Countering Counterfeits on the Supply Chain with Blockchain

Saransh Rajput
Roll No. 2018114016

Manvith Reddy
Roll No. 2018101057

Shourja Mukherjee
Roll No. 2018101009

I. Problem Statement

The trade of counterfeit goods is a growing problem and is affecting the sales and profits of companies affected by this phenomenon. It is a common occurrence to receive a good that has been tampered or isn't the same quality as one would expect when ordering from an online service or even buying in person at a shop. This has the potential to pose severe danger when it affects industries like health and machinery where counterfeiting may even prove to be fatal. To ensure the identification and traceability of real products throughout the supply chain, we propose a fully-functional blockchain system to prevent product counterfeiting.

A. Motivation

Trade in counterfeit and pirated goods has risen steadily in the last few years – even as overall trade volumes stagnated – and now stands at 3.3% of global trade, according to a new report by the OECD and the EU's Intellectual Property Office (as of March, 2019). [1] This is a an extremely large scale problem that has plagued each and every one of us. Additionally, Using the wrong medicine [8], or installing a faulty machine part to big machinery may prove to be fatal when the product is put to use.

To fix this, we propose an end to end blockchain system in this paper that will allow for complete transparency and enables both manufacturers, consumers and sellers to track products at every step of the supply chain. It also seamlessly allows the existence of regulatory bodies such as the FDA [4] as well as the existence for intermediary entities like banks within the supply chain. Putting the supply chain on blockchain has other advantages as well. It significantly reduces paperwork, provides for better tracking of inventory. Each block in the chain is encrypted and distributed to all the participants. The blockchain thus provides a trustworthy and complete trail which makes auditing easier for banks. [9]

B. Who will be the beneficiaries?

Most Industries have multitudes of corporations working together to produce and deliver a product. Therefore, all of these industries take part in the supply chain where our blockchain solution will be deployed. Some examples are -

- Apparel and Accessories
- Pharmaceuticals
- Food
- Cosmetics
- Electronics
- Military items

C. How big is the impact of your problem?

According to Forbes, in 2018 counterfeiting was the largest criminal enterprise in the world. Sales of counterfeit and pirated goods totals $1.7 trillion per year, which is more than drugs and human trafficking. It is expected to grow to $2.8 trillion and cost 5.4 million jobs by 2022. About 5% of goods imported into the European Union in 2013 were fakes, according to the OECD.

Growing over 10,000% in the last two decades, counterfeit products exist in virtually every industry sector, including food, beverages, currency, etc. The spread of counterfeit goods is worldwide, with the International Chamber of Commerce (ICC) in 2008 having estimated the global value of all counterfeit goods at $650 billion annually, increasing to $1.77 trillion by 2015. By 2017, the U.S. alone was estimated to be losing up to $600 billion each year to counterfeit goods, software piracy and the theft of copyrights and trade secrets. [1]

II. Solution

We propose an end to end blockchain system in this paper that will allow for complete transparency and enables both manufacturers, consumers and sellers to track products at every step of the supply chain. Further, we enable organizations like banks to make easy decisions on offering loans to manufactures/sellers because every transaction is made public and money which would otherwise be used in countless audits is saved. Our system also accommodates space for regulatory agencies like the FDA to authorize/approve products. Let us take a closer look at how they all work together in our blockchain system.

A. Architecture

Our Supply chain system based on Blockchain is composed of five main roles, the Manufacturer Role, the Seller Role, the Customer role, Regulatory Agencies (FDA for the the food/drug industry) and financial entities like Banks which offer loans. Explained below is the basic functionality that each role will be able to fulfill (Fig 1 gives a pictoral view of the functionality):

- Manufacturer Role: The manufacturer is the one making the authentic products and distributing them to various sellers. The manufacturer will have the power to add new

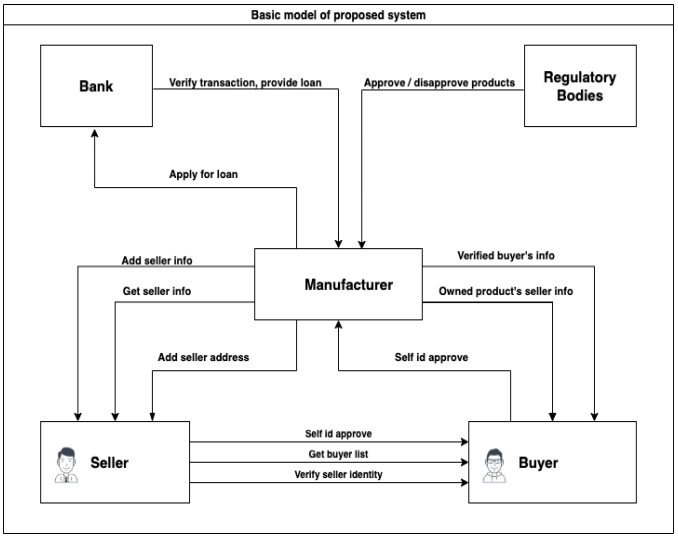

Fig. 1. Basic Model

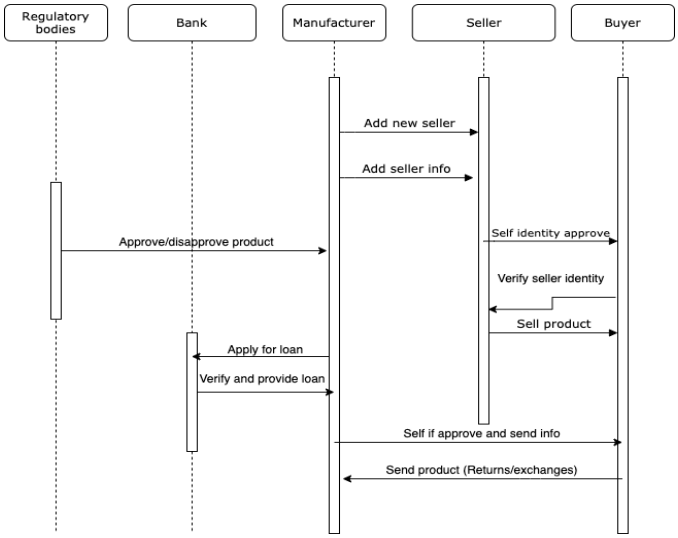

Fig. 2. Purchase flow

seller's address on contracts, adding the number of products that the seller can sell, and retrieving information on sellers so that the latest sales status can be retrieved. The manufacturer will also interact with the customer and will be able to verify whether the product has yet been exchanged or confirm if the current status of the product has yet been verified by the consumer's public key certificate. Manufacturer can use transactions with the seller as proof to banks and receive loans. The regulatory agencies can approve/disapprove of the products made by the manufacturer which will be notified to sellers and consumers when they buy the product.

- Seller Role: The seller buys products from multiple manufacturers and sells them to various customers. The seller can use the system's functions to encrypt the verification information with a private key, and the consumer can use the seller's public key to verify if the seller is what he claims to be. After buying and selling, the seller specifies the purchaser's address in the contract for the manufacturer to obtain the information. The seller can access information about his products, such as sales lists, and the quantity of his remaining stock.
- Customer/Consumer Role: The customer/consumer is a user which buys products of sellers. In our system, the consumer can verify whether the seller has a sales relationship with the manufacturer and also verify whether the seller's stock hasn't been yet sold out. Additionally, the consumers can prove that their identity is consistent with their address and in the case of a well-preserved contract address, the consumers can obtain individual purchase records and product status in their product.
- Regulatory Agencies : Regulatory Agencies are entities like the FDA which have the authority to approve/disapprove products. Only products approved by the FDA will be allowed to be put up for sale.
- Banks : Much of the supply chain runs on loans. In the current system, banks spend millions on audits to determine whether the loan will be worth to a manufacturer. On our blockchain, since all transactions are visible, it makes it much easier for the banks to determine whether the manufacturer will be able to pay off his loan.

B. Smart Contracts

The proposed system uses Ethereum [5] as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity as the high-level programming language for writing smart contracts. If we build a frontend, we will be using react.js alongside drizzle to build the complete Dapp. There is also a potential for using hyperledger [3]. Given below is brief abstract along with examples of how our code will be structured.

1) Entering the Blockchain : Each user must enter the blockchain with a specific role to be able to avail its services. This step is crucial and must be done with utmost care in the real world as different roles will have different privileges. Each role will be designed as a struct and functions in the smart contract will be run based on this authorization. Given below is the rough pseudocode for registering a seller.

Algorithm 1 NewSeller

```
1: if isManufacturer then
1:     Seller.sellerAddress ← newSellerAdd
1:     Seller.sellerProductNum ← productNum
2: else
2:     Alert, Only a manufacturer can add a seller
3: end if=0
```

2) Transparency of Information: With the goal of information disclosure, the information about sellers, manufacturers, products is completely public. Our system

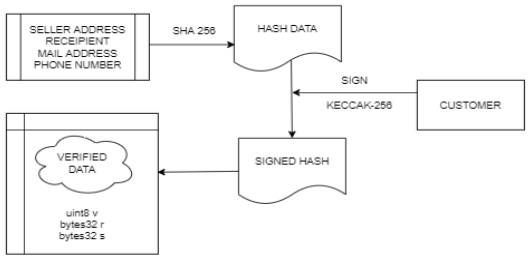

Fig. 3. Flowchart for Customer sign data

provides smart contract data search functions, which can return the seller list, manufacturer list, all seller information, and the remaining number of products of each seller.

3) Transactions on Smart Contracts: When the transaction between seller and consumer is established, the seller will add the consumer address in the smart contract. Each seller has a product structure in the seller structure, the seller will put the consumer addresses into the product owner field. Additionally, the access rights of the seller's product owner field can only be set by the seller.
4) Verification: Verification is one of the most important components in our system. Users in our system can use their address as their own representation. Whenever a user wants to make a change of current Ethereum contract state, the user has to sign the transaction with his private key to make a digital signature. As long as the user's private key is safe, there will be no other means to modify the user's identity.

   To prove a user's identity to each other when necessary, our system allows users to use their private key to sign data and also provides the user with a function on which they can verify one another. Before conducting a transaction with the seller, the consumer needs to ask the seller for a proof of identity.

   The consumer will provide the seller with a message that is to be encrypted. Then, the seller will call a function to encrypt the message, the function will concatenate the message and the current time, and will proceed to encrypt them. The system will then return the v, r, s, and the encryption time back. The seller will then send v, r, s, the encryption time, and the seller address to the customer.

   After the consumer acquires the essential information to verify the identity of the seller, the consumer will then call our system verification function to verify whether the seller identity is correct. Given below are two pseudo functions for verifying a seller.

III. Why do we need a blockchain?

When blockchain record keeping is used, assets such as units of inventory, orders, loans, and bills of lading are given unique identifiers, which serve as digital tokens (similar to

Algorithm 2 SellerSigns

0: data ← concatenateTheInfoTheSellerWillSign
0: dataHash ← dataShaHash
0: signedHash ← sellerPrivateKeySignDataHash
0: separate sginedHash into v, r, s where v r, and s are the values for the transaction's signature =0

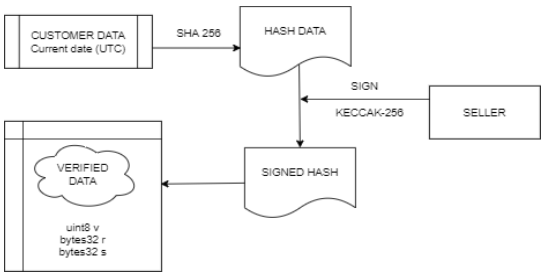

Fig. 4. Flowchart for seller sign data

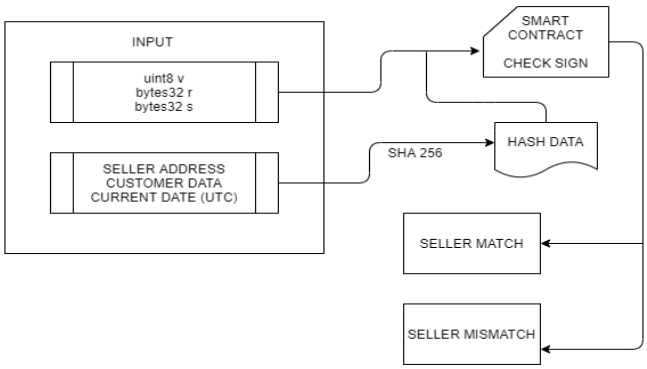

Fig. 5. Flowchart of customer verified seller identity

Algorithm 3 SellerVerify

0: data ← concatenateTheInfoTheSellerSigned
0: dataHash ← dataShaHash
0: signedHash ← sellerPrivateKeySignDataHash
0: call Verification function in smart contract with v, r, s where v r, and s are the values for the transaction's signature
1: **if** signaturematchtheselleraddress **then**
1: The seller is verified
2: **else**
2: The seller is faked
3: **end if**=0

bitcoins). Additionally, participants in the blockchain are given unique identifiers, or digital signatures, which they use to sign the blocks they add to the blockchain. Every step of the transaction is then recorded on the blockchain as a transfer of the corresponding token from one participant to another. No participant can overwrite past data because doing so would entail having to rewrite all subsequent blocks on all shared copies of the blockchain.

A. Why would the solution not be possible without a blockchain?

Execution faults—like errors in inventory data, lost shipments, and duplicate payments—are very hard or even impossible to track in real time. [10] Even when a problem is discovered after the fact, it is difficult and expensive to pinpoint its source or fix it by tracing the sequence of activities recorded in available ledger entries and documents. Although ERP systems capture all types of flows, it can be tough to assess which journal entries (accounts receivable, payments, credits for returns, and so on) correspond to which inventory transaction. This is especially true for companies engaged in thousands of transactions each day across a large network of supply chain partners and products. [7]

Making matters worse, supply chain activities are often extremely complicated—far more so than the exhibit depicts. For example, orders, shipments, and payments may not sync up neatly, because an order may be split into several shipments and corresponding invoices, or multiple orders may be combined into a single shipment. [2]

B. What form of blockchain would be suitable?

Based on our requirements, we would prefer to use a permissionless blockchain such as Ethereum [6] to develop our use case. Therefore, the proposed system uses Ethereum as the back end Blockchain operating system and uses Ethereum's proprietary programming language Solidity as the high-level programming language for writing smart contracts.

IV. Analysis

1) Users generate their own public and private key. Private key is used to sign data, and public key is used to verify the authenticity of the signed data. As long as the private key is kept secure, any data will not leak.
2) Anonymity: Each user is anonymous. A user can have multiple roles but when the system is operating, only one of them is used as the identification. It's highly unlikely that the anonymous address be mapped to the real person, thereby protecting the user's privacy.
3) Transparency and traceability: The data in Blockchain is completely public and anyone can inquire. Within the information flow, one can clearly see who is passing data to whom as a continuous transaction log is mainatined. So it can be easily verified if the product that seller claims is original or not.
4) The overall cost of using our system for preventing counterfeited products would be remarkably low cost to implement, and very straightforward to apply. By paying a very low transaction fee, users of our system no longer need to be concerned about the possibility of acquiring a counterfeited product.

V. Future Work

A. Adding Warehouses

For now, we have only designed the system to include the essential parts of a supply chain. However, we can further extend this to include the various intermediary warehouses and provide tracking of the product as it moves along the supply chain. Implementation of this would require further security.

B. Simpler Consensus Protocols

Blockchain requires a consensus protocol—some mechanism for maintaining a single version of the history of transactions that is agreed to by everyone. Proof of Work is too slow to handle the speed and volume of transactions in supply chains. Therefore, It would be wise to use/develop other kinds of Consensus protocols to keep up speed with the supply chain.

C. Simplifying Code

The total cost of running an application on the Ethereum public chain is directly related to the code simplicity of the distributed application. The future work of this system can be making the code simpler. The customer can trust the distributed application because of the simplicity of code, and no redundancy code in it will have additional consumption.

References

[1] Wikipedia - Counterfeit Consumer goods
https://en.wikipedia.org/wiki/Counterfeit_consumer_goods
[2] Building a Transparent Supply Chain by Vishal Gaur and Abhinav Gaiha
https://hbr.org/2020/05/building-a-transparent-supply-chain
[3] (2018). Hyperledger.
https://www.hyperledger.org/
[4] Blockchain Technology for Detecting Falsified and Substandard Drugs in the Pharmaceuticals Distribution System by Patrick Sylim et al.
https://www.researchgate.net/publication/326286259_Blockchain_Technology_for_Detecting_Falsified_and_Substandard_Drugs_in_the_Pharmaceuticals_Distribution_System_Preprint
[5] Wikipedia - Ethereum
https://en.wikipedia.org/wiki/Ethereum
[6] ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER by DR. GAVIN WOOD.
https://gavwood.com/paper.pdf
[7] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," IEEE Access, vol. 5, pp. 17465–17477, 2017.
https://ieeexplore.ieee.org/document/7961146
[8] World Health Organization. (2017). A study on the public health and socioeconomic impact of substandard and falsified medical products. Geneva: World Health Organization; 2017.
http://www.who.int/medicines/regulation/ssffc/publications/s
[9] S. Matthew English and E. Nezhadian, "Application of bitcoin datastructures design principles to supply chain management," 2017
http://arxiv.org/abs/1703.
[10] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.
https://www.researchgate.net/publication/321057052_Adaptable_Blockchain-Based_Systems_A_Case_Study_for_Product_Traceabil