FAKE PRODUCT IDENTIFICATION BY QR CODE USING BLOCKCHAIN

Mrs.S.Suganya[1], G.Bhuvanesh[2], N.Gopinath[3], M.Sharvesh[4]
[1] Assisstant Professor, Department of Information Technology, K.S.R. College of Engineering, Tiruchengode, Tamilnadu, India
[2][3][4] Student, B.Tech-Information Technology, K.S.R. College of Engineering, Tiruchengode, Tamilnadu, India

ABSTRACT

Since the start of Blockchain technology in 2008, its application has expanded across various sectors to ensure reliable and secure data transmission, from its use in Bitcoin to the rise of Blockchain as a Service (BaaS), a modern trend enabling organizations to develop applications on cloud-based networks. Notably, blockchain has been crucial in developing robust applications, with its popularity steadily increasing. It not only addresses the double-spending problem but also independently verifies the accuracy of transactional data. Serving as the foundation of all applications, blockchain technology guarantees data integrity. This study demonstrates the integration of decentralized blockchain technology and supply chain methodologies, showing that end-users no longer solely rely on intermediaries or third parties to confirm product authenticity. This implementation significantly impacts revenue, brand reputation, and profitability. Through a distributed ledger, genuine and counterfeit products can be distinguished. The study introduces an anti-counterfeiting decentralized blockchain solution, empowering manufacturers to deliver authentic goods without direct oversight. This is achieved by authenticating products at each stage of the supply chain. For every product added, a unique QR code is generated and stored in the database, ensuring transparency and traceability throughout the supply chain.

Keywords: Blockchain, Data Transmission, QR Code Scanning, Data Integrity, Fake Product Identification

1. INTRODUCTION

1.1 BLOCKCHAIN

Blockchain technology is a decentralized system that facilitates secure data storage and transmission across a network of interconnected nodes. Its key attributes include decentralization, which eliminates the need for a central authority and enhances security by distributing control among network participants. Transactions recorded on a blockchain are transparent, visible to all participants, fostering trust and accountability. The immutability of data on the blockchain ensures that once recorded, information cannot be easily altered or deleted, thanks to cryptographic hashing and the chain-like structure of blocks.

Security is further bolstered by cryptographic techniques and consensus mechanisms like Proof of Work or Proof of Stake. Additionally, blockchain platforms enable the creation and execution of smart contracts, self-executing agreements that automate transaction processes without intermediaries. With applications spanning industries such as finance, supply chain management, healthcare, and more, blockchain technology holds the promise of revolutionizing data management, offering efficiency, transparency, and security in various contexts.

1.2 DATA TRANSMISSION

Data transmission involves the conveyance of information from one location to another through various mediums such as cables, wireless signals, or optical fibers. It plays a pivotal role in modern communication systems, enabling the exchange of data between devices, networks, and users. Efficient data transmission relies on robust protocols and technologies to ensure reliable and timely delivery of information. With advancements in technology, data transmission has evolved to accommodate increasing data volumes and higher transmission speeds, facilitating real-time communication, multimedia streaming, and remote collaboration. From simple text messages to complex multimedia files, data transmission supports a wide array of applications across industries including telecommunications, internet services, healthcare, finance, and more. Ensuring the security and integrity of transmitted data is paramount, driving the development of encryption techniques and secure communication protocols to protect sensitive information from interception or tampering. As data continues to be the lifeblood of modern society, the optimization of data transmission methods remains a critical focus for researchers and engineers to meet the ever-growing demands of a connected world.

1.3 QR CODE SCANNING

QR code scanning involves the use of a smartphone or a dedicated scanner to capture and interpret Quick Response (QR) codes, which are two-dimensional barcodes containing encoded information. QR codes can store various types of data, including website URLs, contact information, product details, and more. By scanning a QR code using the camera on a mobile device or a QR code scanner application, users can quickly access the embedded information. This technology is widely used in marketing, ticketing, payment systems, inventory management, and other applications where quick access to data is essential. QR code scanning simplifies processes, enhances user experience, and

facilitates seamless interaction between the physical and digital worlds.

1.4 DATA INTEGRITY

Data integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle. It ensures that data remains unchanged and uncorrupted from creation to retrieval, regardless of storage or transmission processes. Maintaining data integrity is crucial for ensuring the trustworthiness of information and making informed decisions based on reliable data. Various measures, such as checksums, cryptographic hashing, error detection, and redundancy, are employed to verify and preserve data integrity. Additionally, access controls and audit trails are implemented to prevent unauthorized alterations and ensure accountability. Data integrity is fundamental in sectors such as finance, healthcare, and critical infrastructure, where the integrity of data is paramount for compliance, security, and operational efficiency.

1.5 FAKE PRODUCT IDENTIFICATION

Identifying fake products involves the process of verifying the authenticity of goods to distinguish genuine items from counterfeit or fraudulent ones. This task is crucial in combating the proliferation of counterfeit products, which pose significant risks to consumer safety, brand reputation, and revenue streams for businesses. Various methods, including visual inspection, authentication technologies, and blockchain-based tracking systems, are utilized to detect counterfeit products. These methods often involve examining packaging, labels, serial numbers, and security features to identify discrepancies or anomalies that may indicate a product's authenticity. Additionally, digital solutions such as QR codes, RFID tags, and unique identifiers enable consumers and authorities to verify product authenticity through mobile applications or online databases. By implementing robust anti-counterfeiting measures, businesses can protect their brand integrity and ensure consumer trust while mitigating the harmful impacts of counterfeit goods on the market.

2. LITERATURE REVIEW

Swaroop Jambhulkar [1] et.al has propose in this paper In supply chains, counterfeit products are prevalent, necessitating a system for end-user verification of product details to ensure authenticity. Counterfeiting adversely affects company reputation, sales, and profits. Blockchain technology, a distributed, decentralized ledger, is employed to authenticate genuine products and detect counterfeits. Its immutability ensures data security, allowing users to independently verify

product authenticity without third-party confirmation. QR codes are utilized to combat counterfeiting, linking product codes to the blockchain and enabling users to input unique codes for verification. If a match is found, product information is provided; otherwise, the product is deemed counterfeit.

T.Shreekumar [2] et.al proposed in this paper The production and distribution of counterfeit goods pose significant financial, health, and safety risks to consumers and businesses alike. These threats include revenue loss, damage to brand reputation, increased expenses for replacements, and erosion of trust among partners. To address these challenges, a blockchain-based system is utilized to authenticate genuine products and identify duplicates. Leveraging emerging wireless technologies such as QR codes and barcodes, this system offers a robust solution to combat counterfeiting. By linking product codes to a blockchain database, unique identifiers are generated and stored for each item. Customers can verify product authenticity by scanning the QR or barcode with a camera. If a match is found, the customer receives confirmation of the product's authenticity. Conversely, if no match is detected, both the customer and the manufacturer are notified, facilitating action against counterfeit products. This approach empowers consumers to independently verify product authenticity, reducing reliance on merchants.

Vaishnavi Vishwasrao [3] et.al proposed in this paper Counterfeit goods present significant challenges for manufacturers, impacting brand reputation, revenue, and profitability. Blockchain technology enables real-product authentication and counterfeit detection by maintaining a secure, decentralized digital ledger across interconnected databases. By leveraging Quick Response (QR) codes, a widely adopted wireless technology, this system links product codes to the blockchain, facilitating counterfeit identification. QR code scanners can verify product authenticity by comparing unique codes stored in the blockchain database. If a match is found, customers are notified of the product's authenticity; otherwise, they are alerted to the presence of counterfeit goods. This approach empowers consumers to independently verify product legitimacy, reducing reliance on third-party validation.

Tejaswini Tambe [4] et.al proposed in this paper Counterfeit products have significantly impacted manufacturing industries, affecting company reputation, sales, and profits. Blockchain technology is employed for authenticating genuine products and detecting counterfeit ones. Blockchain operates as a secure,

distributed, and decentralized digital ledger, storing transactional data in interconnected databases. With the use of Quick Response (QR) codes, a prevalent mobile and wireless technology, counterfeit products can be identified by linking QR codes to the blockchain. This system records product details and generates unique codes stored as blocks in the database. Users input their unique code, which is then compared against entries in the blockchain database. If a match is found, customers receive a notification confirming product authenticity; otherwise, they are alerted to the presence of counterfeit goods.

Aadeesh Bali [5] et.al proposed in this paper Challenges in today's retail market include the widespread counterfeiting of products, often low-quality replicas of genuine brands. Various methods have been utilized to combat counterfeiting, such as RFID tags, artificial intelligence, and QR code systems, but each has drawbacks. In this project, we aim to enhance fake product detection using blockchain technology. Our approach involves storing product supply chain data at each transaction stage using QR codes, leveraging blockchain's decentralized nature to ensure data security and integrity, thereby preventing tampering by third parties.

Kishan Tiwari [6] et.al proposed in this paper Counterfeit products pose a growing concern for businesses and consumers, jeopardizing company reputation, financial stability, and consumer well-being. Blockchain presents a decentralized and secure solution for verifying product authenticity, empowering consumers to detect and avoid counterfeit goods easily. This paper explores blockchain's role in fake product identification, proposing a system utilizing smart contracts to automate verification. Manufacturers can register products on the blockchain, assigning each item a unique digital identity accessible through QR code scanning. We discuss blockchain's benefits, including enhanced transparency, fraud reduction, and consumer trust improvement, while also addressing implementation challenges like scalability and interoperability. In conclusion, blockchain technology offers a reliable means to combat counterfeit goods, safeguarding both businesses and consumers.

3. EXISTING SYSTEM

In the current system, QR codes for products are generated with strong security measures, but storing rating data proves problematic. This flaw allows fake reviews to proliferate, damaging trust in the product rating system. Without proper storage and analysis of rating data, it's challenging to

differentiate between authentic and fraudulent reviews. Consequently, the system fails to identify patterns of fake review postings, leaving it vulnerable to manipulation. While the emphasis on security in QR code generation is commendable, the oversight in rating data storage undermines the credibility of the product rating system. Fake reviews can deceive consumers and tarnish a product's reputation, posing a significant threat to trust and transparency in the online marketplace. Without mechanisms to detect irregularities in review postings, the system remains susceptible to exploitation by malicious actors. Addressing these challenges requires a multifaceted approach. Improving data management infrastructure is crucial for storing and analyzing rating data effectively. Additionally, implementing advanced algorithms and analytical tools can aid in identifying and mitigating fraudulent review postings. By bolstering the system's resilience against manipulation, stakeholders can foster a more trustworthy online marketplace environment for both consumers and businesses.

4. PROPOSED SYSTEM

In the proposed system, blockchain technology is utilized to combat counterfeit products effectively. Initially, all manufacturers are brought onto the blockchain network, enabling the collection of detailed product information. User reviews and ratings serve as key indicators for identifying fake products within specific blocks of the blockchain. By cross-referencing this feedback with authenticated product data, the system detects discrepancies that may signal counterfeit goods, empowering consumers with valuable insights and protection. Blockchain technology ensures higher performance through decentralization, resilience against tampering, and real-time transparency. Its decentralized nature eliminates single points of failure, while the distributed consensus mechanism ensures trust and integrity. Immutable records prevent unauthorized alterations, enhancing system reliability and deterring fraud. Automated enforcement via smart contracts streamlines processes and improves scalability. Furthermore, blockchain enables comprehensive visibility and traceability throughout the product lifecycle, facilitating proactive risk mitigation. In summary, the proposed system leverages blockchain's strengths to combat counterfeit products effectively. By integrating manufacturers onto the blockchain network and analyzing user feedback, it enhances transparency and empowers consumers with trustworthy information. Through decentralization, immutability, and transparency, this

innovative approach ensures a safer and more reliable marketplace for all stakeholders.

5. MODULE DESCRIPTIONS

5.1 PRODUCT REGISTRATION PROCESS

In the product registration process, manufacturers play a pivotal role as the initial owners, initiating the integration of products into the blockchain ledger. This involves adding essential product details to the blockchain database and assigning a unique QR code to each item. The QR code serves as a gateway for updating and accessing product information securely within the blockchain. With each product registered, a comprehensive record is established, encompassing key attributes such as production data and authentication details. Through cryptographic measures, the integrity of these records is ensured, guarding against tampering or unauthorized alterations. By leveraging blockchain technology and QR codes, this streamlined approach not only enhances transparency and accountability but also empowers consumers with verified and trustworthy product information, ultimately fostering greater confidence and trust within the marketplace.

5.2 DISTRIBUTOR CHAINS

In the subsequent phase of the process, once the manufacturer has shipped the product to the distributor, a critical handover occurs in the supply chain. Upon receiving the product, the distributor undertakes the task of updating the blockchain ledger to reflect the transfer of ownership and other pertinent details. This involves scanning the QR code affixed to the product, which serves as a key access point to the blockchain network. Through this scan, the distributor adds a new chain of information, including their identity, timestamp, and date of receipt. By appending these details to the existing blockchain record, a seamless transition of ownership is recorded in real-time, ensuring transparency and accountability throughout the supply chain. Additionally, this process enhances traceability, allowing stakeholders to track the product's journey from manufacturer to distributor with precision and accuracy. Ultimately, the integration of blockchain technology facilitates efficient and secure data management, bolstering trust and confidence among all parties involved in the product distribution process.

5.3 RETAILER CHAINS

Upon reaching the retailer, the product

undergoes another pivotal transition within

the supply chain. As the retailer takes possession of the product from the distributor, a crucial step ensues in updating the blockchain ledger to reflect the change in ownership. Utilizing a QR code scanner, the retailer accesses the blockchain network by scanning the unique QR code assigned to the product. This scan initiates the addition of a new chain of information, specifically detailing the retailer's identity and ownership of the product. Alongside these details, the retailer includes a timestamp, providing a precise record of when the product was received. By appending this information to the existing blockchain record, the retailer seamlessly integrates their ownership into the product's history, ensuring transparency and accountability throughout the distribution process. Moreover, this step enhances traceability, enabling stakeholders to monitor the product's journey from manufacturer to distributor to retailer with utmost accuracy and confidence. Through the utilization of blockchain technology, the product distribution process is fortified with efficiency, security, and trust, thereby fostering a robust and reliable ecosystem for all involved parties.

5.4 END USER

Upon reaching the end of the distribution chain, the product is finally in the hands of the customer, marking the culmination of its journey from manufacturer to retailer. At this juncture, the customer plays a pivotal role in accessing comprehensive information about the product's history and provenance. Utilizing a website interface, the customer uploads the QR code associated with the product, initiating a query to the blockchain network. Through this process, the customer gains access to a wealth of detailed information, spanning from the manufacturer's origin data to the latest retailer's ownership details. This transparent and accessible data enables the customer to make an informed decision about the product's authenticity, quality, and journey within the supply chain. Armed with this knowledge, the customer retains agency over their purchasing choice, empowered to either proceed with the transaction or explore alternative options based on their preferences and considerations. Ultimately, this integration of blockchain technology and QR code tracking revolutionizes the customer experience, fostering trust, transparency, and informed decision-making within the marketplace.

6. ALGORITHM

6.1 SHA256 ALGORITHM

The SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed-size 256-bit (32-byte)

hash value. It's widely used in various security applications and protocols like SSL/TLS, PGP, SSH, Bitcoin, etc. Here are the steps involved in the SHA-256 algorithm:

Step 1:

Padding: The input message is padded so its length is congruent to 448 modulo 512. Padding is done by appending a single '1' bit, followed by '0' bits, and finally the length of the original message in bits (as a 64-bit big-endian integer).

Step 2:

Initialization: Initialize the hash buffer with the initial hash values, known as the initial hash buffer (H), which are defined by the first 32 bits of the fractional parts of the square roots of the first 8 primes (2 through 19):

H0 = 0x6a09e667

H1 = 0xbb67ae85

H2 = 0x3c6ef372

H3 = 0xa54ff53a

H4 = 0x510e527f

H5 = 0x9b05688c

H6 = 0x1f83d9ab

H7 = 0x5be0cd19

Step 3:

Processing: The message is processed in 512-bit blocks. Each block goes through 64 rounds of processing.

Step 4:

Message Schedule: The 512-bit block is split into sixteen 32-bit words. For the next 48 rounds, new 32-bit words are computed based on the original 16 words.

Step 5:

Compression Function: The compression function combines the current hash value

(H) with the processed block. Each round involves a series of logical functions and bitwise operations (such as AND, XOR, NOT, etc.).

Step 6:

Finalization: After processing all blocks, the final hash value is generated by concatenating the 8 32-bit hash values produced in the last block.

Step 7:

Output: The final 256-bit hash value is obtained, representing the cryptographic hash of the input message.

These steps ensure that the SHA-256 algorithm produces a fixed-length hash value that is unique to the input message and is highly resistant to collisions and reverse engineering.

6.2 PSEUDO CODE

function verifyProductQRCode(qrCodeData, expectedHash):

// Extract data from QR code

productData = decodeQRCode(qrCodeData)

if productData is null or empty: return "Invalid QR code"

// Extract hash from product data qrHash = productData.hash

// Compute hash of remaining data

remainingData = concatenateDataExceptHash(productData)

computedHash = SHA256(remainingData)

// Compare computed hash with hash extracted from QR code

if computedHash == qrHash and qrHash == expectedHash:

return "Product is authentic" else:

return "Product is not authentic"

7. RESULT ANALYSIS

ALGORITHM	ACCURACY
Existing	**85**
SHA256 Algorithm	**96**

Table 1. Comparison Table

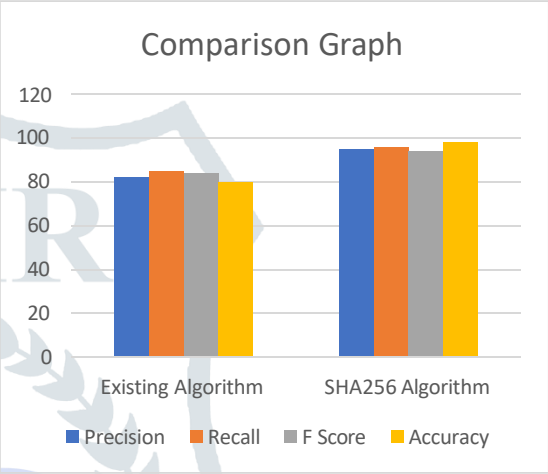

Figure 1. Comparison Graph

The paper compares the performance of an existing algorithm with a new one, introducing a fresh approach to detect fake products. The suggested algorithm achieves a higher accuracy rate of 96%, compared to the existing algorithm's 80% accuracy rate. By utilizing SHA256 algorithm and taking into account dynamic parameters like response time variability and system predictability, the suggested methodology is able to quantify and anticipate harmful online service behavior with a 5% increase in accuracy. To evaluate the suggested algorithm's practical applicability and flexibility in the face of changing risks, however, is still necessary.

8. CONCLUSION

Amidst the surging online market, the increase of imitations is a significant issue. To combat this, blockchain technology emerges as a key tool. By encoding extensive product details into QR codes, consumers gain the ability to authenticate products through scanning. This innovative approach utilizes blockchain's unchangeable ledger to store product data as blocks, enabling transparency and traceability throughout the supply chain. Our proposed solution offers a reliable means to differentiate genuine products from imitations. By scanning the QR code associated with a product, consumers gain access to its entire supply chain history recorded on the blockchain. This ensures that end-users can make informed decisions regarding product authenticity, enhancing consumer trust and guarding against counterfeit practices. Through the integration of blockchain technology and QR code scanning, our system empowers consumers with the knowledge needed to address the proliferation of imitations in the market.

9. FUTURE WORK

In upcoming endeavors, objectives include implementation of methods using varied algorithms to improve efficiency. By utilizing different algorithms, performance can be compared across real-time data sets to gauge effectiveness. This comparative assessment aids in understanding strengths and weaknesses, enabling optimization for better outcomes. Through iterative approaches, refinement is sought in methodology for superior results in identifying counterfeit goods. Real-time datasets offer insights into algorithmic effectiveness in practical scenarios, supporting data-driven decision-making. Additionally, this analysis helps identify suitable algorithms for specific use cases, ensuring adaptability and scalability of the solution. Dedication to leveraging diverse algorithms and analyzing real-time data highlights commitment to developing a robust system for countering counterfeit products. Continuous refinement and innovation aim to remain at the forefront of anti-counterfeiting technology, providing reliable means for product authentication and combating fraudulent practices.

10. REFERENCES

[1] Yildiran Yilmaz, Viet-Hoa Do and Basel Halak, “ARMOR: An anti- counterfeit security Mechanism for low cost Radio frequency identification systems”, 2021.

[2] Wenzheng Li and Mingsheng He, “Comparative Analysis of Bitcoin, Ethereum, and Libra,” 2020.

[3] N. Alzahrani, "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain," 2018.

[4] Hao Shen1, Keren Liu1, Yuxuan Yao, Jun Wang, An ADS-B Anti-counterfeiting System Based on TDOA, IEEE International Conference on Signal, Information and data Processing in 2019".

[5] Ahmad Sghaier Omar, Otman Basir, Smart Phone Anti-counterfeiting System Using a Decentralized Identity Management Framework, in year 2019.

[6] S. M. English and E. Nezhadian, "Application of bitcoin datastructures design principles to supply chain management," arXiv preprint arXiv: 1703.04206, 2017.

[7] Chen Fangfang, Cao Peng, Zhu Jianle, Wang Xuan, Research on Anti- counterfeiting Image Generation Algorithm Based on Halftone-Micro-Character, in year 2018.

[8] DR. GAVIN WOOD, Thereum: A Secure Decentralised Generalised Transaction Ledger, in year 2020

[9] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, "Adept: An iot practitioner perspective," DRAFT COPY FOR ADVANCE REVIEW, IBM, 2015.

[10] V. Buterin et al., "Ethereum white paper," GitHub repository, 2013. [6] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.