International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Utilizing Blockchain for the Detection of Counterfeit Products

**Gitesh Pareek[1], Jatin Tomar[2], Mr. Varun Goel[3]**

[1,2,3]Guru Gobind Singh Indraprastha University, Delhi, India

**Abstract:**
he realm of supply chain management, pervasive challenges such as service Tredundancy, inadequate coordinationamong various departments, and a lack of standardization often stem from a fundamental issue the absence of transparency. The escalating prevalence of product counterfeiting compounds these challenges, with counterfeit items significantly impacting legitimate firms. Unfortunately, the broader populace remains largely unaware of the extensive influence counterfeit products exert on brands. Prior attempts to address this predicament have introduced various methods, including RFID tags, Artificial Intelligence, QR code based systems, among others. However, each method has its drawbacks, such as the susceptibility of QR codes to replication and the computational demands of Artificial Intelligence, particularly in employing Convolutional Neural Networks (CNN).This research proposes a novel approach to tackle the menace of counterfeit products by leveraging Blockchain technology to meticulously track the entire supply chain history. Blockchain, renowned for its decentralized nature, guarantees the identifi- This dilemma places businesses in the difficult posi cation and traceability of authentic products throughout the supply chain. This system allows multiple parties simultaneous access to decentralized information, ensuring heightened transparency and efficiency.

**Keyword:** Blockchain, Counterfeit Product Detection, Web3

## Introduction/Brief Theory Review

The phenomenon of product counterfeiting involves the fraudulent sale of goods, where a product is mis represented as another. This deceptive practice con stitutes consumer fraud, characterized by business practices that inflict financial or other losses upon consumers. According to reports from the Authentication Solution Providers' Association, this illicit activity costs the Indian economy an estimated INR1 trillion annually, with counterfeit incidents on the rise, averaging a 20 perc increase between 2018 and 2020 [1]. Counterfeit products encompass a range of items, including handbags, clothing, cosmetics, and electronics. Beyond its economic implications, counterfeiting can have detrimental effects on consumers, such as skin diseases from poor-quality cosmetics, malfunctions in electronic gadgets due to counterfeit components, and discomfort caused by substandard clothes and shoes. The negative impact extends beyond individual consumers, affecting businesses as well. Counterfeiting tarnishes a company's reputation, as customers may unknowingly purchase knock-offs and subsequently hold the genuine company responsible for any issues encountered. This can lead to customer dissatisfaction, with demands for refunds or replacement products directed at the legitimate company. In dealing with customer complaints about the perceived poor quality of items, companies find themselves in a challenging situation, often unaware that the item in question is a counterfeit. tion

of managing customer relations while grappling with the fallout from counterfeit goods. Successful strategies for mitigating the risks of counterfeiting in global supply chains include enhancing network transparency, implementing cost controls, pre-supply evaluation approaches, and managing relationships with suppliers. Therefore, the primary objective of this paper is to introduce a system designed to combat counterfeiting using Blockchain technology, empowering end-users and suppliers to track the

**Blockchain**

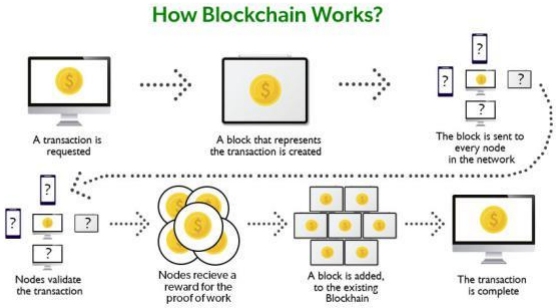



**Figure 1: Working of Blockchain**

product supply chain within a secure environment.

**Why Blockchain**

Blockchain is a distributed ledger comprising inter-connected blocks that store information. Each block is characterized by a timestamp, transaction data, and its unique hash, including the hash of the preceding block. This design makes it inherently resistant to tampering with data. Functioning as a decentralized system, Blockchain ensures that every new block added to the chain represents the singular, universally agreed-upon version accepted by all nodes in the network. The term ”Blockchain” denotes the collaborative upkeep of a technical solution, serving as a secure and continuous record file, functioning as a reliable decentralized database.

**Working of Blockchain**

Upon the initiation of a new transaction, it is broad-casted across a network of peer-to-peer computers distributed globally. This network, comprised of computers commonly referred to as miners, collaboratively engages in solving equations to validate the legitimacy of the transaction. Once confirmed as authentic, these transactions are grouped into blocks. As a reward for their efforts, miners receive proof-of-work awards. Subsequently, these blocks are sequentially linked together, forming an immutable and continuous record of all transactions. This entire process is visually represented in the accompanying figure 1.

**Importance of Blockchain**

Blockchain significantly enhances trust by eliminat-ing the need for reliance on third parties. The implementation of smart contracts, essentially programs embedded in the blockchain, ensures execution only when specific conditions are met. The inherent se-curity of the blockchain is derived from each block storing data along with the hash of the previous block, making it highly resistant to tampering or the introduction of false information. Any attempt to alter a block’s information results in a change in its hash, but the subsequent blocks maintain their in-tegrity. Modifying the entire chain would necessitate

the consensus of more than half of the participants, a highly improbable scenario due to the substantial resources and financial investment required.

The robust security architecture of blockchain fur-ther contributes to its importance. Each block within the chain encapsulates a timestamp, transaction data, and its own hash, along with the hash of the preced-ing block. This interconnected structure creates a virtually tamper-proof system. Attempting to alter the information in a block would not only change its hash but also disrupt the integrity of all subsequent blocks. The decentralized and distributed nature of blockchain ensures that this tamper-resistant charac-teristic is maintained across all nodes in the network.

In essence, blockchain technology establishes a foundation of trust, transparency, and security in digital interactions. Its decentralized nature, cou-pled with cryptographic principles and consensus mechanisms, ensures that the integrity of the data remains intact, making it a cornerstone for building reliable and secure digital systems.

**Experimental Analysis**

The literature survey aimed to comprehend the ori-gins of counterfeits and their societal impact. Several systems for detecting fake products were explored, encompassing Artificial Intelligence, QR codes, Ma-chine Learning, and Blockchain. Shaik proposed a method involving public and private keys as QR codes, where the scanning app decrypts the QR code using cryptographic functionality, and the manu-facturer's server matches buyer details with item codes [9]. Benatia and Baudry et al. introduced a traceability-CPS-based architecture for supply chain management, emphasizing layers interacting to form a traceability-CPS. The architecture enables supply chain monitoring, data analytics, and the detection of abnormal product behavior [10]. Khalil and Doss et al. suggested using an RFID-based system to combat counterfeiting, allowing consumers to query in-store tags to verify product legitimacy. This lightweight scheme is suitable for large-scale implementation in retail environments [11]. Habib and Sardar et al. addressed supply chain management (SCM) challenges by proposing the integration of blockchain technology. They suggested structuring new models to focus on transaction processes at a planning level [12]. Daoud and Vu et al. focused on an AI application archi-tecture, including a dataset, detection models, and trained models, utilizing machine learning to detect fake products. Faster R-CNN achieved high accu-racy and low training speed [13]. Chen and Shi et al. explained the SCQI framework for blockchain-based quality management in supply chains, incorporating RFID technology and smart contracts to enhance supply chain efficiency [14].

Toyoda, Kentaroh, and Mathiopoulos, P. Takis et al. proposed a QR code-based system for detecting fake products, allowing end-users to access prod-uct details and transaction history through QR code scanning [15]. In a blockchain-based system, informa-tion is stored on each node, enhancing transparency and cost efficiency. Ethereum serves as the backend blockchain operating system [7]. A blockchain-based system for information sharing was proposed, em-phasizing data control by the owner and reducing third-party interference. The blockchain block con-tains sender, amount, receiver, transaction id, prod-uct id, and metadata [16]. Ethereum, an open-source blockchain, was discussed as a technology support-ing digital money, global payments, and applications [17].

Abhijeet and Andrew et al. [18] presented findings on counterfeiting in global supply chains, revealing its widespread increase in areas such as low-cost spare parts and the drug market. Counterfeit products were challenging to identify due to the availability of forged certificates. Limitations in existing systems were noted, including the potential copying of QR codes, the susceptibility of RFID tags to cloning, and

challenges in AI and machine learning applications. The lack of power for customers, suppliers, and retail-ers to check product integrity was also highlighted.

**Proposed System**

Counterfeiting has become a global issue, exerting significant repercussions on organizations, manufac-turers, and consumers, with profound implications for their influence and well-being. India is no exception to this pervasive problem. The proposed system specifically addresses consumer products, offering a solution to enhance product and supply chain in-tegrity through the implementation of Blockchain technology. This system empowers customers to Researh Paper trace the complete history of a product, from its origin with the manufacturer to its ultimate destina-tion with the customer, utilizing a combination of Blockchain and QR code technologies.

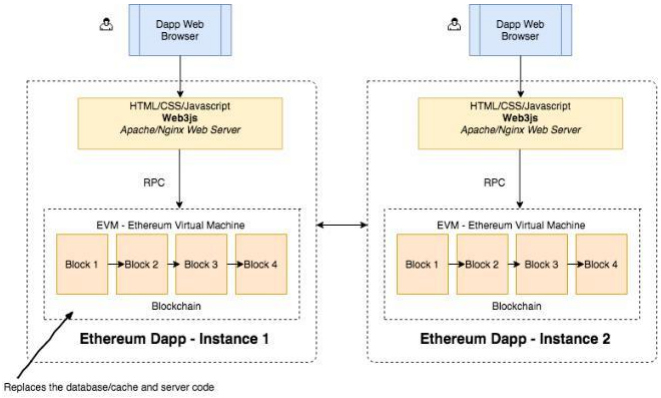


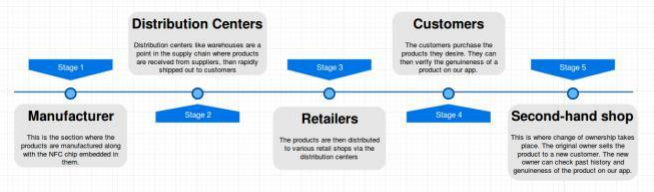

**Figure 2: System Architecture**

**System Architecture**

The proposed system adopts a decentralized applica-tion (Dapp) framework, leveraging the Ethereum Net-work as the primary blockchain to maintain records and facilitate transactions related to products from the featured companies on the Dapp. The fundamen-tal system architecture is depicted in Figure 2.

**Data Flow**

The primary objective of the proposed system is to ensure the authenticity of products by enabling customers to trace the complete supply chain history of a given product. The system empowers customers to independently track the entire product journey from the manufacturer to the end-user using blockchain technology. This anti-counterfeiting system, based on Blockchain, involves three key roles: the Manufac-turer, the Seller, and the Consumer, as elaborated and illustrated in Figure 3.




**Manufacturer**

The manufacturer initiates the process by logging into the manufacturer account. Subsequently, the manufacturer generates a QR Code for the product and includes other essential product details. Utiliz-

ing their Ethereum wallet, the manufacturer adds a block to the Ethereum blockchain. The system ensures a secure connection between the manufacturer's local database userid and their wallet address. This stringent mapping condition mandates that a block will only be added to the digital ledger if the man-ufacturer logs in from their authenticated account and uses their designated .

**Supplier**

The supplier engages with the system by logging into their designated supplier account and scanning the QR code on the product. This action grants the supplier access to information provided by the manufacturer for the respective product. The supplier then appends additional details to the product, such as the shop destination, and subsequently uploads this information to the Blockchain. These enriched details are made available for viewing by the buyer.

**Customer**

Customers play a pivotal role in verifying the in-tegrity of the product. By scanning the QR code, customers gain access to the entire history of trans-actions associated with the product, facilitating the verification of its authenticity. During the customer's purchase of the product, a QR scan of the supply chain history reveals a crucial insight: if the last loca-tion in the history does not align with the purchase location, it signals a potential issue. This discrep-ancy indicates that the product may not be genuine, suggesting that the QR code has been copied, and the customer is alerted to the possibility of counterfeiting.

**Result and Discussion**

The proposed system enables both manufacturers and suppliers to interact with the system, facilitating the addition of their respective blocks containing transaction details to the blockchain without altering others' blocks. Smart contracts for the manufacturer and supplier blocks are implemented using Solidity. For local testing, Ganache is employed as the local blockchain. Web3.js is utilized for actions such as sending Ether, confirming transactions, and read-ing/writing data from smart contracts. Metamask, a browser wallet, is installed to facilitate Ethereum blockchain interaction within the browser. Accounts from Ganache are imported into Metamask. Man-ufacturers and suppliers confirm transactions using their accounts through the Metamask wallet, con-nected via Web3.js.

End-users can verify the supply chain by scan-ning the QR code, ensuring the product's integrity through this blockchain-based system.

**Conclusion**

The decentralized nature of Blockchain in the pro-posed system ensures that local suppliers are unable to manipulate the verification or counterfeiting pro-cesses for products. Manufacturers and suppliers can utilize the system to securely store product details in Blockchain, offering properties such as tamper resistance, data consistency, and confidentiality. These attributes ensure the security and privacy of data on the network.

Customers, through the proposed system, gain visibility into the product's supply chain history, allowing them to verify the product's authenticity. This empowers customers with confidence in the integrity of the goods they purchase. The system has the potential to significantly reduce counterfeiting

rates for branded goods, providing companies with a streamlined approach to instill consumer confidence and prevent the inadvertent purchase of counterfeit items.

Beyond its immediate application, the proposed system lays the foundation for building trust and fostering strong relationships between manufactur-ers and customers. This, in turn, contributes to economic growth and plays a role in reducing cor-ruption. Looking ahead, the system's scope can be expanded to address fraud in various sectors such as banking, healthcare, voting systems, online shopping, and more.

**Literature Review**

network, configured with the host "127.0.0.1" and Counterfeiting poses a pervasive threat in global sup-port 7545 in the truffle-config.js file. Contracts areply chains, necessitating a nuanced understanding of compiled and deployed using Truffle, with migration its sources and societal impact. This research paper files aiding in the deployment process.explores cutting-edge solutions rooted in Artificial The system's interface is built using React, and the Intelligence (AI), QR codes, Machine Learning (ML), Web3.js library allows interaction with the Ethereum and Blockchain technologies. The study synthesizes insights from various works to propose innovative approaches aimed at overcoming the limitations in-herent in existing systems.

In the realm of AI and QR code-based solutions, Shaik advocates for the integration of public and private keys within QR codes, enhancing security through cryptographic functionality in scanning ap-plications. Daoud and Vu contribute by focusing on the architecture of AI applications, utilizing ma-chine learning for anti-counterfeiting through logo detection and model training. The emphasis is on achieving high accuracy and efficiency, particularly demonstrated through the application of Faster R-CNN.

The exploration of Blockchain technology unveils a decentralized system where data is stored on each node, fostering information exchange and trans-parency. Ethereum emerges as a key player, provid-ing an open-source blockchain operating system that facilitates cost-efficient information sharing. Smart contracts within this framework are leveraged for quality control in supply chain management, ensur-ing the integrity of transactions and product infor-mation.

Khalil and Doss present an alternative solution with RFID-based systems, allowing consumers to validate product legitimacy in-store. Despite the suitability for large-scale retail implementation, chal-lenges related to RFID tag cloning are acknowledged, signaling the need for continuous improvement in this approach.

Chen and Shi introduce a theoretical framework for intelligent quality management based on blockchain technology, integrating RFID technology and smart contracts to enhance supply chain quality and effi-ciency. This framework records quality and transac-tion information, providing a structured approach to combating counterfeiting.

The research recognizes the limitations within ex-isting systems. QR codes, while widely adopted, are susceptible to copying, undermining their effec-tiveness. Low-cost RFID tags, while advantageous for auto-identification, are prone to cloning, raising concerns about their reliability. In AI and ML ap-plications, the resource-intensive nature of Convolu-tional Neural Networks (CNNs) is noted, along with challenges in detecting tag reapplication attacks.

In conclusion, this paper contributes to the on-going discourse on anti-counterfeiting measures by delving into advanced technological solutions. By bridging the gap between theory and practical imple-

mentation, these innovations offer promising avenues for strengthening the integrity of global supply chains and safeguarding consumers, suppliers, and retailers against the pervasive threat of counterfeit products.

**References**

1. ASPA, The state of counterfeiting in India 2021, 2021.
2. Y. Lu, Journal of Management Analytics, 5(1), 2018.
3. F. Casino, T.K. Dasaklis, C. Patsakis, Telemat-ics Informatics, 36, 55, 2019.
4. M. Peck, IEEE Spectrum, 54, 26, 2017.
5. S. Idrees, M. Nowostawski, R. Jameel, A. Mourya, Electronics, 10, 951, 2021.
6. Zignuts Technolab, How blockchain architecture works? Basic understanding of blockchain and its architecture, 2022.
7. J. Ma, S.Y. Lin, X. Chen, H.M. Sun, Y.C. Chen, H. Wang, IEEE Access, 8, 77642, 2020.
8. M.J.L.I.N.M. J.M. Bohli, N. Gruschka, IEEE, 10, 9, 2013.
9. C. Shaik, Computer Science & Engineering: An International Journal (CSEIJ), 11, 2021.
10. M.A. Benatia, D. Baudry, A. Louis, Journal of Ambient Intelligence and Humanized Computing, pp. 1–10, 2020.
11. 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 trans-action process, 2021.
13. E. Daoud, D. Vu, H. Nguyen, M. Gaedke, Im-proving Fake Product Detection Using AI-Based Technology, in 18th International Conference e-Society, 2020.
14. S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, A Blockchain-Based Supply Chain Quality Management Framework, in 2017 IEEE 14th Inter-national Conference on e-Business Engineering (ICEBE), pp. 172–176, IEEE, 2017.
15. K. Toyoda, P.T. Mathiopoulos, I. Sasase, T. Ohtsuki, IEEE Access, 5, 17465, 2017.
16. M. Nakasumi, Information Sharing for Supply Chain Management Based on Blockchain Technology, in 2017 IEEE 19th Conference on Busi-ness Informatics (CBI), Vol. 1, pp. 140–149, IEEE, 2017.
17. G. Wood et al., Ethereum Project Yellow Paper, 151, 1, 2014.
18. Ghadge, A. Duck, M. Er, N. Caldwell, Supply Chain Forum: An International Journal, 22, 87, 2021.
19. Singhal, International Journal for Research in Applied Science and Engineering Technology, 9, 291, 2021.
20. Ethereum, https://www.zastrin.com/courses/ethereum-primer/lessons/1-5, 9, 291, 2021.