International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

Elimination of Counterfeit Products using Blockchain

Dr. J. Satheesh Kumar[1], G.Praveen[2], M. Kesavan[3], D. Naveen Raj[4]

[1]Professor, Student, Department of Electronics and Communication Engineering, Hindusthan College of Engineering and Technology, Tamil Nadu, India
[2-5]Student, Department of Electronics and Communication Engineering, Hindusthan College of Engineering and Technology, Tamil Nadu, India

---

Abstract – In the recent years blockchain have gained interest over wide range of field and solving their problem. Since its been a decade since the introduction of blockchain, but till now its most explored use cases have been found in financial sector. This paper gives an overview idea of using decentralized blockchain and digital signature to stop the counterfeit products and to track the supply chain and ownership of the product.

***Key Words*: Ethereum Blockchain, Digital signature, Smart Contracts, Counterfeit etc.,**

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. The **Authentication Solution Providers' Association** (ASPA), a self-regulated industry body of anti-counterfeiting and traceability solutions providers unveil the first edition of its report "The State of Counterfeiting In India - 2020", that highlights the trends of counterfeiting incidents reported in India for the period 2019 and 2020.

As per ASPA India suffers a loss of over one lakh crore rupees per annum owing to the sale/purchase of counterfeit goods by consumers across all sectors. This, naturally, is a great concern for genuine brand-owners, looking to protect the reputation of their brands and their sources of revenue. Globally, counterfeiting now stands at 3.3 percent of global trade and is impacting the social and economic development of countries and 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.

To Stop the Counterfeit products, we must understand the challenges in it.

Challenges in Counterfeit Elimination

II. LITERATURE SURVEY

[1] JINHUA MA , SHIH-YA LIN , XIN CHEN , HUNG-MIN SUN , YEH-CHENG CHEN AND HUAXIONG WANG proposed the paper **"A Blockchain-Based Application System for Product Anti-Counterfeiting",2020** describe a decentralized Blockchain system with products anti-counterfeiting, in that way manufacturers can use this system to provide genuine products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance and can assure that the consumers getting genuine products without the involvement of trusted intermediaries.

[2]HOAI LUAN PHAM, THI HONG TRAN and YASUHIKO NAKASIMA proposed the paper "**Practical Anti-Counterfeit Mesicine management System Based on Technology",2019** which describes a novel Blockchain based product ownership management method for product ownership management method for anti-countefeit medicine system to resist the cloning of drug and improve the practical applicability. Analysys and evaluation results of our proposed system outperform the related proposals based on criteria about a practical application, anti-clone, low cost oriented, and scalability. Furthermore, experimental implementation on a small scale shows that our proposed system works appropriately in a real environment.

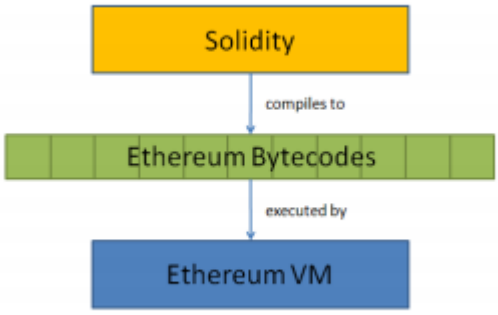
[3]TRIPTI RATHEE, MANOJ MALIK proposed the paper "Authentication of Products & Counterfeit Elimination using Blockchain" which provides an overview of different solutions in the anti-counterfeit area, different blockchain technologies and what characteristics make blockchain especially interesting for the use case. We have developed three different concepts 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.

III. OVERVIEW

Blockchain : Blockchain was first invented and designed by Satoshi Nakamoto in 2008. The Blockchain is a distributed digital ledger. Owing to its advantages, such as transparency, security, immutability, and availability, Blockchain attracts much attention from the tech community.

Ethereum account: Our proposed system on Ethereum Blockchain. There are two types of Ethereum account as Externally Owned Account (EOA) and contract account. Throughout this paper, we refer to EOA. Principally, EOA is considered as an Ethereum public key and controlled by Ethereum private key (EPK). To manage EOA and EPK, we utilize wallet applications.

Smart contract (SC) is a computer program written by a Turing-complete programming language. SC is compiled to a bytecode and stored on the Ethereum Blockchain network associated with a unique address. It is written in Solidity language and run by Ethereum virtual Machine(EVM).



Function is a part content in SC. The function can interact with other SCs, make decisions, store data, and send Ethercoin to others. In this paper, we use functions for data storage. In addition, we specifically apply a modifier function to bind the condition that only the specified EOA can execute the designated function.

Gas used is an internal cost to execute the function in SC. In this Ethereum Blockchain we use Ether for executing the function.

Remix-IDE : Remix is a browser-based compiler and IDE that allows researcher to build and debug the Ethereum SC using Solidity language.

Ganache is an Ethereum-based client using Node.js and uses to develop original projects before implementing on the real Ethereum network. Ganache is a local Ethereum network and responding like a real node.

Node Js is a server side programming that allows users to build network applications.

Web3 Js is a collection of libraries that allow you to interact with a local or ethereum node using HTTP, IPC(Interprocess Communication) or web sockets

Metamask is a browser plugin that serves as an cryptocurrency wallet which acts as gateway to blockchain.

Ethcrypto is a javascript library which is used for encrypting and hashing using public-private key pairs in javascript.

IV.PROPOSED SYSTEM

We propose a decentralized blockchain with digital signature for our system. In our system there will be four stakeholders including Manufacturer, Distributor, Retailer, Consumer. To participate in the system, every stakeholder needs to generate a key pair of EOA(Externally owned Account) and EPK(Ethereum private key). The key pair of EOA and EPK is responsible for deploying or executing the function of ths smart contracts.

The top stakeholder who is Manufacturer when manufacturing or producing a product will register the product unique id, distributor EOA, retailer EOA inn to the blockchain. The Manufacturer uses the asymmetric cryptography.

Backend & Frontend

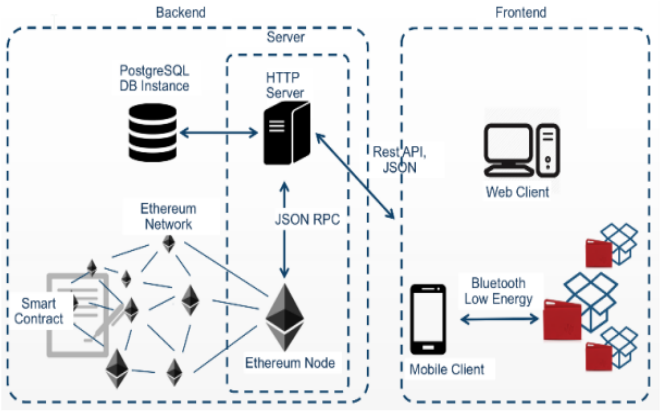
Application which runs decentralized is called Dapps. The backend runs on javascript.

Step 1: The smart contract is written in Remix IDE.It is compiled and run by EVM which converts solidity in to bytecode.

Step2: The smart contract is to be migrated on the blockchain network and then deployed with the help of trufflesuite.

Step3: The localhost is made to be run and the dapp is linked to the localhost.

The frontend is supported by HTML and CSS which makes it easier to understand.



Backend and Frontend

Asymmetric Cryptography :

Asymmetric cryptography is scalable for use in very large and ever expanding environments where data are frequently exchanged between different communication partners. With asymmetric cryptography:

• Each user has two keys: a *public* key and a *private* key.

• Both keys are related mathematically(both keys together are called the *key pair*).

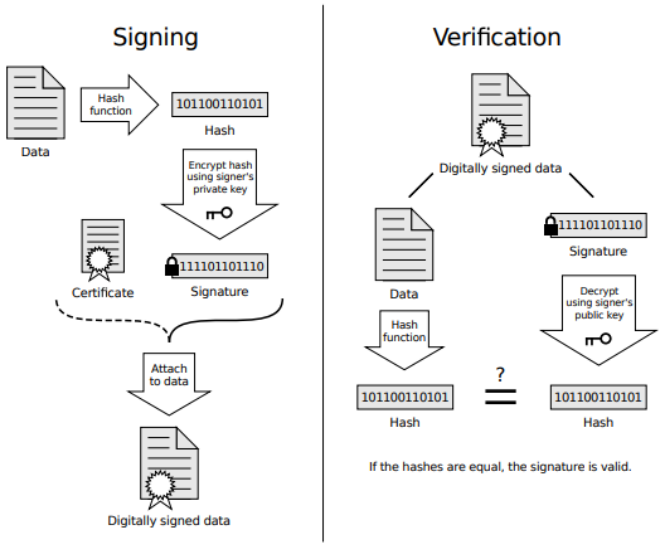
•The public key is made available to anyone. The private key is kept secret.

•Both keys are required to perform an operation. For example, data encrypted with the private key is unencrypted with the *public* key. Data encrypted with the public key is unencrypted with the *private* key.

• Encrypting data with the private key creates a digital *signature.* This ensures the message has come from the stated sender (because only the sender had access to the private key to be able to create the signature).

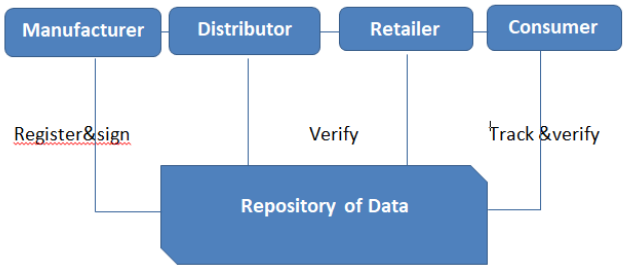
•A digital envelope is signing a message with a recipient's public key. A digital *envelope*, which serves as a means of access control by ensuring that only the intended recipient can open the message (because only the receiver will have the private key necessary to unlock the envelope; this is also known as *receiver authentication*).

• If the private key is stolen for forgotten, a new key pair must be generated.



Signing And Verification

Asymmetric cryptography is often used to exchange the secret key to prepare for using symmetric cryptography to encrypt data. In the case of a key exchange, one party creates the secret key and encrypts it with the public key of the recipient. The recipient would then decrypt it with their private key. The remaining communication would be done with the secret key being the encryption key. Asymmetric encryption is used in key exchange, email security, Web security, and other encryption systems that require key exchange over the public network.



Registering and Signing :

Each and every product will have a pair of global Id and unique Id in the manufacturing unit to identify the product in the Manufacturing Unit. We store data in two ways in this system. Since executing the function costs a small amount of ether, we store the product data, distributor data and retailer data in database and tracking data will be stored in Blockchain. The Manufacturer will sign a message on the blockchain with his own private key and encrypting it with distributor's public key. The message for each stakeholder will be separate. So the manufacturer will create a message for each stakeholder separately. When the Receiver will receive the product, he will decrypt it with his private key

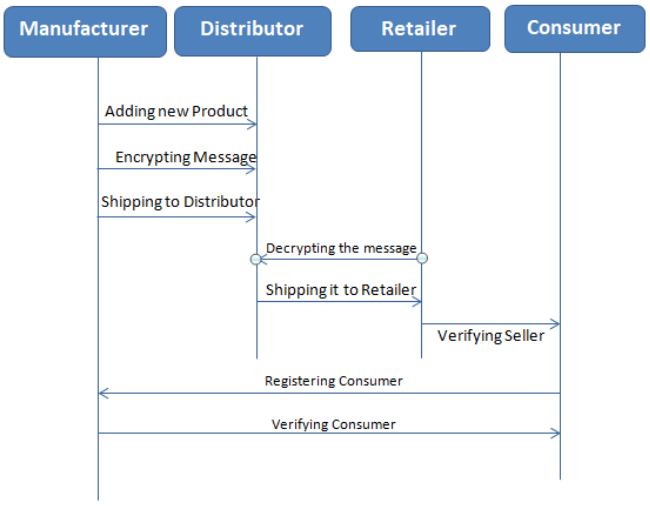
and public key of the Manufacturer. The messages will be encrypted with SHA 256 and Keccak256 algorithm with the help of eth-crypto library in javascript.

Verifying :

Once the message is signed, the receiver side should verify the sign whether it is created by the Manufacturer or not. The Manufacturer would have registered the distributor or retailer EOA in the blockchain. If the address matches they would have to verify the message sign by first decrypting it with receiver's private key and second decrypting it with sender's public key. By this way the Confidentiality, Authenticity and Integrity of the product is achieved. Once the receiver decrypt the message the opwnership of the product will be transferred from the sender to receiver. This is limited to distributor and retailer and not for consumer.

Tracking :

After the ownership is transferred to the retailer, he will update the signed message with his address. Consumer on buying the product the retailer will register his details in to the blockchain which will be available to the manufacturer. Through the blockchain the product can be tracked from the source to destination



V. CONCLUSION

The question if blockchain can reduce counterfeited products is a complex one. Blockchains cannot be considered as the solution to counterfeits, but they can be part of a technological stack to fight counterfeits. It is important to note that reducing counterfeits cannot be achieved by only using technological means. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging must all also taken into account. A holistic approach is required to reduce and prevent counterfeiting. However, blockchains can be an important layer in the technology stack to fight counterfeits. Using IoT or unique identifiers, physical goods can be linked to a blockchain, where every transaction of the item can be stored. This allows for perfect traceability, combined with the fact that the data cannot be tampered with. Using public blockchains, trust in the system can be increased, which adds an extra benefit, especially if there is no trust into central authorities.

VI. FUTURE SCOPE

Within this thesis, multiple approaches to reduce counterfeits were focused on. To be less dependent on external factors, these changes were considered and their impact on reducing counterfeits evaluated. It was not possible to implement all the proposed changes, due to time constraints and the fact that multiple other changes to the system were also necessary. Further work includes the finalizing of these implementations for the proposed system, and considering the possibility to run pilots. The concept and implementation to reduce counterfeits in the humanitarian supply chain is still under development. Further work does not only include finalizing the implementation, but finding partners to run a pilot and evaluate the results. Finally, the combination of blockchain and Digital signature technologies was looked at in this thesis, but not covered in depth. The combination of these two technologies might enable many more interesting use cases.

VII. REFERENCES

[1] J. Leng, P. Jiang, K. Xu, Q. Liu, J. L. Zhao, Y. Bian, and R. Shi, "Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing," J. Cleaner Prod., vol. 234, pp. 767–778, Oct. 2019.

[2] N. Alzahrani and N. Bulusu, "Block-supply chain: A new anticounterfeiting supply chain using NFC and blockchain," in Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock), 2018, pp. 30–35.

[3] (2018). Litecoin. [Online]. Available: https://litecoin.info/index.php/Main Page

[4] (2019). Github. [Online]. Available: https://github.com/ethereum/wiki/ wiki/White-Paper

[5] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, p. 1–32, Apr. 2014.

[6] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, "ADEPT: An IoT practitioner perspective," IBM Inst. Bus. Value, New York, NY, USA, White Paper, 2015, pp. 1–18.

[7] (2018). Cryptokitties. [Online]. Available: https://www.cryptokitties.co/

[8] S. Matthew English and E. Nezhadian, "Application of bitcoin datastructures & design principles to supply chain

management,'' 2017, arXiv:1703.04206. [Online]. Available: http://arxiv.org/abs/1703. 04206

[9] F. Tian, ''An agri-food supply chain traceability system for China based on RFID & blockchain technology,'' in Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM), Jun. 2016, pp. 1–6.

[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. VOLUME 8, 2020 77651 J. Ma et al.: Blockchain-Based Application System for Product Anti-Counterfeiting

[11] 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.

[12] (2018). Solidity. [Online]. Available: http://solidity.readthedocs.io/ en/v0.4.24/

[13] (2018). Node.js. [Online]. Available: https://www.myetherwallet.com/

[14] (2018). Web3.js. [Online]. Available: https://github.com/ethereum/web3.js/

[15] (2018). ETH Gas Station. [Online]. Available: https://nodejs.org/en/

[16] (2018). Remix. [Online]. Available: https://remix.ethereum.org/

[17] Dapp University[Online].Available:

https://www.dappuniversity.com/