Blockchain Based System to Detect Counterfeit Product In Supply Chain

Dr. Prerana N. Khairnar[1], Tushar Chavan[2], Akash Bhoj[3], Piyush Patil[4], Datta Dhas[5]

[1]Assistant Professor, [2,3,4,5]Research Scholar
Department of Computer Engineering, Sir Visvesvaraya Institute of Technology
Nashik, Maharashtra, India.

Abstract

Supply chain management faces numerous challenges, including service redundancy, poor inter-departmental coordination, and a lack of standardization due to transparency issues. Counterfeit products have become prevalent, making it increasingly difficult to discern genuine items from fakes. Counterfeiters pose significant threats to legitimate businesses, often underestimated by the public. Various methods have been proposed to combat product counterfeiting, such as RFID tags, Artificial Intelligence, and QR code-based systems. However, these solutions have their limitations, like QR codes being copied and AI's heavy computational requirements. This project aims to enhance counterfeit product detection by establishing a comprehensive supply chain history. Leveraging Blockchain technology ensures the identification and traceability of authentic products throughout the supply chain. The decentralized nature of the Blockchain system allows multiple parties simultaneous access, while its immutability safeguards data against unauthorized alterations. This paper introduces a blockchain-based system designed to detect counterfeit products, offering an innovative solution to combat a pressing challenge in the supply chain industry.

Keywords: Supply Chain Management Service Redundancy Coordination Standardization Counterfeit Products.

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 6, Nov.-Dec. 2023

INTRODUCTION

In the complex landscape of modern supply chain management, businesses frequently grapple with a myriad of challenges. Service redundancy, poor coordination among various departments, and a lack of standardization within the supply chain ecosystem are persistent issues that can hamper efficiency and profitability. However, one of the most alarming and pervasive problems affecting this industry is the proliferation of counterfeit products. Counterfeiting has become increasingly sophisticated, making it nearly impossible to visually distinguish genuine items from their fraudulent counterparts. This has significant implications for legitimate firms, posing threats that extend far beyond the awareness of many consumers.

The impact of counterfeit goods on brands, economies, and consumer trust is staggering, yet often underestimated. To combat this ever-growing problem, numerous methods have been proposed and employed in the past. Solutions such as RFID tags, Artificial Intelligence, and QR code-based systems have been introduced with varying degrees of success. Nevertheless, each of these methods carries its own set of limitations. QR codes, for instance, can be easily copied and affixed to fake products, undermining their

effectiveness. Meanwhile, Artificial Intelligence, which relies on convolutional neural networks and machine learning, demands substantial computational power.

This project presents a novel approach to addressing the challenge of counterfeit product detection by focusing on the critical aspect of supply chain history. Leveraging the cutting edge capabilities of Blockchain technology, we seek to ensure the identification and traceability of authentic products throughout the entirety of the supply chain. Blockchain's inherently decentralized nature allows multiple stakeholders to access critical information simultaneously. Furthermore, the immutability of data recorded on the Blockchain makes it exceptionally secure, rendering it highly resistant to vulnerabilities and unauthorized modifications.

This introduces a blockchain-based system meticulously designed to tackle the scourge of counterfeit products, offering a transformative solution to one of the most pressing issues confronting the supply chain industry in the present day. Through this innovative approach, we aim to enhance the integrity and security of supply chains, safeguarding the interests of legitimate businesses, and protecting consumers from the detrimental effects of counterfeit products.

PURPOSE

- **Identify need of Project**

The need for the project outlined above is paramount, given the critical challenges and profound consequences associated with counterfeit products in the contemporary supply chain environment. Firstly, counterfeit goods not only erode consumer trust but also pose significant health and safety risks. These products can infiltrate virtually any industry, from pharmaceuticals to electronics, endangering the well-being of unsuspecting consumers. Furthermore, counterfeit products lead to substantial economic losses, impacting both manufacturers and governments through reduced revenues, lost taxes, and increased enforcement costs.

Supply chain stakeholders, including manufacturers, distributors, and retailers, face a constant battle against counterfeiters who undermine their brands, reputations, and revenues. The lack of transparency in supply chains makes it incredibly difficult to trace the origins of counterfeit items and effectively prevent their distribution. Current methods, such as QR codes or RFID tags, are susceptible to manipulation and require intensive resource investments.

In this context, the project is essential as it proposes an innovative solution to combat the counterfeit product epidemic. Leveraging Blockchain technology offers a transparent, secure, and tamper-resistant approach to track and verify the authenticity of products throughout the supply chain. It not only safeguards brand integrity but also ensures consumer safety and confidence. By enhancing detection and prevention mechanisms, this project addresses a pressing need for more robust and efficient tools to combat counterfeit products and protect the interests of legitimate businesses and the safety of consumers.

OBJECTIVE OF SYSTEM

- Enhance Product Authentication: Develop a robust system that allows for the authentication of products at every stage of the supply chain, ensuring the identification of genuine items and distinguishing them from counterfeit counterparts.
- Improve Supply Chain Transparency: Implement a transparent and traceable system that records product movements and transactions on a Blockchain ledger, making the entire supply chain process more visible and accountable.
- Deter Counterfeiters: Create a strong deterrent for counterfeiters by leveraging the inherent security features of Blockchain technology, making it exceedingly difficult for them to introduce fake products into the supply chain.

- Secure Data and Prevent Tampering: Utilize the immutability of Blockchain to secure data, making it resistant to unauthorized modifications. This ensures the accuracy and integrity of the recorded information, protecting against data tampering and fraud.
- Enhance Consumer Safety: Contribute to consumer safety by ensuring that counterfeit products are easily identifiable and distinguishable from genuine ones, reducing the potential risks associated with substandard or unsafe items.
- Boost Brand Protection: Safeguard the reputation and brand value of legitimate businesses by offering a comprehensive solution to counter the threats posed by counterfeit products, ultimately preserving consumer trust and loyalty.
- Reduce Economic Losses: Mitigate economic losses resulting from counterfeit goods by preventing the circulation of fake products, thereby protecting revenues, taxes, and reducing enforcement costs for both private and public sectors.
- Streamline Authentication Processes: Simplify product authentication processes for supply chain stakeholders, reducing the need for resource-intensive methods such as manual inspections and complex technological solutions.
- Facilitate Collaboration: Foster collaboration among various supply chain parties, such as manufacturers, distributors, and retailers, by providing a decentralized, shared platform for real-time information sharing, enhancing coordination and efficiency.
- Contribute to Industry Best Practices: Promote the adoption of Blockchain-based solutions as a best practice within the supply chain industry for combating counterfeit products, setting a precedent for innovation and security.

LITURATURE SURVEY

Sanidhya Raut; Maruti More, "Fake Product Restriction using BlockChain," [1] 2023 - This paper uses blockchain technology to combat the sale of counterfeit products. In today's global marketplace, fake goods detection is a problem that is becoming more and more significant. The growth of fake products can harm consumers, cause brand reputation damage, and cost real firms money. The usage of blockchain technology is one potential fix for this issue. Blockchain is a distributed ledger technology that makes it possible to trace transactions securely and openly. Blockchain can aid in preventing the creation and sale of counterfeit goods by creating an unchangeable and impenetrable record of the supply chain. Smart contracts can be used in this situation to automate the verification process and make sure that only genuine goods are sold through legitimate channels. This essay will examine the drawbacks and potential advantages of using blockchain technology to identify counterfeit goods.

P.M. Lavanya; N. Ananthi, "Fake Product Detection using Blockchain," [2] 2023 – The availability of fake product in the Market is one of the biggest challenges of the online retail industry. These products appear to be genuine but they are imitations of the original branded products. Almost 20% of the products sold on online websites are fake. In recent times, block chain is receiving more engagement and various applications are being emerged from this technology. In this paper, to ensure that consumers need not depend on the distributers to know whether their products are authentic or not, we are using the decentralized Block chain technology approach. We describe a decentralization Block chain network with anti-counterfeiting items, which allows producers to deliver items without having to run clear outlets, lowering product quality assurance costs dramatically.

P. N. Khairnar ,N. K.Khairnar ,"Implementation of Effective Integrated on-Chip ESD Protection in Nanoscale CMOS Regime for RFIC" [3] 2018- in this work we are primarily focus on ESD effect. ESD is happens at higher frequency frequently. It is a main challenge in RFIC design; the survey shows that in all over the world about 70% IC's were failed due to the ESD event and remaining 30% were because of other factors. We are trying to suggest a methodology to reduce the ESD effect for proper operation of RFIC. The circuitry used for the implementation is on chip integrated technique which differsfrom the conventional technologies. A LVTSCR (Low Voltage Triggered Silicon Controlled Rectifier) is used as protectoral architecture. Here LNA

(Low Noise Amplifier) is used as an exemplary RFIC core circuit. By using LVTSCR we try to protect it from ESD event.In this research paper we have select operating frequency 5 GHz to 6 GHz. The 130 nm CMOS technology is selected for circuit implementation. LVTSCR is providing good solution for on chip protection of ESD for various digital & analog IC's. Simulation tool used for design & simulating the design of core circuit (without protection) & RF+ESD circuit (With protection circuit) is Agilent's Advanced Design System software (ADS). It is very good tool compare to other conventional simulator. After simulation it is observed that there is slightly degrade in gain, noise figure, I/O matching, IIP3 etc. in case of with protection circuit. Keywords - ESD Protection, LVTSCR (Low voltage triggered silicon controlled rectifier), LNA (Low Noise Amplifier), nanoscale etc.

P rathipa S; Harish K, "Counterfeit Product Detection in Supply Chain Management with Blockchain," [4] 2022 - Lately, fake items have taken on an undeniably significant role in the businesses that make different items. This affects the standing of the organization, as well as their deals and benefits. The execution of blockchain innovation takes into consideration the recognizable proof of certified items as well as the recognition of fake products. The blockchain is a sort of dispersed, decentralized, and computerized record that keeps value-based data as blocks in various data sets that are associated with the chains. Blockchain innovation is otherwise called Distributed Ledger Technology (DLT). Because of the way that blockchain innovation is a protected innovation, any block can neither be modified nor be hacked. Clients never again need to depend on the affirmation of item security given by outsider because of the use of Blockchain innovation. Quick Response (QR) codes are an incredible asset that can be used in this undertaking to battle the broad issue of item fraud. These codes exploit ongoing advancements in portable and remote advancements. The utilization of a Quick Response code scanner, in which the Quick Response code of the product is connected to a Blockchain, is the technique by which counterfeit merchandise are recognized and dispensed with. Therefore, this method has the potential to be utilised in order to keep product particulars and the created unique code of that product in the database in the form of blocks. It does a comparison of the code with the entries in the Blockchain database after it has obtained the user's unique code and stored it. The consumer will receive a notification indicating the product is authentic if the code is a match; otherwise, the customer will receive a notification that the product is counterfeit.

Deepashri K M, Sachidanand P B, Latha.H.S, "Industrial Appliances Control Using Android Mobile & Bluetooth Technology",[5] 2017- Android is open source software, manufacturers can modify the operating system for a particular application. This becomes a cheap and feasible alternative for the manufacturer, as hiring a software company to do it. The Android platform supports the Bluetooth network stack, which allows a device to wirelessly exchange data with other Bluetooth devices. The application framework provides access to the Bluetooth functionality through the Android Bluetooth. This paper is mainly focused on the implementation of a prototype system for industrial appliances control like the speed of DC motor, heating coil and light intensity using Android mobile & Bluetooth technology.

SYSTEM ARCHITECTURE

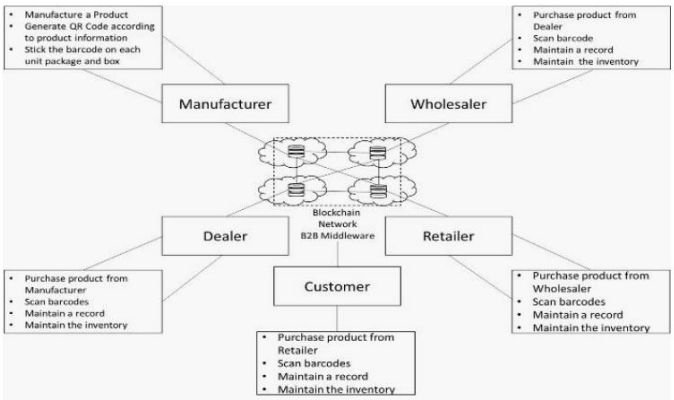

Fig -1: System Architecture Diagram

ADVANTAGES

• Easy to used system
• Control system from anywhere
• Centralized system

SYSTEM REQUIREMENTS

Software Used:

1. Programming Language – Python
2. Libraries – NumPy, TensorFlow, Keras, OpenCV
3. Database – SQLite
4. Tools – Visual Studio Code

Hardware Used:

1. Processor – i3 or above
2. Hard Disk – 150 GB
3. Memory – 4GB RAM

CONCLUSION

In conclusion, the project focused on countering the grave challenges posed by counterfeit products within the supply chain has made substantial strides in enhancing product authentication, supply chain transparency, and consumer safety. The adoption of Blockchain technology as the foundation for this endeavor has proven to be a game-changing solution, offering a transparent and tamper-resistant platform for tracking and verifying product authenticity. Through this innovative approach, the project has not only provided a robust deterrent to counterfeiters but also fortified the defense mechanisms against their illicit activities. The immutability of Blockchain data has ensured that recorded information remains secure, preserving the integrity of the supply chain and protecting it from vulnerabilities and fraud. As a result, the project has not only contributed to the protection of consumer interests but also to the safeguarding of the reputation and brand value of legitimate businesses. It has significantly reduced economic losses stemming from counterfeit goods by preventing the infiltration of fake products into the market.

REFERENCES

1. P. P. Autade, S. M. Turkane and A. A. Deshpande, "Design of Multipliers using Reversible Logic and Toffoli Gates," 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), 2022, pp. 1-4, doi: 10.1109/ESCI53509.2022.9758329.
2. G. Nalinipriya, Srinivas Jangirala, I. Poonguzhali, Prerana Nilesh Khairnar, Priya S & Syed Azahad6,"Role of Machine Learning Algorithms for Supply chain tracking the products to the University Hostel with the utilization of IoT",JOURNAL OF OPTOELECTRONICS LASER,Volume 41 Issue 3, 2022,ISSN:1005-0086.
3. V. Srivastava and A. D. Kalro, "Enhancing the helpfulness of online consumer reviews: The role of latent (content) factors", J. Interact. Marketing, Nov 2020.
4. S.-T. Li, T.-T. Pham and H.-C. Chuang, Do reviewers' words affect predicting their helpfulness ratings? Locating helpful reviewers by linguistics styles, July 2019.
5. 1P. N. Khairnar, 2N. K.Khairnar,(2018)" Implementation Of Effective Integrated On-Chip ESD Protection In Nanoscale CMOSregime For RFIC", Proceedings of WRFER International Conference, 29th April, 2018, Hyderabad, India,pp-5-9.

6. Khairnar Prerana, Pankaj Gopal, Pooja Jadhav,(2018), ELECTRONIC TICKETING MACHINE WITH SMART CARD, International Journal of Computer Engineering and Applications, Volume XII, Special Issue.
7. Prof.Khairnar P.N., Prof.Khairnar N.K.,(2018),"The present operating system and their future with reconfigurable architecture"Proceeding for national conference Advance design and Optimization techniques in Engineering applications,ISBN 978-5291-276-6.
8. Prof .P.N.Khairnar, Kokane Harichandra J., Narkhede Amol A., Narkhede Kunal A,(2017), Industrial Device Control Usingandroid Mobile & Bluetooth technology, Vol-3 Issue-2,PP-2470-2479.
9. RUIGUO YU et al., "Authentication With Block Chain Algorithm and Text Encryption Protocol in Calculation of Social Network", IEEE Access, November 2017.
10. Prof. Autade P. P, Prof.Gaikar M.R2, Prof.Khairnar N.K., (2016)" A Survey on Public Auditing for Shared Data with Efficient User Revocation in the Cloud", International Journal of Innovative Research in Computer and Communication Engineering, VOL-4, ISSUE-2.
11. Prof.S.G. Galande and P.P. Autade,(2015)" An Embedded 1/3 Phase Automatic Transfer Switch With Intelligent Energy Management" International Journal of Computer Engineering and Applications, Volume IX, Issue V,P9-14
12. Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang and Kim-Kwang Raymond Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy", IEEE Cloud Computing, January / February 2011.