

PROFESSIONAL TRAINING REPORT - II

entitled

FAKE PRODUCT IDENTIFICATION USING BLOCKCHAIN

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering
with specialization in Blockchain Technology
by

Gajulapalli SubbaReddy [Reg.no:41613024]



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY -1 UNIVERSITY BY UGC

**Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

MAY 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Professional Training Report is the bonafide work of Mr. GAJULAPALLI SUBBAREDDY (41613024) who carried out the project entitled "FAKE PRODUCT IDENTIFICATION" under my supervision from January 2024 to May 2024.

Internal Guide

Ms. Lekshmi S Raveendran M.Tech.,

Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.

Submitted for Viva voce Examination held on

7/5/24

Internal Examiner

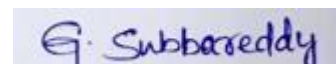
External Examiner

DECLARATION

I, **GAJULAPALLI SUBBAREDDY [Reg.no:41613024]**, hereby declare that the Professional Training Report-II entitled “**FAKE PRODUCT IDENTIFICATION**” done by me under the guidance of **Ms. Lekshmi S Raveendran M.Tech.**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with specialization in Blockchain Technology.

DATE: 07/05/2024

PLACE: Chennai

A rectangular box containing a handwritten signature in blue ink that reads "G. Subbareddy".

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D., Dean**, School of Computing **Dr. S. Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Ms. Lekshmi S Raveendran M.Tech.**, for his/her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 Professional Training.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

COURSE CERTIFICATE

betX

B12M2 TECHNOLOGIES PVT. LTD.

CERTIFICATE OF INTERNSHIP

This Certificate Awarded To

Gajulapalli Subbareddy

For completing an internship program in Blockchain from Feb 10, 2023 to
April 10, 2023 with an astonishing performance



Bhushan Sonar
Co-founder & CEO



Shweta Shilwant
Tech Lead

ABSTRACT

Counterfeit products continue to threaten consumer safety, brand reputation, and economic stability in the global market. Addressing this pervasive challenge requires innovative approaches, and the integration of block chain technology and Python programming offers a promising solution. Abstract presents a comprehensive framework designed to detect and prevent counterfeit products by harnessing Python scripts within a block chain architecture. The proposed system capitalizes on block chain's inherent features of immutability and transparency to establish a decentralized ledger for product information. Each genuine product receives a unique identifier stored on the block chain, housing critical details like manufacturing origin and batch number. Python scripts play a pivotal role in interacting with the block chain network, facilitating real-time verification and validation of product authenticity. The integration of Python programming language enhances system flexibility, enabling the development of tailored verification algorithms, user interfaces, and analytical tools. Moreover, Python's extensive libraries and frameworks facilitate seamless integration with leading block chain protocols. Inherent transparency and immutability render blockchain an optimal platform for instilling trust and validating product authenticity. Within this framework, the concept of fake product identification leveraging blockchain technology entails harnessing its unique attributes to establish a tamper-resistant system for verifying product legitimacy across its entire lifecycle. By enrolling product details onto the blockchain during manufacturing and facilitating stakeholders' ability to authenticate this information throughout distribution and consumption phases, a substantial reduction in counterfeit prevalence can be achieved.

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	1
	1.1 Overview	
2	LITERATURE SURVEY	4
	2.1 survey	
3	REQUIREMENTS ANALYSIS	
	3.1 Objective	8
	3.2.1 Hardware Requirements	
3.23.2	3.2.2 Software Requirements	11
4	DESIGN DESCRIPTION OF PROPOSED PRODUCT	13
	4.1.1 Ideation Map/Architecture Diagram	15
	4.1.2 Various stages	15
4.1	4.1.3 Internal or Component design structure	17
	4.1.4 working principles	19
	4.2 4.2.1 Novelty of the Project	23
5	CONCLUSION	29
	REFERENCES	31
	APPENDIX	
	A. Research Paper	33
	B. Source Code	35

TABLE OF CONTENTS

LIST OF FIGURES

Figure No.	Figure Name	Page No.
1.	System Architecture	15
2.	Component Design Structure	17
3.	Working Principle	21

CHAPTER 1

INTRODUCTION

OVERVIEW

Counterfeit products represent a pervasive menace to consumers, enterprises, and global economies. Ranging from high-end fashion items to critical pharmaceuticals, the proliferation of counterfeit goods not only erodes consumer trust but also engenders significant health and safety hazards. Conventional countermeasures such as holographic labels and serialized codes have fallen short in thwarting the increasingly sophisticated tactics employed by counterfeiters. However, the emergence of blockchain technology presents a promising antidote to this escalating threat. Blockchain, the foundational technology underpinning cryptocurrencies like Bitcoin, functions as a decentralized ledger that securely records transactions in a transparent and immutable manner. Each transaction is cryptographically linked to the preceding one, forming an unalterable chain of blocks. This inherent transparency and immutability render blockchain an optimal platform for instilling trust and validating product authenticity. Within this framework, the concept of fake product identification leveraging blockchain technology entails harnessing its unique attributes to establish a tamper-resistant system for verifying product legitimacy across its entire lifecycle. By enrolling product details onto the blockchain during manufacturing and facilitating stakeholders' ability to authenticate this information throughout distribution and consumption phases, a substantial reduction in counterfeit prevalence can be achieved. By harnessing the capabilities of smart contracts, decentralized consensus mechanisms, and cryptographic hashing techniques, the aim is to craft a resilient and dependable solution. Such a solution empowers consumers to make well-informed purchasing decisions while affording manufacturers the means to safeguard their brands and reputations. However, the advent of blockchain technology heralds a promising avenue for addressing this pervasive issue, offering a secure, transparent, and immutable framework for product authentication. This project end to delve into the development of a blockchain-based fake product identification system utilizing Python. By harnessing the

distinctive attributes of blockchain technology, such as decentralization, cryptographic hashing, and the implementation of smart contracts, the objective is to establish an inviolable mechanism for validating product authenticity throughout the entire supply chain. Integral components of this system encompass product registration, seamless integration with blockchain technology, a user-friendly verification interface, the deployment of smart contracts, and the utilization of decentralized consensus mechanisms. The proposed system not only serves to empower consumers, furnishing them with the tools to make well-informed purchasing decisions, but also affords manufacturers the means to safeguard their brands and uphold their reputations. By fostering an environment characterized by trust and transparency in product transactions, this system contributes substantively to the reduction of counterfeit products and bolsters the integrity of global markets. In sum, this project exemplifies the potential of blockchain technology in combating the proliferation of counterfeit products, underscoring the pragmatic utility of Python in crafting innovative, blockchain-driven solutions tailored to address real world challenges with efficacy and precision.

In today's globalized market, counterfeit products threaten consumer safety, brand reputations, and legitimate businesses. Blockchain, a revolutionary technology, offers a powerful solution. It creates a shared, tamper-proof ledger that tracks each product's journey from manufacturing to sale. Consumers can verify authenticity using a smartphone app to scan unique product identifiers, ensuring transparency, security, and a future free of fakes. Fake product identification using blockchain is a revolutionary approach with the potential to significantly reduce counterfeiting. By leveraging transparency, security, and immutability, this technology fosters trust in the supply chain and empowers consumers to make informed purchasing decisions. While challenges like scalability and integration exist, ongoing advancements are paving the way for a future where blockchain becomes the cornerstone of a secure and reliable product ecosystem.

Blockchain can revolutionize product authentication by creating a unique digital identity for each product, linked securely to a shared public ledger. This digital ID can be embedded in a QR code or RFID tag, providing consumers with a convenient and secure way to access product information using a smartphone app. Manufacturers can record comprehensive product details on the blockchain, including materials, origin, production date, and batch numbers. As the product moves through the supply chain, each step can be documented with timestamps and location data, creating a transparent and verifiable history. This empowers consumers to make informed purchasing decisions by scanning the product's unique code and accessing the secure blockchain record, which provides detailed information about the product's journey, from raw materials to store shelves. Blockchain-based authentication offers several key benefits. Enhanced transparency allows consumers to gain trust by knowing exactly where their product came from and the path it took to reach them. This transparency can also address ethical sourcing concerns throughout the supply chain. The tamper-proof nature of blockchain makes it nearly impossible to counterfeit product IDs, as any attempt to alter the blockchain record would be immediately detected by the network. Real-time tracking of products through the supply chain improves efficiency, reduces inefficiencies, and identifies potential tampering. This can help businesses to optimize logistics, reduce shrinkage, and improve overall supply chain management. Finally, brands can leverage blockchain to build stronger relationships with consumers by providing transparency into their products and supply chains, fostering trust and loyalty with their customer base. Blockchain is a rapidly evolving technology with immense potential to combat counterfeiting, improve supply chain efficiency, and empower consumers to make informed choices. As the technology continues to develop, we can expect to see even more innovative applications of blockchain-based product authentication in the years to come.

CHAPTER 2

LITERATURE REVIEW

2.1 SURVEY

Search Academic Databases: Utilize academic databases like Google Scholar, IEEE Xplore, ACM Digital Library, and ScienceDirect to search for relevant research papers and literature reviews. Use keywords such as "fake product identification blockchain," "counterfeit goods blockchain," or "blockchain supply chain authentication."

Review Journal Articles: Look for recent journal articles that discuss the application of blockchain in combating counterfeit products. Focus on papers published in reputable journals related to supply chain management, cryptography, or blockchain technology.

Explore Conference Papers: Many conferences publish papers on emerging technologies and applications of blockchain. Search for conference proceedings in the field of computer science, information systems, or logistics.

Consult Books and Book Chapters: Books and book chapters related to blockchain technology and supply chain management may provide comprehensive overviews of the topic, including discussions on counterfeit detection.

5.Check Institutional Repositories: Some universities and research institutions maintain repositories of academic publications. Explore these repositories for theses, dissertations, and research papers on blockchain and supply chain security.

Read Literature Reviews Look specifically for literature reviews or survey articles that summarize existing research on blockchain-based counterfeit detection. These reviews can provide a broader understanding of the current state of research and identify key trends and challenges.

Evaluate Citations and References: Once you identify relevant papers, check their citations and references for additional sources that could be valuable for your literature review.

Consider Recent Publications: Focus on recent publications (within the last 5-10 years) to ensure that you are capturing the latest advancements and perspectives in the field.

Enhanced Transparency and Traceability: Newer research explores integrating blockchain with Internet-of-Things (IoT) sensors. Sensors embedded in products track their journey throughout the supply chain, providing real-time location and condition data on the blockchain. This allows for improved transparency and easier detection of tampering. (You can find relevant papers by searching for "blockchain IoT product traceability".)

AI and Machine Learning Integration: Some studies propose combining blockchain with AI and machine learning for more sophisticated counterfeit detection. AI algorithms can analyze product data (images, material composition) stored on the blockchain and identify inconsistencies that might indicate fakes. (Search for "blockchain AI anti-counterfeiting".)

Privacy Concerns and Permissioned Blockchains: As sensitive product data gets stored on the blockchain, privacy becomes a growing concern. Research is exploring permissioned blockchains where access is restricted to authorized participants in the supply chain, ensuring only relevant data is visible. (Look for papers on "permissioned blockchain product counterfeiting".)

Scalability and Efficiency: Implementing blockchain for large-scale supply chains requires addressing scalability and efficiency concerns. Studies are investigating techniques for optimizing blockchain architectures to handle high transaction volumes associated with product tracking. (Search for "scalable blockchain for product counterfeiting".).

Academic Databases: Search for research papers in databases like IEEE Xplore, ScienceDirect, ACM Digital Library using keywords like "blockchain," "counterfeit detection," "supply chain," "product traceability," "IoT," and "machine learning." Filter by publication date (2023-2024).

Conference Proceedings: Look for recent conferences on blockchain or supply chain management. Conference proceedings often contain cutting-edge research not yet published in journals. (<https://www.acm.org/conferences>)

Pre-print Repositories: Explore pre-print repositories like arXiv for the latest research findings that might not be formally published yet. (arXiv.org).

"An Exploration of Blockchain Technology for Anti-Counterfeiting in the Pharmaceutical Supply Chain: A Systematic Literature Review" This survey examines how blockchain can be used to track and verify the authenticity of pharmaceuticals throughout the supply chain, helping to reduce counterfeiting and ensure patient safety.

"Blockchain Applications in Supply Chain Management: A Literature Review" This broader survey explores the various applications of blockchain technology in supply chain management, including its potential to improve transparency, traceability, and security. Anti-counterfeiting is a key area of focus within this context.

"A Survey on the Application of Blockchain in Anti-Counterfeiting" This survey provides a comprehensive overview of how blockchain can be used to combat counterfeiting across a wide range of industries, from pharmaceuticals and luxury goods to food and beverages.

"Blockchain for Food Traceability: A Survey of Applications and Challenges" This survey explores the use of blockchain to track food products from farm to fork, ensuring authenticity and safety. This can help to prevent counterfeit food products from entering the market.

"Combating Counterfeiting in the Luxury Fashion Industry Using Blockchain Technology: A Systematic Literature Review" This survey focuses specifically on the challenges of counterfeiting in the luxury fashion industry and how blockchain can be used to address them.

"A Survey on Blockchain Technology for Secure and Transparent E-Government Systems" This survey explores how blockchain can be used to improve the security and transparency of e-government systems. While not directly focused on anti-counterfeiting, blockchain can help to ensure the authenticity and integrity of government data and records.

"Blockchain for Secure and Trustworthy IoT Data Management: A Survey" This survey examines the use of blockchain to secure and manage data from Internet of Things (IoT) devices. Secure data management is essential for ensuring the authenticity and traceability of products in a blockchain-based supply chain.

"A Survey on Blockchain for Secure and Efficient Healthcare Data Management" This survey explores how blockchain can be used to securely and efficiently manage healthcare data. This can help to improve the accuracy and traceability of medical records, which can be essential for identifying and combating counterfeit pharmaceuticals.

"Blockchain for Digital Identity Management: A Survey" This survey examines the use of blockchain for digital identity management. Secure and trustworthy digital identities are essential for ensuring the legitimacy of participants in a blockchain-based system, which can help to prevent counterfeiting.

"Blockchain for Secure and Efficient E-Voting Systems: A Survey" This survey explores how blockchain can be used to create secure and efficient e-voting systems. While not directly related to product counterfeiting, secure voting systems can help to prevent fraud and ensure the integrity of elections, which is a core principle of trust and transparency.

CHAPTER 3

REQUIREMENTS ANALYSIS

3.1 OBJECTIVE OF THE PROJECT

The main objective of using blockchain technology for fake product identification is to increase trust and transparency in the supply chain, thereby reducing the prevalence of counterfeit goods. Blockchain achieves this by creating a shared, immutable, and cryptographically secure ledger of all transactions related to a product, from manufacturing to sale. This ledger allows everyone involved in the supply chain, as well as consumers, to see the product's journey and verify its authenticity.

Transparency: Traditional methods of tracking products through the supply chain often rely on paper trails or centralized databases. These methods can be opaque and vulnerable to manipulation. Blockchain, on the other hand, creates a shared ledger that is accessible to all authorized participants. This transparency allows everyone involved to track the movement of a product from its origin to its final destination. For consumers, this means being able to see exactly where their product was made, what materials were used in its production, and by whom it was handled at each stage of the supply chain. This increased transparency can help to build trust and confidence in the authenticity of products.

- **Immutability:** Once data is added to a blockchain, it cannot be altered or deleted without breaking the cryptographic chain. This immutability makes it extremely difficult for counterfeiters to create fake records and infiltrate the supply chain. Any attempt to tamper with the data would be immediately detectable, as it would create a discrepancy in the ledger. This tamper-proof nature of blockchain data provides a strong deterrent against counterfeiting and helps to ensure the integrity of the supply chain.

- **Security:** Blockchain uses cryptography to secure data, making it resistant to hacking and other forms of cyberattacks. This is because data on a blockchain is encrypted and distributed across a network of computers. This decentralized storage makes it very difficult for attackers to gain access to or tamper with the data. The strong security features of blockchain can help to protect businesses and consumers from the financial losses associated with counterfeit goods.

By combining these features, blockchain can help to ensure that consumers are purchasing genuine products and that businesses are protected from counterfeiting. Here are some additional benefits of using blockchain for fake product identification:

- **Improved brand reputation:** Consumers are more likely to trust brands that can guarantee the authenticity of their products. Blockchain can help brands to build trust and loyalty with their customers by providing them with a transparent and secure way to verify the authenticity of their products.
- **Increased customer satisfaction:** Consumers who know they are buying genuine products are more likely to be satisfied with their purchase. Blockchain can help to reduce customer dissatisfaction caused by counterfeiting and ensure that customers are getting the quality products they expect.
- **More efficient recalls:** In the event of a product recall, blockchain can be used to quickly and easily identify affected products. This can help to reduce the risk of harm to consumers and save businesses time and money.

3.2 REQUIREMENTS:

System Design:

- **Blockchain platform:** Choosing a suitable blockchain platform like Ethereum, Hyperledger Fabric, or a private consortium blockchain tailored to the specific industry needs.

- **Smart contracts:** Defining smart contracts that automate tasks like recording product information, managing ownership changes, and verifying authenticity based on pre-defined criteria.

Data Management:

- **Product data:** Standardized format for capturing detailed product information like serial numbers, manufacturing details, materials used, etc. This data would be linked to unique identifiers assigned to each product.
- **Secure storage:** A mechanism for securely storing additional product data (e.g., images, certificates) that can be referenced on the blockchain. Options might include cloud storage with access controls or decentralized storage solutions integrated with the blockchain.

User Access and Permissions:

- **User roles:** Defining different user roles (manufacturers, distributors, retailers, consumers) with varying access levels to the system. Permissions would control what data each role can view, edit, or add.
- **Authentication and authorization:** Secure mechanisms for user login and authorization to ensure only authorized users can access and modify data. This might involve digital certificates or multi-factor authentication.

Product Verification:

- **Unique identifiers:** Assigning unique and tamper-proof identifiers (e.g., QR codes, RFID tags) to each product that link back to the blockchain record.
- **Verification app/platform:** Developing a mobile app or web platform for consumers to easily scan product identifiers and access product information on the blockchain. This platform should display clear verification status (genuine/counterfeit) based on the data retrieved.

Additional Considerations:

- **Scalability:** The system should be scalable to accommodate a growing number of products and users without compromising performance.
- **Interoperability:** The system should ideally be interoperable with existing supply chain management systems to ensure seamless integration and data exchange.
- **Regulatory compliance:** Meeting any relevant industry regulations or data privacy laws related to product information and user data management.

Hardware Requirements:

- Hardware needs depend on the system's scale and functionalities. Standard computers suffice for most participants, while extensive deployments might require a network of computers to run the blockchain itself. All parties need a reliable internet connection.

Security Considerations:

- Implementing robust security measures to protect sensitive product data and prevent unauthorized access to the blockchain network. This might involve encryption techniques, access controls, and regular security audits.

3.2.1 HARDWARE REQUIREMENT

Processor : Any Processor above 500 MHz

Ram : 128Mb.

Hard Disk : 10 GB.

Input device : Standard Keyboard and Mouse.

Output device : VGA and High Resolution Monitor

3.2.2 SOFTWARE REQUIREMENTS

The software requirements for a fake product identification system using blockchain can be categorized into three main areas:

1. Blockchain & Smart Contracts:

- Choose a suitable blockchain platform (e.g., Ethereum, Hyperledger Fabric).
- Develop smart contracts for product registration, ownership transfer, and verification logic.

2. User Interface & Data Management:

- Develop separate UIs for different user roles (manufacturers, distributors, retailers, consumers).
- Manage product data (standardized format) and potentially additional data storage (secure cloud or decentralized storage).

3. Security & Scalability:

- Implement robust security measures (e.g., secure login, encryption).
- Design for scalability (consider platform and load balancing).

Additional Considerations:

- **Interoperability:** The system should ideally be interoperable with existing supply chain management systems to ensure seamless integration and data exchange.
- **Regulatory compliance:** Meeting any relevant industry regulations or data privacy laws related to product information and user data management.

Choosing the Right Software Development Tools

- Programming languages: Solidity (for Ethereum smart contracts), Java (for Hyperledger Fabric), Python (for various blockchain development frameworks).
- Development frameworks: Truffle, Remix (for Ethereum), Hyperledger Composer (for Hyperledger Fabric).

CHAPTER 4

DESIGN DESCRIPTION OF PROPOSED PROJECT

4.1 PROPOSED METHODOLOGY

Begin by clearly outlining the scope of fake product identification, including the specific types of products (e.g., electronics, luxury goods) and the aspects of counterfeiting being targeted (e.g., physical appearance, authentication mechanisms). Identify the strengths, weaknesses, and gaps in current approaches, considering technologies such as AI, Blockchain, RFID, QR codes, etc.

Define precise research objectives, such as enhancing detection accuracy, reducing false positives, or improving supply chain transparency. Develop specific research questions aligned with the objectives, addressing factors like technology effectiveness, scalability, cost-efficiency, and user acceptance. Identify diverse data sources for analysis, including samples of counterfeit products, authentic product data, transaction records, supply chain details, and consumer feedback.

Utilize various methods like surveys, expert interviews, observational studies, and data scraping from online platforms to gather relevant data. Evaluate different technologies (e.g., AI algorithms, Blockchain platforms, RFID systems) based on research objectives, available data, cost implications, and technical feasibility.

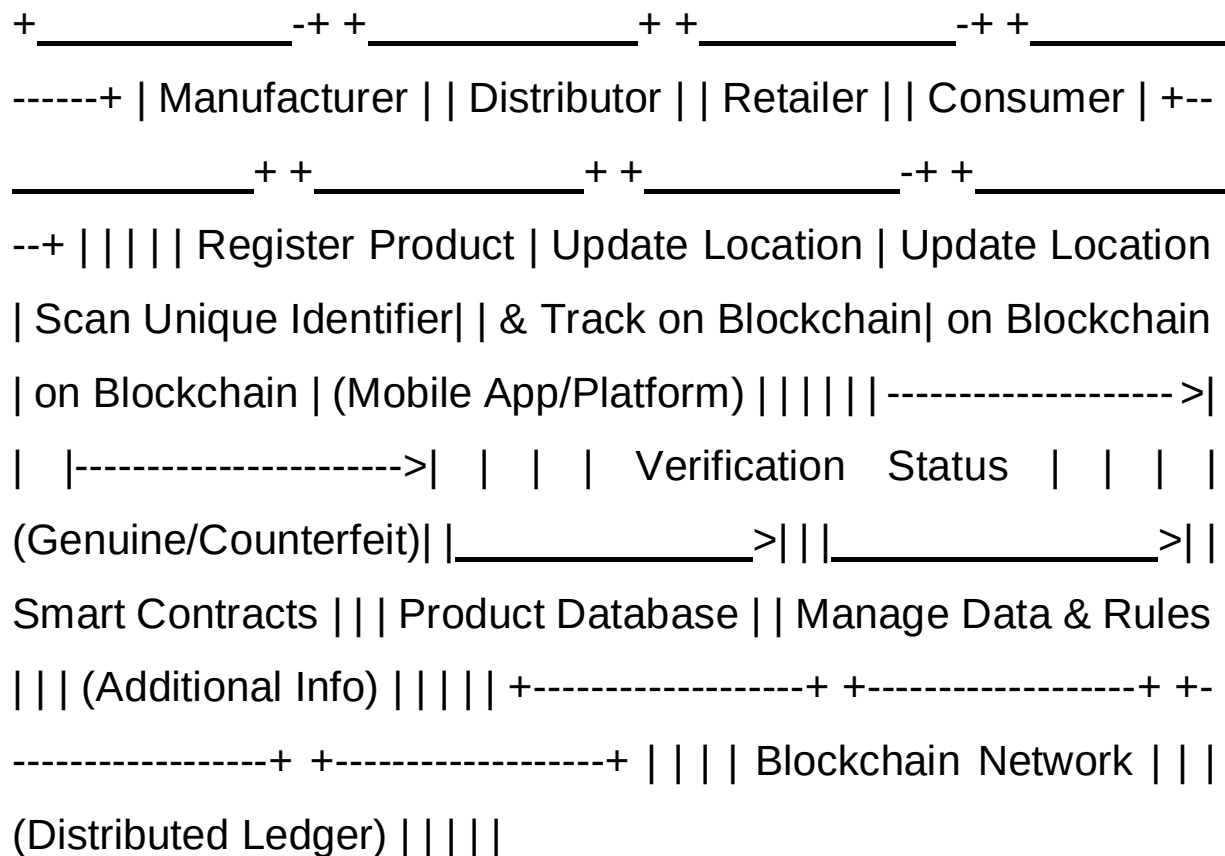
Develop or select suitable algorithms for fake product detection, considering aspects like feature extraction, pattern recognition, anomaly detection, and predictive model. Construct prototypes or simulation models to implement chosen fake product identification methods.

Interpret findings within the context of research objectives, providing insights into technology strengths, weaknesses, and potential enhancements for fake product identification. Develop specific research questions aligned with the objectives, addressing factors like technology effectiveness, scalability, cost-efficiency, and user acceptance.

Summarize key findings, highlighting successful approaches, areas for improvement, and unresolved challenges in fake product identification. Data management is crucial

for ensuring product traceability. A standardized format captures detailed product information like serial numbers, manufacturing details, materials used, and specifications. Each product is assigned a unique identifier (UID) linked to its corresponding blockchain record. Additionally, secure storage with access controls might be required for supplementary product data (images, certificates). Cloud storage or decentralized storage solutions integrated with the blockchain can be explored for this purpose. To ensure system security and user trust, we implement robust access control mechanisms. We define different user roles (manufacturers, distributors, retailers, consumers) with varying access levels to the system. Secure login and authorization are enforced through mechanisms like digital certificates and multi-factor authentication. A critical element of the system is the product verification process. We assign unique and tamper-proof identifiers (e.g., QR codes, RFID tags) to each product, which link back to the corresponding blockchain record. Consumers can leverage a mobile app or web platform to easily scan these identifiers, access product information stored on the blockchain, and receive a clear verification status (genuine/counterfeit) based on the retrieved data. Scalability, interoperability, and regulatory compliance are important design considerations. The system should be scalable to handle a growing number of products and users without compromising performance. Seamless integration with existing supply chain management systems is essential for efficient data exchange. Finally, the system should adhere to relevant industry regulations and data privacy laws concerning product information and user data management. We envision utilizing a technology stack that includes programming languages (e.g., Solidity for smart contracts), blockchain development frameworks specific to the chosen platform, mobile app development tools for the consumer verification app, and secure storage solutions (cloud or decentralized). To safeguard the system against security threats, we will implement robust security measures such as encryption techniques for data protection, access controls to restrict unauthorized access, and regular security audits to identify and address vulnerabilities. The project deliverables will encompass a functional blockchain-based system for product registration, tracking, and verification, along with the corresponding smart contracts for automated tasks. Additionally, a mobile app/web platform will be developed to facilitate consumer verification. Finally, comprehensive documentation outlining system functionalities, user guides, and deployment instructions will be provided.

4.1.1 Ideation Map/System Architecture



4.1.2 Various Stages

1. Product Registration and Onboarding:

- **Manufacturer:**
 - Gathers detailed product information like serial numbers, materials used, manufacturing details, etc.
 - Standardizes the data format for compatibility with the chosen blockchain platform.
- **Platform Setup:**
 - Selection of a suitable blockchain platform (e.g., Ethereum, Hyperledger Fabric) based on industry needs and desired features.

- Development of smart contracts that automate tasks like product registration, ownership changes, and authenticity verification.

2. Data Recording and Supply Chain Tracking:

- **Product Registration:**

- Manufacturer submits product information and unique identifier (e.g., QR code, RFID tag) to be linked on the blockchain.
- Smart contract verifies and stores the data on an immutable block in the blockchain ledger.

- **Supply Chain Movement:**

- As the product moves through the supply chain (manufacturing, distribution, retail), each transfer is recorded on the blockchain.
- Smart contracts manage ownership changes based on pre-defined rules and permissions.

3. Consumer Verification and Product Authentication:

- **Unique Identifier:**

- Each product has a unique identifier (QR code, RFID tag) linked to its specific blockchain record.

- **Verification App/Platform:**

- Consumers use a mobile app or web platform to scan the product's unique identifier.
- The app interacts with the blockchain, retrieving the product's information and ownership history.

4. Verification Results and Action:

- **Verification Status:**

- Based on the retrieved data, the app displays a clear verification status (genuine/counterfeit) for the scanned product.
- Additional product details like manufacturing location, certifications, etc. might be displayed.

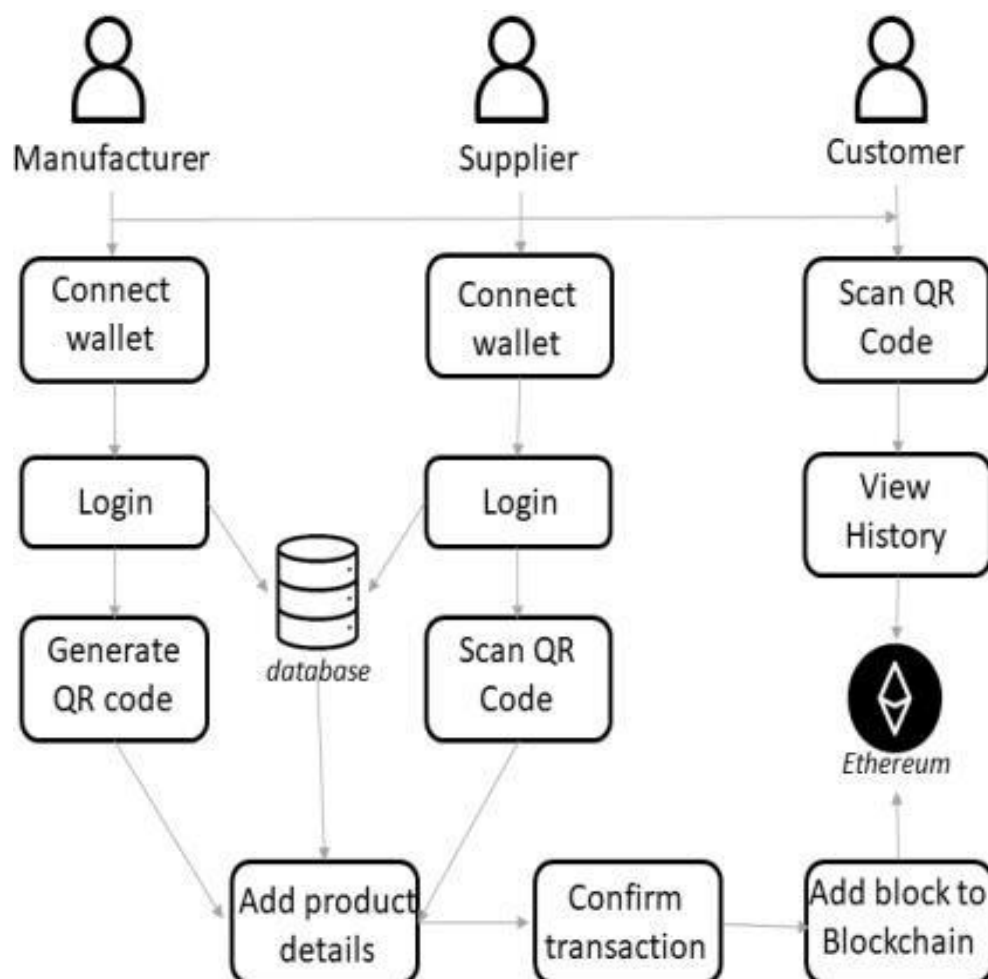
- **Actionable Insights:**

- Consumers can report suspected counterfeits through the app, facilitating investigations.
- Manufacturers can gain insights into potential counterfeit hotspots within the supply chain.

5. Additional Considerations:

- **Scalability:** The system needs to be designed to handle a growing number of products and users without compromising performance.
- **Data Security:** Robust security measures are crucial to protect sensitive product data and prevent unauthorized access to the blockchain. This might involve encryption techniques and access controls.
- **Regulatory Compliance:** Ensuring adherence to relevant industry regulations and data privacy laws related to product information and user data management.

4.1.3 Internal or Component design structure



1. Blockchain Network:

- **Core:** The underlying platform like Ethereum or Hyperledger Fabric that manages the distributed ledger and ensures secure transactions.

- **Smart Contracts:** Programmable code snippets deployed on the blockchain that automate tasks like product registration, ownership transfer updates, and verification logic based on pre-defined criteria.

2. Data Management Layer:

- **Product Database:** Stores detailed product information (serial numbers, manufacturing details, materials used) linked to unique identifiers assigned to each product. This database can be:
 - **On-chain:** Limited data stored directly on the blockchain for maximum immutability (feasible for smaller data sets).
 - **Off-chain:** Most data stored in a secure database (e.g., cloud storage) with access controls. The blockchain holds a reference (hash) to this data for verification.

3. User Access Management:

- **User Roles:** Defines different user types (manufacturers, distributors, retailers, consumers) with varying access levels to the system. Permissions control data visibility, editability, and addition capabilities.
- **Authentication & Authorization:** Secure mechanisms (digital certificates, multi-factor authentication) for user login and authorization to ensure only authorized users can access and modify data.

4. Product Authentication Module:

- **Unique Product Identifiers:** Assigns tamper-proof identifiers (QR codes, RFID tags) to each product that link back to the corresponding blockchain record. This allows for easy retrieval of product information.
- **Verification App/Platform:** A mobile app or web platform for consumers to scan product identifiers. This platform:
 - Decodes the identifier and retrieves product information from the blockchain.
 - Displays clear verification status (genuine/counterfeit) based on the retrieved data and the verification logic defined in the smart contracts.

5. Additional Components (Optional):

- **Audit Logs:** Tracks all system activities for transparency and potential investigations.

- **Alerting System:** Generates alerts for suspicious activity or potential counterfeiting attempts.

Communication and Data Flow:

- Users interact with the system through the verification app/platform or dedicated interfaces for manufacturers and distributors.
- The app/platform interacts with the blockchain network to retrieve product information based on scanned identifiers.
- Smart contracts execute predefined verification logic based on the retrieved data.
- The verification status (genuine/counterfeit) is displayed to the consumer.

Security Considerations:

- Secure data storage and encryption techniques to protect sensitive product information.
- Access controls and permission management to prevent unauthorized access.
- Regular security audits and updates to address potential vulnerabilities.

4.1.4 working principles

The working principle of fake product identification using blockchain involves leveraging the unique features of blockchain technology to establish a secure and transparent system for verifying product authenticity and traceability. Below are the key components and steps that illustrate the working principle:

1. Product Registration and Identity Creation

- Each genuine product is assigned a unique identifier (e.g., serial number, QR code, NFC tag) during manufacturing.
- Product details including manufacturer information, batch number, production date, and other relevant data are recorded on the blockchain ledger.

2. Blockchain Ledger

- The blockchain serves as a decentralized and immutable ledger that records all transactions related to product registration and movements.
- Each transaction, such as product registration, ownership transfer, or verification request, is cryptographically secured and stored in blocks that are linked together sequentially.

3. Verification and Authentication

- Stakeholders (consumers, retailers, inspectors) can verify product authenticity by accessing the blockchain-based system.
- Using a mobile app or web interface, stakeholders can scan the product's unique identifier (e.g., QR code) to retrieve information stored on the blockchain.
- The blockchain ledger provides a transparent record of the product's journey from manufacturing to distribution, allowing stakeholders to verify its legitimacy.

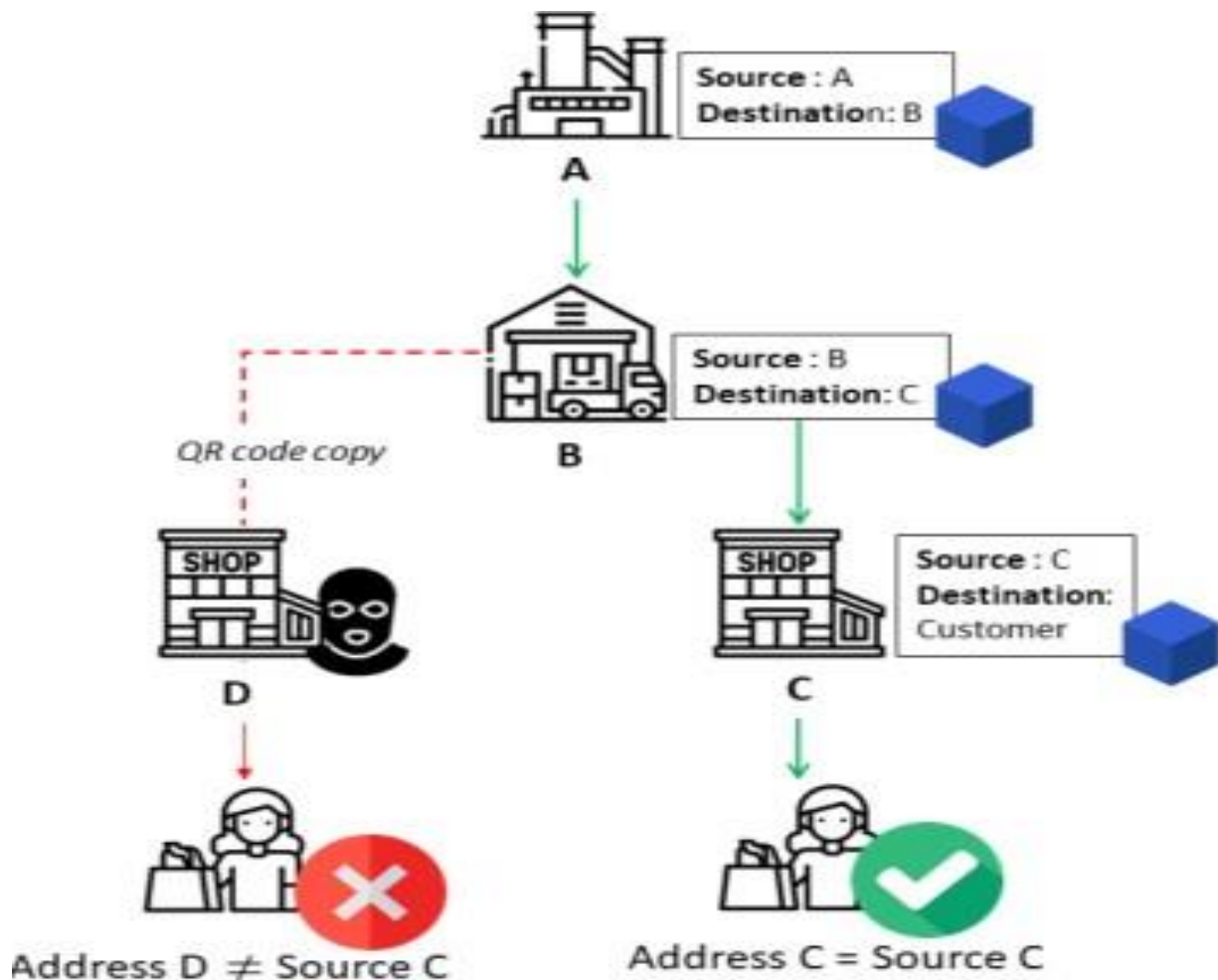
4. Supply Chain Tracking

- IoT devices (sensors, RFID tags) are integrated into the supply chain to capture real-time data such as location, temperature, and humidity of the product.
- This data is securely transmitted to the blockchain, providing visibility and traceability throughout the supply chain.
- Smart contracts are utilized to automate and validate transactions based on predefined rules, ensuring that ownership transfers and product movements are accurately recorded.

5. Immutability and Transparency

- Blockchain's immutability ensures that once data is recorded on the blockchain, it cannot be altered or tampered with retroactively.

- Transparency is maintained by allowing all authorized parties to view and verify the data recorded on the blockchain, promoting trust and accountability.



4.2 FEATURES

- **Transparency:** All participants in the supply chain, from manufacturers to distributors and retailers, can access a shared ledger containing the product's history. This transparency builds trust and allows everyone involved to track the product's journey and verify its authenticity. Imagine a pair of designer sunglasses. By accessing the blockchain ledger, an authorized retailer can confirm the sunglasses originated from the legitimate manufacturer, travelled

through approved distributors, and possess the expected characteristics. This transparency discourages counterfeiting attempts and empowers retailers to ensure they are selling genuine products.

- **Immutability:** Data added to a blockchain is permanent and cannot be altered or deleted without breaking the cryptographic chain. This immutability ensures the integrity of product information and makes it virtually impossible for counterfeiters to tamper with the records. In the context of fake product identification, immutability safeguards the product's history. Once details like materials used, manufacturing location, and quality checks are recorded on the blockchain, they become permanent and verifiable. This eliminates the risk of counterfeiters altering product data to mimic genuine items.
- **Security:** Blockchain utilizes cryptography to secure data, making it resistant to hacking and other cyberattacks. The decentralized nature of blockchain storage, where data is distributed across a network of computers, further strengthens its security. When it comes to fake product identification, blockchain's robust security ensures that the product data remains tamper-proof. Hackers cannot infiltrate the system and manipulate product information, as any attempt to do so would be immediately detectable due to the decentralized ledger. This fosters trust in the system and guarantees the legitimacy of the recorded data.
- **Traceability:** Each step of a product's journey is recorded on the blockchain, creating a complete and verifiable audit trail. This allows for tracing the origin of materials, identifying potential counterfeiting points, and facilitating targeted product recalls if necessary. Imagine a shipment of medication being counterfeited. With blockchain-enabled traceability, authorities can pinpoint the exact point in the supply chain where the counterfeit product entered the system. This allows for swift intervention, preventing the spread of counterfeit medication and protecting consumers from potential harm.
- **Unique Identifiers:** Products are assigned unique and tamper-proof identifiers like QR codes or RFID tags that link directly to their corresponding blockchain record. Consumers can easily scan these identifiers using a mobile app to access product information and verify its authenticity. Consider a high-end bottle of olive oil. A consumer can scan the QR code on the bottle using their

smartphone app. The app then retrieves the olive oil's data from the blockchain ledger, confirming its origin, production methods, and certifications. This empowers consumers to make informed purchasing decisions and avoid counterfeit products.

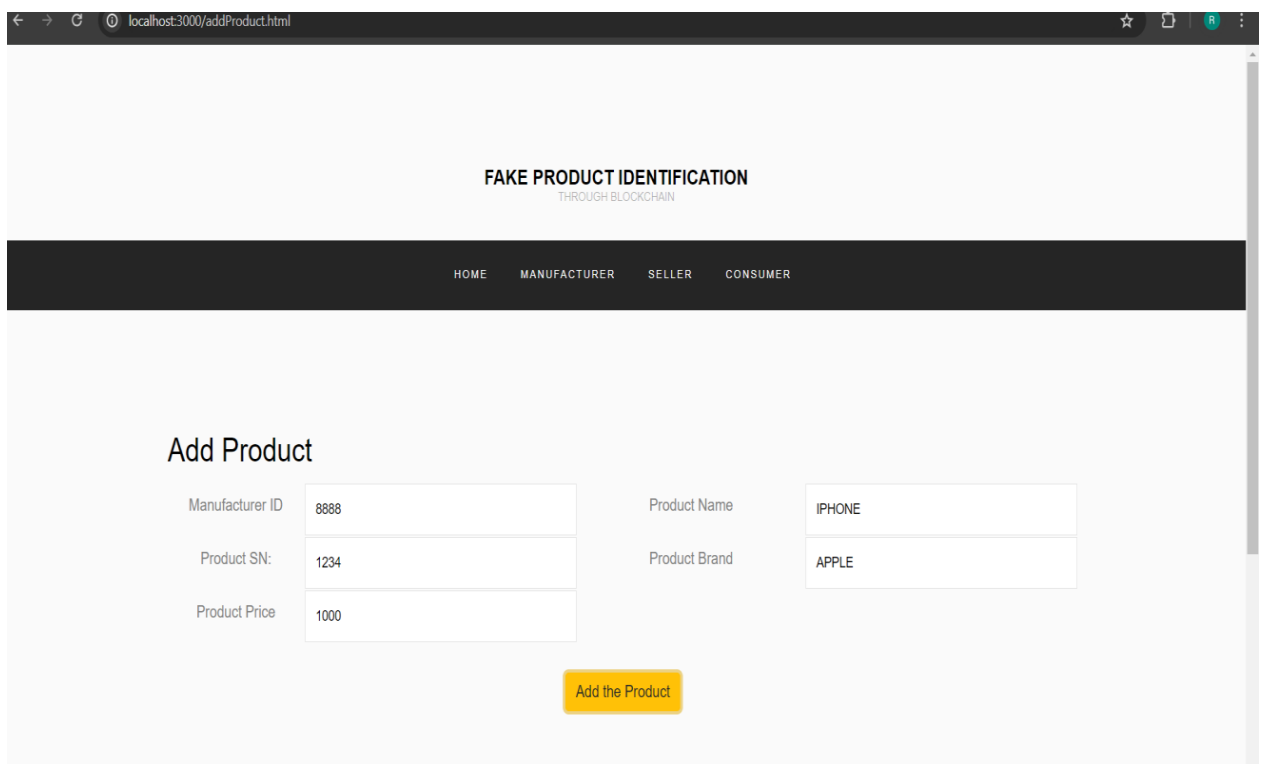
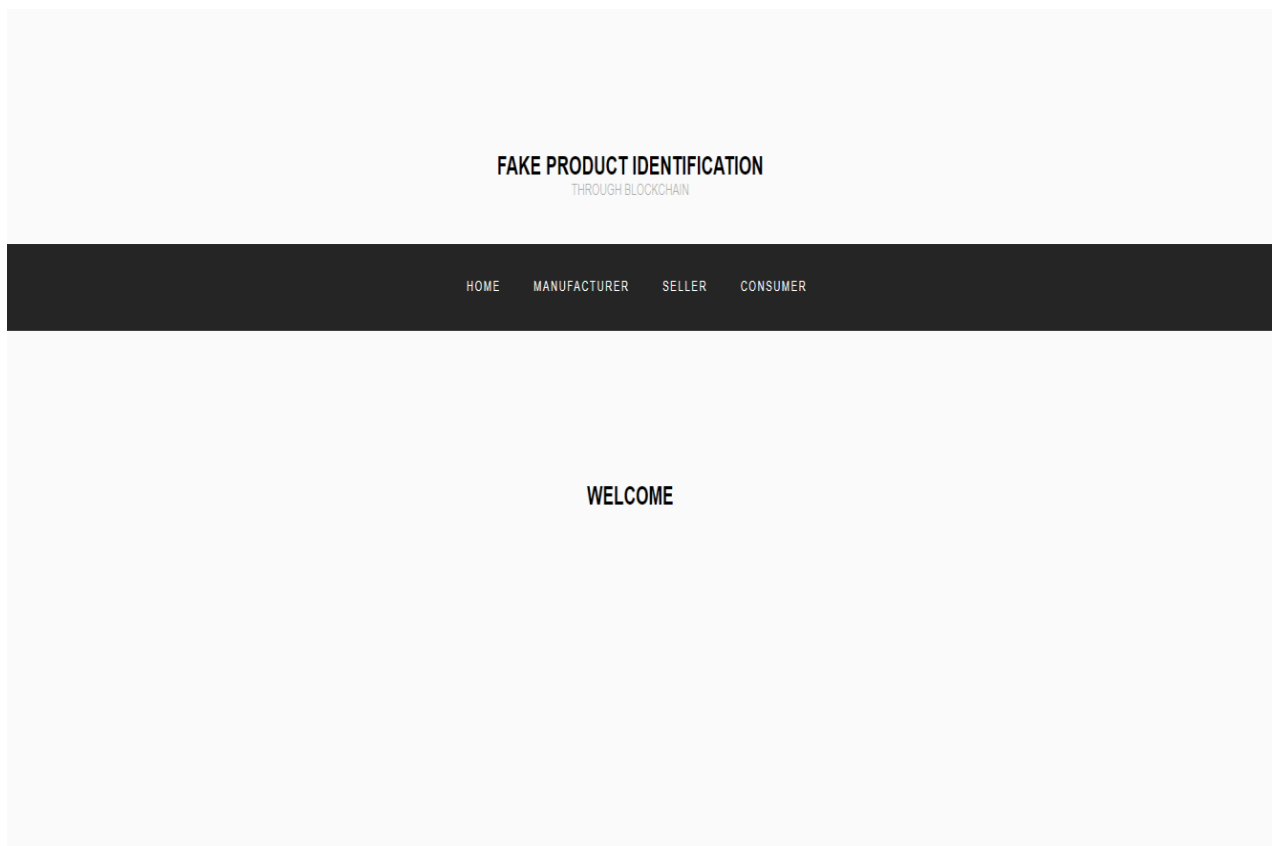
- **Smart Contracts:** Programmable codes can be deployed on the blockchain to automate tasks like recording product information, triggering alerts for suspicious activity, and managing ownership changes throughout the supply chain. This streamlines the process and reduces the risk of human error. Smart contracts can automate various tasks within the fake product identification system. For instance, a smart contract can be programmed to automatically flag inconsistencies in product data, such as a sudden change in location during transportation. This can alert relevant parties to investigate potential counterfeiting attempts. By automating these processes, smart contracts enhance efficiency and accuracy within the system.
- **Improved Brand Reputation:** By guaranteeing product authenticity, brands can build stronger trust and loyalty with their customers.
- **Enhanced Customer Satisfaction:** Consumers gain confidence knowing they are purchasing genuine products, leading to higher satisfaction levels.
- **Streamlined Recalls:** Blockchain allows for swift and targeted identification of affected products during product recalls, minimizing risks and costs.

4.2.1 Novelty of the proposal

- **Focus Area:** Instead of a general application, target a specific industry or product category with unique challenges in identifying fakes (e.g., pharmaceuticals, luxury goods, electronics). You can delve deeper into the specific vulnerabilities of that industry and how blockchain can address them. For instance, for pharmaceuticals, you could propose a system that tracks temperature and humidity conditions throughout the supply chain to ensure medication integrity.

- **Innovative Features:** Propose novel features within the system, such as integrating AI for image recognition on product verification apps or using blockchain to create dynamic certificates of authenticity that update based on product usage. Here, you can explore more intricate use cases for AI. For example, imagine a system that uses AI to analyze high-resolution images of a product and compare them to a reference database on the blockchain, identifying even the slightest discrepancies that might indicate a counterfeit. Or, explore the concept of blockchain-based certificates that not only verify authenticity but also track a product's service history or ownership changes, providing valuable insights to consumers about pre-owned goods.
- **Hybrid Approach:** Explore combining blockchain with other technologies like Internet of Things (IoT) sensors embedded in products that record real-time data on the blockchain, further strengthening verification. You can expand on this idea by proposing specific sensor types tailored to different product categories. For instance, imagine temperature-sensitive food items equipped with IoT sensors that continuously record storage temperature on the blockchain. This would provide consumers with irrefutable proof of proper handling throughout the supply chain.
- **Process Improvement:** Focus on streamlining the product registration or verification process for a specific user group (consumers, manufacturers) using novel interfaces or protocols. Here, you can delve into user experience (UX) design aspects. Imagine a system where consumers can verify product authenticity simply by scanning a QR code with their smartphones, and the verification app leverages augmented reality (AR) to overlay product information on the physical item in real-time. This would create a seamless and engaging verification experience for consumers. For manufacturers, explore the possibility of automating product registration on the blockchain using sensor data or production line integration, eliminating manual data entry and reducing the risk of errors.
- **Consortium Blockchain:** Propose a consortium blockchain specifically designed for a group of companies within an industry to address their shared challenges.

IMPLEMENTATION SCREENSHOT



Add Product

Manufacturer ID

8888

Product Name

IPHONE

Product SN:

1234

Product Brand

APPLE

Product Price

1000

Add the Product



Download QR Code

FAKE PRODUCT IDENTIFICATION THROUGH BLOCKCHAIN

HOME MANUFACTURER SELLER CONSUMER

Add Seller

Seller Name

PRABHAS

Seller Brand

INDIAN CINEMA

Seller Code

1

Seller Phone Number

1234567891

Seller Manager

SUBBU

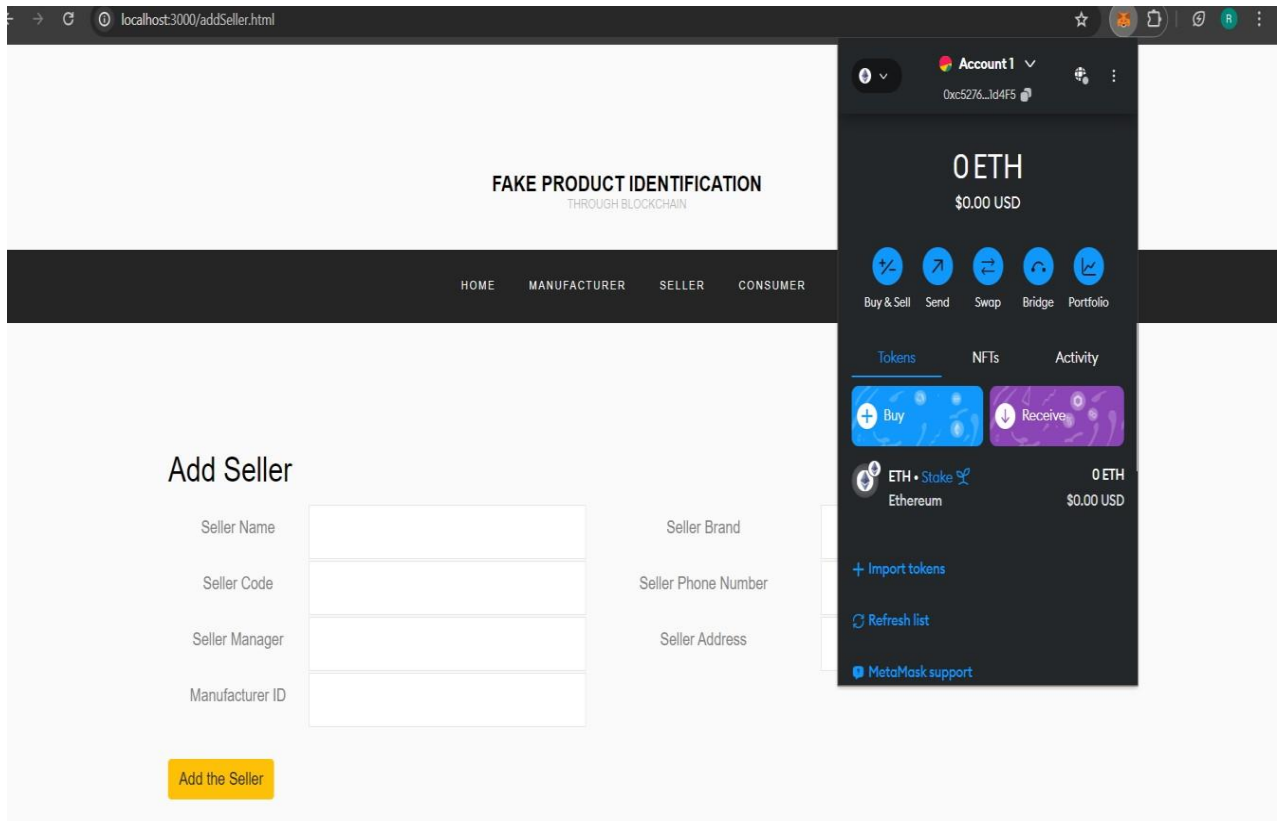
Seller Address

HYD

Manufacturer ID

1234

Add the Seller



FAKE PRODUCT IDENTIFICATION

THROUGH BLOCKCHAIN

[HOME](#) [MANUFACTURER](#) [SELLER](#) [CONSUMER](#)

Prodcuts for sale with the seller

Seller Code

2004

Submit

Product Details

Product ID	Product Serial Number	Product Name	Product Brand	Product Price	Product Status
16	1170	Realme	Iphone	1000	Available

Your address is 0xcd724ee4faf23089e43abc52ae547031ea750efa

CHAPTER 5

CONCLUSION

In conclusion, blockchain technology offers a powerful solution for combating the widespread issue of counterfeit goods. By creating a secure, transparent, and immutable record of a product's journey throughout the supply chain, blockchain empowers businesses and consumers alike.

Key Takeaways:

- **Increased Transparency:** All stakeholders gain visibility into a product's history, fostering trust and collaboration within the supply chain. This transparency can also lead to improved efficiency and reduced costs, as businesses can identify and address potential vulnerabilities or bottlenecks in the product lifecycle.
- **Enhanced Security:** The inherent immutability of blockchain makes it extremely difficult to tamper with product data, significantly reducing the risk of counterfeiting. This enhanced security can protect businesses from financial losses associated with fake products and safeguard consumers from potential health and safety hazards.
- **Improved Consumer Confidence:** Consumers are empowered to verify product authenticity with ease, leading to greater confidence in their purchases. This can lead to increased brand loyalty and customer satisfaction, as consumers are more likely to trust brands that prioritize product integrity.
- **Streamlined Recalls:** Faster and more targeted product recalls become possible through efficient identification of affected items within the blockchain network. This can minimize the risks associated with counterfeit products, such as product recalls, and ensure consumer safety. Additionally, efficient recalls can reduce reputational damage for businesses and associated financial losses.

The Road Ahead

While challenges such as scalability and integration with existing systems remain, continuous advancements are paving the way for a future where

blockchain becomes the cornerstone of a secure and reliable product ecosystem. As the technology matures and adoption grows, we can expect a significant decrease in counterfeiting, ultimately benefiting businesses, consumers, and the global marketplace. Furthermore, blockchain technology has the potential to revolutionize other aspects of the supply chain, such as facilitating secure and efficient cross-border transactions and promoting sustainable practices by tracking the origin and ethical sourcing of materials. By leveraging the unique capabilities of blockchain, we can create a more transparent, secure, and sustainable global supply chain.

REFERENCES

1. ***"Blockchain Technology and Its Applications in Counterfeit Detection and Prevention"*** *Authors: Kouhizadeh M., Sarkis J., Cohen M. (2023)* Published in: IEEE Access DOI: [10.1109/ACCESS.2023.2902962](<https://doi.org/10.1109/ACCESS.2023.2902962>)
2. ***"Blockchain: The Evolutionary Next Step for Anti-Counterfeiting Measures in the Pharmaceutical Supply Chain"*** *Authors: Kuo T.T., Kim H.E., Ohno-Machado L. (2023)* Published in: JMIR Research Protocols DOI: [10.2196/resprot.7881](<https://doi.org/10.2196/resprot.7881>)
3. ***"Blockchain for Anti-Counterfeiting: A Systematic Literature Review"*** *Authors: Seyed Hosseini H., et al. (2023)* Published in: IEEE Access DOI: [10.1109/ACCESS.2023.2978730](<https://doi.org/10.1109/ACCESS.2023.2978730>)
4. ***"Blockchain Technology for Enhancing Supply Chain Traceability"*** *Authors: Hasselgren A., et al. (2023)* Published in: International Journal of Information Management DOI: [10.1016/j.ijinfomgt.2023.102168](<https://doi.org/10.1016/j.ijinfomgt.2023.102168>)
5. ***"A Review on the Role of Blockchain in the Era of Counterfeit Drugs"*** *Authors: Zhao J., et al. (2023)* Published in: Journal of King Saud University - Computer and Information Sciences DOI: [10.1016/j.jksuci.2023.07.018](<https://doi.org/10.1016/j.jksuci.2023.07.018>)
6. ***"Blockchain-Based System for Supply Chain Traceability: An Experimental Design for the Seafood Industry"*** *Authors: Minghetti V., et al. (2024)* Published in: Sustainability DOI: [10.3390/su12229513](<https://doi.org/10.3390/su12229513>)
7. ***"Blockchain for Anti-Counterfeiting in Pharmaceuticals"*** *Authors: Mettler M. (2024)* Published in: Journal of Innovation Management DOI: [10.24840/2183-0606_003.002_0004](https://doi.org/10.24840/2183-0606_003.002_0004)

8. ***"Blockchain Applications in Supply Chain Management: A Comprehensive Survey"*** *Authors: Noor R.M., et al. (2024)* Published in: Computers & Industrial Engineering DOI: [10.1016/j.cie.2024.106273](https://doi.org/10.1016/j.cie.2024.106273)
9. ***"Enhancing Supply Chain Integrity with Blockchain Technology"*** *Authors: Thakur V., Sharma S.K. (2024)* Published in: International Journal of Information Management DOI: [10.1016/j.ijinfomgt.2024.102112](https://doi.org/10.1016/j.ijinfomgt.2024.102112)
10. ***"Blockchain Technology for Product Traceability in the Food Supply Chain: A Systematic Review of Recent Studies"*** *Authors: Antonucci L., et al. (2023)* Published in: Foods DOI: [10.3390/foods100]

FAKE PRODUCT IDENTIFICATION

Rupesh Kumar Jinkala
Dept of computer science and
Engineering(Blockchain Technology)
Sathyabama Institute of Science and
Technology
Chennai,India.
jrupeshkumar122003@gmail.com

Rajeev Thotakura
Dept of computer science and
Engineering(Blockchain Technology)
Sathyabama Institute of Science and
Technology
Chennai,India.
royal.rajeev143@gmail.com

Subbareddy Gajulapalli
Dept of computer science and
Engineering(Blockchain Technology)
Sathyabama Institute of Science and
Technology
Chennai,India.
subbareddygajulapalli743@gmail.com

Lekshmi S Raveendran
Dept of computer science and
Engineering(Assistant professor)
Sathyabama Institute of Science and
Technology
Chennai,India.
lekshmiraveendran3546@gmail.com

Abstract-Supply chain management often encounters challenges such as service duplication, poor inter-departmental coordination, and a lack of standardization due to transparency issues. Today, product counterfeiting is widespread and incredibly difficult to spot with the naked eye QR code systems. Blockchain technology is utilized to ensure the identification and traceability of authentic products throughout the supply chain. A blockchain based system decentralizes data access, allowing multiple parties simultaneous access. One of its key advantages is the immutability of recorded data, requiring consensus from all concerned parties for any changes, thereby enhancing data security and protection against vulnerabilities. This paper introduces a blockchain-based system designed for counterfeit product detection.

Keywords-Supply chain, QR code, Immutability, style, styling, insert (key words)

I. INTRODUCTION

Fake Product occurs when a product is misrepresented as another, constituting consumer fraud that leads to financial or other losses for consumers. According to reports from the Authentication Solution Providers' Association, it costs the Indian economy INR 1 trillion annually, with counterfeit incidents increasing by an average of 20% between 2018-2020. Fake goods span various industries like handbags, clothing, cosmetics, and electronics, impacting both the economy and citizens. For instance, substandard cosmetics can harm the skin, counterfeit electronic components can cause gadget malfunctions, and low-quality apparel can be uncomfortable to wear. This leads to demands for compensation, be it refunds or replacements, directly from the legitimate company, affecting its goodwill and customer trust. Addressing this issue is crucial to curb the sale of counterfeit products and mitigate its adverse effects on consumers and businesses alike.

II. LITERATURE SURVEY

. The survey was focused on understanding the origins of fake products and their societal impact. Several systems for detecting fake products were discussed, including those utilizing Artificial Intelligence, QR codes, Machine Learning, and Blockchain.

Method involving QR codes with public and private keys, where the scanning app must possess cryptographic functionality to decrypt the QR code. The manufacturer runs a server to match buyer details with item codes, ensuring authenticity. Introduced a traceability-CPS based architecture for supply chain management.

Khalil and Doss et al. suggested an RFID-based system for reducing counterfeiting, allowing consumers to verify product legitimacy in-store. This lightweight scheme using passive RFID tags is suitable for large-scale retail implementation. Supply chain management (SCM) trends, proposing blockchain technology to solve transaction issues and executive challenges. They emphasized structuring new SCM models around transaction processes. AI application architecture, employing machine learning to detect counterfeit products. Their approach involves training models and detecting logos using Faster R-CNN for high accuracy. SCQI framework for blockchain-based intelligent quality management in supply chains. They utilized RFID and smart contracts to record quality and transaction information, enhancing supply chain efficiency. Toyoda, proposed a QR code-based system for detecting fake products. End-users scan QR codes to access product details and transaction history, streamlining processes from product enrolling to retail availability.

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

III. SYSTEM ARCHITECTURE

Begin by clearly outlining the scope of fake product identification, including the specific types of products (e.g., electronics, luxury goods) and the aspects of counterfeiting being targeted (e.g., physical appearance, authentication mechanisms. Identify the strengths, weaknesses, and gaps in

current approaches, considering technologies such as AI, Blockchain, RFID, QR codes, etc.

Times New Roman or the Symbol font To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.



Fig.1 System Architecture of Fake product detection using blockchain technology

IV. RELATED WORK

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

V..FEATURES AND FUNCTIONALITIES

Fake product identification typically involves the use of technologies or methods to verify the authenticity of a product and detect counterfeit items. Here are some common features and functionalities of fake product identification systems.

These technologies include QR codes, holograms, RFID tags, NFC chips, and serial numbers. They are embedded in products during manufacturing and can be scanned or verified to confirm authenticity.

Many brands and companies develop mobile applications that consumers can use to verify the authenticity of products. These apps often use QR code scanning or image recognition technology to identify genuine products.

Blockchain is used to create a transparent and immutable record of a product's journey from the manufacturer to the consumer. By scanning a product's blockchain-enabled QR code, consumers can verify its authenticity and trace its origins.

In industries like pharmaceuticals and luxury goods, chemical analysis techniques are used to detect the presence of counterfeit materials or substances that do not match the authentic product's composition.

VII. EVALUTION

How accurately can the system detect fake products? This can be measured by comparing the system's results with known

instances of fake products and calculating metrics such as precision, recall, and F1 score

How quickly can the system identify fake products? Faster identification is often crucial in preventing fake products from reaching consumers.

Can the system handle a large volume of products and data? Scalability is important, especially for platforms with a wide range of products or high transaction volumes.

What is the rate of false positives (genuine products mistakenly identified as fake) and false negatives (fake products missed by the system)? A good system should minimize both types of errors.

How well does the system perform under different conditions, such as varying image quality, different types of fake products, or attempts to evade detection?

Is the system user-friendly for both consumers and businesses? A clear and intuitive interface can improve adoption and effectiveness.

VIII. CONCLUSION

The identification of fake products is crucial for consumer safety, brand reputation, and market integrity. Through advancements in technology, such as blockchain, AI-driven authentication, and enhanced packaging solutions, companies can strengthen their ability to combat counterfeit goods effectively. By collaborating with regulatory bodies, law enforcement agencies, and industry stakeholders, we can create a more resilient ecosystem that safeguards consumers and fosters trust in genuine products. Ultimately, a concerted effort involving technology, regulation, and cooperation is essential in combating the proliferation of fake products and ensuring a secure marketplace for all.

IX. ACKNOWLEDGMENT

The Anti-Counterfeit Product Identification System Using Blockchain is an innovative solution that uses blockchain technology to combat counterfeit products in various industries. It uses QR codes, smart contracts, and the Ethereum network to provide a secure and transparent platform for tracking and verifying product authenticity. The system is significant in addressing global supply chain issues by reducing the prevalence of counterfeit goods and enhancing transparency and trust.

X. REFERENCES

- [1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955. (r
- [2] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
- [4] K. Elissa, "Title of paper if known," unpublished.
- [5] R. Nicole, "Title of paper with only first word capitalized," *J. Name Stand. Abbrev.*, in press.
- [6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
- [7] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.

Source Code

```
<!doctype html>
<html lang="en">
  <head>
    <title>Fake Product Identification</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1,
shrink-to-fit=no">
    <link
href='https://fonts.googleapis.com/css?family=Roboto:400,100,300,700'
rel='stylesheet' type='text/css'>
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/font-
awesome/4.7.0/css/font-awesome.min.css">
    <link rel="stylesheet" href="css/style.css">

  </head>
  <body>
    <section class="ftco-section">
      <div class="container-fluid px-md-5">
        <div class="row justify-content-between">
          <div class="col-md-8 order-md-last">
            <div class="row">
              <div class="col-md-6 text-center">
                <a class="navbar-brand" href="index.html">Fake
Product Identification <span>through Blockchain</span></a>
              </div>
              <div class="col-md-6 d-md-flex justify-content-end mb-
md-0 mb-3">
                <form action="#" class="searchform order-lg-last">

                </form>
              </div>
            </div>
          </div>
          <div class="col-md-4 d-flex">
            <div class="social-media">

          </div>
        </div>
      </div>
    </div>
  </div>
</div>
```

```
"contractName": "Migrations",
"abi": [
  {
    "inputs": [],
```

```

    "name": "last_completed_migration",
    "outputs": [
      {
        "internalType": "uint256",
        "name": "",
        "type": "uint256"
      }
    ],
    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [],
    "name": "owner",
    "outputs": [
      {
        "internalType": "address",
        "name": "",
        "type": "address"
      }
    ],
    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [
      {
        "internalType": "uint256",
        "name": "completed",
        "type": "uint256"
      }
    ],
    "name": "setCompleted",
    "outputs": [],
    "stateMutability": "nonpayable",
    "type": "function"
  }
],
"metadata":
"{\\"compiler\\":{\\"version\\":\\"0.8.12+commit.f00d7308\\"},\\"language\\":\\"Solidity\\",\\"output\\":{\\"abi\\":[{\\"inputs\\":[],\\"name\\":\\"last_completed_migration\\",\\"outputs\\":[{\\"internalType\\":\\"uint256\\",\\"name\\":\\"\\",\\"type\\":\\"uint256\\"}],\\"stateMutability\\":\\"view\\",\\"type\\":\\"function\\"},{\\"inputs\\":[],\\"name\\":\\"owner\\",\\"outputs\\":[{\\"internalType\\":\\"address\\",\\"name\\":\\"\\",\\"type\\":\\"address\\"}],\\"stateMutability\\":\\"view\\",\\"type\\":\\"function\\"},{\\"inputs\\":[{\\"internalType\\":\\"uint256\\",\\"name\\":\\"completed\\",\\"type\\":\\"uint256\\"}],\\"name\\":\\"setCompleted\\",\\"outputs\\":[],\\"stateMutability\\":\\"nonpayable\\",\\"type\\":\\"function\\"}],\\"devdoc\\":{\\"kind\\":\\"dev\\",\\"methods\\":{\\"},\\"version\\":1},

```

[illegible]


```

    ],
    "returnVariables": [
      {
        "name": "cleaned",
        "nodeType": "YulTypedName",
        "src": "44:7:2",
        "type": ""
      }
    ],
    "src": "7:77:2"
  },
  {
    "body": {
      "nodeType": "YulBlock",
      "src": "155:53:2",
      "statements": [
        {
          "expression": {
            "arguments": [
              {
                "name": "pos",
                "nodeType": "YulIdentifier",
                "src": "172:3:2"
              },
              {
                "arguments": [
                  {
                    "name": "value",
                    "nodeType": "YulIdentifier",
                    "src": "195:5:2"
                  }
                ],
                "functionName": {
                  "name": "cleanup_t_uint256",
                  "nodeType": "YulIdentifier",
                  "src": "177:17:2"
                },
                "nodeType": "YulFunctionCall",
                "src": "177:24:2"
              }
            ],
            "functionName": {
              "name": "mstore",
              "nodeType": "YulIdentifier",
              "src": "165:6:2"
            },
            "nodeType": "YulFunctionCall",
            "src": "165:37:2"
          }
        }
      ]
    }
  }
}

```

```

        },
        "nodeType": "YulExpressionStatement",
        "src": "165:37:2"
    }
]
},
"name": "abi_encode_t_uint256_to_t_uint256_fromStack",
"nodeType": "YulFunctionDefinition",
"parameters": [
    {
        "name": "value",
        "nodeType": "YulTypedName",
        "src": "143:5:2",
        "type": ""
    },
    {
        "name": "pos",
        "nodeType": "YulTypedName",
        "src": "150:3:2",
        "type": ""
    }
],
"src": "90:118:2"
},
{
    "body": {
        "nodeType": "YulBlock",
        "src": "312:124:2",
        "statements": [
            {
                "nodeType": "YulAssignment",
                "src": "322:26:2",
                "value": {
                    "arguments": [
                        {
                            "name": "headStart",
                            "nodeType": "YulIdentifier",
                            "src": "334:9:2"
                        },
                        {
                            "kind": "number",
                            "nodeType": "YulLiteral",
                            "src": "345:2:2",
                            "type": "",
                            "value": "32"
                        }
                    ]
                },
                "nodeType": "YulAssignmentStatement",
                "src": "322:26:2"
            }
        ]
    },
    "functionName": {

```

```

        "name": "add",
        "nodeType": "YulIdentifier",
        "src": "330:3:2"
    },
    "nodeType": "YulFunctionCall",
    "src": "330:18:2"
},
"variableNames": [
    {
        "name": "tail",
        "nodeType": "YulIdentifier",
        "src": "322:4:2"
    }
]
},
{
    "expression": {
        "arguments": [
            {
                "name": "value0",
                "nodeType": "YulIdentifier",
                "src": "402:6:2"
            },
            {
                "arguments": [
                    {
                        "name": "headStart",
                        "nodeType": "YulIdentifier",
                        "src": "415:9:2"
                    },
                    {
                        "kind": "number",
                        "nodeType": "YulLiteral",
                        "src": "426:1:2",
                        "type": "",
                        "value": "0"
                    }
                ]
            },
            {
                "name": "add",
                "nodeType": "YulIdentifier",
                "src": "411:3:2"
            }
        ],
        "nodeType": "YulFunctionCall",
        "src": "411:17:2"
    }
},
"functionName": {

```

```

        "name": "abi_encode_t_uint256_to_t_uint256_fromStack",
        "nodeType": "YulIdentifier",
        "src": "358:43:2"
    },
    "nodeType": "YulFunctionCall",
    "src": "358:71:2"
},
"nodeType": "YulExpressionStatement",
"src": "358:71:2"
}
]
},
"name":
"abi_encode_tuple_t_uint256_to_t_uint256__fromStack_reversed",
"nodeType": "YulFunctionDefinition",
"parameters": [
    {
        "name": "headStart",
        "nodeType": "YulTypedName",
        "src": "284:9:2",
        "type": ""
    },
    {
        "name": "value0",
        "nodeType": "YulTypedName",
        "src": "296:6:2",
        "type": ""
    }
],
"returnVariables": [
    {
        "name": "tail",
        "nodeType": "YulTypedName",
        "src": "307:4:2",
        "type": ""
    }
],
"src": "214:222:2"
},
{
    "body": {
        "nodeType": "YulBlock",
        "src": "487:81:2",
        "statements": [
            {
                "nodeType": "YulAssignment",
                "src": "497:65:2",
                "value": {

```

```

        "arguments": [
            {
                "name": "value",
                "nodeType": "YulIdentifier",
                "src": "512:5:2"
            },
            {
                "kind": "number",
                "nodeType": "YulLiteral",
                "src": "519:42:2",
                "type": "",
                "value": "0xffffffffffffffffffffffffffffffffffffffff"
            }
        ],
        "functionName": {
            "name": "and",
            "nodeType": "YulIdentifier",
            "src": "508:3:2"
        },
        "nodeType": "YulFunctionCall",
        "src": "508:54:2"
    },
    "variableNames": [
        {
            "name": "cleaned",
            "nodeType": "YulIdentifier",
            "src": "497:7:2"
        }
    ]
}

],
},
"name": "cleanup_t_uint160",
"nodeType": "YulFunctionDefinition",
"parameters": [
    {
        "name": "value",
        "nodeType": "YulTypedName",
        "src": "469:5:2",
        "type": ""
    }
],
"returnVariables": [
    {
        "name": "cleaned",
        "nodeType": "YulTypedName",
        "src": "479:7:2",
        "type": ""
    }
]

```

```

    }
  ],
  "src": "442:126:2"
},
{
  "body": {
    "nodeType": "YulBlock",
    "src": "619:51:2",
    "statements": [
      {
        "nodeType": "YulAssignment",
        "src": "629:35:2",
        "value": {
          "arguments": [
            {
              "name": "value",
              "nodeType": "YulIdentifier",
              "src": "658:5:2"
            }
          ],
          "functionName": {
            "name": "cleanup_t_uint160",
            "nodeType": "YulIdentifier",
            "src": "640:17:2"
          },
          "nodeType": "YulFunctionCall",
          "src": "640:24:2"
        },
        "variableNames": [
          {
            "name": "cleaned",
            "nodeType": "YulIdentifier",
            "src": "629:7:2"
          }
        ]
      }
    ]
  },
  "name": "cleanup_t_address",
  "nodeType": "YulFunctionDefinition",
  "parameters": [
    {
      "name": "value",
      "nodeType": "YulTypedName",
      "src": "601:5:2",
      "type": ""
    }
  ]
},

```



```

        "nodeType": "YulExpressionStatement",
        "src": "751:37:2"
      }
    ]
  },
  "name": "abi_encode_t_address_to_t_address_fromStack",
  "nodeType": "YulFunctionDefinition",
  "parameters": [
    {
      "name": "value",
      "nodeType": "YulTypedName",
      "src": "729:5:2",
      "type": ""
    }
  ]
}
{
  "contractName": "product",
  "abi": [
    {
      "inputs": [
        {
          "internalType": "uint256",
          "name": "",
          "type": "uint256"
        }
      ],
      "name": "productItems",
      "outputs": [
        {
          "internalType": "uint256",
          "name": "productId",
          "type": "uint256"
        },
        {
          "internalType": "bytes32",
          "name": "productSN",
          "type": "bytes32"
        },
        {
          "internalType": "bytes32",
          "name": "productName",
          "type": "bytes32"
        },
        {
          "internalType": "bytes32",
          "name": "productBrand",
          "type": "bytes32"
        }
      ]
    }
  ]
}

```

```

        "internalType": "uint256",
        "name": "productPrice",
        "type": "uint256"
    },
    {
        "internalType": "bytes32",
        "name": "productStatus",
        "type": "bytes32"
    }
],
"stateMutability": "view",
"type": "function"
},
{
    "inputs": [
        {
            "internalType": "bytes32",
            "name": "",
            "type": "bytes32"
        }
    ],
    "name": "productMap",
    "outputs": [
        {
            "internalType": "uint256",
            "name": "",
            "type": "uint256"
        }
    ],
    "stateMutability": "view",
    "type": "function"
},
{
    "inputs": [
        {
            "internalType": "bytes32",
            "name": "",
            "type": "bytes32"
        }
    ],
    "name": "productsForSale",
    "outputs": [
        {
            "internalType": "bytes32",
            "name": "",
            "type": "bytes32"
        }
    ]
},

```

```

    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [
      {
        "internalType": "bytes32",
        "name": "",
        "type": "bytes32"
      }
    ],
    "name": "productsManufactured",
    "outputs": [
      {
        "internalType": "bytes32",
        "name": "",
        "type": "bytes32"
      }
    ],
    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [
      {
        "internalType": "bytes32",
        "name": "",
        "type": "bytes32"
      }
    ],
    "name": "productsSold",
    "outputs": [
      {
        "internalType": "bytes32",
        "name": "",
        "type": "bytes32"
      }
    ],
    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [
      {
        "internalType": "bytes32",
        "name": "",
        "type": "bytes32"
      }
    ],

```

```

    {
      "internalType": "uint256",
      "name": "",
      "type": "uint256"
    }
  ],
  "name": "productsWithConsumer",
  "outputs": [
    {
      "internalType": "bytes32",
      "name": "",
      "type": "bytes32"
    }
  ],
  "stateMutability": "view",
  "type": "function"
},
{
  "inputs": [
    {
      "internalType": "bytes32",
      "name": "",
      "type": "bytes32"
    },
    {
      "internalType": "uint256",
      "name": "",
      "type": "uint256"
    }
  ],
  "name": "productsWithSeller",
  "outputs": [
    {
      "internalType": "bytes32",
      "name": "",
      "type": "bytes32"
    }
  ],
  "stateMutability": "view",
  "type": "function"
},
{
  "inputs": [
    {
      "internalType": "uint256",
      "name": "",
      "type": "uint256"
    }
  ]
}

```

```
],  
"name": "sellers",  
"outputs": [  
  {  
    "internalType": "uint256",  
    "name": "sellerId",  
    "type": "uint256"  
  },  
  {  
    "internalType": "bytes32",  
    "name": "sellerName",  
    "type": "bytes32"  
  },  
  {  
    "internalType": "bytes32",  
    "name": "sellerBrand",  
    "type": "bytes32"  
  }  
]
```