IJDI-ERET

INTERNATIONAL JOURNAL OF DARSHAN INSTITUTE ON
ENGINEERING RESEARCH AND EMERGING TECHNOLOGIES
Vol. 13, No. 1, 2024
www.ijdieret.in

DOI 10.32692/IJDI-ERET/13.1.2024.2405

(Research Article)

Cosmetic Product Provenance Identification Technique Utilizing Blockchain Technology

Pragati Nehete[1*], Radhika Gaikwad[2], Rachana Y. Patil[3]

[1,2,3]Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Nigdi, Pune, Maharashtra, INDIA*

Abstract

The proliferation of counterfeit goods poses a grave threat to both industrial sectors and consumers, with increasing incidents negatively impacting sales, profits, and brand credibility. Counterfeiting not only hampers a company's revenue streams but also erodes consumer trust in the open market. The lack of transparency in manufacturing and distribution processes exposes consumers to manipulated or falsified information, further undermining trust in product authenticity. To address this pressing issue, we present a blockchain-based anti-counterfeiting system designed for comprehensive product traceability across the supply chain. Leveraging public or permissionless blockchain technology, our proposed system records supply chain data in immutable, transparent, secure, tamper-proof, and trusted blocks. A QR code integration enhances the system's security and usability, allowing consumers to easily verify product authenticity. This innovative solution aims to restore consumer confidence, mitigate the adverse effects of counterfeiting on businesses, and fortify supply chain security. The paper delves into the technical intricacies of the proposed method, highlighting the transformative potential of blockchain technology in safeguarding product traceability and ensuring authenticity throughout the supply chain.

Keywords: Fake product, QR code, Blockchain, Supply Chain

1. Introduction

Product counterfeiting is a common type of consumer fraud that poses a substantial danger to businesses all over the world. This illegal practice involves the selling of counterfeit products that are falsely portrayed as real, and it affects a wide range of industries, including clothing, fast-moving consumer goods (FMCG), and the automotive industry. Furthermore, it expands into medicines, durables, and agrochemicals, hurting the innovation and profitability of other businesses [1]. The selling of counterfeit goods not only undermines customer trust but also impedes real trade, deterring inventors and legitimate producers. To combat this expanding threat, we introduce a revolutionary anti-counterfeiting system that tracks items along the supply chain, allowing customers to verify the legitimacy of their purchases. Our solution makes use of blockchain technology, a decentralized and distributed network recognized for its reliability and transparency [2]. When data is stored on the blockchain, it becomes immutable, and each product is assigned a unique identity throughout the supply chain. It also has a strong method for validating and evaluating product validity [3].

Corresponding Author: e-mail: pragati.nehete20@pccoepune.org, Tel-+91-8530893869

ISSN 2320-7590 (Print) 2583-3863 (Online)

By affixing a QR code to each product, customers can effortlessly verify its authenticity by scanning this code. This innovation offers a proactive and efficient solution to the pervasive issue of product counterfeiting, offering transparency, traceability, and peace of mind to both consumers and businesses [4-6]. In the following sections, we will delve into the technical aspects of our proposed anti-counterfeiting system, showcasing how blockchain technology transforms the landscape of product verification and supply chain security [7].

2. Blockchain Overview

The proposed solution leverages a blockchain platform combined with decentralized blockchain technology to identify products and prevent counterfeiting. This approach focuses on four primary aspects: authenticating products, preventing counterfeits, ensuring traceability, and analyzing data. [8,9] By generating a digital identity for each product on the blockchain network, it may be granted a unique identification. This distinct identification may be connected to product details, making it very straightforward to trace the product's origins. This allows for real-time visibility into the movement of products. [10]. Blockchain technology can integrate various authentication processes into a product's blockchain record. These processes may include digital signatures, unique identifiers like QR codes and barcodes, and even integration with IoT devices. [11,12].

It encourages collaboration and confidence among individuals participating in anti-counterfeiting efforts. Using a shared blockchain network allows all parties to communicate data in real time. This cooperative and collaborative strategy allows for speedier detection and reaction to counterfeit incidents, resulting in more effective enforcement measures. [13] Intellectual property rights may be maintained by keeping track of copyrights, ownership, and trademarks on the blockchain. This creates a verifiable and tamper-proof record of ownership, preventing the unauthorized use of intellectual property and the production of counterfeit goods. [14,15]

As a result, blockchain may be the best choice for an anti-counterfeiting system.

3. Literature Review

Blockchain-based categorization is a novel way of detecting phony products that makes use of blockchain technology. Blockchain is a distributed ledger system that allows data to be stored in a secure, transparent, and impermeable manner. Blockchain is used to trace the source of items along the supply chain in the context of fraudulent product identification. [16] Text or image analysis is widely used in traditional false product identification techniques to detect bogus items. Image recognition algorithms are trained using a dataset of both genuine and counterfeit items. When a new image is analyzed, the model determines its authenticity by comparing it to the training dataset. Similarly, text analysis models are trained on a dataset containing descriptions of real and fake products [17]. The model evaluates the authenticity of a new text description based on its similarity to those in the training dataset.

When compared to traditional phony product identification methods, blockchain-based categorization has several advantages. First, blockchain-based categorization is more secure. Because blockchain is a tamper-proof system, no modifications to the data stored there can be made. As a result, it is more difficult for counterfeiters to create phony items with a valid provenance. Second, BC-based categorization is more scalable. Using blockchain technology, the origin of millions, if not billions, of items may be traced. As a result, it may be employed in large supply chains. Third, blockchain-based categorization is more accurate. Because it is based on data, blockchain-based categorization is less susceptible to deception. [18]

There are also multiple barriers to blockchain-based product authentication that must be considered. Scalability concerns arise when the blockchain grows in size, leading to longer processing times and higher transaction costs. High implementation costs may deter adoption even more. Interoperability across different blockchain networks is challenging due to different protocols and standards. Security issues raise risks because hackers can edit or remove data on the blockchain. [19] Complexity, which necessitates specialized knowledge and skills, is another hurdle to adoption. Despite these disadvantages, research is being conducted to solve them and increase the effectiveness of blockchain in preventing counterfeiting.

Table 1. Comparative analysis

Reference	Methodology	Advantages	Disadvantages
Product tracking and fake product identification using blockchain [16]	1) Compliance 2) Blockchain 3) QR codes 4) Smart contracts 5) RFID tags	1) Security 2) Transparency 3) Immutability 4) Scalability 5) Cost-effective	1) Complexity 2) Cost 3) Energy use 4) Security 5) Regulation
Developing an anti-counterfeit system using blockchain technology [18]	1) Ethereum blockchain 2) Solidity contracts 3) User interface for all parties	1) Traceability 2) Transparency 3) Benefits in various sectors 4) Secure	1) Security risks like hacking and data breaches
Blockchain-based anti-counterfeiting management system for traceable luxury products [19]	1) ECDSA 2) Smart contracts 3) Hyperledger Fabric	1) Traceable records 2) Eliminates third party 3) IoT integration for querying	1) High resources and expertise required 2) Adoption challenges for consumers and stakeholders

4. Methodology

The design and development for the blockchain-based system, creating smart contracts for product verification. Data on product provenance is recorded in the blockchain ledger. We also implement a secure QR code system for user interaction. Testing and validation are performed using a simulated environment like Ganache before deploying the smart contracts on the Ethereum blockchain. We assess the system's performance, security, and scalability. The methodology ensures a robust, transparent, and tamper-proof solution for anti-counterfeiting and product tracking.

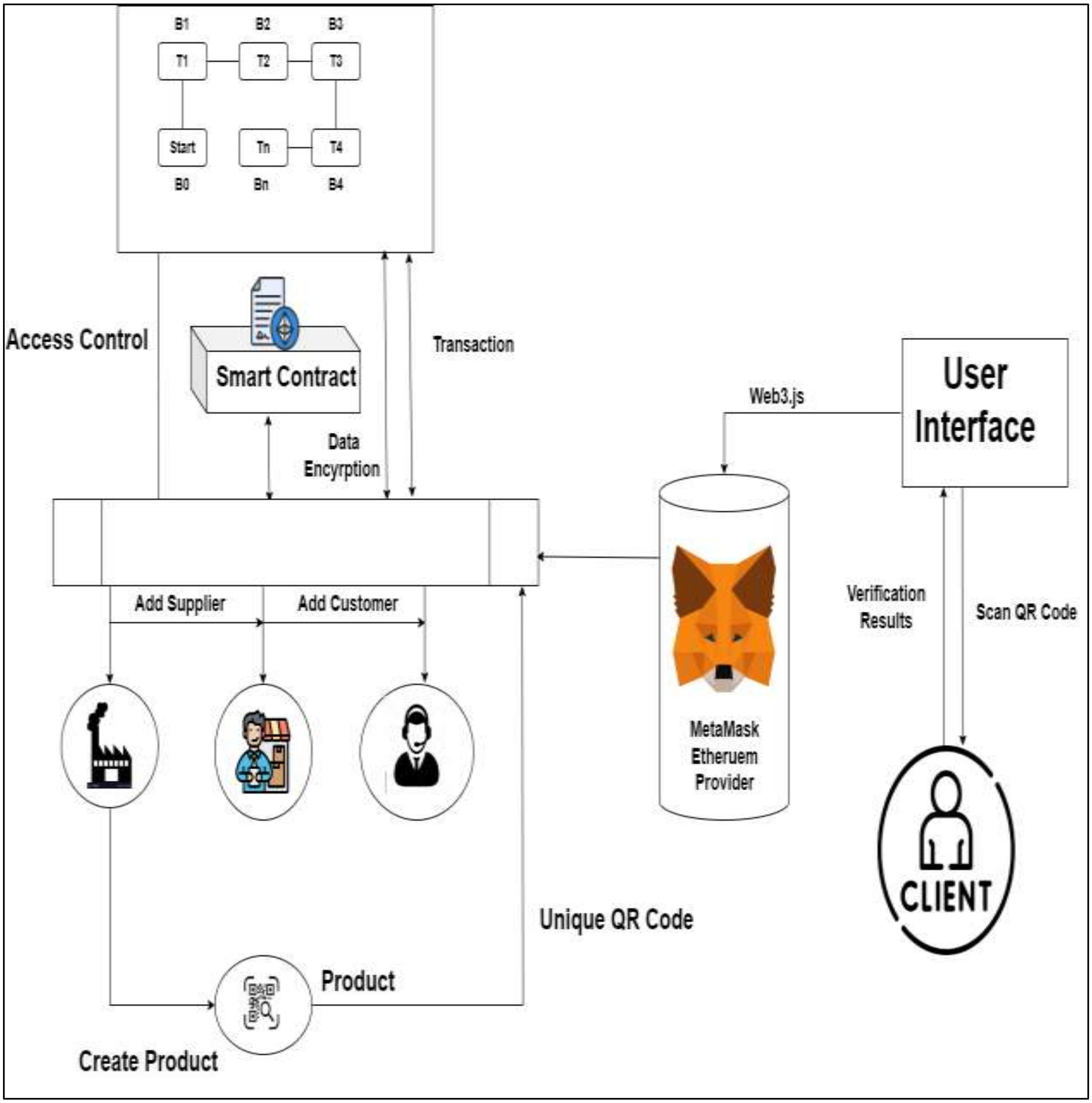


Figure 1. Blockchain-based method for ensuring product authenticity

The proposed blockchain-based technique for recognizing counterfeit products comprises a cohesive ecosystem involving key components that collaborate to ensure the authenticity of products. This ecosystem encompasses the product manufacturer, the blockchain network, network nodes, smart contracts, retailers, and end consumers [20,21].

4.1 Ledger for supply chain transparency: The foundation of our methodology lies in a meticulously designed ledger system that enables real-time product tracking across the supply chain. This transparency is pivotal for detecting and preventing the proliferation of counterfeit goods.

4.1.1 Product information: The ledgers are designed to include detailed product information, such as the product's name, serial number, batch number, manufacturing date, expiration date, and other pertinent details. This information serves as a digital fingerprint for each product and forms the basis for verification.

4.1.2 Product movement tracking: The ledger records the movement of products, detailing their origin, destination, and any intermediate stops along the supply chain. This meticulous tracking ensures that the product's journey is transparent and easily auditable.

4.1.3 Unique identifiers: Manufacturers assign unique identifiers to their products, enhancing traceability throughout the supply chain. These identifiers become the cornerstone of product verification [22].

4.2 Blockchain network and nodes: The blockchain network serves as the decentralized ledger where product data is stored, ensuring its security and immutability. Network nodes, which are individual computers or devices participating in the blockchain network, play a crucial role in verifying and validating transactions.

4.2.1 QR code generation: At the time of manufacturing, a unique QR code is generated based on the product's specific identification code. This QR code encapsulates essential product details, such as the unique identifier, pricing information, manufacturer details, and transaction history [23]. This data is securely stored within the blockchain network.

4.2.2 Smart contract verification: Smart contracts are deployed to verify a product's unique identification code and transaction history, thus confirming its authenticity. Retailers perform this verification by scanning the product's unique identification code, cross-referencing its transaction history stored on the blockchain, or consulting the ledger records [24].

4.2.3 Retailer responsibility: Retailers bear the responsibility of confirming the legitimacy of products before offering them to consumers. This verification process is integral to maintaining trust and safeguarding consumers against counterfeit goods [25].

4.2.4 Customer validation: End consumers play a crucial role in the final validation of product authenticity. They can perform this validation by scanning the product's distinctive identification code and reviewing its transaction history on the blockchain, ensuring their confidence in the products they purchase.

This comprehensive blockchain-based method creates a secure, transparent, and efficient system for product authentication, spanning the entire supply chain. It not only bolsters consumer trust but also provides a robust defense against counterfeit products, fostering a safer and more reliable marketplace.

Table 2. Categories of transactions and events

Type	Name of component	How it works
Transaction	New product is added	Add a new product with data such as the manufacturer ID, product SN, product price, product name, and product brand.
	Add new retailer	Add new vendor information, such as retailer name, retailer code, retailer manager, manufacturer ID, retailer brand, retailer phone number, and retailer address.
	Sell product to retailer	Scan a QR code picture file and input the retailer's code.
	Sell product to consumer	Scan an image file of QR code, enter consumer code.
	Verify products	Scan an image file of QR code, enter consumer code.
Event	Share product verification result	Share the verification result, whether the product is legitimate or not.

5. SCM Integrating with Blockchain Technology

This study looks into the use of blockchain technology into cosmetic supply chain management, with an emphasis on building a reliable provenance identification approach. Smart contracts use blockchain's decentralised and tamper-resistant ledger to automate and enforce agreements across supply chain participants, assuring adherence to quality standards and ethical practices. During the production process, each cosmetic product is issued a digital identity, producing a unique and verifiable record on the blockchain. This technique improves transparency by giving stakeholders real-time access to unchangeable information, reducing fraud and unauthorized changes in the supply chain. Blockchain simplifies supplier verification by giving a full record of raw material source and processing, promoting compliance with industry norms [26].

By providing real-time visibility into product movement, the system enables rapid issue detection and resolution. Consumers receive access to precise information on the cosmetic items they buy, which contributes to greater industry trust.

This integration adheres to principles by resolving data security issues with blockchain's cryptographic capabilities, increasing supply chain transparency, and assuring compliance with industry laws. The implied apparatus improves the area by developing a secure and efficient mechanism for cosmetic product provenance identification, which contributes to the overall integrity and reliability of cosmetic supply chain management

5.1 Ensuring the authenticity of the products: Counterfeiting presents substantial issues for both organizations and consumers. Counterfeit items, which are characterized by possible danger and inferior quality, can harm the reputation of genuine brands. The implications include financial losses for both businesses and people [27].

Several methods can be used to ensure the authenticity of a product. Security elements such as holograms, watermarks, microprinting, and UV printing are common. Serialization and traceability, which involve unique serial numbers and supply chain tracking, make counterfeit products more difficult to enter the market. Furthermore, digital technology like QR codes and RFID tags is critical to ensuring product authenticity at the point of sale.

It is critical to work with law enforcement and industry partners. Businesses can share information and work together to combat counterfeiting. Consumers, too, play an important role by being cautious [28]. They are encouraged to buy only from reliable shops, inspect items for signs of counterfeiting, and confirm their legality by contacting the manufacturer if they have any doubts.

5.2 Mapping smart contracts with blockchain: This groundbreaking research pioneers the synergistic use of smart contracts with blockchain technology, resulting in a cutting-edge framework for enhancing cosmetic product provenance verification. Smart contracts, like digital maestros, are delicately weaved into the architecture of the decentralized blockchain. Their stance is nothing short of revolutionary, orchestrating a symphonic convergence of automated governance across the cosmetic supply chain, from ingredient sourcing to manufacturing subtleties to distribution complexities. Smart contracts emerge as virtuoso performers in the realm of cosmetic product provenance, encoding and executing agreements with immutable correctness that safeguard the integrity of the supply chain.

These digital agreements, imbued with established rules on product information, origin characteristics, and high certification criteria, go beyond mere automation to represent a safe and tamper-resistant data choreography along the product's path. This study not only demonstrates the skill of combining smart contracts and blockchain, but it also reveals a fresh story in cosmetic supply chain management. The combination of automatic contractual duties not only streamlines processes but also transforms the blockchain into an impenetrable repository of data, encouraging resilience and transparency. This orchestral synthesis, a hymn to innovation, promises a climax in traceability and trustworthiness, ushering in a new era in cosmetic product provenance identification.

5.3 Backend technologies: In the development of our smart contract-based product identification system, we employed a combination of technologies to ensure security, transparency, and robustness. The backbone of our system is the Solidity programming language, utilized for crafting smart contracts on the Ethereum blockchain. These smart contracts are at the heart of our product verification mechanism.

5.3.1 Solidity: Solidity serves as the primary programming language for creating smart contracts on the Ethereum blockchain. These contracts define the rules and logic governing the product identification and verification process.

5.4 Front-end development and user interaction: The front-end of our system is a user-friendly web application that facilitates interaction with the Ethereum blockchain and allows users to input data for product verification. Several technologies were employed to develop this interface.

5.4.1 JavaScript: JavaScript was used for the front-end development, enabling the web application to interact with the blockchain. Users can input data and receive real-time results regarding product authenticity.

5.4.2 HTML and CSS: These technologies were employed for the design and layout of the web application's user interface, ensuring an intuitive and visually appealing experience.

5.4.3 Web3.js: This JavaScript library provides a crucial interface for seamless interaction with the Ethereum blockchain. It enables the web application to communicate with smart contracts and retrieve data.

5.4.4 Node.js: Node.js, as an open-source, cross-platform JavaScript runtime environment, supports the development of scalable and high-performance server-side applications, contributing to the overall robustness of the system.

5.5 Development environment and tools:

5.5.1 Ethereum blockchain: We leveraged the Ethereum blockchain to securely store transaction and product data. Its transparent ledger ensures the integrity of our product identification system [21].

5.5.2 MetaMask: To facilitate user interaction with the Ethereum blockchain and manage user accounts, we integrated MetaMask, a browser extension. Users can securely store, manage, and transfer Ethereum and other ERC-20 tokens, ensuring safe access to the Ethereum network.

5.5.3 Ganache: For smart contract testing and debugging, we utilized Ganache, a local blockchain development environment [22]. It allows developers to test their smart contracts in a simulated environment before deploying them to the Ethereum blockchain, ensuring a reliable and bug-free system.

5.5.4 Truffle suite: The Truffle suite was utilized to streamline the development, testing, and deployment of smart contracts on the Ethereum blockchain. This framework offers essential tools for creating, testing, and deploying smart contracts, thereby simplifying the development of Ethereum-based applications.

The combination of these technologies and tools ensures a secure, user-friendly, and efficient product identification system, empowering users to verify product authenticity through interaction with smart contracts deployed on the Ethereum blockchain.

5.6 Smart contract: The proposed system employs various smart contract functions to handle product and seller information on the blockchain:

5.6.1 Adding a new produc: The addProduct function registers a new product on the blockchain, storing its details in the productItems mapping. This includes the product's name, serial number, brand, price, and availability.

5.6.2 Adding a new seller: The add seller function adds a new seller to the blockchain, recording their information in the seller mapping. Additionally, the seller code is linked to the corresponding manufacturer ID in the sellers with manufacturer mapping.

5.6.3 Manufacturer sells product: The manufacturer sell product function allows a manufacturer to sell a product to a designated seller. It logs the product's serial number in the seller's inventory and updates the product's current owner to the seller code.

5.6.4 Seller sells product: The seller Sell Product function enables sellers to sell a product to a consumer. It tracks the product's serial number in the seller's list of sold products.

6. Failure Scenarios

The integration of blockchain technology in product provenance systems offers a promising avenue for enhanced transparency and security. However, it comes with a set of critical challenges that must be carefully addressed.

Counterfeit blockchain records pose a substantial risk, as malicious actors may attempt to insert false information, compromising the accuracy of provenance data. Privacy concerns arise when sensitive customer data is linked to product provenance on a public blockchain, potentially exposing confidential information.

Vulnerabilities in smart contracts, often pivotal in blockchain systems, can be exploited to manipulate provenance data, highlighting the need for rigorous security measures. Scalability issues emerge as data accumulates in the blockchain, potentially slowing transaction speeds, which can impact real-time product tracking.

Interoperability challenges arise when various stakeholders use different blockchain platforms or standards, leading to fragmented tracking systems. Convincing all supply chain parties to adopt blockchain technology can be a daunting task, and resistance can hinder its effectiveness.

The accuracy of blockchain data relies on external sources and oracles, making them vulnerable points. Regulatory changes can necessitate costly updates, and technical issues like network outages or infrastructure failures can disrupt real-time tracking. Finally, the loss of private keys poses a significant risk, potentially causing gaps in product tracking.

These challenges underscore the need for meticulous planning, security protocols, and industry-wide standards in implementing blockchain-based product provenance systems in the cosmetic industry.

7. Results

Table 3. Transaction and execution costs per function

Function	Transaction cost	Execution cost
addSeller	401,586	323,162
viewSellers	646,893	550,581
addProduct	398,742	320,762
viewProductItems	510,143	510,143
sellerSellProduct	404,334	326,362

The costs related to executing each function or the entire program on the blockchain are summarized in Table 2. The transaction cost indicates the gas consumed by the blockchain network to perform each function. Meanwhile, the execution cost signifies the computational resources used during the execution of these functions. The total transaction cost for the program amounts to 2,000,809 units, while the execution cost totals 1,808,105 units. The visual representation of transaction and execution cost is shown in figure 2.

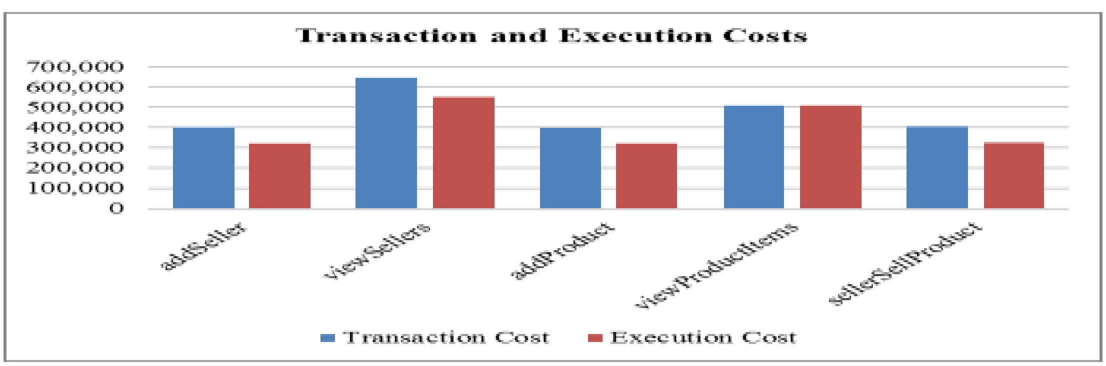


Figure 2. Visual representation of transaction and execution cost

8. Conclusion

The enactment of a counterfeit product detection system is vital for enhancing consumer safety and preserving corporate integrity in today's global economy. Incorporating technologies like blockchain and QR codes improves the system's precision and efficiency, erecting substantial barriers against counterfeiters. This not only protects consumers from deceptive products but also empowers enterprises with heightened supply chain awareness, enabling proactive issue identification and resolution. By integrating advanced authentication methods and leveraging blockchain's transparency, this approach signifies a significant stride in ensuring product authenticity and consumer trust, highlighting the ongoing need for innovative solutions in combating counterfeit items.

References

[1] C.-L. Chen *et al.*, "Blockchain-Based Anti-Counterfeiting Management System for Traceable Luxury Products," *Sustainability*, vol. 14, no. 19, p. 12814, Oct. 2022, doi: 10.3390/su141912814.

[2] A. A. Monrat, O. Schelen, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[3] E. I. Vazquez Melendez, P. Bergey, and B. Smith, "Blockchain technology for supply chain provenance: increasing supply chain efficiency and consumer trust," *Supply Chain Management: An International Journal*, vol. 29, no. 4, pp. 706–730, Jun. 2024, doi: 10.1108/SCM-08-2023-0383.

[4] H. Liu, "Enhancing Data Integrity and Confidentiality in Construction Cost Management Using Blockchain and Proxy Re-Encryption Techniques," in *IoT, Blockchain, and Smart Environments*, Design Computation, Nov. 2023. doi: 10.47330/CBC.2023.IAEJ8806.

[5] Srikrishna Shastri C, Vishal K, Sushmitha S, Lahari, and A. R. Shetty, "Fake Product Detection Using Blockchain Technology," *IJARCCE-International Journal of Advanced Research in Computer and Communication Engineering*, vol. 11, no. 5, pp. 420–427, May 2022, doi: 10.17148/IJARCCE.2022.11578.

[6] H. Chougule, S. Dhadiwal, M. Lokhande, R. Naikade, and R. Patil, "Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption and Blockchain," *Procedia Computer Science*, vol. 215, pp. 71–77, 2022, doi: 10.1016/j.procs.2022.12.008.

[7] G. Narayanan, I. Cvitić, D. Peraković, and S. P. Raja, "Role of Blockchain Technology in Supplychain Management," *IEEE Access*, vol. 12, pp. 19021–19034, 2024, doi: 10.1109/ACCESS.2024.3361310.

[8] C. L. Tan, Z. Tei, S. F. Yeo, K.-H. Lai, A. Kumar, and L. Chung, "Nexus among blockchain visibility, supply chain integration and supply chain performance in the digital transformation era," *Industrial Management & Data Systems*, vol. 123, no. 1, pp. 229–252, Feb. 2023, doi: 10.1108/IMDS-12-2021-0784.

[9] D. Nouichi, M. Abdelsalam, Q. Nasir, and S. Abbas, "IoT Devices Security Using RF Fingerprinting," in *2019 Advances in Science and Engineering Technology International Conferences (ASET)*, Dubai, United Arab Emirates: IEEE, Mar. 2019, pp. 1–7. doi: 10.1109/ICASET.2019.8714205.

[10] Y. Xiao, B. Xu, W. Jiang, and Y. Wu, "The HealthChain Blockchain for Electronic Health Records: Development Study," *Journal of Medical Internet Research*, vol. 23, no. 1, p. e13556, Jan. 2021, doi: 10.2196/13556.

[11] S. Prajapati, J. Gadhari, T. Sawant, J. Kini, and S. Solanki, "Strengthening Supply Chain Integrity with Blockchain-based Anti-Counterfeiting Measures," in *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, Uttarakhand, India: IEEE, Mar. 2023, pp. 786–790. doi: 10.1109/ICIDCA56705.2023.10100264.

[12] E. Ehioghae, S. Idowu, and O. Ebiesuwa, "Enhanced Drug Anti-Counterfeiting and Verification System for the Pharmaceutical Drug Supply Chain using Blockchain," *International Journal of Computer Applications*, vol. 174, no. 21, pp. 1–12, Feb. 2021, doi: 10.5120/ijca2021921105.

[13] J. Ma, S.-Y. Lin, X. Chen, H.-M. Sun, Y.-C. Chen, and H. Wang, "A Blockchain-Based Application System for Product Anti-Counterfeiting," *IEEE Access*, vol. 8, pp. 77642–77652, 2020, doi: 10.1109/ACCESS.2020.2972026.

[14] G. Jain, A. Shrivastava, and M. Brahmi, "Consumer acceptance toward blockchain technology for anti-counterfeiting: hype, credence or future," *International Journal of Business Innovation and Research*, vol. 34, no. 1, pp. 90–108, 2024, doi: 10.1504/IJBIR.2024.138144.

[15] T. Sureshkumar and M. Vijayakumar, "Blockchain based Security System for the Devices in Internet of Things," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India: IEEE, Jan. 2020, pp. 1–4. doi: 10.1109/ICCCI48352.2020.9104092.

[16] L. M R, S. Ahmed M N, and S. Khan, "Block Chain Based Supply Chain Management for Counterfeit Drugs in Pharmaceutical Industry," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 7, no. 1, pp. 100–108, Jan. 2021, doi: 10.32628/CSEIT217122.

[17] X. Gao, W. Zhang, B. Zhao, J. Zhang, J. Wang, and Y. Gao, "Product Authentication Technology Integrating Blockchain and Traceability Structure,"

Electronics, vol. 11, no. 20, p. 3314, Oct. 2022, doi: 10.3390/electronics11203314.

[18] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Bitcoin. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

[19] C.-L. Chen *et al.*, "A Blockchain-Based Anti-Counterfeit and Traceable NBA Digital Trading Card Management System," *Symmetry*, vol. 14, no. 9, p. 1827, Sep. 2022, doi: 10.3390/sym14091827.

[20] G. O. Karame, E. Androulaki, and S. Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," 2012, 2012/248. [Online]. Available: https://eprint.iacr.org/2012/248

[21] A. Bamnote and R. Patil, "Identity Management using Blockchain - A Review," *International Journal of Darshan Institute on Engineering Research and Emerging Technologies*, vol. 12, no. 1, pp. 29–35, Aug. 2023, doi: 10.32692/IJDI-ERET/12.1.2023.2305.

[22] J. F. Xiao, B. Zhou, and H. W. Ressom, "Metabolite identification and quantitation in LC-MS/MS-based metabolomics," *TrAC Trends in Analytical Chemistry*, vol. 32, pp. 1–14, Feb. 2012, doi: 10.1016/j.trac.2011.08.009.

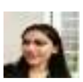
[23] J. Abou Jaoude and R. George Saade, "Blockchain Applications – Usage in Different Domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019, doi: 10.1109/ACCESS.2019.2902501.

[24] S. Wang, D. Li, Y. Zhang, and J. Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario," *IEEE Access*, vol. 7, pp. 115122–115133, 2019, doi: 10.1109/ACCESS.2019.2935873.

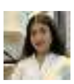
[25] N. Mahamuni, G. Pattewar, H. Nikam, O. Loka, and R. Patil, "A Blockchain and Proxy Re-encryption Based Approach for IoT Data Security: A Review," in *Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems*, vol. 584, M. A. Al-Sharafi, M. Al-Emran, M. N. Al-Kabi, and K. Shaalan, Eds., Cham: Springer International Publishing, 2023, pp. 587–595. doi: 10.1007/978-3-031-25274-7_51.

[26] M. Borse, P. Shendkar, Y. Undre, A. Mahadik, and R. Y. Patil, "A Review of Blockchain Consensus Algorithm," in *Expert Clouds and Applications*, vol. 444, I. J. Jacob, S. Kolandapalayam Shanmugam, and R. Bestak, Eds., Singapore: Springer Nature Singapore, 2022, pp. 415–426. doi: 10.1007/978-981-19-2500-9_31.

Biographical notes



Pragati Nehete has completed her BTech in Computer Science and Honors in Cybersecurity from PCCOE, Pune. She is working as a Business Analyst at Dentsu. She has worked on various research paper in email phishing detection for detecting malicious URL's and QR codes. She has completed various courses and contributed to several survey and research papers. She is also a Member of (WiCyS) Women in Cyber Security India.



Radhika Gaikwad has completed her BTech in Computer Science and Honors in Cybersecurity from PCCOE, Pune. She is a Cyber Security enthusiast and IT Analyst. She is also a member of ACM and GDSC. She has published a paper "Auto Safety Technology with Enhanced Facial Recognition to Prevent Replay Attacks" in IEEE ISCON.

Rachana Patil is an Associate Professor at the Department of Computer Science and applications, Faculty of Science, PCCOE, Pune, India. She received PhD from University of Mumbai, India in 2020. She has published 60+ papers in international journals and conferences. Her primary areas of research are Cryptography, Network Security, Cyber Security and Digital Forensics (specially Network forensics). She is also a Member of IEEE, ACM and IETE.