A

Project Report

on

Product Authentication using Blockchain

submitted for partial fulfillment for the award of

BACHELOR OF TECHNOLOGY

DEGREE

in

Computer Science

By

Abhishek Singh Yadav (2000290120011)
Aditi Batra (2000290120012)
Anurag Tripathi (2000290120036)
Kshitij Pal (2000290310092)

Under the Supervision of

Ms. Shivani
Assistant Professor

Department of Computer Science
KIET Group of Institutions, Ghaziabad
Affiliated to
Dr. A.P.J. Abdul Kalam Technical University, Lucknow

May 2024

DECLARATION

I hereby declare that this submission is my work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material that to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Abhishek Singh Yadav (2000290120011)
Aditi Batra (2000290120012)
Anurag Tripathi (2000290120036)
Kshitij Pal (2000290310092)

Date:

CERTIFICATE

This is to certify that the Project Report entitled "**Product Authentication using Blockchain"** which is submitted by **Abhishek Singh Yadav, Aditi Batra, Anurag Tripathi, and Kshitij Pal** in partial fulfillment of the requirement for the award of degree B. Tech. in the Department of Computer Science of Dr. A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidate's work carried out by him under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Date: **Supervisor Signature**

Ms. Shivani
Assistant Professor
Department of Computer Science

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the project report of the B.Tech. Major Project was undertaken during B.Tech. Fourth Year. We owe a special gratitude to Prof. Shivani, Assistant Professor, Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for her constant support and guidance throughout our work. Her sincerity, thoroughness, and perseverance have been a constant source of inspiration for us. It is only his/her cognizant efforts that our endeavors have seen the light of day.

We also take the opportunity to acknowledge the contribution of Dr. Ajay Kumar Shrivastava, Head of the Department, Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the department's faculty members for their kind assistance and cooperation during thedevelopment of our project.

Last but not least, we acknowledge our friends for their contribution to the completion of the project.

Signature:
Aditi Batra
2000290120012

Signature:
Anurag Tripathi
2000290120036

Signature:
Abhishek Singh Yadav
2000290120011

Signature:
Kshitij Pal
2000290310092

TABLE OF CONTENTS

ABSTRACT

Counterfeit products pose a significant problem in the global market, affecting industries from medicine to consumer electronics. To address this, our proposal aims to leverage blockchain technology for product authentication, offering a robust solution to ensure product genuineness. At the heart of this initiative are smart contracts, which play a crucial role in securely recording product information on the blockchain's immutable ledger. This setup creates a reliable environment where consumers can easily verify product authenticity, thereby deterring fraudulent activities.

Throughout the project, blockchain technology serves as a guiding force, acting as both the foundation for trust and the mechanism for ensuring security. This technology's unique characteristics are leveraged in various sectors, including finance, medicine, manufacturing, and education, each benefiting from blockchain's robust security and transparency. This approach builds a solid foundation for consumer trust while combating the pervasive issue of counterfeit products.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

dApp: Decentralized App

BT: Blockchain Technology

QR: Quick Response

API: Application Programming Interface

AI: Artificial Intelligence

IoT: Internet of Things

IP: Internet Protocol

SSL: Secure Socket Layer

SDLC: Software Development Life Cycle

DFD: Data Flow Diagram

ER: Entity Relationship

CHAPTER 1
INTRODUCTION

1.1 Introduction to Project

Product certification can reflect product quality, maintain product reputation, and protect the legitimate rights and interests of consumers, however, with the continuous increase in the number and types of products sold by online platforms, the possibility of consumers buying fake and shoddy products has gradually increased. This violates the consumers' legitimate rights and interests and leads consumers to question product brand reputation, therefore, the market demand for product certification is constantly increasing. Blockchains are distributed and decentralized databases. On a blockchain, both parties do not need to reach a consensus or rely on third-party agencies to conduct transactions.

The transactions on the chain are traceable, undeniable, and nonmodifiable, which can well ensure the credibility of transactions. Currently, blockchains are widely used in different application scenarios, such as product certification, the Internet of Things, supply chain, and smart cities to ensure data security and traceability. Therefore, in this project, we came up with the idea of using unbreachable blockchain technology to verify or authenticate the credibility of a product. We will store the product's information, based on blockchain technology, and let the consumer see whether the product they are about to use is legitimate or not.

1.2 Project Category

1.2.1 Applications of Technology and Blockchain

This project is in the technology category, with a particular emphasis on blockchain applications. With its reputation for being decentralized and unchangeable, blockchain technology is being investigated more and more for uses outside of cryptocurrencies. Blockchain technology is used in this project to improve the processes involved in product certification and verification. Utilizing the transparency, security, and tamper-proof characteristics of blockchain technology, the initiative seeks to mitigate the issues associated with low-quality and counterfeit products on online marketplaces. This creative method demonstrates how blockchain technology can transform conventional systems and promote confidence in digital ecosystems, which is in line with the rapidly changing landscape of blockchain applications.

1.3 Objectives

The main objective of this project is to authenticate a product. Other specific objectives are as follows:

- Develop a blockchain-based system to combat counterfeit goods.
- Use smart contracts to securely and automatically validate product information.
- Ensure immutability and transparency of product data to prevent unauthorized modifications.
- Enhance consumer trust with a reliable method for verifying product authenticity.

1.4 Structure of Report

Chapter 1

The report outlines the development of a blockchain-based product authentication system. It begins with an introduction highlighting the need for product certification amidst rising online sales and counterfeit products. Emphasizing blockchain's potential, it delves into project categories, particularly focusing on technology and blockchain applications. Objectives include reducing counterfeit products, enhancing the company's reputation, and improving consumer-producer relations. The report's structure entails a comprehensive exploration of project implementation, including methodologies, results, and conclusions, with a focus on achieving transparent and credible product authentication.

Chapter 2

This chapter deep dives into a comprehensive literature review on blockchain technology and its applications, focusing on product authentication and traceability. Various scholarly papers are summarized, highlighting key insights into blockchain architecture, smart contracts, and frameworks for combating counterfeiting. Research gaps include interoperability challenges, scalability issues, and security concerns. The chapter formulates the problem statement, addressing the urgent need for innovative solutions to ensure product authenticity and quality in online markets. The project aims to establish a decentralized and tamper-proof system for product certification through blockchain technology, enhancing consumer trust and market integrity.

Chapter 3

This chapter outlines the proposed system for combating counterfeit goods using blockchain technology. It emphasizes features such as blockchain integration, smart contract implementation, user-friendly interface, MetaMask integration, real-time tracking, QR code generation, enhanced transparency, and scalability. The system's unique approach ensures decentralized, tamper-resistant product authentication, distinguishing it from existing methods.

Chapter 4

This chapter delves into the requirement analysis and system specifications for implementing a blockchain-based product authentication system. It conducts a feasibility study encompassing technical, economic, and operational aspects. The software requirement specification outlines the system's introduction, overall description, assumptions, and dependencies. It details the proposed methodology, operating environment, constraints, external interface requirements, and non-functional requirements.

Chapter 5

This chapter introduces the implementation phase, outlining the languages, tools, and technologies employed in developing the blockchain-based product authentication system. It highlights the utilization of Solidity, JavaScript, HTML/CSS, Truffle Suite, Ganache, MetaMask, Node.js, Web3.js, and QR Code Generator. This comprehensive approach aims to ensure robustness and security in product authentication, enhancing confidence and transparency for consumers and stakeholders.

Chapter 6

This chapter focuses on testing and maintenance, detailing various testing techniques and test cases employed. Test cases cover user registration, login, product registration, and product verification scenarios, ensuring the system's functionality, reliability, and security. This meticulous testing process aims to deliver a high-quality and dependable product authentication system.

Chapter 7

This chapter showcases the results and discussions of the implemented system, presenting user interface representations, module descriptions, snapshots, back-end representations, and database tables. It provides insights into the various functionalities and components of the system, illustrating how manufacturers register products, users authenticate them, and smart contracts ensure transaction integrity. The snapshots offer a visual understanding of the system's interface and backend processes, enhancing comprehension.

Chapter 8

This chapter concludes the report by summarizing the research's significance in utilizing blockchain for product authentication, emphasizing consumer protection and market trust. It outlines future scope, suggesting avenues for improvement like IoT integration and smart contract automation, to enhance product quality assurance and brand reputation.

CHAPTER 2
LITERATURE REVIEW

2.1 Literature Review

With its roots in Bitcoin, blockchain technology has gained a lot of interest lately because of its potential to revolutionize several industries. Blockchain serves as an immutable record that enables decentralized transaction processing while providing security and transparency. Applications for it have proliferated in fields such as the Internet of Things (IoT), finance, and reputation management. However, blockchain still has problems, including issues with scalability and security. This paper presents a thorough analysis of blockchain technology [1], beginning with a summary of its architecture. We explore the complexities of standard consensus methods used on various blockchains and explain their advantages and disadvantages. We also provide our perspectives on the technological obstacles and recent advancements that blockchain faces. These obstacles, which range from security flaws to scalability problems, necessitate coordinated efforts to overcome them.

Nevertheless, we are still positive about blockchain's future despite these difficulties. We envisage improvements in layer-two protocols and sharding as scalability solutions to increase transaction throughput. Furthermore, advances in security mechanisms—such as strong encryption methods and consensus algorithms—will strengthen blockchain's resistance to malevolent attacks. Furthermore, there is a great deal of promise for expanding the use cases and promoting the widespread use of blockchain technology through its integration with cutting-edge fields like artificial intelligence (AI) and the Internet of Things (IoT). We expect blockchain to spread throughout industries and become woven into the very fabric of our digital economy as it continues to develop. Blockchain is positioned to realize its disruptive potential with collaboration from industry partners and continued research and development activities.

The rise of cryptocurrencies and blockchain technology in recent years has given new life to Szabo's initial concept of smart contracts. Computer protocols known as "smart

contracts" are made to automatically enable, validate, and uphold digital contracts in place of middlemen. Their possible uses include the Internet of Things (IoT), healthcare, management, finance, and other domains. These weaknesses were highlighted by the infamous "The DAO Attack" in June 2016, which resulted in the loss of nearly $50 million worth of Ether.

This paper aims to provide a thorough and organized overview of blockchain-enabled smart contracts [2] to encourage additional study in this rapidly developing topic. The paper first presents the general platforms and workings of blockchain-enabled smart contracts. It suggests a six-layer architecture research framework that offers an organized method for researching smart contracts. The presentation then outlines the legal and technological difficulties related to smart contracts as well as the latest developments in resolving these problems.

All things considered, this research makes a significant contribution to our understanding of blockchain-enabled smart contracts by shedding light on their working processes, difficulties, potential uses, and future possibilities. The study seeks to direct and inspire future research efforts in this dynamic and quickly expanding topic by offering a thorough overview and research strategy.

An overview of Hyperledger, Ethereum, and blockchain technology [3] that is both brief and educational may be found in the paper "Hyperledger, Ethereum, and Blockchain Technology: A Short Overview". It seeks to provide an understanding of these platforms and the technology that powers them, illuminating their features, capabilities and uses in a range of industries.

The writers start by outlining blockchain, Ethereum, and Hyperledger technologies and emphasizing their importance in the digital world. The Linux Foundation is the home of Hyperledger, an open-source collaborative project aimed at promoting blockchain technologies across industries. It provides an adaptable framework with several tools and modules designed for enterprise use cases, including identity management, supply chain management, and healthcare.

Ethereum, on the other hand, is described as a decentralized platform that facilitates the development and operation of decentralized apps (dApps) and smart contracts. It is based on blockchain technology and comes with Solidity, a Turing-complete programming language that lets programmers write sophisticated smart contracts with

a wide range of capabilities.

This article explores the architectural distinctions between Ethereum and Hyperledger, clarifying the design principles and consensus techniques of each platform. Hyperledger is suited for enterprise-grade applications that need privacy and scalability because it emphasizes permissioned blockchains, where participants are recognized and vetted. Conversely, Ethereum functions as a permissionless blockchain, enabling anyone to join the network and carry out smart contracts without a permit.

The paper "Framework for Product Anti-Counterfeiting using Blockchain Technology" [4] offers a thorough framework for using blockchain technology to prevent product counterfeiting. In many different industries, counterfeiting seriously jeopardizes consumer safety, brand integrity, and market integrity. Conventional anti-counterfeiting methods frequently fail to adequately handle this widespread problem. Innovative technologies that can guarantee product authenticity and traceability along the supply chain are therefore desperately needed.

Moreover, the architecture includes a data analytics component that uses the abundance of data kept on the blockchain to extract useful insights. Algorithms for data analytics examine transaction data, spot trends, and look for abnormalities that could be signs of fraud. This module improves anti-counterfeiting efforts and makes it possible to take pre-emptive steps against counterfeiters by utilizing big data and machine learning.

Using blockchain technology, the article concludes with a strong foundation for product anti-counterfeiting, providing a viable answer to an enduring and complicated issue. The architecture improves supply chain transparency, consumer confidence, and product authenticity by utilizing blockchain's special qualities. In addition, the report emphasizes how crucial it is to keep innovating and working together to advance blockchain-based anti-counterfeiting initiatives that safeguard customers and maintain market integrity.

R. S. Bhatnagar, S. M. Jha, S. S. Singh, and R. Shende's study "Product Traceability Using Blockchain" [5] examines the use of blockchain technology in product traceability. Robust traceability solutions are in greater demand as global supply chains expand and worries about product safety and authenticity develop.

Conventional traceability techniques frequently include drawbacks including data silos, a lack of openness, and a vulnerability to manipulation. Blockchain technology provides a decentralized, transparent, and unchangeable ledger for product transactions, which presents a viable solution to these problems.

In-depth descriptions of the main elements and features of blockchain-based product traceability systems' architecture are provided in this article. The blockchain, which acts as a distributed ledger to record all product-related transactions, lies at the heart of this system. The writers go over the use of smart contracts in automating and enforcing traceability regulations in addition to the blockchain. Self-executing contracts, or smart contracts, are designed to carry out predetermined tasks in response to specific events.

The study concludes by highlighting how blockchain technology has the potential to revolutionize product traceability. Blockchain offers a potent way to improve supply chain accountability and visibility by offering a decentralized, transparent, and unchangeable ledger. However, resolving organizational, technical, and regulatory issues is necessary for a successful deployment. Blockchain-based product traceability has the potential to transform supply chain management and guarantee the integrity and authenticity of products throughout their lifecycle through more study, cooperation, and innovation.

The paper "A Journey of WEB and Blockchain towards Industry 4.0: An Overview" [6] offers a thorough analysis of how blockchain technology and web technologies are merging within the framework of Industry 4.0. Explaining how the integration of these technologies is changing industrial processes and propelling the shift toward the fourth industrial revolution is the goal of Writers AG. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz, and T. M. Alam.

The first section of the paper introduces the idea of Industry 4.0, which is the introduction of digital technology into industrial processes and manufacturing to create "smart factories." To support autonomous, networked, and data-driven operations, these smart factories make use of technologies like the Internet of Things (IoT), blockchain, artificial intelligence (AI), and big data analytics.

The writers stress how important it is for web technologies to support data sharing, teamwork, and communication in Industry 4.0 settings. In smart factories, web-based

platforms and protocols—like WebSocket and RESTful APIs—are the foundation for facilitating smooth integration and interoperability across diverse systems and devices.

The report concludes by highlighting how combining blockchain and web technologies can revolutionize the way we move toward Industry 4.0. Through the utilization of these technologies advantages, businesses can develop production systems that are more intelligent, effective, and durable. But to make this vision a reality, more research, creativity, and cooperation are needed to address organizational, technical, and regulatory obstacles. All things considered, the study offers insightful information on how Industry 4.0 is developing and how web and blockchain technologies will affect its direction.

Table 2.1 Literature Review

PAPER TITLE	AUTHORS	PUBLISH YEAR	SUMMARY
An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends	Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang	2017	Provides a comprehensive overview of blockchain technology, covering architecture, consensus mechanisms, and future trends
Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends	S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.-Y. Wang	2019	Explores the architecture, applications, and future trends of blockchain-enabled smart contracts, highlighting their significance in various industries.
Hyperledger, Ethereum and	A.H. Mohammed, A.	2021	Offers a brief overview of Hyperledger, Ethereum,

Blockchain Technology: A Short Overview	A. Abdulateef, I. A. Abdulateef		and blockchain technology, providing insights into their features and potential applications.
Framework for Product Anti-Counterfeiting Using Blockchain Technology	P. William, D. Jadhav, P. Cholke, M. A. Jawale, A. B. Pawar	2022	Presents a framework for combating product counterfeiting using blockchain technology, offering strategies to enhance product authentication.
Product traceability using blockchain	R. S. Bhatnagar, S. M. Jha, S. S. Singh, R. Shende	2020	Discusses the implementation of blockchain for product traceability, focusing on its role in improving transparency and accountability in supply chains.
A Journey of WEB and Blockchain Towards Industry 4.0: An Overview	AG. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz, T. M. Alam	2019	Explores the integration of web and blockchain technologies towards Industry 4.0, highlighting their combined impact on various industrial sectors

2.2 Research Gaps

2.2.1 Interoperability Challenges:

- Diverse blockchain platforms lack standardized interoperability.
- Research needed for seamless data exchange across different blockchain ecosystems.

2.2.2 Scalability and Performance:

- Blockchain systems face limitations in handling large-scale authentication requests.
- Research focuses on optimizing throughput, reducing latency, and enhancing network scalability.

2.2.3 Security and Privacy Concerns:

- Blockchain systems require stronger security against attacks and privacy breaches.
- Explore innovative cryptographic methods and privacy-enhancing technologies for enhanced data protection

2.3 Problem Formulation

The ease of use and wide range of options provided by internet platforms have completely changed how consumers obtain goods. Nonetheless, there are a lot of difficulties in this online market, especially when it comes to ensuring the authenticity and quality of the products. The quantity and variety of products that are offered online are expanding, putting consumers in greater danger of purchasing phony or inferior goods. In addition to belittling customer confidence, this also presents health and safety hazards.

Furthermore, the increased popularity of Internet shopping makes these problems worse since buyers do not have the tools necessary to confirm a product's legitimacy before making a purchase. This makes individuals susceptible to dishonest tactics and scams, which eventually erodes trust in internet-based businesses.

Thus, creative solutions that make use of cutting-edge technologies are desperately needed to improve the processes involved in product certification and verification. The goal of this project is to create a decentralized, tamper-proof system for product authenticity certification by utilizing blockchain technology. In addition to enabling customers to make knowledgeable judgments about what to buy, this kind of technology would increase integrity and trust in online markets.

CHAPTER 3
PROPOSED SYSTEM

3.1 Proposed System

The research introduces a groundbreaking method to combat counterfeit goods using blockchain technology for product authentication. Through blockchain's immutability, it safeguards product data, fostering trust among producers and consumers globally. Smart contracts play a vital role in validating product information and deterring counterfeiters. Future focus includes integrating the solution into supply chains, exploring real-time tracking, and automating supply chain operations. Leveraging public blockchains enhances accessibility and trust, with ongoing efforts to reinforce authenticity and confidence in product authentication. Through continuous innovation, the project aims to protect market integrity for the benefit of consumers and legitimate producers.

3.2 Unique Features of The System (Difference from Existing System)

Our project utilizes blockchain technology and smart contracts to revolutionize product authentication, offering a decentralized, tamper-resistant solution. By ensuring the openness and immutability of product data, we combat counterfeit goods and build trust between producers and consumers. Through transparency and automation, our project significantly impacts the market by deterring counterfeiters and protecting consumers and legitimate producers. Overall, our unique approach combines blockchain technology, smart contracts, and transparency to provide a reliable and secure solution to the pervasive issue of fake goods.

FEATURES:

- **Blockchain Integration**: The project leverages blockchain technology to ensure the security and immutability of product authentication data, providing a reliable foundation for verifying product authenticity.
- **Smart Contract Implementation**: Smart contracts are employed to automate and validate product registration processes, ensuring accuracy and efficiency while minimizing the need for manual intervention.
- **User-Friendly Interface**: The project features an intuitive and user-friendly interface for manufacturers to register products and for consumers to verify product authenticity easily using QR code scanning or uploading.
- **MetaMask Integration**: MetaMask integration adds an extra layer of security by requiring blockchain validation for product registration, enhancing trust and reliability in the authentication process.
- **Real-Time Tracking**: The system offers real-time tracking capabilities, allowing stakeholders to monitor product movements continuously, providing comprehensive insights, and enhancing supply chain transparency.
- **QR Code Generation**: Upon successful product registration, the system generates a unique QR code that can be affixed to the product, facilitating easy verification by consumers using smartphones or web browsers.

- **Enhanced Transparency**: By utilizing blockchain technology, the project promotes transparency in product authentication, fostering trust between consumers and manufacturers and deterring counterfeit activities effectively.
- **Scalability**: The architecture of the project is designed to be scalable, allowing for seamless integration with existing supply chain management systems and accommodating future expansion and growth.

Table 3.1 Comparative Analysis

Aspect	File-based Authentication	Blockchain-based Authentication
Data Storage	Data is stored in centralized files or databases.	Decentralized data and stored across a distributed ledger.
Security	Vulnerable to single points of failure and unauthorized access if the centralized system is compromised.	Enhanced security through cryptographic hashing, decentralization, and immutability of records.
Transparency	Limited transparency; users rely on the integrity of the central system.	Provides transparency with immutable records visible to all participants, enhancing accountability.
Trust Model	Relies on trust in centralized authorities managing the authentication system.	Based on trust in cryptographic algorithms and consensus mechanisms ensuring data integrity.
Scalability	Challenging, with increasing data volume and user base.	Offers scalability with distributed nodes processing transactions concurrently.

CHAPTER 4
REQUIREMENT ANALYSIS AND SYSTEM SPECIFICATION

4.1 Feasibility Study

4.1.1 Technical Feasibility

- **Blockchain Integration:** Ethereum and Hyperledger are two blockchain protocols that must be thoroughly understood to implement blockchain for product authentication.
- **Smart Contracts Development:** Writing secure and effective contracts requires familiarity with programming languages such as Solidity, which is necessary for developing smart contracts.
- **Database management:** The system's effectiveness depends on the effective storage, retrieval, and indexing of product data on the blockchain**.**

4.1.2 Economic Feasibility

- **Resource Allocation:** Estimating how much money will be needed to pay for maintaining the system, employing qualified developers, and purchasing the required hardware and software.
- **Return on Investment:** Calculating the difference between the initial investment and ongoing operating expenses and the possible cost savings from fewer instances of counterfeit products.
- **Market Demand:** Examining the need for product authentication solutions in the market as well as prospective sources of income like subscription or license fees.

4.1.3 Operational Feasibility

- **User Training:** Educating consumers and manufacturers on the steps involved in product verification and registration**.**
- **Supply Chain Integration:** To reduce disturbance, make sure that current supply chain management systems and procedures integrate seamlessly.
- **Regulatory Compliance:** Regulatory compliance is the process of abiding by legal and regulatory obligations, such as industry-specific standards and data privacy laws, to stay out of trouble with the law and avoid penalties.

4.2 Software Requirement Specification Document

4.2.1 Introduction

Several businesses have struggled for years with the problem of fake goods being marketed to unwary customers. Customers now find it more challenging to distinguish between real and phony goods due to the growth of e-commerce and online marketplaces. The selling of counterfeit goods is still a major issue, costing consumers and legitimate businesses money, despite the efforts of brands and regulatory organizations. Yet, there may be a solution to this problem with the development of blockchain technology. A secure and trustworthy method for product authentication can be developed by utilizing the transparency and immutability of blockchain, ensuring that customers can buy authentic products with confidence.

This software system's purpose is to offer a solution for product authentication that makes use of blockchain technology to guarantee the authenticity of products. Using blockchain technology, the system will let product makers give each product a digital identity that users can access via a smartphone application. Customers can scan a product's QR code with the mobile application to verify its authenticity. The system will also allow product makers to monitor the flow of goods via the supply chain, preventing the introduction of fake goods.

4.2.2 Overall Description

4.2.2.1 Product Perspective

Blockchain technology will be included in the software system to offer a reliable and secure mechanism for product authentication. Using blockchain technology, the system will let product makers give each product a digital identity that users can access via a smartphone application. Customers can scan a product's QR code with the mobile application to verify its authenticity. The system will also allow product makers to monitor the flow of goods via the supply chain, preventing the introduction of fake goods.

The software system will be compatible with existing systems and will provide an API for integration. The system will use secure cryptographic algorithms to

protect the digital identities of products and will comply with relevant data protection regulations.

4.2.2.2 Product Functions

The software system will have the following functions:

- **Product Identity Creation**: The system will allow product producers to build a digital identity for each product using blockchain technology.
- **Product Movement Tracking**: The system will enable product manufacturers to track the movement of products through the supply chain.
- **Mobile Application**: Customers will be able to scan a product's barcode to confirm its authenticity using the system's mobile application. The mobile application will be available for both Android and iOS platforms.
- **Real-Time Authentication**: The system will be able to authenticate products in real-time, allowing customers to quickly and easily verify the authenticity of a product.
- **API Integration**: The system will provide an API for integration with existing systems.
- **Data Protection**: The system will use secure cryptographic algorithms to protect the digital identities of products and will be compliant with relevant data protection regulations.

4.2.2.3 User Characteristics

- **Customers**: Customers will be the primary users of the system. They should have basic experience in utilizing a mobile application and the ability to scan barcodes.
- **Product manufacturers** will use the system to give their goods digital identities and follow their progress through the supply chain. They ought to be familiar with supply chain management and blockchain technology on a fundamental level.
- **System Administrators**: System administrators will be responsible for managing the software system. They should be highly skilled in database management, blockchain technologies, and software development

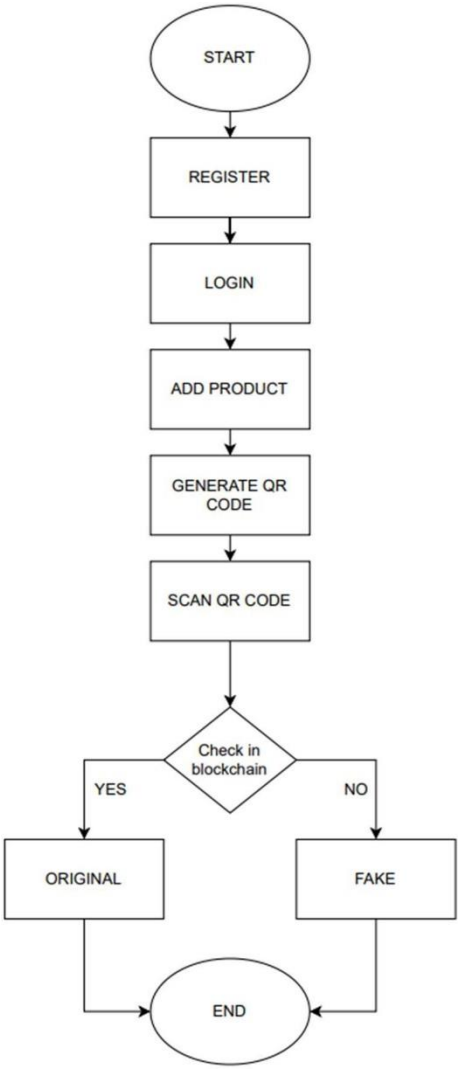

Fig. 4.1 Proposed Methodology-Flowchart

STEPS:

1. The manufacturer initiates the registration process by providing a unique ID and password.
2. Clicking the register button triggers a MetaMask confirmation prompt for blockchain validation.
3. The manufacturer logs in with the same credentials and proceeds to register a product.

4. The manufacturer inputs a unique product ID and name during product registration.
5. Addition to blockchain confirmed by clicking the “add” button, triggering MetaMask confirmation.
6. Upon successful registration, a corresponding QR code is generated for download.
7. QR code affixed to product for authentication.
8. Users or customers scan/upload QR code on the website.
9. System verifies product authenticity, displaying relevant information.
10. Confirm whether the product is genuine or counterfeit.

4.2.2.4 Operating Environment

The software system will operate in the following environment:

- **Hardware**: The system will require a server to host the blockchain network and the database for product authentication and supply chain tracking. To process large numbers of transactions, the server needs to have enough processing power and memory.
- **Software**: The system will require blockchain software, database management software, and a mobile application for customers. The database management software should be able to handle large amounts of data, and the blockchain software should be compatible with the server's operating system.
- **Network**: The system will require a secure network connection to ensure the privacy and integrity of data. The network should be protected with firewalls and other security measures to prevent unauthorized access.
- **Operating system**: The blockchain software and database management software should work together with the server's operating system. Both the Android and iOS operating systems should be supported by the customer's mobile application.

- **Maintenance**: The system will require regular maintenance and updates to ensure optimal performance and security. This includes updating software versions, keeping an eye out for bugs and security holes, and applying patches and fixes as necessary.
- **Backup and recovery**: In the event of a system failure or disaster, the system should have a backup and recovery plan in place to guarantee that data is not lost. A recovery plan should be created to restore the system in the event of a failure, and regular backups should be made and stored on-site.

4.2.2.4 Constraints

- **Security**: The software system must be designed with robust security measures to ensure the protection of digital identities and prevent unauthorized access to the system. The system must be compatible with current devices and systems and must offer APIs for simple integration.
- **Data Privacy**: The system must comply with relevant data privacy regulations, such as GDPR, and ensure that customer data is protected.
- **Performance**: The system must be designed to handle high numbers of product authentication requests in real time.
- **Cost**: The system must be cost-effective and provide value to both customers and product manufacturers.
- **Scalabilit**y: The system must be designed to scale as the number of products and users grows.

4.2.3 Assumptions and Dependencies

4.2.3.1 Assumptions

Product manufacturers will be willing to participate in the system and create digital identities for their products. Customers will be willing to use the mobile application to authenticate products and will have access to mobile devices and internet connectivity.

- Product barcodes will be unique and accurately depict the product's identification.

- The blockchain network and database will be secure, reliable, and capable of handling high volumes of transactions.
- The system will comply with relevant regulations and industry standards for data privacy and security.
- The system will be scalable and versatile to adapt to changing company needs and technology improvements.

4.2.3.2 Dependencies

- **Blockchain Technology**: The system depends on the availability and reliability of blockchain technology to provide a secure and tamper-proof method of tracking products through the supply chain.
- **QR code Scanners**: The system depends on the availability of barcode scanners to scan product barcodes and verify their authenticity.
- **Mobile Devices**: The system depends on the availability of mobile devices to run the mobile application for customers.
- **Internet Connectivity**: The system depends on the availability and reliability of internet connectivity to connect to the blockchain network, database, and mobile application.

4.2.4 EXTERNAL INTERFACE REQUIREMENTS

4.2.4.1 User Interfaces

- **Mobile Application for Customers**: The mobile application will allow customers to scan the product's QR code and check their legitimacy. The interface will be intuitive and user-friendly, providing clear instructions and feedback to the user.
- **Web Application for Product Manufacturers**: The web application will allow product manufacturers to create digital identities for their products and track them through the supply chain. The interface will be secure and accessible only to authorized users.

4.2.4.2 Hardware Interfaces

- **QR code Scanners**: To scan the product's QR code and confirm its authenticity, the system will interface with barcode scanners.

- **Mobile Devices**: To access the camera and internet connectivity features, the mobile application will interface with mobile devices.
- **Server:** The system will require a server to host the blockchain network and the database for product authentication and supply chain tracking. The system will interface with the server's hardware components, such as processors, memory, and storage devices.

4.2.4.3 Software Interfaces

- **Blockchain Software**: The system will utilize blockchain software to provide a secure and tamper-proof method of tracking products through the supply chain. The blockchain software will interface with the database management software to store and retrieve product information.
- **Database Management Software**: The system will utilize database management software to store and retrieve product information. The database management software will interface with the blockchain software to ensure data integrity and security.

4.2.4.4 Communication Interfaces

- **Mobile Data Network**: The mobile application will communicate with the blockchain network and the database management software through the mobile data network. For the system to authenticate products in real-time, it will need a strong and dependable mobile data connection.
- **Internet Protocol (IP) Network**: Using the IP network, the web application for manufacturers of goods will interact with the blockchain network and the database management program. The system will require a stable and reliable IP network connection to create and track digital identities for products.
- **Application Programming Interface (API)**: The system will operate an API that enables access to the database management system and the blockchain network by third-party applications. The API will enable integration with other systems, such as e-commerce platforms, to provide seamless product authentication and supply chain tracking.

- **Secure Sockets Layer (SSL)**: The system will utilize SSL to provide secure communication between the mobile application, the web application, and the server hosting the blockchain network and the database management software. SSL will ensure data confidentiality and integrity during transmission.
- **Messaging Protocol**: The system will utilize a messaging protocol to provide real-time notifications to customers and product manufacturers regarding product authentication and supply chain tracking. The messaging protocol will ensure timely and accurate communication between the system components.

4.2.5 Other Non-Functional Requirements

- **Performance Requirements:** The system shall be able to authenticate products in less than 3 seconds. A daily minimum of 10,000 authentication requests must be handled by the system. The system shall have a 99.9% uptime.
- **Security Requirements:** The system shall use secure cryptographic algorithms to protect the digital identities of products and multi-factor authentication for user accounts. The system shall be compliant with relevant data protection regulations.

4.2.5.1 Software Quality Attributes

- **Scalability**: The system will have a strong capacity for growth, allowing it to support an increasing quantity of goods and users on the blockchain network. Also, the system will be able to process a large number of transactions instantly.
- **Usability**: The system will be user-friendly, offering customers and product makers a straightforward and intuitive interface to obtain product information and follow supply chain data. Also, the system will give the user feedback and clear directions.
- **Maintainability**: With a modular and scalable design that enables simple upgrades and improvements, the system will be simple to maintain. In the event of a problem, the system will also be simple to troubleshoot and diagnose.

- Customers and product producers will be able to access the system from a variety of platforms and devices because of the system's compatibility with different operating systems, browsers, and mobile devices.

4.2.5.2 Business Rules

- Throughout the production process, a special identifying number must be assigned to each product.
- Any transactions involving the supply chain, such as product transfers and ownership changes, must be documented on the blockchain network.
- Access to and modification of product data on the blockchain network is restricted to authorized parties such as product makers and distributors.
- To confirm a product's validity, customers must be able to scan or input its unique identification number.
- On the blockchain network, any attempt to alter or tamper with product data must be found and stopped.
- In the event of any suspicious activity or product fraud, the system must immediately notify product makers and distributors.
- Product authentication and supply chain tracking laws and regulations must be adhered to by the system.
- Every product transaction and activity on the blockchain network must have a clear and verifiable audit trail provided by the system.
- Customers and product makers must be able to obtain product information and track supply chain data through the system's user-friendly interface.
- All product data and transaction privacy and security on the blockchain network must be guaranteed by the system.

4.2.6 Other Requirements

Blockchain: It is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Key elements of Blockchain:

- **Distributed ledger technology**: All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.
- **Immutable records**: No participant can change or tamper with a transaction after it's been recorded in the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.
- **Smart contracts**: To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically.
- **Ethereum**: Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority.
- **QR code**: A QR code (Quick Response code) is an array of black and white squares or pixels set in a grid that stores data for a machine to read. A smartphone or camera can quickly process the information contained in a QR code's specific arrangement of pixels, making it a convenient way to store and access data.

4.3 SDLC Model Used

We applied the Agile paradigm to our project to improve productivity and flexibility. The agile technique divides the project into smaller units called sprints, which have a duration of two to four weeks on average.

We work as a team to prioritize jobs according to their priority and complete them within each sprint. With the help of this iterative process, we can efficiently meet the client's expectations by continuously gathering feedback and making improvements as we go.

Using Agile principles, which include regular communication, adaptability, and customer involvement, we were able to produce excellent outcomes on schedule and in response to changes quickly.

4.4 System Design

4.4.1 Data Flow Diagram

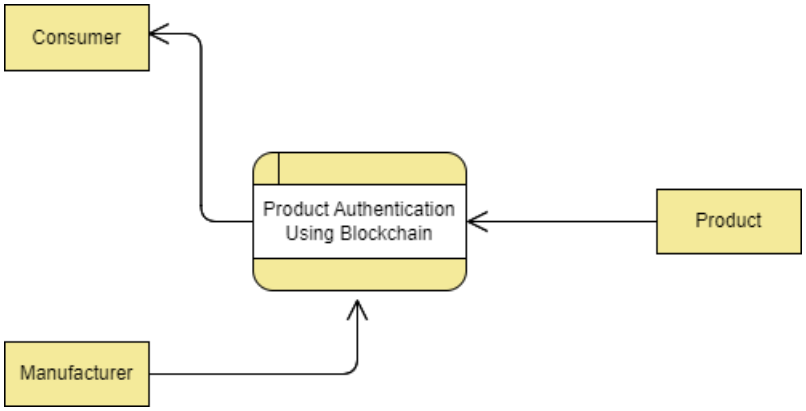

Fig. 4.2 Level – 0 DFD

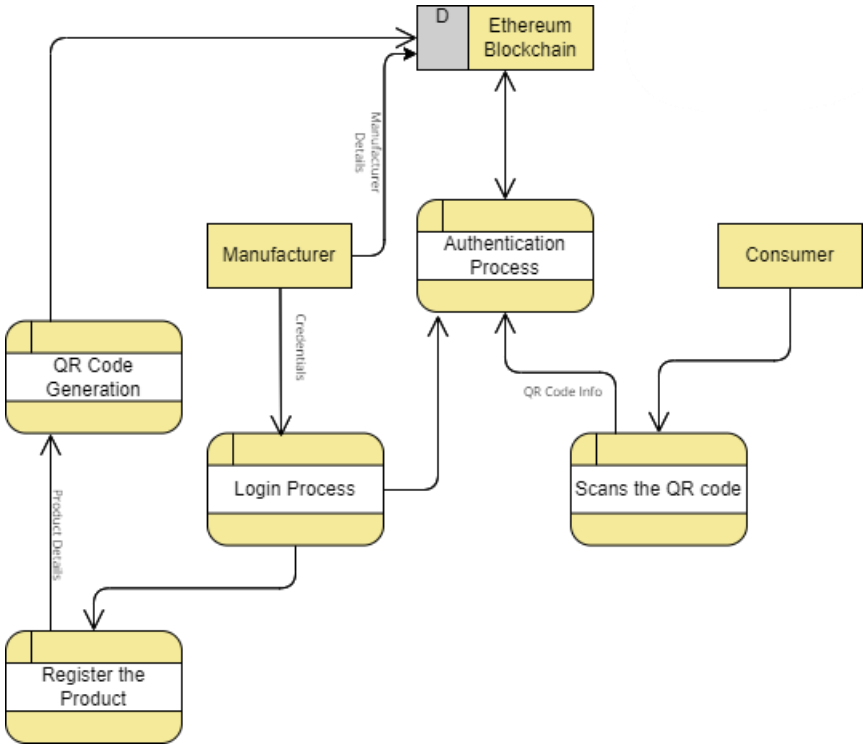

Fig. 4.3 Level – 1 DFD

4.4.2 ER Diagram

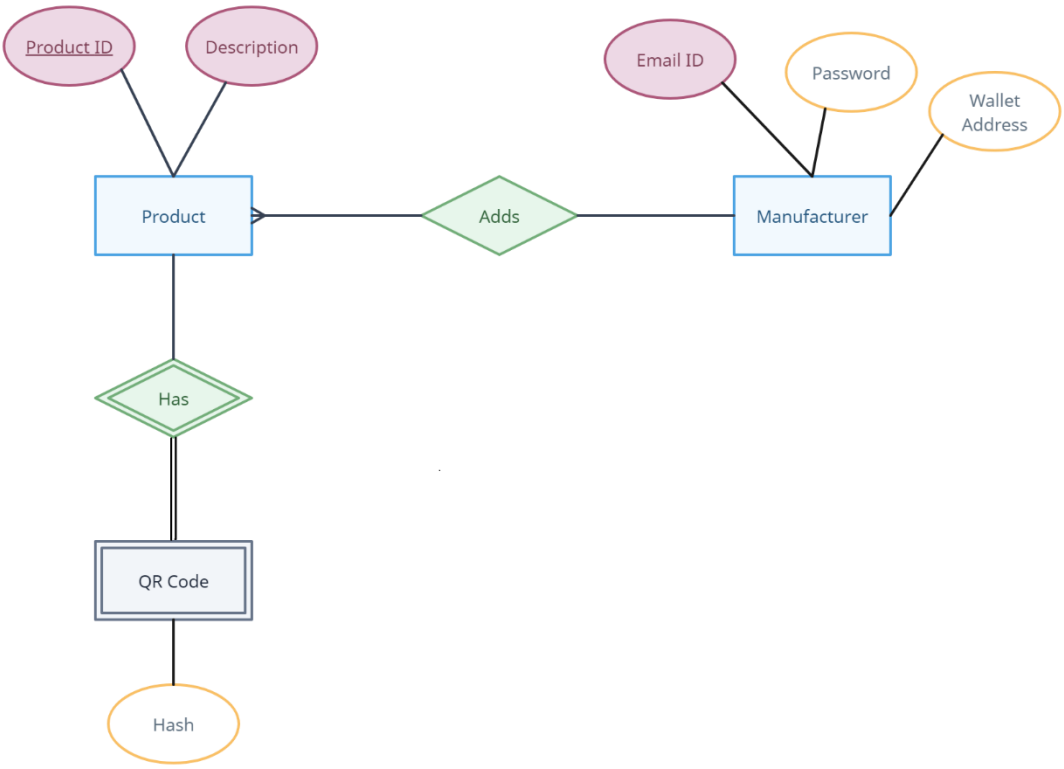

Fig. 4.4 ER Diagram

CHAPTER 5
IMPLEMENTATION

5.1 Introduction to Languages, Tools, and Technologies Used for Implementation.

The project builds a strong blockchain-based product authentication system by combining a variety of languages, tools, and technologies.
Summary of the essential elements:

5.1.1 Languages

1. Solidity: A programming language used to create smart contracts that control the blockchain's authentication procedure.
2. JavaScript: Used in front-end and back-end programming, it can be used to handle server-side functionality and create interactive user interfaces.
3. HTML/CSS: Frontend developers utilize HTML and CSS to organize web pages and design user interfaces.

5.1.2 Instruments and Technology

1. Truffle Suite: The Truffle Suite is a development framework designed to compile, test, and implement smart contracts for Ethereum-based applications.
2. Ganache: Use Ganache, a personal blockchain for Ethereum development, to create and test applications, deploy contracts, and manage your code. It can be downloaded as a command-line program or as a desktop application. Without requiring a real Ethereum network, developers may create and test smart contracts and decentralized apps (dApps) with Ganache by simulating a local blockchain environment.
3. MetaMask: MetaMask is a mobile application and browser plugin that serves as an Ethereum gateway and cryptocurrency wallet. Users may transfer and receive cryptocurrencies, manage Ethereum and ERC-20 tokens, and see transaction histories

with it. Furthermore, MetaMask introduces Web3.js into browsers to enable communication with decentralized apps (dApps) based on Ethereum. All things considered, MetaMask makes access to Ethereum and dApps easier, which has led to its widespread adoption by Ethereum developers and cryptocurrency enthusiasts.

4. Node.js: A runtime environment used for server applications and backend development that allows JavaScript code to be executed server-side.

5. Web3.js: Web3.js is a JavaScript library designed to facilitate communication between front-end apps and Ethereum-based blockchains.

6. QR Code Generator: An application or library designed to create QR codes for goods, making them simple to scan and validate.

The project intends to provide a comprehensive and safe product authentication system that improves confidence and transparency for customers and stakeholders by utilizing these languages, tools, and technologies.

CHAPTER 6

TESTING AND MAINTAINANCE

6.1 Testing Techniques and Test Cases Used

Table 6.1 Test Case 1: User Registration

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-1	Test user registration process	Go to the registration page.	Users can access the registration page.	Pass
		Enter a valid username and password.	Username and passwordfields are accepted.	Pass
		Click the “Register” button.	A confirmation pop-up of MetaMask appears.	Pass
		Confirm the registration.	The user successfully registered.	Pass
TC-2	Test User registration With invalid credentials	Go to the registration page	Users can access the registration page.	Pass
		Enter an invalid username and password.	Username and passwordfields are accepted.	Pass
		Click the “Register” button.	Confirmation pop-up of MetaMask appears.	Pass

		Cancel the registration.	The registration process is canceled.	Pass

Table 6.2 Test Case 2: User Login

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-3	Test user login process	Go to the login page.	Users can access the login page.	Pass
		Enter a valid username and password.	Username and password fields are accepted.	Pass
		Click the "Login" button.	Logged in successfully.	Pass
TC-4		Go to the login page.	Users can access the login page.	Pass
		Enter an invalid username and password.	Username and password fields are accepted.	Pass
		Click the "Login" button.	Error message displayed.	Pass

Table 6.3 Test Case 3: Product Registration

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-5	Test product registration by manufacturer	Log in as a manufacturer.	Successful Login.	Pass
		Navigate to the	Access to the	Pass

		product registration page.	registration page.	
		Enter the unique product ID and Name.	Information accepted.	Pass
		Click the register product button	Confirmation pop-up of MetaMask appear	Pass
		Confirm the product registration.	The product is successfully registered on the blockchain.	Pass
TC-6	Test product registration with invalid credentials	Log in as a manufacturer.	Successful Login.	Pass
		Navigate to the product registration page.	Access to the registration page.	Pass
		Enter the unique product ID and Name.	Information accepted.	Pass
		Click the “Register Product” button	Confirmation pop-up of MetaMask appears.	Pass
		Confirm the registration	Error message	Pass

Table 6.4 Test case 4: Product Verification

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-7	Test product verification by users	Go to the product verification page.	Access to the verificationpage.	Pass
		Upload the valid QR code.	Product ID accepted.	Pass
		Click the "verify" button.	The product's authenticity is verified.	Pass
TC-8	Test product verification with an invalid product ID	Go to the product verificationpage.	Access to the verification page.	Pass
		Upload the invalid QR code.	Product ID accepted.	Pass
		Click the "verify" button.	Error message.	Pass

CHAPTER 7

RESULTS AND DISCUSSION

7.1 User Interface Representation

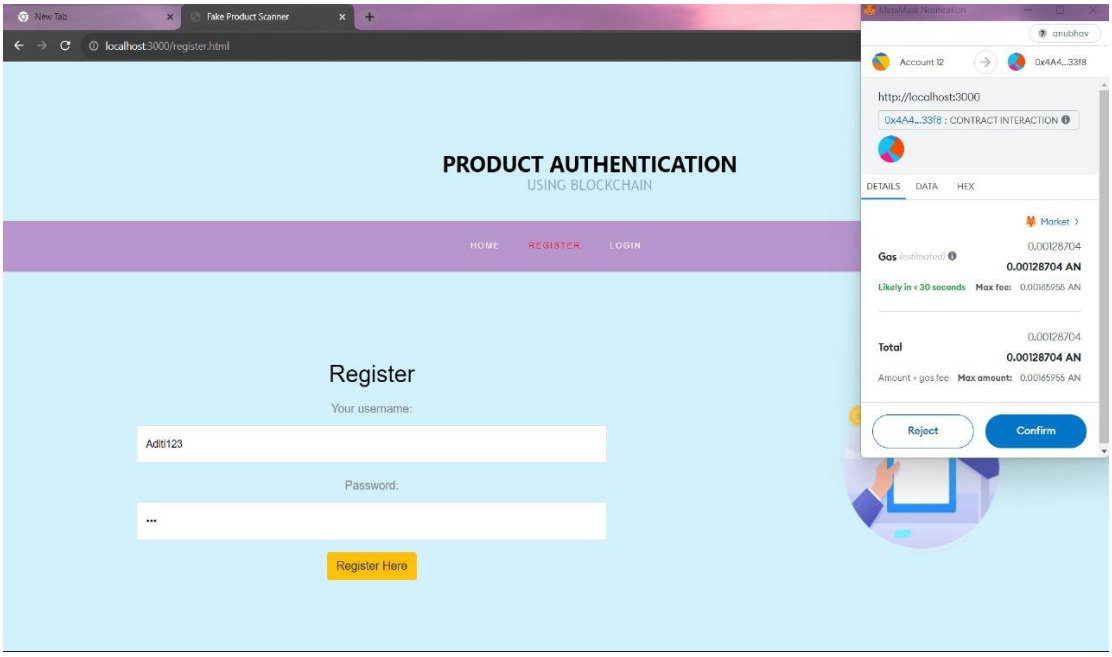

Fig. 7.1 User Registration Page

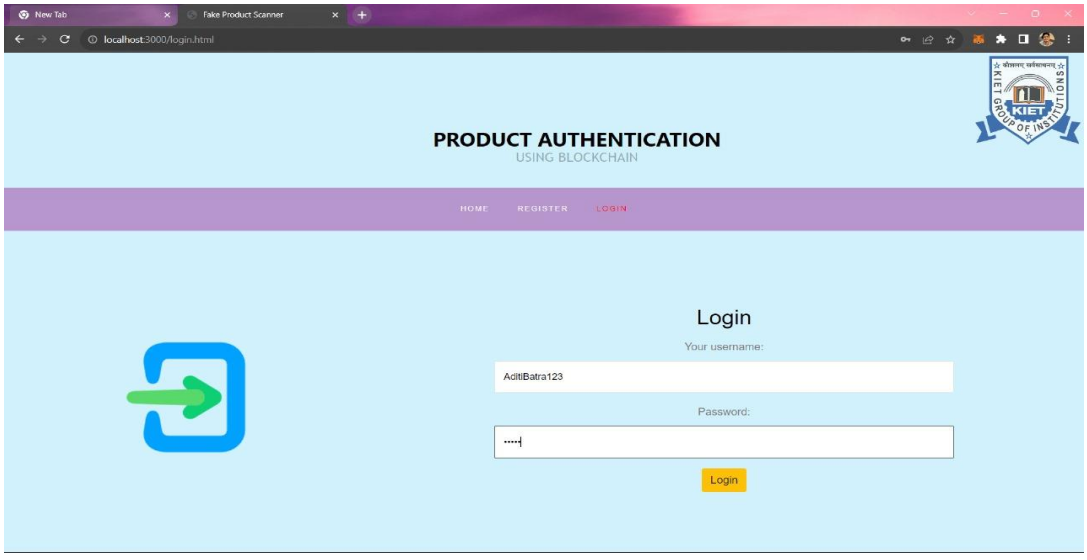

Fig. 7.2 User Login Page

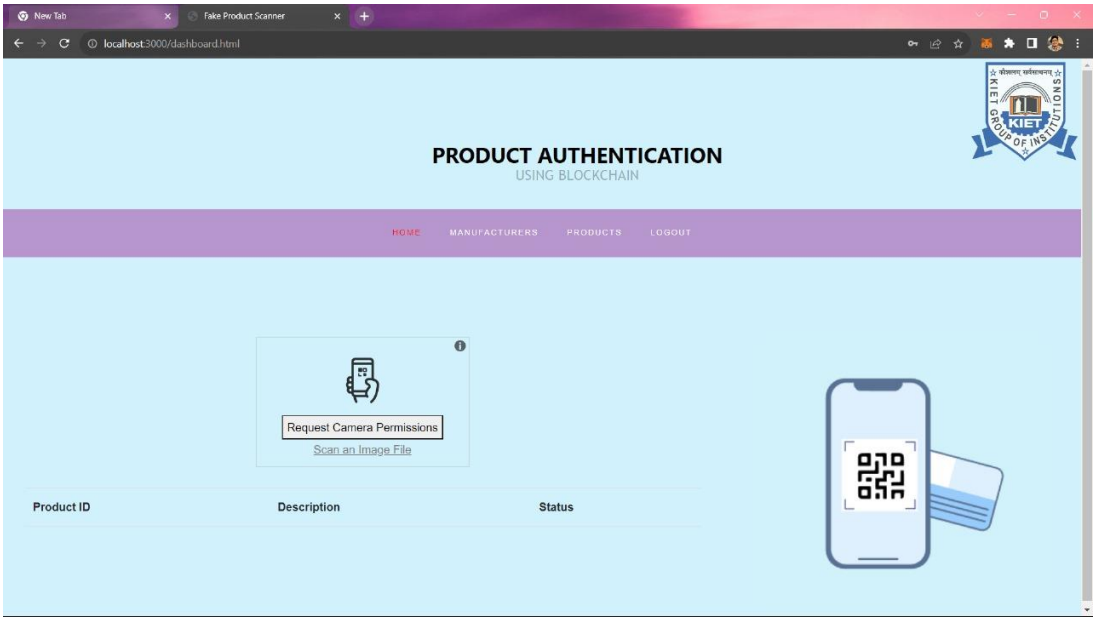

Fig. 7.3 After login Landing Page

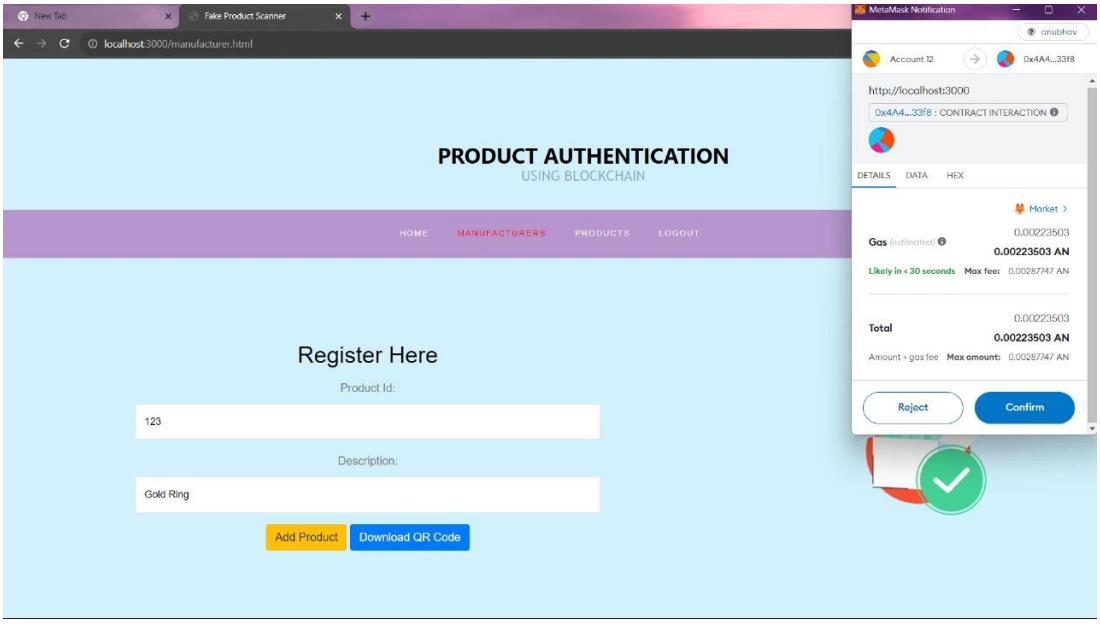

Fig. 7.4 Product Registration Page

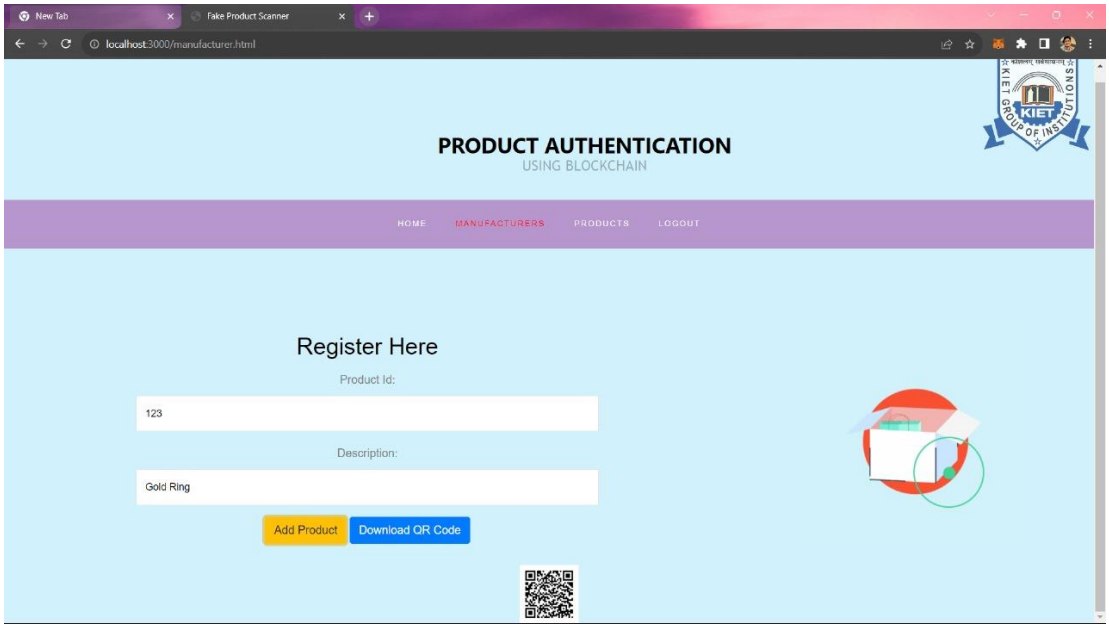

Fig. 7.5 QR Code Generation

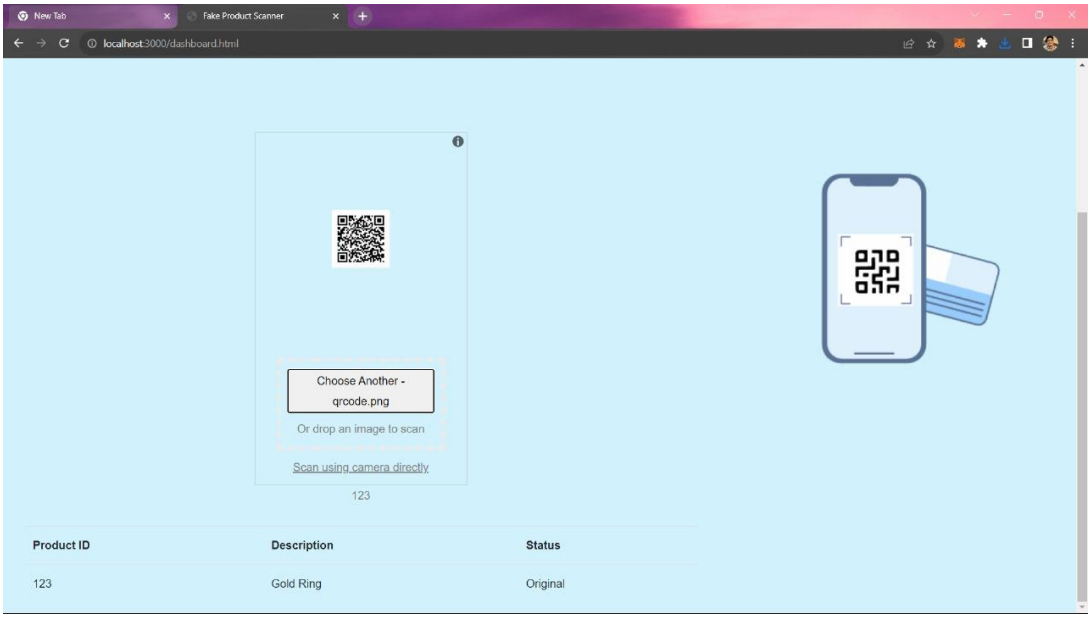

Fig. 7.6 Scanner

7.2 Brief Description of Various Modules of the System

- **Manufacturer**: Manufacturers may easily add and register their items on the blockchain by using the Manufacturer module, which serves as a centralized hub. Manufacturers provide comprehensive product details using this interface, including specs and credentials for authenticity, guaranteeing a clean and safe procedure.

- **Products:** Users have access to an extensive catalog of all registered products under the Products module. By acting as a repository, this module promotes customer and stakeholder confidence in the legitimacy of the products on offer by making it simple for them to search, view, and validate product facts.

- **Scanner**: When on the go, the Scanner module offers a convenient way to confirm the legitimacy of products. Customers may easily access real-time information recorded on the blockchain by scanning the QR codes linked to each product, assuring the authenticity and integrity of the goods they come across.

- **Contracts**: The Contracts module, which is at the heart of the system, contains the smart contracts that control the authentication procedure. Deployed on the blockchain, these contracts uphold predetermined rules and logic, assuring transaction immutability and transparency as well as the legitimacy of registered products.

7.3 Snapshots of the System with Brief Details of Each

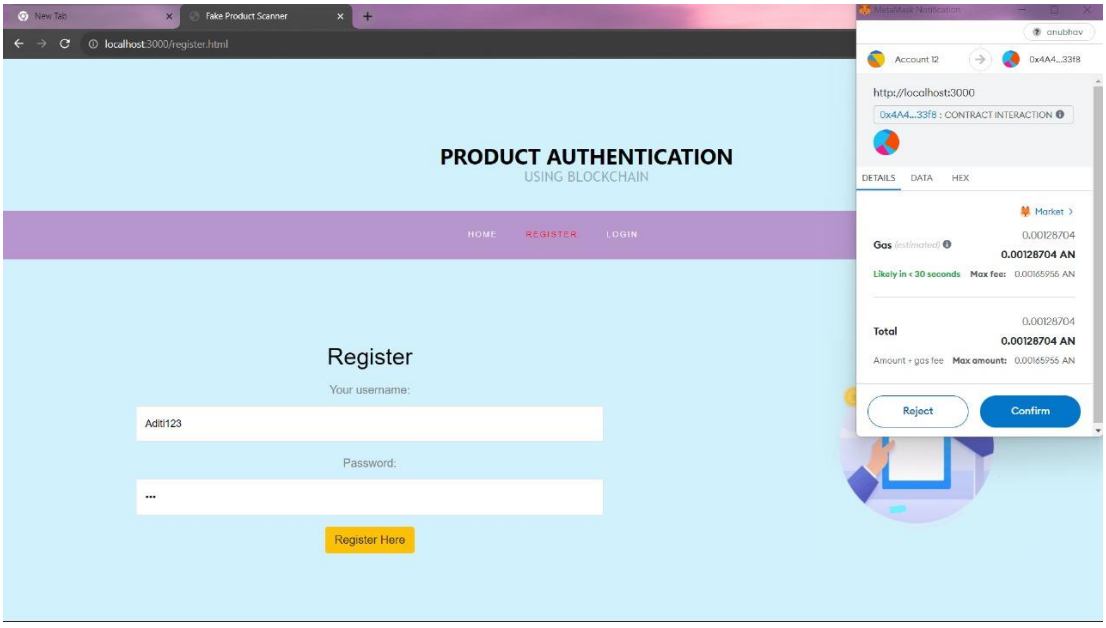

Fig.7.7 Registration Page

- The above snapshot is the page where manufacturers can come and register themselves. The top-right corner has the popup of the MetaMask wallet from which ether gas will be used for transactions to the blockchain.

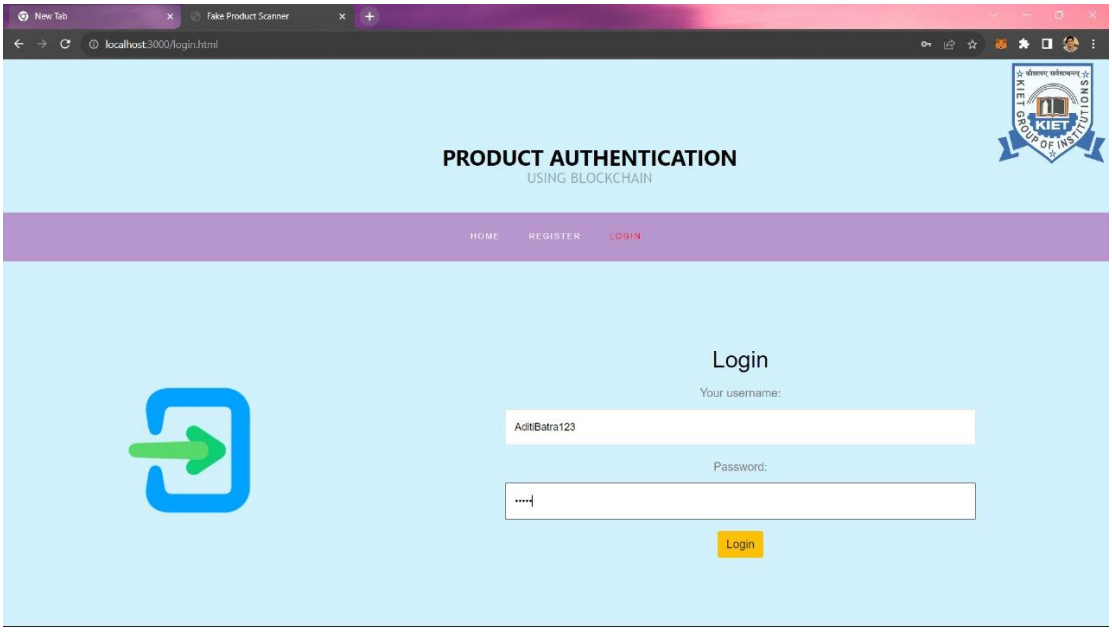

Fig. 7.8 Login Page

- The registered user can log in to the App on the login page.

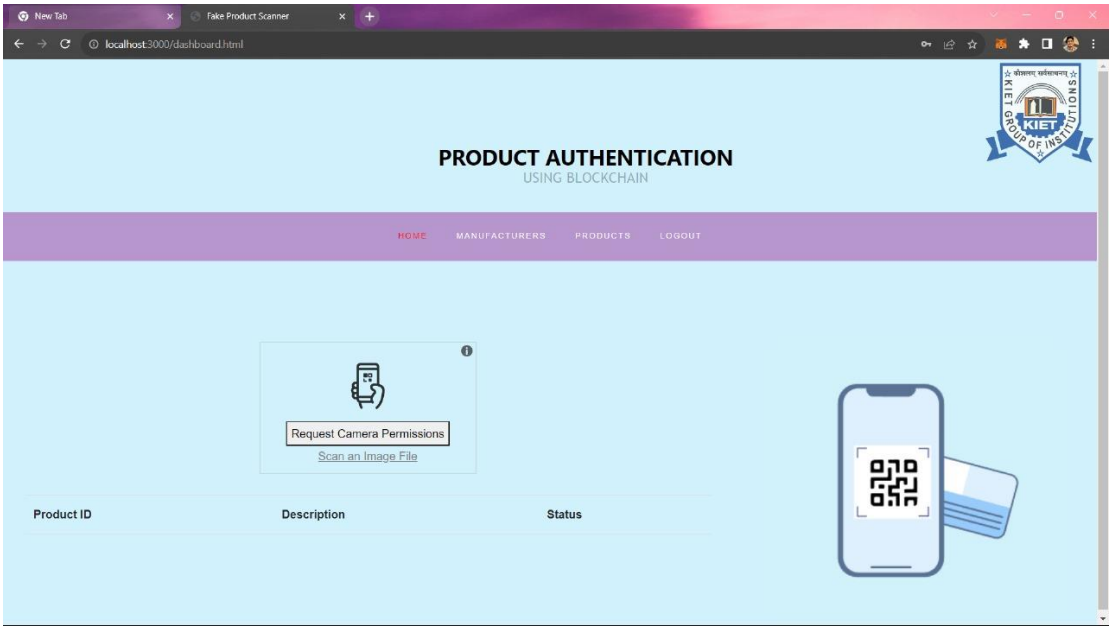

Fig.7.9 Landing Page

- It is the landing page of our App after login, there are multiple tabs which first tab is for our scanner of the app and second one is for adding the products and the other one is for listing added products.

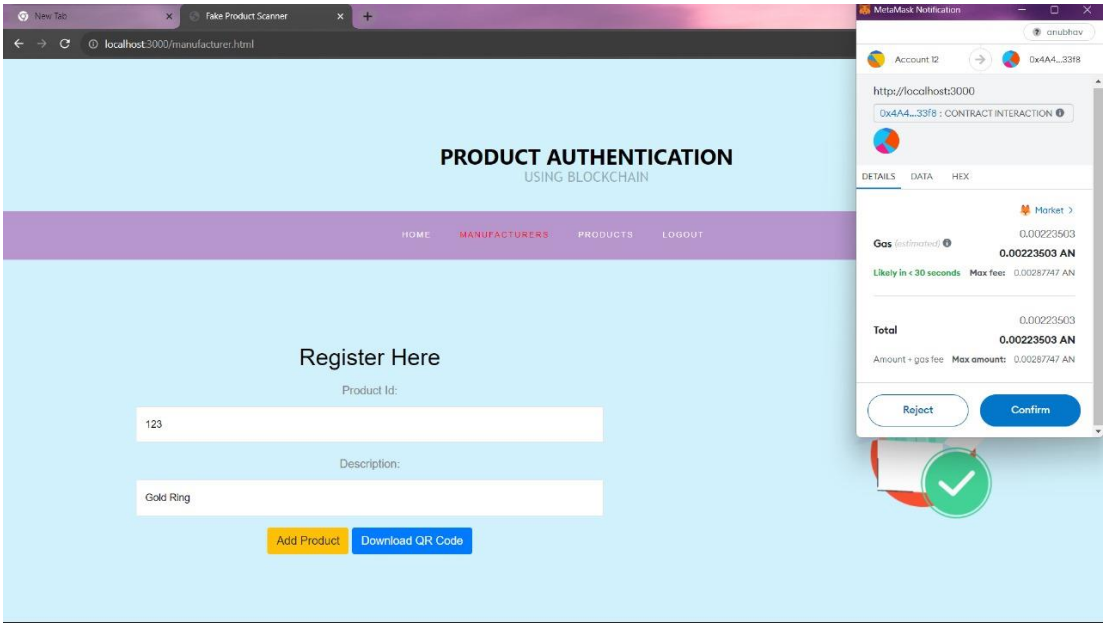

Fig.7.10 Product Registration Page

- On this page, manufacturers can add/register products by using the gas which is visible in the popup on the top right corner.

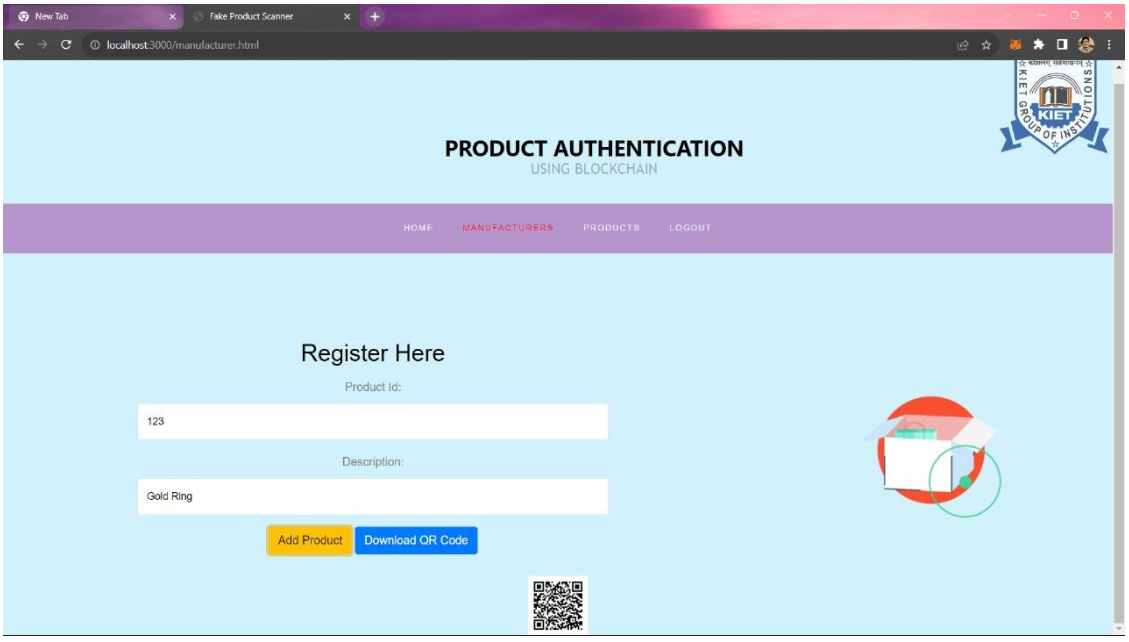

Fig.7.11 QR Generation

- After registering the product, a QR code is generated by our system which is made by using QRcode.js.

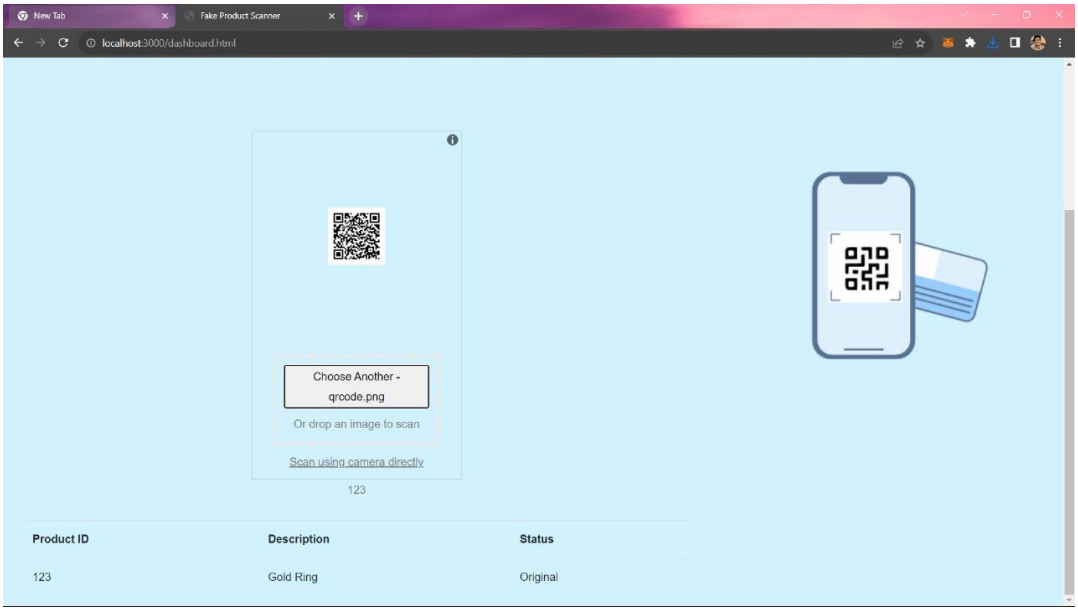

Fig.7.12 Product Authenticated

- QR code is then scanned or uploaded that tells the product's status whether it is an original or counterfeited product. Hence, the authenticity of the product is checked.

7.4 Back Ends Representation (Database to Be Used)

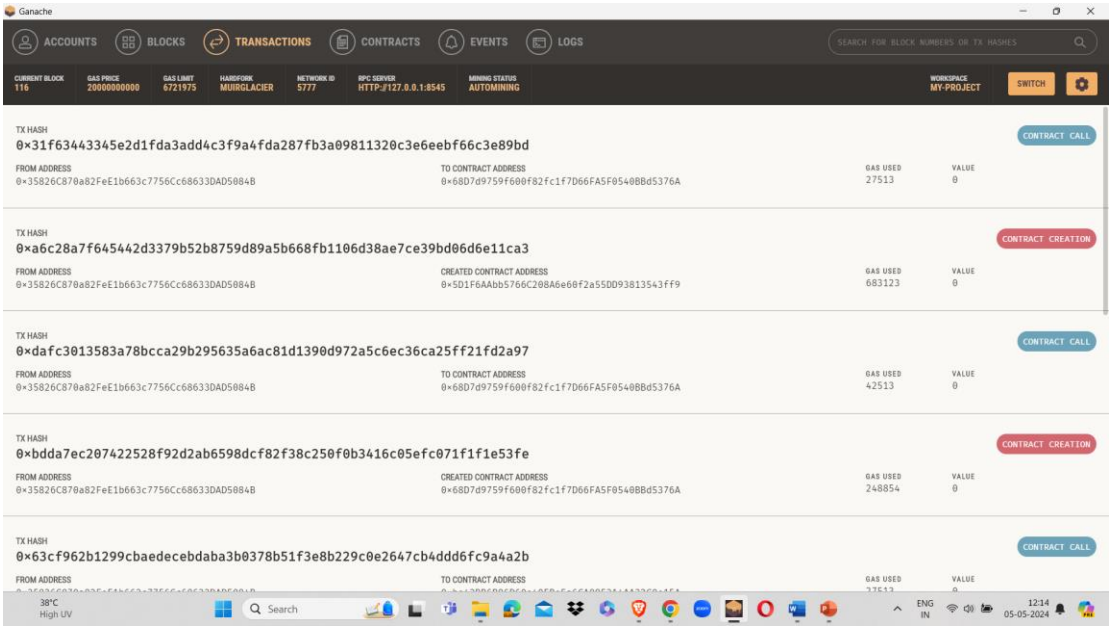

Fig.7.13 Ganache-Ethereum account information

7.5 Snapshots of Database Tables with Brief Description

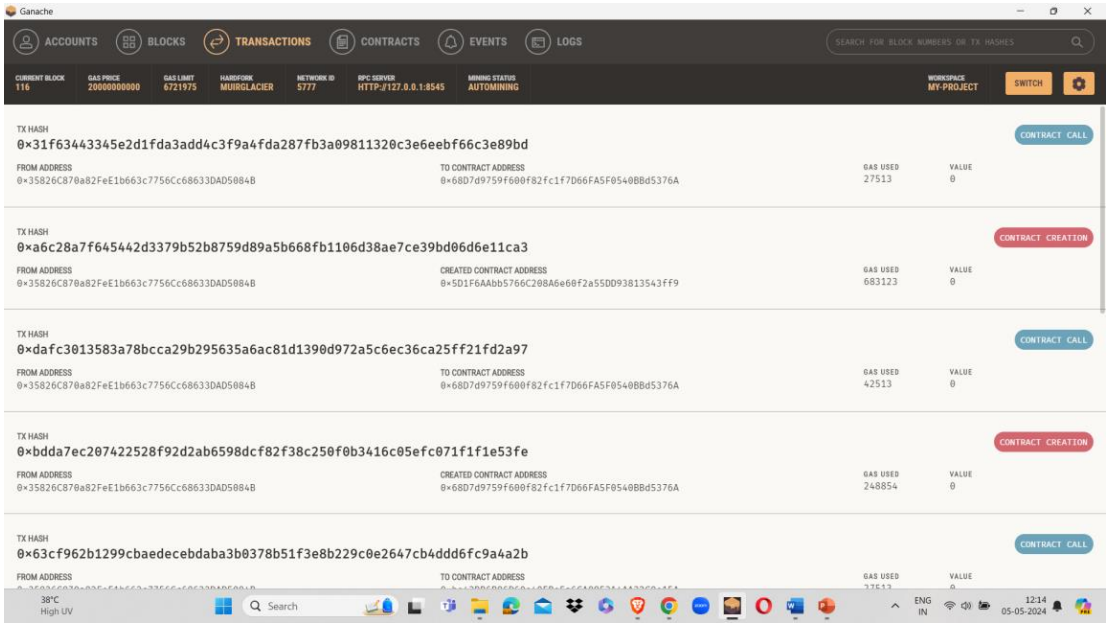

Fig.7.14 Database

- The above-given snapshot is of the transactions that have been done through the blockchain network that has been set up locally on the system. It is the Ganache tool that gives the dummy Ethereum Blockchain network that can be used for the transactions taking place in our app through smart contracts

CHAPTER 8

CONCLUSION AND FUTURE SCOPE

To sum up, our research has shown how blockchain technology can be used to safeguard consumer rights in the digital era and tackle issues like counterfeit goods. We have created a strong system for product certification and authentication that ensures the veracity of transactions and product information by utilizing the decentralized and unchangeable nature of blockchain technology.

By introducing blockchain-based product certification, we have given customers a dependable and transparent way to confirm the legitimacy of the goods they are buying, which has increased confidence and trust in the market. Furthermore, we have established the groundwork for a safer and more responsible environment for product certification by encouraging cooperation and openness throughout the supply chain.

As Future Scope of this project, there are many chances to improve and broaden the project's scope in the future, such as connecting it to IoT devices, automating tasks using smart contracts, and branching out into new markets. We can fully utilize blockchain technology in the future to guarantee product quality, uphold the brand reputation, and defend consumer rights by carrying on with innovation and working with stakeholders.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of Blockchain Technology: Architecture, Consensus, and Future Trends” 2017 IEEE International Congress on Big Data Honolulu, HI, USA, 2017, pp. 557-564, doi:10.1109/BigDataCongress. 2017.85.

[2] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F.-Y. Wang, “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi:10.1109/ TSMC.2019.2895123.

[3] A.H. Mohammed, A. A. Abdulateef and I. A. Abdulateef, “Hyperledger, Ethereum and Blockchain Technology: A Short Overview,” 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2021, pp. 1-6, doi: 10.1109/HORA52670.2021.9461294.

[4] P. William, D. Jadhav, P. Cholke, M. A. Jawale and A. B. Pawar, “Framework for Product Anti-Counterfeiting using Blockchain Technology,” 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1254-1258, doi:10.1109/ICSCDS53736.2022.9760916

[5] R. S. Bhatnagar, S. M. Jha, S. S. Singh and R. Shende, “Product Traceability Using Blockchain,” 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2020, pp. 891-895, doi:10.1109/ ICACCCN51052.2020.9362807.

[6] AG. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz and T. M. Alam, “A journey of WEB and Blockchain towards the Industry 4.0: An Overview,” 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 2019, pp. 1-7, doi:10.1109/ICIC48496.2019. 8966700

[7] Blockchain technology in supply chain operations: Applications, challenges and research opportunities https://doi.org/10.1016/j.tre.2020. 102067

[8] AG. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz and T. M. Alam, “A journey of WEB and Blockchain towards the Industry 4.0: An Overview,” 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 2019, pp. 1-7, doi:10.1109/ICIC48496.2019.8966700.

[9] Lee, WM. (2023). Using the MetaMask Crypto-Wallet. In: Beginning Ethereum Smart Contracts Programming. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9271-65.

[10] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, “Blockchain contract: Securing a blockchain applied to smart contracts,” 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2016, pp. 467-468, doi:10.1109/ICCE.2016.7430693.

[11] Remya Stephen and Aneena Alex 2018 IOP Conf. Ser.: Mater. Sci. Eng.396 012030 “A Review on BlockChain Security” doi10.1088/1757- 899X/396/1/012030

[12] Architecture to Enhance Tr[ansparency in Supply Chain Management Using Blockchain Technology, “https://doi.org/10.1016/j.promfg.2020.10.225”

[13] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, “Certificate Transparency Using Blockchain,” 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[14] R. S. Bhatnagar, S. M. Jha, S. S. Singh and R. Shende, “Product Traceability Using Blockchain,” 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2020, pp. 891-895, doi:10.1109/ICACCCN51052.2020.9362807.

[15] P. William, D. Jadhav, P. Cholke, M. A. Jawale and A. B. Pawar, “Framework for Product Anti-Counterfeiting using Blockchain Technology,” 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1254-1258, doi:10.1109/ICSCDS53736.2022.9760916

[16] A. Mishra, H. Khatter, G. Gupta, A. Jamshed, A. K. Srivastava, “Enabling Secure and Transparent Crowd Funding Approach Powered by Blockchain”, Third

International Conference on Emerging Technologies in Data Mining and Information Security, Institute of Engineering Management, Kolkata, West Bengal, India, 23-25 February 2022, Proceedings in LNNS, vol 490. Springer, Singapore https://doi.org/10.1007/ 978-981-19-4052-1 64

[17] H. Khatter, H. Chauhan, I. Trivedi, and J. Agarwal, "Secure and Transparent Crowdfunding Using Blockchain," 2021 International Conference on Recent Trends in Electronics, Information, Communication Technology (RTEICT), 2021, pp. 76-80, DOI:10.1109/RTEICT52294. 2021.9573956.

PROJECT LINK

https://github.com/KIET-Github/CS-2024-B/tree/main/PCS24-12-AditiBatra

Acceptance of Research Paper

2024 External Inbox

DoSCI-2024 1 Feb

to me

Dear **Author(s)**,

Based on the review report, your paper **can be considered for the Elsevier SSRN Reputed Series**. This means that your paper is among the top 30% of the papers received/reviewed.

Your paper with submission ID **164** and Paper Title '**PRODUCT AUTHENTICATION USING BLOCKCHAIN' has been accepted for publication in Elsevier SSRN**.

You are requested to submit the following documents to dosci.ui@gmail.com at the earliest.
1. Revised Final Camera-Ready Copy (CRC) as per the Elsevier format. (https://www.dosci-conf.com/downloads)
2. Copy of e-receipt of registration fees. (https://www.dosci-conf.com/registrations) - see Registration Fee For DoSCI 2024 (Poster Paper Presentation)

Research Paper Link: https://ssrn.com/abstract=4831092

Product Authentication Using Blockchain

Created Date: 05/16/2024

Status Info

Page Name	Status	Description
Abstract	Complete	
Authors	Complete	Aditi Batra Shivani . Abhishek Singh Yadav Anurag Tripathi Kshitij Pal
Reference	Complete	
Paper	Complete	PDF Uploaded
Classification	Complete	
Submission	Submitted	Your paper has been submitted.

Abstract

In today's globalized market, the prevalence of counterfeit products poses a significant threat to consumers and businesses alike. To combat this issue, this study proposes leveraging blockchain technology for product authentication. Central to this innovative approach issmart contracts, which securely record product information on the immutable ledger of the blockchain. This creates a reliable environment where consumers can easily verify product authenticity while thwarting fraudulent activities. The paper explores the evolution of this product authentication system, delving into its planning, implementation, and potential to mitigate counterfeiting and enhance consumer trust. Throughout this journey, blockchain technology emerges as the cornerstone, guiding our path, serving as our currency, and fostering trust among stakeholders.

Research Paper

Product Authentication Using Blockchain

Shivani[a], Aditi Batra[b], Abhishek Singh Yadav[c], Anurag Tripathi[d], Kshitij Pal[e]

[a]KIET Group of Institutions, Delhi-NCR Meerut Road, Ghaziabad, 201206, India
[b]KIET Group of Institutions, Delhi-NCR Meerut Road, Ghaziabad, 201206, India
[c]KIET Group of Institutions, Delhi-NCR Meerut Road, Ghaziabad, 201206, India
[d]KIET Group of Institutions, Delhi-NCR Meerut Road, Ghaziabad, 201206, India
[e]KIET Group of Institutions, Delhi-NCR Meerut Road, Ghaziabad, 201206, India

Abstract: In today's globalized market, the prevalence of counterfeit products poses a significant threat to consumers and businesses alike. To combat this issue, this study proposes leveraging blockchain technology for product authentication. Central to this innovative approach is smart contracts, which securely record product information on the immutable ledger of the blockchain. This creates a reliable environment where consumers can easily verify product authenticity while thwarting fraudulent activities. The paper explores the evolution of this product authentication system, delving into its planning, implementation, and potential to mitigate counterfeiting and enhance consumer trust. Throughout this journey, blockchain technology emerges as the cornerstone, guiding our path, serving as our currency, and fostering trust among stakeholders.

1. INTRODUCTION

The counterfeit product problem is a serious issue in today's worldwide economy. It affects many different types of items, including medicine, high-end consumer gadgets, and even food. These sneaky knockoffs not only put customers at risk but also damage the credibility and bottom line of legitimate businesses. The advent of blockchain technology, a ray of hope against fake goods, is a game changer. Using the disruptive power of this technology [1] builds an unbreakable wall around product authenticity. This study sets out on a mission to expose the genius of this blockchain-based system by investigating its inner workings, demonstrating its promise, and analyzing the potential benefits it contains for all parties involved.

2. LITERATURE SURVEY

2.1. Hyperledger Technology

Imagine a digital ledger shared across a network of users, where all data, events, and transactions are permanently recorded in indelible ink. This is the fundamental concept of blockchain technology, a revolutionary force with applications in various industries that extend beyond its origins in cryptocurrency. At its core, blockchain operates as a distributed, decentralized ledger [2] resembling a network of interconnected blocks. Each block, like pages in a ledger, contains a collection of transactions. What sets blockchain apart is its distinct characteristics:

- **Delocalization**: Unlike conventional centralized databases controlled by a single entity, blockchain operates as a decentralized network. Transactions are distributed among numerous nodes or computers instead of being stored in a single location.
- **Open and Transparent:** Blockchain's ledger is open and transparent. With access to the complete transaction history, accountability, and trust are fostered since everyone on the network can verify the information.
- **Immutability**: Once data is stored on the blockchain, it becomes nearly unchangeable. Altering one block would necessitate changing every other block on the network, a nearly impossible task.
- **Security:** Blockchain data is highly resistant to fraud and unauthorized access due to the use of cryptographic techniques for protection.

In the context of our product authentication system, blockchain serves as the cornerstone of trust. It provides an immutable and transparent platform for recording product details and transactions, creating an impenetrable trail of authenticity throughout a product's lifecycle, from manufacturing to the hands of the customer.

2.2. Automation Rules

If blockchain is the trust ledger, then smart contracts are the architects of automation. Smart contracts are self-executing agreements with predefined conditions and rules. As digital counterparts to contracts, they possess the remarkable ability to enforce conditions without the need for intermediaries autonomously. Smart contracts play a pivotal role in our system. Imagine the complexity of manually tracking and verifying the authenticity of each product. Smart contracts step in as champions of efficiency and integrity. Most importantly, they precisely validate the authenticity of products, track changes in ownership, and record product information. Consider this scenario: A product arrives at a retailer's door. A smart contract, upon scanning the product into the system, activates and verifies the product's credentials against predefined criteria. When a product meets all the requirements, it is certified as authentic, and this event is permanently recorded on the blockchain. Smart contracts are ingenious because they automate these processes, eliminating the need for intermediaries and reducing the potential for human error. They epitomize technological innovation, offering efficiency, security, and trust in a world riddled with counterfeit goods.

3. SYSTEM ARCHITECTURE

3.1. Smart Contracts

Smart contracts [3] are the digital architects at the core of the product authentication system, orchestrating every aspect of the entire process with precision and consistency. These smart contracts control the registration, verification, and management of products on the blockchain, making them a vital component of the system.

a) Contract for Migrations: Think of the migrations contract as the" invisible hand" of the blockchain, simplifying the deployment and administration of other contracts. This contract plays a crucial role in ensuring the smooth operation of interactions between smart contracts [18]; it is more than just a bureaucratic tool. It serves as the bridge between the blockchain realm and the real world.

In simple terms, the migrations contract simplifies the often-complex process of implementing smart contracts [4], making it more comprehensible and efficient. It ensures that the interactions between smart contracts are well-planned and deployed in the correct order. While it may not steal the spotlight, it is the unsung hero that keeps the system running seamlessly and coherently.

b) Contract for Product: Now, let's focus on the product contract, the cornerstone of the system. This smart contract acts as the guardian of each registered product's integrity and authenticity.

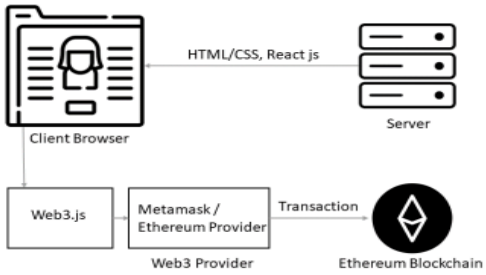

Fig. 1 – System architecture.

Think of it as the custodian of a historical treasure vault. When a product is registered, all relevant details, including its unique identification number and owner's identity, are documented. This data is permanently etched into the blockchain [5], ensuring that it cannot be tampered with or counterfeited. But the product contract doesn't stop there; it continues to play an active role in product authentication. When a customer seeks to confirm a product's legitimacy, this contract comes into action. It performs real-time checks on the product's status, comparing it to predefined standards. If the product meets these criteria, its authenticity is confirmed, and the status is updated on the blockchain. If it falls short, it remains labeled as "Available," providing a reliable indicator.

In essence, in a world filled with imitations, the product contract stands as the guardian of authenticity. It guarantees that the journey of every product is publicly and verifiably documented on the blockchain, from its creation to its verification. It serves as the bedrock of trust upon which both producers and consumers can rely.

These smart contracts are the dancers in the intricate ballet of blockchain-based product authentication [6], ensuring that every step is executed gracefully and precisely. They exemplify how blockchain technology can revolutionize an industry by offering an immutable and transparent ledger of authenticity in a world inundated with counterfeit goods.

3.2 Ethereum

It is a decentralized blockchain network that employs a proof-of-work consensus mechanism. This consensus mechanism involves adding blocks to the blockchain by solving mathematical expressions. The process of solving these puzzles serves as proof that nodes within the network have expended computational resources to perform the required "work". Once a node successfully solves the puzzle, the block is confirmed and recorded in the blockchain. This process is commonly referred to as mining. While mining often involves brute force trial and error, successfully adding a block in Ethereum is rewarded with the cryptocurrency Ether (ETH).

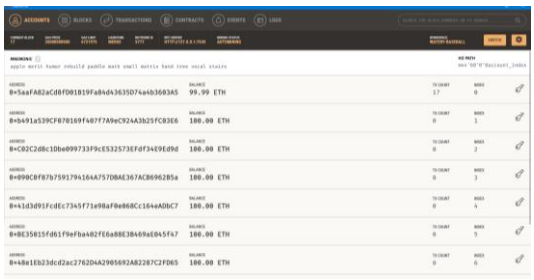

Fig. 2 – Ethereum account information.

4. USER MANAGEMENT

User management is an integral part of the blockchain-based product authentication system, ensuring a smooth experience for all users. This section delves deeper into user management, emphasizing its importance and security measures.

4.1. Registration Of Users

The user registration process is one of the initial interactions individuals have with the system. It offers a user-friendly experience, requiring each user to select a unique login and password. These credentials serve as the keys to the system, ensuring that only authorized individuals can access its features.

4.2. Security Measures

Data security stands as the paramount concern in any online system. In this product registration system, blockchain technology is employed to store user data, encompassing usernames and passwords securely. Blockchain utilizes robust security protocols to safeguard private data. Even in the event of unauthorized access to the blockchain, malicious entities would face significant challenges in deciphering or altering user data.

4.3. Immutable User Records

Once a user completes registration, their information is permanently logged into the blockchain. This immutability ensures that user identities and passwords remain unaltered and resistant to tampering by unauthorized parties. It establishes a reliable record of all individuals who have utilized the system.

4.4. Mitigating Data Breaches

In today's digital age, concerns about data breaches and unauthorized access to user information are pervasive. The use of blockchain for storing user data mitigates the likelihood of data breaches. Unlike traditional centralized systems, blockchain's decentralized nature substantially reduces the risks associated with security breaches. Users can trust that their personal information remains secure when utilizing the system, instilling a sense of "Enhanced Trust". Blockchain's reputation for openness and security extends to user management, fostering trust between the company and its users.

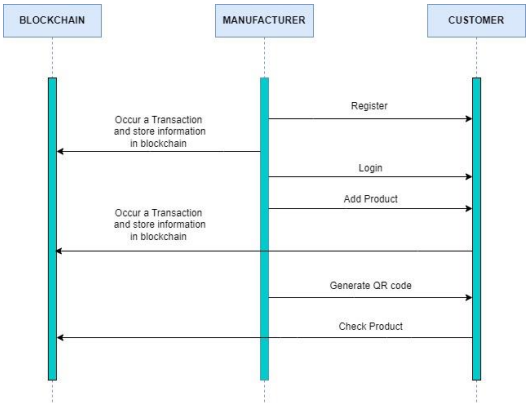

Fig. 3 – Diagram of processes in our system.

4.5. Product Registration

Manufacturers and trusted suppliers play crucial roles in the sophisticated blockchain-based product authentication system's product registration process. These trusted entities ensure the authenticity of the products they introduce into the system, endowing them with a unique identity to distinguish them from counterfeits. Upon registration as trusted participants, these authorized entities gain access to the system. This digital identity certification enables them to register products and provide essential data that enriches product information.

a) Product ID: A product's unique identifier is its Product ID, consisting of a distinctive alphanumeric code. This code serves as the product's digital identity, setting it apart from other entities within the system and rendering it tamper-resistant.

b) Ownership Details: In this digital ledger, ownership is a critical component. Registration allows manufacturers or suppliers to assert ownership of the product, reinforcing their stake in its journey.

After meticulously inputting these critical details, the system orchestrates secure blockchain data recording [7]. This process extends beyond simple data entry, it involves creating a digital birth certificate for the product. The blockchain's immutability and transparency ensure that once recorded, the product's identity remains unalterable. Registering each

product fosters trust and eliminates ambiguity surrounding counterfeit goods. Consumers can now place their trust in products within this system, knowing they possess a permanent marker of authenticity, certified by trusted institutions.

4.6. Product Verification

Now, let's journey into the consumer realm [8], where trust is paramount, and authenticity is non-negotiable. When consumers encounter a product within the system, they have access to a straightforward yet powerful tool—the Product Verification process.

Imagine a scenario where a consumer stands before a product, contemplating its authenticity. Users can easily access the system by inputting the product's unique identification number, often embedded within a QR code. The blockchain's smart contract springs to life instantly, acting as a vigilant sentry to verify the product's authenticity.

Here's how the magic unfolds:

a) Entering the QR Code: The consumer deftly scans or enters the QR code—a digital sigil that serves as the gateway to the product's history. This QR code encapsulates the product's identity, a digital Rosetta Stone for decoding its journey.

b) Smart Contract Vigilance: The smart contract steps onto the stage as the guardian of truth. It swings into action, promptly scrutinizing the product's status against predefined criteria. Is it a genuine article or a cunning imitation? If the product checks all the predefined boxes, it is christened "Available"—a digital insignia of trust and authenticity. But if, by the slimmest chance, the product's status diverges from "Available", the smart contract raises an alarm—a digital red flag that beckons for further examination. The result is swift and trustworthy. When marked as "Available", the product shines as a beacon of authenticity amidst counterfeits. Consumers can proceed with confidence, assured of a genuine purchase. Product verification not only upholds confidence but also ensures commitment to immutability. The blockchain's immutable ledger and the vigilance of smart contracts shield consumers from counterfeit products. This innovative, trust-driven approach empowers consumers to make informed choices, secure in the knowledge that authenticity is not a fleeting hope but an unwavering certainty.

5. EXECUTION

The manufacturer initiates the registration process on the website by providing a unique ID and password. Upon clicking the register button, a MetaMask [9] confirmation prompt appears for blockchain validation. Subsequently, the manufacturer logs in using the same credentials and proceeds to register a product. During product registration, the manufacturer inputs a unique product ID and product name, confirming the addition to the blockchain by clicking the "add" button. A MetaMask confirmation is triggered again. Upon successful registration, a corresponding QR code is generated, downloadable by the manufacturer for affixing to the product. When users or customers scan or upload this QR code on the website, the system verifies the product's authenticity, displaying relevant information and confirming whether the product is genuine or counterfeit.

5.1. User Authentication

User Authentication is a crucial aspect of computer systems that involves verifying the identity of users attempting to access a system. Within this domain focused on the needs and preferences of users, the concepts of simplicity and security are intricately interconnected. Users are guided into the system using an authentication process that is designed to be user-friendly. Users possess the ability to easily complete the registration and login processes, which serve as their access point to the realm of authenticity. Novice users commence their expedition by furnishing a username and password, a customary undertaking akin to establishing an electronic mail account. The credentials above serve as the users' digital authentication mechanisms, providing them with authorization to utilize the various functionalities of the system. The utilization of blockchain technology for enhancing security measures. The user data, specifically the usernames and passwords, are stored in a secure database that is not susceptible to conventional vulnerabilities and breaches. Conversely, the data is safely saved on the blockchain, encapsulated under a robust layer of cryptographic safeguards. The smart contract [10] serves as a crucial component in ensuring security by facilitating user authentication throughout the login procedure. The process of authentication extends beyond a mere login, encompassing a secure handshake that establishes confidence between entities.

5.2. Registration Of the Product

The conditions are prepared for approved entities, who serve as guardians of authenticity, to introduce their items into the system. Users adeptly navigate through an interface that is designed to be intuitive and easy to use, demonstrating painstaking attention to detail as they register each product.

a) Identification of Products and Ownership Details: The guardians of authenticity not only provide a unique ID for the product but also create a digital document that proves its identity and includes ownership details. This process validates their ownership claim and ensures the product's inclusion in the system.

b) The Assurance of Smart Contracts: Upon the careful input of these particulars, the smart contract proceeds to verify and record the product information accurately onto the blockchain. Every individual product, while maintaining its distinct character, is originally labeled as "Available". The smart contract not only captures and stores data but also ensures the veracity and consistency of each product.

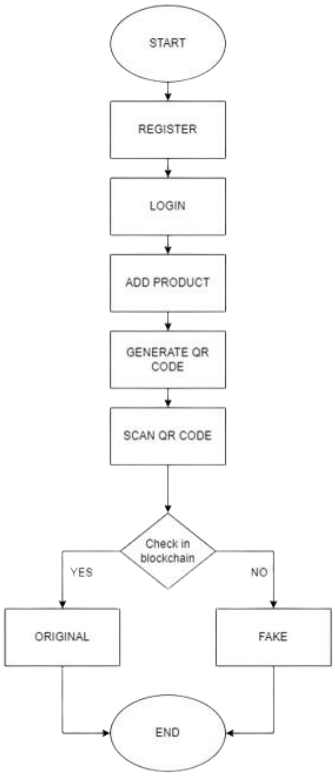

Fig. 4 – Workflow.

5.3. Product Verification

Product Verification refers to the process of confirming the accuracy and reliability of a product. Within the domain of consumerism, where the significance of choices is substantial and the importance of authenticity is important, the process of Product Verification arises as a prominent guiding principle.

a) Seamless Verification: When consumers are faced with a product, they possess the ability to verify its authenticity with ease. The technology enables users to efficiently verify the legitimacy of a product through several means, such as scanning a QR code or entering a distinct identification number.

b) The Importance of Smart Contract Security: In this scenario, the smart contract plays a vital role once more. It acts as a vigilant guardian of truth, quickly assessing whether a product is genuine or a skillful fake. If the item meets all set conditions, it receives the label "Available", confirming its authenticity digitally.

The focus shifts to the login process for manufacturers and the use of QR codes. Manufacturers, as the creators of authenticity [11], hold a pivotal role in the process. They access the system through a specialized login procedure. Each product receives a unique identification number and is accompanied by a QR code, acting as a digital key for further verification. Within this intricate technological framework, the successful integration of the product authentication system stands as a testament to the profound impact of innovation. This technology empowers consumers to navigate a marketplace filled with counterfeit goods with confidence [12], knowing that their choices are based on a solid foundation of trust.

6. ADVANTAGES OF THIS APPROACH

The implementation of our product authentication system using blockchain technology brings forth a multitude of appealing benefits and serves as evidence of the significant impact that trust and technology can have.

6.1. Enhanced Product Authentication

In an international marketplace, fake goods are common trust becomes the essential medium of exchange for business dealings. An essential part of the process of authenticating a product is the technology used in corporate trust.

A theoretical construct that is resistant to modification or change is referred to as the "Immutable Shield". With its immutable ledger, blockchain technology is a strong defense against illegal changes and dishonest behavior. After product data has been registered, it is stored in the blockchain permanently and cannot be altered in any way. Counterfeiters are successfully neutralized by the digital fortress, which prevents them from creating false narratives or altering product records.

Within the field of digital security, the Digital Guardian is a well-known entity. Smart contracts act as digital stewards in this system, carefully monitoring each product's integrity. Consistent monitoring and defined standards serve as a strong barrier against fraudulent infiltrations. Authenticity is not just a guarantee rather, it's a condition of being that never changes.

a) Enhancing Supply Chain Security: The ability of the system to ensure the security of product information throughout all stages of the supply chain is a significant transformative factor. Manufacturers, suppliers, and consumers can place their trust in the assurance that the trajectory of every product is characterized by transparency and verifiability. The enhanced degree of openness not only

serves to combat counterfeit products but also strengthens consumer trust and assurance.

2) Consumer Empowerment: Consumer empowerment refers to the process of enabling individuals to make informed decisions and assert their rights as consumers in the marketplace. In a market saturated with counterfeit goods, customers frequently exercise caution. The method we have developed provides consumers with the capacity to make well-informed decisions, offering them a sense of empowerment. By swiftly scanning a QR code or entering a distinctive identification number, individuals can differentiate authentic products from fraudulent ones. The emergence of this increased confidence has a profound impact on the consumer landscape, cultivating a sense of brand loyalty and engendering trust among consumers.

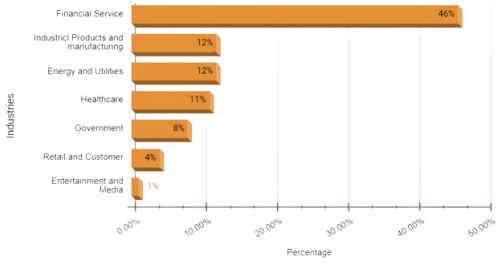

Fig. 5 – Industries – those are most advanced in developing through blockchain today.

6.2. Transparency

Our blockchain-based product authentication technology ushers in a new era of unmatched transparency in a world where trust can frequently feel like a finite resource. The benefits of this transparency [13] flow down the entire supply chain, acting as a powerful elixir that nurtures the relationship between makers and consumers.

a) Encouraging the Customer: Transparency is a gift to customers, not just a catchphrase. Customers may quickly and easily verify a product's legitimacy by using the blockchain [14]. Rather than relying solely on blind faith, they can now go on a journey of informed choices.

- **Building Digital Bricks to Build Trust**: The foundation of commerce is trust. The capacity for customers to confirm the legitimacy of products helps to build confidence in suppliers and manufacturers as they navigate the market. It's a guarantee of authenticity, not just a commodity they are buying. This trust is the cornerstone of enduring relationships and brand loyalty; it is not just transactional.
- **The Removal of All Doubt:** Purchasing decisions are typically clouded by doubt, particularly in an environment where counterfeit goods are common. Our system shines like a lighthouse, clearing the mists of doubt. Customers can choose products with confidence since the blockchain's transparency [15] has made authenticity easier to find.

2) Filling the Void: Consumers want openness in the freely available digital era. Manufacturers who accept this openness [16] help to close the gap between their clients and themselves. Selling a product is only one aspect of the process; another is enlisting customers as active participants in the search for authenticity.

6.3. Reduced Counterfeiting

Counterfeit items have been thriving in secrecy for a while now, undermining credibility and endangering consumers' security [17]. By exposing these fakes and taking away their market share, our approach serves as a shining light, preserving the caliber of genuine goods. In essence, transparency and a decline in counterfeiting are related to a dance that modifies the market. When customers recognize that real goods and services are the real currency of trade, they gain power, confidence is restored, and counterfeiters are compelled to hide.

7. CONCLUSION

In confronting the pervasive challenge of counterfeit goods, this study presents a groundbreaking solution through a blockchain-based product authentication mechanism, offering respite to both producers and consumers globally. The immutable nature of blockchain establishes an unassailable foundation of trust by safeguarding [18] product data against unauthorized alterations. Integral to this method, smart contracts serve as vigilant guardians, meticulously validating product information against predefined criteria, thereby fortifying the market against counterfeit infiltrations. The emphasis on transparency extends beyond mere transactional interactions, fostering a trustful relationship between consumers and manufacturers. By effectively exposing counterfeiters, this approach diminishes the market value of fraudulent goods, acting as a formidable deterrent to illicit production. This dual protection shields consumers and legitimate producers alike.

Looking ahead, the fusion of product authentication and blockchain technology opens up exciting avenues for future exploration. A pivotal focus is on integrating our solution into supply chains, streamlining their intricate networks for enhanced efficiency. Further research can delve into the

dynamic realm of real-time tracking, offering continuous monitoring of goods movement for comprehensive insights. Our solution's potential in automating supply chain operations through smart contracts holds promise, reducing the need for manual intervention. Exploring the use of public blockchains, known for their accessibility and transparency, is a pathway to further elevate trust. This shift not only embraces technological advancement but also signifies a commitment to transparency and diversity, fostering increased consumer confidence. As public blockchains continue to gain popularity in the interconnected marketplace, future work aims to propel this transformative journey, reinforcing authenticity and confidence in the evolving landscape of product authentication.

8. LIMITATIONS

However, it is essential to acknowledge certain limitations within the present work. The system's dependency on blockchain technology and the reliance on smart contracts, while robust, introduce external factors that may pose challenges, such as potential issues with third-party tools and initial implementation costs. Despite these considerations, the transformative impact of blockchain technology on counterfeiting reduction, product safety assurance, and reliability enhancement is evident. The call to action at the conclusion underscores the system's viability, urging further research and advancements to refine consumer protection and enhance societal acceptance through ongoing technological innovation.

REFERENCES

Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of Blockchain Technology: Architecture, Consensus, and Future Trends” 2017 IEEE International Congress on Big Data Honolulu, HI, USA, 2017, pp. 557-564, doi:10.1109/BigDataCongress. 2017.85.

A.H. Mohammed, A. A. Abdulateef and I. A. Abdulateef, “Hyperledger, Ethereum and Blockchain Technology: A Short Overview,” 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2021, pp. 1-6, doi: 10.1109/HORA52670.2021.9461294.

S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F.-Y. Wang, “Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends,” in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi:10.1109/ TSMC.2019.2895123.

M. Wohrer and U. Zdun, Smart contracts: security patterns in the Ethereum ecosystem and solidity,” 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 2018, pp. 2-8, doi:10.1109/IWBOSE.2018.8327565.

Product Authentication Technology Integrating Blockchain and Traceability Structure https://doi.org/10.3390/electronics11203314

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

Blockchain technology in supply chain operations: Applications, challenges and research opportunities https://doi.org/10.1016/j.tre.2020. 102067

AG. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz and T. M. Alam, “A journey of WEB and Blockchain towards the Industry 4.0: An Overview,” 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 2019, pp. 1-7, doi:10.1109/ICIC48496.2019.8966700.

Lee, WM. (2023). Using the MetaMask Crypto-Wallet. In: Beginning Ethereum Smart Contracts Programming. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-9271-6 5.

H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J.Kishigami, “Blockchain contract: Securing a blockchain applied to smart contracts,” 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2016, pp. 467-468, doi:10.1109/ICCE.2016.7430693.

Remya Stephen and Aneena Alex 2018 IOP Conf. Ser.: Mater. Sci. Eng. 396 012030 “A Review on BlockChain Security” doi10.1088/ 1757- 899X/396/1/012030

Architecture to Enhance Transparency in Supply Chain Management Using Blockchain Technology, “https://doi.org/10.1016/j.promfg.2020.10.225”

D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, “Certificate Transparency Using Blockchain,” 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

R. S. Bhatnagar, S. M. Jha, S. S. Singh and R. Shende, “Product Traceability Using Blockchain,” 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2020, pp. 891-895, doi:10.1109/ ICACCCN51052.2020.9362807.

P. William, D. Jadhav, P. Cholke, M. A. Jawale and A. B. Pawar, “Framework for Product Anti-Counterfeiting using Blockchain Technology,” 2022 International Conference on SustainablecComputing and Data Communication Systems (ICSCDS), Erode, India, 2022, pp. 1254-1258, doi:10.1109/ICSCDS53736.2022.9760916

A. Mishra, H. Khatter, G. Gupta, A. Jamshed, A. K. Srivastava, “Enabling Secure and Transparent Crowd Funding Approach Powered by Blockchain”, Third International Conference on Emerging Technologies in Data

Mining and Information Security, Institute of Engineering Management, Kolkata, West Bengal, India, 23-25 February 2022, Proceedings in LNNS, vol 490. Springer, Singapore https://doi.org/10.1007/ 978-981-19-4052-1 64

H. Khatter, H. Chauhan, I. Trivedi, and J. Agarwal, "Secure and Transparent Crowdfunding Using Blockchain," 2021 International Conference on Recent Trends in Electronics, Information, Communication Technology (RTEICT), 2021, pp. 76-80, DOI: 10.1109/RTEICT52294. 2021.9573956.

Amrita Jyoti, Sonam Gupta, Pradeep Gupta, Harsh Khatter, Anurag Mishra, "Inherent Insights using systematic analytics of development tools in Ethereum-Blockchain Smart Contract", Recent Advances in Electrical Electronic Engineering, submitted in Feb 2023, Revision Submitted 15 April 2023, Second Revision: 26 April 2023, Accepted on 28 Sep 2023. ISSN: 2352-09

Proof of Patent Publication

TITLE OF INVENTION	METHOD AND SYSTEM FOR BLOCKCHAIN-BASED PRODUCT VALIDATION
FIELD OF INVENTION	COMPUTER SCIENCE
E-MAIL (As Per Record)	vardhan2520@gmail.com
ADDITIONAL-EMAIL (As Per Record)	
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	09/02/2024

Application Status	
APPLICATION STATUS	Awaiting Request for Examination

View Documents

In case of any discrepancy in status, kindly contact ipo-helpdesk@nic.in