Product Ownership Management System (POMS) in the Post Supply Chain Using BlockChain

Hanmant D Magar
MIT World Peace University
School of Computer Engineering and Technology
Pune, India

Sandip Mane
Rajarambapu Institute of Technology
Islampur,India

Abstract – Nowadays, the authenticity of the RFID tags cannot be assured in the supply chain since these can be easily duplicated in the public space. We propose a novel Product Ownership Management System (POMS) of products for anti-counterfeits that can be used in the post supply chain by using the QR code. With the projected POMS, a consumer can reject the buying of counterfeits by scanning a QR code, if the seller does not have their proprietorship.
This paper gives an application of the system that will help to overcome the problems related with the presently functioning supply chain management system and runs the mechanism to show the ownership of the products.

Keywords: Product Ownership Management System (POMS), QR code, Anticounterfeits, Supply Chain Management

1. INTRODUCTION

Decentralized [3], the distributed system in which transactions are recorded in successive blocks making an immutable ledger is referred to as “blockchain”. A crypto currency network where anyone in the network can check the proof of possession of the balance or tokens is previously used in the blockchain. In our system, the concept of “proof of possession of balance” is replaced with an equivalent concept referred to as “proof of possession of products” within a supply chain.
Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes has its copy of the distributed ledger [1] that contains the full history of all transactions the network has processed. Blockchain in supply chain management is expected to boom over the next five years [2]. Blockchain will improve business for all global supply chain stakeholders by providing enhanced traceability, facilitating digitization, and securing chain-of-custody.
Supply chain traceability means corporations can handle the possession of products starting from the manufacturer to the current owner. The ability to trace a product throughout its life cycle supports risk management, fraud mitigation, quality assurance, worker rights, informed management decisions, and establishes direct responsibility for each link in the product life cycle.
Addressing the problem of supply chain traceability requires collaboration among stakeholders and deploying technical solutions to aid the transition. Blockchain is a nascent technology with a lot of hype that promises to disrupt status quo operations in many industries and supply chains. With the idea of this proposed system, counterfeits may be detected if a party cannot prove the possession of claimed products with the help of a quick response (QR) code [3].

2. LITERATURE REVIEW

Martin Westerkamp et al.[4] propose a blockchain-based supply chain traceability system using smart contracts. In such contracts, manufacturers define the composition of products in the form of recipes. Each ingredient of the recipe is a non-fungible token that corresponds to a batch of physical goods. When the recipe is applied, its ingredients are consumed and a new token is produced. The given mechanism preserves the traceability of product transformations. The system is implemented for the Ethereum Virtual Machine and it applies to any blockchain configuration that supports it.
The author of the paper [5] discusses how the traditional cloud storage model runs in a centralized manner, so a single point of failure might lead to the collapse of the system. The system is a combination of the decentralized storage system, IPFS, the Ethereum blockchain, and attribute-based encryption technology. Based on the Ethereum blockchain, the decentralized system has a keyword search function on the ciphertext solving the problem in traditional storage systems where cloud server returns wrong results.
A blockchain-based solution to address the problems of the supply chain such as Double Marginalization and Information Asymmetry etc is given in [6]. The SCM systems provide information sharing and analysis to companies and support their planning activities. The sharing of data between manufacturers, suppliers, and customers become very important to ensure reactivity towards market variability in Supply Chain Management (SCM).
Shanahan et al. [7] Suggested an RFID-based framework for beef traceability from farm to slaughter. By using RFID for the identification of individual cattle, this system was proposed as a solution to the inaccessibility of traceability records and fraudulent activities. To build an automated system this integrates online traceability data and chill chain condition monitoring information, Abad et al. [8] Tried to validate an RFID smart tag developed for real-time traceability and cold-chain monitoring of food under the case study of an intercontinental fresh fish logistics chain.
Christian Esposito [8] focuses on the various opportunities of blockchain for usage in the health-care sector. This paper proposes an Ethereum blockchain technology for a decentralized healthcare database.
From this paper, we get the general idea of how a decentralized network can be brought into effect for the Product Ownership Management System. This concept can be used to exchange data between various stakeholders in a supply chain.
Folinas et al [10] pointed out that the efficiency of a traceability system depends on the ability to track and trace individual product and logistics units, in a way that enables continuous monitoring from primary production until final disposal by the consumer.

3. PROPOSED SYSTEM

The proposed system provides a reliable and secure product transaction history using blockchain. Blockchain-based POMS in SCM that works in a decentralized environment based on consensus algorithm.

Figure 1 shows the architecture of the proposed system followed by the details working of the system.

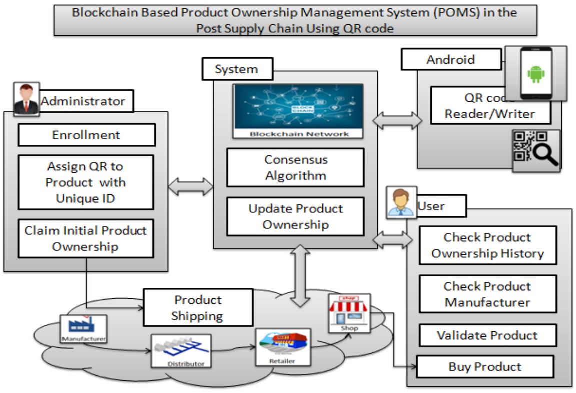

Figure: 1 System Architecture

3.1 Manufacturer Enrollment:

The manufacturer will enroll him with valid information on the blockchain with the company name and other details.

3.2 Assign QR code to the product:

The manufacturer will manufacture products and assigns a unique ID to each product with QR cod

3.3 Claim initial ownership of the product:

With the product, a unique ID admin can add a new transaction in blockchain to claim the initial ownership of the products. The detailed information of the product can fetch through the assigned QR code.

3.4 Shipping Product:

The manufacturer ships products to the Distributor where a distributor can check the manufacturer details and ownership of the products, etc. Distributor verifies the genuineness of the EPC using the assigned QR code and issues a transaction.

Ownership of the product will be transfer from the manufacturer to the distributor. Similarly, when any party receives products, a recipient follows the same procedure as above. At every time the product ownership transfer details are updated against the product's unique id through the QR code.

3.5 Check Product Ownership Using Blockchain:

Every product has its QR code, so through the QR code, we get the product history. The product history from manufacturing to shipping details is stored in the DB with the unique ID by using blockchain technology. So, after scanning the product QR code we get the unique identification number and through it, we get the overall product history.

3.6 Buying Product:

Customers should be able to buy products at the shop by validating the product information like the manufacturer of the product, Current owner of the product, etc using their assigned QR code. After that, the customer can buy and make a new transaction on the blockchain network if the product is valid or deny buying if fake product information is found in the product history.

4 .SYATEM FLOW

The below figure shows the overall flow of the system.

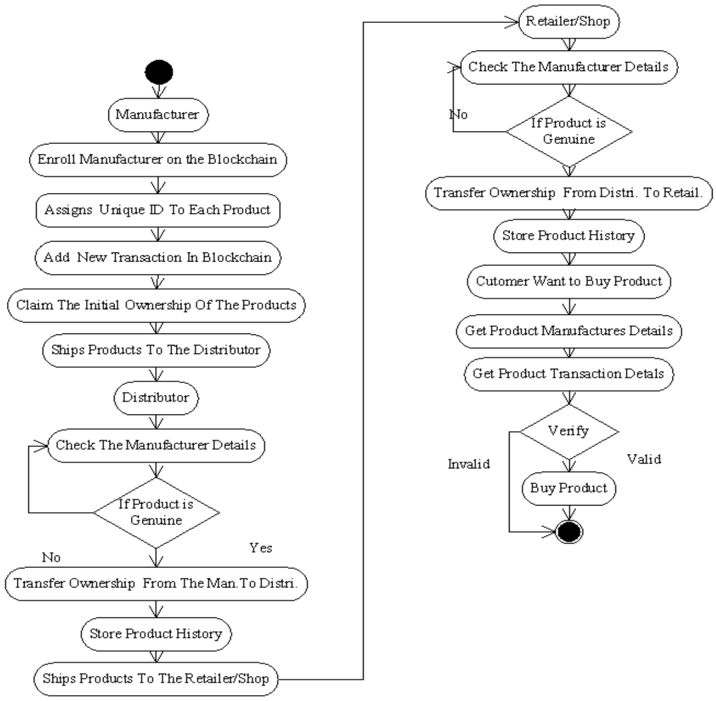

Figure: 2 System Flowchart

5. ALGORITHM USED

5.1 Consensus Algorithm:

In Consensus algorithm work in both decentralized and consortium way. Ethereum is used as a decentralized/permission-less consensus algorithm. Ethereum [1] [3] is a widely recognized and popular technology. Comparative protocols are likely also implemented on Ethereum, thus giving a better basis of comparison with protocols with similar goals.

5.1.1 Initialization Phase:

During the initialization of an election, a genesis contract must be placed on the blockchain (Algorithm 1).

Algorithm 1 Initialisation Phase

1: **procedure** ELECTIONGENESIS(*_candidates, _pubk, _lengthPhaseOne, _lengthPhaseTwo, _cancelBallots*)
2: $candidates \leftarrow \_candidates$
3: $pubk \leftarrow \_pubk$
4: $electionEndTime \leftarrow timeNow() + \_lengthPhaseOne$
5: $countEndTime \leftarrow electionEndTime + \_lengthPhaseTwo$
6: $cancelBallots \leftarrow \_cancelBallots$

5.1.2 Voting Phase (Initial Ballot):

To place a ballot on the blockchain, (Algorithm 2) the voter must have first communicated with the CA to receive a signed token authorizing the ballot.

Algorithm 2 Voting Phase - Initial Ballot

```
procedure PLACEBALLOT(vid,vote,msghashed, v,r,s)
    require((timeNow() < electionEndTime) And (verifyToken(msghashed,v,r,s))
    new InitialBallot(vid, vote)
procedure INITIALBALLOT(_vid,_vote)
    vid ← _vid
    vote ← _vote
    sealed ← true
    unsealedTimeStamp ← null
```

5.1.2 *Voting Phase (Altering Ballot):*

The process for pushing an altering ballot, (Algorithm 3) is similar to the process for creating an initial ballot.

Algorithm 3 Voting Phase - Altering Ballot

```
procedure PLACEALTERBALLOT(vid,vote,msghashed, v,r,s)
    require((timeNow() < electionEndTime) And (verifyToken(msghashed,v,r,s) And cancelBallots)
    new InitialBallot(vid, vote)
procedure ALTERINGBALLOT(_vid,_vote, _replacedBallot)
    vid ← _vid
    vote ← _vote
    replacedBallot ← _replacedBallot
    sealed ← true
    unsealedTimeStamp ← null
```

5.1.3 *Counting Phase:*

Once the election has concluded, votes will need to be counted (Algorithm 4).

Algorithm 4 Counting Phase

```
procedure RETRIEVEVOTE
    require(electionEndTime < timeNow())
    if isSealed then
        isSealed ← false
        unsealedTimeStamp ← timeNow()
    return(vote)
```

5.1.4 *Challenging Count:*

Nodes on the blockchain also have the functionality to examine the blockchain (Algorithm 5).

Algorithm 5 Challenging Count

```
procedure RETURNSEALED
    return(isSealed)
procedure RETURNTIMEUNSEALED
    return(unsealedTimeStamp)
```

5.2. EXPERIMENTAL RESULTS AND DISCUSSION

- USERS-

1. Company.
2. Manufacturer.
3. Distributor.
4. Retailer
5. End Users (Customer)

- Company sales their products to Manufacturer.

Following steps are that are taken to sale the product;

1. Selection of Product.
2. Changing the ownership

The ownership can be changed among;

- Company to Manufacturer
- Manufacturer to Distributor
- Distributor to Retailer
- Retailer to End Users

Example: -For transferring the ownership from Company to Manufacturer the following steps are performed;

- Transfer the generated OTP to the Manufacturer.
- Verify OTP of Manufacturer.
- The verified manufacturer will get the product's ownership.

But For transferring the ownership from Retailer to End Users the step changes as follows;

- View generated QR Code to User.
- Users can scan the QR code and get product ownership history.
- The user gets Ownership of the product.

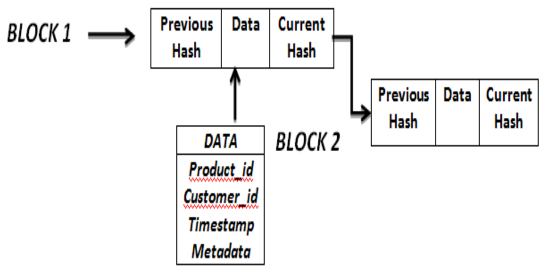

Figure 3: Structure of Block

- The above Figure elaborate the structure of blocks in the block chain.
- The block contains 3 parts **Previous Hash, DATA,** and **Current Hash**.
- The data in the block contain the following attributes:-

Product_id, Customer_id, Timestamp, Metadata.

- A separate block is generated for each transaction.
- For each product, a separate block chain is created.

6. CONCLUSION

Here we have developed a system that provides security to the product data and other details with blockchain technology in a manufacturing company. With the help of the system, we can also track the product ownership transaction history from the manufacturing stage to the end-user buying stage. With the use of this system, the customer can get valid product information when he wants to buy products. The proposed system is working for only verifying product ownership they do not give the transportation details. So, in the future, we implement a system that controls, monitors the product owner as well as the product transportation details. Also, we will use some hardware for checking the product quantity while product transporting or shipping.

7. REFERENCE

[1] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digitalsignature algorithm (ecdsa),” International Journal of Information Security,vol. 1, no. 1, pp. 36–63, 2001.

[2] MELISSA J. RUSINEK, HAO ZHANG, AND NICOLE RADZIWILL,"Blockchain for a Traceable, Circular Textile Supply Chain: A Requirements Approach" SQP VOL. 21, NO. 1/© 2018, ASQ.

[3] Po-Yeuan Chang1, Min-Shiang Hwang, and Chao-Chen Yang1,"A Blockchain-Based Traceable Certification System",Springer International Publishing AG, part of Springer Nature 2018.

[4] Martin Westerkamp ,Friedhelm Victor,Axel Küpper,"Blockchain-based Supply Chain Traceability: Token Recipes model Manufacturing Processes", 2018 IEEE International Conference on Blockchain, At Halifax, Canada.

[5] UIGUO YU et al, “Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network, IEEE Access November 28, 2017.

[6] Mitsuaki Nakasumi, “Information Sharing for Supply Chain Management based on Block Chain Technology”, 19th Conference on Business Informatic, IEEE, 2017.

[7] Shanahan, C., Kernan, B., Ayalew, G., McDonnell, K., Butler, F., & Ward, S., A framework for beef traceability from farm to slaughter using global standards: an Irish perspective. Computer and Electronics in Agriculture. 2009. 66(1), 62-69.

[8] Abad, E., et al., RFID smart tag for traceability and cold chain monitoring of food: demonstration in an intercontinental fresh fish logistic chain. Journal of Food Engineering. 2009, 93(4), 394-399.

[9] Christian Esposito, Alfredo De Santis, GennyTortora, Henry Chang, Kim-Kwang Raymond Choo.” Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy”. IEEE Cloud Computing, January / February 2018.

[10] Folinas, D., Manikas, I., & Manos, B., Traceability data managementfor food chains. British Food Journal. 2006, 108(8),622-633. 11