Anti-Counterfeit Method for Computer Hardware using Blockchain

C.D. Britto
Department of Computing and Information Systems, Faculty of Applied Sciences, Wayamba University of Sri Lanka, Sri Lanka

N.G.J. Dias
Faculty of Computing and Technology, University of Kelaniya, Sri Lanka

ABSTRACT
Counterfeited computer hardware are products designed looks exactly the same as their genuine products. Most of the people are tricked by the counterfeiters using online markets. This influences the need for a secure and efficient mechanism to identify fake/counterfeited products. The proposed method is implemented using the Blockchain technology. Each Block represents a product and the hash key of that product, calculated using the specified Block attributes. The buyer details were updated by a verified retailer. Thereafter any user can check the validity of the product using the hash key and retailer name. Tampered Block is notified to the customer and then the product is invalid. This system can be upgraded by hosting the application on a web server for distribution and separating the application functions according to the user levels (Manufacturer, retailer, and buyer). Therefore, the proposed method provides a more secure and reliable way to handle computer hardware counterfeits.

Keywords
Blockchain, Smart Contract, API, Anti-Counterfeit, Computer Hardware Devices

1. INTRODUCTION
At present, most of the people own a personal computer, a laptop or a mobile phone. With the growth in the technology field, computer hardware manufacturers extend their manufacturing by shifting production operations into various countries. So, the leakage of secrets of the manufacturing process also becomes higher. Most of the people in the world spend huge amounts of money to upgrade their computers. Unfortunately, most of them are unable to get the genuine products because there are many fake products in the market. Everything from desktop and/or laptop computers to modems and circuit boards are counterfeited well by counterfeiters.

A blockchain is decentralized, distributed, at often public, digital ledger consisting of records called blocks that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. Smart contracts are merely programs held on a blockchain that runs once the planned conditions are met [4]. They generally would not automatize the execution of an agreement, so all participants are right away bound to the outcome, with none intermediary's involvement or time loss. They would additionally automate a workflow, triggering subsequent action when conditions are met.

The common mechanism available for the customers to verify the product is to use the product serial number, but it is not relatively successful because contacting the manufacturer is a difficult and time-consuming process. Also, there are many counterfeit detection methods like Physical inspection (Exterior, interior and material check), electrical inspection, etc. But all the customers do not have the ability to perform such methods. However, the majority of current counterfeit identification methods are based on centralized infrastructure and those methods have availability issues with security threats.

There are many counterfeit attacks that could occur in the process of customer receiving the computer hardware from the manufacturer. Modification, cloning and tag reapplication are three kinds of product counterfeiting attacks according to Lehtonen et al [7].

This study proposes a method to create a system that ensures fake product identification on their own in less time with high reliability. The system is able to view the first owner of a product when it comes to the consumer in the consumer market. The security of this system should be maximum to ensure that the customers are safe. Thus, the proposed method for anti-counterfeit is more effective and efficient since it uses a decentralized mechanism.

2. LITERATURE REVIEW
Qi Xia et.al [6], have proposed a method of Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments, where that blockchain-based information sharing system adequately addresses the access control difficulties related with delicate information put away in the cloud utilizing changelessness and underlying self-sufficiency properties of the blockchain. They have proven that using the blockchain method can lead to handling data with higher security and efficiency.

J. Kishigami et.al [2], have proposed a method, where it helps to distribute digital content over a Digital Content Distribution System. Their system users are of two kinds: owners and receivers. Owners have full control over the content they share and 10 minutes of time is used to mine a block. They have sufficient feedbacks from users where they have implemented the system and let the users provide details on the system.

Ijazul Haq and Olivier Muselemu Esuka [8] have proposed a method to prevent the counterfeit of drugs using blockchain. They have presented a way to use Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs. The method follows the whole supply chain of drugs from the manufacturer to the Doctor who prescribes them. This system pre-requisites a trusted and secure network where only trusted

parties have access. The manufacturer creates a unique hash and assigns it to the product. The ownership of the drug can be transferred using the mobile app which will be recorded in the blockchain. The doctor can confirm the Genuity by the journey of drug from manufacturer to doctor.

Naif Alzahrani and Nirupama Bulusu [9] have proposed a new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol. It does not require Proof of Work and randomly employs a different set of different sized validators each time a new block is proposed. The proposed Block-Supply chain is in a decentralized supply chain where each node maintains a blockchain for each product. However, they did not implement the solution.

In some studies, the proposed systems can check the path/transfer history of the product only by the specific authorized users. Therefore, the genuineness of the product cannot be determined by the public. This leads the blockchain to be a closed permissioned blockchain, where both read and write is restricted for the public. Some of the solutions made each node of the chain to manage one product. Therefore, the number of trusted nodes in the chain is increased and higher computation power is needed for validators to validate a newly proposed block. The public acquires the ability to check the genuineness of the product using the proposed solution in this study and the first buyer who buys the product from the retailer is also recorded in the blockchain. Each Block in the proposed solution blockchain was an authorized, partially updatable block of the product. Therefore, the customer/buyer details can be added and the genuineness can be easily predictable to the consumer-consumer market.

3. METHODOLOGY

3.1 Blockchain

3.1.1 Block

The Block developed in this study represents a transaction of an item which is stored in the chain. Basically, a Block has a certain storage capacity to store many transactions. But here one Block is a descriptive tuple of a specific item, where a Block containsa hash key, serial No, product Name, product Description, retailer, previous Hash, current timestamp, buyer ID, buyer Name and buyer Contact No., nonce and status. Nonce is a special attribute which count the number of iterations to generate the hash with defined difficulty and used at computing hash key.

When creating a Block, only Serial No, product Name, product Description, retailer, previous Hash and current timestamp areprovided. Therefore, each Block has a separate method to add user details to the Block. Status attribute of the Block indicate whether an item is sold or not. The status attribute gets updated when the buyer details are added to the Block. Hash key of the Block will be generated using theserial no, product name, product description, previous hash, current timestamp and nonce.

Mining a Block into the chain is an iterative process where the process gets successful when the predefined nonce is reached. Hash will again be calculated and compared with the current hash stored in the Block when checking the validity of the Block.

3.1.2 Blockchain

This study presents a Blockchain that has a difficulty level 4 in calculating the hash. At first, the Blockchain has Genesis product is restricted because it will affect the consumer-consumer market. This application includes additional basic Block that will be the first Block of the chain. Also, there are validators to validate the Chain and user-requested Block hash. The Blockchain is shared within the manufacturing company, distributers, wholesalers and Retailers.

3.1.3 Blockchain API

The Blockchain API consists of requests which are,

I. Get Chain request: Returnsa list of Blocks.

II. Minerequest: Serial No, product Name, product Description and retailer name should be passed as parameters that is used in mining the Block. Finally, the API send the response with generated hash key.

III. Buyer update request: Block hash key, buyer ID, buyer name and buyer contact Number should be passed as parameters that is used for updating the buyer details only if the chain and the hash key is valid.

IV. CheckValidity request: Block hash key and Retailer name should be passed as parameters that is used in validation check of requested Block. The Retailer name was an extra security added to the process of validation. Even though the provided hash was available on the Blockchain, the hash was recalculated and compared with the hash stored in the Block.

Validaterequest: Check if the Blockchain is valid and response the validity.

3.2 Decentralized Application

The developed system is a Proof of Concept Application and it contains 3 parts, namely, add product, Update Buyer Details and Validate the Product.

3.2.1 Add Product

Product details such as serial number, name and description of the product along with retailer name have to be submitted in order to get the hash key of the product.

3.2.2 Update Buyer Details

Buyer details along with the generated hash key in previous step have to be provided by the verified Retailer.

3.2.3 Validate the Product

The user can validate the product using the hash and retailer's name.

4. RESULTS AND DISCUSSION

Serial number, product name, product description and retailer name should be submitted to add a product to the Blockchain. All fields are mandatory and after adding a product to the chain, hash key of the product is displayed. A successful mining of a block to the Blockchain after entering necessary details returned the generated hash key of the block. The user needs to copy that value for later usage. The developed system is a Proof of Concept Application. Therefore, the most common user scenario is used. The use of hash key in validation can be enhanced by a QR code or any other similar mechanism. After submitting the product details, the user/retailer has to update the buyer details of the product by submitting hash key of the product along with buyer id, name and contact number.Realteration of the buyer details for a

functionalities such as notifying the user if the product is not found in the chain or disables the user details update facility.

In order to check the validity of a product, the user must provide the hash key and the retailer name. The Retailer name provide an extra reliance since counterfeited products were not sold by the verified Retailers. If the hash is available on the blockchain and the block is not tampered, then the system identifies that the product is not fake/counterfeited. If the product details are tampered (counterfeited) or an invalid hash was entered, then the system gives an error. The Ijazul Haq and Olivier Muselemu [8] proposed system can check the path/transfer history of the medicine only by the doctor whoprescribe it. Then the blockchain should be a closed permissioned blockchain, where both read and write is restricted for the public. Therefore, the patient who buys the medicine cannot check the validity. But the proposed solution makes the public aware of the genuineness of the product. The Naif Alzahrani and Nirupama Bulusu [9] proposed solution enables each node of the chain to manage one product which increases the number of trusted nodes in the chain. Also, it does not handle the first buyer who buys the product from the retailer. But the proposed solution was developed with an authorized partially updatable block for each product. Therefore, the customer/Buyer details can be added and the genuineness can be easily predictable to the consumer-consumer market.

5. CONCLUSION

The proposed blockchain based anti-counterfeit method for Computer hardware uses a standard Blockchain as the ledger of transactions. But it differs from traditional blockchains because of its structure. The structure makes a clear distinction where each Block in the blockchain represents a single product. The products could be a computer graphic card, RAM card, or any other computer hardware peripheral which was identified using the serial number. The product details were added to the blockchain by the manufacturer and the retailer can update the buyer details on it since the buyer details do not affect the hash key calculation. Once the buyer details were updated, the re-update was restricted. Therefore, only the first buyer details were stored in the block. When it comes to the 2nd hand market the buyer can verify this by checking the buyer details and product details. So, this method gives an assurance to the buyer that the buyer can contact the first buyer in case of any problem. Since the blockchain can be made publicly available, because of the distributed architecture, a buyer of the computer hardware can validate the product by hash code and retailer name.

In order to implement the method, a decentralized application was developed. The decentralized application accesses the blockchain API which has level 4 difficulty. The difficulty is a measure of how difficult it is to mine a block in a blockchain and a higher difficulty level means it takes additional computing power to verify transactions entered on a blockchain. Because of the lack of high-end computer resources, a level 4 difficulty measure was used to implement the methodology. The Blockchain in the proposed solution should be an Open permissioned Blockchain wherein open permissioned blockchains anyone can read its data but only authorized nodes can write the data. This concludes that the proposed method can be used publicly with more security. The study can be extended more significantly by adding public-private key encryption to the Block hash and adding two-factor authentication to the user login process. Also, hosting the application on a web server and distributing the blockchain around the network will increase the measure of security.

6. ACKNOWLEDGMENTS

I express my deepest gratitude to the people who encouraged me to complete the project. In addition, I offer my special thanks to all the staff members of the Department of Computing and information systems, Faculty of Applied Sciences, Wayamba University of Sri Lanka for their vital aspiration and instructions.

7. REFERENCES

[1] Maher Alharby, Amjad Aldweesh, and Aad van Moorsel. Blockchain-based smart con- tracts: A systematic mapping study of academic research (2018). In 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), pages 1–6. IEEE, 2018.

[2] Junichi Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira, and Akihiko Akutsu. The blockchain-based digital content distribution system. In 2015 IEEE fifth international conference on big data and cloud computing, pages 187–190. IEEE, 2015.

[3] Damiano Di Francesco Maesa, Paolo Mori, and Laura Ricci. Blockchain based access control. In IFIP International Conference on Distributed Applications and Interoperable Systems, pages 206–220. Springer, 2017.

[4] Szabo N. The idea of smart contracts. 1997.

[5] SEO Noble. About Blockchain. 2020. https://seocompanylosangeles.us/rules/. Accessed Aug 2021.

[6] Xia, Qi & Sifah, Emmanuel & Smahi, Abla & Amofa, Sandro & Zhang, Xiaosong. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information. 8. 44. 10.3390/info8020044.

[7] Lehtonen M, Staake T, Michahelles F. From identification to authentication–a review of RFID product authentication techniques. In: Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting. Berlin, Germany: Springer-Verlag Berlin Heidelberg; 2008:169-187.

[8] Haq, Ijazul & Muselemu, Olivier. (2018). Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs. International Journal of Computer Applications. 180. 8-12. 10.5120/ijca2018916579.

[9] Alzahrani, N, Bulusu, N. A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol. Concurrency Computat Pract Exper. 2020; 32:e5232. https://doi.org/10.1002/cpe.5232.

[10] Gamage, H.T.M., Weerasinghe, H.D. & Dias, N.G.J. A Survey on Blockchain Technology Concepts, Applications, and Issues. SN COMPUT. SCI. 1, 114 (2020). https://doi.org/10.1007/s42979-020-00123-0.