International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025
© 2025 IJERST. All Rights Reserved

Research Paper

BLOCKCHAIN BASED FRAMEWORK FOR PRODUCT AUTHENTICATION AND COUNTERFEIT ELIMINATION

[1]Dr.N.CHANDRAMOULI, [2]CHANDA ANEESH BABU

[1]Professor & Head Department of CSE ,Vaageswari College of Engineering, Karimnagar.Email-id: cmnarsingoju@gmail.com.

[2]Research Scholar,H.no:21S41D5825,Department of CSE,Vaageswari College of Engineering, Karimnagar,Email-id: aneeshbabu.chanda@gmail.com.

ABSTRACT

Blockchain technology, while primarily recognized for its applications in monetary transactions, has the potential to revolutionize a wide range of sectors. Its key advantages include transparency, faster transactions, and the elimination of trusted intermediaries. This paper explores the potential of blockchain technology in reducing counterfeiting. A review of various anti-counterfeit solutions, blockchain frameworks, and their suitability for this application is presented. Three novel approaches are discussed, along with ongoing efforts to improve existing system foundations. The study emphasizes that technical solutions alone are insufficient to curb counterfeiting; complementary measures such as public education, judicial enforcement, reliable warning systems, and tamper-proof packaging are also necessary. By integrating these strategies with blockchain, a comprehensive approach can be developed to effectively combat counterfeiting.

Index Terms:- Anti-Counterfeiting, Blockchain Technology, Counterfeit Detection, Decentralization, Digital Transactions, Distributed Ledger, Fraud Prevention, Product Authentication.

Received: 09-08-2025 Accepted: 11-09-2025 Published: 18-09-2025

1.INTRODUCTION

Counterfeiting has emerged as a global crisis, inflicting severe economic, social, and health-related consequences. Despite efforts to curb its spread, the scale of forgery across industries remains overwhelming. In the United States alone, various sectors—including apparel, retail, software, digital media, electronics, and intellectual property—report combined annual losses of approximately $600 billion due to counterfeiting. Globally, the situation is even more alarming; by 2022, counterfeiting and piracy were projected to cost the world economy $4.2 trillion, jeopardizing more than 5.4 million legitimate jobs, according to the International Chamber of Commerce.Among the most devastating impacts is the fake pharmaceutical industry, a sector valued at nearly $75 billion annually. Counterfeit medicines are responsible for over 1 million deaths each year, with forecasts suggesting that this illicit industry could become up to 25 times more profitable than the global narcotics market due to its higher growth rate compared to legal drug manufacturing. Such alarming statistics highlight the urgent need

for advanced and reliable anti-counterfeiting measures.

At the core of this issue lies trust. In any transaction—whether financial or commercial—trust plays a vital role. Traditional systems rely heavily on intermediaries such as banks, clearinghouses, and regulatory bodies to ensure security and authenticity. However, this dependency increases complexity, raises transaction costs, reduces transparency, and slows down processes. The advent of Bitcoin demonstrated that transactions can be executed directly between parties without intermediaries. Using cryptographic algorithms instead of institutions, authenticity is verified in a decentralized manner, thereby ensuring transparency, speed, and reduced costs.The underlying technology that enables such capabilities is blockchain. Beyond its application in cryptocurrencies, blockchain provides a tamper-proof, cryptographically secure, and globally accessible ledger. With its ability to support irreversible and verifiable transactions, blockchain has the potential to redefine the digital economy and reshape the way product authentication and provenance tracking are managed.

This study focuses on the application of blockchain in combating counterfeiting. Specifically, it explores how a decentralized framework—integrating blockchain with Near Field Communication (NFC) technology—can establish a secure and transparent block-supply chain. Unlike centralized anti-counterfeiting supply chains that suffer from single points of failure and isolated storage systems, the proposed decentralized consensus mechanism ensures both efficiency and security. Comparative simulations further demonstrate that this approach outperforms conventional consensus protocols such as Tendermint, thereby offering a robust and scalable solution to counterfeiting threats.



Fig.1 Challenges in counterfeit elimination

2.LITERATURE SURVEY

Ralph C. Merkle described new cryptographic protocols that take full advantage of the unique properties of public key cryptosystems. Several protocols for public key distribution and digital signatures are briefly compared with each other and with conventional alternatives.

Jinhua Ma, Shih-Ya Lin, and Xin Chen proposed that blockchain has received increasing attention, with numerous applications emerging from this technology. A renowned blockchain application is the cryptocurrency Bitcoin, which not only effectively solves the double-spending problem but also confirms the legitimacy of transactional records without relying on a centralized system. Therefore, any application using blockchain technology as its base architecture ensures that the data remains tamper-proof. This paper adopts a

decentralized blockchain approach to ensure that consumers do not fully rely on merchants to determine if products are genuine. The authors describe a decentralized blockchain system for product anti-counterfeiting, enabling manufacturers to provide authentic products without managing direct-operated stores. This approach can significantly reduce the cost of product quality assurance.

I. C. Lin and T. C. Liao introduced blockchain technologies as one of the most popular issues in recent years. Blockchain has already changed people's lifestyles in some areas due to its significant influence on many businesses and industries, and its impact will likely continue to expand. Although blockchain offers more reliable and convenient services, the security issues and challenges behind this innovative technology remain important topics that need to be addressed.

Si Chen, Rui Shi, and Zhuangyu Ren emphasized that quality scandals highlight the importance of quality management from a supply chain perspective. Although many studies have focused on supply chain quality management, traditional technologies still face difficulties in resolving problems caused by the lack of trust in supply chains. The root issues lie in three challenges within centralized trust mechanisms: the self-interest of supply chain members, information asymmetry in production processes, and the costs and limitations of quality inspections. Blockchain is a promising technology to address these challenges. In this paper, the authors propose a blockchain-based framework for improving supply chain quality management.

H. Pun, J. M. Swaminathan, and P. Hou addressed the severe issue of counterfeiting in many sectors. There are two types of counterfeits: non-deceptive and deceptive. While both pose significant business challenges, deceptive counterfeits create an additional negative impact—customers experience post-purchase regret when they expect to purchase a genuine product but receive a fake. This study is among the first to examine the effectiveness of blockchain as a solution to supply chain challenges. Specifically, the unique feature of blockchain modeled in this work—unlike any traditional strategy—is its ability to shift the analysis from a deceptive counterfeit setting to a non-deceptive one. The authors also consider the role of government as a decision-maker and the issue of customer privacy in blockchain adoption, two aspects rarely addressed in the literature. Their model analyzes a market with a manufacturer and a deceptive counterfeiter, where the manufacturer can signal product authenticity either through blockchain technology or differential pricing. The government may also provide subsidies to encourage blockchain adoption. The study concludes that blockchain should be adopted when counterfeit quality is intermediate or when customers have intermediate levels of distrust. With government subsidies, blockchain can be more effective than differential pricing strategies in eliminating post-purchase regret. The results advocate for government-provided subsidies, as they benefit both customers and society and may

be a better approach than strict enforcement efforts.

3.PROBLEM STATEMENT:

Without a clear understanding of the counterfeit problem, approaches to identifying and preventing counterfeit products become ineffective. Public education and awareness, particularly regarding pharmaceutical items, are of paramount importance. Timely inspection and verification of suspected products are critical in combating counterfeiting. The initial step often involves the visual examination of the medicine, its packaging, and any accompanying materials, such as pamphlets or labels. If the product is found to be counterfeit, a structured process of risk assessment and patient notification must follow to minimize potential harm.

Moreover, effective countermeasures require the active involvement of law enforcement authorities to trace the origins of counterfeit products and dismantle the criminal networks behind their production and distribution. The overarching goal is to enhance awareness of the dangers posed by counterfeit goods while exerting greater pressure on illicit actors. Addressing this issue demands a comprehensive approach that combines technical solutions, public education, regulatory enforcement, and judicial action to ensure the authenticity of products and protect consumers.

DISADVANTAGES:

- This opens the risk that the outsourced supplier will not only produce legitimate products, but also counterfeits, with having access to all the original assets.

4.PROPOSED MODEL:

The proposed model enables buyers to verify product authenticity through a simple and secure process. First, the buyer uses a mobile device with a QR or NFC scanner to read the product's tag. Once scanned, a web page is automatically opened in the browser, which forwards the request to the Authentication Module. If the request is valid, the Authentication Module verifies the product's legitimacy, records the scan in both the database and the blockchain, and returns a response containing the product details along with its complete scan history. The browser then displays this information, allowing the buyer to review the scan history and confirm the product's validity. By examining the scan records, users can detect any irregularities, ensuring transparency and trust in the product's authenticity.

ADVANTAGES:

- In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be consider as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all blocks hash code will be verified.

5.SYSTEM MODEL

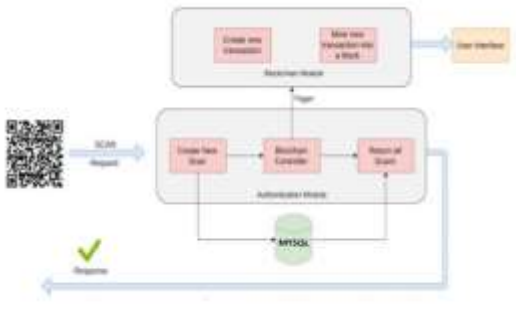


Fig .2 System Model

6. IMPLEMENTATION:

1) Save Product with Blockchain Entry: In this module user will enter product details and then upload product bar code image and then digital signature will be generated on uploaded barcode and then this transaction details will be store in Blockchain. Before storing transaction Blockchain will verify all old transaction and upon successful verification new transaction block will be store
2) Retrieve Product Data: Using this module user can search existing product details by entering product id
3) Authenticate Scan: Here in this module we don't have any scanner so we are uploading original or fake bar code images and then Blockchain will verify digital signature of uploaded bar code with already store bar codes and if match found then Blockchain will extract all details and display to user else authentication will be failed.

7.SCREENSHOTS

To run project double click on 'run.bat' file to get below screen



In above screen enter product details and then click on 'Save Products with Blockchain Entry' button to store product details in Blockchain



In above screen I entered product details and then selecting and uploading associated BARCODE image and then click on 'Open' button to get below result



In above screen Blockchain generated new Block with id 2 and we can see Blockchain hash code of old and new transaction with uploaded bar code digital signature and all this details will saved inside Blockchain and now to search product details click on 'Retrieve Product Data' button to get below details



In above screen I entered product id as 2 and then click on 'Retrieve Product Data' button to get above details. Now click on 'Authenticate Scan' button to upload product Barcode and then Blockchain will match this uploaded Barcode signature with

available stored signatures and if match found then authentication will be successful else failed



In above screen I am selecting and uploading '2.jpg' file and then click on 'Open' button to get below result



In above screen in browser author can see all authentication details uploaded product bar code. Now check with fake barcode by uploading from 'fake bar code' folder



In above screen uploading barcode from fake folder and below is the result



In above screen in text area we can see uploaded bar code authentication failed.

8.CONCLUSION

We develop project based on online transaction require third party to complete transaction and peoples has to trust on third parties to complete their transaction and sometime this third parties can make fraud transaction or misuse user data. To avoid this problem author using Blockchain technology which does not require any third party and verification will be done by software algorithm itself without involvement of any third party. In this to avoid forge counterfeit we are converting all productsdetails/barcode into digital signatures and this digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by an chance if its data alter then verification get failed at next block storage and user may get intimation about data alter. In Blockchain technology same transaction data stored at multiple server with hash code verification and if data alter at one server then it will detected from other server as for same data hash code will get different. For example in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one server then its hash code will get changed in one server and other servers left unchanged and this

changed hash code will be detected at verification time and future malicious user changes can be prevented.

9. FUTURE SCOPE

In this thesis, a variety of methods for minimising counterfeits were studied. In order to be less dependent on external variables, several enhancements were explored and their impact on reducing counterfeits was assessed. Time and other system modifications made it impossible to make all the adjustments that had been requested. To move forward, we need to finalise these systems' implementations and consider performing pilots. Improving humanitarian aid supply chain security by eliminating counterfeit goods is currently being conceptualised and implemented.

10.REFERENCES

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[2] Hyperledger, Hyperledger Blockchain Performance Metrics, V1.01, Oct. 2018.

[3] R. C. Merkle, "Protocols for public key cryptosystems," in Proc. IEEE Symposium on Security and Privacy, Apr. 1980, pp. 122–133.

[4] A. Ronacher, "Flask Documentation." [Online]. Available: http://flask.pocoo.org/docs/

[5] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, Tech. Rep., 2014.

[6] OECD, Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies. Paris: OECD Publishing, 2016. [Online]. Available: https://doi.org/10.1787/9789264251847-en

[7] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.

[8] C. Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, "Making Byzantine fault tolerant systems tolerate Byzantine faults," in Proc. 6th USENIX Symp. on Networked Systems Design and Implementation (NSDI), 2009, pp. 153–168.

[9] C. Cachin, Architecture of the Hyperledger Blockchain Fabric, Tech. Rep., Jul. 2016.

[10] S. Underwood, "Blockchain beyond Bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.

[11] Deloitte, Israel: A Hotspot for Blockchain Innovation, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf. [Accessed: Nov. 2, 2016].

[12] G. Greenspan and M. Zehavi, "Will provenance be the blockchain's break-out use case in 2016?" CoinDesk, Jan. 2016. [Online]. Available: http://www.coindesk.com/provenance-blockchain-tech-app/. [Accessed: Dec. 12, 2016].

[13] World Health Organization (WHO), Counterfeit Medicines: Questions and Answers, 2009. [Online]. Available: http://www.who.int/medicines/services/counterfeit/faqs/QACounterfeit-october2009.pdf. [Accessed: Jun. 12, 2010].

[14] International Chamber of Commerce (ICC), Business Action to Stop Counterfeiting and Piracy (BASCAP): Brand Protection Directory. [Online].

Available: http://www.iccwbo.org/bascap. [Accessed: Jun. 10, 2010].
[15] L. Li, "Technology designed to combat fakes in the global supply chain," Business Horizons, vol. 56, no. 2, pp. 167–177, 2013.