Identification of Counterfeit Products using Blockchain

R.S.Ravindra Babu[1], K.Sruthi[2], G.Harish Kumar[3], Ch.Manoj Ratna Kumar[4], G.Venkata Karthik[5]
[1]*Assistant Professor, Dept Of CSE, Lendi Institute Of Engineering And Technology*
[2,3,4,5]*Dept Of CSE, Lendi Institute Of Engineering And Technology*

Abstract*—Counterfeiting has a huge impact on businesses, consumers, and public safety. This paper explores the merging of the IPFS with the SHA-256 cryptography algorithm to eliminate counterfeit products. This methodology involves methods like secures data storage using the block chain and authenticates products for consumers, allowing them to detect frauds and build trust with the companies. The research illustrates that the proposed method increases the product information traceability and enhances the consumers' trust in the products. The integration of the IPFS and SHA-256 with the QR technology offers a safe and user-friendly product authentication platform, which is an essential tool in eliminating counterfeiting.

***Index Terms*— Block chain, Interplanetary File System, SHA-256**

I. INTRODUCTION

The global issue of counterfeit products has been steadily increasing, the sale of counterfeit products is estimated as 3.3% of world trade, amounting to over $500 billion annually (OECD, 2019). Fake goods not only undermine brand reputation and consumer confidence but also pose serious risks to public health and safety. Addressing this challenge has become a pressing concern for businesses, policymakers, and consumers alike.

Emerging technologies, such as block chain and decentralized storage solutions, offer promising solutions for combating the problem of counterfeit products. The immutable and transparent nature of block chain-based systems can provide a secure platform for product authentication, while decentralized storage solutions, like the Interplanetary File System (IPFS), can ensure the integrity and accessibility of product data.

This research paper works on the integration of IPFS and the SHA-256 cryptography algorithm to develop a comprehensive solution for the identification of fake products. By leveraging the strengths of these technologies, the study aims to enhance product traceability, improve consumer trust, and contribute to the ongoing efforts to combat the global issue of counterfeiting.

In this study we will be looking at how IPFS and SHA-256 cryptography algorithm can be integrated so as we come up with a full proof method for identifying counterfeit products. The main goal is to boost product traceability, improve customer confidence among other things like supporting worldwide fight against counterfeiting through employment of such powerful tools given their abilities.

To sum up the proposed methodology combines the secure storage capabilities of IPFS, the reliable hash generation of SHA-256 algorithm, and the transparency of the block chain to create a verifiable and user friendly platform for product authentication.

II. RELATED WORK

As of now, many researchers have proposed different methods for establishing a block chain based supply chain management system. One of the biggest advancement in this is utilization of distributive ledgers and smart contracts . Which also include studies on rising counterfeit products problem Block chain is used in cryptocurrency. A fully functional anti-product forgery system was designed by a group of researchers that uses digital signature for verification [5].In other paper they mentioned about using D App using block chain to track product ownership[1].Some other solutions also include bar code based authenticity system [2].Some more solutions include usage of anonymity and supply chain in block chain system[3]

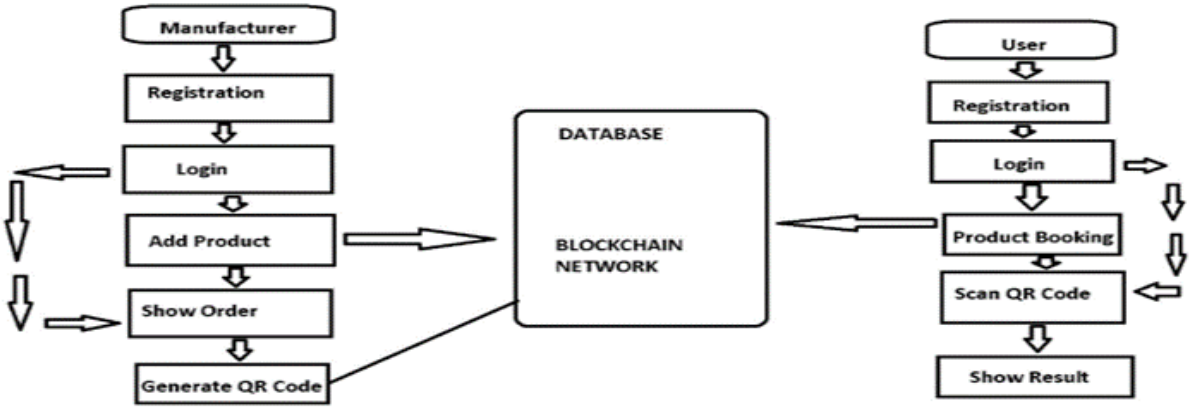

Fig. 1. System Architecture

III. METODOLOGY

The system proposed here involves usage of cryptography algorithms and block chain system for enabling the fake product detection in the large and complex supply chain.

The system consists of two different modules for both manufacturer and the consumer.

A. Manufacturer

The manufacturer module in the system enables the services to the manufacturer where they can come and register to the application and add their product and whose details are stored in IPFS and created hash using cryptography algorithm and added to the QR code which can be added to the product.

Algorithm 1: Manufacturer Module

Input: Product Name, Product Price, Product details

Output: Added Product,QR code

Steps:

i. Enter the company details and register
ii. Enter the product details
iii. Added to IPFS
iv. Created the hash using SHA 256
v. Inscribing hash in QR code
vi. Providing the QR to the manufacturer

Here in Fig.2. we are clearly explaining the methodology of the manufacturer module and representing the manufacture module procedure using the flow diagram

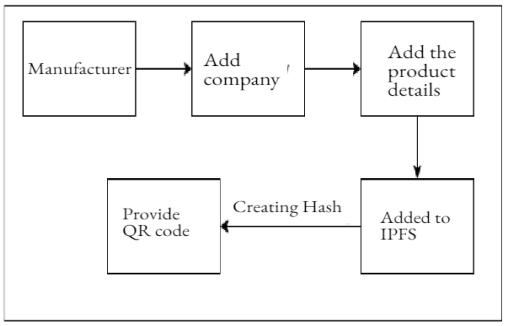

Fig. 2. Manufacturer's Working Process

B. *Consumer*

The consumer module in this system enables the services to the consumer where they can come and register to the application and scan the Qr code on the product package and then scan it if the product is authenticated then block chain code in the QR is authenticated and then the product details stored in IPFS are fetched.

Algorithm 2: Consumer Module

Input : Qr Code

Output : Product details and Product authenticity

Steps :

i. Register to the application
ii. Scan the Qr code
iii. Authenticate the hash code in QR
iv. If authenticated :
Product details fetched
Else:
Product is fake

Here in Fig.3. we are clearly explaining the methodology of the consumer module and representing the consumer module procedure using the flow diagram

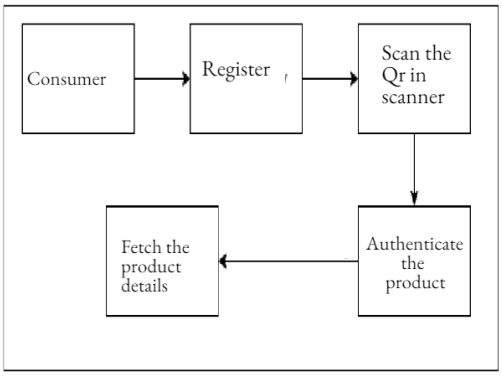

Fig. 3. Consumer's Working Process

C. *Block chain*

Block chain technology provides promising opportunities in the supply chain management paradigm. Block chain data is stored on nodes where each node has a complete copy of the block chain database. Orders, payments, accounts, price of products etc. can be tracked, shared and secured using a block chain network. Some important features of block chain technology in supply chain management includes:

1) Security and Privacy: Block chain uses public key encryption method of cryptography for data security. Users have public and private key pair which are used to validate transactions and these transactions are immutable and permanent.

2) Decentralization: As block chain is a distributed ledger technology, it doesn't rely on third party or any centralized authority.

3) Transparency: Data stored in Block chain is public and anyone can enquire on their transactions. The transactions can be governed by a set of rules known as the smart contract. The system proposed here uses Meta Mask cryptocurrency wallet for transactions and the smart contract here has been deployed in the Rinkeby Test Network of the Ethereum Block chain. The D App is based on two major stakeholders, The Manufacturer and the consumer.

D. *Ethereum App Architecture*

The base architecture of the system includes

user interface (UI) here has been developed using Flask and Bootstrap. If the user wants to interact with the smart contract, the App will use Web3.js which communicates with smart contract through its provider. Meta Mask creates a transaction and signs it with the user's private key. This transaction is then sent to Ethereum network. The transaction is processed, verified and added to a block in the network. The private keys of the user are never the indicating that you request color printing. Do not use color unless it is necessary for the proper interpretation of your figures. There is an additional charge for color printing. Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity―Magnetization, ‖ or ―Magnetization M, ‖ not just ―M.‖ Put units in parentheses. Do not label axes only with units. As in Fig. 1, for example, write ―Magnetization (A/m)‖ or―Magnetization ($A \cdot m^{-1}$), not just ―A/m. Do not label axes with a

E. *IPFS*

IPFS, the Inter Planetary File System, revolutionizes the way data is stored and shared on the internet by offering a decentralized and permanent solution. By utilizing content addressing and peer-to-peer networking, IPFS ensures that files are uniquely identified based on their content rather than their location. This approach not only enhances reliability and scalability but also makes the system resistant to censorship. IPFS enables efficient storage and retrieval of data through versioning, duplication, and offline access, making it ideal for applications where internet connectivity may be limited or unreliable. With its wide range of use cases, including distributed file sharing, decentralized websites, and content delivery networks, IPFS empowers users to take control of their data and build a more resilient and secure internet ecosystem

F. Flask

A Flask is a Web Application Framework that is built with Flexibility and Speed In the Mind. Flask is Built in Python, which many data Scientists are familiar with Flask takes care of the Environment and Project setup involved in web Applications Allowing the Developer to focus on their application rather than thinking about HTTP, routing, datasets etc. Flask allows Data Scientists to create simple Single page Applications and one should Help or look into if they want to create Products for Consumers Flask is a micro web framework written in Python. It is classified as a micro framework because it doesn't require particular tools or libraries. There is no database abstraction

layer, form validation, or the other components where preexisting third-party libraries provide common functions. However, Flask supports extensions which will add application features as if they were implemented in Flask itself. Flask was created by Armin Ronacher of Pocoo, a world group of Python enthusiasts formed in 2004.According to Ronacher, the thought was originally an April Fools joke that was popular enough to form into significant application. 28 When Ronacher and Georg Brandl created a bulletin board system written in Python, the Pocoo projects Werkzeug and Jinja were developed. Flask has become popular among Python enthusiasts. As of October 2020, its second most stars on GitHub among Python web development frameworks, only slightly behind Django, and was voted the foremost popular web framework within the Python Developers Survey 2018.

IV. RESULT ANALYSIS

Our system include two different types of inputs and outputs corresponding to the modules. The table below indicates various test cases for the system and also depicts how the system is responding to various outputs

S. No	Description	Input	Expected value	Actual value	Result
1.	Sending text data	Text	Sent	Sent	Pass
2.	Creating a QR	Text	Recieved	Recieved	Pass
3.	Storing image data	Image file	Stored	Stored	Pass

In this testing we have checked 4 important tasks of the system which include sending text data i.e product details storage and creating QR with the details and storing image data which include scanning of the QR

V CONCLUSION

Our project will eliminate the problem of counterfeit products using the blockchain technology. Blockchain Technology is the most secured and transparent technique so it is reliable to use this technology in the complex supply chains which is most ambiguous

In this digital era it is very hard to know whether the product is real or fake so one can rely on our project to get the original products in the chain filled with multiple fake products.

VII FUTURE WORK

In future developments of the block chain-based anti-counterfeiting solution, there are several key areas to focus on. Enhancing the system's scalability will be paramount, ensuring that it can handle the extensive data and transaction volumes of global supply chains without sacrificing performance. This may include investigating second-layer solutions or alternative consensus protocols. Additionally, creating more sophisticated analytic features will be important for harnessing the data stored on the block chain, allowing businesses to not only track products in real-time but also gain predictive insights into counterfeit trends. Equally crucial will be ensuring the system's compliance with international trade laws and regulations, which will require ongoing legal analysis and adaptation to varied jurisdictional requirements. Moreover, bolstering the integration capabilities with existing supply chain infrastructures and Internet of Things (Io T) devices will enhance the seamless adoption of the technology. This future work will solidify the D App's position as a robust tool against the proliferation of counterfeit good

REFERENCE

[1] “Identifying Counterfeit Products using Block chain Technology in Supply Chain System” by Nafisa Anjum, and Pramit Dutta

[2] “Strengthening Supply Chain Integrity with Block chain-based AntiCounterfeiting Measures” by Shubham Prajapati, Juilee Kini, Jayesh Gadhari, Sheetal Solanki, and Tushar Sawan

[3] “Fake Product Detection using Anonymity and Supply Chain in Block chain” by Shaarmitha, Akhash, Harihara

[4] Bitcoin: A Peer-to-Peer Electronic Cash System‖, 2008,Satoshi Nakamoto

[5] “Identifying Counterfeit Products using Block chain Technology in Supply Chain System” by Nafisa Anjum, and Pramit Dutta Hyper ledger, ―Hyper ledger Block chain Performance Metrics‖, V1.01, October 2018

[6] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
[7] Armin Ronacher, ―Flask Docs‖, http://flask. pocoo.org/docs/‖
[8] G. Wood, Ethereum: A secure decentralized generalized transaction ledger,‘‘ Tech. Rep., 2014.
[9] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https:// doi.org /10.1787/9789264251847-en.
[10] https://phys.org/news/2019-03 counterfeit-pirated-goods-global.html
[11] https://www.statista.com/statistics/1117921/sales-losses-due-to-fakegood-by-industry-worldwide/
[12] T. J. Sayyad, ”Fake Product Identification Using Block chain Technology,” in International Journal of Future Generation Communication and Networking, vol. 14, pp. 780-785, 2021, ISSN: 2233-7857 IJFGCN
[13] T. Tambe, S. Chitalkar, M. Khurud, M. Varpe, S. Y. Raut, ”Fake Product Detection Using Block chain Technology,” in International Journal of Advance Research, Ideas and INNOVATIONS in Technology, vol. 7, pp. 314-319, 2021, IJARIIE-ISSN(O)-2395-4396
[14] J. Ma, S. Lin, X. Chen, H. Sun, Y. Chen and H. Wang, ”A Block chain-Based Application System for Product Anti-Counterfeiting,”in IEEE Access, vol. 8, pp. 77642-77652, 2020, doi: 10.1109/ ACCESS.2020.2972026.
[15] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, ”A Novel Block chain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain,” in IEEE Access, vol. 5, pp.17465-17477, 2017, doi:10.1109/ACCESS.2017.2720760.