GJETA

Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(Research Article)

Check for updates

Identification of fraudulent products using blockchain technology

Oluwaseyi Segun Adediran *, Mercylina Eyaofun Udeh, Opeyemi Joshua AdelowoIsrael, Kitan Josiah, Ikechukwu Tamunokuro Kalu and Emmanuel Ifeoluwa Oyerinde

Department of Information Technology, School of Computing, Babcock University, Ilishan-Remo, Ogun State, Nigeria PMB 4003, Ilishan Remo, Ogun State, Nigeria.

Global Journal of Engineering and Technology Advances, 2025, 24(01), 229-244

Publication history: Received on 11 June 2025; revised on 20 July 2025; accepted on 22 July 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.24.1.0222

Abstract

Fraudulent products pose a significant threat to consumer safety, brand reputation, and global economic stability. Traditional product authentication technologies struggle to offer tamper-evident and scalable functionalities, especially in the modern digital economy. This paper proposes Digi Seal, a product authentication system based on blockchain technology that offers secure, open, and efficient tracking of products from manufacturers to consumers. On top of Ethereum and smart contracts, using QR code scanning and role-based access, the system offers product registration, authentication, ownership transfer, and reporting counterfeit. The paper outlines Digi Seal design, development, implementation, and testing, illustrating how blockchain technology can effectively be used to combat counterfeiting.

Keywords: Blockchain; Product Authentication; Counterfeit Detection; Smart Contracts; Supply Chain Security

1. Introduction

The globalization of the economy has made counterfeiting a compounding issue that is now a harrowing challenge for manufacturers, governments, and consumers alike. Pharmaceuticals, electronics, and luxury brands are not exempt from counterfeiters, as product quality is compromised, consumer confidence is shaken, and gigantic economic losses are suffered. According to Lall (2023), illegal medicines make up about 10 percent of the global pharmaceutical market, and this accounts for over 1.2 million deaths every year. Similarly, counterfeit components in the electronics industry caused a projected 75 billion dollars in losses per annum between 2021 and 2023, halting production and increasing expenses (Singh and Kesari, 2023).

Historical product authentication solutions have typically relied on physical labels, serial numbers, packaging techniques, and central databases. These solutions offer some level of security but are increasingly falling short against advanced counterfeiting techniques. Security labels are easily counterfeited or duplicated, serial numbers can be replicated, and central tracking databases can be compromised or altered. Further, these methods are challenging to implement at scale in sophisticated global supply chains and do not generally offer the transparency required to build user confidence (Lukacs et al., 2025).

Blockchain technology introduces a very different product verification solution. It enables data to be recorded in a secure, transparent, and tamper-evident form on a distributed network. Because all transactions are time-stamped and cannot be altered except by consensus from all of the nodes on the network, blockchain is the ideal system for verification and guaranteeing the authenticity of products. Producers and consumers alike can both verify the origin and history of ownership of a product without trusting in a central authority. Decentralization like this encourages responsibility, increases transparency, and makes the supply chain an awful lot safer (Dong et al., 2023).

* Corresponding author: Oluwaseyi Segun Adediran

Recent innovations have proven that integrating blockchain with technologies such as QR codes, RFID tags, and Near Field Communication (NFC) can support real-time product authentication. When these unique identifiers are connected to a blockchain ledger, the products can be tracked from their origin to their destination. Razi et al. (2023) have depicted the use of non-fungible tokens (NFTs), underpinning the ERC-721 standard, to offer digital identities to physical goods that are identifiable, verifiable, and impossible to counterfeit.

The pharmaceuticals and electronics sectors have actually seen a boom in the utilization of blockchain pilot projects for tracking goods and preventing fraud. Platforms such as Vacherin and Medi Ledger utilize smart contracts to enable the automation of verification processes and increase transparency within supply chains (Munyao, 20222; Talwandi et al., 2025). Solutions are solving more and more problems related to energy efficiency and privacy as well. Laslo et al. (2022), for example, developed a blockchain consensus mechanism that reduced energy usage by 87 percent from what would be used with traditional proof of work paradigms. Other authors have employed zero knowledge proofs and homomorphic encryption to ensure data security without sacrificing user privacy (Jung et al., 2024).

To present a practical application of these technologies, this project suggests Digi Seal, a blockchain platform for the authentication of products. Digi Seal has a hybrid blockchain topology that takes advantage of the open Ethereum blockchain for transparency and Hyperledger Fabric for efficient and private supply chain operations. Solidity smart contracts execute basic operations such as product registration, ownership transfer, and counterfeiting reporting. The system has role-based access and a web frontend through which customers can verify products by scanning QR codes or entering product IDs.

While blockchain has tremendous advantages, there remain issues. Ethereum-like public chains experience issues with the speed of adding transactions and gas costs. Additionally, the integration of blockchain into existing enterprise settings and encouraging user acceptance requires efforts, time, and collaboration among stakeholders (Laslo et al., 2022).

This study therefore aims to establish and evaluate a blockchain framework for counterfeit product detection through designing a secure, scalable, and easy-to-use verification platform that leverages the advantages of decentralized technology.

Objectives

- To develop a blockchain-based platform for real-time product authentication.
- To ensure secure product registration and tracking using unique identifiers.
- To enable users to verify authenticity and report counterfeits via a web interface.
- To evaluate the system's effectiveness in scalability, usability, and tamper-resistance.

2. Review of literature

2.1. Blockchain Technology

Blockchain technology is a decentralized digital ledger that keeps data on multiple nodes in a network, thus highly resistant to tampering or any form of unauthorized modification. Its four prominent features (transparency, immutability, decentralization, and cryptographic security) are exactly what render it highly efficient in the fight against trust and data integrity challenges in product authentication. Trailor et al. (2022) assert that blockchain bypassed the need for central authorities since it offers peer-to-peer verification. It is especially useful in supply chains, where several stakeholders must be able to view and verify the authenticity and passage of goods. Every transaction, from the point of production to the point of final sale, can be stamped and stored on the blockchain forever, enabling all concerned parties to track the origin and travel of the product with certainty.

Ethereum, among the most mature public blockchain platforms, facilitates smart contracts that will automate verification procedures. These contracts execute pre-determined terms automatically, making them convenient for counterfeiting prevention and detection. Razi et al., (2023) highlighted the way Ethereum-based ERC-721 tokens can establish separate digital identities for physical goods like electronics or medication. The non-fungible tokens ensure that each product has a traceable identity and cannot be replicated. In business use, there are private blockchains like Hyperledger Fabric that give more control, speed, and privacy. Alkhateeb et al. (2022) explained that hybrid versions, where public as well as private blockchain characteristics are blended, provide transparency as well as system efficiency and are best suited for commercial product verification scale.

Other than blockchain design, advancements in cryptography methods also supported the potential of blockchain. Methods such as zero-knowledge proofs and homomorphic encryption allow secure verifications of data without revealing the original information (Zhou et al., 2024). This is especially important in sectors like healthcare and pharmaceuticals, where confidentiality is paramount. Despite these strengths, there are some weaknesses. Public blockchains have high transaction fees and slower processing rates, which discourage user adoption (Appelbaum et al., 2022). There is also the problem of interoperability between various blockchain systems, where it becomes hard to interlink with legacy enterprise technology (Kit Santas, 2022). But there is current research that shows these are transitory problems that should diminish as the technology matures.

2.2. Identification of Fraudulent Products

Identification of fraudulent products involves determining if a product is authentic or counterfeit. Traditionally, this identification has been physical identification such as holograms, barcodes, watermarks, and exclusive packaging. While these systems provide an added layer of protection, they are generally not sufficient against sophisticated counterfeiting techniques. Counterfeiters can simply replicate or bypass these physical indicators with advanced manufacturing tools in the majority of situations, making traditional measures less effective in high-risk areas.

Gugala et al. (2023) explained that traditional product authentication systems are generally centralized and therefore vulnerable to internal tampering and external hacking. Also, conventional systems do not always offer real time visibility, which is required for the management of the complexity of world supply chains. Blockchain gives a more secure and transparent solution. It enables producers, customers, and other stakeholders to be in a position to verify instantly the authenticity of a product by scanning product codes that are linked to a tamper proof ledger. Projects such as IBM Food Trust and Ever ledger have established the use of blockchain technology in tracking products such as diamonds, wine, and organic produce by assigning RFID tags or QR codes that allow customers to trace the origin of a product (Oates, 2022).

Pharma has been an exemplar of blockchain technology used for regulatory compliance through Medi Ledger. The system enables manufacturers of drugs to trace drugs from manufacturing to the retail level, such that counterfeit drugs cannot be introduced into the supply chain. Duan et al. (2024) argue that such systems enhance accountability and reduce fraud. One key advantage of blockchain technology in product identification is its ability to remain immutable. Once stored, they cannot be changed and thus it is very difficult for fraudsters to manipulate the product history (Razi et al., 2023). Smart contracts are also capable of automating verification processes such as change of ownership or authentication verification without human intervention. However, Dong et al. (2023) observed that adoption has not been a straightforward process. The majority of consumers lack both the technical capability and the know-how necessary to utilize these tools effectively, and their unstandardized processes within supply chains hinder broader implementation.

3. Theoretical frameworks

This study draws from Trust Theory and the Technology Acceptance Model (TAM). Trust Theory identifies transparency, dependability, and verifiability as fundamental principles for building trust among entities in contact. In product authentication, trust is essential since consumers and manufacturers have to rely on authentic and safe information throughout the supply chain. Blockchain technology directly facilitates this through the provision of an immutable and unambiguous ledger, thereby imposing stakeholder trust (Bello et al., 2024).

The Technology Acceptance Model, first proposed by Davis, illustrates how and why a new technology is accepted and utilized by the users. It specifies perceived usefulness and perceived ease of use as drivers of adoption. For this study, TAM helps assess consumers', manufacturers', and sellers' views on a blockchain-based product verification system like Digi Seal. If the platform is found to be useful in fraud detection and user-friendly, it's most likely to be embraced and utilized on a consistent basis (Usamas, 2022).

The integration of Trust Theory and TAM assists in bringing solid reasoning to the assessment of both the technical and behavior dimensions of utilizing blockchain to identify counterfeit products in modern supply chains.

4. Methodology

4.1. System Requirements

4.1.1. Functional Requirements

- User Registration and Login
- Product Verification via QR Code or Product ID
- Secure Blockchain Interaction
- Product History and Details Display
- Counterfeit Reporting Feature

4.1.2. Non-Functional Requirements

- Scalability (supports 1000+ concurrent users)
- Data Security through encryption
- User-Friendly Interface
- High Reliability with RESTful APIs

4.1.3. System Constraints

- Blockchain performance may affect speed
- Must ensure data privacy
- Cross-device compatibility required

4.1.4. Stakeholder Analysis

- End-Users: Verify product authenticity
- Manufacturers: Register and track products on blockchain
- Sellers: Sell verified products and manage ownership transfer

4.2. Software Development Approach

The project adopts the Incremental Software Development Model, which allows the system to be built in functional modules. Core features like product registration and verification are delivered first, followed by enhancements such as counterfeit reporting. This model ensures early testing, progressive feature deployment, and adaptability based on feedback.

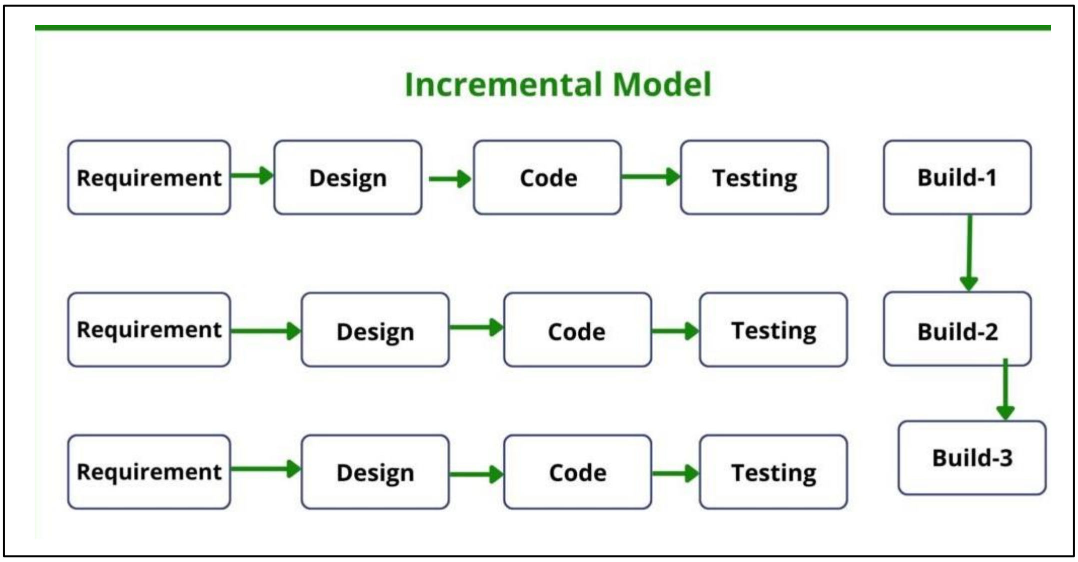

Figure 1 Incremental Process Model

4.3. System Architecture

The system uses a multi-layered architecture consisting of the presentation layer, application logic, and blockchain integration layer. Each layer supports separation of concerns, efficient processing, and secure data handling.

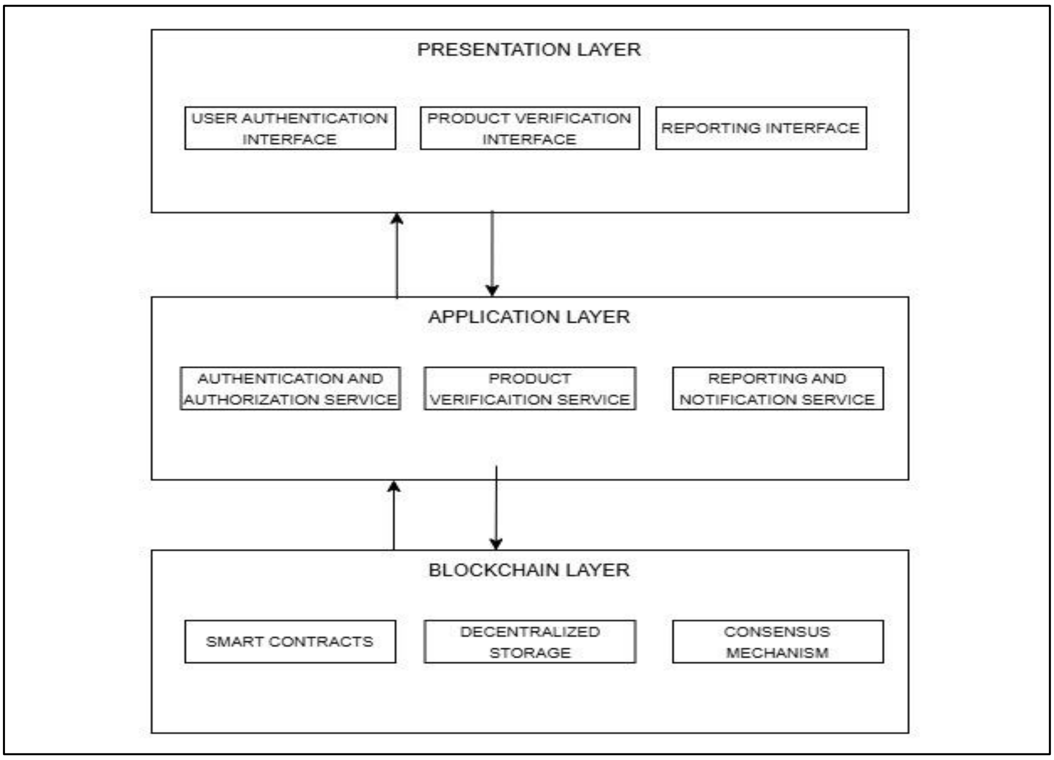

Figure 2 System Architecture Design

4.4. System Use Cases and Diagrams

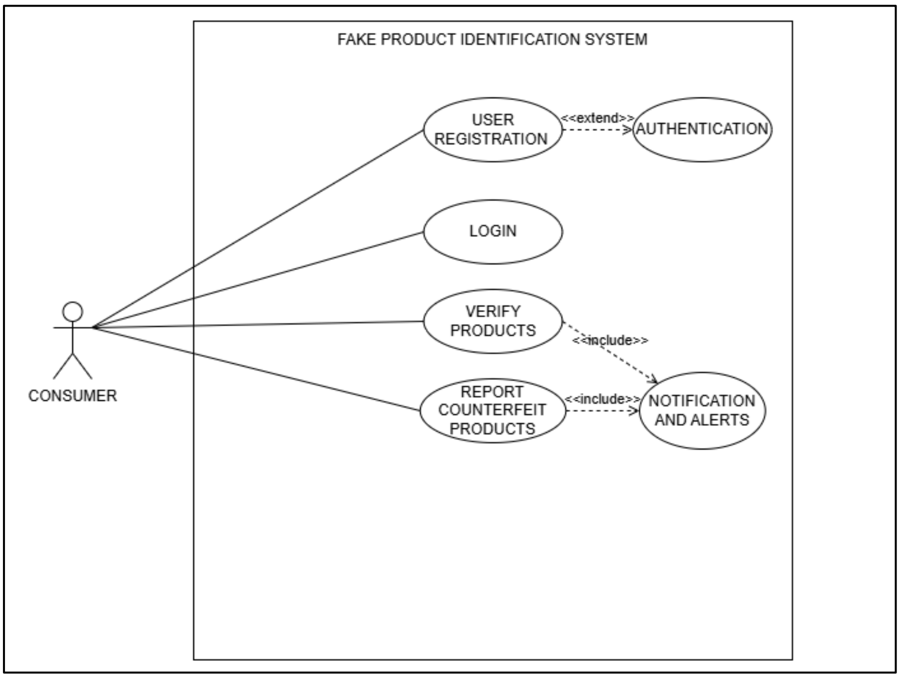

Figure 3 Consumer Use Case Diagram

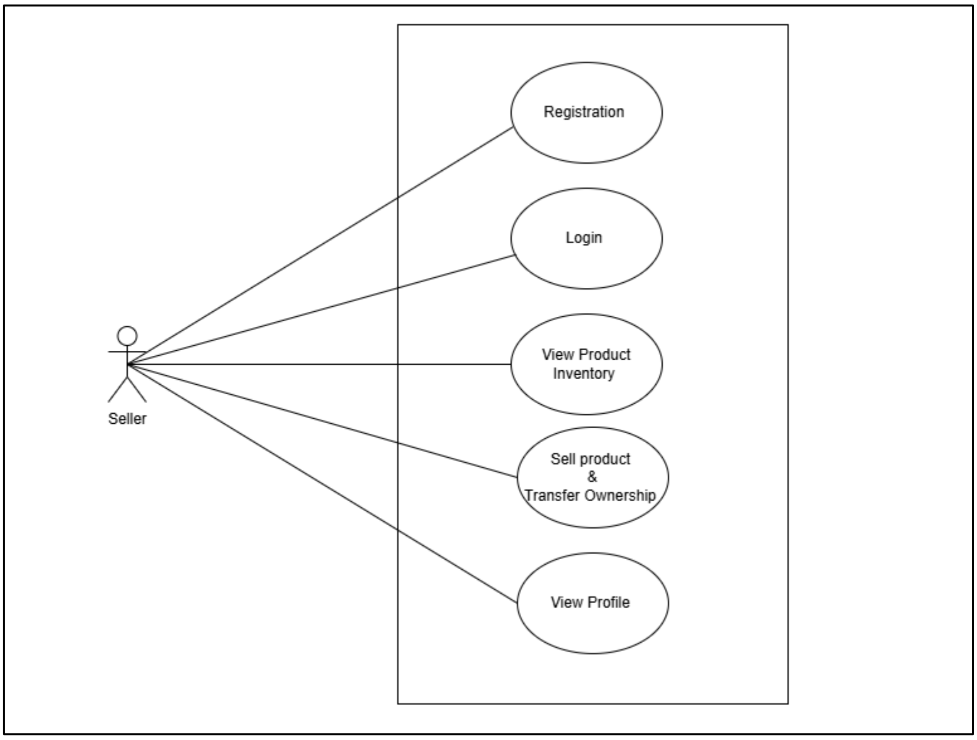

Figure 4 Seller Use Case Diagram

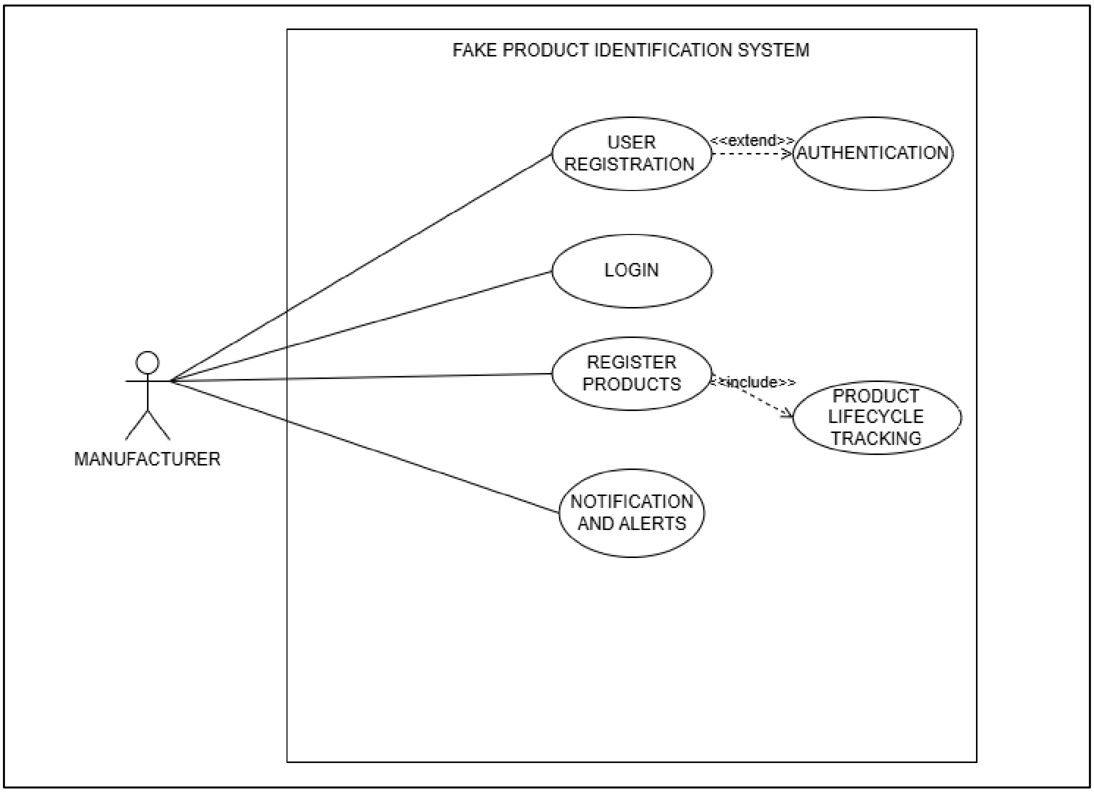

Figure 5 Manufacturer Use Case Diagram

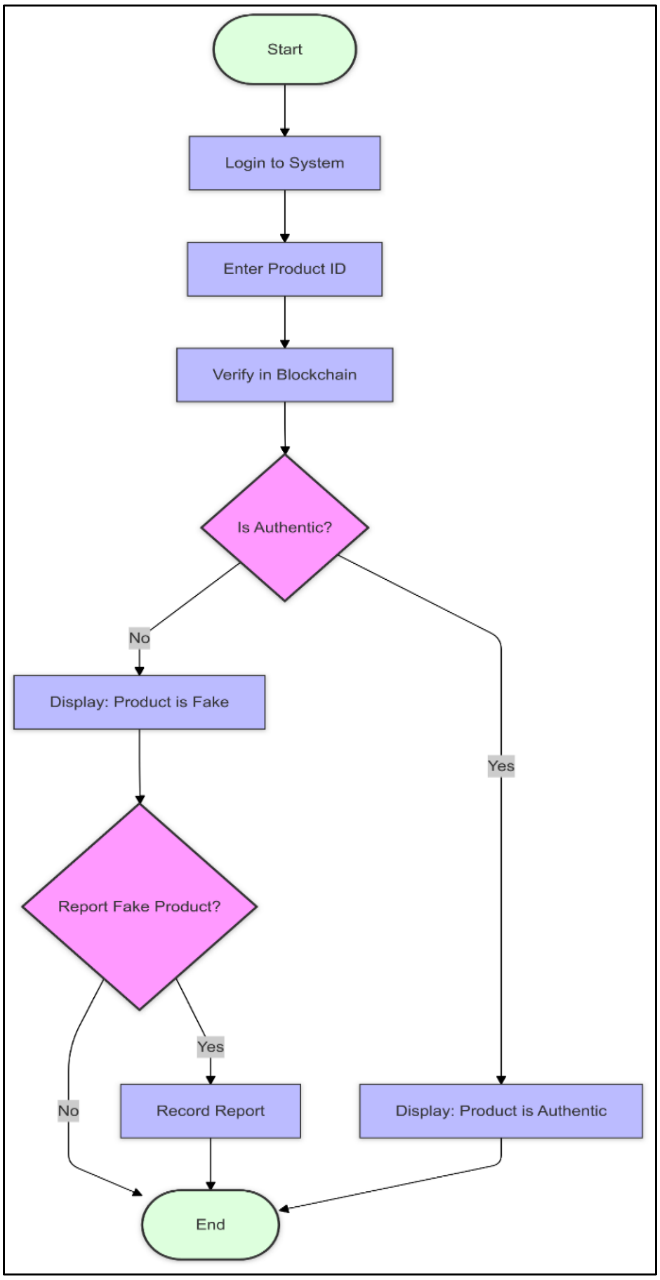

Figure 6 Product Verification Flow Chart

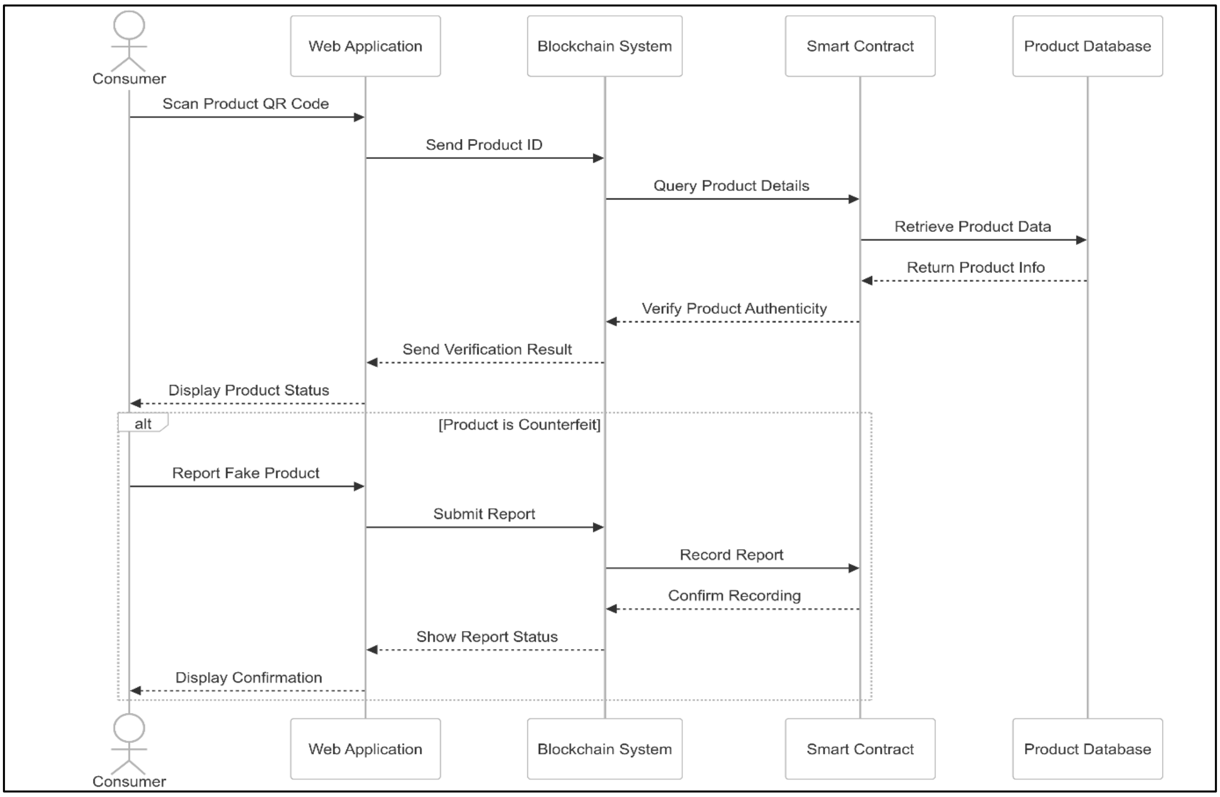

Figure 7 Sequence Diagram

4.5. Development Tools and Stack

4.5.1. Frontend

- React Bootstrap and Formic/Yup for UI and validation
- Web3.js for blockchain interaction
- MetaMask for wallet integration
- QR code features and responsive design

4.5.2. Backend

- Node.js with Express.js for RESTful APIs
- Smart contracts in Solidity (v0.8.19)
- Truffle for deployment on Ethereum Hole sky test net
- Alchemy as blockchain node provider
- Role-based access, product tracking, and reporting

5. System implementation, testing, and results summary for journal publication

5.1. Implementation Process

The system followed an incremental development model. The frontend was built using React.js, the backend with Node.js and Express, and the smart contracts with Solidity. Deployment was completed on the Ethereum Hole sky test net. Core implementation steps included environment setup, frontend and backend development, smart contract design, integration, and security testing.

5.1.1. Implementation Challenges and Solutions

Table 1 Implementation Challenges and Solutions

Challenge	Solution
Ensuring data integrity between the blockchain and off-chain storage	A hybrid data storage approach was used, with critical information stored on the blockchain and supplementary data stored off-chain. Data consistency checks were implemented in the backend API.
Managing the asynchronous nature of blockchain interactions	Asynchronous programming techniques, such as Promises and async/await, were used to handle Ethereum transactions' asynchronous behaviour and ensure a smooth user experience.
Optimizing gas costs for smart contract operations	Smart contracts were carefully designed and optimized to minimize gas consumption. Data packing and efficient data types were used to reduce storage costs.
Providing a user-friendly interface for blockchain interactions	The frontend user interface abstracted away the complexities of blockchain interactions, providing a seamless and intuitive user experience. Users could interact with smart contracts through simple button clicks and form submissions.
Scalability concerns with increasing product registrations and transactions	The system architecture was designed to be scalable, leveraging the power of Ethereum's distributed network. Off-chain data storage solutions were employed to handle large amounts of supplementary data.

5.2. System testing and validation

Unit Testing: Unit tests on React components, API endpoints, and smart contract functions were performed using Jest and Mocha. Product registration and user authentication functions were tested.

Integration Testing: Integration testing ensured proper communication among frontend, backend, and smart contracts. Tests included full user registration and verification processes.

System Testing: The entire system was tested for reliability, performance, and security. Load testing guaranteed consistent operation under concurrent use.

5.2.1. Test Cases and Results

Table 2 Summary of Testing Results

Test Case	Test Procedure	Expected Result
Successful Product Registration	User logs in with manufacturer account User navigates to the product registration page User enters valid product details User submits the registration form	The product is successfully registered on the blockchain and appears in the manufacturer's product list.
Failed Product Registration	User logs in with manufacturer account User navigates to the product registration page User enters invalid or incomplete product details User submits the registration form	The system displays appropriate error messages indicating the missing or invalid fields. The product registration fails.
Successful Product Verification	User scans the QR code of a registered product User is redirected to the product verification page User clicks on the Verify button	The system retrieves the product details from the blockchain and displays the verification result as "Authentic".
Failed Product Verification	User scans the QR code of a counterfeit or unregistered product User is redirected to the product verification page	The system displays the verification result as "Counterfeit" or "Product Not Found".

	User clicks on the "Verify" button	
Reporting a Counterfeit Product	User navigates to the counterfeit reporting page User enters the product ID, evidence details, and description User submits the counterfeit report	The counterfeit report is successfully submitted and stored on the blockchain. The product's status is updated to "Reported".

5.3. Graphical overview and user interface

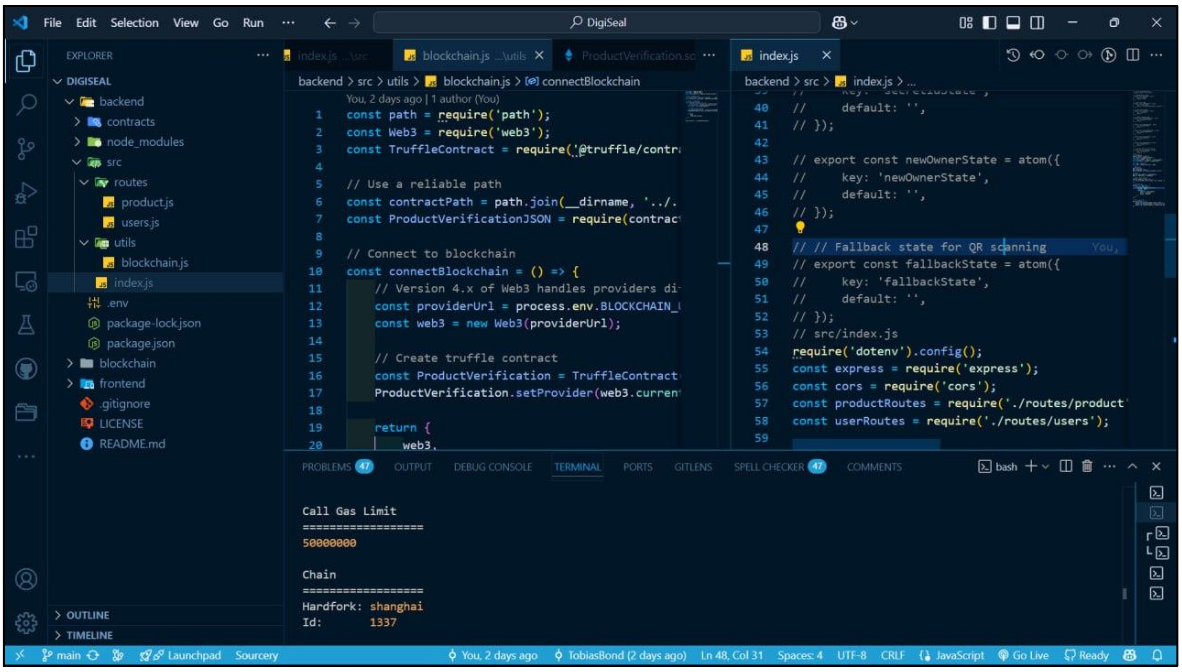

Figure 8 Project Development View

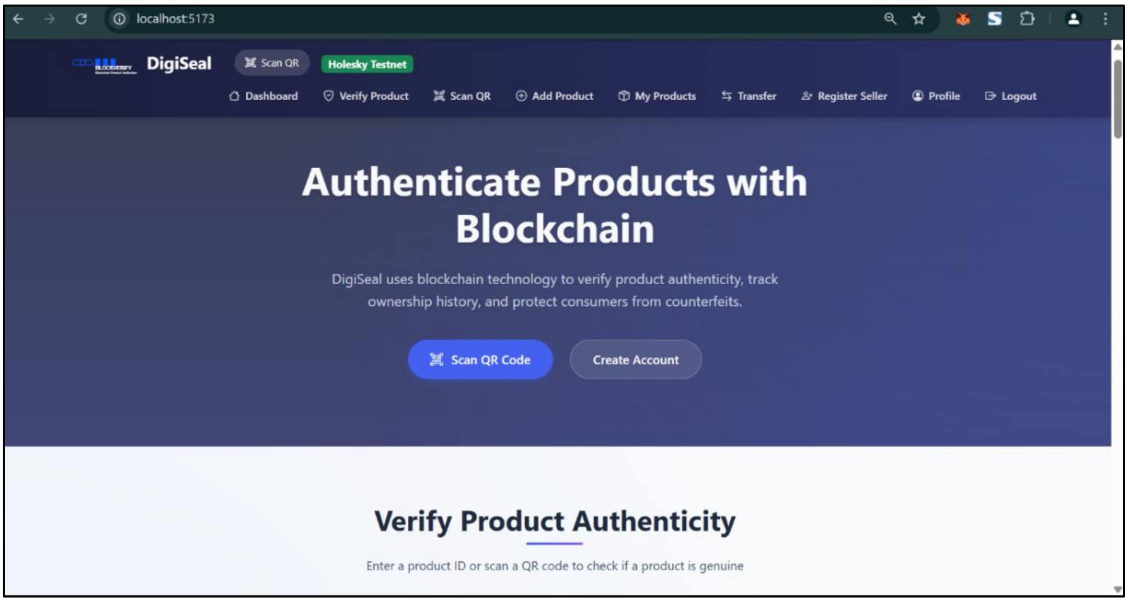

Figure 9 Home Page

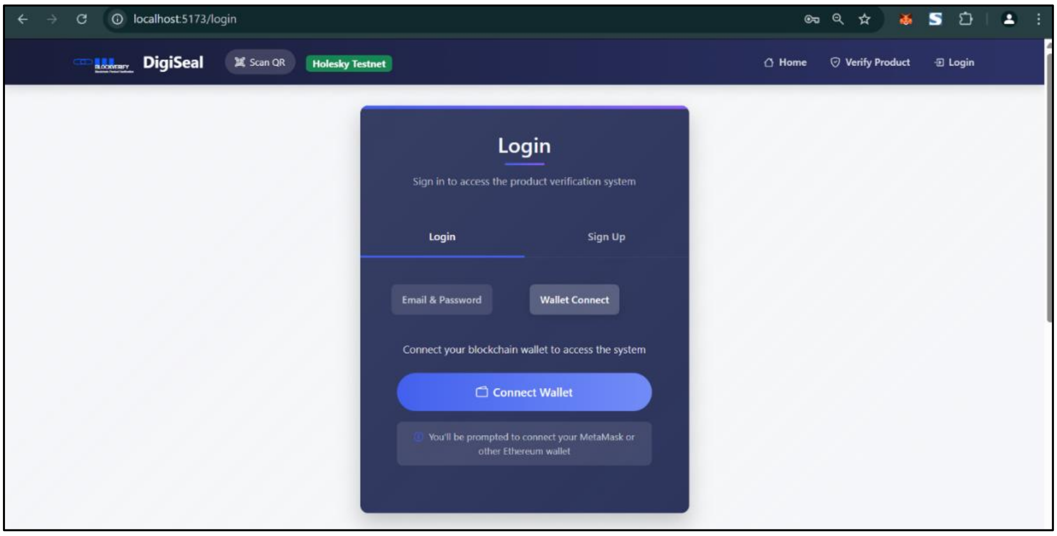

Figure 10 Login Page

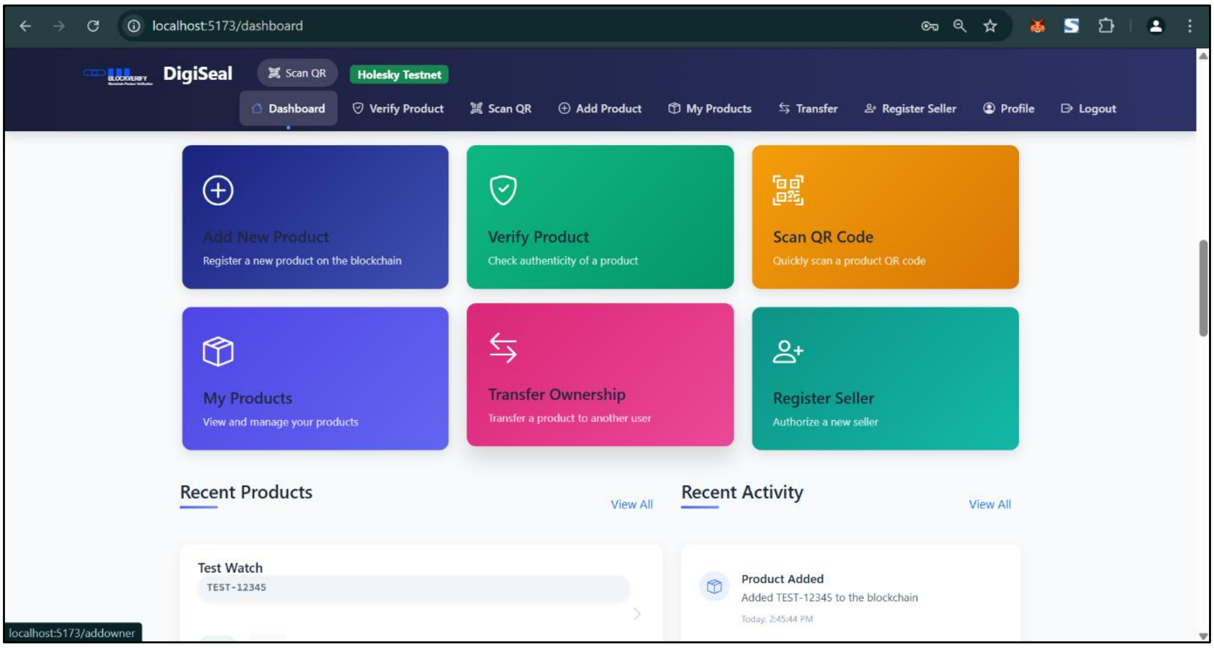

Figure 11 Dashboard Page

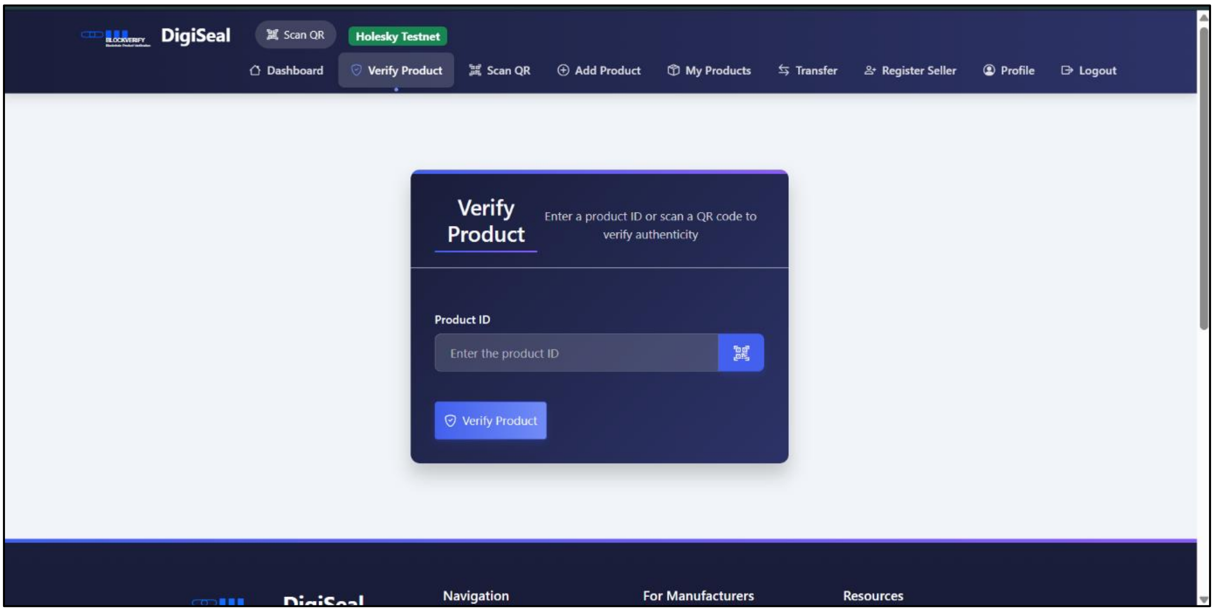

Figure 12 Verify Product Page

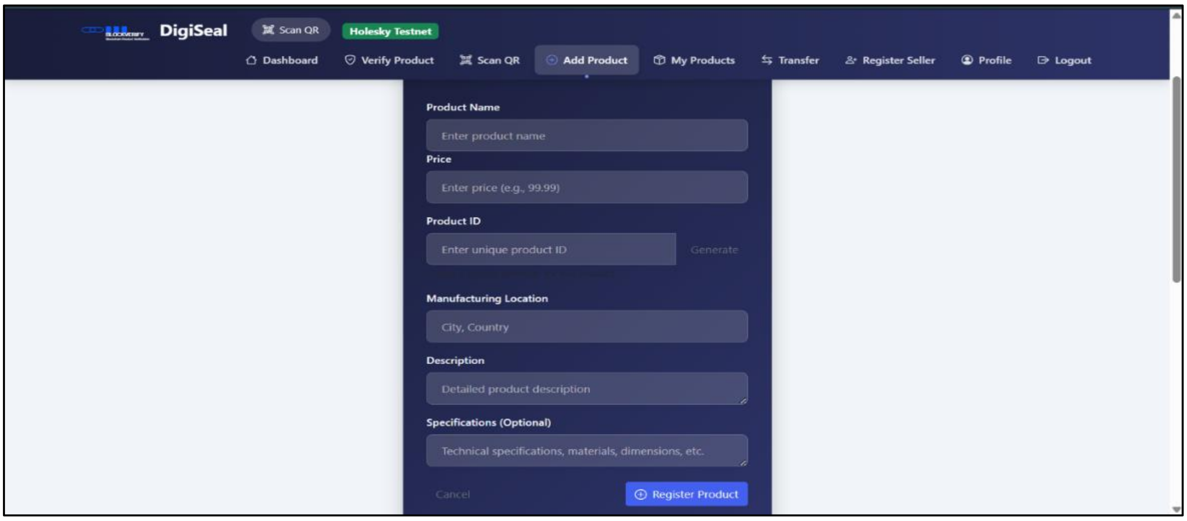

Figure 13 Add Product Page

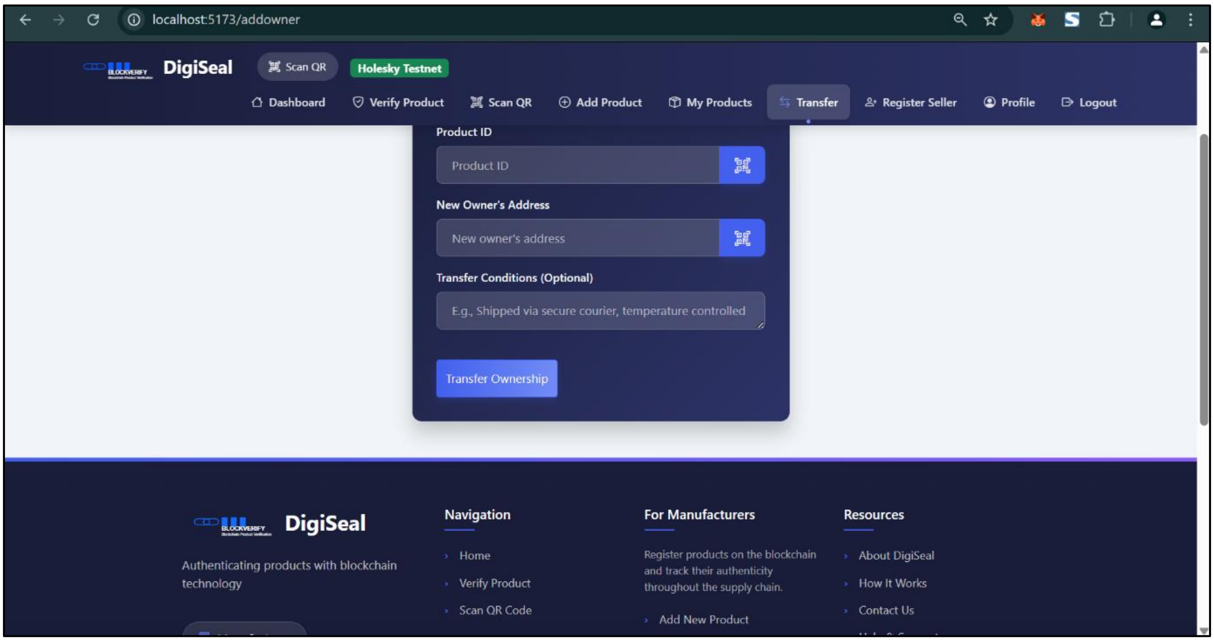

Figure 14 Transfer Ownership Page

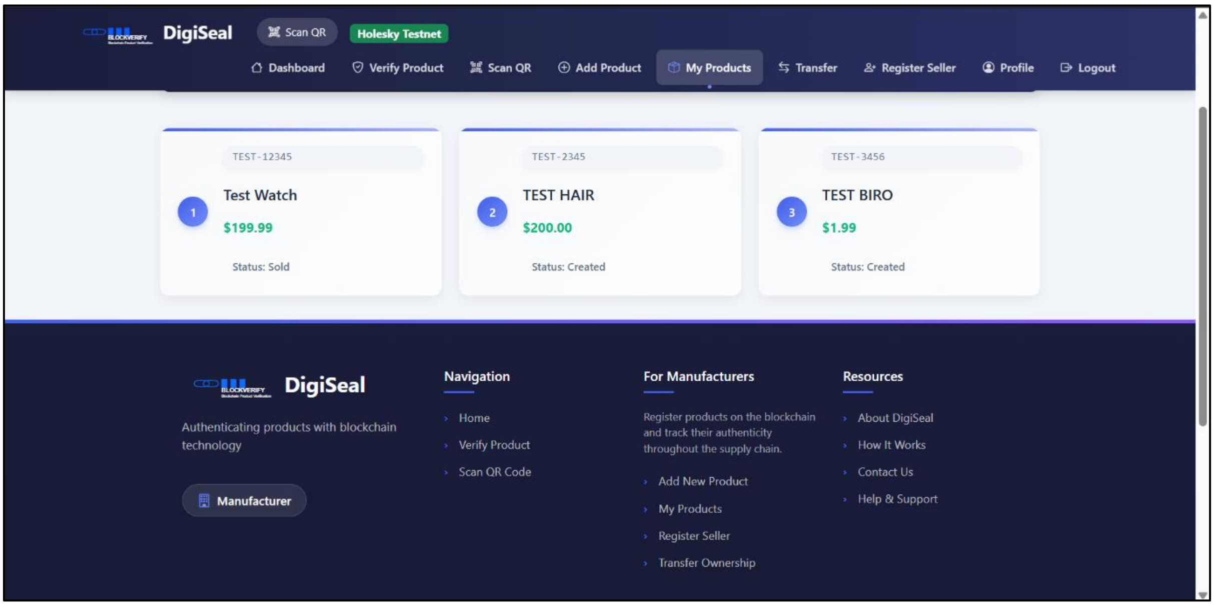

Figure 15 My Product Page

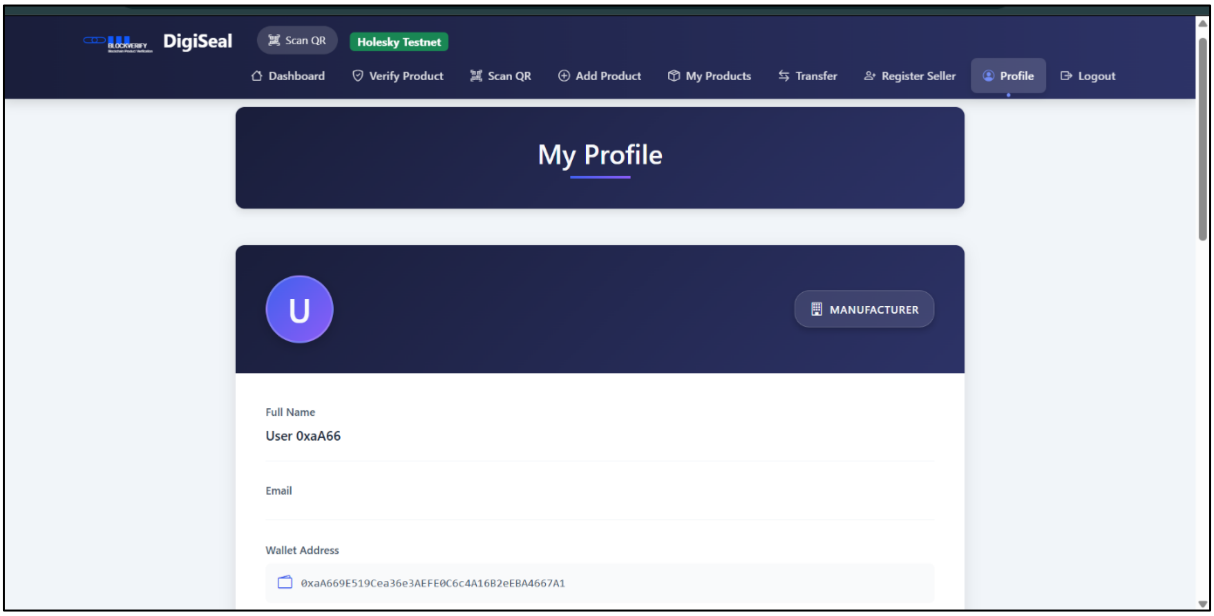

Figure 16 Profile Page

6. Discussion of findings

Implementation and testing of the Digi Seal system demonstrated that blockchain technology had the capability to efficiently address the problem of authenticating fraudulent products. Through its simple-to-use React front end, robust Node.js and Express.js based backend API, and secure Ethereum smart contracts, Digi Seal was able to successfully implement key features such as product registration, ownership transfer, verification, and counterfeiting reporting. These results support Slapdash (2023) claims that blockchain decentralization and immutability make it an efficient tool in securing product supply chains and preventing malicious transactions.

Unit testing, integration testing, and system testing all validated the system's reliability, performance, and security. Smart contracts authored and deployed on Solidity ensured the integrity of data when a transaction took place and allowed for product provenance creation on blockchain. This concurs with Kostas et al. (2023), who elucidated that the use of ERC-721 tokens and smart contracts enhances traceability of products and does away with duplications. Employment of cryptographic identifiers and keeping in place real-time verification processes provided consumers with an open, trustworthy system, seconding Trautmann et al. (2024) arguments that blockchain can enhance customers' trust through tamper-proofed records.

Despite successful deployment of the system, implementation was not straightforward. Scalability was a challenge, especially with growing quantities of transactions and data for registered products. This is in line with fears by Liu et al. (2024), who clarified that Ethereum transaction costs and latency have the capacity to degrade performance in high-volume environments. Digi Seal addressed this with the use of gas optimization and off-chain storage of supplemental data to optimize efficiency while ensuring security.

User interaction was another prominent aspect. The system would make it simple to use blockchain complexity and possess a simple-to-use interface for consumers, manufacturers, and sellers. Song et al. (2022) noted that user acceptance will largely rely on perceived ease of use and access to the system. Digi Seal's design made this principle simple, making blockchain interactions simple by simple to do things like form submission and QR code scanning.

Overall, Digi Seal's results affirm the emerging literature in favor of the implementation of blockchain for anti-counterfeiting systems. With incremental development, constant feedback, and incremental testing, not only did Digi Seal achieve its technical goals but also effectively demonstrated the applied feasibility of blockchain for protecting product integrity along digital supply chains.

7. Conclusion

The innovation and successful pilot of the Digi Seal system confirms real-world applications of blockchain technology to address the problem of counterfeit products, like in the gadget sector. With the use of Ethereum smart contracts, Digi Seal enables product registration, ownership transfer, and verification to happen in a safe and tamper-proof environment. The platform offers an end-to-end solution by packaging a secure back end, responsive front end, and blockchain integration that makes the tracking of products highly accurate and authenticates in real-time.

Digi Seal has a simple, user-friendly system that allows manufacturers, retailers, and purchasers access to the system without having higher technical know-how. It is easy to verify genuineness of a product through QR code scan or inputting product ID, which is convenient. It gives customers greater confidence, guarantees traceability along the supply chain, and protects against loss of brand reputation.

The system was tested strenuously at multiple layers to ensure its performance, security, and reliability. The testing demonstrated that Digi Seal is effective under diverse usage patterns and user conditions. Evidence confirms the use of blockchain for product authentication and approves that such systems can be made practically effective in practical applications. Digi Seal demonstrates the possibility of using sophisticated technologies against counterfeiting and creates a scalable path for industrial uptake.

Recommendations

To enhance the functionality and adoption of the Digi Seal system, it is recommended to integrate it with existing supply chain management systems to streamline product tracking and data flow. Expanding compatibility to include other blockchain platforms such as Hyperledger and EOS would allow for broader industry use and flexibility. Developing a mobile application would increase user accessibility and convenience. Collaboration with regulatory bodies is required in order to encourage adoption and establish industry standards. Periodic checks of security measures and modifying them for reacting to evolving threats have to be conducted. Educating users and conducting awareness programs are also essential to promote confidence and global acceptance of the platform. Finally, consistent efforts need to be put in toward enhancing the scalability and performance of the system for hosting more users and transactions.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alkhateeb, A., Catal, C., Kar, G., and Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. Sensors, 22(4), 1304.

[2] Appelbaum, D., Cohen, E., Kinory, E., and Stein Smith, S. (2022). Impediments to blockchain adoption. Journal of Emerging Technologies in Accounting, 19(2), 199-210.

[3] Bello, A., Abdulraheem, A. A., Afolabi, O. P., Aka, A., and Gbenga, P. O. (2024). Assessing the underlying factors affecting trust and transparency in the construction industry: a mixed method approach. Construction Economics and Building, 24(1-2), 9-28.

[4] Dong, S., Abbas, K., Li, M., and Kamruzzaman, J. (2023). Blockchain technology and application: an overview. PeerJ Computer Science, 9, e1705.

[5] Duan, K., Onyeaka, H., and Pang, G. (2024). Leveraging blockchain to tackle food fraud: Innovations and obstacles. Journal of Agriculture and Food Research, 101429.

[6] Gugała, Ł., Łaba, K., and Dul, M. (2023). Protecting web applications from authentication attacks. Advances in Web Development Journal, 1.

[7] Jung, J. W., Islam, M. M., and In, H. P. (2024). Proof of Work with Random Selection (PoWR): An Energy Saving Consensus Algorithm with Proof of Work and the Random Selection Function. Sustainability, 16(21), 9342.

[8] Kitsantas, T. (2022). Exploring blockchain technology and enterprise resource planning system: Business and technical aspects, current problems, and future perspectives. Sustainability, 14(13), 7633.

[9] Koustas, S. G., Jalowski, M., Reichenstein, T., and Oks, S. J. (2023). A blockchain-based IIoT traceability system: ERC-721 tokens for Industry 4.0. Procedia CIRP, 120, 1280-1285.

[10] Lall, M. M. (2023). IN BLOCKCHAIN WE TRUST? The examination of an anti-counterfeiting solution (Doctoral dissertation, City, University of London).

[11] Lasla, N., Al-Sahan, L., Abdallah, M., and Younis, M. (2022). Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. Computer Networks, 214, 109118.

[12] Liu, Y., He, J., Li, X., Chen, J., Liu, X., Peng, S., and Wang, Y. (2024). An overview of blockchain smart contract execution mechanism. Journal of Industrial Information Integration, 100674.

[13] Lukacs, M., Toth, F., Horvath, R., Solymos, G., Alpár, B., Varga, P., and Friedrich, L. (2025). Advanced digital solutions for food traceability: enhancing origin, quality, and safety through NIRS, RFID, Blockchain, and IoT. Journal of Sensor and Actuator Networks, 14(1), 21.

[14] Munyao, S. M. (2022). A Blockchain-based Drug Traceability Solution: a Case of Drug Counterfeiting in the Pharmaceutical Industry (Doctoral dissertation, university of nairobi).

[15] Oates, N. L. (2022). Blockchain from farm to fork-a new business model for tracing local South African market food supply chains using blockchain technology.

[16] Razi, Q., Devrani, A., Abhyankar, H., Chalapathi, G. S. S., Hassija, V., and Guizani, M. (2023). Non-fungible tokens (NFTs)—Survey of current applications, evolution, and future directions. IEEE Open Journal of the Communications Society, 5, 2765-2791.

[17] Selvaprabhu, P. (2023). An examination of distributed and decentralized systems for trustworthy control of supply chains. IEEE Access, 11, 137025-137052.

[18] Singh, S., and Kesari, K. (2023). The Ustr Special Report 301: Analyzing Intellectual Property Disputes And Counterfeit Goods In Asian Countries (Working Paper, 2023).

[19] Song, Y., Yang, Y., and Cheng, P. (2022). The investigation of adoption of voice-user interface (VUI) in smart home systems among Chinese older adults. Sensors, 22(4), 1614.

[20] Talwandi, N. S., Khare, S., and Thakur, P. (2025). Revolutionizing Pharmaceuticals: Harnessing Blockchain for Industry Solutions. Blockchain-Enabled Solutions for the Pharmaceutical Industry, 19-40.

[21] Toorajipour, R., Oghazi, P., Sohrabpour, V., Patel, P. C., and Mostaghel, R. (2022). Block by block: A blockchain-based peer-to-peer business transaction for international trade. Technological Forecasting and Social Change, 180, 121714.

[22] Trautmann, L., Hübner, T., and Lasch, R. (2024). Blockchain concept to combat drug counterfeiting by increasing supply chain visibility. International Journal of Logistics Research and Applications, 27(6), 959-985.

[23] Ursavaş, Ö. F. (2022). Technology acceptance model: History, theory, and application. In Conducting technology acceptance research in education: Theory, models, implementation, and analysis (pp. 57-91). Cham: Springer International Publishing.

[24] Zhou, L., Diro, A., Saini, A., Kaisar, S., and Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, 103678.