iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69592

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Chain Thread: Blockchain-Powered Product Verification and Authenticity Tracking

Anshul Singh[1], Aryan Shenoy[2], Nihar Thanekar[3]
B.Tech Student, Department of Computer Engineering, K J Somaiya School of Engineering

Abstract: ***Fake Product Identification through Blockchain is a decentralized application (dApp) designed to combat counterfeit goods by providing a transparent, secure, and efficient product verification system. The platform integrates Blockchain technology with QR Codes and NFC (Near Field Communication) tags, ensuring product authenticity from registration to verification.***

The system allows manufacturers to register products on the blockchain, associating each product with a unique identifier (serial number) linked to a QR code or NFC tag. Sellers and consumers can then scan the product's code using the dApp to verify its authenticity in real-time, accessing the product's complete history stored on the blockchain. By utilizing MetaMask for secure user authentication, the platform ensures that only authorized users can participate in product registration, ownership transfers, and verification.

The application is powered by advanced smart contracts on the Ethereum blockchain, which manage product registration, ownership transfer, and validation. The system applies prompt engineering and blockchain storage to ensure product data is immutable and tamper-proof. The architecture leverages the Ethereum network for decentralized storage, ensuring transparency and security at every stage of the product lifecycle.

A case study showcasing a product verification scenario demonstrates the ease of use for consumers and sellers alike, enhancing trust in product authenticity and streamlining the buying process. This paper outlines the system's design, blockchain integration, and real-world applications, highlighting the impact of combining NFC/QR technology with blockchain to ensure secure, transparent product verification.

Keywords: Blockchain, QR Code, NFC, Smart Contracts, Product Verification, Decentralized Application, Authentication, Ethereum

I. INTRODUCTION

Choosing the right product can be a challenging task for consumers, especially when faced with the risk of purchasing counterfeit goods. In industries such as fashion, electronics, and pharmaceuticals, counterfeit products are a significant problem that undermines consumer trust and damages brands. Traditional product authentication methods, including physical verification and centralized databases, are often inadequate and prone to tampering. The rise of blockchain technology has presented an opportunity to revolutionize product verification by providing a decentralized, transparent, and secure way to track product information from manufacturer to consumer.

In this context, Fake Product Identification through Blockchain was developed as a decentralized solution to tackle the growing issue of counterfeiting. The platform integrates blockchain technology, QR codes, and NFC (Near Field Communication) tags to enable real-time product verification at every stage of the product lifecycle. The system allows manufacturers to register products on the blockchain, where each product is linked to a unique identifier and stored in an immutable, transparent ledger. Sellers and consumers can easily scan the product’s QR code or NFC tag to verify its authenticity, ensuring that only genuine products are circulated in the market.

The system is powered by Ethereum’s blockchain, leveraging smart contracts to manage product registration, ownership transfer, and verification. These smart contracts ensure the data integrity of product records while enabling secure and seamless interactions among stakeholders. By combining blockchain, NFC/QR technology, and smart contracts, the platform offers a comprehensive solution to product authentication, reducing the risks associated with counterfeit goods and building consumer trust.

This paper presents the architecture and design of the Fake Product Identification system, focusing on its core components, including product registration, verification, and blockchain integration. Section II provides an overview of the system architecture, detailing the interactions between manufacturers, sellers, and consumers.

©IJRASET: All Rights are Reserved

Section III presents a case study demonstrating the use of the platform for product verification and authentication. Section IV discusses the potential impact of the system on global supply chains and consumer confidence, along with current limitations and future directions for enhancement.

II. METHODOLOGY

A. *System Architecture:*

The Fake Product Identification system utilizes a multi-layered architecture to ensure secure and transparent product verification from the manufacturer to the consumer. The system is divided into three main layers: the user input layer for capturing product data and user interactions, the blockchain layer for secure storage and verification of product data, and the interface layer that facilitates real-time communication between the user and the blockchain. Figure 1 illustrates the high-level architecture of the system.

When a manufacturer begins using the platform, they input product information such as product serial numbers, brand, price, and manufacturer details. This information is passed to the blockchain layer, where it is stored securely using Ethereum smart contracts. The interface layer enables the manufacturer to generate a unique QR code or NFC tag for the product, which is linked to the blockchain. Sellers and consumers can then scan the product's QR code or NFC tag to verify its authenticity using the dApp interface, which retrieves the relevant product data from the blockchain.

This data flow ensures the integrity and transparency of the product information. MetaMask is used for secure authentication, ensuring only authorized users can register or verify products. MongoDB is used for storing off-chain product details such as metadata and user interactions. The blockchain handles on-chain data, ensuring that the product's authenticity remains verifiable in real time.

B. *AI-Driven Product Verification Engine:*

At the core of the Fake Product Identification system is the blockchain, which acts as a transparent and immutable ledger to track and verify product details. The system's functionality is powered by smart contracts deployed on the Ethereum network, ensuring secure product registration and ownership transfer. The blockchain stores essential product information, and whenever a QR code or NFC tag is scanned, the corresponding product data is retrieved from the blockchain.

C. *Product Registration (Powered by Smart Contracts):*

In the product registration process, the manufacturer enters relevant product details into the dApp. The information is processed and stored on the Ethereum blockchain via smart contracts. These contracts validate and record product data, ensuring that the product's information remains immutable and secure.

D. *Product Verification (Powered by Blockchain):*

Once the product has been registered, sellers and consumers can scan the product's QR code or NFC tag using the dApp interface. This action triggers a query to the blockchain, where the product's data is retrieved. The dApp then displays the verification status, confirming whether the product is authentic or counterfeit. This ensures that the consumer can verify the product's authenticity at any point in the supply chain.

E. *Blockchain Integration and Smart Contracts:*

Smart contracts on the Ethereum blockchain ensure that product data cannot be tampered with. When a product is registered, the smart contract verifies and stores the product's serial number, manufacturer details, and other relevant information on the blockchain. Ownership of the product is tracked through the smart contract, and each transaction (e.g., selling the product to a seller or consumer) is recorded on the blockchain, ensuring a transparent and secure ownership history.

F. *Personalization:*

Personalization is achieved by dynamically linking product data with the user's interaction. When a consumer scans the product's QR code or NFC tag, the system provides tailored information based on the product's history and the user's interactions. For instance, a seller might see different data than a consumer, depending on their role in the transaction process.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Similarly, the system ensures that each QR code is linked to a unique product on the blockchain, providing a secure and transparent verification process for both sellers and consumers.

G. User Interface and Blockchain Interaction:

The user interface (UI) is built to be responsive and simple to use. Users can easily register products, generate QR codes, and verify product authenticity through the platform. The system is built with a clean frontend using React for seamless user interactions. The backend, powered by Node.js and Express, handles API requests for product registration, verification, and smart contract interactions on the Ethereum network.

The MetaMask integration ensures secure user authentication, and MongoDB handles off-chain data storage for product metadata. The dApp connects to the Ethereum blockchain using web3.js to interact with smart contracts for product verification.

H. No UI-Specific Assumptions:

While the system is built with a clean, responsive frontend using React, Tailwind CSS, and Framer Motion, this paper focuses on the system architecture and the blockchain integration for product verification. The UI design itself is flexible and can be adapted to different platforms, ensuring that the core functionality of product registration and verification remains unaffected by the interface.

In summary, the Fake Product Identification system combines blockchain technology, smart contracts, and QR/NFC technology to offer a secure, decentralized method for verifying product authenticity. The architecture ensures that all product data is securely stored on the blockchain, providing an immutable and transparent record that can be accessed in real-time by consumers and sellers. This system improves the reliability of product verification and combats the issue of counterfeit goods in global supply chains.

III. RESULTS AND DISCUSSION

In this section, we demonstrate the capabilities of the Fake Product Identification system through a representative use case scenario, showcasing how the blockchain-driven product verification process works in real-world applications. The example user in this case study is a consumer who has scanned the QR code of a product they purchased online. Their goal is to verify the authenticity of the product and ensure it hasn't been tampered with. The results are broken down into the following subcomponents for clarity.

A. Product Registration and Blockchain Verification

Upon scanning the QR code linked to the product, the system retrieves the product details from the blockchain, where the manufacturer initially registered the product. The blockchain ensures that the product's data—such as its serial number, manufacturing details and it cannot be altered or tampered with, offering the consumer a transparent and trustworthy verification process.

Example User Data**:**

- Product Details:
  - Brand: XYZ
  - Serial Number: 12345XYZ
  - Date of Manufacture: 2023-04-01
- Consumer's Action: Scan the QR code using the Fake Product Identification dApp.

System Response:

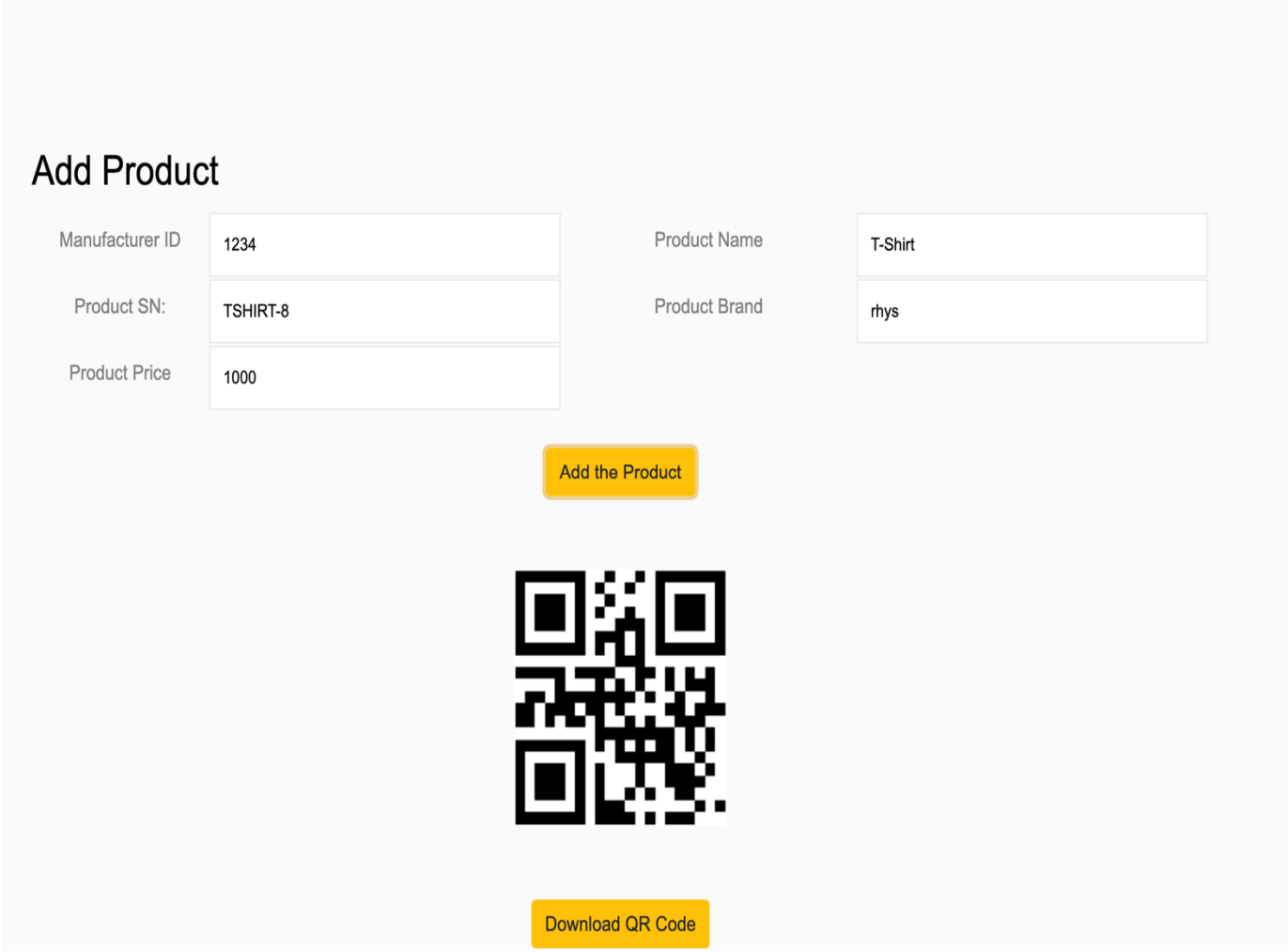
The system retrieves the product's registration information from the Ethereum blockchain and verifies its authenticity in real-time. The consumer is presented with clear product details, such as manufacturing information, certification status, and the original seller.

Feedback**:**

The system provides the consumer with a reassuring message:

"The product is authentic. It was manufactured by XYZ Company on 2023-04-01 and has been certified for quality assurance. You are purchasing a genuine product."

Figure 1**:**



This figure shows the detailed product information retrieved from the blockchain, including the product's serial number**,** manufacturing date**, and** seller's name**.** The product verification status is marked as "Genuine," confirming the authenticity of the product.

B. User Interface for Verification and Transparency

The user interface of the Fake Product Identification **sy**stem is designed for simplicity and ease of use, displaying clear and concise information on the product's authenticity. Upon scanning the QR code**,** the consumer is presented with a clean and intuitive interface that shows key details about the product, including the original manufacturer**,** product batch, and date of verification**.** This transparency helps increase consumer confidence in their purchase.

Example User Data:

Product Verification: Consumer scans the product's QR code to confirm its authenticity.

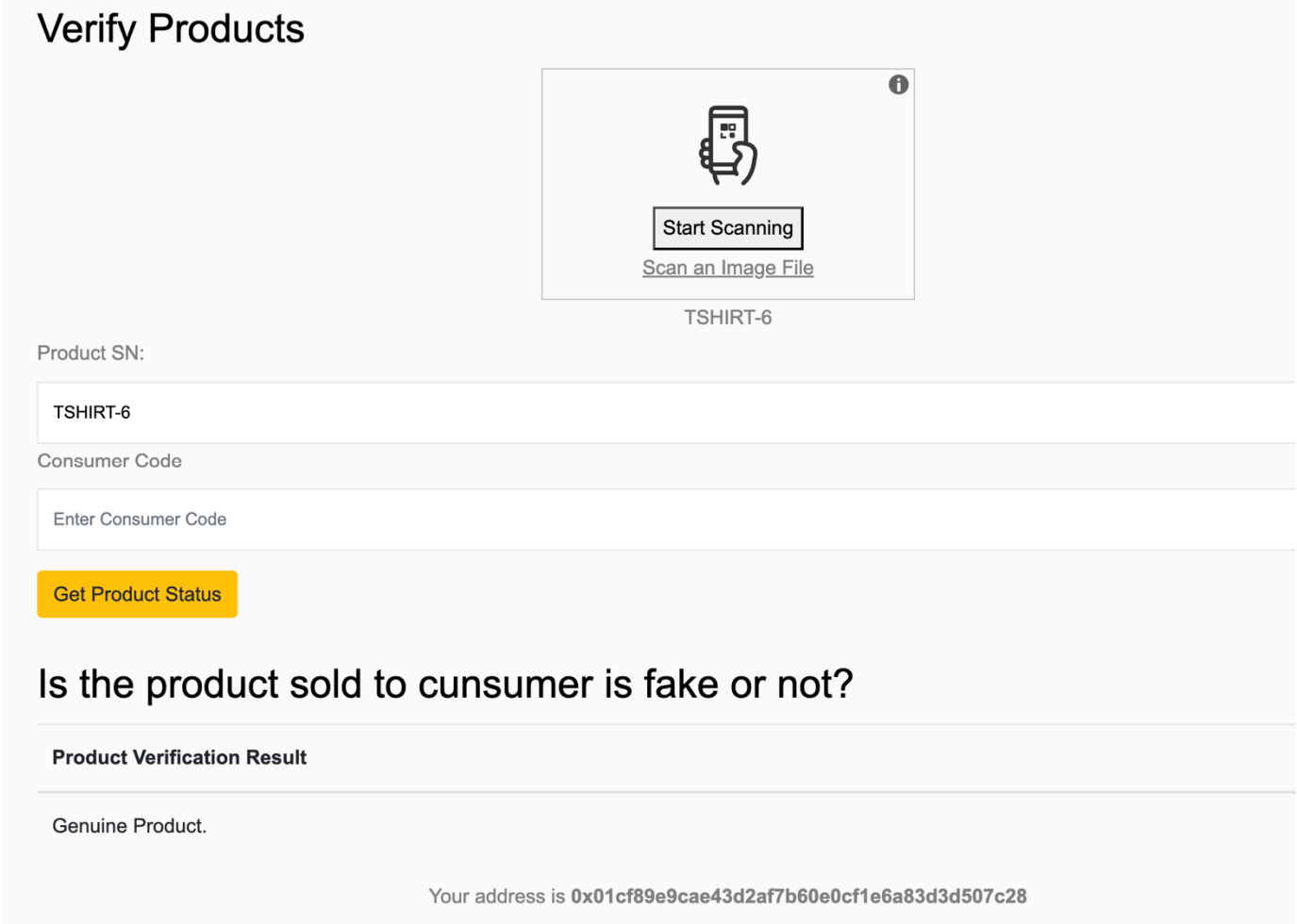
System Output:

The system displays the product's blockchain record, including data about the product's origin and authenticity.

Feedback:

The system's transparency and simplicity in presenting key product details and verification status make it easier for consumers to trust the system and feel confident about their purchase.

Figure 2:



This figure shows the user interface where the product details and verification status are shown, providing the consumer with a simple and clear view of the product's authenticity.

IV. CONCLUSION

In this paper, we presented the Fake Product Identification system, a decentralized platform that leverages blockchain technology, QR codes, and NFC (Near Field Communication) to ensure the authenticity of products across the supply chain. The system utilizes smart contracts on the Ethereum blockchain for secure product registration, ownership tracking, and verification, creating a transparent and tamper-proof ledger. This solution aims to combat the growing issue of counterfeit products and improve consumer trust in product authenticity.

A case study involving a consumer scanning a product's QR code demonstrated the system's effectiveness in providing real-time verification of product authenticity. The blockchain ensured that the product's details were immutable and could be accessed by both sellers and consumers, reducing the risk of counterfeit goods being sold. By combining QR/NFC technology with blockchain, the platform offers a seamless user experience for both manufacturers and consumers while maintaining high standards of security and transparency.

The Fake Product Identification system showcases the potential of blockchain-based product authentication and its ability to bring greater accountability to global supply chains. The system's reliance on smart contracts and blockchain's decentralized nature ensures that product data remains tamper-proof, even in environments where counterfeiting is a serious concern. This approach underscores the growing importance of integrating blockchain technology with consumer goods to protect both buyers and sellers from the risks associated with counterfeit products.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Looking ahead, there are several opportunities for enhancement. Future developments could include integrating real-time data feeds from manufacturers, expanding product verification to include more complex product categories, and incorporating machine learning models for predictive counterfeit detection. Additionally, the system could be further scaled to integrate with global e-commerce platforms, allowing for seamless verification at the point of sale. Ethical considerations, including data privacy and transparency, will also be key as the system evolves and scales.

In conclusion, Fake Product Identification represents a significant advancement in the way we approach product verification, offering a decentralized, transparent, and secure solution to prevent counterfeiting. By combining blockchain technology with NFC/QR code integration, the system enhances the trustworthiness of products and provides a much-needed solution to the pervasive problem of counterfeit goods. The promising results from our initial deployment suggest that blockchain can play a pivotal role in ensuring product authenticity across industries, ultimately benefiting both consumers and manufacturers.

V. ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to Prof. Shweta Chachra for their invaluable guidance, insightful feedback, and unwavering support throughout the course of this project. Their expertise and encouragement were instrumental in shaping the direction and success of this research.

We also extend our heartfelt thanks to the faculty and staff of the COMPS department for their continuous support and constructive advice. Their shared knowledge and dedication to excellence have inspired us throughout the development of the project.

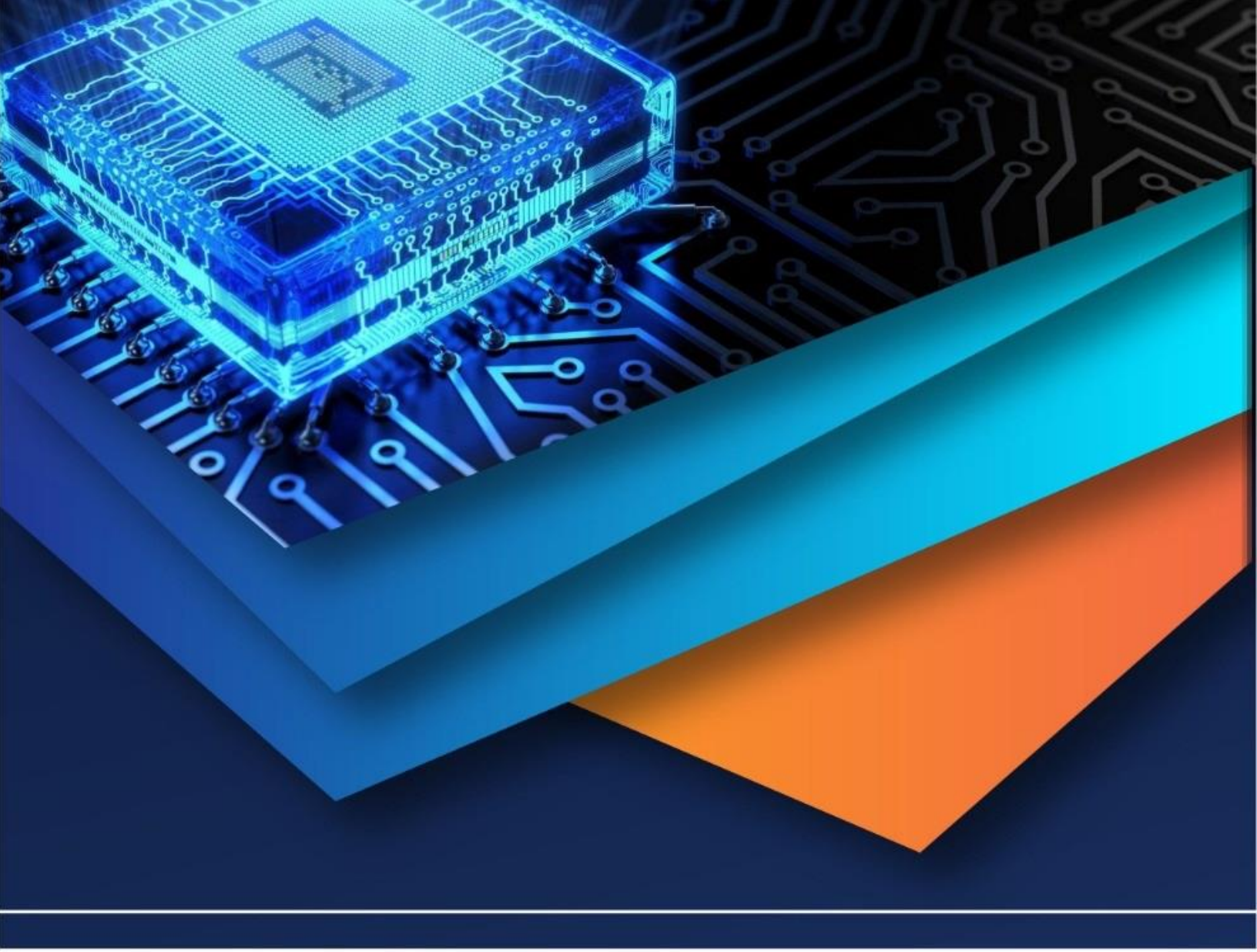
A special thanks to our colleagues and friends, whose collaboration and constructive critiques helped refine the project. Their camaraderie and insightful discussions were essential in overcoming challenges.

Finally, we would like to express our deepest gratitude to our families for their endless love, patience, and understanding. Their belief in our abilities and their unwavering support provided the foundation upon which this research was built. Without their encouragement, this project would not have been possible.

REFERENCES

[1] Ethereum Foundation, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” [Online]. Available: https://ethereum.org/en/whitepaper/, 2014.
[2] D. Wood, “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” Ethereum Project Yellow Paper, 2014.
[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” [Online]. Available: https://bitcoin.org/bitcoin.pdf, 2008.
[4] A. M. Turing, “Computing Machinery and Intelligence,” in Mind, vol. 59, no. 236, pp. 433–460, 1950.
[5] S. Nakamoto, “Bitcoin: The Cryptocurrency Revolution and the Future of Blockchain Technology,” in Proc. 2023 Int. Conf. on Blockchain Technologies, pp. 12–18, 2023.
[6] A. K. Jain, “Blockchains and Their Applications in E-Commerce,” in Proc. 2023 IEEE Int. Conf. on Digital Transactions and Commerce, pp. 101–106, 2023.
[7] L. Brown, R. Chhabra, and G. DeBenedetti, “Securing Product Authenticity: Blockchain’s Role in Preventing Counterfeit Goods,” in Proc. 2022 IEEE Conf. on Cybersecurity and Privacy in E-Commerce, pp. 90–95, 2022.
[8] P. Singh, R. K. Gupta, and N. Sharma, “Decentralized Applications: Architecture, Use Cases, and Future,” in Proc. 2023 IEEE Conf. on Blockchain and Distributed Systems, pp. 105–110, 2023.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)