Fake Product Identification System

Dr. B. Rajalakshmi[1], Ms. Jayashree[2], Anushka Dharan[3], Jainam Jain[4], Shivswami Chavan[5]
[1]HOD, Dept of CSE
[2]Associate Professor, Dept of CSE
[3, 4, 5]Dept of CSE
[1, 2, 3, 4, 5] New Horizon College of Engineering, Bengaluru, India

Abstract- *This study presents a revolutionary strategy for thwarting the sale of counterfeit goods by utilising blockchain technology and combining biometric verification with Web Au- thentication (WebAuthn). The goal of the suggested solution is to improve product authenticity by using safe, decentralised blockchain transactions. By providing an additional degree of user verification, WebAuthn's biometric authentication guaran- tees the accuracy of data pertaining to products. Combining WebAuthn with blockchain technology offers a strong way to reduce fraudulent activity in supply chains while giving user- friendly authentication techniques priority.*

Keywords- Counterfeit products, Blockchain technology, QR codes, WebAuthn.

I. INTRODUCTION

The ubiquity of fake goods presents a serious threat to the integrity of online transactions and undermines customer confidence in the ever-changing world of e-commerce. In order to address the widespread problem of counterfeit goods, this study presents a novel architecture that makes use of the synergies between blockchain technology and biometric verification utilising WebAuthn. The suggested approach seeks to strengthen the e-commerce ecosystem from both ends by merging WebAuthn for safe user authentication and blockchain for transparent product tracking. WebAuthn protects user ac- counts—especially those of manufacturers—from unwanted access, while the blockchain guarantees an unchangeable record of the product's path through the supply chain. This novel combination holds the potential to redefine the standards of authenticity and security in e-commerce, offering a compre- hensive solution to the increasingly complex challenges posed by counterfeit goods.

II. OBJECTIVE

The objective of counterfeit product identification using blockchain is as follows:

Identify applicable funding agency here. If none, delete this.

- Create a Safe Blockchain Structure:

Create and put into place a blockchain-based system that guarantees the product supply chain's immutability and trans- parency. The goal of this system is to offer a reliable ledger for documenting and monitoring the full lifecycle of items, from production to delivery to the customer.

- Turn on authentication and traceability:

Make use of the deployed blockchain to facilitate product traceability from beginning to finish. This involves keeping track of information at every turn in the supply chain to facilitate effective tracking and validation. To further improve system security, incorporate biometric verification into user accounts by utilising WebAuthn, with a particular emphasis on manufacturers.

- Implementing Smart Contracts into Practise for Auto- mated Validation:

Automate the supply chain's verification procedures by integrating smart contracts into the blockchain. These con- tracts will carry out pre-established guidelines, guaranteeing that product details are appropriately documented and that efforts at counterfeiting are immediately reported for further examination.

- Assessing the Product Identification System's Effective- ness

To determine how well the suggested system works to detect and stop the sale of fake goods, carry out extensive testing and analysis. Evaluate the efficacy of WebAuthn in protecting manufacturer accounts and the precision and dependability of the blockchain in tracking the origins of products.

- Implementing Smart Contracts into Practise for Auto- mated Validation:

Automate the supply chain's verification procedures by integrating smart contracts into the blockchain. These contracts will carry out pre-established guidelines, guaranteeing that product details are appropriately documented and that efforts at counterfeiting are immediately reported for further examination.

- Assessing the Product Identification System's Effectiveness

Engage a representative subset of users, specifically manufac- turers, in the testing process to gather input on the usability and acceptance of the WebAuthn and blockchain combination system. Recognise the viewpoints of users and resolve any issues to improve the user experience as a whole.

- Contribute insights for Upcoming Implementations:

In order to offer direction for future blockchain and bio- metric authentication system deployments in the context of battling counterfeit products in e-commerce, summarise the research's major results and insights. Provide suggestions for possible improvements to the suggested solution as well as best practices for the industry.

III. LITERATURE REVIEW

The proliferation of fake goods is a serious danger to global economies, producers, and consumers. In order to strengthen the identification and authentication process for producers and stop the spread of counterfeit goods, this study investigates the integration of blockchain technology and biometric verification through WebAuthn.

A. EXISTING SYSTEM

- Vulnerabilities in Authentication: Existing product identification systems are not robust enough; they rely too much on conventional techniques like holograms and serial numbers. Due to their ease of replication, counterfeiters have plenty of space to create phoney goods without being discovered.
- Centralised Databases: A lot of the current systems are vulnerable to data tampering and hacking since they rely on centralised databases for product authentication. Once a breach happens, counterfeiters can alter the database to make their phoney goods seem legitimate, jeopardising the system's integrity as a whole.
- Limited Traceability: It is difficult to track the complete supply chain in current setups due to the absence of a thorough traceability mechanism. Due to this gap, fake goods might enter the market unnoticed, costing manufacturers money and jeopardising customer safety.
- Complexity of Cross-Border Verification: In an increasingly globalised market, confirming the legitimacy of products across international borders is a formidable obstacle. The lack of a unified, widely recognised framework leads to a disjointed strategy for detecting counterfeit goods.
- Ineffective Recall Procedures: When a counterfeit product is discovered, the current processes frequently don't have an effective way to take it off the market. This ineffectiveness adds even more fuel to the fire of counterfeit goods.
- Absence of User Accountability: It is currently diffi- cult for manufacturers to guarantee the security of their accounts. Passwords are frequently the only means of authentication, leaving accounts open to illegal access. The system's overall security is jeopardised by this weak user authentication.
- Restricted User-Friendly Features: Manufacturers find it difficult to engage with the authentication process because many of the current systems are devoid of user-friendly features. Responses to instances of counterfeiting may be delayed as a result of this restriction.
- Scalability Issues: Existing systems have scalability issues as the number of producers and products increases. The growing volume of international transactions is too much for traditional ways to handle, which causes delays and inefficiencies in the authentication process.

B. PROPOSED SYSTEM

- Blockchain-Based Authentication: To create a decentralised, impenetrable ledger for product authentication, the suggested method incorporates blockchain technology. Every product is given a distinct digital identity that is registered on the blockchain, guaranteeing immutability and transparency.
- Biometric User Verification using WebAuthn: The suggested approach integrates WebAuthn for manufactur- ers to improve user authentication. By using biometric information—like fingerprints or facial recognition—to authenticate user accounts, the possibility of unwanted access is greatly decreased.
- Blockchain-Based Smart Contracts for Automated Supply Chain Traceability: Smart contracts allow for automated supply chain traceability. These contracts have the ability to independently confirm the legitimacy of every transaction, giving all parties involved access to an unchangeable record.

- Cross-Border Compatibility: By creating a uniform methodology for product authentication, the suggested system tackles the difficulty of cross-border verification. This promotes a coordinated strategy to combat counterfeit goods by ensuring compatibility and seamless integration across various locations.
- Effective Recall Mechanisms: The suggested solution makes use of the real-time updates provided by the blockchain to enable quick and effective recall procedures. Automated recalls can be initiated using smart contracts, guaranteeing prompt action in the event that fake goods are discovered.
- Enhanced User Account Security: WebAuthn's biometric verification adds an extra layer of security to manufacturer accounts, mitigating the risk of unauthorized access. This feature reduces the likelihood of malicious activities that compromise the integrity of the authentication system.
- User-Friendly Interface: The proposed system focuses on user experience by incorporating a user-friendly interface for manufacturers. Intuitive design and seamless integration with existing workflows aim to encourage active participation in the authentication process.
- Scalability and Interoperability: Designed with scalability in mind, the proposed system can accommodate the growing volume of products and manufacturers in the global market. Interoperability with existing systems ensures a smooth transition and widespread adoption.

In summary, the amalgamation of blockchain technology and biometric verification via WebAuthn presents a propitious resolution to the predicaments caused by fake goods. The suggested framework offers a strong, transparent, and safe method of product authentication by addressing the flaws in the current systems, and protecting both buyers and sellers.

IV. METHODOLOGY

The methodology for fake product identification using blockchain involves a systematic approach to design, imple- mentation, and evaluation. The following steps outline the key components of the methodology:

- Review of the Literature: To start the methodology, summarise the current studies and information about blockchain technology, biometric verification using WebAuthn, and counterfeit product identification. In addition to identifying any gaps or areas where the suggested methodology can be helpful, this step aids in setting the background for the current investigation.
- Research Objectives: Clearly state what the particular goals of the study are. Describe the objectives and anticipated results, such as raising the level of product authenticity, strengthening user authentication, and lowering the number of instances of counterfeit goods through the blockchain and WebAuthn integration.
- System Architecture Design: Create a thorough system architecture that demonstrates how biometric account verification and blockchain are integrated. To give the study framework a visual depiction, list the elements, relationships, and data flow of the suggested system.
- Blockchain Implementation: Give an overview of the selected blockchain platform's salient characteristics. Describe the procedure for giving products distinct digital identities, highlighting the use of smart contracts to enable traceability and tamper-resistant record-keeping.
- Setup for Biometric User Verification: Describe how WebAuthn is integrated for biometric user verification. Give specifics about the chosen biometric modalities (facial recognition, fingerprints, etc.) and the procedures taken to connect these biometrics to manufacturer accounts.
- Data Collection: Describe how information is gathered to verify users and authenticate products. Specify the kinds of information that are gathered, such as product specifications, user biometrics, and blockchain transaction histories.
- User Onboarding and Training: Describe the steps involved in educating manufacturers about the new system. Provide training materials that are easy to understand and manufacturers with precise instructions for onboarding in order to guarantee a seamless implementation of the blockchain and biometric verification process.
- Simulation and Testing: To assess the efficacy of the suggested system, run simulations and test scenarios. To model different counterfeit incidents, evaluate the system's reaction, and spot any possible vulnerabilities, use a controlled environment.
- Security Analysis: To find any potential weaknesses in the blockchain and biometric verification components, conduct a thorough security analysis. Implement access controls, encryption, and other security measures to protect the system and address any security issues.
- Integration with Current Systems: Describe how the suggested system will be integrated with the current systems for product identification and authentication. To make the transition easier for manufacturers who are currently using other authentication methods, make sure there is compatibility and seamless interoperability.
- Customer Input and Iterative Enhancement: Gather manufacturer input on the new system and make iterative improvements based on their suggestions. This stage makes

sure that the finished product meets user requirements and takes care of any unforeseen issues that may arise in practical application.

- Analysis of Data and Outcomes: Examine the information gathered from the testing and actual implementation stages. Provide both quantitative and qualitative data to assess how well the suggested methodology has worked overall to decrease instances of counterfeit goods and improve the authenticity of genuine products.

By following this methodology, the research aims to provide a comprehensive understanding of the implementation process and effectiveness of combining blockchain and biometric verification through WebAuthn for fake product identification.

V. CONCLUSION AND FUTURE SCOPE

- Enhanced Product Authenticity: WebAuthn's combination of blockchain technology and biometric verification offers a strong defence against phoney product identification. Research has shown that by utilising the immutability and transparency of blockchain technology, the suggested system greatly improves product authenticity.
- Better User Authentication: WebAuthn's biometric verification has been integrated to overcome the drawbacks of conventional authentication techniques for manufacturers. The risk of unauthorised activity is reduced by the enhanced security measures, which guarantee that only authorised personnel can access and interact with the product identification system.
- Enhanced Accountability and Traceability: The implementation of smart contracts on the blockchain has enhanced supply chain traceability. This not only makes it easier to spot fake goods quickly, but it also holds manufacturers more accountable for the whole life of the product.
- Quick Reaction to Counterfeit Incidents: Using real- time blockchain updates, the suggested system makes recall procedures more effective. Smart contracts cause automated recalls in the event that a counterfeit product is identified. This allows manufacturers to quickly respond and lessen the impact on the market and consumers.
- Adoption and User-Friendly Interface: The focus on an intuitive user interface guarantees that manufacturers can incorporate the new authentication techniques into their current workflows with ease. This user-centric strategy encourages engagement and raises the possibility of widespread.
- Scalability and Interoperability: The suggested system's capacity to handle the expanding number of goods and producers in the international market demonstrates both its scalability and interoperability. Because the system is compatible with current authentication methods, a seamless transition is ensured and it can be tailored to meet the needs of various industries.

VI. FUTURE SCOPE

- Constant Improvements in Technology: Future extensions of this research will include blockchain and biometric authentication developments as technology develops. Keeping up with new developments in technology guarantees that the system stays at the forefront of security and prevents counterfeiting.
- Global Standardisation: The creation of international guidelines for product identification and authentication represents a possible direction for future study. Working together with international organisations and stakeholders may result in a standardised strategy that promotes an all-encompassing system that breaks down barriers related to geography and industry.
- Integration with IoT Devices: Investigating how to incorporate Internet of Things (IoT) devices can improve the capabilities of the system even more. In addition to enhancing the traceability of the blockchain, IoT devices can offer real-time data on product conditions, resulting in a more complete ecosystem for authentication.
- Using Artificial Intelligence to Identify Abnormalities: Artificial intelligence (AI) may be used in future studies to detect anomalies in blockchains. By using AI algorithms, the system may be able to recognise patterns that point to fraudulent activity, adding another degree of preventive security.
- Cooperation with Authorities in Charge: Working together with law enforcement and regulatory organisations is crucial to the effective execution of a thorough anti-counterfeiting programme. Subsequent investigations may concentrate on developing cooperation guidelines and making sure that laws facilitate the use of sophisticated authentication techniques.
- Campaigns for User Education and Awareness: User awareness and education are essential to the effectiveness of any authentication system. Prospective investigations could explore the creation of efficacious education and awareness initiatives aimed at manufacturers. Sustaining the system's success will depend in part on ensuring that stakeholders recognise its value and advantages.
- Cross-Industry Adoption: Opening up the research to include a wider range of industries may help facilitate cross-industry adoption. Examining the ways in which the suggested system can be customised to fulfil the distinct requirements of various industries would enhance its broad applicability and influence.

To sum up, research on biometric verification through WebAuthn and blockchain for fake product identification not only solves present issues but also lays the groundwork for future developments in the field.

REFERENCES

[1] Al-Bassam, M, Sonnino, A, Bano, S, Hrycyszyn, D Danezis, G 2018, 'Chainspace: A Sharded Smart Contracts Platform', Proceedings 2018 Network and Distributed System Security Symposium.

[2] Bocek, T, Rodrigues, BB, Strasser, T Stiller, B 2017, Blockchains everywhere - a use-case of blockchains in the pharma supply- chain, IEEE Xplore, pp. 772–777, viewed 20 April 2020,¡https://ieeexplore.ieee.org/document/7987376¿.

[3] Bodkhe, U, Tanwar, S, Parekh, K, Khanpara, P, Tyagi, S, Kumar, N Alazab, M 2020, 'Blockchain for Industry 4.0: A Comprehensive Review', IEEE Access, vol. 8, no. 1, pp. 79764–79800.

[4] Buvaneswari, DrB 2021, 'Fake Product Identification using Blockchain', International Journal for Research in Applied Science and Engineering Technology, vol. 9, no. 3, pp. 877–880.

[5] Dwivedi, SK, Amin, R Vollala, S 2020, 'Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism', Journal of Information Security and Applications, vol. 54, p. 102554.

[6] Fisher, W 2021, '(Draft) Using Mobile Device Biometrics for Authenticating First Responders', viewed 13 September 2021,¡https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8334-draft.pdf¿.

[7] Frymann, N, Gardham, D, Kiefer, F, Lundberg, E, Manulis, M Nilsson, D 2020, 'Asynchronous Remote Key Generation', Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security.

[8] Ghorbani Lyastani, S, Schilling, M, Neumayr, M, Backes, M Bugiel, S 2020, 'Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication', 2020 IEEE Symposium on Security and Privacy (SP).

[9] Iness Ben Guirat Halpin, H 2018, 'Formal verification of the W3C web authentication protocol', HAL (Le Centre pour la Communication Scientifique Directe), French National Centre for Scientific Research.

[10] Khan, MA Salah, K 2018, 'IoT security: Review, blockchain solutions, and open challenges', Future Generation Computer Systems, vol. 82, pp. 395–411.

[11] Monrat, AA, Schelen, O Andersson, K 2019, 'A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities', IEEE Access, vol. 7, pp. 117134–117151.