ISSN PRINT 2319 1775 Online 2320 7876

Research paper Volume 11, Iss 5, 2022

FAKE PRODUCT IDENTIFICATION SYSTEM USING BLOCK CHAIN TECHNOLOGY

M.Chenna Keshava, V.Kavitha, L.Bhavya, CH. Srilakshmi Prasanna, M.Pujitha

Assistant Porofessor, CSE Department, JNTUACE, Pulivendula keshava1047@gmail.com
Assistant Porofessor, CSE Department, JNTUACE, Pulivendula
kavithareddy.velagalapalli@gmail.com
Assistant Porofessor, CSE Department, JNTUACE, Pulivendula
bhavyalevadala@gmail.com
Assistant Porofessor, CSE Department, KVSRIT, Kurnool
srilakshmi1023@gmail.com
Assistant Professor, CSE Department, ECE&T, Hyderabad
mpujitha46@gmail.com

***Abstract*—** The manufacturing and selling of counterfeit goods pose a serious threat to consumers' finances, health, and safety, as well as negatively impacting the original manufacturers' economic growth. To combat this problem, a camera scanner can be used to detect fraudulent products, and their QR or barcode can be linked to a block chain database to store their unique code and information. If the code on the product matches the code in the database, a notification is sent to the customer confirming the product's authenticity. However, if the code does not match, the customer is prompted to accept a request to notify the manufacturer of the location of the purchase. This method provides customers with an additional tool to verify the authenticity of products, rather than solely relying on retailers' judgement.

***Keywords*—** *Block chain, cryptographic, SHA256, Counterfeit*

I. INTRODUCTION

The existence of fake products in supply chains is a common problem, and a system is needed to ensure the authenticity of products. To verify the genuineness of a product, it is necessary to maintain its ownership history. One potential solution is the use of IPFS, which is a peer-to-peer distributed file system capable of storing large volumes of data in the form of objects, blocks, or files. IPFS operates similarly to block chain protocols and offers advantages over HTTP, which only downloads files from a single device. With IPFS, it is possible to distribute large amounts of data efficiently across a network.

Another significant characteristic of IPFS is its ability to prevent duplication. When a product is stored on the network, a hash code is generated for it, enabling the maintenance of a complete transaction history for the product, including its current owner. The transactions form a chain for the product, which can be tracked. The proposed system involves assigning a QR code to each product, allowing end customers to scan the code and obtain all relevant information about the product.

Whenever a product or brand gains global popularity, it inevitably becomes susceptible to risks such as counterfeiting and duplication, which can damage the company's reputation, revenue, and customer satisfaction. The trade and marketing of fake products are increasing at alarming rates, resulting in negative impacts on companies' sales, reputation, and profits. Additionally, these counterfeit products pose a severe threat to unsuspecting buyers.

To combat the issue of counterfeit goods in the supply chain and ensure their identification and traceability, a complete block chain system has been proposed. This system provides several benefits, including low transaction fees for companies and the assurance that fake products will not be delivered to end-users. Counterfeit product manufacturers pose a significant threat to original manufacturers, who often suffer from brand damage and substantial revenue losses as a result.

A fully functional block chain technology can be utilized to determine the authenticity of a product. Block chain is a series of recorded data that is linked together, making it challenging or impossible to modify or hack the system. Once a product is stored on the network, a hash code is created for it, and all of the product's transaction records can be maintained along with its current owner as a chain is formed for the product's transactions. All of the transaction records are stored as blocks within the block chain.

The manufacturer creates a distinctive QR code or barcode for each product and associates it with the product's pertinent information in this system. End customers can scan this code to obtain complete information about the product. Scanning the QR code or barcode allows users to verify whether the product is genuine or counterfeit.

II. LITERATURE SURVEY

[1] The authors of this paper have introduced digital medical passports (DMP) and immunity certificates to keep track of individuals who have taken COVID-19 tests. They have developed smart contracts using the Ethereum block chain, which have been effectively written and tested. These smart contracts ensure that test-takers have a secure digital medical identity that allows for swift and reliable

ISSN PRINT 2319 1775 Online 2320 7876

Research paper Volume 11, Iss 5, 2022

communication with medical authorities. By leveraging the block chain's immutability, false information can be prevented from spreading, and the response time of medical facilities can be reduced. DMP also plays a vital role in controlling the spread of the disease.

[2] This paper focuses on developing an insurance application that utilizes block chain technology to address industry problems. The goal is to ensure the claim process of insurance companies is transparent, accountable, and secure. Through the use of consensus, every transaction in the claim process is cryptographically signed and recorded as a block in the block chain. This approach ensures the integrity of the claim process and prevents fraudulent activities. A prototype application is created utilizing the IBM block chain platform and its underlying components. The experimental findings show that the suggested implementation can efficiently deter fraudulent claims in the insurance sector.

[3] The main focus of this paper is to assess the effectiveness of block chain technology in the construction industry and determine its potential for adoption by examining real-world cases. The research explores how block chain technology can be incorporated with building information modeling and information management, as well as the potential applications of smart contracts. The study suggests that using block chain technology can significantly improve the effectiveness of construction processes and resolve issues related to trust, transparency, and verification, which are currently common in the industry.

[4] This paper focuses on the problems of ticket fraud and scalping in event ticketing systems, which harm fans financially and create trust issues, particularly in the secondary market. To tackle these problems, various initiatives and publications have proposed the use of block chain technology to ensure ticket authenticity and digital trust. The paper presents a novel strategy for managing end-user digital identity, which is referred to as self-sovereign identity (SSI). The purpose of this approach is to enable control over the secondary market. To create and evaluate an SSI-based event ticketing framework, the authors employ a design science research methodology. The research concludes that utilizing SSI-based event ticketing can aid in regulating the secondary market by implementing the centralized exchange model in practice. The article provides design principles for effective, reliable, and privacy-focused ticket and identity verification, as well as the use of revocation registries, to apply their results to a wider audience.

[5] This paper presents a food safety traceability system that utilizes block chain and EPC Information Services (EPCIS) technology. The authors also create a prototype system and propose management architecture for on-chain and off-chain data to address the challenge of data explosion in the block chain for Internet of Things (IoT). Additionally, the paper outlines an enterprise-level smart contract to prevent data tampering and sensitive information disclosure when participants interact with information. The prototype system is built on the Ethereum block chain.

[6] This paper introduces the Block chain-based Online Education Content Ranking system, which aims to provide an online review and ranking platform with decentralized trustworthiness. The system ensures the reliability of the ratings and the independence and integrity of content reviews by Subject Matter Experts (SMEs).

[7] This paper proposes a decentralized block chain approach to prevent consumers from relying solely on merchants to verify the authenticity of products. The authors outline a block chain system designed for anti-counterfeiting purposes, which allows manufacturers to offer genuine products without the need for direct-operated stores. This approach can significantly reduce the cost of product quality assurance.

[8] This paper provides a review of cloud architecture and identifies different security events that may occur at different cloud deployment models. It also discusses Network Intrusion Detection Systems (NIDS) in the cloud, including their classification, detection approaches, and collaborative NIDSs for block chain applications. The authors highlight how block chain technology can help overcome data privacy and trust management challenges. Additionally, the paper outlines research challenges and suggests future research directions in these areas.

[9] This paper explores a new approach to pharmaceutical governance using IoT and Block chain technology. It proposes using an IoT-based block chain, which is a type of distributed ledger that keeps an unchangeable record of all transaction information that is transparent to all parties involved. By implementing an IoT-based block chain system, the pharmaceutical industry can enhance drug governance throughout the supply chain, resulting in greater efficiency and reliability in healthcare.

[10] The paper aims to address the issue of the technical integration of block chain and cloud computing. It explores three main technical aspects related to this fusion. Firstly, the authors review the emerging cloud-related block chain service model, Block chain –as-a-Service (BaaS). Secondly, they focus on security by assessing access control and searchable encryption schemes. Lastly, the performance of cloud data centers with block chain support is examined from hardware and software perspectives. The paper's findings provide theoretical support for future block chain-enabled reengineering of cloud data centers..

In [11] The paper presents a general outline of a framework for preventing the spread of fake news using block chain technology. It also discusses the different aspects that need to be considered and designed for effectively using block chain to address the issue of fake news.

[12] The paper introduces an innovative supply chain finance platform that utilizes block chain technology to manage the entire process, with the goal of addressing the limitations of the conventional supply chain finance system. The platform resolves trust issues among participants, streamlines the flow of capital and information, lowers costs, and provides superior financial services to those involved in the supply chain. To safeguard user privacy, the paper recommends using homomorphic encryption in the block chain to address the privacy concerns related to sensitive data in supply chain financial situations.

[13] The use of Block chain Technology (BT) in Supply Chain Management System (SCMS) for the automotive components industry is a recently explored research field.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper Volume 11, Iss 5, 2022

Prior studies have concentrated on BT in fields such as virtual currency, security, and Internet of things (IoT). However, the automotive industry has encountered various issues in their SCMS, notably with the abundance of counterfeit components. As a result, Block chain Technology (BT) has been recognized as a promising solution for constructing SCMS for automotive components.

[14] In this paper, the authors aim to comprehensively examine the possible attack surface of Block chain technology, with a particular focus on public Block chains. They identify three contributing factors to attack viability: the cryptographic constructs of the Block chain, the distributed architecture of systems using Block chain, and the application context of Block chain. They explore several types of attacks that can result from these factors, such as selfish mining, DNS attacks, DDoS attacks, , Block chain forks etc.

[15] This paper aims to provide a comprehensive analysis of the potential attack surface of Block chain technology, with a specific focus on public Block chains. The authors identify three critical factors that contribute to the feasibility of attacks on Block chain systems: the cryptographic constructs used in Block chains, their distributed architecture, and the context in which Block chain technology is utilized. The paper explores different types of attacks that could arise from these factors, including selfish mining, DNS attacks, DDoS attacks, Block chain forks etc.

III. PROPOSED SOLUTION

Counterfeit products are becoming a significant issue for manufacturers, consumers, and regulatory authorities. One potential solution to tackle this problem is to use block chain technology. By leveraging block chain, it's possible to create a secure, transparent, and an unchangeable record of a product's journey from manufacturing to the end user. Here, we propose a solution for a system that uses block chain technology to identify fake products:

Stage 1: The Admin need to register themselves in the website by giving their details correctly.

Stage 2: Later, they need to login using their credentials, Admin needs to upload the product details.

Stage 3: Users need to register and login with credentials to view the products.

Stage 4: User should scan the QR code to find whether the product is real or fake.

Constraints of the proposed system:

- High Cost: Implementing a block chain-based product identification system requires significant investment in terms of infrastructure, software development, and maintenance, which may be a barrier for some manufacturers.
- Data Privacy: While block chain technology provides security and transparency, it also raises concerns about data privacy. As all the data is stored on the block chain, it may be accessible to unauthorized parties, and the data privacy laws may not be compatible with block chain technology.
- Scalability: As the number of products increases, the block chain network may become slow, and the transaction processing time may increase.

IV. METHODOLOGY

In this paper, we construct a frontend for a webpage using HTML, CSS, JavaScript and Bootstrap to provide information about products to buyers and sellers. Connect the frontend and backend using the Python programming language to grasp different algorithms and the workings of block chain technology.

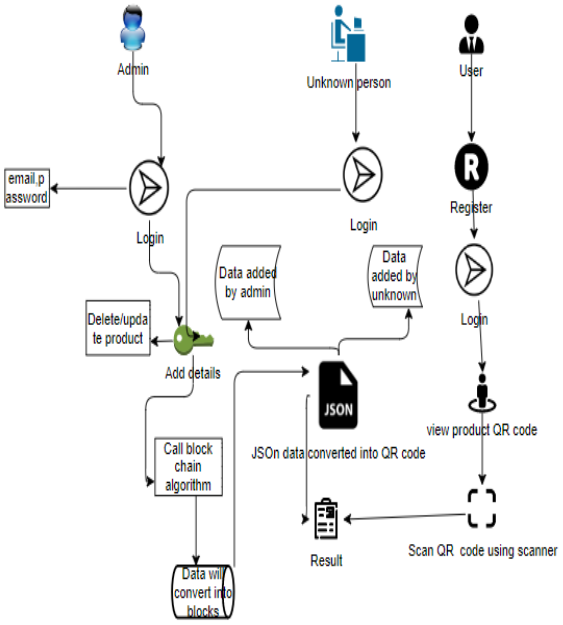

Fig 1: Project Architecture

The following technologies would be used in order to develop this system.

1. Algorithm:

To generate unique hash value for each block during the transaction we used cryptographic hash algorithm called as SHA256.In reality, revealing the originating data from a hash value is practically difficult. Furthermore, due to the astronomical number of possible combinations, a brute force attack is extremely difficult to take place. Furthermore, it is extremely improbable that two data values (known as collision) share the same hash.

2. User Interface (UI):

We design User Interface for adding the products for sellers and viewing the products for buyers:

- HTML, CSS, JAVASCRIPT, BOOTSTRAP for frontend.
- MYSQL, XAMPP and PYTHON for designing and connecting backend.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper Volume 11, Iss 5, 2022

V. RESULT ANALYSIS

We have made use of SHA256 algorithm in this proposed system.

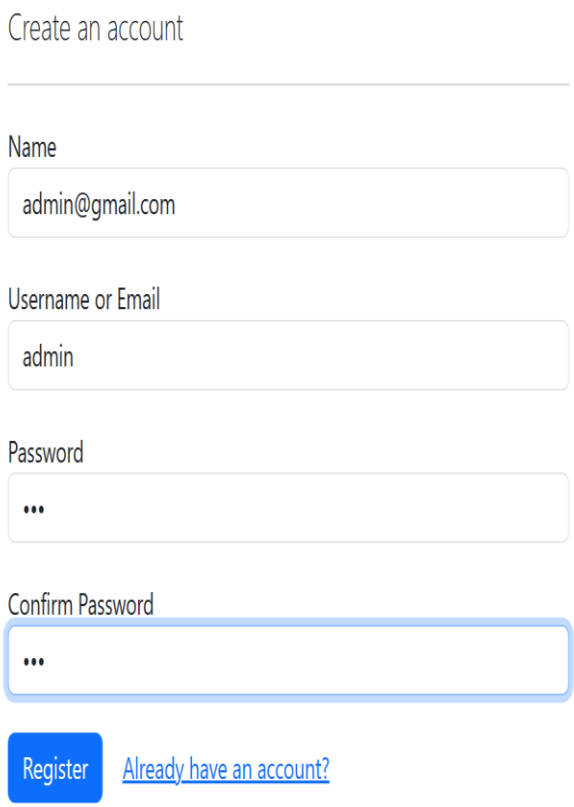

Fig 2: Account creation page

Firstly, Admin and users need to register in the website and then login to their accounts.

While registering in to the website they need to enter the details of his/her name, email id and password.

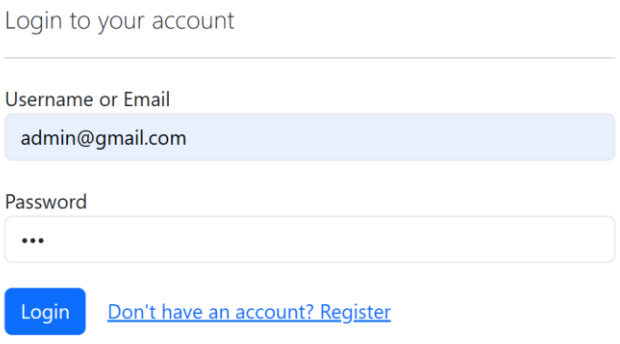

Fig 3: Login page

After registering into the website, need to login by using their credentials of email and password in order to access the website.

If, any unknown person/hacker will login in to the website and add the products that particular product will be marked as fake.

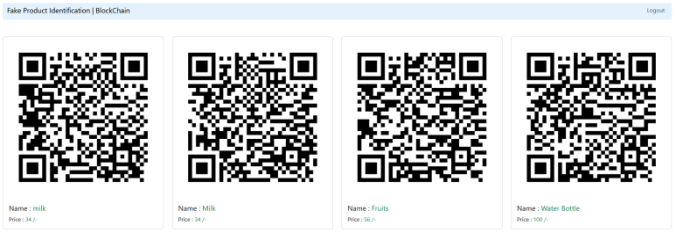

Fig 4: QR codes of the products

Admin can add the products whatever they want, the buyer view the products as per his/her interests.

Buyer can scan the QR code by using any scanner, will get either that particular product is really fake or real.

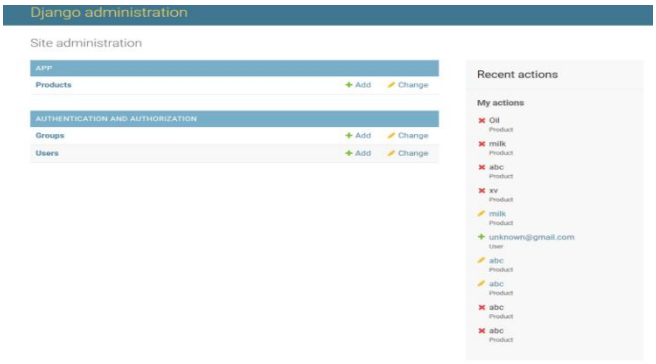

Fig 5: Data Base Page to store the data of the customers and product details

All the data regarding users and products would be stored in this database.

The entire data related to products are associated with the database, which is highly confidential and secure and cannot be altered.

VI. CONCLUSION

As a result, the proposed system can assist end users in detecting fake products in the supply chain. The end user can scan the QR code assigned to a product to obtain all of the information such as Transaction history and current owner information can be used by the end user to determine whether the product is genuine or not. In the future, we will put in place a system that controls and monitors product transportation details.

Block chain technology has proven to be an effective tool for identifying and eliminating counterfeit products from the retail market and supply chain. The proposed system enables users to easily verify and access information about the product they are interested in. This provides users with a greater sense of trust in both the seller and manufacturer, and empowers them to make better purchasing decisions. The use of block chain technology eliminates the need for a third-party verification, resulting in a more seamless and secure experience for users.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper Volume 11, Iss 5, 2022

The use of block chain technology not only helps prevent economic losses due to counterfeit products for manufacturing companies but also allows them to focus on improving their services based on customer feedback. By keeping track of the products released in the market, manufacturers can avoid losses and maintain stability. If block chain technology can establish trust among customers, it has the potential to significantly boost a country's economic growth and prevent fraud-related losses. In summary, block chain technology can serve as a valuable asset for companies, providing a secure and user-friendly trade system.

REFERENCES

[1]. HAYAR.HASAN, KHALEDSALAH, RAJAJAYARAMAN, "Block chain-based Solution for COVID-19 Digital Medical Passports and Immunity Certificates", DOI:10.1109/ACCESS.2020.3043350, IEEE Access, 2020.

[2]. Dr.Jaideep Gera, Anitha Rani Palakayala, "Block chain Technology for Fraudulent Practices in Insurance Claim Process", 978-1-7281-5371-1/20/$31.00 ©2020 IEEE.

[3]. Vincent Hargaden, Nikolaos Papakostas, "The Role of Block chain Technologies in Construction Engineering Project Management", 978-1-7281-3401-7/18/$31.00 ©2019 IEEE.

[4]. Simon Feulner, Johannes Sedlmeir, "Exploring the use of self sovereign identity for event ticketing systems" https://doi.org/10.1007/s12525-022-00573-9 © The Author(s) 2022

[5]. QIJUN LIN, HUAIZHEN WANG, "Food Safety Traceability System based on Block chain and EPCIS", DOI: 10.1109/ACCESS.2019.2897792, IEEE Access 2018.

[6]. Anuj Garg, Sharmila A, "Block chain based online educationcontentranking", https://doi.org/10.1007/s10639-021-10797-5, springer 2021.

[7]. JINHUA MA, SHIH-YA LIN, "A Block chain-Based Application System for Product Anti-Counterfeiting", 10.1109/ACCESS.2020.2972026, IEEE 2020.

[8]. OSAMA ALKADI, NOUR MOUSTAFA, "A Review of Intrusion Detection and Block chain Applications in the Cloud: Approaches, Challenges and Solutions", 10.1109/ACCESS.2020.2999715, IEEE ACCESS 2020.

[9]. Victoria Ahmadi1, Sophia Benjelloun, "Drug Governance: IoT-based Block chain Implementation in the Pharmaceutical Supply Chain", https://doi.org/10.1109/MobiSecServ48690.2020.9042950,IEEE2020.

[10]. Keke Gai, Senior Member, Jinnan Guo, Liehuang Zhu, "Block chain meets cloud computing: A Survey", 1553-877©2020 IEEE.

[11]. Adnan Qayyum, Muhammad Umar Janju, Junaid Qadir, "Using Block chain to Rein in the New Post-Truth World and Check the Spread of Fake News", 1520-9202 2019 IEEE.

[12]. Mingxiao Du, Qijun Chen, "Supply Chain Finance Innovation Using Block chain" 0018-9391 © 2020 IEEE.

[13]. Surjandy, Meyliana, Edi Abdurachrnan, "Block chainTechnology Open Problems and Impact to Supply Chain Management in Automotive Component Industry", 978-1-7281-9189-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICCED51276.2020.9415836.

[14]. Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, "Exploring the Attack Surface of Block chain: A Comprehensive Survey", 1553-877X (c) 2019 IEEE.

[15]. Ye Liu, Xiaoyuan Ma, Lei Shu, "From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges", 1551-3203 (c) 2020 IEEE.