the Adaptive Proof-of-Work (A-PoW) algorithm relies on the outcomes of the local network node edge verification mechanism checks. This mechanism scrutinizes the behavior of edge nodes and calculates their contributions accordingly. The

creation of nodes follows diverse methods to ensure that the input value calculation formula for each node accurately reflects its contribution to the input blockchain.

The node bounds checking mechanism is instrumental in determining the contribution of each corresponding node, and it operates by evaluating the behavior of the node under examination. This ensures that the calculated node contribution, governed by the provided formula, effectively captures and represents the node's impact on the input blockchain. Through this intricate process, the adaptive handshake algorithm optimizes transaction efficiency while maintaining the security integrity of the local network.

$$Ci= \lambda 1CiP+ \lambda 2CiN$$

$$CiP= \sum nk=1T1(t)*a(b).$$

4. Result and Discussion

To deploy a smart contract using Ganache and Remix IDE, start by opening Remix IDE in your browser and creating a sample smart contract in Solidity. Compile the smart contract within Remix IDE. Next, select "Web3 provider" in Remix, which will prompt you to connect to an Ethereum node; provide the Web3 provider endpoint from Ganache. Ensure Ganache is running and then deploy the contract from Remix IDE. Finally, you can verify the deployment by checking Ganache's transaction log [11]. The results of the user interface developed are shown in Figure 4.1 to 4.6.

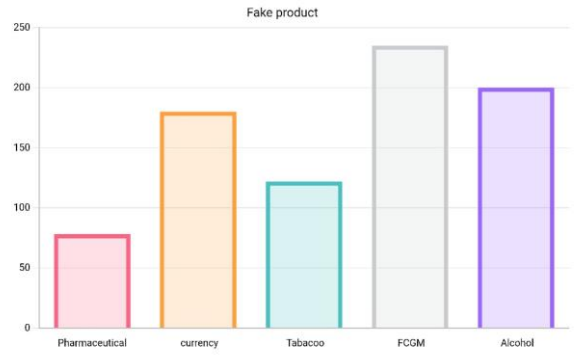

Figure 4.1. Predicted Data

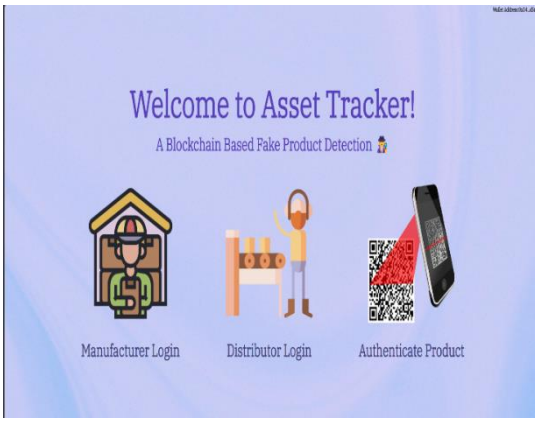

Figure 4.2. Home Page

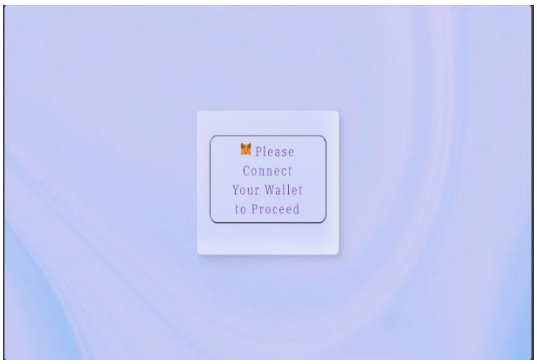

Figure:4.3. Connect to Wallet

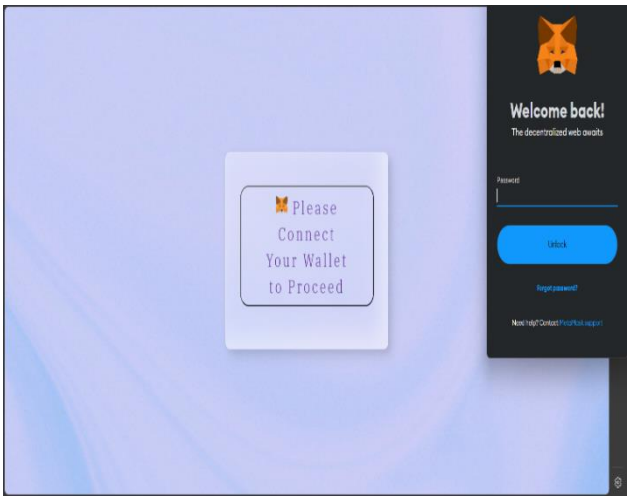

Figure 4.4. Connect to Metamask

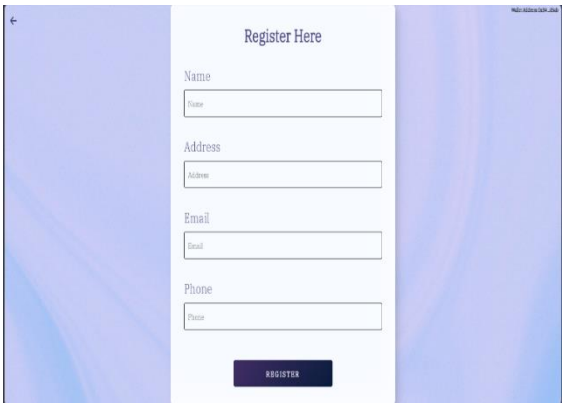

Figure 4.5. Distributor Form

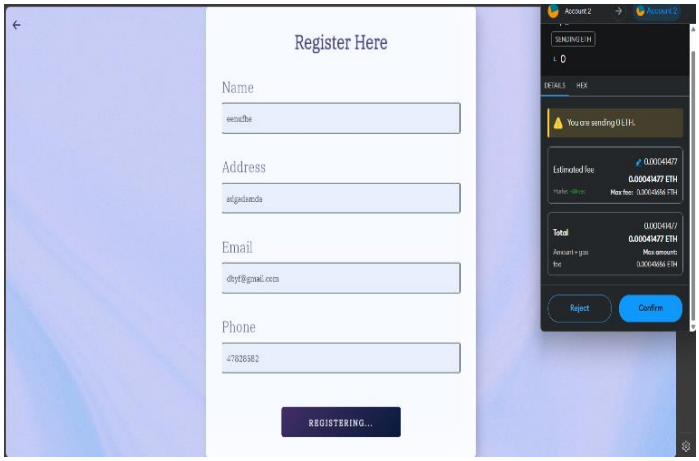

Figure 4.6. Transaction Completed

5. Conclusion

In conclusion, leveraging blockchain technology for fake product identification offers a robust solution by ensuring transparency, traceability, and authenticity throughout the supply chain. The immutable nature of blockchain provides a tamper-resistant system, enhancing consumer trust and combating counterfeit products effectively. This innovative approach not only safeguards consumers but also benefits manufacturers, distributors, and retailers in maintaining the integrity of their products.

5.1. Future Work

To enhance fake product identification using blockchain technology in the future, consider integrating smart contracts to automate verification processes, leveraging IoT devices

for real-time tracking, and implementing AI for advanced pattern recognition to detect counterfeit products more efficiently. Additionally, collaborating with industry stakeholders to establish a standardized blockchain protocol for product authentication can improve overall effectiveness.

References

[1] Abri, F., Gutierrez, L.F., Namin. Fake reviews detection through analysis of linguistic features. arXiv preprint arXiv:2010.04260.

[2] Alharthi, S., Siddiq, R. Detecting Arabic fake reviews in E-commerce platforms using machine and deep learning approaches. J. King Abdulaziz Univ. Comput. Inf. Technol. Sci. 11, 27–34.

[3] The prevalence of current SCM systems is attributed to their ease of implementation on a large scale and cost-effectiveness

[4] Yang, Jie, Hongming Xie, Guangsheng Yu, and Mingyu Liu. "Achieving a just–in–time supply chain: The role of supply chain intelligence." International journal of production economics 231 (2021): 107878.

[5] Hamilton, William L., Cormac Doyle, Mycroft Halliwell-Ewen, and Gabriel Lambert. "Public health interventions to protect against falsified medicines: a systematic review of international, national and local policies." Health policy and planning 31, no. 10 (2016): 1448-1466.

[6] Sunny, Justin, Naveen Undralla, and V. Madhusudanan Pillai. "Supply chain transparency through blockchain-based traceability: An overview with demonstration." Computers & Industrial Engineering 150 (2020): 106895.

[7] Menon, Sheetal, and Karuna Jain. "Blockchain technology for transparency in agri-food supply chain: Use cases, limitations, and future directions." IEEE Transactions on Engineering Management 71 (2021): 106-120.

[8] Mirabelli, Giovanni, and Vittorio Solina. "Blockchain and agricultural supply chains traceability: Research trends and future challenges." Procedia Manufacturing 42 (2020): 414-421.

[9] Staake, Thorsten, and Elgar Fleisch. Countering counterfeit trade: Illicit market insights, best-practice strategies, and management toolbox. Springer Science & Business Media, 2008.

[10] Chen, Si, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, and Jinyu Zhang. "A blockchain-based supply chain quality management framework." In 2017 IEEE 14th international conference on e-business engineering (ICEBE), pp. 172-176. IEEE, 2017.

[11] https://github.com/rohit-raje-786/Fake-product-identification?tab=readme-ov-file