Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6 –Issue 2,August 2023
Paper:67

Design and Implementation of Anti-Counterfeit System Using Blockchain

Saranya S S[1]
Department of Computer Science and Engineering,
Kongu Engineering College,
Erode, India.
saranya.sowndarajan@gmail.com

Kavitha M N[2]
Department of Computer Science and Engineering,
Kongu Engineering College,
Erode, India.
kavithafeb1@gmail.com

Gowtham R[3]
Department of Computer Science and Engineering,
Kongu Engineering College, Erode, India.
gowthamr.20bir@kongu.edu

Shivaas G[4]
Department of Computer Science and Engineering,
Kongu Engineering College, Erode, India.
shivaasg.20bir@kongu.edu

Vishnu Priyan M[5]
Department of Computer Science and Engineering,
Kongu Engineering College, Erode, India.
vishnupriyanm.20bir@kongu.edu

Abstract: Due to a lack of transparency, supply chain management often experienced issues such as service redundancy, poor coordination between departments, and lack of standardization. Most people are unaware of the extent to which counterfeit items affect brands, but counterfeiters pose significant challenges for legitimate firms. Counterfeit products have been dealt with in the past using several methods. The most popular methods are using Radio Frequency Identification tags (RFID), Artificial Intelligence (AI), Quick Response code (QR) code system etc. Although each of them had some disadvantages, such as that QR codes can be copied from a genuine product and placed on a fake one, Artificial Intelligence uses CNNs and ML, which require an enormous amount of computing power, etc. Blockchain technology ensures the identification and traceability of real products throughout the supply chain. With blockchain technology, everything becomes decentralized so that multiple parties can access the same information at the same time. Its main advantage is that all parties involved must consent to any changes to the recorded data, making it extremely secure and risk free. A new proposed system is designed to perceive counterfeit products is presented that uses blockchain technology. HMAC stands for Keyed-based Hashing for Message Authentication. It is a message authentication code that is created by using a shared secret key and a cryptographic hash function on the data that must be authenticated (such MD5, SHA1, or SHA256).

Keyword: Blockchain, counterfeit, products, QR code and HMAC

I. INTRODUCTION

When a product is sold pretending to be another, this is called product counterfeiting. Consumer fraud is generally understood to be dishonest company actions that result in substantial financial or other damages for consumers. It costs the Indian economy INR 1 trillion annually, according to reports from the Authentication Solution Providers' Association. Incidences of counterfeit goods are rising 20% on average between 2018 and 20. Electronics, apparel, cosmetics, and purses are examples of counterfeit products. It has detrimental effects on both citizens and the economy. Poor cosmetics, for instance, can irritate the skin and result in skin conditions and rashes, while fake electrical components can cause devices to malfunction and result in undesirable circumstances and accidents. When worn, cheap clothing and shoes can be uncomfortable. Therefore, a solution to the problem of the sale of fake goods is required. The reputation of a corporation is also harmed by counterfeiting. Because many buyers have no idea what they are holding, if a knock-off product does not work as expected, falls apart quickly, or does not meet their expectations, they will blame the real company. Transparency of Network controlling cost, strategies of pre-supply evaluation, finally relationship management among supplier are the most efficient mitigating actions for reducing the danger of ambiguous counterfeit goods in global supply chains. The objective of this paper is to provide a blockchain based anti-counterfeit system that gives suppliers and end users the ability to follow a product's supply chain in a safe setting. In an overview of

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6 –Issue 2,August 2023
Paper:67

the proposed system, it is intended to address the issue of trademark counterfeiting and give customers, vendors, and distributors the ability to verify the authenticity of the product.

II. RELATED WORK

In this study [1], Mitsuaki Nakasumi et al. argue that systems for management of supply chains give firms with info exchange and analysis, as well as help their planning efforts. They are not based on genuine facts since there is asymmetric knowledge between organizations, causing the planning algorithms to be disrupted. On the other side, data exchange among manufactures, vendors, and clients becomes critical from ensuring market responsiveness. Double marginalization, throughout particular, is a prevalent and important issue in distribution network administration. Scattered systems with wholesale price contracts are studied, and double marginalization effects are demonstrated to cause supply insufficiencies in both deterministic and random requests.

In this study [2], Si Chenet.al. suggested Recent quality scandals highlight the necessity of quality control in the supply chain. Despite several relevant research concentrating on supply chain quality management, the technologies deployed continue to have difficulty resolving challenges caused by a lack of confidence in supply networks. The main cause is a combination of three challenges to the conventional centralized trust mechanism: supply chain participants' self-interest, knowledge asymmetry in manufacturing processes, and the costs and constraints of quality checks. Block chain is a potential remedy to dealing with these issues. The ongoing rise of counterfeit items and product quality scandals has highlighted the necessity of quality control in the supply chain.

Eduard Daoudet et al. proposed in this article Research and Markets reported on May 15, 2018[3], that up to 1.2 trillion USD of items were fake in 2017. According to the analysis, the worldwide cost of this harm will be $1.82 trillion USD in 2020. This study does not address copyright or digital piracy, counterfeiting, or fake papers, but rather studies counterfeiting prevention on a technical level. Because the existence of counterfeit items on the European market is increasing, the list of inspections agencies and officials is Insufficient client may contribute to and support this process

In this study [4], Muhammad Asif Habibet al. offered the transaction problem is critical among stakeholders in a distribution network administration. The exchange of transactions is critical for the proper transportation and logistics procedures in the supply chain. The present supply chain management system has various flaws in terms of security and confidence during the deal-making process. As a result, data is shared on the document and in a semi-digitized format. We look at a problem with confidence in the distribution chain and present a creative, ledger plan for resolving it and automate the whole financial transactions using smart contracts. Case studies are used for validation.

III. EXISTING WORK

There are numerous systems for spotting phone goods that make use of AI, QR codes, ML and blockchain. The approaches include using an item that also included public keys and secret keys as a QR code, and the app that was used scan the code needed to have cryptography capabilities to decode it. Additionally, the maker is required to operate a server that accepts requests and matches the dealer's name and product code. To decode the barcode that is contained in the cypher text of the QR code, the scanning app must have cryptographic functionality. The supply chain track and trace frameworks are made up of several interconnected layers.

DISADVANTAGES OF EXISTING WORK

- The usage of QR codes by manufacturers to validate their items is one of the disadvantages of the current systems. However, it is possible to copy the barcode and use it mark fake goods.
- Low-cost RFID tags can be used in RFID-based systems to automatically identify items, but this technology is unsuitable because RFID tags could be copied.
- In AI and ML application, CNN consumes more memory and time. Before being deployed, it must undergo testing and training. Tag reapplication attacks, in which a scammer removes a valid tag off an actual thing and initializes it to a fake or expired goods, are not recognized by artificial intelligence.
- Customers, producers, and merchants have no authority to examine the product’s integrity.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6 –Issue 2,August 2023
Paper:67

IV. PROPOSED METHODOLOGY

End users are at risk of financial loss, health problems, and injury due to counterfeit and duplicate goods. Additionally, it harms the economic development of product or brand and companies via loss of sales, brand slander, delay, replacement, causing many companies to invest money combating counterfeit goods, possibly jeopardizing the faith of business associates, snatching sales, etc. Blockchain technology enables the identification of original products as well as the detection of duplicate products to prevent these crucial effects of counterfeiting. As wireless technology continues to develop, QR codes and barcodes can be used to reduce the practice of counterfeiting. The fraudulent goods are detected using a camera scan, and the QR of the item is connected to a blockchain to save the item's information and the verified distinct codes are stored in a database such as information of blocks. If the code in the item fits the code in the database, an alert will be sent to the client implying the authenticity of the item. If the buyer receives the user's request, a notice also will be sent to the producer confirming the location of the user's purchase if a code in an item does not fit the code in a block of database. This strategy for reducing fake assures that customers won't solely rely on retailers to judge whether things are genuine or fake. A private key and a hash function are used in the cryptographic authentication system known as HMAC. HMAC, as contrast to methods which use signature and asymmetric encryption, allows verification and the verification that information is true and legitimate.

ADVANTAGES OF PROPOSED SYSTEM:

- It requests the customer's special identifier, then checks that against records in a database.
- If the code fits, the customer will be notified. If not, the consumer will receive a message that the goods are fake.
- If the transmitter and recipient both have access to a private key, an HMAC could be utilized to detect if a data delivered over an unsecured connection has been changed with.
- The sender generates a hash code for the source data and delivers the hash code together with the actual information in one message. Recalculating the hash value for the receiver, the recipient verifies that the calculated and sent HMACs are same.

A. ARCHITECTURE DIAGRAM

The technology will identify fake goods using QR (Quick response) codes, which are linked to contracts and linked to objects, allowing mobile phones and other scanning devices to read the codes. This will indicate whether the goods are genuine or counterfeit. A company will be given access to post the product details with a system-generated QR code after having their mail id and registration system verified. The product information includes the name and brand of the product, the year it was manufactured, its price, its values in the table, its quality, and the company's information. This will be kept inside a database, and the QR code will be saved in a blockchain. A distinct QR code that cannot be used by the manufacture for multiple products will be included in each block transactions. Manufacturers can employ serialized QR codes to convey information about the product, engage with customers, and increase sales, improving the security and dependability of the tracking and identification process.

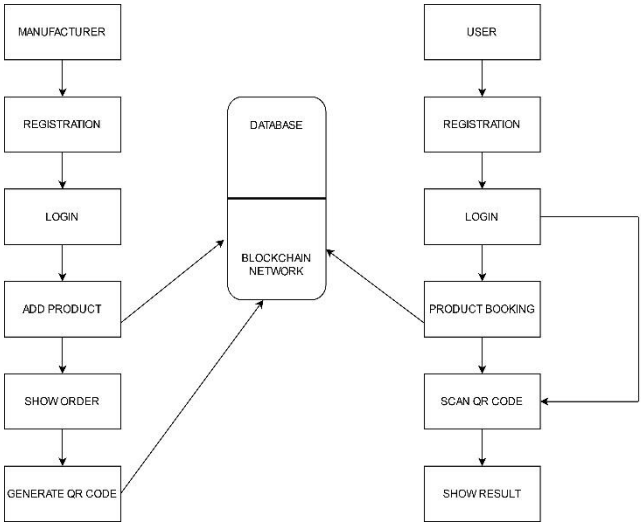

Fig. 1. System Flow Diagram

Before reading the QR code of the item, the client must first sign in or enroll with the system. The clients unique scanned code will be checked to the company's code, which is kept in blocks of smart contracts, after user verification is complete. The user will be informed that the item is genuine with all the information and a genuine certification from the databases if the code matches. If the barcodes do not fit, the user will be warned that the product is fake, helping to avoid purchases of counterfeit goods that could cause serious harm to one's heath or substantial financial loss. If the item is false, a notification will be issued to the manufacturer. The manufacturer then can take extra legal proceedings against the distributors, reseller, and black-market distributor. This promotes user pleasure, guarantees that buyers have faith in merchants, and can help manufacturers avoid spending

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 6 –Issue 2,August 2023
Paper:67

money and time battling false advertising and revenues caused by fake good.

V. IMPLEMENTATION

A. Manufacturer End

After confirming the mail ID for signup and authentication process purposes, the company. They could login into the system, add new items or products and submit the product information using a system generated code containing all the information about the product. It is also suggested to serialize the QR code for further security and to maintain track of the goods. The product data will be stored in a database, and a secured graphical method was used to make the QR code copy sensitive, meaning that when replicated, data is lost and printing is irreversible.

B. Customer End

The customer's email ID and password are required to register and login. After user verification is complete, the product starts up with a scan button to read the QR code of the goods. The user in this case is a customer looking to verify the legitimacy of the goods. The block-produced code from producer will be contrasted with distinctive scanned data from of the client. The user will then be informed of the product's validity. Customers can view product information such as name, manufacturing year, price, overall quality, quality of products, and production level.

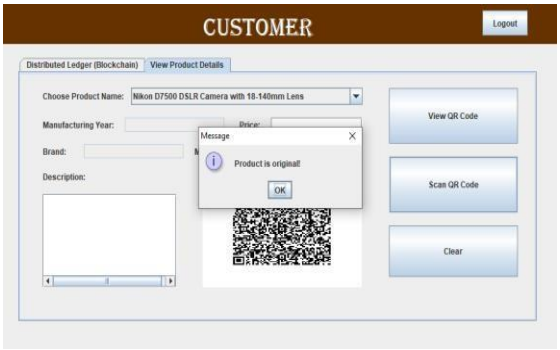

Fig. 2 Product is Original

Fig. 3 Product is Fake!

VI. CONCLUSION

The prevalence of fake items is constantly growing as a result of the vast selection of them available online. Because of this, it is crucial to find fake goods, and blockchain technology is being utilized to do this. The information is also encoded as a QR code. Scannable QR codes can be used by users or clients to identify bogus goods. Virtual product details can be saved in blocks using blockchain technology. The data can be kept in a database. The proposed approach can therefore help buyers identify bogus goods in the supply chain. The end-user can check whether a product is authentic by scanning the QR codes attached to it to acquire details like previous transactions and the owner. Customers can scan the QR codes attached to products to get all the information they require, like transaction records and the owner, which even the finished can utilize to verify whether the products are real or not.

REFERNCES

[1]. M. Nakasumi, Information sharing for supply chain management based on block chain technology, in 2017 IEEE 19th conference on business informatics (CBI) (IEEE, 2017), Vol. 1, pp. 140–149.

[2]. S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, A blockchain-based supply chain quality management framework, in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE) (IEEE, 2017), pp. 172–176.

[3]. E. Daoud, D. Vu, H. Nguyen, M. Gaedke, Improving Fake Product Detection Using Ai- Based Technology, in 18th International Conference e-Society (2020).

[4]. M.A. Habib, M.B. Sardar, S. Jabbar, C.N. Faisal, N. Mahmood, M. Ahmad, Blockchain- based supply chain for the automation of transaction process Case study-based validation, in Technologies (ICEET) (IEEE, 2020), pp. 1–7 Y. Lu, Journal of Management Analytics 5, 1 (2018). 2020 International Conference on Engineering and Emerging

[5]. Sahin F and Robinson EP (2002) Flow coordination and information sharing in supply chains, review, implications, and direction for future research. Decision Sciences 33 (4), 505– 536, 2006

[6]. Rai A, Patnayakuni R and Patnayakuni N, Firm performance impacts of digitally enabled supply chain integration capabilities. MIS Quarterly 30 (2), 225–246, 2006.

[7]. Huang GQ, Lau JSK and Mak KL, The impacts of sharing production information on supply chain dynamics: a review of the literature. International Journal of Production Research 41 (7), 1483–1517,2003

[8]. Ho DC, Au KF and Newton E, Empirical research on supply chain management: a critical review and recommendations. International Journal of Production Research 40, 4415–4430, 2002.

[9]. Handfield RB and Pannesi RT, Antecedents of lead time competitiveness in make-to-order manufacturing firms. International of Journal of Production Research 33 (2), 511–537, 1995.

[10]. Handfield RB and Bechtel C, The role of trust and relationship structure in improving supply chain responsiveness. Industrial Marketing Management 31 (4), 367–382, 2002.

[11]. Gunasekaran A, Patel C and Tirtiroglu E, Performance measures and metrics in a supply chain environment. International Journal of Operations & Production Management 21 (1/2), 71, 2001.

[12]. D.M. Freeman, Converting pairing-based cryptosystems from composite-order groups to prime-order groups, in Proceedings of Advances in Cryptology, EUROCRYPT'10, 2010, pp. 44–61.

[13]. inghui Li, Tiancheng Li, and Suresh Venkatasubramanian, t-closeness:Privacy beyond k-anonymity and l-diversity, in ICDE, volume 7, pages 106–115, 2007.

[14]. AshwinMachanavajjhala, Daniel Kifer, Johannes Gehrke, and MuthuramakrishnanVenkitasubramaniam, l-diversity: Privacy beyond kanonymity, ACM Transactions on Knowledge Discovery from Data(TKDD), 1(1):3, 2007.