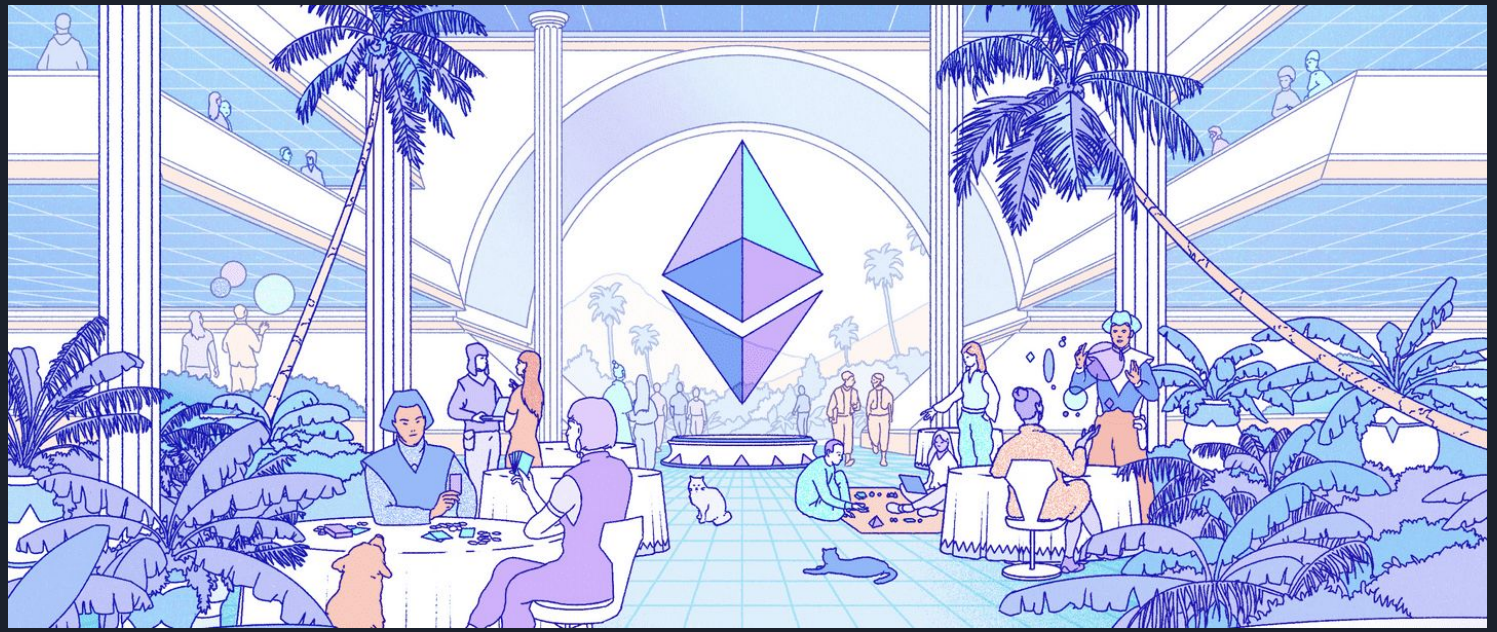
Blockchain Enabled AntiCounterfeiting Suite

by Aditya Mondal
(1MV18EC004)



Powered by Ethereum

For the next generation web

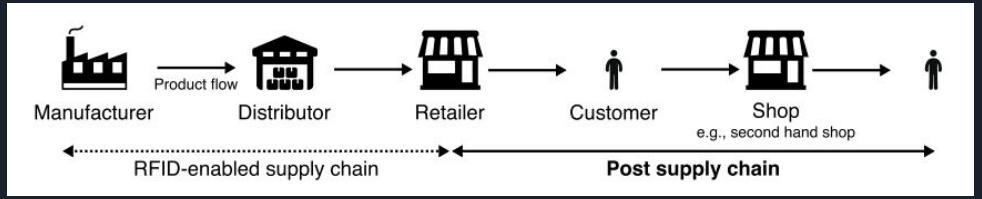
Introduction

1. The total trade in fakes is estimated at around $4.5 trillion, and fake luxury merchandise accounts for 60% to 70% of that amount, ahead of pharmaceuticals and entertainment products.
2. For years, the luxury industry has waged a battle against counterfeiters. It has invested heavily in ultra-sophisticated tech solutions which use the latest advances in nanotechnology, internet of things (IoT).
3. Supply chains, manufacturing, and pricing are often controlled by relocating production to low-cost countries. The outsourcing also led to relaxed control over supply chain, design ,and manufacturing just as counterfeiters were putting unprecedented pressure on each of these processes.
4. Anti-Counterfeit Packaging Market Worth $ 17.47 Billion, Globally, by 2027 at 17.25% CAGR.

Problem Statement

For more than a decade now, radio frequency identification (RFID) technology has been quite effective in providing anti-counterfeits measures in the supply chain. However, the genuineness of RFID tags cannot be guaranteed in the post supply chain, since these tags can be rather easily cloned in the public space. Here, we explore a novel approach of RFID-attached products to detect anti-counterfeits and explore a solution that can be used in the post supply chain. For this purpose, we leverage the idea of Bitcoin's blockchain that anyone can check the proof of possession of balance. With the proposed solution, a customer can reject the purchase of counterfeits even with genuine RFID tag information, if the seller does not possess their ownership. We implement a proof-of-concept experimental system employing a blockchain-based decentralized application platform, Ethereum, and evaluate its cost performance.

Literature Survey



System Model

The typical product flow consisting of two chains, namely the RFID-enabled and post supply chains. The first one is typically composed of three parties, i.e., manufacturers, distributors, and retailers. A manufacturer creates, composes, and ships products to the distributors while they decompose the received products and ship them further to the retailers. In the post supply chain, retailers stock and sell their products to customers who in turn may resell them, e.g. at a second hand shop or over the Internet.

- For over a decade now, RFID technology has been integrated into the supply chain for anti-counterfeits. The first systematic RFID-based approach for anti-counterfeits in the food and drug industry was proposed by the FDA (Food and Drug Administration) in the USA. In their proposal, each supply chain party is equipped with RFID readers and keeps track of shipping and receiving events for each product. In this way, the supply chain parties have the ability to track and trace the product flow of products.
- Such an approach is vulnerable against cloned tags. Specifically, once RFID tags attached to the genuine products are copied by an attacker, counterfeits with cloned RFID tags can be inserted in the supply chains. In this way, counterfeits with cloned tags cannot be identified by the aforementioned track and trace approach.

Blockchain

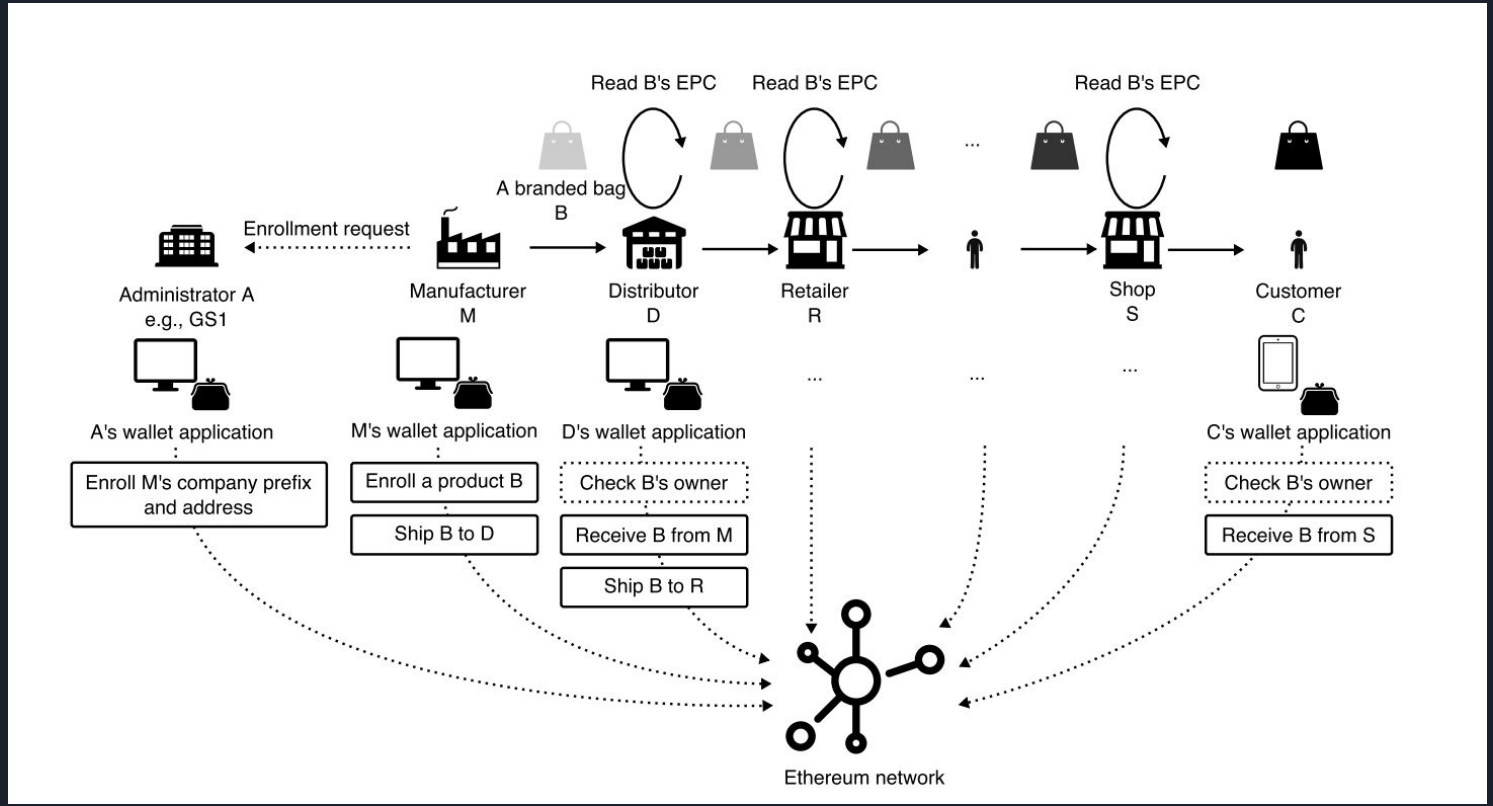
- Immutable Distributed Ledger Technology : which is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.
  - A blockchain is a type of database. It differs from a typical database in the way it stores information; blockchains store data in blocks that are then chained together.
  - As new data comes in it is entered into a fresh block. Once the block is filled with data it is chained onto the previous block, which makes the data chained together in chronological order
  - Different types of information can be stored on a blockchain but the most common use so far has been as a ledger for transactions.
  - In Bitcoin’s case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.
  - Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.

Objective

Leveraging the DLT we create a system in which the possession of the product can be proven in the public ledger, also referred to as the blockchain. We allow

- Only the legitimate manufacturers are able to claim the initial ownership (origin) of products (EPCs or Electronic Product Codes);
- Each manufacturer can declare only their own products;
- The Products be trackable under the blockchain;
- The events ‘‘Shipped’’ and ‘‘Received’’ can be separated;

Methodology Followed



enrollManufacturer

```
146
147     /*
148      *  Registers a Manufacturer with the blockchain
149      *  @params
150      *  _manufacturerAddress: address of the manufacturer
151      *  _companyPrefix: Unique prefix assigned by the Admin
152      *  _companyName: Name of the company
153      *  _validityTime: Time for which the company is valid in the blockchain
154      *
155      *  @emits
156      *  ManufacturerCreated event
157      */
158     function enrollManufacturer(
159       address _manufacturerAddress,
160       uint256 _companyPrefix,
161       bytes32 _companyName,
162       uint256 _validityTime
163     ) external onlyOwner {
164       ManufacturerInfo memory _info = ManufacturerInfo(
165         _companyName,
166         _companyPrefix,
167         block.timestamp + _validityTime
168       );
169
170       _manufacturers[_manufacturerAddress] = _info;
171
172       emit ManufacturerCreated(_companyName, _companyPrefix, _info.expireTime);
173     }
174
```

enrollProduct

```
174
175     /*
176      *  Registers a Product with the blockchain
177      *  @params
178      *  _EPC: electronic product code (EPC) of the Product
179      *
180      *  @emits
181      *  ProductCreated event
182     */
183     function enrollProduct(uint256 _EPC) onlyNotExist(_EPC) onlyManufacturer() external {
184         ManufacturerInfo memory _info = _manufacturers[msg.sender];
185         _EPCtoCompanyPrefix[_EPC] = _info.companyPrefix;
186         _companyPrefixToAddress[_info.companyPrefix] = msg.sender;
187
188         products[_EPC].owner = msg.sender;
189         products[_EPC].status = ProductStatus.Owned;
190         products[_EPC].creationTime = block.timestamp;
191         products[_EPC].nTransferred = 0;
192
193         emit ProductCreated(_EPC, msg.sender, products[_EPC].creationTime);
194     }
195
```

shipProduct

```
196     /*
197      *  Ships the Product
198      *  @params
199      *  _recipient: address of the expected recipient of the product
200      *  _EPC: Electronic Product Code of the Product
201      */
202     function shipProduct(address _recipient, uint256 _EPC)
203     onlyExist(_EPC) onlyProductOwner(_EPC) onlyStatusIs(_EPC, ProductStatus.Owned) external {
204         require(msg.sender == products[_EPC].owner, "Sender is not the Owner");
205 
206         products[_EPC].status = ProductStatus.Shipped;
207         products[_EPC].recipient = _recipient;
208     }
```

receiveProduct

```
210     /*
211      *  Recieve the Product
212      *  @params
213      *  _EPC: Electronic Product Code of the Product
214     */
215     function receiveProduct(uint256 _EPC) onlyExist(_EPC)
216     onlyRecipient(_EPC) onlyStatusIs(_EPC, ProductStatus.Shipped) external {
217         products[_EPC].owner = msg.sender;
218         products[_EPC].status = ProductStatus.Owned;
219         products[_EPC].nTransferred = products[_EPC].nTransferred + 1;
220     }
221
```

Outcome

Counterfeits can be easily detected post supply chain. And a counterfeits is identified as follows,

1) The seller possesses counterfeits with fake EPCs;
2) The seller possesses counterfeits and knows their true EPCs but does not possess their ownership;
3) The seller owns the genuine product and its ownership and possesses a number of counterfeits too.

Conclusion

A novel blockchain-based product ownership management system has been developed for the post supply chain, which makes the efforts of counterfeiters to clone genuine tags redundant since they cannot prove the possession of products on this system.

1. The overall practical system requirements have been identified,
2. Introduced a full-fledged protocol that enables each party, including supply chain partners and customers, to transfer and prove the ownership of RFID tag-attached products.

Future Scope

There can be more improvements and extensions of the Project. The Future Scope of the project can be as follows,

1. Write an extensive test suite to test the utilities and functions of the contracts,
2. Audit the contracts for bugs and possible hacks by some professional cybersecurity or blockchain security firm,
3. Build a Dapp (Decentralized Application) to consume the contracts and provide a UI,
4. Incentivize the users to keep using the application to update the owners by introducing some tokenomics.

References

1. Investopedia : https://www.investopedia.com/terms/b/blockchain.asp
2. The Economist : https://www.economist.com/business/2015/07/30/counterfeitcom
3. Harvard Business Review : https://hbr.org/2019/05/how-luxury-brands-can-beat-counterfeiters
4. Ethereum : https://ethereum.org/en/