

# Authentication of Product & Counterfeits Elimination Using Blockchain

Tripti Rathee<sup>1</sup>, Manoj Malik<sup>2</sup>

<sup>1,2</sup>*Department of Information Technology, MSIT, Janakpuri, New-Delhi, India*

**Abstract-** Blockchain technologies have gained interest over the last years. While the most explored use case is financial transactions, it has the capability to agitate other markets. Blockchain remove the need for trusted intermediaries, can facilitate faster transactions and add more transparency. This paper explores the possibility to deflate counterfeit using blockchain technology. This paper provides an overview of different solutions in the anti-counterfeit area, different blockchain technologies and what characteristics make blockchain especially interesting for the use case. We have developed three different concepts and the expansion of an existing system concept, is pursued further. It is shown, that reducing counterfeits cannot be achieved by using technological means only. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging are all important aspects. These factors combined with blockchain technology can lead to an efficient and comprehensive approach to reduce counterfeiting

**Keywords – Authentication, Blockchain, Encryption**

## I. INTRODUCTION

Although it may seem like a far off idea, we are surrounded by a lot of counterfeits. From fashion and retail products to software, digital media, electronics, piracy, and intellectual property, reports put the cost of counterfeiting somewhere around \$600bn a year in the US alone. In fact, the International Chamber of Commerce predicts that the “negative impacts of counterfeiting and piracy are projected to drain US\$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022. In Pharmaceuticals, the counterfeit medicine market is now responsible for around 1 million deaths per year, in an industry estimated to be worth \$75bn annually. In fact, the counterfeit medicine industry is estimated to be growing at twice the rate of legitimate pharmaceuticals, making it up to 25 times more lucrative than the global narcotics trade. Trust is a central element in all transactions. No matter if sending money or exchanging goods, it becomes difficult if there is no trust between the entities involved. It becomes even more difficult, as with many transactions, third parties are involved, such as banks. Often, not only one third-party is involved in a transaction, but multiple. An international money transfer does not only include the bank of the sender, the bank of the receiver, but also multiple intermediary entities such as clearing houses. The entities involved in the transaction do not only have to trust each other, but also the third parties. Removing these third parties can decrease transaction cost, facilitate faster transactions and add more transparency. Bitcoin has successfully shown that removing such third-parties is possible. The cryptocurrency permits direct sending coins to a transaction partner, without the need to use banks and clearing houses. The assets are directly transferred from one account to another. There are no intermediaries and thereby no need to trust third parties. In addition, the question if a transaction is valid is not answered by an institution, but by algorithms used. Therefore, it completely removes the need to trust any third party. The technology behind Bitcoin, the blockchain, can however not only be used for financial transactions and crypto currencies in general. The technology has potential to “redefine the digital economy” [10], because it allows immutable transactions, which can be checked at all times from everyone. This is because the information is publicly available and distributed globally. It is “chronologically updated and cryptographically sealed” [11]. The full range of applicable use cases for this technology has to be seen, but tracking ownership and history of a product is surely one of them [12]. This paper explores the possibility to reduce counterfeit using blockchain technology.

Authentication ,the act of establishing or conforming something as genuine. Authentication is of utmost importance because the use of counterfeit medicines can be harmful to the health and wellbeing of the patients. Their use may result in treatment failure or even death. Authentication is generally done through the overt or covert features upon the product [13, 14].

“We now have more fakes than real drugs in the market.” — Christophe Zimmermann, the anti-counterfeiting and piracy coordinator of the World Customs Organization [6]. Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. This architecture results in issues such as single point processing, storage, and failure. Blockchain technology has emerged to provide a promising solution for such issues. In this paper, we propose the block-supply chain, a new decentralized supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC) technologies. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security. Our simulations show that the proposed protocol

offers remarkable performance with a satisfactory level of security compared to the state of the art consensus protocol Tendermint.



Fig. 1.1 Challenges in counterfeit elimination

The rest of the paper is organized as follows. The background of anti-counterfeits approaches is explained in section II. The architecture and Requirement specification are presented in section III. Implementation details are given in section IV. Concluding remarks are given in section V.

## II. BACKGROUND

### 2.1 Anti Counterfeits Approach

Anti-counterfeiting solutions should protect organizations from financial and reputation losses, and, especially in the case of pharmaceutical products, customer safety. [15] argues that good anti-counterfeiting techniques should generally be simple to apply, but difficult to imitate and have four main features: They should be difficult to duplicate, it should be possible to identify them without special equipment, it should be difficult to re-use them, and it should be visible if they were tampered with. From a product perspective, there are three general technologies to reduce counterfeits [15]:

Overt (Visible) Features expected to assist the users to confirm the genuineness of a pack. Such features will be significantly visible, and complex or expensive to reproduce.[16] . This includes holograms, color shifting inks, security threads, water marks etc. The advantage of overt technologies is that they can be checked by the end consumer.

Covert (Hidden) Features the rationale of a covert feature is to aid the brand owner to recognize a counterfeit product. The general public will not be aware of its presence nor will have the resources to confirm it. This includes UV, bi-fluorescent and pen-reactive ink, as well as digital watermarks and hidden printed messages. Covert technologies help to identify counterfeits in the supply-chain and are especially efficient combined with overt technologies.

Track and trace includes Radio Frequency Identification (RFID) tags, Electronic Product Codes (EPCs) and barcodes. Track and trace technologies allow for simpler tracing of products, thereby enabling the reduction of counterfeits, as the history of a product is available. The tag or barcode is included by the manufacturer. Distributors scan the identification, enabling them to check the authenticity of the product and update the status. Finally, retailers can also scan the product, to check the history and authenticity of the product. This approach does not only tackle the counterfeit problem, but also enables track and trace through the whole product lifecycle.

### 2.2 Secondary Factors For Anti-Counterfeiting Approaches

Protecting the production is, however, not enough to decrease counterfeiting. [17, 18] have identified further factors to reduce counterfeits:

Monitor, deter, and remove counterfeits [17]: Companies need to ensure that they have the legal protection and registrations in place to be protected against counterfeits, this includes trademarks, copyrights, design patents etc. With this in place, it can still be costly to actively fight against counterfeits. Especially luxury goods companies spend millions to actively fight counterfeits and work together with private investigators. Having a budget for acting upon counterfeits is therefore important.

Controlling outsource suppliers [17]: Many companies use outsourced suppliers. This opens the risk that the outsourced supplier will not only produce legitimate products, but also counterfeits, with having access to all the original assets. Outsourcers should be carefully evaluated and monitored. Another option is to not outsource the whole product to one company, but split the product manufacturing to multiple companies, or keep part of the production in-house. This ensures, that no single external company has all the assets to create counterfeited products. It must also be ensured, that upon contract termination, all assets are returned to the outsourcing company.

Developing early warning signals of counterfeiting [17]: Counterfeits are often not discovered for a significant time. This leads to issues, as the longer counterfeits have been available, the more they can spread and finding the source becomes more difficult. Organizations therefore should have warning signals in place to identify counterfeits.

Increase Awareness [18]: Approaches which help to identify counterfeits do not help, if there is no awareness of the issue with counterfeits. Especially critical for pharmaceuticals, the public must be aware of such products.

Support of the analytics [18]: If a product is suspected to be a counterfeit, it should be analyzed as soon as possible. This typically starts with a visual inspection of the packaging, the packaging content (such as leaflets) and the medicine itself. If the product turns out to be counterfeited, the risk should be evaluated and patients informed. Furthermore, law agencies should take the requisite steps to identify where the counterfeit has come from and act upon it. This fights counterfeit by increasing awareness and by fighting criminal organizations introducing counterfeits.

### 2.3 Blockchain

Basically, blockchain is a peer-to-peer network where the interconnected systems are fully open and transparent to each other [1]. It consists of N number of blocks which are chained together to form a Blockchain. Each and every block consists of the transactions which have been signed by the peers. The entity which becomes the part of the blockchain is called as node. Every transaction is verified and validated before it is added to the block. The first introduction of a blockchain was by Satoshi Nakamoto in 2008 and implemented as a core part of Bitcoin. There are various blockchains with different goals (e.g., Bitcoin uses its own blockchain called Bitcoin blockchain [1], whereas Ethereum uses its own blockchain called Ethereum blockchain [13]) but the followings are common elements.

## III. PROPOSED ARCHITECTURE AND REQUIREMENT SPECIFICATION

### 3.1 Architecture

In perspective of a user, a user is able to do the following thing in the specified order to check the authenticity of the product.



Fig. 3.1 Example Product QR code

- (i) Scan QR/NFC (example Fig 3.1) tag of the Product using any scanner present on a mobile phone.
- (ii) The scan will open a page in the browser, The product info is requested from the Authentication Module. Authentication module verifies if it is a genuine request, if yes, it creates a new entry of scan in the database and blockchain and sends response with the Product data and its scan history.
- (iii) Browser shows if the product is authentic and shows its scan history. User is able to view the scan history to check for any anomalous scan history.

### 3.2 Proposed Blockchain Data Store

Service that sits between the Blockchain module and the user. It handles the product data and can (i) Create product transactions in Database & Blockchain. (ii) Initiate new block creation. (iii) Retrieve product data. (iv) Authenticate scans and notify if genuine

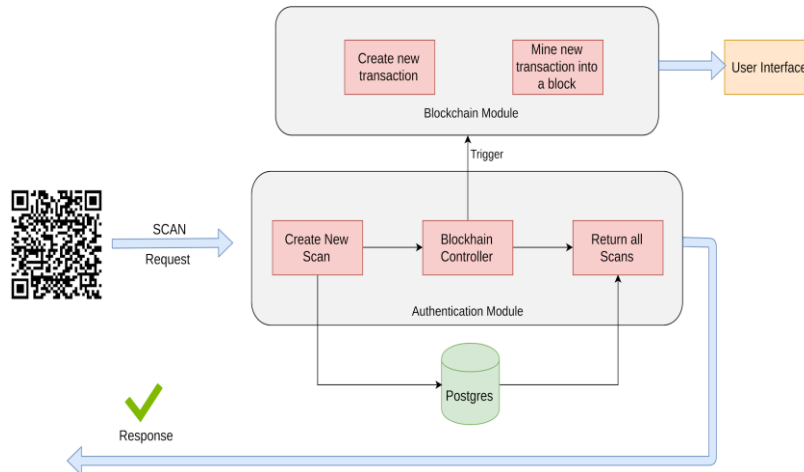


Fig. 3.2 Core Architecture: Authentication module connecting database and blockchain

### 3.3 Specifications

The basic working implementation of this requires a blockchain and a node server working on the network. A simple blockchain with in-memory storage, a simple proof of work algorithm and a consensus algorithm to resolve conflicts is required.

### 3.4 Blockchain Specifications

**Transactions:** A transaction contains the file hash and any metadata about the files, like the author name, created at, updated at timestamps etc.

**Proof of Work:** A simple proof of algorithm: Find a number that when hashed with the previous block's solution, a hash with 4 leading 0s is produced.

**Consensus:** It means that the nodes in the network agree on the same state of a blockchain.

**Consensus Algorithm:** "Longest verifiable chain is the authoritative chain."

**Decentralized:** Multiple servers can be spun up on different ports of a same node or on different nodes on the same network. Each node has to register itself with the other node with the nodes/register' api.

## IV. IMPLEMENTATION DETAILS

### 4.1 Customer Ui:

The Blockchain transactions and blocks can be visualized in a UI can be seen in Fig. 4.1

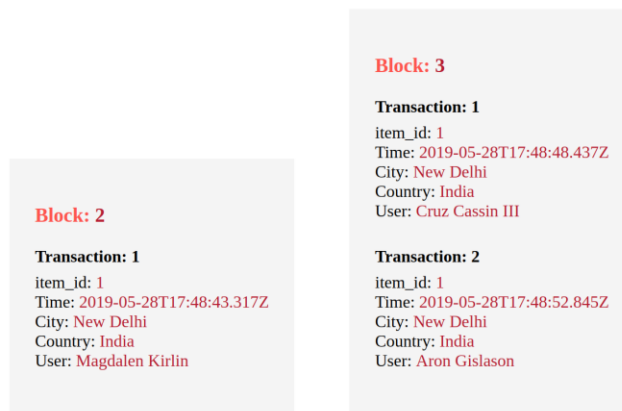


Fig. 4.1 Visualizing the blocks

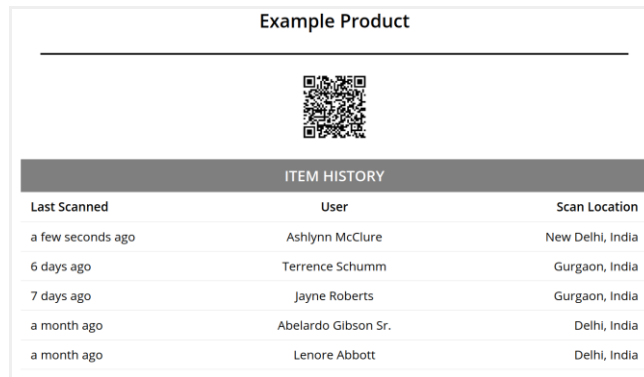
### 4.2 Database

Store metadata of products storage using PostgreSQL

CLIENT:

Scans QR Code or NFC tag using any Application QR Code or NFC have encoded data within them, which point to the product.

Every time the code is scanned, a new immutable entry is created in the Chain as shown in Fig. 4.2



The screenshot shows a web interface for an 'Example Product'. At the top, there is a QR code. Below it is a table titled 'ITEM HISTORY' with three columns: 'Last Scanned', 'User', and 'Scan Location'. The table contains five rows of scan data.

Last Scanned	User	Scan Location
a few seconds ago	Ashlynn McClure	New Delhi, India
6 days ago	Terrence Schumm	Gurgaon, India
7 days ago	Jayne Roberts	Gurgaon, India
a month ago	Abelardo Gibson Sr.	Delhi, India
a month ago	Lenore Abbott	Delhi, India

Fig 4.2 Client showing scans of a Product

#### 4.3 Authentication Module:

Allow addition of new products and items

Creates Unique QR Code for each item as seen in Fig. 3.1

Every time the code is scanned:

Trigger New Scan and save details in Postgres Database

Trigger a creation of new transaction in Blockchain

After a while Trigger a mining action to Blockchain. Blockchain mines recent transactions into a new Block.

#### 4.4 Nodejs Authentication Server

Serve Product scan page with product and scan history data to client

Record new scan data in PostgreSQL

Initiate a block creation in Blockchain

```
Sending data to Blockchain
POST /items/1/scans 201 83.334 ms - 20
{ message: 'Transaction will be added to Block 2' }
Mining new block
{ index: 2,
  message: 'New Block Forged',
  previous_hash:
    'bbe4b89ce4dd12ec66c4a6791ec0a9fd6ed3131fd123c1e65bd5c8c82cb1a7d3',
  proof: 1844,
  transactions:
    [ { city: 'New Delhi',
      country_name: 'India',
      dealt_via: 'Lexi Emarad',
      item_id: 1,
      time: '2019-05-28T18:00:35.420Z' },
      { city: 'New Delhi',
        country_name: 'India',
        dealt_via: 'Murray Reichel',
        item_id: 1,
        time: '2019-05-28T18:00:39.408Z' },
      { city: 'New Delhi',
        country_name: 'India',
        dealt_via: 'Mrs. Easter Schroeder',
        item_id: 1,
        time: '2019-05-28T18:01:05.313Z' },
      { city: 'New Delhi',
        country_name: 'India',
        dealt_via: 'Lawson Christiansen',
        item_id: 1,
        time: '2019-05-28T18:01:31.154Z' } ] }
```

Fig. 4.3 Authentication server logs

#### 4.5 Blockchain Creating Blocks And Mining:

On startup, create the genesis block

Node server initiates creation of new block and send the required data

Create a new block with the scan data.

Mine the block.

```
Adding the New Transaction
{
  'city': 'New Delhi',
  'country_name': 'India',
  'dealt_via': 'Lawson Christiansen',
  'item_id': 1,
  'time': '2019-05-28T18:01:31.154Z'}

127.0.0.1 - - [28/May/2019 23:31:31] "POST /transactions/new HTTP/1.1" 201 -

Found Proof of work: 1844

Creating New Block
{
  'index': 2,
  'previous_hash': 'bbe4b89ce4dd12ec66c4a6791ec0a9fd6ed3131fd123c1e65bd5c8c8',
  'proof': 1844,
  'timestamp': 1559066491.5715458,
  'transactions': [
    {
      'city': 'New Delhi',
      'country_name': 'India',
      'dealt_via': 'Lexi Emard',
      'item_id': 1,
      'time': '2019-05-28T18:00:35.420Z'},
    {
      'city': 'New Delhi',
      'country_name': 'India',
      'dealt_via': 'Murray Reichel',
      'item_id': 1,
      'time': '2019-05-28T18:00:39.408Z'},
    {
      'city': 'New Delhi',
      'country_name': 'India',
      'dealt_via': 'Mrs. Easter Schroeder',
      'item_id': 1,
      'time': '2019-05-28T18:01:05.313Z'},
    {
      'city': 'New Delhi',
      'country_name': 'India',
      'dealt_via': 'Lawson Christiansen',
      'item_id': 1,
      'time': '2019-05-28T18:01:31.154Z'}]]
```

## V. CONCLUSION

With this system, the products journey from manufacturing to customer can be recorded, and the customer is assured that the scans weren't faked. Manufacture is able to prove their product is authentic and is also able to track their product's pathway. The setup is easy to implement and requires less operation cost. Manufacturer can also adopt RFID or NFC tokens instead of QR codes to further strengthen their system.

## VI. REFERENCE

- [1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
- [2] Hyperledger, "Hyperledger Blockchain Performance Metrics", V1.01, October 2018
- [3] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
- [4] Armin Ronacher, "Flask Docs", <http://flask.pocoo.org/docs/>
- [5] G. Wood, "Ethereum: A secure decentralised generalized transaction ledger," Tech. Rep., 2014.
- [6] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, <https://doi.org/10.1787/9789264251847-en>.
- [7] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.
- [8] Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, "Making byzantine fault tolerant systems tolerate byzantine faults," in Proc. 6th USENIX Symp. Netw. Syst. Design Implement., 2009, pp. 153–168.
- [9] Cachin, "Architecture of the hyperledger blockchain fabric," Tech. Rep., Jul. 2016..
- [10] S. Underwood, "Blockchain Beyond Bitcoin", in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016.
- [11] Deloitte, Israel: A Hotspot for Blockchain Innovation, 2016. [Online]. Available: [https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel\\_a\\_hotspot\\_for\\_blockchain\\_innovation\\_feb2016\\_1.1.pdf](https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financial-services/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf). [Accessed: 2.11.2016].
- [12] G. Greenspan and M. Zehavi, Will Provenance Be the Blockchain's Break Out Use Case in 2016?, 7.1.2016. [Online]. Available: <http://www.coindesk.com/provenance-blockchain-tech-app/>. [Accessed: 12.12.2016].
- [13] Counterfeit medicines. QA counterfeit. World Health Organization (WHO) 2009. Available from: <http://www.who.int/medicines/services/counterfeit/faqs/QACounterfeit-october2009.pdf> [last cited on 2010 Jun 12].
- [14] An ICC initiative Business Action to Stop Counterfeiting and Piracy (BASCAP). Brand protection directory. The World Business Organization. Available from: <http://www.iccwbo.org/bascap> [last cited on 2010 Jun 10].
- [15] L. Li, "Technology designed to combat fakes in the global supply chain", in Business Horizons, vol. 56, no. 2, p. 167-177, 2013.
- [16] White paper. Dhar R. Anti counterfeit packaging technologies. A strategic need for the Indian industry. Confederation of Indian Industry 2009:1-47. Available from: [http://www.bilcare.com/pdf/CI\\_anti\\_counterfeit\\_pkg\\_technologies\\_report.pdf](http://www.bilcare.com/pdf/CI_anti_counterfeit_pkg_technologies_report.pdf) [last cited on 2010 Oct 29].
- [17] Berman, "Strategies to detect and reduce counterfeiting activity", in Business Horizons, vol. 51, no. 3, p. 191-199, 2008.
- [18] K. D'egardin, Y. Roggo and P. Margot. "Understanding and fighting the medicine counterfeit market", in Journal of Pharmaceutical and Biomedical Analysis, vol. 87, p. 167-175, 2013
- [19] R. C. Merkle, "A digital signature based on a conventional encryption function," in Proc. Conf. Theory Appl. Cryptogr. Techn., 1987, pp. 369–378