Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21558780

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Review Article

Volume-06|Issue-04|2026

Ethereum-Backed Blockchain and Cryptocurrency Integration for Advanced Anti-Counterfeiting Measures in Supply Chains

Reshma DSouza[1], Sheela S[2], Sameena H S[3], Jyothi S[4], Padmaja R[5], K V Vaishnavi[6]

[1,3,4,5,6]Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India.
[2]School of CSE, RV University, Bengaluru, Karnataka, India.

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
D'Souza, R., Sheela, S., Sameena, H. S. & Jyothi, S., Padmaja, R., Vaishnavi, K. V. (2026). Ethereum-Backed Blockchain and Cryptocurrency Integration for Advanced Anti-Counterfeiting Measures in Supply Chains. *Indiana Journal of Multidisciplinary Research, 6*(4), 36-44.

Abstract: In this era where technology is used to create unidentical counterfeit products, Finding the original objects is a very tedious task for the users. These Counterfeit Products affect the health of the user in the case of medical and skin care products also. This project implements Blockchain, a new Technology which is used to overcome this problem. Blockchain technology is the distributed, and immutable technology that provides data consistency and security. Here a QR code is generated for each product that is linked to the database which in turn is mapped to the chain nodes. By scanning this QR code the user can detect the original products amongst the fake ones. It highlights the need of cryptocurrency in the broader vision of supply chain security, elaborating on how Blockchain network, particularly using Ethereum Framework, provides a decentralized and transparent ledger for tracking and validating products.

Keywords: Counterfeit, QR code, Blockchain, Ethereum, ledger

INTRODUCTION

Counterfeiting occurs when suppliers are selling goods pretending like some other items. Counterfeit goods have a poor impact on the economy, citizens, and electronics. Poor quality cosmetics may lead to skin problems and fake electronic equipment's can cause flaws and mishaps. To address this, solutions must be found for the sale of counterfeit products. This has a negative effect on a company's reputation, as customers are often unaware that the object they are holding is a fake one. This can lead to customers demanding compensation, as a refund or a brand new item. Companies are caught between trying to overcome delay and effort handling with inadequate replication of their products parallelly keeping their users satisfied.

The problem led by malicious manufacturers decreases users' association, as distributors, retailers, and other business partners lose faith in legitimate enterprises. This work presents a system designed for the identification of counterfeit products implementing blockchain technology to provide the customers and the suppliers for holding the ability to track the supply chain of the item in safe surroundings. Blockchain is a distributed system that guarantees that each new block appended to the blockchain is the only accurate version accepted by every node. It is used for maintaining a regular document as a genuine database through distributed system. It aims to fix the complication of counterfeiting brands and provide an opportunity to verify the integrity of a product using smart contracts.

Blockchain Methodology is a decentralized framework that enables secure and transparent transactions. It uses a distributed ledger across a network of computers, reducing the need for a centralized authority. Cryptography and Hash Functions ensure the security of transactions, making them tamper-resistant. Once block including transaction details is added to a Blockchain, information on it is difficult to alter. Smart contracts, coded agreements, automate and enforce contract terms on platforms like Ethereum. Transactions are visible to all participants, enforcing transparency and accountability. Blockchain has applications in cryptocurrencies, supply chain management, healthcare, government related applications and more.

Smart contracts are self-executing contracts in terms of the agreement directly written as code statements based on the agreement mechanisms or in other words consensus mechanisms. These contracts run on Blockchain framework and automatically enforce and execute the terms of the contract when some predefined conditions are fulfilled. Smart contracts help remove the need for mediators, reduce the risk of fraud, and increase the efficiency of transactions.

***Corresponding Author:** Reshma D'Souza

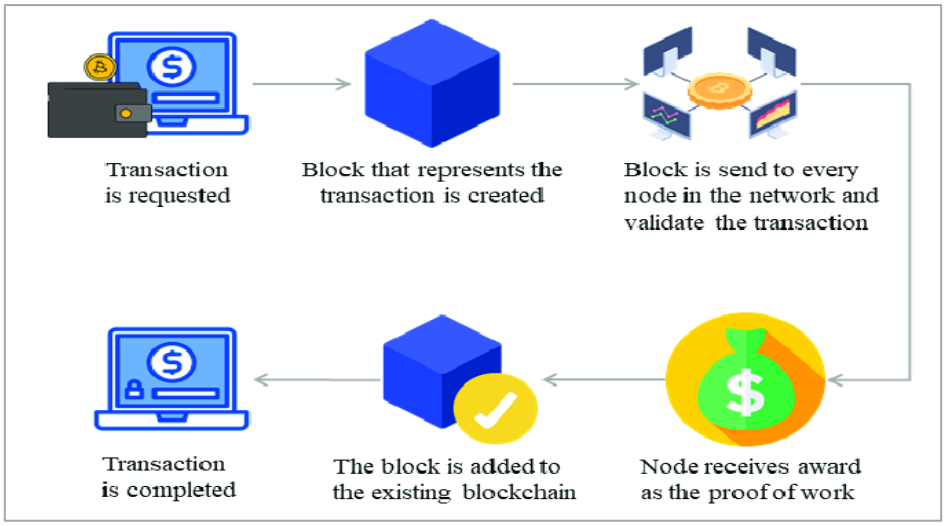

Fig 1. Blockchain System

LITERATURE SURVEY

In the study by Khalil G. et al. [1], a method for detecting counterfeit goods is introduced, utilizing Radio Frequency Identification (RFID) tags. The approach involves placing RFID tags on products and employing remote sensor networks to assess them for authenticity. RFID technology relies on low-frequency radio waves to collect and store data. This collection of data takes place in environments such as cellular systems or central warehouses. This entire process involves the RFID transceiver scanning radio waves before transmitting them to the RFID tag. Subsequently, the RFID reader sends the collected data to a microchip, which is exceptionally small in size. This methodology presents a novel approach to combat counterfeiting by using RFID technology for authentication and data collection.

In [2], The decentralized application (DApp) using Ethereum Blockchain for simulating a supply chain offers enhanced transparency and security. It ensures the secure transfer and recording of product ownership on the tamper-resistant Ethereum blockchain. Integrating Radio Frequency Identification (RFID) addresses previous security and privacy concerns. Extending the system to E-commerce and retail brings transparency for consumers. Blockchain's immutability guarantees data integrity, and smart contracts automate processes, while decentralization reduces the risk of manipulation. Regular updates and collaboration with the blockchain community are essential for ongoing success.

[3] The paper discusses the application of Blockchain technology, using Bitcoin as an example, to address issues related to product counterfeiting. It emphasizes the decentralized nature of Blockchain, which ensures the legitimacy of transactional records and solves the double-spending problem. The proposed decentralized Blockchain system aims to enable consumers to independently verify the authenticity of products, reducing reliance on merchants. Manufacturers can utilize this system to provide genuine products without the need for direct-operated stores, leading to significant cost savings in product quality assurance. The paper highlights Bitcoin as an example of a Blockchain, emphasizing its consensus mechanism, Proof-of-work (POW) algorithm. In this mechanism, nodes in the network compete using their computing power to solve a complex SHA256 math problem.

[4] This study assessed the level of dissimilarity needed between authentic and counterfeit logotypes to enable accurate counterfeit identification. Participants had to choose if a brand's emblem was an imitation or the real thing as it appeared in the center of the screen. via the "E" or "I" keys on a computer keyboard (key mapping was counterbalanced between participants). Each authentic and fake brand logo was exhibited for a maximum of three seconds, and participants were free to respond at any point after the logo was displayed. To draw focus to the center of the screen before the brand logo appeared, a "" was shown for 700 milliseconds. Each logo from the LLF (low-level fake logo), MLF (mid-level fake logo), and HLF(high-level fake logo) categories was presented once, totaling 60 trials per participant. The logos were presented in random order (12OLs were presented twice). Only after receiving a correct or incorrect response were the participants given the opportunity to move on. Twelve practice trials using real and false versions of the "Ford" and "Google" brand logos were conducted prior to the study's start. The LLF logos, which likewise had the greatest likeness to the original designs, and for which the error rate in logo recognition was the highest, caused the most uncertainty. The study includes Five different types of brand logos (LLF, MLF, HLF, RLF, and OL) and two visual target words ("Fake" and "Real") were employed as the seven visual stimuli.

SYSTEM ARCHITECTURE

System architecture is a conceptual model that defines the structure and behavior of the system. It includes the components of the system and the

***Corresponding Author:** Reshma DSouza

relationship depicting how these components work together to achieve the overall system performance, as shown in Figure.

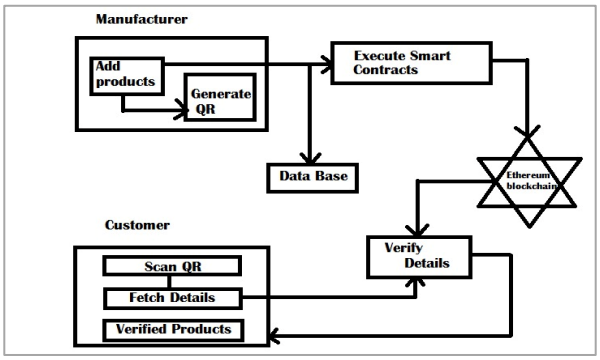

Fig 2. System Architecture

The proposed system involves manufacturers logging into a website to upload product details, generating unique QR codes for products, and pushing this information to the Ethereum Blockchain using Remix Ethereum IDE. Customers scan QR codes, and if the code matches the manufacturer's, the product is deemed original, displaying its details. If not, it's flagged as fake, preventing the purchase of counterfeit goods. Smart contracts, immutable programs on the Blockchain, automate transactions, enabling decentralized execution of agreements without intermediaries. Ganache provides a secure testing environment for decentralized applications and smart contracts. Ethereum, with its cryptocurrency Ether, facilitates deploying decentralized applications and is known for its smart contract capabilities.

USE CASE DIAGRAM

It is used to represent the dynamic behavior of a system. It encapsulates the system's functionality by incorporating use cases, actors, and their relationships.

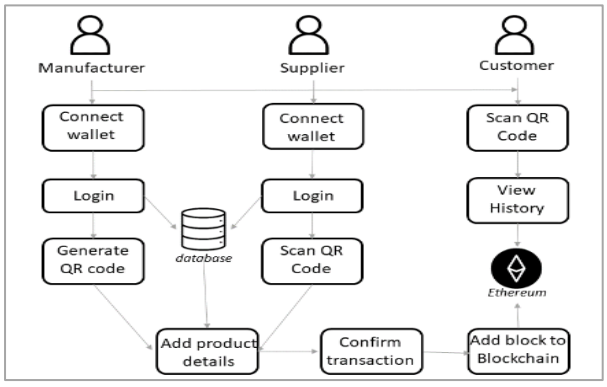

Fig 3. Use Case Diagram

In this system, the manufacturer logs into their account to generate a QR code and input product details. Using their MetaMask wallet, the manufacturer adds a block to the Ethereum blockchain.

The seller, upon scanning the QR code, can access product information entered by the manufacturer and subsequently sell the product, transferring ownership.

Consumers can verify product integrity by scanning the QR code, revealing the transaction history and confirming authenticity. If the product is identified as fake during verification, the consumer becomes aware of potential counterfeiting, as the status indicates a discrepancy in the information. This ensures transparency and helps prevent the purchase of counterfeit goods.

In the case of Fake Products Identification using Blockchain, the use case diagram serves as a visual representation of the different steps required to identify a fake product. The use case diagram starts with a user requesting identification of a product. The system then verifies the product by using a Blockchain to securely store and share data about the product. This data is then compared to the data stored on the Blockchain for the product, and if the data does not match, the product is identified as a fake. Once the product is identified as fake, the user can take appropriate action, such as returning the product or alerting the authorities. The use case diagram can also represent the different activities that can be taken to prevent the sale of fake products in the future, such as using smart contracts to authenticate products before they are sold. This smart contract can be set up to require vendors to provide proof of authenticity before they are allowed to sell a product. Overall, the use case diagram of Fake Products Identification using Blockchain is an important tool for understanding the processes and activities used to identify and prevent the sale of fake products. By understanding the different steps involved, it is possible to create a secure system that can detect and prevent fraud while still allowing legitimate vendors to sell genuine products.

METHODOLOGY

Stage 1: Deploy smart contracts.

In this stage, open Remix Ethereum IDE then compile and run the solidity code. Later QuickStart the Ganache application and copy the RPC address and paste the address in Remix Ethereum IDE by selecting Ganache as the service provider. This is the deployment of smart contracts which is completed by using Remix Ethereum Integrated Development Environment and Ganache application. Languages used to write smart contracts are Solidity.

Stage 2: Connect data to the Blockchain network through Jupyter notebook.

In this stage, we must copy the path of the python file in the project folder, then open the anaconda command prompt change the directory to the copied path. Then open Jupyter notebook via anaconda prompt. Later copy the address generated in Remix Ethereum

***Corresponding Author:** Reshma DSouza

IDE while deploying the smart contracts and paste it in the Jupyter notebook files in place of the address text. This will connect the data to the Ethereum blockchain network via Jupyter notebook.

Stage 3: Run the project in NetBeans.

After connecting data to the Blockchain network by using Jupyter notebook, then run the project in the NetBeans IDE. It will provide a web Interface for the manufactures where the manufactures can login and add the product details. This information will be stored in the database and the QR code will be generated which is unique for every product. Further the product details will be added to the Blockchain network.

Stage 4: Product verification through android application.

In this stage an android application will be provided to the users. Before buying any product, the users can scan the QR code which is attached to the product. After scanning the QR code, if the product is valid and present in Blockchain network then it will display the product details or else it will be displayed as no record found.

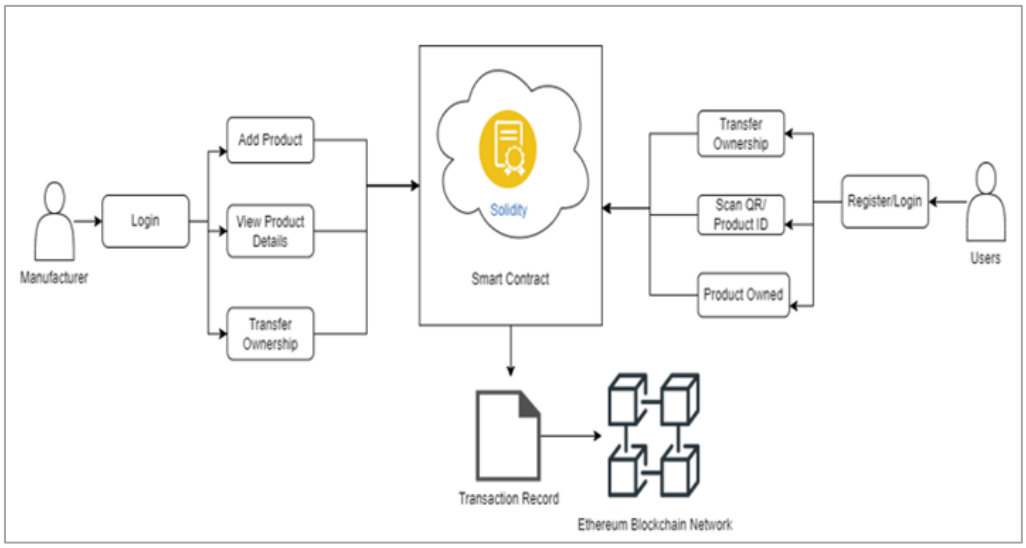

Fig 4. Proposed System Architecture

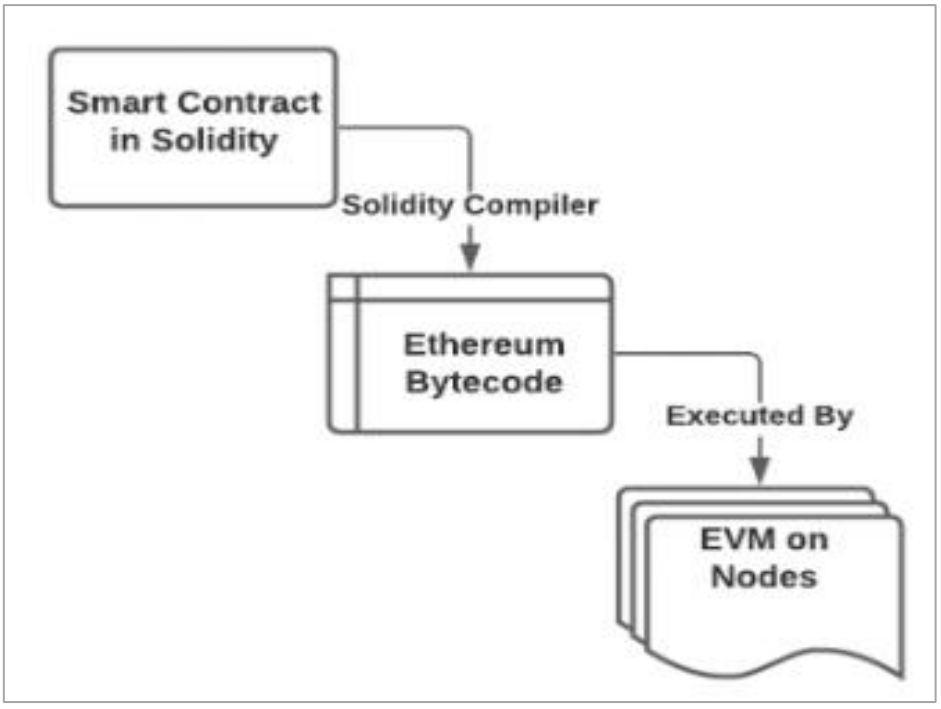

Fig 5. The workflow of Ethereum Smart Contract

***Corresponding Author:** Reshma DSouza

RESULTS

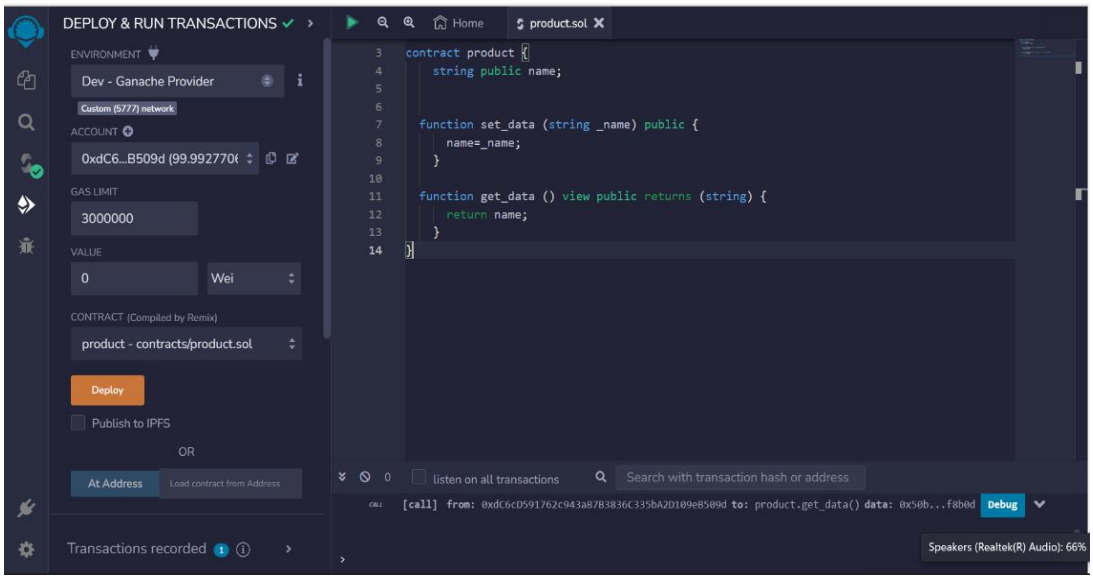

Fig 6. Remix Ethereum IDE to deploy data into Blockchain.

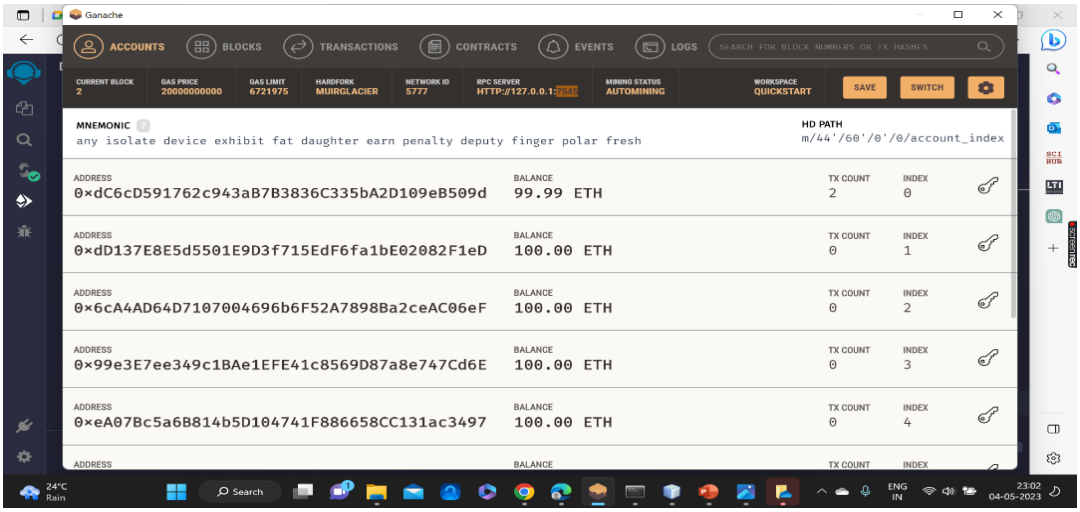

Fig 7. QuickStart of Ganache

```
(base) D:\product_blockchain\Product_Track_Blockchain_py>jupyter notebook
[I 2023-05-04 20:41:15.289 LabApp] JupyterLab extension loaded from C:\Users\ramad\anaconda3\lib\site-packages\jupyterla
b
[I 2023-05-04 20:41:15.290 LabApp] JupyterLab application directory is C:\Users\ramad\anaconda3\share\jupyter\lab
[I 20:41:15.297 NotebookApp] Serving notebooks from local directory: D:\product_blockchain\Product_Track_Blockchain_py
[I 20:41:15.297 NotebookApp] Jupyter Notebook 6.3.0 is running at:
[I 20:41:15.298 NotebookApp] http://localhost:8888/?token=d49f4c204b1fe63e65bc5f9c4d05996919c116ef3fb42e2e
[I 20:41:15.298 NotebookApp]  or http://127.0.0.1:8888/?token=d49f4c204b1fe63e65bc5f9c4d05996919c116ef3fb42e2e
[I 20:41:15.298 NotebookApp] Use Control-C to stop this server and shut down all kernels (twice to skip confirmation).
[C 20:41:15.402 NotebookApp]

    To access the notebook, open this file in a browser:
        file:///C:/Users/ramad/AppData/Roaming/jupyter/runtime/nbserver-19016-open.html
    Or copy and paste one of these URLs:
        http://localhost:8888/?token=d49f4c204b1fe63e65bc5f9c4d05996919c116ef3fb42e2e
     or http://127.0.0.1:8888/?token=d49f4c204b1fe63e65bc5f9c4d05996919c116ef3fb42e2e
[I 20:41:33.803 NotebookApp] Kernel started: 87278d69-2a0d-4ef6-8c4b-eab715a43599, name: python3
[I 20:41:54.646 NotebookApp] Kernel started: b22c7159-6a88-4977-9a5f-754ba052db7a, name: python3
[I 20:43:34.242 NotebookApp] Saving file at /ipfs_download.ipynb
[I 20:43:55.191 NotebookApp] Saving file at /upload.ipynb
[I 20:45:55.209 NotebookApp] Saving file at /upload.ipynb
```

Fig 8. Anaconda Prompt

***Corresponding Author:** Reshma DSouza

With the help of frontend part of manufacturer, manufacturer can register the product with the product information. After product was added to Block Chain, manufacturer would be able to generate and download the QR code given the product information. Manufacture also can attach the QR code.

Transaction Cost	Execution Cost	Input	Decoded Input	Decoded Output
308771	308771	0x448...00000	"3421SAfewe", "Balenciaga Triple S", "23", "14 January 2020", "15", "16 January 2020", "20 January 2020", "seller 1", "Balenciaga Limited "	"Product Registration Successful"

Table 1: Product Registration

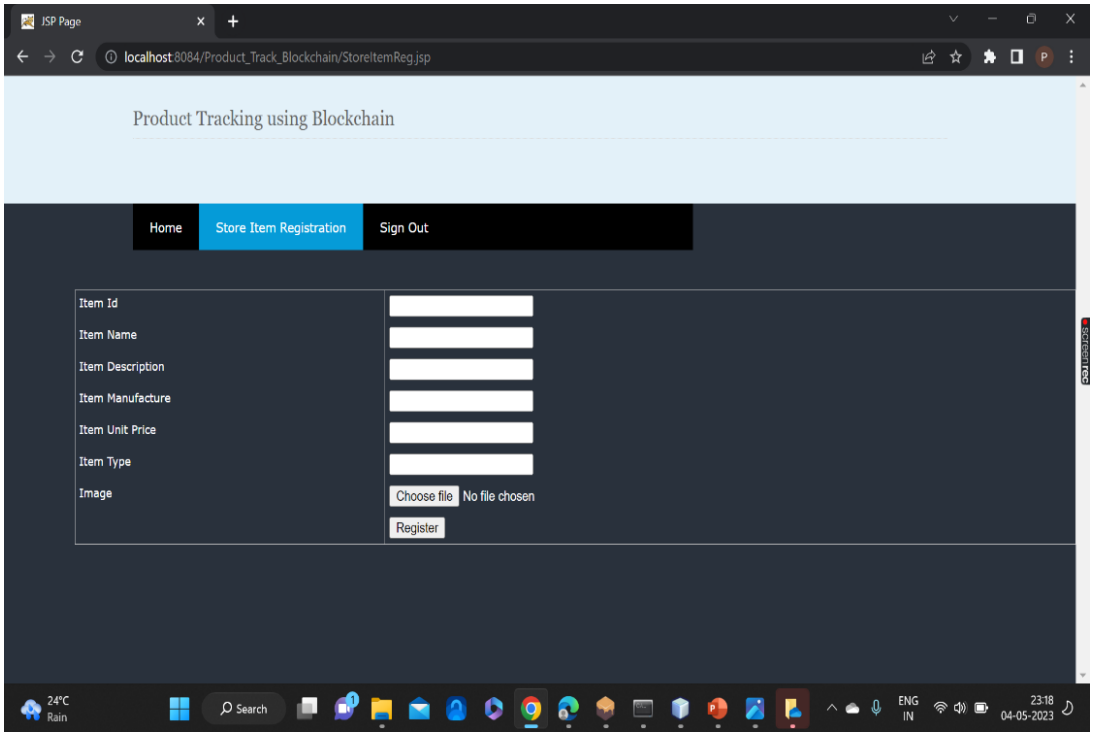

Fig 9. Adding product details.

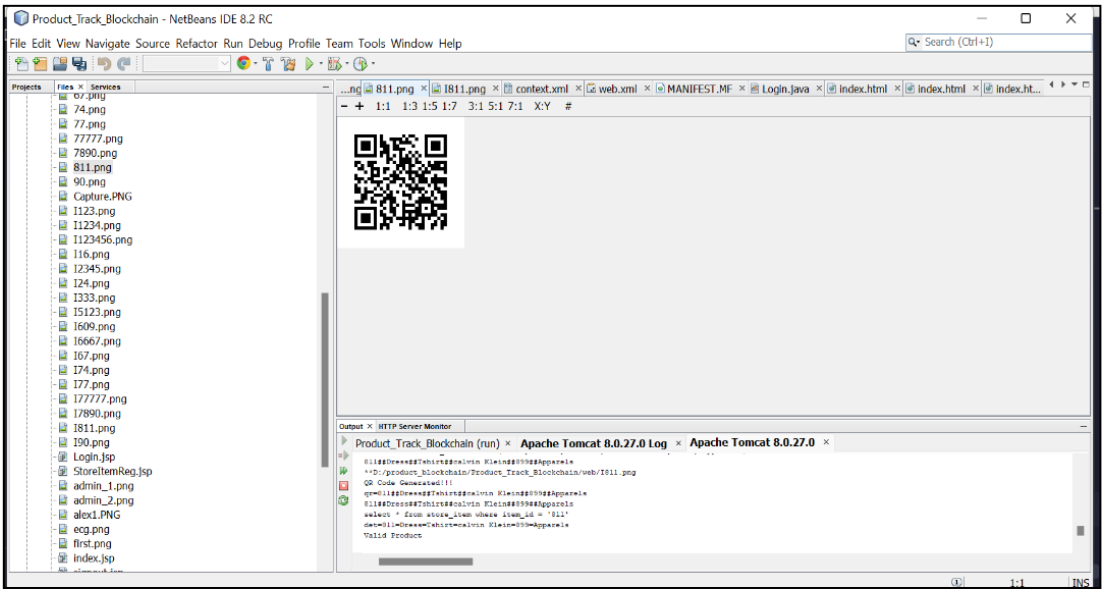

Fig 10. Generated QR Code

***Corresponding Author:** Reshma DSouza

Fig11. Product verification by the customer.

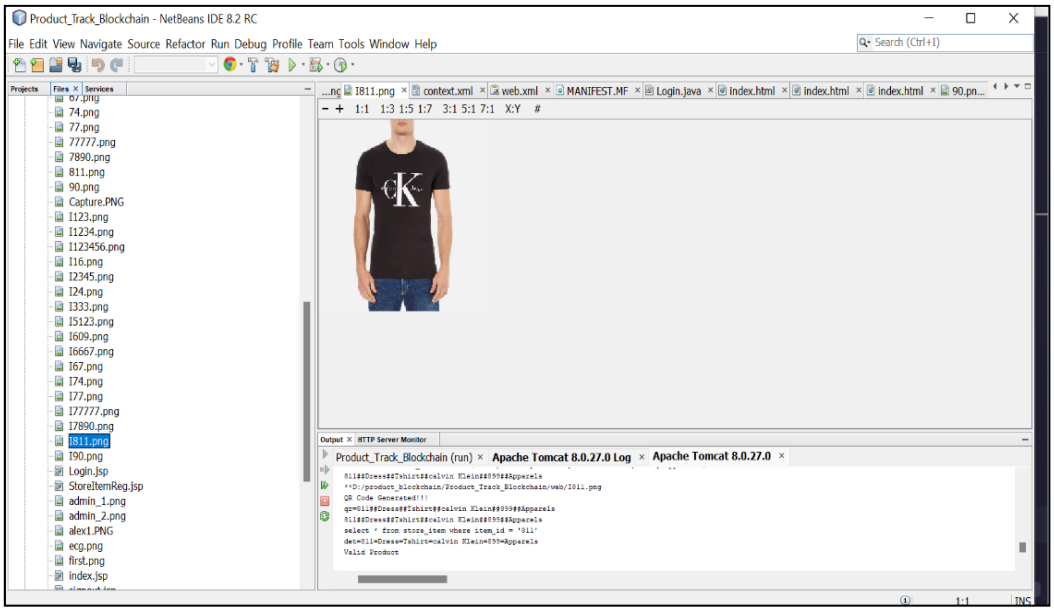

Fig12. Output after scanning QR code.

The whole business logic is implemented with the help of smart contracts written in the solidity programming language. Implementing business logic using smart contracts, helps to program secure contracts which helps to reduce the loophole in the system.

Table 2: Product Transfer from Manufacturer to Seller

Transaction Cost	Execution Cost	Input	Decoded Input	Decoded Output
175284	175284	0x934...00000	"3421SAfeW0", "Seller 1"	"Transfer from Manufacturer to Seller Successful"

Table 3: Product Transfer from Manufacturer to Seller

Transaction Cost	Execution Cost	Input	Decoded Input	Decoded Output
74536	74536	0x97c...00000	"3421SAfeW0", "Seller 1", "Consumer"	"Transfer from Seller to Consumer Successful"

***Corresponding Author:** Reshma DSouza

Table 4: Comparison with various anti-counterfeiting techniques available.

SL. No.	Technology	Product Type	Advantage	Limitation	Block Chain
1	RFID	Any	Reliable track and trace through any environment.	1. Reader collision. 2. Unable to transmit through metal objects.	No
2	Magnetic Strips	Hotel Key Cards	1.More secure than barcodes. 2. Easy and fast to use.	1. Can be damaged even from small scratches 2.Does not work from a distance.	No
3	Security Hologram	Currency	If tried to remove it leaves residue behind.	1.Production is expensive and time-consuming. 2. Easy to clone	No
4	Barcodes	Daily use products	1.Simple implementation. 2. Scalable	1. Easy to replicate. 2. Editable.	No
5	SHA1/SHA2	Digital Biodata	Hard to replicate.	Easy to encrypt and decrypt.	No
6	Fingerprinting	Digital Content	1.High security. 2. Nontransferable	1.System failures. 2. High cost.	No
7	Block Chain	Any	1.Can be applied at the time of manufacturing. 2. Data once stored cannot be modified.	1.Demands high memory. 2.Expensive to implement	Yes

CONCLUSION & FUTURE WORK

Employing Block Chain technology for fake product identification offers a robust and innovative solution to address the issue of counterfeit products. By using the inherent characteristics of Block Chain, such as decentralization, immutability, and transparency, organizations can create a reliable framework to identify and confirm the authenticity of products throughout the supply chain. This proposed a Block chain-based anti-counterfeiting system ensures that every product that exists within the system is an authentic and valid. The proposed system was successfully developed this system using Remix IDE and Solidity.

In the future, upscaling and improving our system will be possible, automation can be applied to ease the manual input process and minimize human errors which may occur. Blockchain has proven to be effective in building a system that detects counterfeiting activities and there are so many areas which can adopt this Block Chain technology to make the system secure from malicious access and tampering of the data.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest that could have appeared to influence the work reported in this paper.

REFERENCES

1. Khalil, Ghaith, Robin, and Morshed Chowdhury, (2019). “A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems,” *Journal of Sensor and Actuator Networks, Switzerland, vol.8, pp. 37.*
2. N. T. Singh, Saurav, V. Sharma, A. Raizada, S. Sharma and N. Pathak, (2023). "Identification of Fake Products using Blockchain Technology," *5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 736-740, doi: 10.1109/ICSSIT55814.2023.10060998*.
3. Jinhua Ma, Shih-Ya Lin, Xin Chen, Hung-Min Sun, Yeh-Cheng Chen, Huaxiong Wang, (2016). “A Blockchain-Based Application System for Product Anti-Counterfeiting”, *IEEE Access, Volume 4.*
4. Pathak, A., Velasco, C. and Calvert,G.A.(2019). “Implicit and explicit identification of counterfeit brand logos based on logotype transposition”, *Journal of Product & Brand Management, Vol. 28, No. 6, pp. 747-757. https://doi.org/10.1108/JPBM-06-2018-1921*.
5. B. S, S. Pramanick, R. Singh and D. Kumar, (2022). "An Ethereum based Fake Product Identification System using Smart Contract", *6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 292-296, doi: 10.1109/ICICCS53718.2022.9788449*.
6. M. M et al., "Fake Product Identification System Using Blockchain, (2022). "*4th International Conference on Circuits, Control, Communication and Computing (I4C), Bangalore, India, pp. 163-167, doi: 10.1109/I4C57141.2022.10057923*.
7. B. Subashini and D. Hemavathi, (2022). "Detecting the Traceability Issues in Supply chain Industries using Blockchain Technology", *International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-8, doi: 10.1109/ACCAI53970.2022.975247.*

***Corresponding Author:** Reshma DSouza

8. Tiago M. Fernández-Caramés, Paula Fraga-Lamas, Manuel Suárez-Albela, Luis Castedo, (2024). "Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications," arXiv preprint.
9. Israelin Insulata J. and J. Roselin, (2025). "AI-Blockchain System: Enhancing Supply Chain Trust with Vision Transformers", *Journal of Intelligent Systems and Applications, Anna University Regional Campus – Tirunelveli, Tamil Nadu, India, https://doi.org/10.1016/j.future.2025.10*.

***Corresponding Author:** Reshma DSouza