MAIN PROJECT REPORT

ON

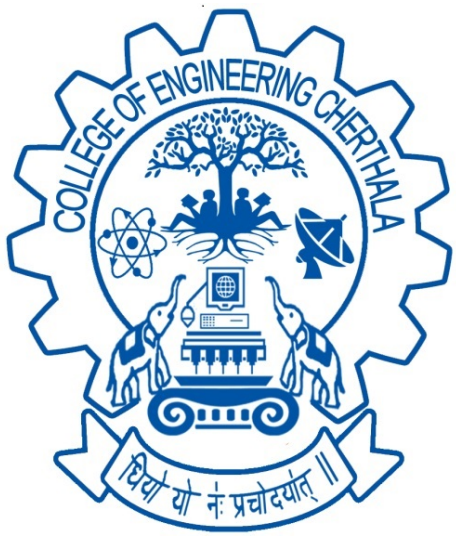
GRAND SMART : FAKE PRODUCT DETECTION USING BLOCKCHAIN

Submitted By

DEVANANDANA S (CEC23MCA-2014)

in partial fulfillment for the award of the degree of

Master of Computer Application



Department of Computer Engineering

College of Engineering, Cherthala

Alappuzha - 688541

APJ Abdul Kalam Technological University

March 2025

MAIN PROJECT REPORT

ON

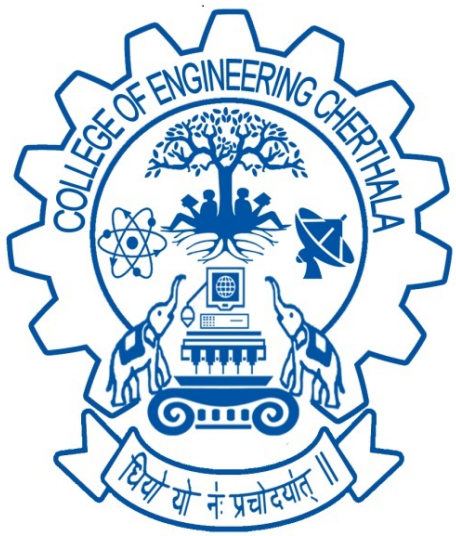
GRAND SMART : FAKE PRODUCT DETECTION USING BLOCKCHAIN

Submitted By

DEVANANDANA S (CEC23MCA-2014)

in partial fulfillment for the award of the degree of

Master of Computer Application



Department of Computer Engineering

College of Engineering, Cherthala

Alappuzha - 688541

APJ Abdul Kalam Technological University

March 2025

DEPARTMENT OF COMPUTER ENGINEERING

COLLEGE OF ENGINEERING, CHERTHALA

ALAPPUZHA-688541

C E R T I F I C A T E

This is to certify that , the project report titled **"GRAND SMART : FAKE PRODUCT DETECTION USING BLOCKCHAIN"** is a bonafide record of the **20MCA246 Main Project** presented by **DEVANANDANA S (CEC23MCA2014)**, Fourth semester Master of Computer Aplication student, under our guidance and supervision, in partial fulfillment of the requirements for the award of the degree, **Master of Computer Application** of **APJ Abdul Kalam Technological University during the academic year 2024-2025**.

Guide	**Co-ordinator**	**HOD**
Ms. Nazeema H	**Ms. Renjusha Aravind**	**Dr. Preetha Theresa Joy**
Assistant Professor	Assistant Professor	Professor
Dept. of Computer Engg.	Dept. of Computer Engg.	Dept. of Computer Engg.

ACKNOWLEDGEMENT

This work would not have been possible without the support of many people. First and the foremost, we give thanks to Almighty God who gave us the inner strength, resource and ability to complete our project successfully.

I, DEVANANDANA S would like to thank **Dr. Jaya V.L**, our Principal, who has provided with the best facilities and atmosphere for the project completion and presentation.I would also like to thank our HoD **Dr. Preetha Theresa Joy** (Professor, Department of Computer Engineering), our project co-ordinator **Ms.Renjusha Aravind** (Assistant Professor, Department of Computer Engineering), and my guide **Ms.Nazeema H** (Assistant Professor, Department of Computer Engineering) for the help extended and also for the encouragement and support given to us while doing the project.

I would like to thank my dear friends for extending their cooperation and encouragement throughout the project work, without which we would never have completed the project this well.Thank you all for your love and also for being very understanding.

DECLARATION

I hereby declare that the project “GRAND SMART : FAKE PRODUCT DETECTION USING BLOCKCHAIN” is a bonafide work done by me during the academicyear 2024-2025 under the guidance of Ms.Nazeema H ,Assistant Professor at College of Engineering,Cherthala and this report has not been previously formed the basis for the award of any degree, diploma, fellowship or any other similar title or recognition in any other university.

DEVANANDANA S

CEC23MCA2014

27/03/2025

ABSTRACT

The proliferation of counterfeit products continues to threaten consumer safety, brand integrity, and economic stability across various industries. Traditional methods of product authentication often rely on centralized databases, making them susceptible to manipulation, fraud, and limited transparency. This project proposes a robust solution by integrating blockchain technology, IPFS (InterPlanetary File System), and watermarked QR codes to create a secure, decentralized counterfeit detection system.

In this system, manufacturers register product information on a blockchain ledger, ensuring immutability and traceability. Detailed metadata, including product certificates or images, is securely stored on IPFS, providing a decentralized and tamper-resistant storage layer. Each product is tagged with a uniquely generated QR code embedded with a watermark, which serves as a visual deterrent against counterfeiting. Consumers can scan the QR code to retrieve product information via IPFS and verify its authenticity through blockchain-backed validation.

This solution is highly applicable in domains such as pharmaceuticals, electronics, luxury goods, and agriculture, where the authenticity and traceability of products are crucial. By combining blockchain for transaction integrity, IPFS for decentralized file storage, and watermarking for visual security, the system offers a transparent, scalable, and user-friendly platform for counterfeit prevention.

Contents

List of Figures

Chapter 1

INTRODUCTION

The increasing presence of counterfeit products across industries such as pharmaceuticals, electronics, fashion, and agriculture poses serious threats to consumer safety, brand reputation, and economic stability. Traditional methods of product verification, which often rely on centralized systems and manual checks, are susceptible to tampering, inefficiency, and a lack of transparency.

To address these limitations, this project proposes a counterfeit detection system that leverages three key technologies: Blockchain, IPFS (InterPlanetary File System), and Watermarked QR Codes. Blockchain ensures data immutability, decentralization, and transparency, making it nearly impossible for counterfeiters to manipulate product information once it's recorded. Each product's lifecycle is traceable from manufacturing to end-use, increasing trust and accountability.

The use of IPFS enhances the system by providing decentralized and secure file storage for metadata like product images and certificates. IPFS ensures fast, reliable access to product data using cryptographic hashes, reducing dependency on centralized servers.

Watermarked QR codes serve as the consumer interface, offering a secure and scannable means of verifying product authenticity. These QR codes are embedded with invisible watermarks that are hard to duplicate and act as a gateway to retrieve the product's record from IPFS and verify it via blockchain.

This chapter provides an overview of the problem statement, the objectives of the proposed system, and the scope of the work undertaken to address the challenge of counterfeit product detection using emerging decentralized technologies.

Chapter 2

PROBLEM STATEMENT

2.1 Problem Statement

Counterfeit products have become a significant issue across various industries, leading to economic losses, reputational damage, and safety risks for consumers. Traditional product authentication methods, such as holograms, barcodes, and centralized verification systems, are often ineffective due to their vulnerability to forgery, tampering, and unauthorized replication. As a result, counterfeiters continue to exploit these weaknesses, flooding markets with fake goods that are nearly indistinguishable from genuine products.

Consumers often lack a reliable and instant method to verify product authenticity before making a purchase. Even when verification systems exist, they are frequently centralized, which makes them prone to data breaches, unauthorized modifications, and inefficiencies. Furthermore, businesses struggle to maintain trust in their brands as counterfeiters produce near-identical copies of their products, leading to loss of revenue and customer confidence.

To address this issue, a decentralized, tamper-proof, and user-friendly verification system is required. Blockchain technology, known for its immutability and transparency, offers an ideal solution for securely storing and verifying product data. By integrating blockchain with QR code-based verification, consumers can easily check a product's authenticity by scanning a QR code, retrieving secure data directly from the blockchain, and ensuring that the product information remains unaltered and trustworthy.

This project, "Fake Product Detection Using QR Code," aims to eliminate reliance on centralized verification methods by implementing a secure, decentralized solution that empowers consumers and businesses to combat counterfeiting efficiently.

2.2 Objective

The primary objective of this project, "Fake Product Detection Using QR Code," is to develop a secure, decentralized, and efficient system for verifying product authenticity using blockchain technology and QR codes. The system aims to empower consumers and businesses by providing a tamper-proof solution that prevents counterfeiting and enhances trust in the supply chain.The key objectives of the project are:

1. Blockchain Network : The project utilizes blockchain technology to store product details in a tamper-proof and decentralized manner, ensuring data integrity and transparency.

2. QR Code Generation : Each registered product is assigned a unique QR code that links to its blockchain-stored information, allowing easy verification by consumers.

3. Web-Based Front-End : A user-friendly interface developed using HTML, CSS, and JavaScript enables consumers to scan QR codes and check product authenticity.

4. Web3.js Integration : Web3.js is used to connect the front-end with the blockchain, enabling seamless interaction for retrieving and verifying product data.

5. Smart Contract : A smart contract is deployed on the blockchain to handle product registration and verification, ensuring that data remains immutable and verifiable.

6. QR Code Scanner : The system includes an integrated QR code scanner to allow consumers to scan and validate products instantly.

7. Decentralized Data Storage : Unlike traditional databases, product details are stored on a blockchain, eliminating the risk of data manipulation or unauthorized modifications.

Chapter 3

EXISTING SYSTEM

In the current scenario, counterfeit products have become a major challenge in various industries, including pharmaceuticals, luxury goods, electronics, and consumer products. The existing systems for counterfeit detection primarily rely on centralized databases, traditional QR codes, and manual verification methods.

3.1 Centralized Databases and Limited Security

Many companies store product details in centralized servers that act as the main source of authentication. When a consumer or retailer wants to verify a product, they must cross-check it with the company's database. However, these centralized systems are prone to hacking, data breaches, and unauthorized modifications. If attackers gain access to these databases, they can manipulate product records, making counterfeit products appear genuine.

3.2 Traditional QR Code-Based Verification

Some brands use basic QR codes for product verification. Consumers can scan these codes using a mobile application to retrieve product details. However, these QR codes do not have additional security layers and can be easily copied or cloned by counterfeiters. Fraudsters can print duplicate QR codes and attach them to fake products, deceiving consumers into believing they are purchasing authentic goods.

3.3 Manual and Third-Party Verification

In many cases, authentication requires manual verification by the manufacturer or a third-party certification agency. This process is time-consuming, costly, and prone to errors. Since it relies on human intervention, it is inefficient for large-scale verification. Moreover, consumers do not always have direct access to such verification systems, leading to delayed responses and limited trust in the authentication process.

3.4 Lack of Transparency and Consumer Trust

Consumers often have to rely solely on the brand's reputation to determine a product's authenticity. If a counterfeit product enters the market with a copied QR code or fake packaging, customers may unknowingly purchase it, leading to financial loss and health risks. Since existing systems do not provide an open and verifiable authentication process, consumer trust is easily exploited by counterfeiters.

3.5 Inaccuracy in Counterfeit Detection

Current anti-counterfeiting methods struggle to differentiate between genuine and fake products accurately. Since QR codes and labels can be duplicated, counterfeiters continuously find ways to bypass existing security measures. Without a tamper-proof and immutable record of authenticity, the risk of counterfeit products circulating in the market remains high.

Chapter 4

LITERATURE REVIEW

Counterfeit products have become a significant issue in various industries, including pharmaceuticals, electronics, and consumer goods. The rise in counterfeit goods not only causes financial losses to manufacturers but also endangers consumer safety. Traditional counterfeit detection methods rely heavily on centralized authorities, manual verification, and third-party authentication, making them prone to inefficiencies and fraud. With the advent of blockchain technology, researchers have explored decentralized and immutable solutions for counterfeit detection. Blockchain provides transparency, security, and traceability, allowing consumers and stakeholders to verify product authenticity with ease. This literature review examines five key research papers on blockchain-based counterfeit detection systems, highlighting their contributions, methodologies, and limitations.

1. **Fake Product Identification for Small and Medium Firms (FPISMF) Using Blockchain Technology**

   Proposed a blockchain-based fake product identification system tailored for small and medium enterprises (SMEs) [1]. Their research addressed the financial constraints of SMEs, offering a cost-effective blockchain solution that enables product authentication. The proposed system ensures decentralized verification, preventing unauthorized modifications to product data. By using a secure ledger, SMEs can register their products, and consumers can verify authenticity by scanning a QR code linked to the blockchain. While this approach enhances transparency and security, the study lacks an in-depth discussion on scalability and the po-

tential cost implications of blockchain transactions for SMEs. Moreover, advanced security measures, such as watermark codes or AI-based verification, were not considered in the research, limiting its robustness in detecting sophisticated counterfeits.

Advantages

- Tailored for SMEs with financial constraints.
- Cost-effective blockchain solution.
- Decentralized verification; avoids third-party interference.
- Secure QR code-based authentication.

Disadvantages

- Scalability concerns are not addressed.
- No detailed cost analysis of blockchain implementation.

  Lacks advanced verification (e.g., watermarking, AI-based detection).
- May be vulnerable to sophisticated counterfeiting techniques.

2. **Fake Product Detection System Using Blockchain (2023)**

   Introduced a blockchain-powered fake product detection system that leverages smart contracts to automate authentication processes [2]. Their study emphasized real-time verification, allowing consumers to instantly check a product's authenticity by scanning a QR code. Smart contracts played a crucial role in eliminating the need for third-party verification, ensuring that all transactions and product registrations were immutable. However, the paper did not provide a comprehensive analysis of scalability, making it unclear whether the system could efficiently handle a large number of transactions. Additionally, while QR code-based verification was an effective approach, the absence of multi-factor authentication methods, such as biometric verification or watermarking, was a notable limitation. Furthermore, the study focused on product verification but did not integrate supply chain tracking, which is essential for comprehensive counterfeit detection.

Advantages

- Smart contracts automate product verification.
- Real-time consumer-side verification via QR code.
- Eliminates third-party authentication dependency.

Disadvantages

- Scalability and performance under high transaction loads are not analyzed.
- No multi-factor authentication (e.g., biometrics, watermarking).
- No supply chain tracking component included.

3. **BCPIS: Blockchain-Based Counterfeit Product Identification System**

   Introduced the Blockchain-Based Counterfeit Product Identification System (BCPIS), which emphasizes decentralized verification without reliance on third-party authorities [3]. Their system enables manufacturers to securely register their products while allowing consumers to verify authenticity through blockchain-stored data. One of the key strengths of this approach is its peer-to-peer verification mechanism, which allows multiple stakeholders to validate product information independently. Additionally, the study analyzed security threats in counterfeit detection and demonstrated how blockchain prevents unauthorized modifications. However, the research lacked supply chain tracking features, making it difficult to trace a product's journey from manufacturer to consumer. Moreover, while the paper extensively discussed blockchain security, it did not integrate external verification technologies such as IoT sensors or AI-based counterfeit detection. Another limitation was the absence of performance analysis concerning transaction volume, raising concerns about potential bottlenecks when scaling the system.

   Advantages

   - Peer-to-peer verification enables decentralized trust.
   - Strong security discussion highlighting blockchain's integrity.

- Prevents unauthorized data tampering.

Disadvantages

- No supply chain tracking; limits end-to-end visibility.
- Lacks integration with external tech (e.g., IoT, AI).
- No performance testing; potential issues with high transaction volumes.

4. **Fake Product Detection Using Blockchain Technology (2022)**

Proposed a blockchain-integrated supply chain management system for counterfeit detection, focusing on transparency and real-time updates [4]. Their research introduced smart contracts to automate product authentication and track product movements throughout the supply chain. By implementing real-time updates, the system ensured that counterfeit items could be easily identified when a product changed ownership. The integration of blockchain with supply chain management was a crucial advantage, as it prevented fake products from entering the distribution network undetected. However, the study primarily focused on supply chain security rather than direct consumer verification, making it less user-friendly for consumers looking to check product authenticity. Additionally, the research did not examine the financial feasibility of blockchain adoption in large supply chains, where transaction costs could be a concern. The system also lacked additional authentication features, such as watermark codes or AI-driven verification techniques, which could further enhance counterfeit detection. **Advantages**

- Integrates blockchain with supply chain management.
- Enables real-time product tracking and updates.
- Smart contracts automate and secure authentication.

Disadvantages

- Consumer-facing verification is not emphasized.

- Financial feasibility and transaction cost concerns not addressed.
- Missing advanced authentication (e.g., watermark or AI).

5. **Detection of Counterfeit Products using Blockchain**

   Explored the role of blockchain in securing supply chains against counterfeit products by analyzing different consensus mechanisms and their effectiveness in counterfeit detection [5]. This paper proposes a blockchain-based solution aimed at detecting counterfeit products by creating a decentralized, transparent platform for recording product information. The main idea is to maintain a tamper-proof ledger of all legitimate products, with every entry uniquely identified and linked to a QR code. Consumers can scan these codes to verify authenticity, while manufacturers can upload product information directly to the blockchain. The authors emphasize the importance of decentralization and traceability, asserting that blockchain can eliminate the risks associated with centralized databases that are prone to tampering.

   The approach involves registering products on the blockchain using metadata (product ID, manufacture date, etc.) and generating a QR code for each item. The consumer can scan the QR code to access the product history and verify legitimacy. This adds a strong layer of transparency and trust to the system.

   Advantages

   - The use of blockchain ensures immutability and tamper-resistance of product data.
   - QR code integration allows for easy and real-time product verification.
   - Eliminates the need for third-party verification, reducing cost and complexity.

   Disadvantages

   - The paper lacks performance evaluation or scalability analysis under real-world load.
   - It does not address challenges in counterfeit packaging or lookalike branding, where visual inspection tools could be useful.

- There's no exploration of integration with supply chain systems or IoT devices for dynamic updates.

6. **Fake Product Detection System Using Blockchain**

   This study introduces a system that leverages blockchain and smart contracts to enable real-time counterfeit product detection [6].The system stores each product's data on a blockchain, allowing buyers to verify product details using a QR code. A unique selling point of this paper is the implementation of smart contracts that automate the verification and registration process. When a product is manufactured, its information is hashed and stored on the blockchain. Consumers can then scan the QR code and compare it to the data on-chain to check for legitimacy.

   The authors focus on improving user experience by providing instant verification without requiring third-party services. The smart contract aspect eliminates delays and ensures automatic responses when a consumer checks a product.

   Advantages

   - Smart contracts automate product verification, improving efficiency.
   - Eliminates centralized control, enhancing trust and reducing manipulation.
   - Focuses on a user-friendly approach with QR-based real-time verification.

   Disadvantages

   - Lacks exploration of security features beyond QR codes, such as watermarking or biometric verification.
   - Supply chain involvement and tracking are not deeply discussed, limiting visibility into the product lifecycle.
   - Doesn't specify how the blockchain network is maintained or its consensus method, leaving questions about energy and cost efficiency.

7. **Detection using Blockchain (IEEE, 2024)**

This IEEE publication presents a comprehensive approach to fake product detection through blockchain-integrated supply chain management[7].Unlike papers focused solely on consumer verification, this research highlights the importance of end-to-end product traceability across the supply chain. The authors suggest that every product transaction—from manufacturer to retailer—should be recorded on the blockchain. As the product moves across stakeholders, smart contracts automatically update its status, ensuring transparency and making it difficult for fake products to infiltrate the network.

The study also explores stakeholder collaboration, proposing that manufacturers, distributors, and retailers all participate in the blockchain ecosystem. Each party validates the transaction at their stage, helping to build a trustworthy product trail. The system includes a secure user interface where stakeholders can input and view product status updates.

Advantages

- Provides full supply chain traceability, improving detection of counterfeit infiltration points.
- Enables real-time tracking of product ownership and location using smart contracts.
- Multi-party involvement enhances accountability and trust across the ecosystem.

Disadvantages

- Less focus on direct consumer usability—real-time QR verification for buyers is not emphasized.
- No discussion of implementation cost, particularly for small retailers or rural supply chains.
- Advanced verification technologies (e.g., image recognition, watermarking) are not included to detect physical counterfeit traits.

Chapter 5

PROPOSED SYSTEM

The proposed system aims to ensure the authenticity and traceability of products using a blockchain-based fake product detection system integrated with QR code verification and IPFS for decentralized file storage. This system allows registered companies to upload product data securely, and enables consumers to verify product authenticity using a QR code scanner.

5.1 IPFS Integration

Product metadata or associated files (e.g., images, certificates, or product manuals) are uploaded to IPFS.It returns a unique content hash (CID), which is then stored on the blockchain.This ensures decentralized, tamper-proof storage of documents, reducing storage costs and improving transparency.

5.2 Decentralized and Tamper-Proof Product Registration

Unlike centralized databases, the proposed system stores product details on a blockchain, making the records immutable and secure. Each product is assigned a unique identifier, which is permanently recorded on the blockchain. Once registered, the product data cannot be modified or deleted, eliminating the risk of data manipulation and hacking. This ensures trust and transparency in product authentication.

5.3 Enhanced Security with Watermarked QR Codes

Instead of using basic QR codes, this system generates watermarked QR codes with hidden encrypted layers. These watermarks make it nearly impossible for counterfeiters to replicate or tamper with the QR code. When scanned, the system verifies the embedded watermark and product details against blockchain records. If the watermark does not match, the system flags the product as counterfeit, preventing fraud.

5.4 Automated Verification with Smart Contracts

The proposed system uses smart contracts to automate product verification. When a consumer scans the QR code, the smart contract retrieves the stored product details from the blockchain and verifies authenticity instantly. If the scanned product exists in the blockchain with matching details, it is marked as genuine; otherwise, the system raises an alert for counterfeit detection. This eliminates manual verification, making the process faster, more efficient, and cost-effective.

5.5 Transparent and Consumer-Friendly Authentication

The system provides a web-based interface that allows consumers to verify product authenticity in real time. Instead of relying on brand reputation or third-party verification, users can simply scan the QR code using their smartphone or computer to retrieve blockchain-stored product details. This empowers consumers to make informed decisions and prevents them from falling victim to counterfeit goods.

5.6 Improved Accuracy in Fake Product Detection

Since the blockchain ledger is immutable and decentralized, counterfeiters cannot manipulate the stored data. Additionally, the combination of blockchain and watermarked QR codes adds multiple layers of security, making it nearly impossible for fake products to pass as genuine.

Chapter 6

SYSTEM DESIGNS

6.1 System Architecture

- User Interface Layer – Web application for product registration and verification.
- Application Layer – Smart contracts, backend processing, and database management.
- Blockchain Layer – Secure, decentralized ledger for storing product data.
- Sales and Payment Integration:

6.2 System Components

6.2.1 User Interface (Front-End)

- Developed using React.js for a user-friendly experience.
- Provides separate interfaces for companies (to register products) and consumers (to verify authenticity).
- Allows QR code scanning for quick product verification.

6.2.2 Smart Contract (Blockchain)

- Developed in Solidity and deployed on Ethereum blockchain.

- Functions include:

  registerProduct() – Stores product details on blockchain.

  verifyProduct() – Checks authenticity using the product ID.

  transferOwnership() – Updates product ownership details.

6.2.3 Watermarked QR Code Generation

- Each product is assigned a unique QR code with an embedded watermark to prevent tampering.
- The QR code links to product data stored on the blockchain.

6.2.4 Backend (Node.js Web3.js)

- Node.js handles API requests for blockchain interaction.
- Web3.js facilitates smart contract communication.
- SQL database is used for company authentication (login/signup).

6.2.5 Database (SQL)

- Used to store company login details (companies must be authenticated before product registration).
- Ensures secure access control for product registration.

6.3 Data Flow Diagram

6.3.1 Level 0

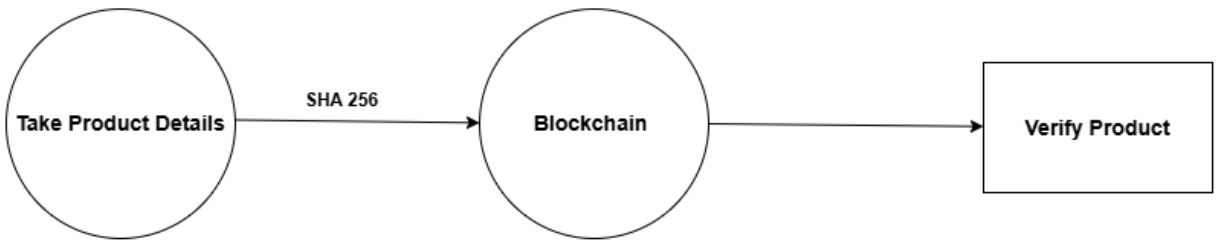


Fig. 6.1: Data Flow Diagram - Level 0

6.3.2 Level 1

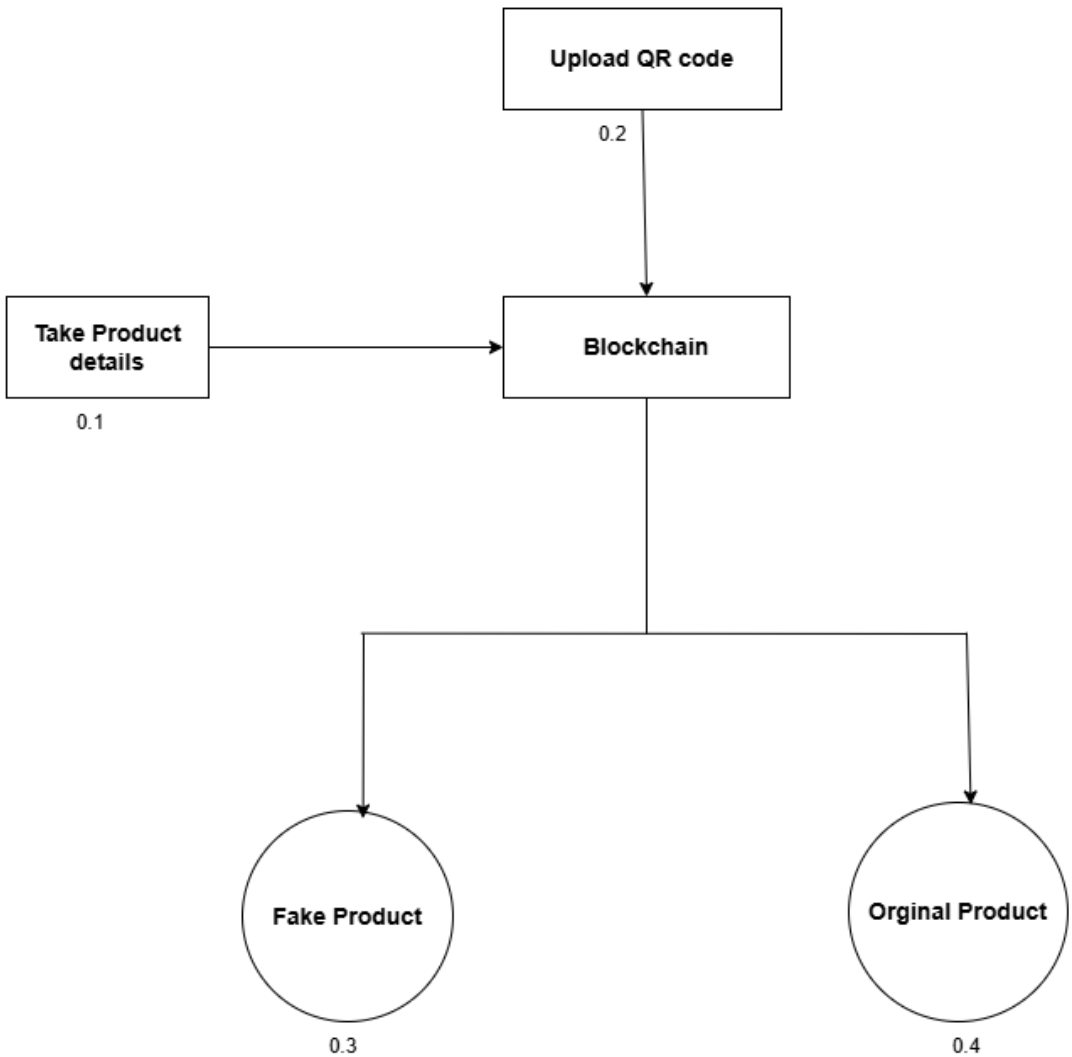


Fig. 6.2: Data Flow Diagram - Level 1

6.3.3 Level 2

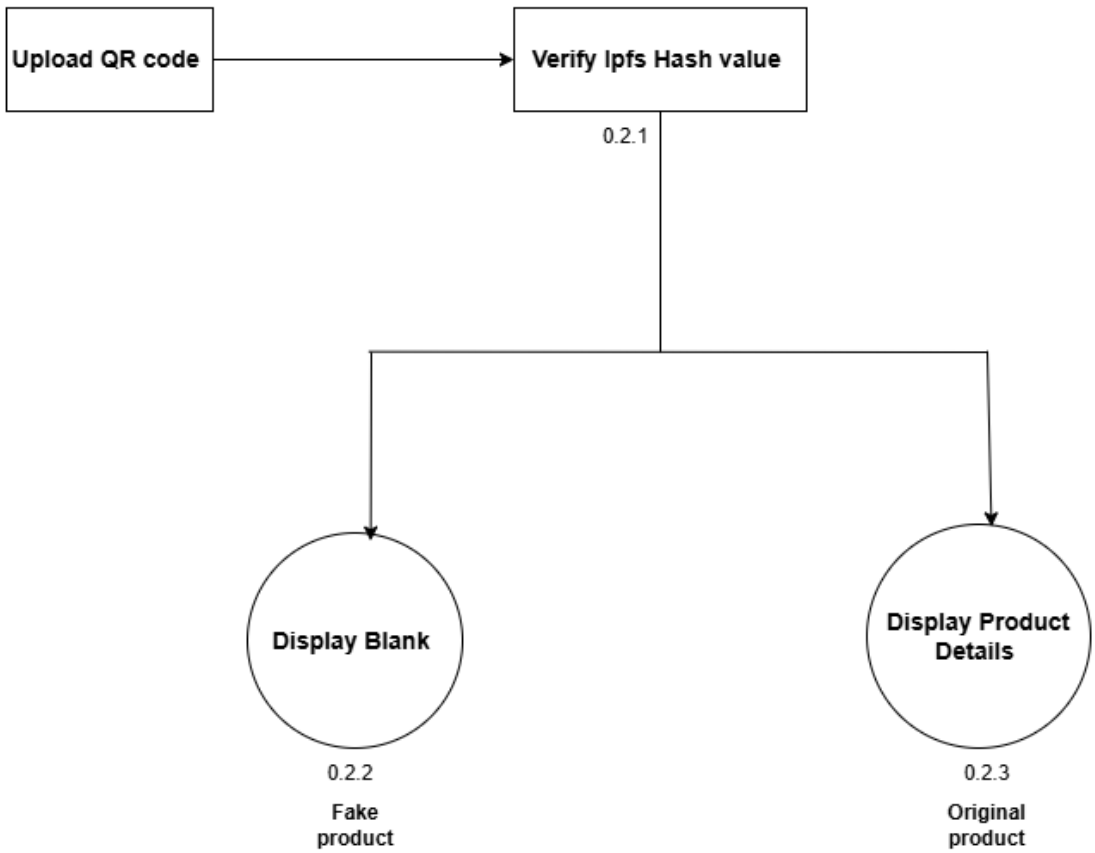


Fig. 6.3: Data Flow Diagram - Level 2

6.4 System Design Diagram

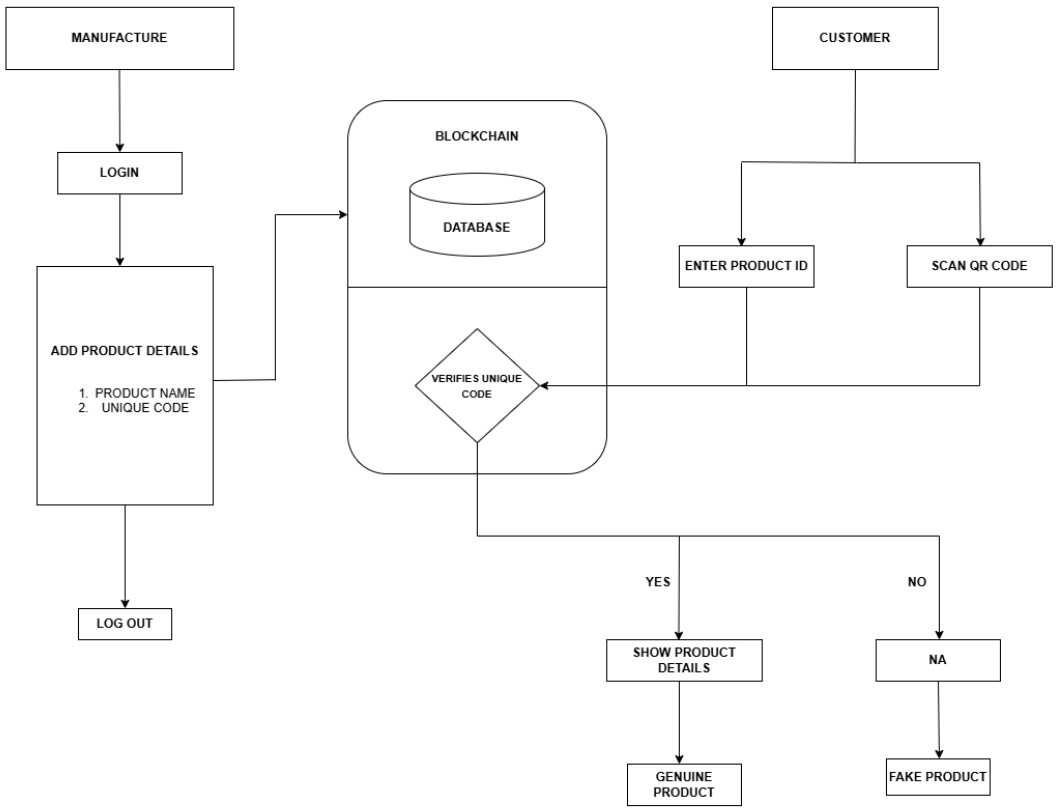


Fig. 6.4: System Design Diagram

Chapter 7

SOFTWARE AND HARDWARE REQUIREMENTS

7.1 Software Requirements

Software	Description
Operating System	Windows/Linux/MacOS
Blockchain Platform	Ethereum
Smart Contract Language	Solidity
Backend Framework	Node.js
Frontend Framework	React.js
Database	SQL (for authentication data)
Blockchain API	Web3.js
QR Code Library	qrcode.js for generation
IPFS	Decentralized file storage system for product-related documents
Remix IDE	Online IDE for writing, compiling, and deploying smart contracts
Ganache	Local Ethereum blockchain for testing smart contracts

Table 7.1: Software Requirements

7.2 Hardware Requirements

Hardware	Description
Processor	Intel Core i5 or higher
RAM	8 GB minimum
Storage	100 GB SSD
Internet Connection	Required for blockchain interaction

Table 7.2: Hardware Requirements

7.3 Other Requirements

7.3.1 Security Requirements

- Data encryption for transactions.
- Smart contract validation before deployment.
- Role-based access control for manufacturers and consumers.

7.3.2 Performance Requirements

- QR code scanning should return results within 3 seconds.
- Blockchain transactions should be processed within 10 seconds.

Chapter 8

IMPLEMENTATION

8.1 System Development Phases

8.1.1 Smart Contract Development

- The core of the system is built on blockchain technology, where a smart contract is developed and deployed using Remix IDE.
- The smart contract ensures secure product registration and verification through Ethereum blockchain.
- Solidity is used to define the contract's functions, such as product authentication and ownership transfer.

8.1.2 Watermarked QR Code Generation

- Each product is assigned a unique QR code embedded with a digital watermark to prevent tampering.
- This QR code is linked to blockchain data, ensuring authenticity and traceability.

8.1.3 Database and Web Integration

- The project integrates a SQL database for storing user credentials (for company authentication).

- A Node.js backend with Web3.js interacts with the blockchain for data retrieval and verification.

8.1.4 1.4 Front-End Development

- Company Registration/Login
- Product Registration Form
- Product Verification Page (via QR code scan or product ID entry)

8.1.5 Testing and Deployment

- Unit testing of smart contracts is conducted using Truffle and Ganache.
- The system is tested on a local blockchain before considering deployment on a testnet (e.g., Ropsten or Goerli).
- The front-end and backend are integrated and tested for seamless interaction.

8.2 Project Timeline

The project's timeline is planned to ensure efficient execution. The following Gantt chart represents the estimated time frame for each phase.

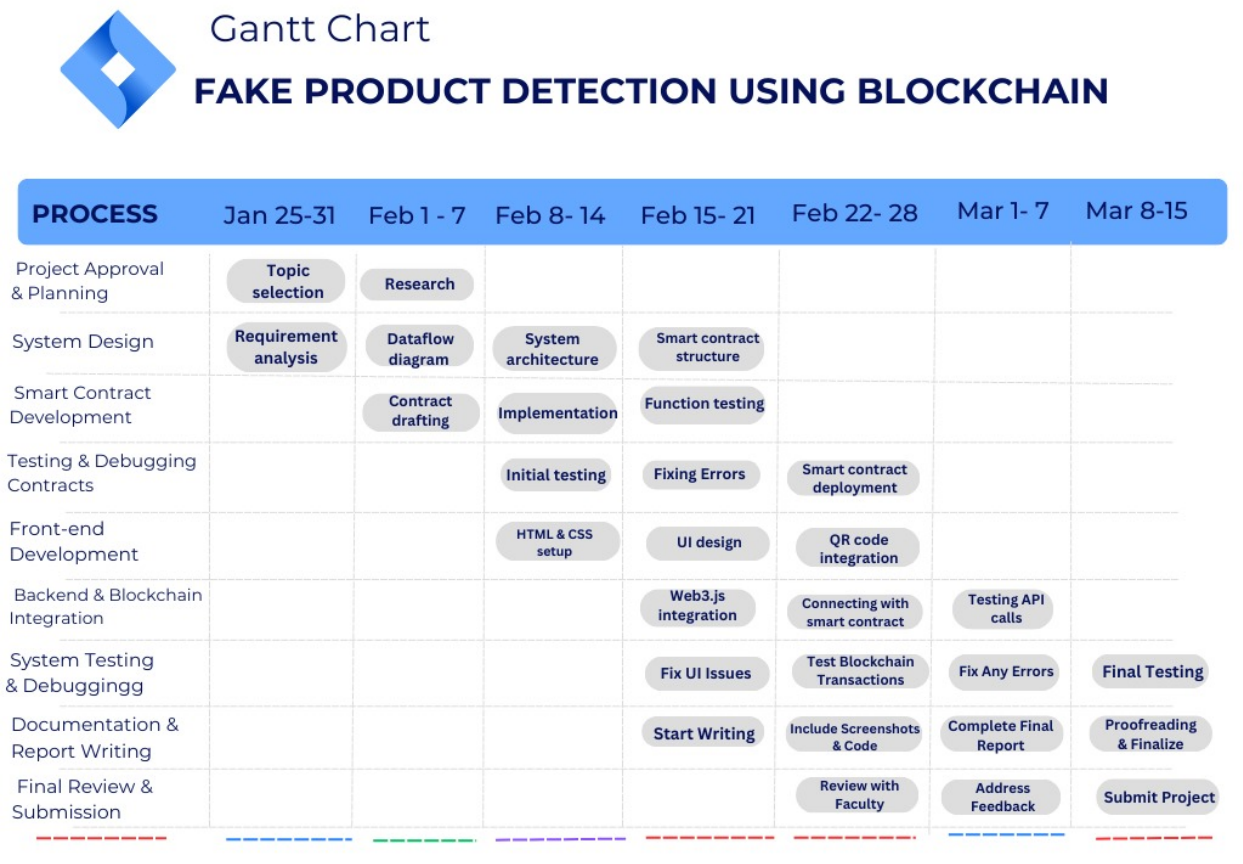


Fig. 8.1: Gantt Chart for Project Implementation

8.3 Deployment Strategy

- Hosting the front-end using Vercel or Netlify.
- Deploying the smart contract to a public blockchain (e.g., Polygon or Ethereum testnet).
- Ensuring security audits for smart contracts.

Chapter 9

RESULT AND ANALYSIS

9.1 Home Page

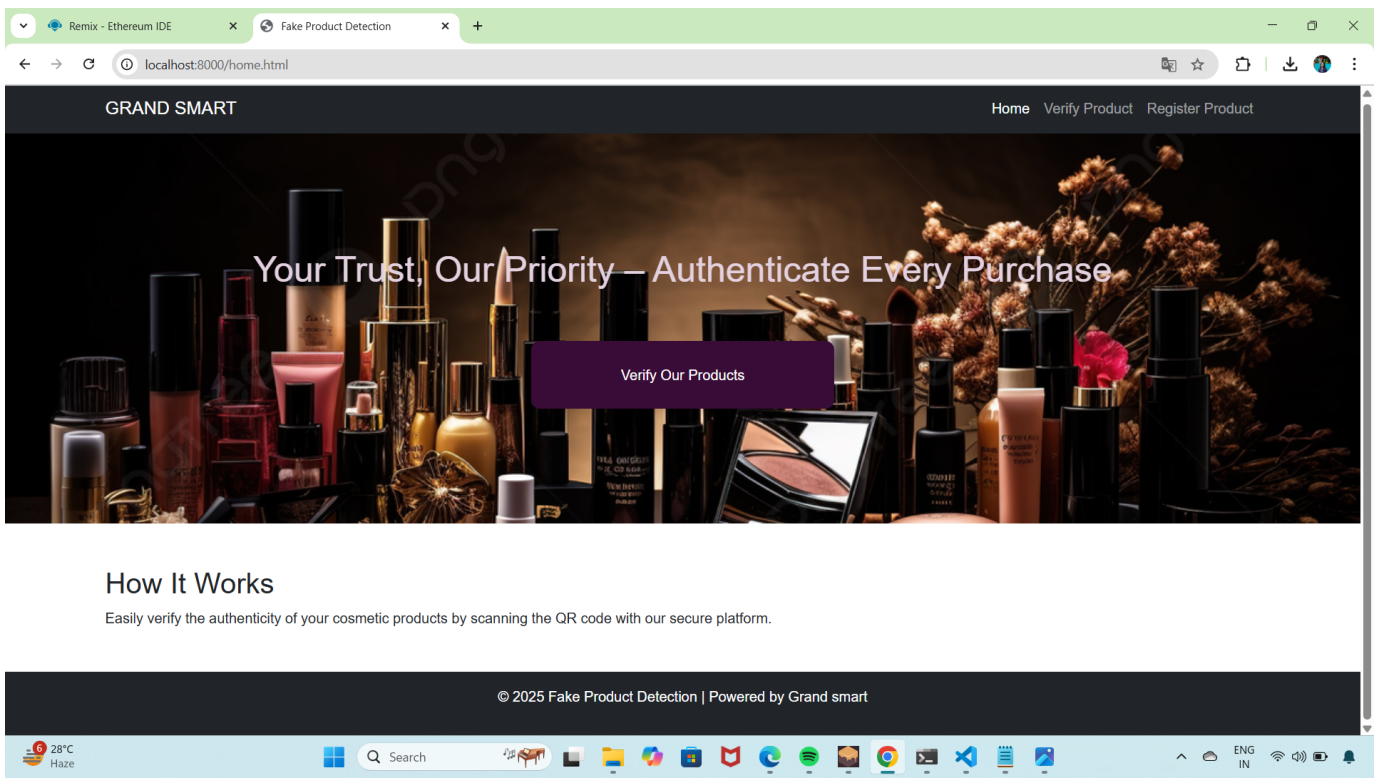


Fig. 9.1: Home Page

9.2 Company login page

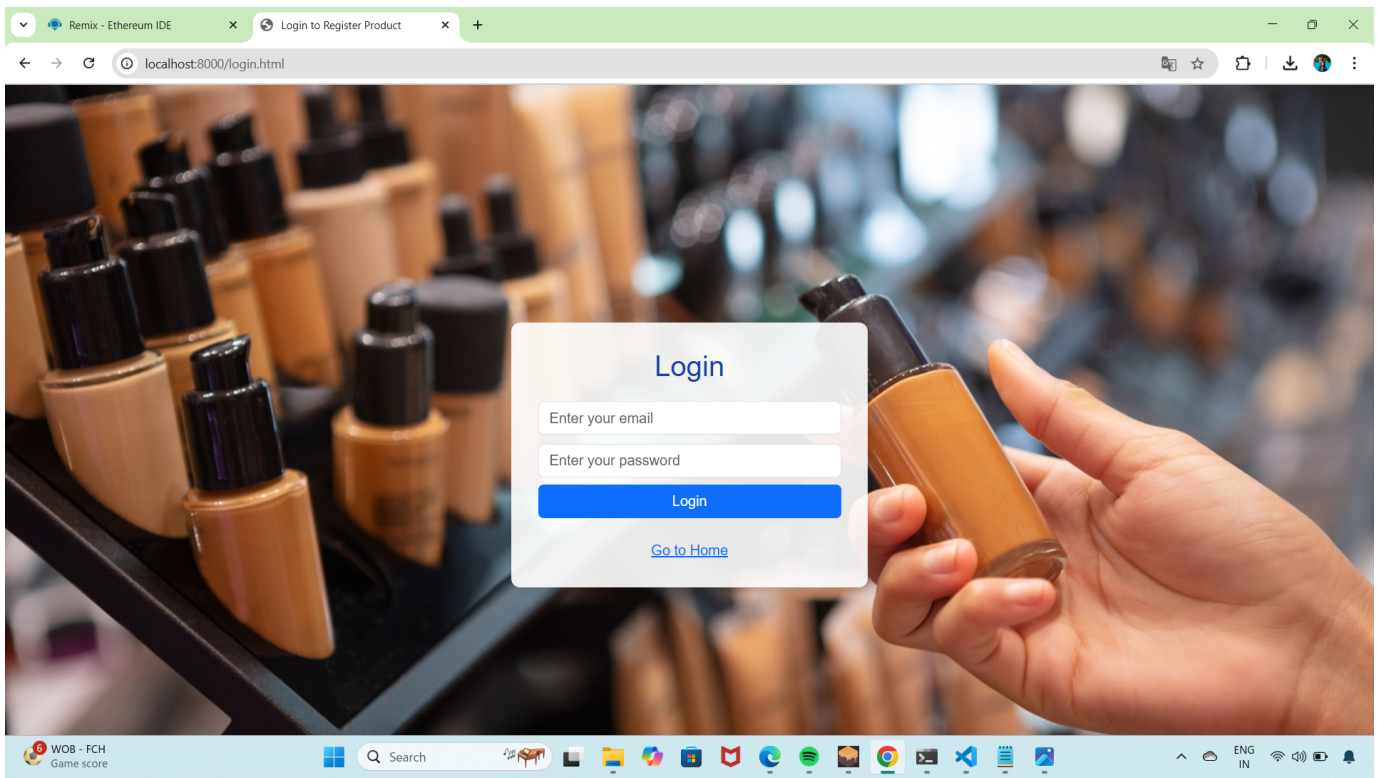


Fig. 9.2: Login Page for registering products

9.3 Registration Page

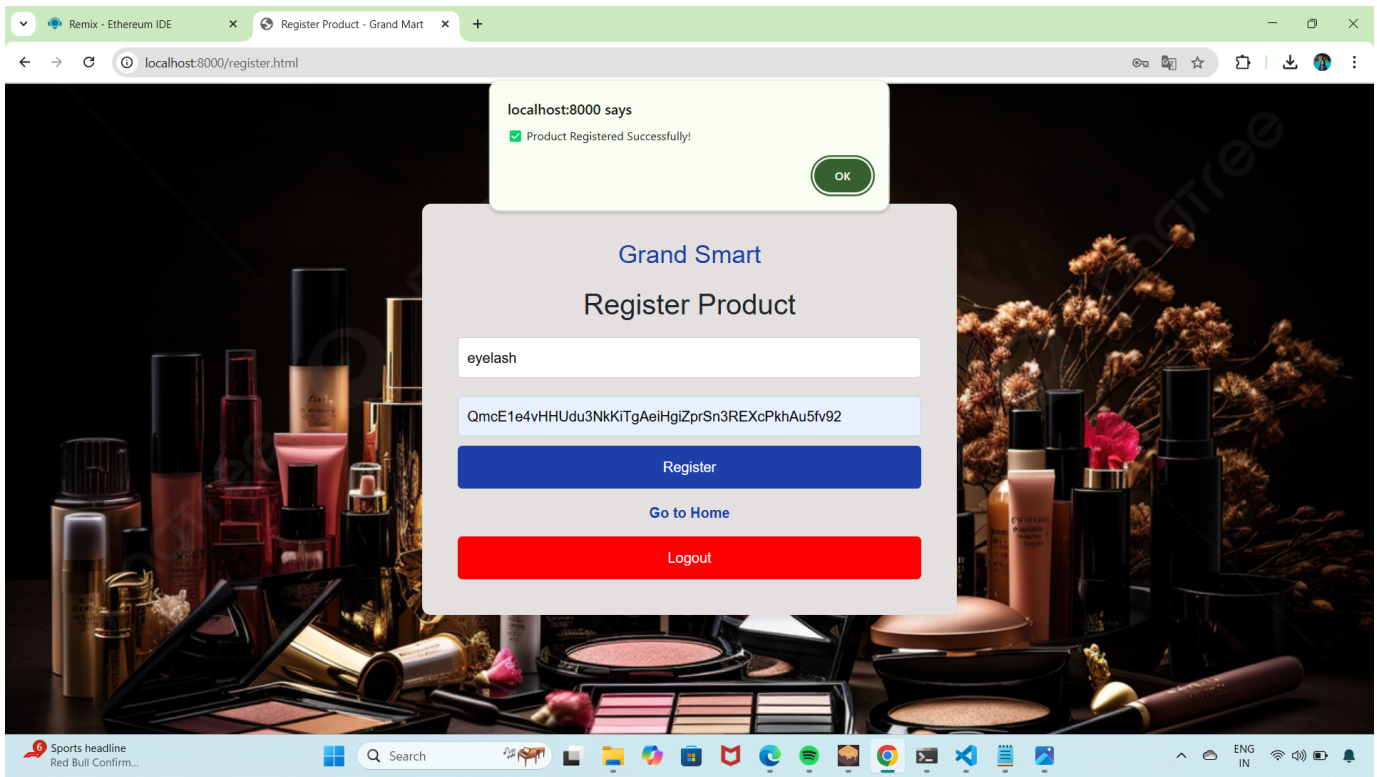


Fig. 9.3: Registering Product

9.4 Verification Page

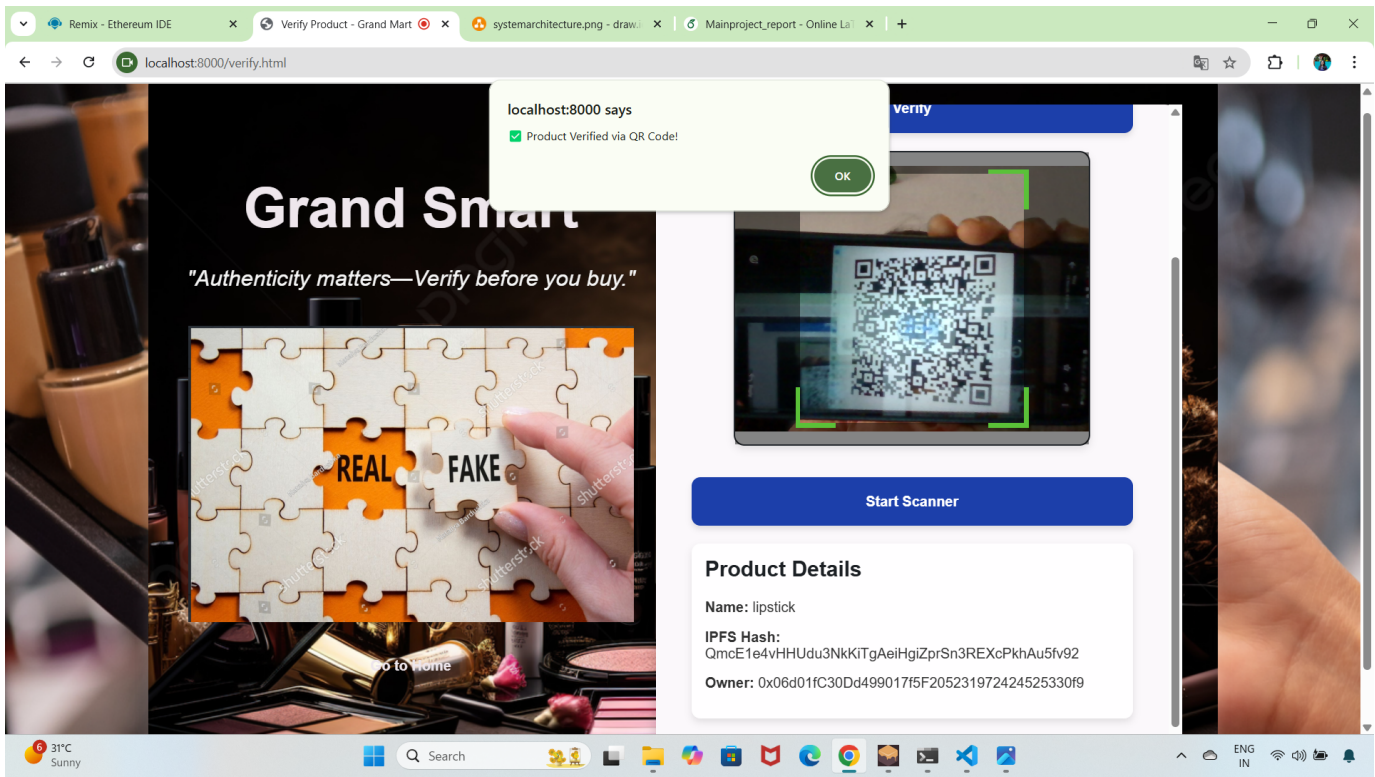


Fig. 9.4: Product verified by users

Chapter 10

SAMPLE CODES

10.1 Smart contract code

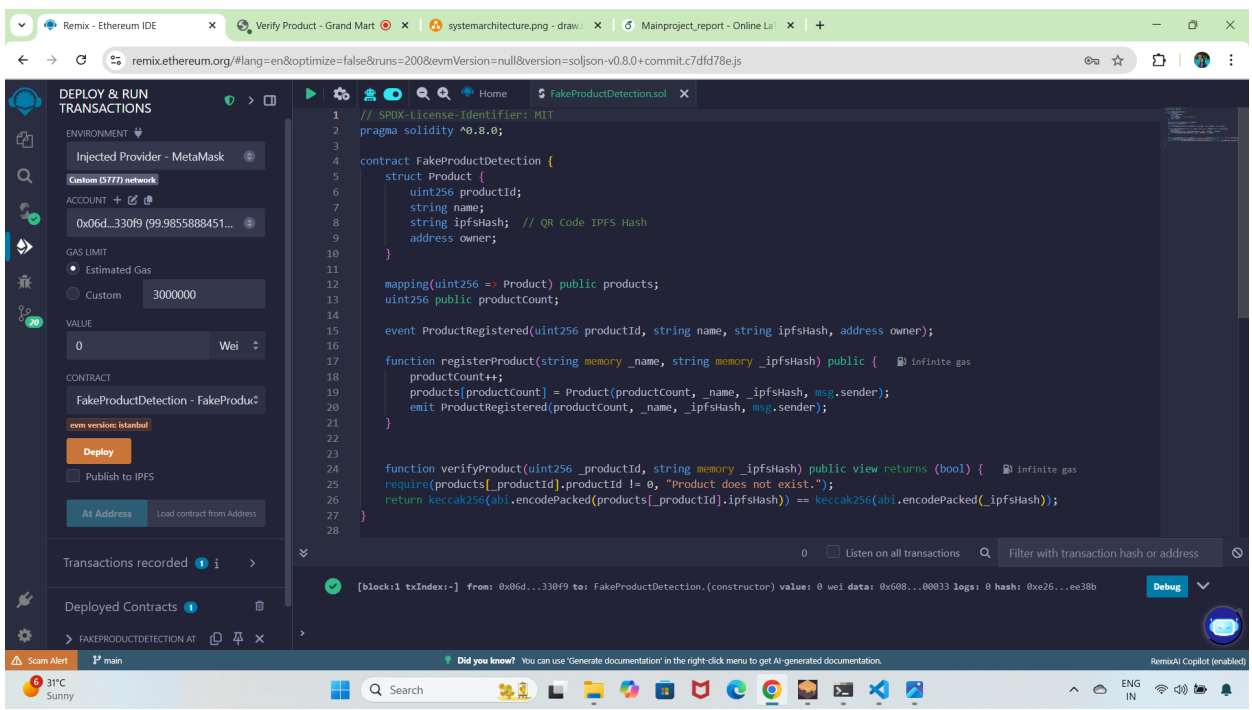


Fig. 10.1: Smart contract code run on remix IDE

10.2 Transaction in Ethereum

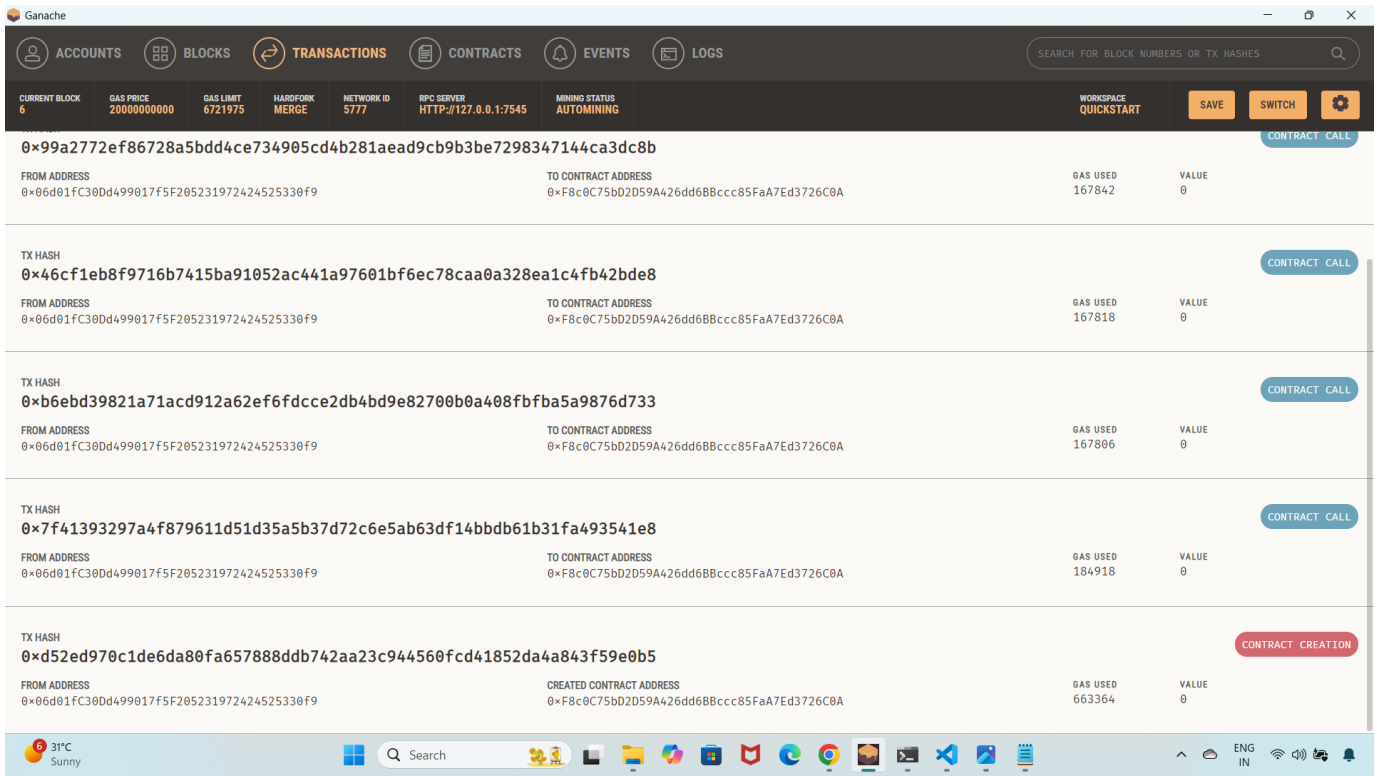


Fig. 10.2: Each transaction generate different hash values

10.3 Metamask connection

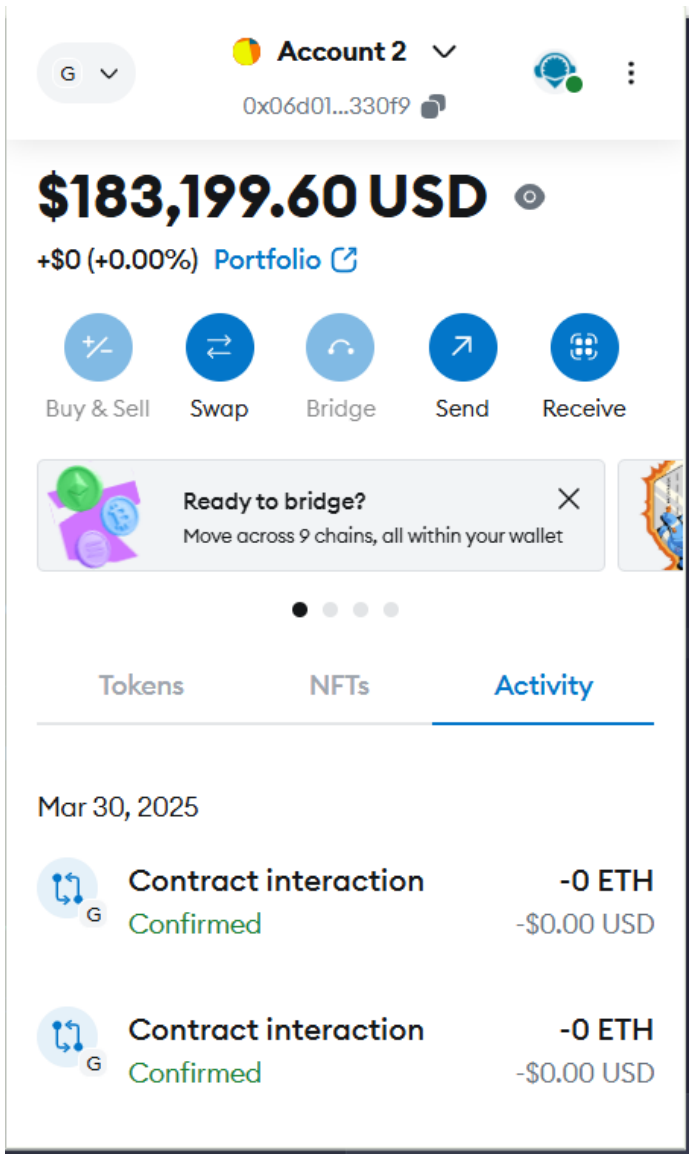


Fig. 10.3: Contract interaction

10.4 Connection code

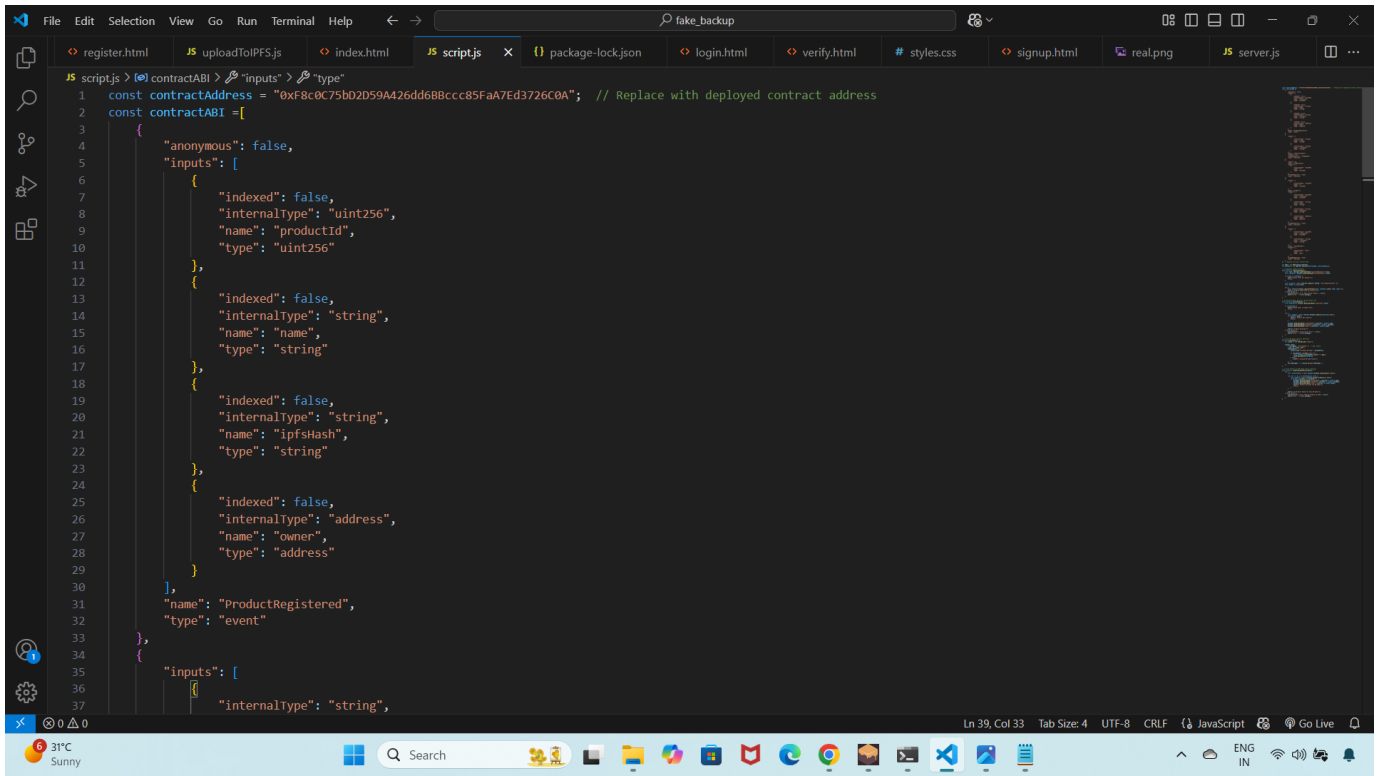


Fig. 10.4: Connection between blockchain and interface by using this code

Chapter 11

SCOPE OF FUTURE WORK

While the current system provides a strong foundation for counterfeit detection, there remains significant potential to enhance its capabilities in terms of scalability, automation, and industry-specific adaptability. The following directions are proposed for future improvements:

- **AI-Based Anomaly Detection:** Machine learning models can be integrated to automatically analyze verification data and identify suspicious or irregular patterns indicating potential fraud.
- **IoT and Smart Packaging Integration:** Smart packaging, embedded with IoT sensors, can provide real-time product tracking and environmental monitoring throughout the supply chain.
- **Real-Time Supply Chain Monitoring:** By linking the system with supply chain management platforms, businesses can achieve end-to-end transparency, from manufacturing to consumer delivery.
- **Decentralized Identity Management (DID):** Enabling verified entities (manufacturers, distributors, and retailers) to register their identity on the blockchain adds an additional layer of security, ensuring only authorized parties can register products.
- **Cross-Industry Expansion:** The system can be adapted to meet the specific needs of other

critical industries such as healthcare, automotive parts, luxury fashion, and electronics, where verifying authenticity is vital.

By implementing these enhancements, the system can evolve into a comprehensive, multi-functional platform for counterfeit detection and supply chain transparency. Future work should also explore user interface improvements, blockchain scalability solutions, and compatibility with global logistics standards to increase adoption across diverse industries.

Chapter 12

CONCLUSION

The project titled Blockchain-Based Fake Product Detection Using Watermarked QR Codes introduces a secure and transparent framework to combat counterfeit products. Conventional verification systems are often limited by centralized architectures, lack of transparency, and susceptibility to tampering. To overcome these limitations, this project utilizes blockchain technology for decentralized record-keeping, combined with watermarked QR codes for secure product tagging.

Through this system, manufacturers can register product information on a blockchain, ensuring immutability and traceability. Consumers, in turn, can authenticate products by scanning a QR code embedded with a unique watermark. The unchangeable nature of blockchain records, along with the visual security offered by watermarking, makes the system highly resistant to fraud and duplication.

The prototype demonstrates effective application in high-risk industries such as pharmaceuticals, luxury goods, electronics, and agriculture, where counterfeit products can cause serious harm. The approach builds trust among consumers, reduces financial losses, and enhances the integrity of the supply chain. Ultimately, the project highlights the practical advantages of combining blockchain with watermarking techniques for real-world counterfeit detection.

References

[1] S. Gupta, A. Sarabu, R. Kuchipudi, M. Sohail, and K. Singh, "Fake product identification for small and medium firms (fpismf) using blockchain technology," *Measurement Sensors*, 2023.

[2] K. Patel, M. Sonker, A. K. Srivastava, and D. J. Srivastava, "Fake product detection system using blockchain," *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 5, no. 4, pp. 1041–1044, 2023.

[3] M. Mhatre, H. Kashid, T. Jain, and P. Chavan, "Bcpis: Blockchain-based counterfeit product identification system," *Journal of Applied Security Research*, 2022. [Online]. Available: https://doi.org/10.1080/19361610.2022.2086784

[4] T. Shreekumar, P. Mittal, S. Sharma, R. N. Kamath, S. Rajesh, and B. N. Ganapathy, "Fake product detection using blockchain technology," *Journal of Algebraic Statistics*, vol. 13, no. 3, pp. 2815–2821, 2022. [Online]. Available: https://publishoa.com

[5] K. Wasnik, I. Sondawle, R. Wani, and N. Pulgam, "Blockchain for counterfeit detection," in *ITM Web of Conferences*, vol. 44, 2022, p. 03015.

[6] A. Bali, A. Singh, and S. Gupta, "Fake product detection system using blockchain," *Algebraic Statistics*, 2022.

[7] P. Lavanya, N. Ananthi, K. Kurnaran, M. Abinaya, B. Kalaivani, and V. Krithika, "Fake product detection using blockchain," in *IEEE Conference*, 2024.

[8] M. Jayaprasanna, V. Soundharya, M. Suhana, and S. Sujatha, "A blockchain based management system for detecting counterfeit product in supply chain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, 2021, pp. 253–257.

[9] M. A. K. Azrag, S. K. Shareef, J. Ann, and M. Suraya, "A novel blockchain-based framework for enhancing supply chain management," *International Journal of Computer Engineering Research Trends*, vol. 10, no. 6, pp. 22–28, 2023.

[10] J. Davies and Y. Wang, "Physically unclonable functions (pufs): A new frontier in supply chain product and asset tracking," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 116–125, June 2021.

[11] S. Mthethwa, N. Dlamini, and G. Barbour, "Proposing a blockchain-based solution to verify the integrity of hardcopy documents," in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, Mon Tresor, Mauritius, 2018, pp. 1–5.

[12] N. Agrawal, H. Kushwaha, S. Shetty, and V. Lobo, "A system to detect fake products using blockchain technology," in *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2022, pp. 874–878.

[13] G. Lakshmi, S. Gogulamudi, B. Nagaeswari, and S. Reehana, "Blockchain-based inventory management by qr code using opencv," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2021, pp. 1–6.

[14] V. B. Ali, Y. Zhang, and M. Bhavsingh, "A blockchain-based framework for enhancing privacy and security in online transactions," *International Journal of Computer Engineering Research Trends*, vol. 10, no. 11, pp. 1–9, 2023.

[15] B. Pretty, "Online ticket booking using secure qr code," *International Journal of Research in Engineering Science and Management*, vol. 1, no. 12, December 2018.