IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SUPPLY CHAIN COUNTERFEIT PRODUCT DETECTION SYSTEM USING BLOCKCHAIN TECHNOLOGY

[1]Sayyina sharo shaiju, [2]Ms.Sumi M

[1]MCA Scholar, [2]Assistant Professor,

[1]Department of MCA,

[1]Nehru College of Engineering and Research Centre, Pampady, India

Abstract: Counterfeit goods have become increasingly important in the creation of products in recent years. The companies' sales and profit are impacted by this phenomenon. Product counterfeiting is prevented by using a functional block chain technology, which guarantees the identification of genuine products along the supply chain. By employing block chain technology, customers may reliably determine the product's origins without depending on reliable third parties. Any application that makes use of block chain technology as its foundational technology guarantees "tamper-resistant" data content. Considering that a block chain is a distributed, decentralized, digital ledger that keeps track of public transaction records called blocks across numerous databases and networks. The problem of product counterfeiting has been addressed in the past by the development of several techniques. The most popular methods include RFID tags, artificial intelligence, and systems based on QR codes. However, there were a few issues with each of them: artificial intelligence uses CNN and machine learning, which are computationally intensive; a QR code can be copied from a legitimate product and used on a phony one, and some other issues. By tracking the origins of the supply chain, this research aims to improve the detection of counterfeit items. This is made feasible by blockchain technology, which ensures the identification and tracking of authentic products across the supply chain. Everything in a blockchain-based system is decentralized and available to multiple parties at once.

Index Terms **– Blockchain, Counterfeit Products, Ethereum, QR Code, Supply chain.**

I. INTRODUCTION

For all supply chain participants, identifying counterfeit goods in the marketplace has proven to be difficult over time. The Organization for Economic Cooperation and Development (OECD) and the EU Intellectual Property Office (EUIPO) have released a report that shows the worrisome rise in sales of counterfeit and pirated goods to 460 billion euros worldwide, or around 3.3% of global trade .This phenomena has an impact on the sales and earnings of businesses worldwide. Sales losses in the apparel and pharmaceutical industries were around 26.3 billion euros and 10.2 billion euros, respectively [1]. Furthermore, the market for counterfeit goods has flourished on social media platforms due to the introduction of new technology and E-commerce. Counterfeiters now have an easier time operating because of the anonymity, reach, and segmentation capabilities offered by social media and e-commerce. Therefore, creating identical or near-identical replicas of genuine goods, or counterfeiting, is a serious danger to economic progress and innovation. Over the past ten years, blockchain technology has drawn a lot of attention, and several applications are currently being developed. Blockchain is a distributed, unchangeable ledger system that operates decentralized. It lowers risks and lowers expenses for all parties involved by making the process of tracking, exchanging, and registering assets over a corporate network easier. Therefore, any application that uses blockchain technology as its foundation guarantees that the data is secure against tampering. This article presents the architecture of a decentralized application system (DApp) built on the Ethereum network. The DApp makes sure that product

ownership is transferred and registered in the blockchain network, simulating a real-world supply chain. Additionally, the technique suggested here can be used in retail and e-commerce websites, which can significantly increase transparency for all users on virtual platforms. While RFID has been employed in this field of study in the past, it has presented security and privacy problems that can be effectively addressed using blockchain technology. The best ways to reduce misleading counterfeit risk in international supply chains are through supplier relationship management, cost control, and pre-supply evaluation techniques, as well as network transparency. Therefore, this paper's goal is to propose 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.The suggested method aims to address the issue of brand counterfeiting and give suppliers, vendors, and customers the ability to verify the authenticity of the product.

Blockchain

Blockchain is a collection of interconnected blocks used to store data. Data tampering is challenging since each block contains a timestamp, transaction data, and hashes of both the previous and current blocks. The system behind blockchain is decentralized. It guarantees that each new block that is added to the blockchain is the one and only authentic version that has been approved by every node. It alludes to the cooperative upkeep of a decentralized technical system that sustains a continuous record file as a trustworthy database [2].

Working of blockchain

Following the entry of a new transaction, it is sent over a global network of peer-to-peer computers. After that, the computer network solves the equations to verify that the transaction is legitimate. We refer to them as miners. Once verified as authentic transactions, they are grouped into blocks. As a reward for their efforts, the miners are given an award. Once these blocks are linked together, a lengthy history of all lasting transactions is produced. The deal has been finalized .Everything is done as the following figure 1 shows [3] :

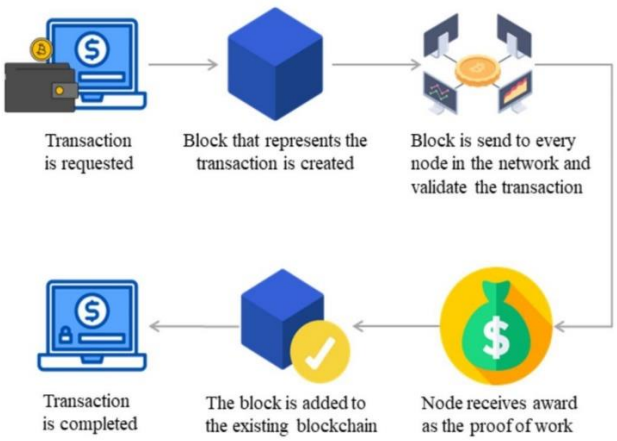

figure 1: working of blockchain [3].

Blockchain Features

Blockchain is able to add records to its database using its own consensus procedures, without the need for a centralized authority to act as an arbiter. Blockchain is a highly dependable, publicly accessible database. The following is a detailed description of the features of Blockchain technology. The graphical figure 2 illustrates the characteristics of Blockchain:

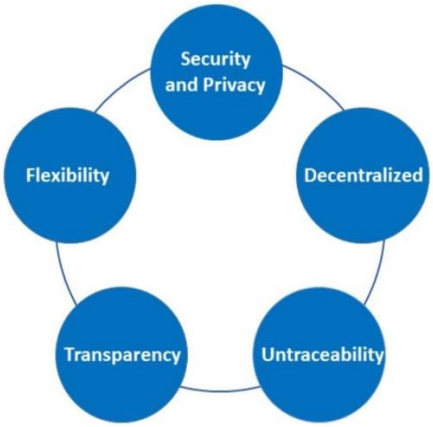

figure 2 : features of blockchain [4].

1) Security and privacy: Blockchain protects its data with cryptography. Data is signed with a private key; its authenticity can be checked and whether or not it has been altered can be confirmed with a public key. To guarantee the security of its data on blockchain, a user should safeguard their private key in the same way that they would passwords and bank OTPs, and keep it from leaking.

2) Decentralized: No one needs to know or have faith in another person in a decentralized blockchain network. In the form of a distributed ledger, every member of the network possesses a duplicate of the exact same data. Most other members of the network will reject a member's ledger if it has been changed or corrupted in any way.

3) Untraceability: A block cannot be altered once it is added to the blockchain. As a result, if a block on the Blockchain is changed, it is rejected or removed right away.

4) Transparency: All participants have access to and may observe the data stored on the blockchain.

5) Flexibility: One of blockchain's main benefits is that it is open source. Users have access to a variety of public and private blockchains, which they can employ in accordance with the kind of application that needs to be developed [4].

Importance of Blockchain

Because blockchain eliminates the need for third parties, it fosters greater trust. Smart contracts, which are essentially blockchain programs, only execute when specific requirements are satisfied. It is more difficult to alter the blockchain with fraudulent information since each block keeps its data along with the hash of the previous block. The hash of a block changes if an attacker modifies its contents, while the hash of the subsequent block stays unchanged. Since a large number of resources and money are needed, it is doubtful that more than half of the participants will agree to change the chain. It would also inform other members of this significant shift [4].

II. LITERATURE SURVEY

The survey's main objectives were to identify the causes of counterfeit goods and their effects on society. There are several techniques for identifying counterfeit products that make use of blockchain, QR codes, machine learning, and artificial intelligence. Different approaches to building a blockchain-based supply chain management system have been put out by various researchers.

Khalil and Doss et al. devise an RFID-based system as a means of mitigating counterfeiting. With the use of this technology, customers can check the authenticity of an item by asking questions about its tag in-store. Large-scale deployment of RFID-based anti-theft and anti-counterfeiting programs is appropriate for retail settings. The suggested plan is simple to execute and works well with inexpensive passive RFID tags [5].

Habib and Sardar et.al gives explanation on SCM trends. They are assessed as part of their work process to determine that transactional problems and executive challenges are SCM concerns. Therefore, a solution known as SCM was put up, taking into account the blockchain as a technological element to address them [6].

Daoud and Vu et.al focuses on the architecture of AI Application. The data set, detection models, and trained model are its three key components. An anti-counterfeiting machine learning system for identifying counterfeit goods. The two necessary processes are the training of models and the logo detection step. High accuracy and low training speed are achieved via faster R-CNN [7].

Chen and Shi et.al explains SCQI. Structure for blockchain-based Theoretical underpinnings for intelligent supply chain quality management based on blockchain technology are provided by SCQI. Quality and transactional information are recorded using RFID technology. Supply chain efficiency is increased and quality monitoring is implemented with the help of smart contracts [8].

Toyoda, Kentaroh and Takis, P. Mathiopoulos, et al suggested a method that uses a QR code to identify counterfeit goods. Customers can obtain product details and transaction history by scanning the QR code linked to the product. They can also obtain information about the product, including the stages involved in product enrollment, shipping the goods to a distributor, and shipping it to a retailer [9]

III. RESEARCH METHODOLOGY

With the use of Blockchain technology, the method being described here helps track consumer products by preserving the integrity of the product and the supply chain. Customers now have the ability to use blockchain technology and QR codes to follow the complete product's history from maker to customer. The Ethereum Network will be used as the primary blockchain for the implementation of the proposed system, a decentralized application (Dapp), which will be used to store all the information and handle the transactions pertaining to the items of the businesses listed on Dapp. Figure 3 depicts the fundamental architecture of the system:

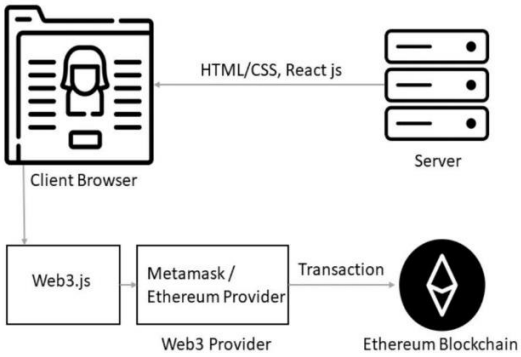

figure 3 : system architecture [11].

Ethereum

It is a decentralized blockchain that operates on a consensus method based on proof of work.Blocks are added to the blockchain by proof-of-work, which involves solving mathematical formulas. The puzzle's solution "proves" that nodes have used computing resources to complete the "work."It attests to the block's addition and recording in the chain. We call this process mining. In Ethereum, adding a block is rewarded, however mining is usually done by brute force trial and error[10].

Smart contract

Programs kept within Blocks are called smart contracts. Third-party members' engagement is replaced by smart contracts. In essence, these are protocols that start working as soon as the requirements are met. Since they are unchangeable, nobody can alter the agreement[11].

Flow of Proposed System Manufacturer

The maker logs into his manufacturer account, generates a QR code for the product, adds any required information, and, using his Ethereum wallet, adds a block to the Ethereum blockchain. If the entity's wallet address and the userid from our local database are both present, only then will the block be added to the digital ledger. For instance, if a manufacturer signs in with his wallet and personal account. The main objective of the suggested method is to maintain the product's uniqueness by allowing consumers to follow the product's supply chain history. Using blockchain technology, customers can utilize the system to track a product's whole lifecycle from maker to customer. Three roles comprise this Blockchain-based product anti-counterfeiting system: Manufacturer, Seller, and Consumer, as depicted and explained in the figure 4 :

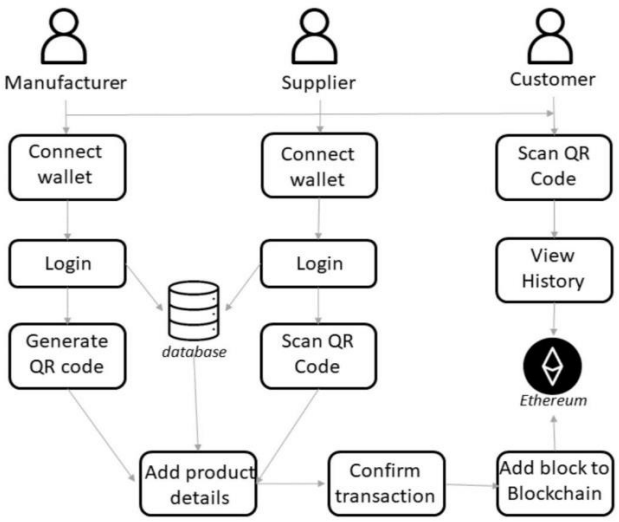

figure 4 : system flow.

Manufacturer

The maker logs into his manufacturer account, generates a QR code for the product, adds any required information, and, using his Ethereum wallet, adds a block to the Ethereum blockchain. If the entity's wallet address and the user id from our local database are both present, only then will the block be added to the digital ledger. For instance, if a manufacturer signs in with his wallet and personal account.

Supplier

Supplier scans the QR code on the product after logging into their supplier account. The manufacturer has entered information about the products that the seller can view. It pushes the product information into the Blockchain and adds its own details, such as the shop's destination. The buyer has access to those particulars.

Customer

By scanning the QR code, customers may verify the product's authenticity and examine its integrity by viewing a history of transactions. If the last location does not match the purchase location when the customer scans the product's QR code in the supply chain history, they will be able to tell that the goods is fake at the time of purchase. The customer learns about counterfeiting and comes to the conclusion that the QR code was copied.

The procedure a customer uses to identify a fake product during a purchase is depicted in figure 5 :

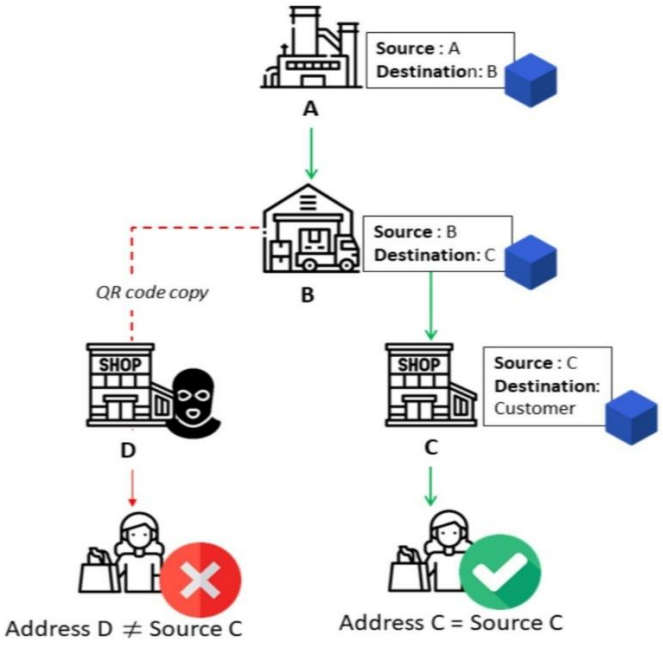

figure 5 : dealing with counterfeit product.

IV. RESULTS AND DISCUSSION

The suggested solution enables communication between suppliers and manufacturers so that each can contribute a block to the blockchain with transaction details without altering the other's block. Solidity is used in the writing of the manufacturer and supplier block contracts. Truffle is then used to compile and deploy the contracts. To prepare for deployment, migration files are made. On an Ethereum blockchain network, migrations are files that facilitate the deployment of contracts .React is used in the interface's creation. The Web3.js library is used to enable interaction with the Ethereum blockchain. It is utilized for transmitting ether, validating transactions, and reading and writing data from smart contracts. Installing Metamask on a browser acts as a wallet to communicate with the Ethereum blockchain and permits browser-based access to the Ethereum wallet. Ganache accounts are loaded into the metamask. They must use their wallet, which is connected via Web3.js, to validate transactions before adding supplier and manufacturer blocks. After that, the end-user can verify the product integrity and supply chain by scanning the QR code.

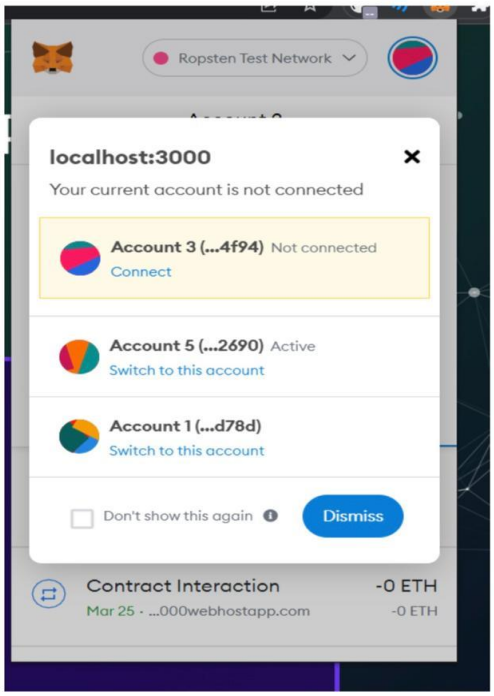

figure 6 : Ethereum connection through metamask wallet.

As seen in Figure 7, the Manufacturer accesses his account by entering his username and password.

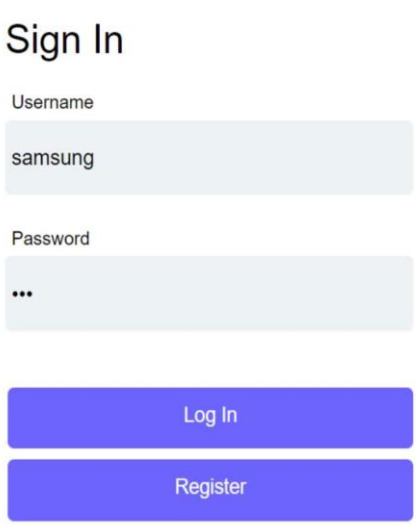

figure 7 : manufacturer login page.

As seen in Figure 8 , the credentials are kept in SQL Server. The address and login credentials of manufacturers and suppliers are kept in a SQL database.

id	name	uid	addr	category	password
10	samsung	26513	Samsung Electronics Huizhou Co., Ltd., Industrial ...	Electronics	202cb962ac
59	louis_vuitton	65464	116 Greene St, New York, NY 10012, United States	Fashion	df2a3e9e50

figure 8 : sql database.

As seen in Figure 9 , the producer creates the product's QR Code and assigns a unique serial number after logging into his account. The merchandise has this QR code attached to it when it is being moved to other locations. The product's name, present address, source, and destination are all filled in by the manufacturer in

addition to these details. The manufacturer adds all of the filled-out facts to the blockchain by clicking the "add block" button after they have finished.

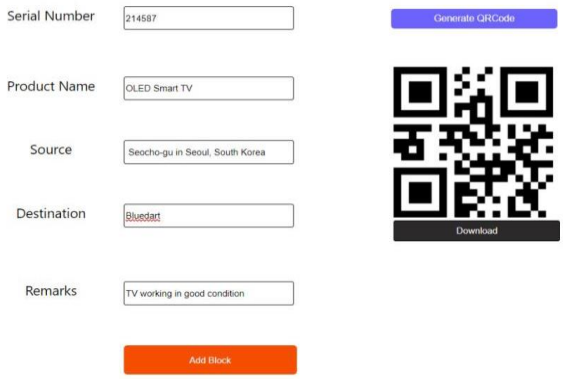

figure 9 : manufacturer adding the details of the product.

A confirmation window for Metamask appears and requests confirmation, similar to what's shown in Figure 10 :

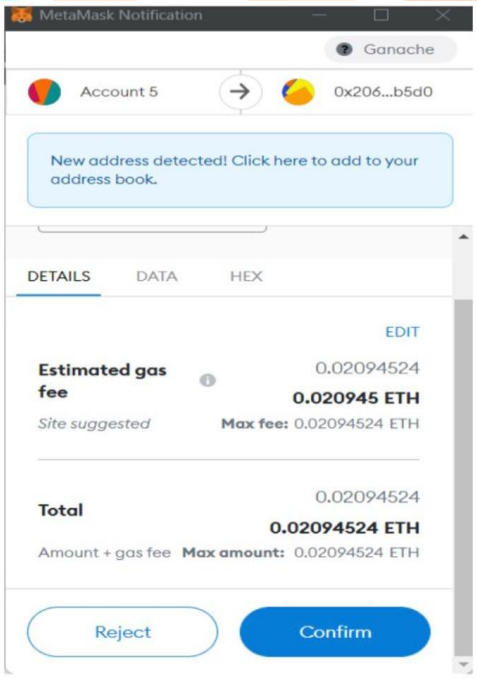

Figure 10 : completing the transaction with metamask wallet.

After confirmation, a success page is presented as depicted in Figure 11 and a block containing all the details is published to the blockchain.

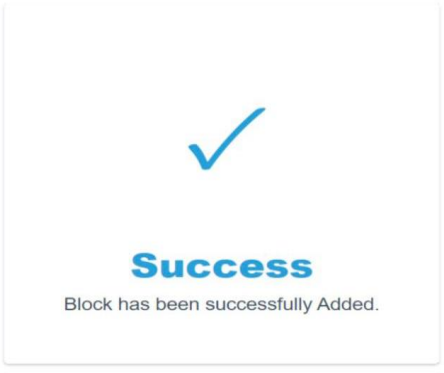

figure 11 : message shown after addition of block to blockchain.

After the product arrives at the provider's destination, the supplier must connect his Metamask wallet and enter into his account, as depicted in Figure 12 :

figure 12 : supplier login page.

After completion, a screen is displayed for the supplies to complete with the necessary product details. This time, the supplier scans the QR code by clicking on "Scan QR" instead of creating the code. The supplier clicks on add block after entering the product's necessary information, as seen in Figure 13.Once the provider logs out and validates his transaction using the Metamask wallet, the block is appended.

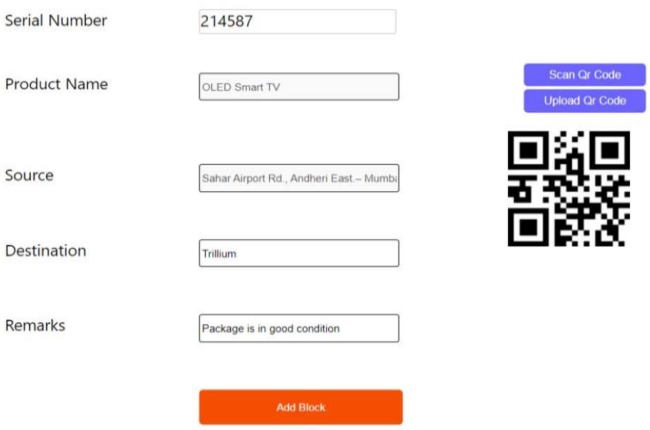

figure 13 : supplier adding details for the product.

In a similar manner, the other suppliers log into their accounts and contribute their own blocks to the blockchain. When the customer receives the product, he can visit the customer page, scan the QR code (as indicated in Figure 14), and view the product's entire supply chain history.

figure 14 : customer page to check supply chain history of the product.

The product id, name, source, destination address, timestamp of the block's insertion, ethereum account address of the entities involved, and any further remarks, if supplied, are just a few of the details displayed in the supply chain history as seen in the accompanying Figure 15 and Figure 16 :

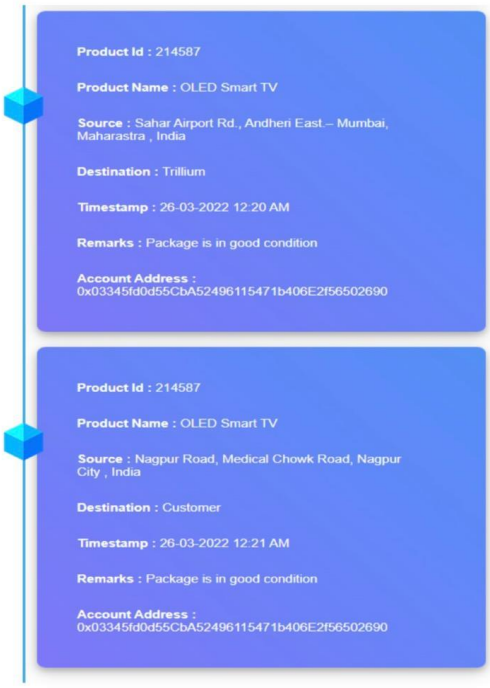

figure 15 : supply chain history – 1

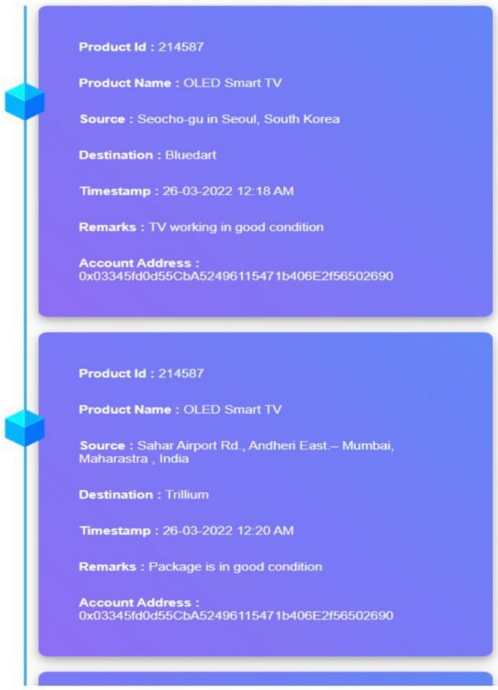

figure 16 : supply chain history – 2

If the final location does not match the purchase location at the moment the consumer purchases the product after scanning the product's QR code in the supply chain history, the customer will be able to tell that the product is not authentic. The customer learns about counterfeiting and comes to the conclusion that the QR code was copied.

V. FUTURE SCOPE

The supply chain and logistics may greatly benefit from the improvement and implementation of block chain technology. The next challenge for safeguarding counterfeits in supply chains will be economic strengthening, even though this decentralized technology may be beneficial for all applications. Blockchain technology offers the ability to lower expenses, simplify procedures, and improve trade partner transaction transparency. Supply chain management may be made more transparent and less expensive and risky by using blockchain technology. The ancillary advantages of blockchain technology for supply chain management must also be considered. Transparency in product manufacture has the potential to improve brands' standing with consumers. Furthermore, by granting public access to supply chain data, blockchain has the potential to increase credibility and win over public trust. Above all, prompt identification of malpractice risks in the supply chain helps to prevent problems with public relations.

VI. CONCLUSION

Since, blockchain technology is decentralized, local suppliers are unable to tamper with the product's verification or counterfeiting within the proposed system. The technology allows suppliers and manufacturers to store product information in Blockchain, which provides tamper-resistance, data consistency, and confidentiality properties that ensure the security and privacy of data on the network. The buyer checks to see if the goods is authentic by looking at its supply chain history. Consumers can feel secure in the quality of the products they buy. With the help of the suggested system, the rate of branded items being counterfeited can be significantly reduced, and businesses will have an easier time convincing customers not to buy counterfeit goods. In addition to strengthening the bonds of trust and goodwill between the maker and the client, this

approach will really aid in lowering corruption and boosting the economy. Additional systems can be implemented to prevent fraud in the banking, healthcare, voting, internet shopping, and other sectors.

VII. REFERENCES

[1] https://www.statista.com/statistics/1117921/sales-losses-due-to-fake-goodby-industry-worldwide/
[2] Y. Lu, Journal of Management Analytics 5, 1 (2018)
[3] Zignuts Techno lab, How blockchain architecture works? basic understanding of blockchain and its architecture., https : / / www.zignuts.com /blogs / how - blockchain - architecture - works - basic understanding- of- blockchain- and- itsarchitecture/(2022)
[4] J. Ma, S.Y. Lin, X. Chen, H.M. Sun, Y.C. Chen, H. Wang, IEEE Access 8, 77642 (2020)
[5] G. Khalil, R. Doss, M. Chowdhury, IEEE Access 847952 (2020)
[6] M.A. Habib, M.B. Sardar, S. Jabbar, C.N. Faisal, N. Mahmood, M. Ahmad, Blockchain-based sup-ply chain for the automation of transaction process:8 ITM Web of Conferences 44, 03015 (2022) https://doi.org/10.1051/itmconf/20224403015ICACC-2022Case study based validation, in 2020 International Conference on Engineering and Emerging Technologies (ICEET) (IEEE, 2020), pp. 1–7
[7] E. Daoud, D. Vu, H. Nguyen, M. Gaedke, Improving Fake Product Detection Using Ai-Based Technology, in 18th International Conference e-Society (2020)
[8] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, blockchain-based supply chain quality management framework, in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE) (IEEE 2017), pp. 172–176
[9] K. Toyoda, P.T.Mathiopoulos, I. Sasase, T. Ohtsuk, IEEE access 5, 17465 (2017)
[10] G. Wood et al., Ethereum project yellow paper 151,1 (2014)
[11] I. Singhal, International Journal for Research in Applied Science and Engineering Technology 9, 291(2021