Volume 9, Issue 4, April – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

Counterfeit Product Detection using Blockchain Technology

Sanket Mungase[1]; Vinayak Shinde[2]; Tejas Wakchaure[3]; Bhavana Chaudhari[4]
[1,2,3]Student, Department of Information Technology, PES Modern College of Engineering, Pune
[4]Professor, Department of Information Technology, PES Modern College of Engineering, Pune

Abstract:- A fraudulent practice where products that are passed off as genuine, product counterfeiting represents consumer fraud, which translates to financial losses. Transparency in supply chain management also faces a big challenge in terms of service repetition and lack of coordination. Numerous remedies have been implemented to battle counterfeiting, among them Artificial Intelligence and RFID, among others, all of which have significant issues such as incivility. This project tackles the problem by applying blockchain technology to improve counterfeit determination and assure product items' authenticity all over the source chain. The scheme is built on blockchain encryption techniques, which promote a decentralized service for genuine authentication and duplication identification. Through the usage of QR codes and barcodes found in wireless technologies, counterfeit items are eradicated . When scanning a product's QR or barcode with a camera scanner, the product's unique code is linked to the blockchain, and all its complete details are stored within it. The database consists of multiple blocks, each one representing a unique product. In case of scanning, if the entered code matches with the database, a popup notification will display on the customer's device that this product is genuine. Contrary to it, if there is no match found, means it is a counterfeit product; then a popup displays on the customer's mobile, computer screen about the fraud transaction of the manufacturer from which points this scam is originating if the customer allows doing this action using the application . This will enable users to authenticate products independently without relying on sellers.

***Keywords*:-** *Counterfeiting, Blockchain Technology, Supply Chain Management, QR Codes, Product Authenticity, Fraud Detection, RFID Tags, Decentralization, Data Security.*

I. INTRODUCTION

Counterfeiting is when a product is sold masquerading as another product. Consumer fraud itself, is generally defined as deceptive business practices that cause financial and other harm to consumers. According to a report by the Association of Authentication Solution Providers, the Indian economy costs Rs 1 trillion annually. Fraud is expected to increase by 20% in 2018-20.[1] Counterfeit goods include fake plants and trees, handbags, clothing, cosmetics and electronics. It has negative effects not only on the economy, but also on society. For example, diseased plants and trees can be sold without the user's knowledge, poor cosmetic products can touch the skin and cause skin infections and burns, counterfeit electronics can prevent machines from doing it work poorly and have caused bad conditions and accidents poor quality clothing, shoes can cause discomfort when worn . Therefore, it is important to find a solution to sell counterfeit goods in this regard. Another consequence of counterfeiting is damage to the company's reputation. Since many consumers are clueless that what they are wearing is a knock-off, they will blame the real company if the knock-off product doesn't work properly, disconnects quickly, or fails to meet their expectations Consumers ask for a refund they, in the form of a refund or new or other product, were applying directly to a legal entity. Most affected businesses are probably in a situation where they are dealing with an unhappy customer who complains about the poor quality of the product, and the customer service representative is unaware that the product in question is counterfeit.

A fully functional blockchain system is proposed to eliminate this practice by ensuring that counterfeit goods or products are detected and traced throughout the supply chain Companies should pay minimum fees on marketing and they don't have to worry about the possibility of spurious distribution to their end users. The biggest problems and biggest losses are in the sense of raw material damage and loss of money for the original manufacturers due to counterfeiters. Functional blockchain technology can be used to determine the original state of an object. A blockchain is a chain system of encrypted data that makes it difficult or impossible to change or crack the system. Once a resource is stored on the network, a hash code is generated for that resource and it is possible to maintain all transaction records of the resource as well as its current owner as a chain created for that resource transaction. This will store all transaction records as blocks in the blockchain. In the proposed system, we provide a QR code or barcode designed for a specific product by the manufacturer with all the details of the product. The end customer can scan that QR code to get all the information about that product. By scanning the QR code or barcode on the product, the user can determine whether the product is genuine or fake.

II. MOTIVATION

The motivation behind implementing a blockchain-based fake product detection system lies in safeguarding consumer safety, reducing economic losses, preserving brand reputation, and ensuring compliance with regulations in an

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

increasingly globalized marketplace. By leveraging the transparency and tamper-resistant properties of blockchain technology, this project aims to instill trust, protect public health, and promote responsible business practices while addressing environmental concerns, enhancing data security, and embracing innovation, ultimately contributing to a safer and more reliable marketplace for consumers and businesses alike.

III. LITERATURE SURVEY

The literature survey explores the sources of counterfeits and social impact, and discusses detection systems such as artificial intelligence, QR codes, machine learning, blockchain, etc. Shaik suggests public and private keys are not used as QR codes, with cryptographic functionality to be defined app for scanning objects. Shaik's proposal to use QR codes with cryptographic functionality highlights a step towards secure consumer products [2]. Benatia and Baudry et al. Present the traceability-CPS framework for supply chain management, enhancing product safety and quality through data analytics. Benatia and Baudry's traceability-CPS architecture provides a holistic approach to supply chain management, with an emphasis on data analytics to enhance product security. [3]. Khalil and Dos, among others. RFID-based systems are recommended to reduce counterfeiting, enabling product legitimacy to be verified in-store, Khalil and Doss recommend supporting RFID-based systems, which provide real-time verification of product legitimacy for counterfeit transactions Tran and Hong's anti-counterfeiting protocol enables them to stop denial-of -service attack prevention, thereby making security detection systems more enhanced. [4]. Tran and Hong proposed an anti-counterfeiting system that is impervious to DOS attacks, Khalil and Doss recommend supporting RFID-based systems, which provide real-time verification of product legitimacy for counterfeit transactions Tran and Hong's anti-counterfeiting protocol enables them to stop denial-of -service attack prevention, thereby making security detection systems more enhanced.. Habib, Sardar and others. Recommendations for integrating blockchain into supply chain management to address transaction issues, Habib and Sardar's integration of blockchain in supply chain management solves transaction challenges, promising increased transparency and security. [5]. David and Wu et al. presents an AI framework for lie detection using training samples and detection algorithms, To detect lies,

David and Wu used AI. Chen and Shi's blockchain-based framework for supply chain quality intelligence uses smart contracts to execute quality control measures, enhancing supply chain efficiency [6]. Chen and Shi et al. propose a blockchain-based system for better supply chain intelligence, using RFID technology and smart contracts[7]. Toyoda , Kentaroh and Mathiopoulos , P. Takis et al. Introduce a QR code-based system to validate products and capture transaction history. The blockchain system ensures data integrity and user control, with Ethereum acting as the backend processing system, Toyoda, Kentaroh and Mathiopoulos, P. Takis proposes a QR code-based system for consumer goods trust, facilitating transparency and follow-through. Furthermore, the discussion on Ethereum as a blockchain operating system highlights the role it plays in enabling digital transactions and services[8]. Abhijeet and Andrew et al. They examine the phenomenon of counterfeiting in the global supply chain and highlight various methods of counterfeiting by companies. Limitations of existing systems include QR code copying and RFID tag cloning, as well as resource-intensive AI and machine learning. Buyers, sellers and retailers should be empowered to verify products. In a comprehensive study, Abhijeet Andrew et al. discusses findings on counterfeiting in the global supply chain. Counterfeiting is on the rise, especially in areas such as low-cost raw materials and pharmaceuticals[11]. Strategies used by companies to reduce this issue include avoidance, prevention based on past experiences, and waste. Challenges remain in counterfeit detection due to the presence of forged certificates. Limitations are specified for existing systems. QR codes, although often used by companies for authentication purposes, can be copied and used for counterfeit goods. Similarly, low-cost RFID tags in RFID-based systems are susceptible to cloning, making the method inefficient. Artificial Intelligence and Machine Learning applications, although promising, face obstacles such as high computational requirements of Convolutional Neural Networks (CNN) and unpredictability of tag reuse attacks

A key feature lacking in current policies is the ability to verify products for customers, suppliers and retailers. This gap highlights the need for innovative solutions that not only detect counterfeiting but also provide stakeholders with options for authentication throughout the supply chain emphasize. Furthermore, the study highlights the potential of blockchain technology to ensure transparency and data integrity, emphasizing the importance of its application to data collection and use plant. Continuing the research, the literature examines possible solutions and progress in the fight against counterfeiting.

Overall, the literature survey provides a comprehensive overview of the challenges posed by counterfeiting and the diverse array of solutions proposed by researchers and practitioners. By addressing limitations in existing systems and leveraging emerging technologies, the fight against counterfeiting continues to evolve towards greater transparency, security, and consumer protection.

IV. WORKING OF BLOCKCHAIN

The main objective of blockchain is to make the stored data irrevocable from the system. The approximately five steps that shows how a blockchain works are:

- The user should register and authenticated prior to inputting data in the transaction blockchain.
- Creation of a new block and storage of transaction.
- The copy of newly created block is sent to every node of the computer.
- By the use of different chaining techniques, the acceptance of transaction is done by the authorised nodes which is in decentralized manner, in forward the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

transaction information is stored in already existing blocks.

- Later the updates are distributed throughout the network.

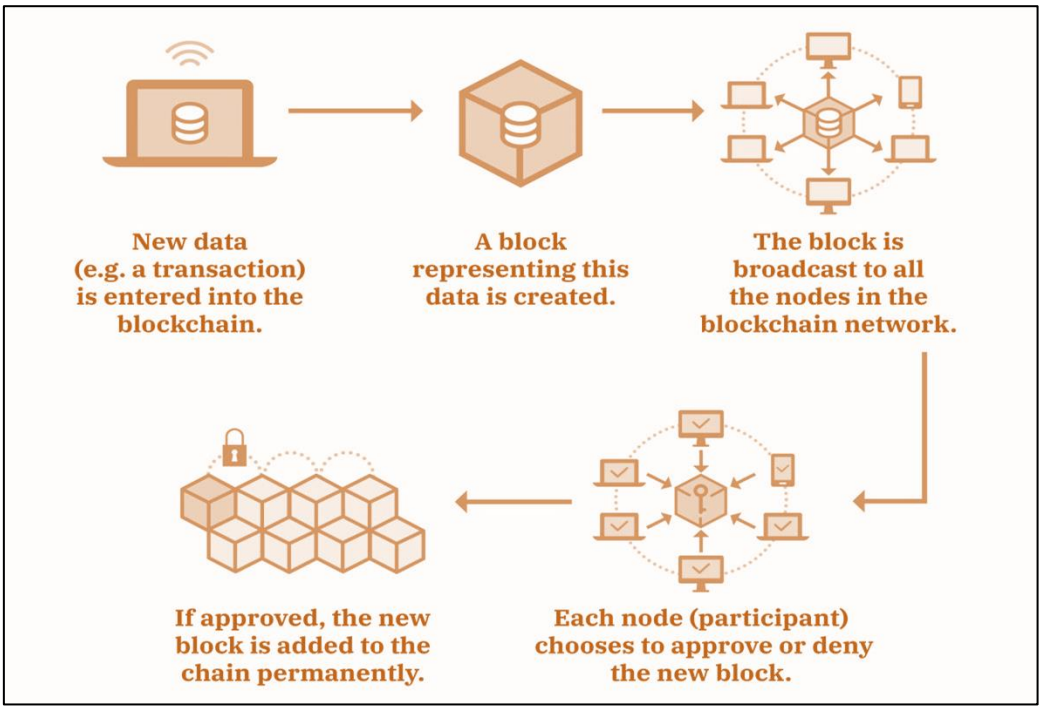

Fig 1. Working of a Blockchain Network

V. METHODOLOGY

A. Proposed System

To address the increasing prevalence of counterfeit goods globally, we propose the development of a comprehensive application system. This system will focus on storing the product's supply chain information and preserving ownership histories. By providing buyers with access to detailed product information, they can make informed decisions about the legitimacy of the item they are purchasing. Our approach involves the utilization of QR codes to validate products and add relevant product information. QR codes offer a convenient and efficient means of accessing product details, enhancing transparency in the purchasing process. Additionally, we will implement mechanisms to safeguard product data from unauthorized modifications. Blockchain technology emerges as a viable solution in this regard, offering tamper-resistant data storage capabilities. In this suggested system, the integration of blockchain and QR codes plays a pivotal role in identifying counterfeit products. Blockchain ensures the integrity and immutability of product data, while QR codes facilitate easy access to this information for consumers. Together, these technologies create a robust framework for combating the proliferation of counterfeit goods.

Furthermore, the application system will incorporate features to streamline the verification process for consumers, enabling them to quickly authenticate products and ascertain their authenticity. By leveraging blockchain and QR codes, we aim to instill greater confidence in consumers while simultaneously deterring counterfeiters from engaging in fraudulent activities.

Overall, our proposed system represents a proactive approach to addressing the challenges posed by counterfeit goods. Through the seamless integration of blockchain and QR codes, we can establish a reliable mechanism for authenticating products and safeguarding consumer interests.

B. System Model

In the system model, the flow begins with the user visiting a web page and interacting with the blockchain through the web3.js library. Web3.js is a JavaScript library that allows you to interact with the Ethereum blockchain. It acts as a bridge between the frontend web application and the blockchain network.

When a user initiates a transaction or interaction with smart contracts on the web, the request is sent to Metamask , which acts as a Web3 WebProvider. Metamask securely manages the user’s Ethereum account and private key, enabling them to sign transactions and communicate with smart contracts securely.

Finally, MetaMask forwards the transaction request to the Ethereum blockchain, where it is processed by smart contracts. A transaction results in changes to the blockchain state, which are recorded and verified by participants in the network.

Overall, this management system ensures smooth data and transactions between the web application, Metamask, and the Ethereum blockchain, enabling secure and transparent transactions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

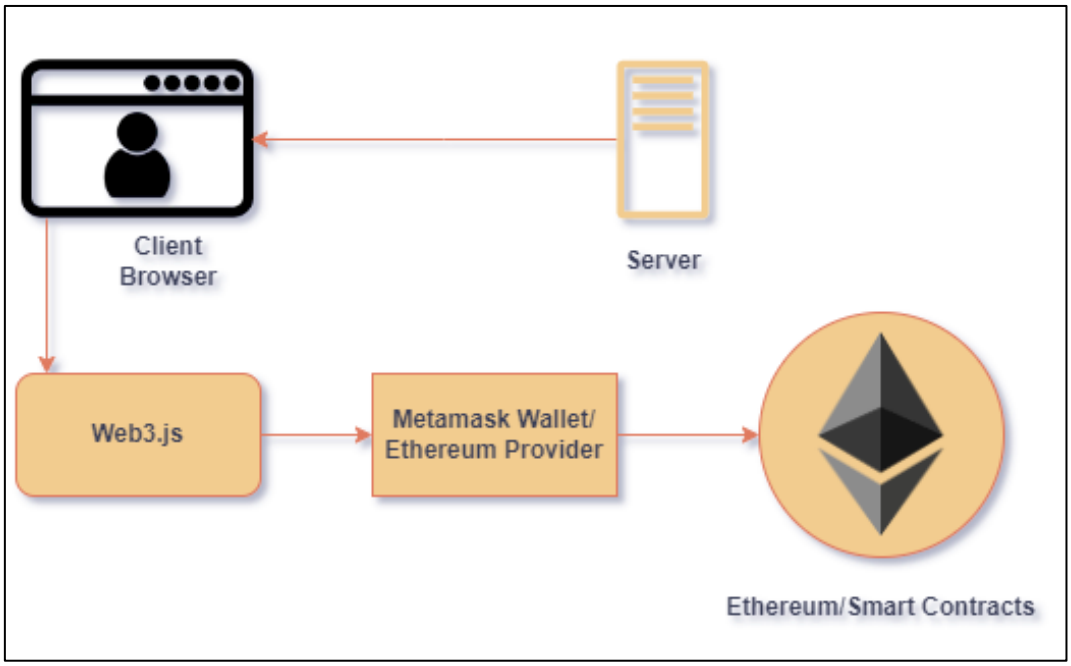

Fig 2 System Model

C. Tools Requirement

➢ *Ganache*

This software package enables you to create a personalized Ethereum blockchain community. It provides the necessary tools to use and interact with blockchain-based smart contracts. Ganache allows Ethereum blockchain simulation, facilitating seamless transactions and smart contracts tailored to specific applications.

➢ *Metamask*

As a web browser extension, Metamask acts as a bridge between the browser and the Ethereum blockchain. It acts as a secure Ethereum blockchain wallet for users, allowing them to manage their Ethereum accounts and transact directly from their web browser Metamask improves the user experience with easy and secure transactions by enabling them to interact with blockchain applications.

➢ *Truffle Suite*

Truffle is a comprehensive framework that simplifies the development, testing, and deployment of blockchain-based applications. It offers a suite of tools for creating and managing smart contracts, as well as for automating various aspects of the development process. Truffle's robust features streamline the development workflow, making it easier for developers to build and deploy decentralized applications (DApps) on the Ethereum blockchain.

➢ *Node.js*

Node.js is a runtime environment that allows developers to create server-side applications using JavaScript. For blockchain development, Node.js is often used to create front-end web pages for websites or DApps. Its asynchronous and event-driven architecture makes it ideally suited for handling concurrent transactions and interacts with the blockchain network via the JavaScript library web3.js for Ethereum development.

➢ *Solidity*

Solidity is a high-level programming language specifically designed for writing smart contracts on blockchain platforms, par

D. Algorithm

The following algorithms can be used to deal with counterfeit goods using blockchain technology.

- Recording product information: The first step is to record detailed product information including information and transaction history on the blockchain. Each product is assigned a unique identifier for easy tracking throughout the supply chain.
- Supply Chain Verification: It is important to verify the entire supply chain. This process includes authentication of raw materials, verification of manufacturing processes, and documentation of distribution channels on the blockchain.
- Smart Contract Implementation: Smart contracts are implemented on the blockchain to ensure that every transaction in the supply chain is authentic and authorized by the relevant stakeholders This reduces risks such as double spending and under unauthorized uses.
- Verification by stakeholders: All stakeholders involved in the supply chain must have access to the blockchain to verify the authenticity of the product at every stage. This can be done by looking for a unique QR code or barcode associated with blockchain records.
- Verification by Consumers: Consumers also have the ability to verify the authenticity of products by scanning the product's unique code and accessing blockchain records. This enables consumers to avoid counterfeit purchases, increasing consumer safety.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

- Alert generation: Any suspicious activity or attempts to modify blockchain records should trigger alerts for relevant parts of the supply chain. This proactive approach helps prevent fraudulent activities and ensures supply chain integrity.

By implementing this system, both manufacturers and consumers can ensure product authenticity, thus reducing the risk of buying counterfeit goods.

E. System Architecture

Overall, the whole system uses QR code as a base to detect fake products. The verification can be done using a smartphone or a scanner where each product will have its separate QR code which then will be linked to smart contracts. The company, after verifying the ID and corresponding registration system, gets to add a machine-generated QR code to add product information. This ensures that only authorized entities can support the system, maintaining the integrity and accuracy of false identification.

In the blocks of the blockchain under the QR code, the product details would be stored such as brand name, product name, manufacturing time, price, quality, size, and manufacturer information. Each retail block will be associated with a unique QR code, ensuring it can't be reused for different products from the manufacturer. The use of returned QR codes increases the security and reliability of the tracking and identification process. These reissued QR codes provide complete product information, keep customers connected and increase productivity. Before a product's QR or barcode can be scanned, customers are required to register and log into the system. This ensures accountability and enables the system to monitor user interactions, contributing to the overall security and integrity of the product authentication process.

If the user is successful, the unique code checked by the customer will be compared with the code generated by the manufacturer, which is stored in smart contracts blocks and if the codes match, the user will receive a notification stating that the item is the beginning. In addition, the user will be provided with all relevant product information and authentic documentation obtained from the database. In the event of a discrepancy between the codes, the user will immediately be notified that the product is counterfeit. This information is critical to preventing counterfeit purchases, which can result in serious health or financial consequences. By detecting counterfeit products early, consumers can make informed purchasing decisions and minimize potential risks.

Indeed, manufacturers benefit from the detection of counterfeits. If an item is found to be counterfeit, the system can record the status of the person with the appropriate authorization. A warning can then be sent to the manufacturer, enabling further legal proceedings against distributors, stores and illegal manufacturers. This not only increases trust between customers and businesses but also increases customer satisfaction. Furthermore, it saves the manufacturer from wasting valuable time and resources in dealing with reputational and business losses caused by counterfeit products. Legal action against illegal distributors, retailers and manufacturers protects the integrity of the supply chain, and maintains consumer confidence and satisfaction.

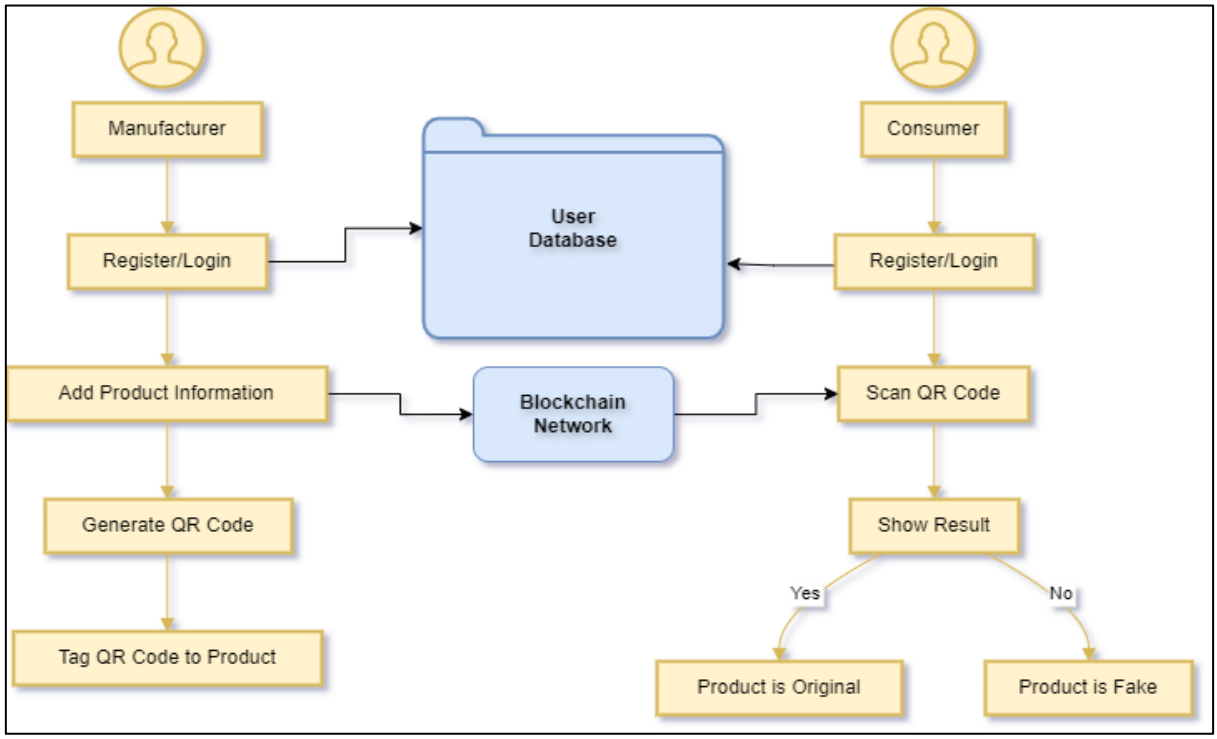

Fig 3.System Architecture of Proposed System

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

F. Security Algorithm

The algorithm used in the blockchain to generate a consistent hash of 256 bits is an integral part of encryption technology. This process requires several steps to ensure data integrity and security.

Initially, the algorithm uses an initialization vector (IV) of 256 bits. The input data, which can be very large, is divided into 512 bit blocks. Since an input size cannot always be an exact number of 512 bits, padding is applied to the rest of the input. The input is combined with a 10-bit sequence before proceeding to this padding.[13]

Once the input is appropriately padded and segmented, each block is processed with a compression function. The output, a 256-bit hash, is then combined with the next 512-bit input block. This process continues iteratively until the last block (segment n) is reached.

At this point, the last block compresses with a compression function, producing a final 256-bit output. This output is a hash of the input data.

It is important to check the specifications for message length and digestion length. The clear text must be less than 264 bits long to keep randomness random in the digester. In addition, the hash digest length for the SHA-256 algorithm must be exactly 256 bits to ensure accuracy and reliability.[14]

Also, hash functions like SHA-256 are immutable by design. This means that it is not computationally feasible to obtain the original simple information from a hash digest, or to reconstruct the original hash digest from a simple digest This transformation is a key property of cryptographic hash implementations and contributes to its efficiency in protecting data.[15]

G. Truffle Framework

Truffle is a comprehensive development environment, testing framework, and asset pipeline designed for blockchain development utilizing the Ethereum Virtual Machine (EVM). It provides support for developers throughout the entire lifecycle of their projects, whether they are building on Ethereum, Hyperledger, Quorum, or other compatible platforms. Complemented by Ganache, a personal blockchain, and Drizzle, a front-end dApp development kit, the Truffle suite offers a complete solution for dApp development.

Ganache serves as a personal blockchain platform that enables developers to create smart contracts, decentralized applications (dApps), and test software. It is available as both a desktop application and a command-line tool, offering compatibility with Windows, Mac, and Linux operating systems.

Drizzle is a specialized front-end development library built around the Redux JavaScript library. It is designed to automatically synchronize contract data, transaction data, and other relevant information, providing a seamless integration with blockchain applications.

H. Firebase Authentication

Firebase Authentication provides all the server-side features to authenticate the user. With the SDK, Firebase Authentication becomes easier. This makes the API easier to use. Firebase Authentication provides all the server-side features to authenticate the user. With the SDK, Firebase Authentication becomes easier. This makes the API easier to use. Firebase Authentication also provides a number of user interface libraries that enable screens for us when typing. Firebase authentication supports authentication using password, phone number, popular identity providers like Google, Facebook, Twitter etc. [2] User authentication is one of the most important requirements for Android apps nowadays. Getting users to agree is important, more difficult if we have to write all this code ourselves. This is very easy with the help of Firebase.

- By securely authenticating our users, it provides a customized experience based on their interests and preferences.
- We can make sure that many devices have no problem accessing their private data while using our app.
- Firebase Authentication provides all the server-side features to authenticate the user. With the SDK, Firebase Authentication becomes easier. This makes the API easier to use.
- Firebase Authentication also provides a user interface library that enables screens for us while logging in.
- Firebase authentication supports authentication by password, phone number, popular identity providers like Google, Facebook, Twitter etc.
- We can provide users access to our app using FirebaseUI.
- Manages a continuous UI flow for user login with email addresses and passwords, phone numbers, and popular providers, including Google Sign

VI. FUTURE WORK

Future work of the system may be evidence of regulatory weaknesses that may indirectly increase customer confidence due to distributed applications. It can be difficult to include all details of products manufactured at the manufacturer's side so instead of manually adding product information, data can be extracted via the company's API to increase productivity and let the manufacturer good friendly. It is more efficient to print the QR code and scan and retrieve the information so that it can be used in order to extract a secure graphic QR code which if when the QR code is photocopied will lose the information due to inking. These image recognition images or encrypted images are digital images that are formatted so that they lose information when copied and are printed irreversibly. Also to create a Price negotiation chatbot which will directly deal with consumers in order to negotiate the price of the product that the consumer is ready to purchase.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR680

VII. CONCLUSION

A fully functional application can effectively reduce anti-counterfeit counterfeiting of branded products and provide companies with limited financial resources and an easy way to give consumers confidence and assurance that they won't buy counterfeit unconventional objects. Overall, this blockchain technology-based application could emerge as a lifesaver for companies and enable new systems of trading, marking and procurement that are secure and user-friendly. The total cost of running on the Ethereum public chain is directly related to the soft code of the distributed applications. Future operations of the system may be evidence of regulatory weaknesses that may indirectly increase consumer confidence due to distributed applications. It can be difficult to include all details of products manufactured at the manufacturer's side so instead of manually adding product information, the data can be extracted using the company's API to increase efficiency and make it friendlier. The QR code is not hack able, but the information is copied or known to give the same QR code and the printing of the QR code works well to scan and retrieve the information so to tackle this, secure graphic QR code can be released as the QR code one day no is photocopied and then information disappears due to ink smearing will. These visual images or encrypted images are digital images that are formatted so that information is irreversibly lost when copied and printed. The system should be able to show the customer the same products when the product is counterfeit but show the original from different price points to make the system usable, efficient and effective.

REFERENCES

[1]. ASPA, The state of counterfeiting in india 2021, https : / / www.aspaglobal.com / pre_upload / nation / 1623216858-4730baa0efdb83aba174859af0a3a6a5-Report % 20The % 20State % 20of % 20Counterfeiting % 20in % 20India % 202021.pdf (2021)
[2]. C. Shaik, Computer Science & Engineering: An International Journal (CSEIJ) 11 (2021)
[3]. M.A. Benatia, D. Baudry, A. Louis, Journal of Ambient Intelligence and Humanized Computing pp. 1–10 (2020)
[4]. G. Khalil, R. Doss, M. Chowdhury, IEEE Access 8, 47952 (2020)
[5]. M.A. Habib, M.B. Sardar, S. Jabbar, C.N. Faisal, N. Mahmood, M. Ahmad, Blockchain-based supply chain for the automation of transaction process: 8 ITM Web of Conferences 44, 03015 (2022) https://doi.org/10.1051/itmconf/20224403015 ICACC-2022
[6]. E.Daoud, D.Vu, H.Nguyen, M.Gaedke, Improving Fake Product Detection Using Ai-Based Technology, in 18th International Conference-Society(2020)
[7]. S.Chen, R.Shi, Z.Ren, J.Yan, Y.Shi, J.Zhang, A blockchain-based supply chain quality management framework, in 2017 IEEE 14th International Con-ference on e-Business Engineering (ICEBE) (IEEE,2017), pp.172–176
[8]. K.Toyoda, P.T.Mathiopoulos, I.Sasase, T.Ohtsuki, IEEE access 5, 17465 (2017)
[9]. M.Nakasumi, Information sharing for supply chain management based on blockchain technology, in 2017 IEEE 19th conference on business informatics (CBI) (IEEE,2017), Vol.1,pp.140–149
[10]. G.Woodetal., Ethereum Project Yellow Paper 151, 1 (2014)
[11]. A.Ghadge, A.Duck, M.Er, N.Cald-well, Supply Chain Forum: An In-ternational Journal 22, 87 (2021), https://doi.org/10.1080/16258312.2021.1908844
[12]. I.Singhal, International Journal for Research in Ap-plied Science and Engineering Technology 9, 291 (2021)
[13]. https://aws.amazon.com/what-is/blockchain/?
[14]. https://ijarcce.com/wpcontent/uploads/2022/05/IJARCCE.2022.11578.pdf?
[15]. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=efa5995829c4c989f4ca78ff07c2ad9c15322782?