iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50151

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Mitigating Counterfeiting Using Blockchain Enabled Product Authentication

Harsha Vardhan V[1], Rohan L[2], Aditya Reddy K[3], Murlidher Mourya[4]
[1, 2, 3]*Student,* [4]*Assistant Professor, Department of Computer Science & Engineering, Vardhaman College of Engineering, Hyderabad, India*

Abstract: ***Counterfeit goods pose a significant challenge to businesses, particularly those involved in the production and sale of high-value items. Traditional methods of product verification have limitations and often fail to detect counterfeit products quickly and efficiently. The emergence of blockchain technology offers a promising solution to this problem, allowing for the creation of a secure and transparent system for product authentication and tracking. Blockchain technology leverages a decentralized and tamper-proof ledger to enable product verification and tracking across the supply chain. By using blockchain, businesses can establish a system that verifies the authenticity of products from the point of manufacture to distribution and beyond. This can help businesses combat the production and sale of counterfeit goods. To implement blockchain technology for product verification and counterfeit removal, technical expertise is required. This involves creating a blockchain-based system that can uniquely identify each product, developing secure networks of nodes to maintain the blockchain, and creating smart contracts to automate the verification process. By adopting blockchain technology for Products Authentication and counterfeit Elimination, businesses can benefit from increased customer trust, brand reputation protection, and reduced risk of health and safety hazards associated with counterfeit goods. Ultimately, the implementation of blockchain technology offers a more efficient and effective solution to the problem of counterfeit goods, benefiting businesses, customers, and the economy.***
Keywords—Product Authentication, Decentralized ledger, Secure system, Smart Contracts, Tamper-Proof

I. INTRODUCTION

In recent years, blockchain technology has emerged as a promising solution to address the problem of counterfeit products [1]. Blockchain is a decentralized and distributed digital ledger that allows multiple parties to store and access data in a secure, transparent, and immutable manner [2]. Each block in the blockchain contains a cryptographic hash of the previous block, forming a chain of blocks that cannot be altered once added [3]. This makes blockchain an ideal technology for product authentication and counterfeits elimination, as it provides a tamper-proof and transparent system for tracking and verifying goods throughout the supply chain [4]. Blockchain-based authentication systems can be used to ensure the authenticity of goods at every stage of the supply chain, from production to distribution and beyond [5]. These systems use digital tokens or smart contracts to create a unique identity for each product, which is stored on the blockchain [6]. This identity can be used to verify the product's authenticity by scanning a code or accessing the blockchain directly [7]. This ensures that only genuine products are sold to consumers, while counterfeit products can be easily identified and eliminated. Furthermore, blockchain technology can be used to address other issues related to product authentication and counterfeits elimination, such as supply chain visibility, transparency, and traceability [8]. By providing a shared and immutable ledger, blockchain enables all parties involved in the supply chain to access and share real-time data on the movement of goods [9]. This improves supply chain efficiency, reduces costs, and enhances trust between parties, which can further reduce the risks associated with counterfeits. The potential of blockchain-based product authentication and counterfeits elimination systems has been widely recognized in both academic and industry circles. Researchers have proposed various models and frameworks for implementing these systems, and several pilot projects and commercial deployments have been launched in recent years. For example, Walmart, the world's largest retailer, has implemented a blockchain-based product tracing system that allows for the real-time monitoring of food products, reducing the time it takes to track the source of contaminated products from weeks to seconds [10]. In another example, IBM has launched a blockchain-based platform that enables companies to verify the authenticity of diamonds, reducing the risk of purchasing conflict diamonds [11]. Notwithstanding the potential advantages of blockchain technology for product identification and preventing counterfeits, there are still several issues that need to be resolved. These include technical issues such as scalability, interoperability, and privacy, as well as legal and regulatory challenges related to the adoption of blockchain-based authentication systems.

II. LITERATURE SURVEY

Blockchain technology can be used for product authentication by creating a unique digital identity for each product. The digital identity can include information about the product, such as its origin, manufacturing date, and batch number. The digital identity is then stored on the blockchain, providing a secure and transparent record of the product's journey through the supply chain. By generating a safe and transparent record of each product's travel through the supply chain, blockchain technology can aid in the prevention of counterfeit goods.

Each product's digital identity is verified at each stage of the supply chain, providing an end-to-end traceability and authenticity of the product. Several studies have explored the usage of blockchain technology for product authentication and counterfeits elimination. For example, [12] proposed a blockchain-based solution for product authentication and counterfeits elimination in the pharmaceutical industry.

The proposed solution uses a combination of blockchain technology, QR codes, and Near Field Communication (NFC) to create a tamper-proof and transparent record of each pharmaceutical product's journey through the supply chain. Another study by Li et al [13] explored the usage of blockchain technology for food safety and traceability.

The authors proposed a blockchain-based solution that provides end-to-end traceability of food products, enabling consumers to verify the authenticity of the food products.

Track and trace technologies, such as Electronic Product Codes (EPCs), barcodes, and Radio Frequency Identification (RFID) tags, are widely used to monitor and trace products. Manufacturers include a tag or barcode, which allows for easy identification and tracking of the product.

This helps in reducing counterfeits by providing a product's history. The distributors can scan the identification, authenticate the product, and update its status. Similarly, retailers can also scan the product to check its history and authenticity. By enabling tracking and tracing of products throughout their lifecycle, this method addresses the issue of counterfeiting while enhancing supply chain visibility.

III. EXISTING SYSTEM

The reliance on physical security features alone is a major limitation of the existing system for product authentication and counterfeit elimination.

These features can be easily replicated or tampered with, which makes it easier for counterfeiters to produce convincing fakes. Additionally, the verification process for physical security features can be time-consuming and costly for both manufacturers and consumers.

Furthermore, the traditional system is not reliable, as it is vulnerable to human error, and the authenticity of a product can be difficult to verify when it moves through multiple parties. Moreover, the lack of a centralized system makes it difficult to track the movement of products from the manufacturer to the end-user.

This can make it challenging to identify when and where counterfeit products are introduced into the supply chain. In addition, the existing system is not very efficient, and it is often difficult to establish a secure and trustworthy communication between different stakeholders.

IV. PROPOSED SYSTEM

The proposed system utilizes blockchain technology to create a tamper-proof and secure system for authenticating products. Blockchain technology offers a decentralized, distributed database that can be used to store information in a secure and transparent manner. Proposed system consists of three main components: the user interface, the smart contract, and the blockchain network. The user interface is the front-end of the system that provides a user-friendly interface for users to interact with the system. The smart contract is the code that executes the business logic of the system, and the blockchain network is the underlying infrastructure that stores and validates the data.

The user interface component of the system architecture is responsible for providing a user-friendly interface for users to interact with the system. The user interface can be web-based, mobile-based, or a combination of both. The user interface provides various features such as product search, product tracking, product verification, and transaction history. Users can search for products by entering the product name, brand, or serial number. Once a product is found, users can track the product through the supply chain and verify its authenticity. The user interface also provides a transaction history that shows all the transactions related to a specific product.

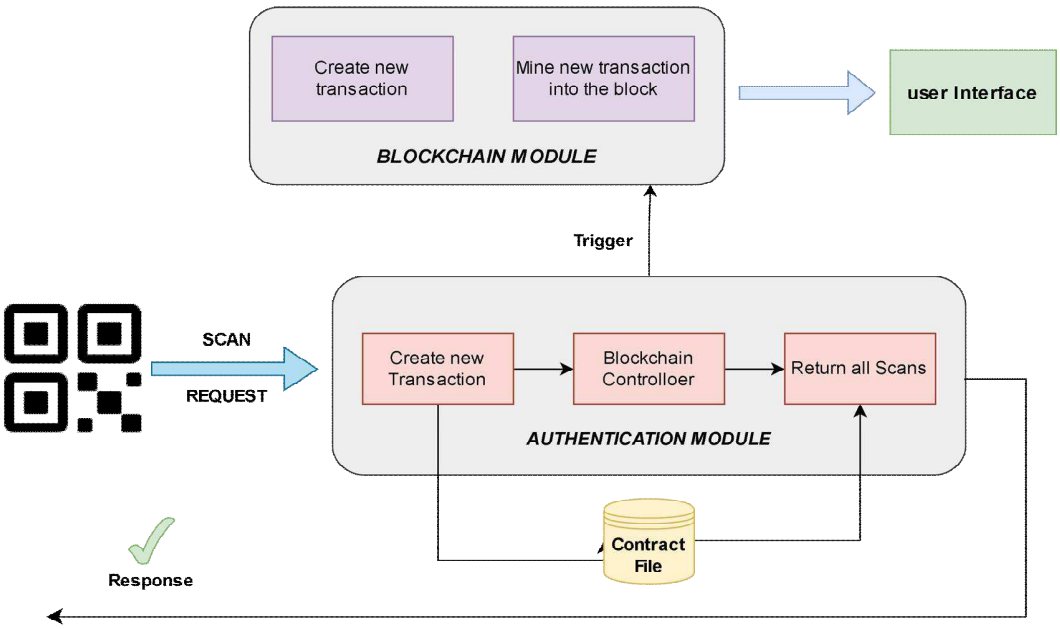


Fig. 1 Proposed System

The smart contract component of the system architecture is responsible for executing the business logic of the system. The smart contract is a self-executing code that runs on the blockchain network. The smart contract is responsible for storing and enforcing the rules and regulations of the product authentication and counterfeit elimination system. The smart contract is written in a programming language such as Solidity and is stored on the blockchain network. The smart contract includes the terms and conditions of the product authentication and counterfeit elimination system, such as the rules for product verification, product tracking, and transaction validation. The blockchain network component of the system architecture is responsible for storing and validating the data. The blockchain network is a decentralized and distributed database that stores all the information related to the product authentication and counterfeit elimination system. The blockchain network consists of a network of nodes that validate and record transactions on the network. Each node on the blockchain network has a copy of the blockchain ledger, which is a complete history of all the transactions that have occurred on the network. The blockchain network ensures that the data stored on the network is tamper-proof and transparent. The product authentication and counterfeit elimination system using blockchain can be deployed in a variety of industries, including pharmaceuticals, luxury goods, electronics, and food products. The system architecture provides a secure and transparent platform for tracking products throughout the supply chain, enabling authentication and identification of counterfeit products.

A. Hashing

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed-length output (Hash) of 256 bits for any input message, regardless of its size or type. SHA-256 works by processing the input message in blocks of 512 bits, padding the message if necessary, and then applying a series of mathematical operations that transform the input into a fixed-size output. This implemented algorithm uses a set of constants and functions, such as logical AND, OR, and XOR operations, as well as modular arithmetic and bitwise rotations, to process the input data and generate the output digest. SHA-256 working involves several stages, including message padding, message expansion, round function computation, and finalization. In the padding stage, the input message is padded with zeros and a one-bit to ensure that the message length is a multiple of 512 bits. Then, the message is divided into 512-bit blocks, and each block undergoes a message expansion process that generates 64 32-bit words from the original 16 32-bit words. These words are then used in the computation of a series of round functions that transform the input block through a series of nonlinear operations. The final output digest is generated by combining the results of the last round function applied to the final block with a set of constants.

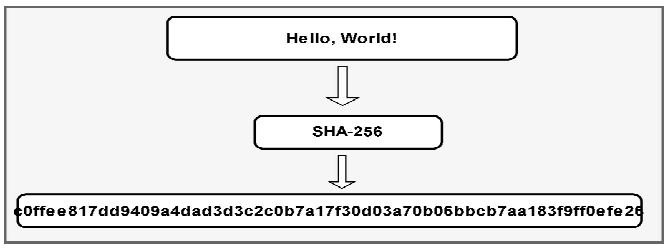


Fig. 2 Hash Value

B. Digital Signature

A digital signature is used to ensure the authenticity and integrity of the product information stored in the QR code. A digital signature is a cryptographic technique that allows the recipient of a message to verify the authenticity of the sender and that the message has not been tampered with during transmission. The digital signature in this code is formed by generating a hash of the product information, and then encrypting the hash. The resulting encrypted hash is then embedded in the QR code along with the product information. The Authentication module in this system allows the user to authenticate a product by selecting the product barcode image. The barcode is hashed using sha256, and the digital signature is compared with the digital signature of the barcode stored in the blockchain. If the digital signatures match, the product is considered authentic, and a message is displayed in the text box. If the digital signatures do not match, the product is considered counterfeit, and a message is displayed in the text box. This digital signature system helps with the authentication of the products by ensuring that only trusted sources can sign the product information. It also helps to eliminate counterfeits by making it more difficult for counterfeiters to replicate the digital signature and sign fake product information.

C. Proof of Work (PoW)

Proof of Work (PoW) is a consensus mechanism used in blockchain networks to validate transactions and create new blocks. In PoW, a node, known as a miner, needs to solve a cryptographic puzzle, also known as a hash puzzle, to add a new block to the blockchain. The puzzle is designed to be computationally difficult and requires a significant amount of computational power to solve. Once the puzzle is solved, the miner broadcasts the new block to the network for verification. In this project implementation, difficulty is a class variable of the Blockchain class, which is set to 2. This difficulty level represents the level of complexity required to add a new block to the blockchain by solving a proof-of-work problem. In the proof-of-work algorithm, a certain number of leading zeros are required in the hash of a block to make it valid, and the difficulty level represents the number of leading zeros required. Setting the difficulty level to 2 means that the proof-of-work algorithm requires a hash that starts with two leading zeros for a new block to be added to the blockchain. This makes the computation of the proof-of-work problem more difficult, as the probability of a hash starting with two leading zeros is lower than the probability of a hash starting with one leading zero. A higher difficulty level would make the computation even more difficult. Setting this higher difficulty level in the proof-of-work algorithm makes it harder to add new blocks to the blockchain, which increases the security of the blockchain. This is because it requires more computational power to add new blocks, which makes it more difficult for attackers to take over the network by creating fraudulent blocks.

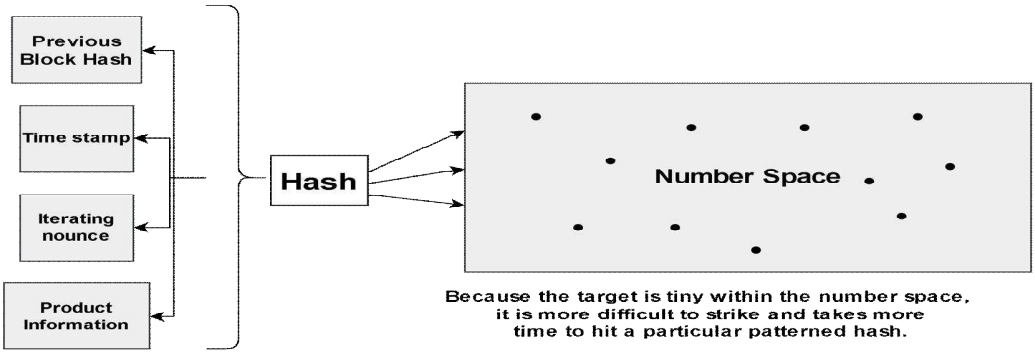


Fig. 3 Proof of Work

V. IMPLEMENTATION & RESULTS

Firstly, when a product is manufactured, it is assigned a unique digital signature that is recorded on the blockchain. This digital signature is generated using cryptographic algorithms and is unique to each product, ensuring that it cannot be duplicated or forged. As the product moves through the supply chain, each transaction is recorded on the blockchain, along with the unique digital signature of the product. This information is stored in a distributed ledger, which is tamper-proof and transparent, providing a verifiable record of the product's movement and authenticity. The graphical user interface is created with CustomT Kinter, a Python GUI package. This widget is made up of four fields: Product ID (strictly numeric) refers to the number issued to the product in order to quickly access the product and is unique to the product, followed by the product name, Company/User data, and address, all of which are alphanumeric.

1) Saving Product with Blockchain Entry is linked with addproduct () function in the backend that handles the submission of a product form in a blockchain-based application. The function checks if all the required input fields are filled, and if so, it performs various validations and operations on the submitted data. If all input fields are valid, the function generates a digital signature for a selected QR code image file and creates a new transaction with the product details, including the digital signature. The transaction is then added to the blockchain, and the blockchain is mined to generate a new block.

2) The output in the front end is a message indicating whether the product form submission was successful or not, as well as any relevant error messages that may have been triggered during validation. The text area in the user interface should also be updated with the relevant blockchain and digital signature information.

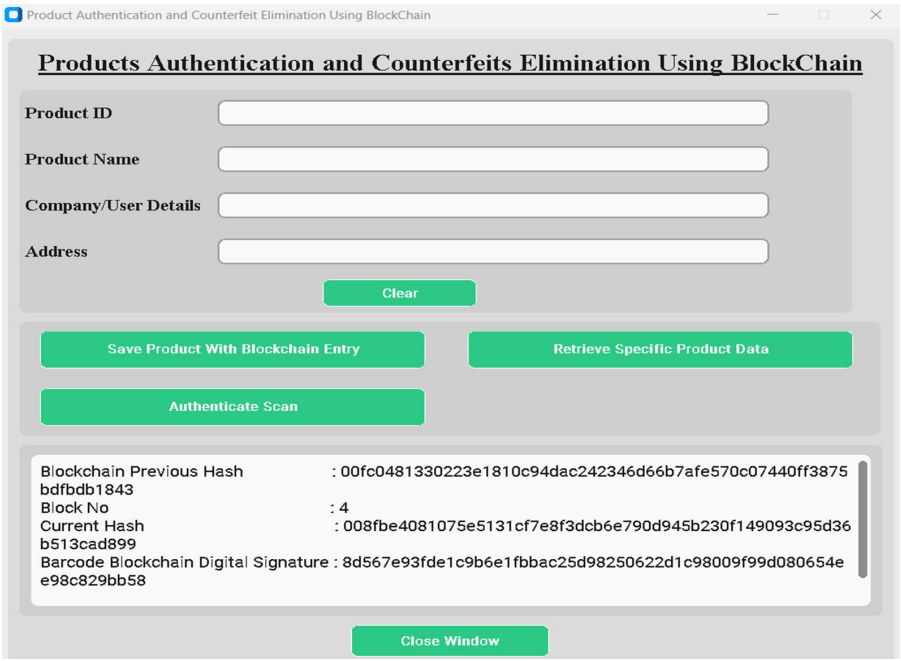


Fig. 4 Saving Product with Blockchain Entry Result

3) Authenticate Scan is linked with authenticateProduct () function that takes care of authenticating a product by scanning its barcode. When called, the function opens a file dialog box, allowing the user to choose an image file of the barcode. The function then checks if the file is a PNG, JPEG, or JPG file, and if so, reads the image and decodes the QR code using OpenCV's QRCodeDetector. If the QR code is successfully decoded, the function searches the blockchain for a transaction that matches the product's digital signature, which is computed using SHA-256. If a matching transaction is found, the function displays the details of the product in a text area, including the product ID, name, company or user details, address details, scan date and time, and digital signature. If no matching transaction is found, the function displays a message in the text area indicating that the product authentication failed. In the event of an error, such as an invalid file or an exception, the function displays an error message. Overall, the authenticateProduct () function provides a way to authenticate a product using its barcode and the blockchain, giving users greater confidence in the authenticity of the products they purchase.

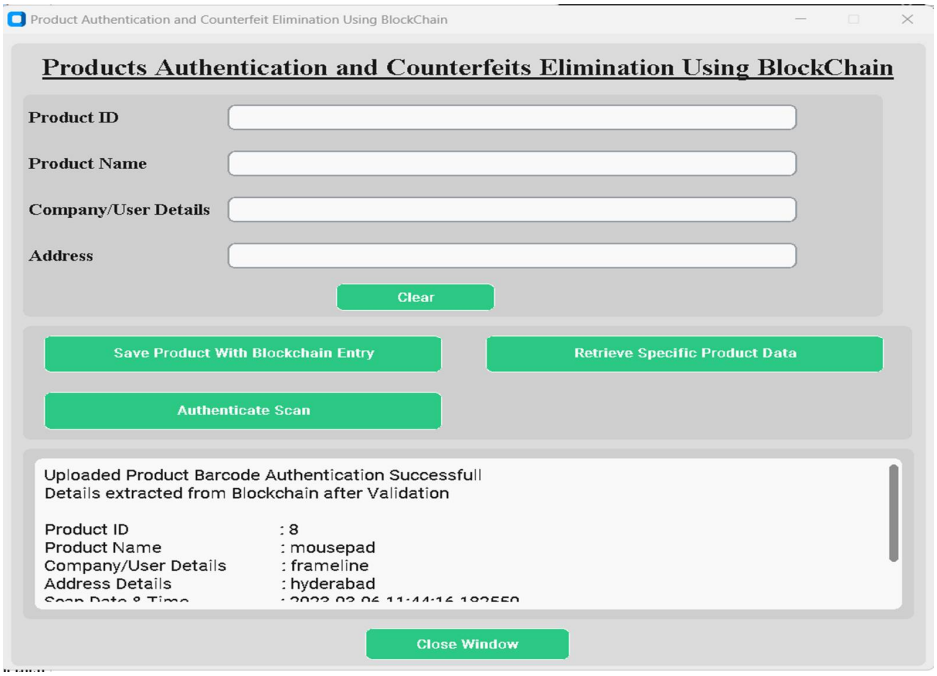


Fig. 5 Authenticated Scan

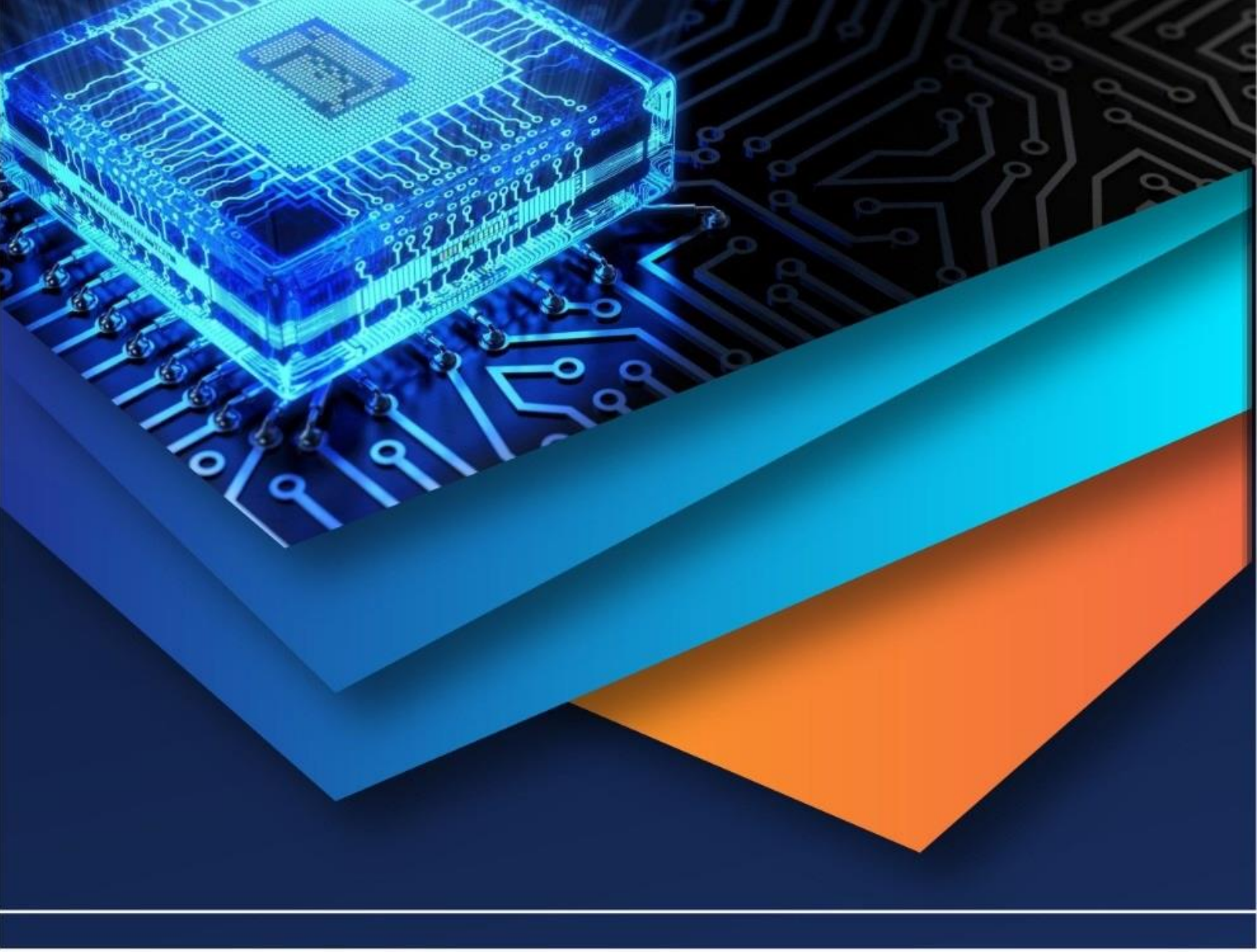
VI. CONCLUSION AND FUTURE SCOPE

In conclusion, the blockchain-based supply chain management system developed provides an efficient, transparent, and secure way of tracking and managing the supply chain of products. The use of blockchain technology has the potential to transform the supply chain industry, enabling faster, more efficient, and cost-effective supply chain management. This work showcases the immense potential of blockchain technology and how it can be leveraged to bring about transformative changes in various industries. By incorporating real-time tracking, the system could provide enhanced transparency to all stakeholders in the supply chain. Manufacturers and distributors would be able to track the movement of products in real-time, providing valuable insights into the overall supply chain. This would lead to better inventory management, reduced wastage, and improved product tracking. Blockchain technology can help streamline regulatory compliance in several ways. For instance, the system could be programmed to automatically flag any products that do not meet regulatory standards, allowing manufacturers to take corrective action before the product reaches consumers. This would improve compliance with regulations and help reduce the risk of legal and financial penalties. The system could be expanded to include a rating system for products. Customers could rate products on various factors such as quality, authenticity, and price. This would allow businesses to get feedback on their products and improve their offerings accordingly.

REFERENCES

[1] Chen, L., Xu, L. D., & Zhao, S. (2018). Blockchain-Based Supply Chain Systems: A Framework for Security and Privacy Preservation. IEEE Transactions on Industrial Informatics, 14(8), 3415-3425.
[2] Swan, M., 2015. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".
[3] Nakamoto, S. and Bitcoin, A., 2008. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. Pdf.
[4] Kshetri, N., 2018. 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of information management, 39, pp.80-89.
[5] Fan, K., Wang, S., & Ren, Y. (2018). Blockchain and its applications in industries. IEEE Access, 6, 6900-6919.
[6] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
[7] Zhang, L., Luo, X., & Wen, Q. (2019). Blockchain-based anti-counterfeiting for traceability of goods in supply chains. International Journal of Production Economics, 207, 96-110. https://doi.org/10.1016/j.ijpe.2018.10.015
[8] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71-81. https://doi.org/10.1016/j.apin.2016.10.008
[9] Iansiti, M. and Lakhani, K.R., 2017. The truth about blockchain. Harvard business review, 95(1), pp.118-127.
[10] Walmart. (2018). Walmart completes blockchain pilot for tracking US pork supply chain. Retrieved from https://www.walmart.com/newsroom/2018/09/24/walmart-completes-blockchain-pilot-for-tracking-us-pork-supply-chain

[11] IBM. (n.d.). IBM blockchain for ethical diamond certification. Retrieved from https://www.ibm.com/blockchain/solutions/ethical-diamond-certification
[12] Choudhary, A., Shankar, R., & Saxena, A. (2020). Blockchain based solution for product authentication and counterfeits elimination in pharmaceutical industry. Journal of King Saud University-Computer and Information Sciences, 32(8), 913-920.
[13] Li, X., Sun, X., & Zhu, M. (2019). A blockchain-based food safety and traceability system for agri-food supply chain quality management. International Journal of Information Management, 49, 461-471. doi: 10.1016/j.ijinfomgt.2019.03.008
[14] Panigrahi, A., Sahu, B., Panigrahi, S.S., Khan, M.S. and Jena, A.K., 2021. Application of Blockchain as a solution to the real-world issues in health care system. In Blockchain Technology: Applications and Challenges (pp. 135-149). Cham: Springer International Publishing.
[15] Sahu, B., Panigrahi, A. and Mohanty, S.N., 2022. Health monitoring system for cancer care using iot. In Real-Life Applications of the Internet of Things (pp. 203-229). Apple Academic Press.
[16] Petre, A. and Haï, N., 2018. Opportunities and challenges of blockchain technology in the healthcare industry. Medecine Sciences: M/S, 34(10), pp.852-856.
[17] Panigrahi, A., Nayak, A.K., Paul, R., Sahu, B. and Kant, S., 2022. CTB-PKI: Clustering and Trust Enabled Blockchain Based PKI System for Efficient Communication in P2P Network. IEEE Access, 10, pp.124277-124290.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY