Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA
© Creative Research Publishers
Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Devising an Enhanced Blockchain-Driven Fake Product Identification System

Nwaocha Vivian O.
Department of Computer Science
National Open University of Nigeria
Abuja, Nigeria
E-mail:
Phone:

ABSTRACT

An increasingly pervasive issue affecting multiple industries universally, is the illicit production and distribution of counterfeit goods. This pose significant economic and health risks, costing legitimate businesses billions of dollars annually and endangering consumer safety. Conventional product authentication techniques are prone to manipulation and lack real-time verification. This study presents an enhnaced Block-Driven Fake Product Identification System, as well as Interplanetary File System as the database. The system provides secure product registration, QR code generation, and consumer verification, enabling product owners to authenticate their items while affording consumers the opportunity to scan QR codes or manually enter product IDs to verify authenticity of products. MetaMask authentication ensures that only verified product owners can register products. The system's architecture emphasizes security, decentralization, and transparency, preventing counterfeiters from tampering with product details. The results of the study demonstrate that blockchain-based product verification enhances trust, reduces counterfeiting, and improves supply chain security. The study equally presents recommendations for future enhancement of the work.

Keywords: Security, Blockchain-Driven, Fake Products, Identification System, Supply Chain

Nwaocha, V.O. (2023): Devising an Enhanced Blockchain-Driven Fake Product Identification System. Journal of Advances in Mathematical & Computational Science. Vol. 11, No. 3. Pp 89-104. Available online at www.isteams.net/mathematics-computationaljournal. dx.doi.org/10.22624/AIMS/MATHS/V11N3P6

1. INTRODUCTION

The illicit production and distribution of counterfeit goods pose significant economic and health risks, costing legitimate businesses billions of dollars annually and endangering consumer safety globally. Typically, counterfeit pharmaceuticals, can result in severe health consequences, while fake electronics and automotive parts may lead to hazardous failures (Sharma et al., 2021). The World Health Organization (WHO) has reported that counterfeit drugs alone account for nearly 10% of global pharmaceutical trade, exacerbating public health crises. The rise of global supply chains and e-commerce platforms has further amplified this challenge, making it easier for counterfeiters to infiltrate legitimate markets. Traditional anti-counterfeiting measures, such as holograms, barcodes, and centralized databases, have proven to be inadequate in mitigating these risks due to their susceptibility to tampering, lack of real-time traceability, and dependency on intermediaries.

On the other hand, blockchain technology has emerged as a groundbreaking solution to counterfeiting by offering a decentralized, immutable, and transparent ledger system. Initially designed as the underlying technology for cryptocurrencies such as Bitcoin, blockchain has since evolved into a versatile tool applicable across various sectors, including supply chain management, healthcare, and the Internet of Things (IoT). Unlike traditional centralized databases, blockchain eliminates single points of failure by distributing data across multiple nodes, making it resistant to tampering and unauthorized modifications. Furthermore, blockchain's immutability ensures that once data is recorded, it cannot be altered, thereby providing a reliable mechanism for product authentication.

A key component enhancing blockchain’s utility in anti-counterfeiting efforts is the use of smart contracts. These self-executing agreements are encoded onto the blockchain and automatically enforce predetermined rules without requiring intermediaries (Banerjee et al., 2023). When applied to product authentication, smart contracts can automate verification processes, enhance trust, and reduce manual intervention. Additionally, advancements in IoT technology have further strengthened blockchain-based anti-counterfeiting systems. IoT-enabled sensors can collect real-time data on product movement and status, enabling seamless tracking across supply chains (Vangala et al., 2021). Therefore, this study aims to develop an enhanced blockchain-driven counterfeit product identification system to address existing gaps in anti-counterfeiting frameworks and enhance consumer confidence.

1.1. Statement of Problem

Existing product authentication systems face several critical challenges that limit their effectiveness in combating counterfeit goods. Most conventional anti-counterfeiting measures rely on centralized databases managed by a single entity. These databases are prone to single-point failures, unauthorized access, and data breaches. When an attacker gains control over the central system, they can manipulate records, making counterfeit goods appear genuine (Sharma et al., 2021). Additionally, centralized systems often lack mechanisms for independent verification, forcing consumers and businesses to trust intermediaries without transparent validation processes. Other challenges include lack of transparency. Current authentication techniques do not offer consumers direct access to product verification data. Instead, verification is often conducted by manufacturers or third-party agencies, making it difficult for end-users to independently confirm authenticity. This opacity fosters distrust and allows counterfeit goods to infiltrate legitimate supply chains. Furthermore, inefficiencies in manual verification processes result in delays, increasing the risk of counterfeit products reaching consumers before detection. Traditional systems also lack robust traceability features, making it difficult to track products from manufacturing to end-user delivery in real time.

Vulnerability to tampering is another pressing issue. Many existing authentication methods, such as holograms and barcodes, can be easily replicated or altered. Fraudsters continuously develop sophisticated techniques to bypass security measures, rendering traditional anti-counterfeiting tools ineffective (Unal et al., 2020). These limitations necessitate a more robust, decentralized, and tamper-proof solution that ensures end-to-end traceability and fosters consumer confidence.

1.32 Aim and Objectives

Aim: To develop an enhnaced blockchain-driven system for authenticating products and mitigating counterfeiting.

Objectives:

1. To design a decentralized architecture integrating blockchain and IoT for real-time product tracking.
2. To implement smart contracts for automated verification and audit trails.
3. To ensure data immutability and transparency in supply chain transactions.
4. To evaluate the system's scalability, security, and usability.

1.3. Significance of the Study

This study is significant as it provides an innovative approach to mitigating the growing threat of counterfeit products. By leveraging blockchain's decentralized framework, the proposed system offers an advanced authentication mechanism that enhances transparency and reduces dependency on intermediaries. Consumers will be able to independently verify product authenticity, thereby fostering greater trust in the market. Businesses, particularly those in industries such as pharmaceuticals, luxury goods, and agriculture, will benefit from reduced financial losses due to counterfeit goods. Furthermore, by integrating IoT devices for real-time data collection and smart contracts for automated verification, this research contributes to the advancement of blockchain applications in anti-counterfeiting. It also aligns with the Sustainable Development Goals (SDGs) related to ethical consumption and industry innovation by promoting transparency and accountability in global supply chains (Kampan et al., 2022).

1.4. Scope of Study

This research focuses on developing an enhanced blockchain-driven authentication system specifically for consumer goods. The study emphasizes supply chain traceability and end-user verification, incorporating QR codes for real-time data input, Ethereum-based smart contracts for logic execution, and a private blockchain network for secure data storage. Testing will be conducted through simulated real-world scenarios, including product registration, distribution tracking, and consumer verification. The study does not cover financial transactions or non-IoT-based verification methods.

2. REVIEW OF RELATED WORKS

Khan & Salah (2018) provide a comprehensive review of blockchain solutions in IoT security, including its potential in healthcare applications. The paper highlights how blockchain can secure IoT-based medical devices, such as heart rate monitors, by ensuring data integrity and reducing vulnerabilities to cyberattacks.

A notable strength of this study is its systematic categorization of IoT security issues, which offers a broad perspective on potential threats. However, a limitation is the lack of experimental validation of blockchain's effectiveness in real-world heart rate monitoring systems, leaving open questions about its implementation feasibility in resource-constrained medical devices. Khatoon (2020) explores blockchain-based smart contracts for healthcare management, with a focus on secure medical data exchange. This work is highly relevant to heart rate monitoring systems, as it proposes a blockchain-based framework to ensure the secure transfer and storage of biometric health data. A key strength is the practical implementation of smart contract-based medical workflows, demonstrating feasibility. However, a significant drawback is the potential scalability issue, as the blockchain's transaction processing speed may hinder real-time heart rate monitoring applications that require low-latency responses.

Esposito et al. (2018) examine blockchain's role in enhancing the security and privacy of cloud-based healthcare data. Their discussion on integrating blockchain with cloud-based heart rate monitoring systems presents a promising approach to data protection and real-time accessibility. The study effectively outlines security challenges in conventional cloud-based health data storage and offers blockchain as a viable alternative. Nonetheless, the paper lacks a detailed discussion on energy efficiency, an essential factor for wearable heart rate monitors, which often operate on limited battery life. Sharma et al. (2020) analyze the potential of blockchain and smart contracts in the Internet of Medical Things (IoMT), particularly in e-healthcare applications. Their proposed architecture enhances the security and interoperability of connected medical devices, including heart rate monitors. A significant strength of this work is the inclusion of performance metrics such as packet delivery ratio and energy efficiency, making it highly applicable for real-world deployment. However, the study does not address regulatory challenges, such as compliance with HIPAA or GDPR, which are critical for the adoption of blockchain in heart rate monitoring.

Wang et al. (2019) present a systematic review of blockchain-enabled smart contracts, outlining their architecture and applications in various industries, including healthcare. The study provides a structured framework for integrating smart contracts into heart rate monitoring systems, ensuring data authenticity and reducing reliance on centralized authorities. While the paper offers a solid theoretical foundation, it does not provide experimental or simulation-based evaluations, limiting its practical applicability for developers and researchers working on real-world heart rate monitoring solutions. Khan et al. (2021) conduct a comprehensive survey on blockchain-enabled smart contracts, discussing their applications and challenges. While the paper primarily focuses on financial and legal aspects, it also highlights the potential for healthcare integration, including heart rate monitoring. The strength of this study lies in its detailed taxonomy of smart contract applications, offering valuable insights for designing secure, automated heart rate monitoring solutions. However, a weakness is the lack of emphasis on latency and real-time data handling, which are crucial for continuous heart rate tracking.

Banerjee et al. (2023) critically analyze smart contract applications in blockchain technology. Their discussion on automation and decentralized data management is relevant to heart rate monitoring, as smart contracts could facilitate automated alerts for abnormal readings. The paper's strength is its extensive review of smart contract implementation over a decade. However, it falls short in discussing integration with wearable devices, an essential aspect of heart rate monitoring systems.

Sharma et al. (2021) propose a blockchain-based decentralized architecture for secure cloud storage. This work is relevant to heart rate monitoring systems since cloud storage is often used to manage large volumes of health data. A notable strength is the inclusion of an access control mechanism to ensure data integrity. However, a limitation is the lack of discussion on real-time data synchronization, which is crucial for continuous heart rate monitoring. Wang et al. (2021) focus on security enhancement technologies for smart contracts in blockchain. The paper's relevance to heart rate monitoring lies in its emphasis on privacy and secure transactions, which are necessary for transmitting biometric data. A key strength is its comparative analysis of security techniques. However, the study does not address the computational overhead of implementing these security features in lightweight, battery-operated heart rate monitors.

Unal et al. (2020) examine the policy specification and verification of blockchain-based financial transactions, with potential applications in healthcare. The paper discusses security measures that could be adapted for protecting heart rate monitoring data. The strength of this study is its structured approach to policy enforcement using smart contracts. However, it does not explore the feasibility of implementing these policies in resource-constrained IoT medical devices. Taherdoost (2023) reviews blockchain-based business models and discusses their implications for various industries, including healthcare. The study highlights the use of blockchain in managing secure transactions and medical records. The strength of this work is its analysis of long-term trends in blockchain adoption. However, it lacks specific technical details on how blockchain can be integrated with heart rate monitoring devices.

Deng et al. (2021) investigate the use of blockchain for e-commerce and propose a new framework for transaction verification. Their approach to decentralized data management is applicable to heart rate monitoring systems, where data privacy and security are critical. A major strength of this study is its optimization of resource allocation using blockchain. However, a limitation is the absence of a discussion on energy efficiency, which is crucial for wearable heart rate monitors. Christidis & Devetsikiotis (2016) explore the intersection of blockchain and the Internet of Things (IoT), a critical area for heart rate monitoring systems. The paper highlights blockchain's role in enabling secure device-to-device communication. Its strength lies in providing a structured framework for IoT-blockchain integration. However, a notable weakness is that it does not address latency concerns, which are crucial for real-time heart rate monitoring applications. Ante (2021) presents a bibliometric analysis of smart contracts in blockchain, identifying key research trends and intellectual structures. The study discusses smart contracts' role in automation, security, and decentralized applications, which are relevant to heart rate monitoring. A strength of this work is its identification of security vulnerabilities and solutions, providing a roadmap for securing heart rate data. However, the paper lacks empirical studies on real-world implementations, leaving its applicability to heart rate monitoring largely theoretical.

Atzori (2017) explores blockchain's impact on decentralized governance and data management, with indirect implications for healthcare applications. The study highlights how blockchain can enhance transparency and security in data transactions, which is crucial for heart rate monitoring systems. A key strength is its thorough discussion of decentralized decision-making models. However, the paper does not address the energy consumption of blockchain applications, a crucial factor for wearable medical devices.

Hasan & Salah (2018) propose a proof-of-delivery system using blockchain and smart contracts, ensuring secure digital asset transfers. While the study focuses on digital content, its security framework can be adapted for heart rate monitoring data transmission. A major strength is its implementation of Ethereum smart contracts to ensure data integrity. However, a limitation is the lack of discussion on real-time data processing, which is essential for continuous heart rate tracking.

Oliva et al. (2020) conduct an exploratory study on Ethereum smart contracts, analyzing their usage patterns and complexity. Their findings highlight the efficiency of smart contracts in managing transactions, which can be applied to securely recording heart rate data. The study's strength lies in its extensive dataset analysis, revealing common trends in smart contract development. However, it does not address privacy concerns specific to biometric data, which is a critical consideration for heart rate monitoring.

Philipp et al. (2019) investigate the use of blockchain and smart contracts in supply chain management, with indirect applications to healthcare. The paper discusses automation and cost reduction through decentralized systems, which could enhance efficiency in heart rate monitoring data management. A key strength is its focus on reducing dependency on centralized authorities. However, the study lacks a discussion on interoperability with existing medical systems, limiting its immediate application to healthcare.

Xuan et al. (2020) propose a blockchain-based incentive mechanism for data sharing, using game theory to encourage participation. This approach is relevant to heart rate monitoring, where secure and transparent data sharing between healthcare providers is essential. The study's strength is its integration of smart contracts to enforce participation rules. However, its weakness is the lack of discussion on real-time performance, which is crucial for continuous health monitoring applications.

Sharma et al. (2020) examine blockchain's role in the Internet of Medical Things (IoMT), proposing a decentralized architecture for secure medical device communication. Their work is directly relevant to heart rate monitoring systems, as it outlines security challenges and solutions. A major strength is the inclusion of performance metrics such as latency and energy efficiency. However, the study does not explore regulatory challenges, which are critical for real-world implementation in healthcare settings. Wang et al. (2019) present a systematic overview of blockchain-enabled smart contracts, discussing their architecture, applications, and future trends. Their research highlights potential use cases in healthcare, particularly in ensuring data authenticity for heart rate monitoring systems. The study's strength is its structured framework for integrating smart contracts with IoT devices. However, it lacks real-world case studies, making its findings more theoretical than practical for immediate adoption in heart rate monitoring.

2.1 Knowlage Gaps Identified

The integration of blockchain technology with the Internet of Things (IoT) presents numerous challenges, many of which remain underexplored, leaving critical knowledge gaps that hinder the full realization of its potential, particularly in counterfeit detection. One major gap is the lack of real-time data synchronization between IoT devices and blockchain networks. Many existing studies fail to address how QR codes can efficiently transmit and validate data on a blockchain without introducing delays, which are critical in applications such as supply chain tracking and counterfeit prevention (Khan et al., 2018).

The inability to achieve seamless synchronization often results in outdated or inconsistent records, reducing the effectiveness of blockchain-based verification. Another significant issue is scalability. Public blockchains, while secure and decentralized, suffer from low transaction throughput, making them unsuitable for high-frequency IoT transactions. Hybrid blockchain models, which could balance scalability and security, remain underexplored in the context of anti-counterfeiting applications (Yli-Huumo et al., 2016). Furthermore, regulatory frameworks for blockchain-based authentication are still in their infancy.

The absence of clear legal guidelines and standardized policies makes it difficult to implement blockchain solutions across different jurisdictions, creating barriers to international adoption and enforcement (Gatteschi et al., 2018). Without robust legal structures, blockchain's role in counterfeit detection remains legally ambiguous, limiting its practical deployment. Additionally, energy efficiency poses a critical challenge. Many blockchain networks rely on energy-intensive consensus mechanisms such as Proof-of-Work (PoW), which are unsuitable for resource-constrained IoT environments. Alternative mechanisms like Proof-of-Stake (PoS) or lightweight consensus protocols have been proposed, but their effectiveness in ensuring both security and efficiency for IoT applications is still an open research question (Khatoon, 2020). Addressing these gaps is crucial to enhancing the feasibility and effectiveness of IoT-blockchain integration for counterfeit detection.

3. RESEARCH METHODOLOGY

This study adopted the agile methodology in order to ensure an iterative, flexible, and user-centered approach to development.

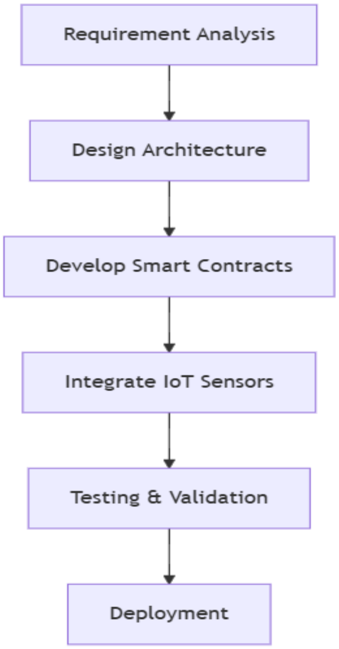


Figure 3.1 Methodology of proposed system

By employing this methodology, the development process is split into smaller, manageable cycles known as sprints, allowing for frequent evaluations and refinements. The methodology promotes collaboration among developers, stakeholders, and end-users to ensure that the system meets real-world requirements effectively.The system development adopts a structured flow, as illustrated in Figure 1.1: Each phase in this process ensures a smooth transition from conceptualization to implementation, reducing the risk of design flaws and improving overall system efficiency. Requirement analysis defines the functional and non-functional specifications. The design phase involves structuring the blockchain, smart contract logic, and IoT integration framework. Development follows, where Solidity smart contracts are coded, QR codes configured, and backend integration executed using Node.js. Testing and validation ensure system robustness, while deployment marks the transition to real-world application.

3.1 Analysis of the Existing System

Existing anti-counterfeiting systems primarily rely on centralized databases, making them highly vulnerable to cyberattacks, data tampering, and unauthorized modifications. The lack of a decentralized mechanism increases security risks, as a single breach can compromise the entire system (Sharma et al., 2021). Moreover, traditional QR-code-based authentication techniques have significant shortcomings. While they provide a quick method for verifying product information, they lack real-time updates and rely on databases that can be manipulated. Additionally, these systems do not offer a transparent audit trail, leaving consumers with limited means to verify authenticity independently.

3.2 Weaknesses of the Existing System

The existing system suffers from multiple limitations, including: single-point failure risks, No mechanism to detect data tampering, delayed counterfeit detection.

3.3 Analysis of the Proposed System

The proposed system leverages blockchain technology while retaining the use of QR codes to enhance security and ensure authenticity verification. Blockchain provides a decentralized and immutable ledger, reducing the risks associated with centralized systems. QR codes serve as an accessible and efficient interface for consumers to interact with the system. Each product is assigned a unique QR code, linking to a blockchain-registered digital certificate containing product details, ownership history, and transaction records. When scanned, the QR code triggers a smart contract that fetches the product's authenticity details from the blockchain. Unlike traditional QR-based authentication methods, this approach ensures real-time updates and tamper-proof verification. The integration of blockchain and QR codes enhances consumer trust by providing verifiable product information while ensuring scalability and ease of adoption. This hybrid approach effectively balances technological advancement with user accessibility, making it a practical solution for combating counterfeiting.

3.3.1 System Architecture

The system is designed using a hybrid blockchain approach, combining Ethereum for smart contract execution and Hyperledger for private transaction storage. This architecture leverages the strengths of both public and private blockchains to achieve a balance between transparency and confidentiality.

Ethereum, as a public blockchain, facilitates the execution of smart contracts that automate authentication processes and enforce business rules without the need for intermediaries. On the other hand, Hyperledger provides a permissioned environment where sensitive transactional data can be securely stored and accessed only by authorized parties. A key component of this system is the use of QR codes embedded within products. These QR codes capture real-time data on product movement, enabling continuous monitoring and verification of authenticity throughout the supply chain. When scanned, the QR code triggers the recording of a transaction on the blockchain, creating an immutable and transparent log of events. This approach not only deters counterfeit activities but also enhances consumer trust by providing verifiable product information. By integrating real-time data capture with blockchain's immutable ledger, the system ensures a robust mechanism for tracking and validating product provenance, thereby reinforcing the integrity of supply chains.

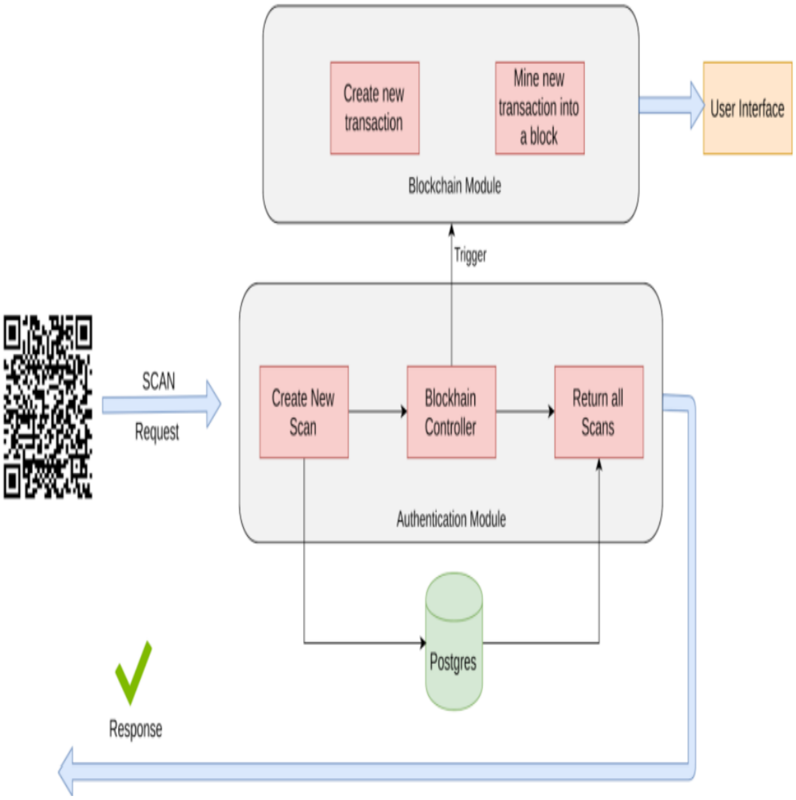


Figure 3.2: System Architecture of the Proposed System

3.3.2 Program Design of the Proposed System

The system's program design follows a structured process involving QR code scanning, blockchain interaction, and authenticity verification. The key components include smart contracts for transaction validation, a blockchain ledger for data integrity, and a user interface for seamless interaction. Below are the PlantUML diagrams illustrating different aspects of the system:

Sequence Diagram:

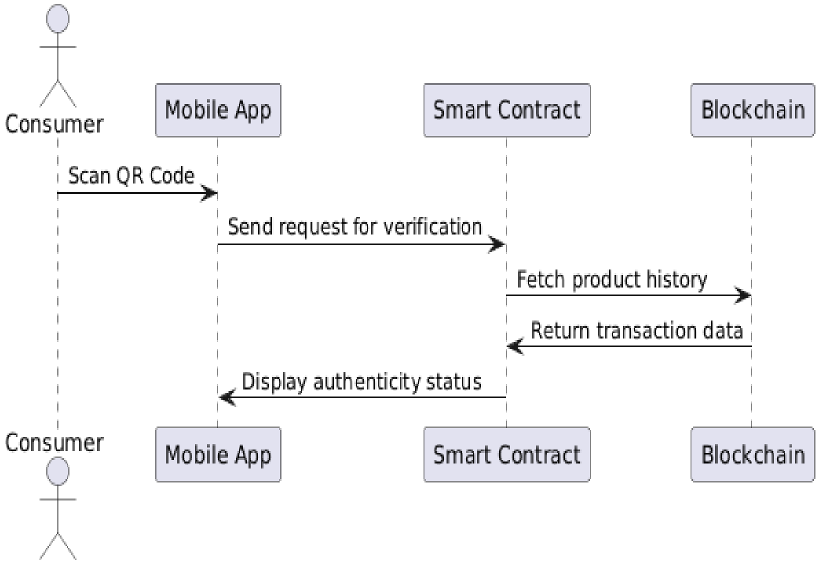
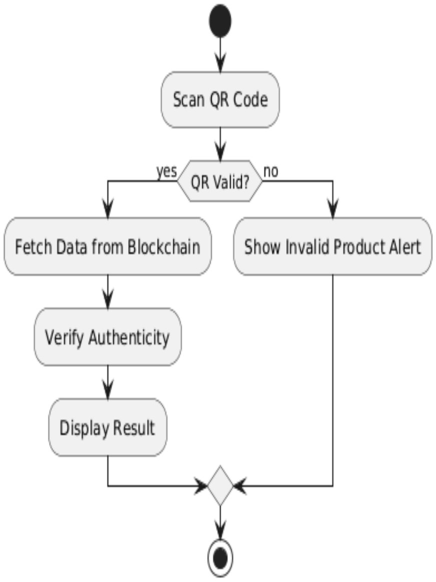


Figure 3.3: Sequence Diagram:

This sequence diagram outlines the flow from scanning a QR code to receiving authentication status. The consumer scans the QR code, triggering a smart contract to fetch data from the blockchain, which is then displayed via the mobile app.

Activity Diagram:



Fg 3.4: Activity Diagram

The activity diagram details the process flow when a consumer scans a QR code. If valid, blockchain data is retrieved and verified; otherwise, an alert is displayed.

3.3.3 Software Development Approach

The development of the proposed system employs a modular architecture using Solidity for smart contract development, Node.js for backend integration, and React.js for the user interface. The decentralized nature of blockchain ensures reliability, while the modularity of the system allows for scalability and ease of maintenance.

3.3.4 Data Collection and Analysis

The system collects data from QR code embedded in products, which is then securely stored on the InterPlanetary File System (IPFS). IPFS offers decentralized data storage, enhancing system security and reliability. Analytical tools developed in Python process the collected data to provide insights into supply chain behavior, counterfeit detection trends, and system performance metrics. By leveraging a decentralized framework and integrating real-time IoT data, the proposed system offers a robust solution for counterfeit prevention, improving efficiency, security, and transparency in global supply chains.

4.PROGRAM MODULE SPECIFICATION

The system consists of several interdependent modules, each responsible for handling a specific functionality. These modules ensure the smooth execution of authentication, product registration, and verification processes. The main modules include:

1. Authentication Module: Handles MetaMask login and user authentication.
2. Product Registration Module: Allows product owners to add new products and store details in IPFS.
3. QR Code Generation Module: Generates unique QR codes for registered products.
4. Product Verification Module: Enables consumers to scan or manually enter product ID to verify authenticity.
5. Database Interaction Module: Manages read and write operations on IPFS for user and product data.

Each of these modules interacts through API endpoints, ensuring smooth communication between the frontend and backend.

4.1 Algorithm

The Fake Product Identification System follows a structured approach to register, generate QR codes, and verify products. The algorithm ensures that only registered products can be authenticated, preventing counterfeit entries.

Algorithm Description

The algorithm begins by authenticating the product owner through Metamask. Once authenticated, the system allows the user to register a product by entering details such as name, brand, serial number, and manufacture date. The system then stores this information in IPFS and generates a unique QR code based on the product’s unique identifier.

For verification, when a QR code is scanned or a product ID is manually entered, the system retrieves the product details from IPFS. If a matching product is found, the system confirms its authenticity. If the product is not found in the database, it is flagged as potentially counterfeit.

Pseudo-Code Representation

```
BEGIN
    DISPLAY "Connect to Metamask"
    IF User logs in successfully THEN
        STORE Wallet Address in IPFS and Local Storage
        REDIRECT to Dashboard
    ENDIF
    IF User selects "Register Product" THEN
        PROMPT User to enter Product Details
        GENERATE Unique Product ID
        STORE Product Details in IPFS
        GENERATE QR Code for Product
        DISPLAY "Product Registered Successfully"
    ENDIF
    IF Consumer selects "Verify Product" THEN
        PROMPT User to Scan QR Code OR Enter Product ID
        SEARCH IPFS for Matching Product
        IF Product Found THEN
            DISPLAY Product Details and "Authentic "
        ELSE
            DISPLAY "Product Not Found - Possible Counterfeit x"
        ENDIF
    ENDIF
END
```

This pseudo-code outlines the step-by-step process the system follows for authentication, product registration, QR code generation, and verification.

4.5 System Flowchart

The system flowchart provides a visual representation of the process flow, showing how different components interact in the Fake Product Identification System.

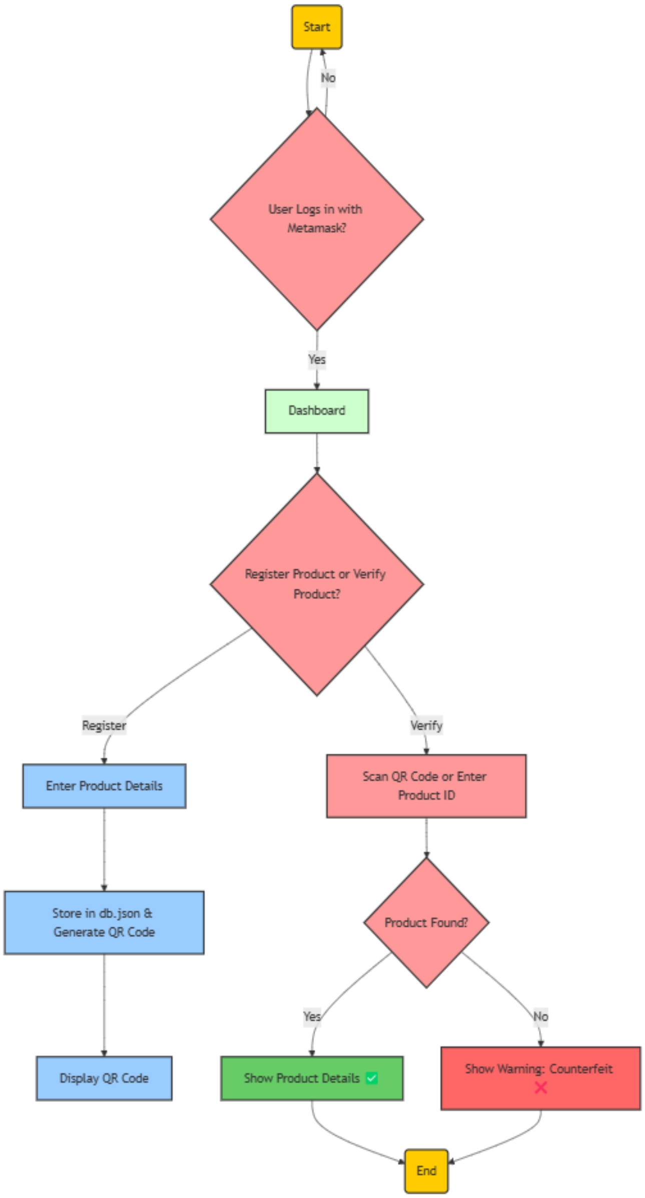

Start
No
User Logs in with Metamask?
Yes
Dashboard
Register Product or Verify Product?
Register
Verify
Enter Product Details
Store in db.json & Generate QR Code
Display QR Code
Scan QR Code or Enter Product ID
Product Found?
Yes
No
Show Product Details ✅
Show Warning: Counterfeit ❌
End

Figure 4.1: Flowchart of the system

5.1 Summary

The development of the enhanced Blockchain-Driven Fake Product Identification System sought to tackle the rising issue of counterfeit goods by providing a decentralized and transparent product verification solution. This system ensures that product owners can register their products securely, generate unique QR codes, and allow consumers to verify product authenticity before making a purchase. The system was developed using Node.js for the backend, React.js for the frontend, and JSON (IPFS) as the database. Metamask authentication was integrated to provide secure login for product owners, ensuring that only verified individuals could register products. The QR code generation feature allows each product to be assigned a unique scannable code, which links to the product details stored in IPFS. Consumers can then scan the QR code or manually enter the product ID on the verification page to check if a product is authentic or counterfeit. The system was designed with security and efficiency in mind, incorporating tamper-proof QR codes, local storage authentication, and real-time data retrieval. The user interface was built to be simple and intuitive, ensuring ease of use for both product owners and consumers. Additionally, a structured training program, detailed documentation, and a gradual changeover strategy were implemented to ensure smooth adoption of the system.

The system's modular approach allows for future scalability, making it possible to integrate blockchain-based smart contracts if resources become available. By providing a reliable, decentralized, and user-friendly platform for product authentication, this system serves as an effective solution for combating counterfeit goods and ensuring consumer trust in product authenticity.

5.2 Conclusion

In conclusion, the enhanced Blockchain-Driven Fake Product Identification System successfully addresses the challenge of product counterfeiting by leveraging blockchain-based authentication, QR code verification, and a decentralized database approach. Unlike traditional centralized verification methods, which are prone to data manipulation and security breaches, this system ensures tamper-proof product registration and authentication using MetaMask login and JSON-based storage. The integration of QR codes as a means of product verification simplifies the authentication process for consumers while providing a scalable and efficient method for product owners to register and track their inventory. The system also promotes transparency and trust between manufacturers, retailers, and consumers, making it an essential tool for industries affected by counterfeiting.

5.3. Application Areas

The Fake Product Identification System can be applied across various industries that suffer from counterfeiting and product authenticity challenges namely: pharmaceutical, fashion, automobile industry, agricultural and food industries. The blockchain-driven anti-counterfeiting system offers several benefits, including: real-time authentication, reduced operational cost, enhanced consumer trust.

5.4 Suggestions for Further Research

While the system established offers a solid basis for counterfeit product verification, future improvements could include expanding the database structure to support larger-scale deployments and enhanced security mechanisms to further strengthen the system’s effectiveness. To this end, future research should focus on incorporating smart contracts to facilitate automated product verification on a blockchain network. Future enhancement of the system should explored by employing the InterPlanetary File System or decentralized databases to improve scalability and security. The integration of machine-learning to analyze product verification patterns and predict potential counterfeit trends based on user queries and scanned QR codes. should equally be explored.

REFERENCES

1. Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. Telematics and Informatics, 57, Article 101519. https://doi.org/10.1016/J.TELE.2020.101519
2. Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5
3. Banerjee, S., Bouzefrane, S., & Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. Information, 14(2), Article 117. https://doi.org/10.3390/INFO14020117
4. Bodó, B., Gervais, D., & Quintais, J. P. (2018). Blockchain and smart contracts: The missing link in copyright licensing? International Journal of Law and Information Technology, 26(4), 311–336. https://doi.org/10.1093/IJLIT/EAY014
5. Deng, S., Cheng, G., Zhao, H., Gao, H., & Yin, J. (2021). Incentive-driven computation offloading in blockchain-enabled e-commerce. ACM Transactions on Internet Technology, 21(1), Article 43. https://doi.org/10.1145/3397160
6. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? Future Internet, 10(2), Article 20. https://doi.org/10.3390/FI10020020
7. Hasan, H. R., & Salah, K. (2018). Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access, 6, 65439–65448. https://doi.org/10.1109/ACCESS.2018.2876971
8. Kampan, K., Tsusaka, T. W., & Anal, A. K. (2022). Adoption of blockchain technology for enhanced traceability of livestock-based products. Sustainability (Switzerland), 14(20), Article 13148. https://doi.org/10.3390/su142013148
9. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/J.FUTURE.2017.11.022
10. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Networking and Applications, 14(5), 2901–2925. https://doi.org/10.1007/S12083-021-01127-0
11. Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. Electronics (Switzerland), 9(1), Article 94. https://doi.org/10.3390/ELECTRONICS9010094
12. Oad, A., Razaque, A., Tolemyssov, A., Alotaibi, M., Alotaibi, B., & Zhao, C. (2021). Blockchain-enabled transaction scanning method for money laundering detection. Electronics (Switzerland), 10(15), Article 1766. https://doi.org/10.3390/ELECTRONICS10151766
13. Oliva, G. A., Hassan, A. E., & Jiang, Z. M. (2020). An exploratory study of smart contracts in the Ethereum blockchain platform. Empirical Software Engineering, 25(3), 1864–1904. https://doi.org/10.1007/S10664-019-09796-5
14. Pănescu, A. T., & Manta, V. (2018). Smart contracts for research data rights management over the Ethereum blockchain network. Science and Technology Libraries, 37(3), 235–245. https://doi.org/10.1080/0194262X.2018.1474838

15. Philipp, R., Prause, G., & Gerlitz, L. (2019). Blockchain and smart contracts for entrepreneurial collaboration in maritime supply chains. Transport and Telecommunication, 20(4), 365–378. https://doi.org/10.2478/TTJ-2019-0030
16. Sharma, P., Jindal, R., & Borah, M. D. (2021). Blockchain-based decentralized architecture for cloud storage system. Journal of Information Security and Applications, 62, Article 102970. https://doi.org/10.1016/J.JISA.2021.102970
17. Taherdoost, H. (2023). Smart contracts in blockchain technology: A critical review. Information, 14(2), Article 117. https://doi.org/10.3390/INFO14020117
18. Unal, D., Hammoudeh, M., & Kiraz, M. S. (2020). Policy specification and verification for blockchain and smart contracts in 5G networks. ICT Express, 6(1), 43–47. https://doi.org/10.1016/J.ICTE.2019.07.002
19. Wang, Y., He, J., Zhu, N., Yi, Y., Zhang, Q., Song, H., & Xue, R. (2021). Security enhancement technologies for smart contracts in the blockchain: A survey. Transactions on Emerging Telecommunications Technologies, 32(12), Article e4341. https://doi.org/10.1002/ETT.4341
20. Xuan, S., Zheng, L., Chung, I., Wang, W., Man, D., Du, X., & Guizani, M. (2020). An incentive mechanism for data sharing based on blockchain with smart contracts. Computers and Electrical Engineering, 83, Article 106587. https://doi.org/10.1016/J.COMPELECENG.2020.106587
21. Zhuansun, F., Chen, J., Chen, W., & Sun, Y. (2021). The mechanism of evolution and balance for e-commerce ecosystem under blockchain. Scientific Programming, 2021, Article 5984306. https://doi.org/10.1155/2021/5984306