A Supply Chain Management System to Prevent Counterfeiting and Trace Different Transactions Instead of using PUF Device

Yusuke Abe[1], Kosei Arisaka[1], Kitahiro Kaneda[2] and Keiichi Iwamura[1]
[1]*Tokyo University of Science, 6-3-1 Nijuku, Katsushika-ku, Tokyo 125-8585, Japan*
[2]*NAGASE & CO., LTD., 5-1 Nihonbashi-Kobunacho, Chuo-ku, Tokyo 103-8355, Japan*

Keywords: Blockchain, Supply Chain, Raw Material, Physical Unclonable Function (PUF), Counterfeiting.

Abstract: The distribution of counterfeit products in supply chains has been increasing in recent years. Physical unclonable function (PUF), which takes advantage of the difficulty of duplication inherent in devices, is attracting attention as a way to overcome this problem. However, PUF can only be applied to a few objects, notably semiconductor chips, and is, therefore, unable to cover the wide variety of products in a supply chain. Moreover, it is necessary to use noise reduction technology, such as a fuzzy extractor, to remove noise from the output through PUF. There is a concern that costs may increase to implement such technology. Therefore, this paper proposes a system that can perform the same function as PUF on objects for which PUF has not yet been established, without using noise reduction technology. An arbitrary feature of an object is measured, and if the feature satisfies a certain criterion, the object can be safely delivered. In addition, the proposed method is able to distinguish between individual transactions between one company and another. This prevents unauthorized resale and diversion by controlling even the location of the products once they are dispatched from the supplier.

1 INTRODUCTION

Logistics has evolved over the years with the dramatic advances in information technology (IT), and has become an inseparable part of modern life. Here, the distribution process from the procurement of raw material to the delivery of products to consumers is called the supply chain. The supply chain consists of suppliers, logistics providers, wholesalers, retailers, and end users. To improve the added value of products and services for customers, a management system that optimizes the integrated management of objects, money, and information has been attracting attention in recent years. This is known as supply chain management (SCM).

Companies involved in the supply chain are aware of SCM and focus on how to provide products efficiently. Therefore, damage caused by counterfeits around the world still cannot be stopped. A report (OECD and EUIPO, 2016, 2019) by the Organisation for Economic Cooperation and Development (OECD) and the European Union's (EU) Intellectual Property Office explains that the global trade value of counterfeit and pirated goods reached $461 billion in 2013 and $509 billion in 2016. For example, have you ever wondered whether the product you purchased through e-commerce is authentic and has been delivered to you through the right channels? To eliminate such concerns, products are currently managed through the physical attachment of radio-frequency identification (RFID) tags or barcodes (QR codes). For those with malicious intent, however, it is easy to physically remove such tags or codes from the products. This makes it possible to attach the original RFID or barcode to a fake product and sell the counterfeit. When such an attack occurs, it is usually very difficult for end users to determine the authenticity of the product, necessitating counter-measures. In addition, each company manages its own transaction history. Even if the end user reads the information from the tag, the user will only be able to view the information that has been made accessible to the public at the discretion of the individual company.

Given this background, technologies such as blockchain and PUF are expected to be used. As for the information the user browses, it is expected that blockchain, which is a distributed ledger that is difficult to tamper with, will be introduced into SCM. This technology can be used to track products with reliability. For intentional tag replacement, an individual identification system that uses a technology called physical unclonable function

Abe, Y., Arisaka, K., Kaneda, K. and Iwamura, K.
A Supply Chain Management System to Prevent Counterfeiting and Trace Different Transactions Instead of using PUF Device.
DOI: 10.5220/0010571301010108
In *Proceedings of the 18th International Conference on e-Business (ICE-B 2021)*, pages 101-108
ISBN: 978-989-758-527-2

(PUF) has been proposed, instead of information that is externally attached to products, such as RFID or barcodes. PUF is a function that outputs different eigenvalues for each object, utilizing unique physical properties of the product that are difficult to replicate. For example, when a semiconductor chip with the same circuit receives the same input, the output is the same for all chips, but the response time is slightly different. This technology identifies individual chips with the same circuit using the difference in response time as a unique property of the device, which makes it difficult to duplicate. A buyer of the device can determine the authenticity by utilizing this feature.

However, PUF has a drawback in that it cannot be applied to all products. Due to PUF's features, it is limited to a very small number of products, such as semiconductor chips. The technology is not versatile and cannot cover a wide variety of commerce. In this paper, we propose a system that can perform the same functions as PUF for a range of materials (powders, liquids, individuals, precious metals, etc.) as examples of a commodity supply chain for which PUF cannot be used. Mere substances are often identified by their composition and size, and few individual identification technologies, like PUF, have been studied that clearly confirm the match. It is, however, possible to judge if a product is legitimate based on whether it meets a criterion. This judgment is called normal judgment. In normal judgment, by measuring the physical properties of a product, a substance that has the specified components and size is judged to be genuine, and a substance that does not meet the specified components and size is judged to be fake. Accordingly, when an end user purchases and receives a substance, it is preferable to have a technology that not only determines whether the product is legitimate by satisfying the specified features, but also utilizes unpredictable values like PUF. Hence, the main goal is to realize an SCM system that can be used for various products, with or without the application of PUF.

The remainder of this paper is organized as follows. Chapter 2 explains the related work against counterfeits, Chapter 3 describes the proposed methods, Chapter 4 is devoted to the evaluation, and Chapter 5 provides a summary.

2 RELATED WORK

2.1 Blockchain in Supply Chain

Current supply chains have difficulty in tracking product history (traceability). Even if consumers view the product history, they cannot determine if the data such as "who", "when", "where", "what", and "how" are correct. Therefore, a platform for sharing accurate information is needed, and there is a lot of research being done on the use of blockchain, a secure and highly available distributed ledger. Dietrich et al. (2021) and Pournader et al. (2020) survey and review many blockchain projects in the supply chain. Hackius et al. (2017) sought input from logistics experts and found that most experts are positive. Tijan et al. (2019) argue that blockchain can minimize major issues in logistics such as order delays, errors, and multiple data entry.

2.2 Detection of Counterfeiting

This section lists the issues regarding RFID-based external tag technology, PUF-based technology, and identification by substance features. The study of the issues is a stepping stone in proposing effective methods.

Sun et al. (2019) claim that RFID and the information associated with it cannot be tampered with, and that different users are provided with different query permissions to maintain their authenticity. Toyoda et al. (2017) argue that end users can reject counterfeits by having each entity transfer products and their ownership while determining the authenticity of the RFID tags. No matter how much the authenticity of the tag is guaranteed, as shown by Sun et al. (2019) and Toyoda et al. (2017), an end user has no way of checking the authenticity of the content. The physical space where products exist and the cyberspace where authenticity is guaranteed are not well connected. The use of RFID tag anti-counterfeiting technology with PUF, as described by Devadas et al. (2008), is therefore not a sufficient solution.

Previous studies (Hori et al., 2015; Aniello et al., 2019; Negka et al., 2019) focus mainly on individual identification systems that utilize PUF.

Three points are worth noting. First, as mentioned previously, PUF can only be applied to specific products. Target products need to be expanded to meet a wide range of modern needs. Second, noise reduction technology, called a fuzzy extractor (Dodis et al., 2004), is required. When using PUF, ideally, a certain semiconductor chip should always produce a same output, but in reality, it is difficult because of its vulnerability to noise. In addition, PUF uses a minute variation in each semiconductor chip. There are therefore problems such as not being able to get an appropriate output or getting a similar output from different devices. Fuzzy extractor is a means to solve this problem. However, installing a fuzzy extractor makes the process more complicated and increases the processing time and circuit size. This is also a factor that increases implementation costs. Third, systems that use PUF only determine whether the device shipped and the device delivered to the end user is an exact match. Strictly speaking, this is not an authenticity judgment. This just verifies that the end user has received the product declared by the supplier. However, it is generally not important for the end user that the shipment and purchased product are identical. In many cases, it is important that the product meets a required criterion and is legitimate. Consider, for example, the situation in which a diamond is purchased from a catalog. The purchaser does not necessarily want a diamond that is exactly the same as the picture in the catalog. It is important that the diamond's carats, hardness, and size meet the criteria.

The system proposed by Koike (2010) verifies legitimacy based on the features extracted from the target object. The normal judgment is more predictable than PUF because the judgment value of a legitimate device is fixed. We take the example of a diamond once again. An attacker realizes that if a product has a specified range of carat, hardness, and size, it is considered real. In this case, even if the identification target is out of range, the attacker can pass off a counterfeit as genuine by creating a device that outputs a judgment value satisfying the criteria. By the way, it is difficult to predict an output of PUF, even if the value of one device is stored, it cannot be diverted to other devices. The normal judgment does not have this feature of PUF. Therefore, there are few proposals for judgment systems based on features of objects.

In summary, technology is required to output different values for each individual (or each transaction between companies), similar to PUF, without fixing the output value of the normal judgment. This prevents fraud by logistics providers.

3 PROPOSED METHOD

3.1 Overview

In this study, we propose a technology to determine authenticity by normal judgment. The goal of the proposed system is to achieve the same functionality as PUF for the SCM of substances that have been difficult to identify in the past. The system consists of a registration device, verification device, and identification device, as shown in Figure 1. The registration device in SCM is assumed to be used by suppliers who generate and ship products. A verification device is used by logistics providers who transport products. The identification device is used by end users who receive the products. The focus is on commercial transactions; therefore, suppliers and end users have no incentive to commit fraud, and fraud or errors by outsiders or logistics providers can be controlled. Furthermore, each function is realized by blockchain, which improves the common information management and traceability among other companies. Blockchain improves the efficiency of the entire SCM and clarifies where responsibility lies. The following sections describe in detail the algorithms of the registration device in Section 3.2, the verification device in Section 3.3, and the identification device in Section 3.4.

3.2 Registration Device

The registration device is handled by a supplier. It serves to generate a product-specific key and registers the key in the blockchain by inputting the feature values of the product and information, which are different for each product. This device consists of four elements: measurement, judgment, generation, and registration.

The measurement section extracts the feature value from the target as input signal P1 and outputs the measurement value.

The judgment section determines whether the product is legitimate based on the value obtained from the measurement section. For this purpose, the feature value to be acquired for each product and its legitimate range are set in advance. A judgment value is output after determining that the product is legitimate if within the range, and that it is illegitimate if it is outside the range. The value is then expressed as a relatively large bit string of 128 bits, for example, as binary values of legitimate or not legitimate. In this way, noise reduction technology is no longer necessary and the judgment result is effective in suppressing forgery.

The generation section concatenates the judgment value and "transaction information" U1 unique to each product, which is independent of the product features. Concatenation is performed by an exclusive disjunction. A hash of the concatenated values is then generated as the identification key, Key1. Transaction information identifies products and utilizes, for example, the manufacturer, serial number, temperature, number of verifications, and random numbers. There are no obstacles even if outsiders possess the same type of product. This is because the judgment value is not output to the outside of the

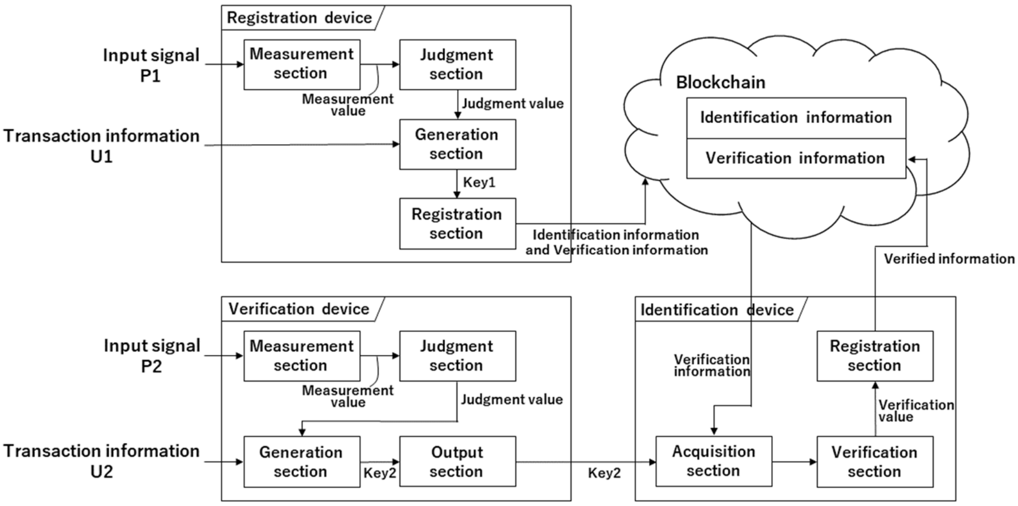

Figure 1: Overview of the system.

device and is kept secret by transaction information, including random numbers. Therefore, the identification key becomes random and unpredictable for each transaction.

The registration section links the information to be verified with the information to identify it. First, “verification information” is generated by hashing to use the Key1 output from the generation section. Then, “identification information” is utilized to identify the information corresponding to the product for which judgment is conducted from among a large amount of verification information. The identification information applies to the manufacturer and serial number pair that is part of the transaction information. Finally, the generated verification and identification information are mapped and registered in the blockchain. Owing to the features of the blockchain, all values are made public. If Key1 is made public as is and a malicious logistics provider forges a verification device to output the value, an end user may be fooled. To prevent fraud, Key1 is hashed and the identification key is unpredictable.

The following shows the specific flow of the registration device.

(1) A supplier inputs an input signal P1, which depends on the product’s features and transaction information U1.

(2) The judgment section determines whether the measurement results are valid.

(3) The generation section generates Key1 from the judgment value and transaction information.

(4) The registration section generates verification information from Key1 and registers it in the blockchain with identification information.

3.3 Verification Device

The verification device is a device handled by the deliverer who transports the product. In much the same way as the registration device, a product-specific key is generated by inputting product features and transaction information, which are different for each product. At this point, the end user, who is notified by the supplier, can input the transaction information and make a judgment using the product to confirm its legitimacy. This device consists of four elements: measurement, judgment, generation, and output.

The measurement section measures a feature value of the target as an input signal P2 and outputs a measurement value.

The judgment section outputs a judgment value based on the acquired measurement values. It determines that the product is legitimate if it is within the pre-set range and illegitimate if it is outside the range.

The generation section concatenates the judgment value and “transaction information” U2 unique to each product, which is independent of the product’s features. Concatenation is performed by an exclusive disjunction. A hash of the concatenated values is then generated as the identification key, Key2. When an end user purchases a product, the information used in the registration device is notified by the supplier as transaction information.

The output section provides Key2 generated by the generation section to the identification device.

In the proposed method, the verification device consists of four parts: measurement, judgment, generation, and output. It can be implemented freely according to the application, such as by installing a generation and output section in the identification device described below. The measurement, judgment, and generation sections are the same as those in the registration device. Thus, if an input signal P2 and transaction information U2 input to the verification device are identical to the input signal P1 and the transaction information U1 input to the registration device, it is obvious that Key2 without noise is always equal to Key1. There is also no property that the key is slightly different each time as in SCM using PUF. Since there is no need to implement techniques such as a fuzzy extractor, it is not necessary to consider the increase in processing time and implementation cost.

The specific flow of the verification device is as follows.

(1) A user provides input signal P2 and transaction information U2 to the device.

(2) The judgment section determines whether the measurement results are valid.

(3) The generation section generates Key2 from the judgment value and transaction information.

(4) The output section outputs Key2 to the identification device.

3.4 Identification Device

The identification device is a device that is handled by an end user. It checks whether the verification information (hash of Key1) registered in the blockchain matches the value of hashed Key2 from the verification device presented by the deliverer. This process confirms the authenticity of the product. This device consists of three elements: acquisition, verification, and registration.

The acquisition section obtains verification information from the blockchain based on the identification information, and obtains Key2 from the verification device. The identification information is extracted using part of the transaction information provided by the supplier to the end user in this process.

The verification section checks for consistency between the verification information and the information in Key2. Specifically, Key2 is hashed, and whether the hash matches the verification information is examined. If it matches, the section outputs the success information to the registration section, indicating that the verification is successful.

The registration section links the "verified information" to the verification information when it is successfully verified and registers it in the blockchain. The information with the verified information is restricted so that it cannot be verified again when verified later. This prevents the same transaction information from being used in a malicious manner.

The specific flow of the identification device is as follows.

(1) The acquisition section obtains Key2 from the verification device. Additionally, it searches the blockchain based on the input identification information, and obtains verification information if the verified information is not attached.

(2) The verification section hashes Key2 obtained in (1). It verifies whether the hash value matches the verification information and outputs the result.

(3) The registration section adds the verified information to the identification information if the result is valid. This is then registered in the blockchain.

4 EVALUATION

To evaluate the proposed method, we discuss possible attacks in Section 4.1. Section 4.2 presents a comparison with conventional SCM using barcodes, RFID, mere substances, and PUF. Furthermore, the implementation cost is described in Section 4.3.

4.1 Attacks on the Proposed Method

4.1.1 Fraud by Logistics Providers

The simplest example of a supply chain is a supplier, a logistics provider, and an end user. It is assumed that there is no fraud in the commercial transactions between a supplier and an end user because they can simply terminate the contract if they are dissatisfied with the other party. The main possible source of an attack is that the logistics provider may swap the authentic item with a counterfeit and the end user receives a counterfeit. In general, an end user does not have a large-scale verification device. The verification is carried out using a verification device owned by a logistics provider for authenticity judgment or normal judgment. The following is an example of a diamond transaction. If a diamond is simply swapped with an object that is not a diamond, such as zircon or zirconia, it can be easily detected as unjustified. However, even if the object is a fake that does not fit into the range, it is possible to make the fake real by forging the device.

The proposed method counters this attack by generating a different key for each transaction. The term "transaction" in this context does not refer to the entire commercial transaction between a supplier and an end user. Instead, it refers to transactions between companies, such as transactions between a supplier and a logistics provider, and transactions between a logistics provider and an end user. The following describes the countermeasure method in detail.

The success or failure of the normal judgment for input signal P2 is noted, but the judgment value itself is not output. It is also difficult to obtain the value from the outside by analyzing the device. The judgment value is then secreted into the device using transaction information U2, including random numbers, and output as the identification key Key2. The random number is known only to the supplier and the end user. Key2 is difficult to predict unless the judgment value is leaked to the outside and randomness is maintained as long as the random number is not known. In summary, the judgment value is not output to the outside of the device but is kept secret in the transaction information to generate Key2, which is difficult to predict and random. This means that even if PUF is not applicable to the target, the function is equivalent to that of PUF. Furthermore, a logistics provider does not have the advantage of storing the Key2 value; because they generate a unique identification key for each transaction, it is meaningless and cannot be used for other transactions. This feature is not found in PUF. In addition, by adding verified information to the transaction once it is used, the system prevents unauthorized double use. Unless a famous brand adds verified information to its own products, it will be possible for an unknown brand to sell its products fraudulently. Using the identification information in the blockchain, an unknown brand can falsely sell products that are identical to the quality of a famous brand. The products are indistinguishable from those of famous brands. It is therefore necessary to add the verified information to the verification information used to limit double use. However, even if the information is verified once, it can be verified again. The number of verifications included in the transaction information is added by one, and the verification information for that is generated. By registering this information, a new verification can be performed.

4.1.2 Blockchain-based Attacks

A blockchain is a public ledger. Therefore, a third party can view the blockchain to obtain information about transactions. This subsection describes the study of the possibility of fraud using the proposed method.

The only information to be registered in the blockchain is identification and verification information. The identification information is used to obtain verification information for the corresponding transaction from the blockchain. It is created using part of the transaction information. In the proposed method, when a product is registered, a supplier notifies all transaction information only to the end user through a secure channel. The system works properly only when the product meets the required standard, and the correct transaction information is entered. Even if an outsider obtains the identification and verification information by browsing the blockchain, he/she will not be able to know the transaction information, such as random numbers. It is not possible to generate the correct Key2. Thus, there is no room for an outsider to show the authenticity of the product using the proposed method. In addition, it is very difficult to falsify the identification and verification information published on blockchain, and attacks using such information are hard. This is because blockchains are virtually impossible to tamper with in terms of computational complexity.

4.2 Comparison with Conventional Methods

The proposed method and conventional methods are compared from four perspectives, as shown in Table 1. Conventional methods include SCM with external tags using barcodes or RFID, SCM utilizing mere substances, and SCM using PUF.

The method using PUF is superior in that it provides an exact match between the shipment and the product received. This is not necessarily important, however. The fact that the product is verified as legitimate is generally sufficient. Furthermore, fraud is possible if a verification device's output indication for a shipped PUF device is forged. Using external tags or mere substances is also flawed in both respects and cannot dispel concerns of end users. It is difficult to determine whether a product is legitimate if an attacker removes a barcode or RFID tag and attaches it to a counterfeit product, or replaces only contents. In the case of mere substances, an end user cannot know an exact result as long as an attacker can produce a verification device to tamper with an output. On the other hand, the proposed method does not fix a judgment value but outputs it randomly for each transaction, so it is possible to determine whether a product is legitimate. This method does not use PUF. However, it provides advantages of unpredictability and randomness like PUF. It can also be applied to products that can use PUF.

Table 1: Comparison with conventional methods (1=lowest; 3=highest).

Method	Exact match with the shipment	Legitimate product	Cost	Distinction per transaction
Proposed method	2	3	1	3
External tag (Barcode/RFID)	1	1	3	1
Mere material	2	2	1	1
PUF	3	2	1	1

External tags are the best in terms of cost, and although they are not as secure, they are relatively easy to install in existing systems. The other three methods are not so simple, as they consist of somewhat complex systems to detect counterfeit products. However, there is a trade-off between high security and cost (simplicity), and supply chain members must pursue what users want.

The distinguishing feature between each transaction is found only in the proposed method. For example, the PUF-based method does not distinguish between each transaction in the process of product flow from user A to user B to user C. The proposed method can generate individualized unique keys using transaction information in the process of product flow from user A to user B and from user B to user C. Double use such as unauthorized resale or diversion can thus be prevented, and suppliers can understand how the products they sell are resold. This is important for ensuring traceability and safety for users.

4.3 Simulation

A blockchain substrate called Ethereum was used to simulate the proposed method from the viewpoint of ease of development and payment in virtual currency. Ethereum generates a fee every time a smart contract is executed. This provides incentives to miners, who are responsible for approving transactions and keeping the blockchain secure. The fee is managed in units called gas. The behaviors of the registration, verification, and identification devices were checked in a test environment. Remix (2021), a web browser integrated development environment (IDE) for developers of the dedicated language Solidity, was employed. Cost calculations were performed using the rate on February 15, 2021. Etherscan (2021) showed that the average gas price was 178.715 Gwei. CoinGecko (2021) showed that the dollar rate was 1804.98 USD/ETH. The implementation cost of each device was calculated as shown in Table 2. “Transaction cost” used in Remix (Table 2) is expressed as the sum of the commonly used transaction cost and execution cost. The cost was high due to the steep rise in the gas price and Ethereum rate. The former involves the limitations of the current processing power of Ethereum, that is, scalability issues. The latter involves a complex combination of factors, but the increase in the number of users and the scalability problem can be cited as factors. However, this is not the essence of the proposed method. This is because other programs have calculated similarly high costs. Although not optimistic, the Ethereum Foundation is already pushing for migration and integration into Ethereum 2.0. This is expected to solve the continuous rise in gas prices and make it possible to advance to faster technology with lower costs. Therefore, it is important to improve the system to an advanced level, in parallel, while paying attention to cost.

Table 2: Cost of each device.

Device	Transaction cost [gas]	Cost [USD]
Registration device	84673	27.31
Verification device	35050	11.31
Identification device	34675	11.19

5 CONCLUSIONS

We proposed a method for determining authenticity using normal judgments for supply chain management. It has the feature of being able to perform the same function as PUF for devices and materials for which PUF has not yet been established. The use of blockchain improves traceability within the entire SCM and increases the difficulty of data tampering. The weakness of the public ledger was overcome using an algorithm based on hash functions. We will continue to study more secure and efficient requirements for practical use, with the goal of reducing the cost of implementation.

REFERENCES

OECD, and EUIPO (2016). Trade in counterfeit and pirated goods: Mapping the economic impact, OECD Publishing, 68, Retrieved March 5, 2021, from https://www.oecd-ilibrary.org/governance/trade-in-counterfeit-and-pirated-goods_9789264252653-en.

OECD, and EUIPO (2019). Trends in trade in counterfeit and pirated goods, OECD Publishing, 11, Retrieved March 5, 2021, from https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en.

Dietrich, F., Ge, Y., Turgut, A., Louw, L., and Palm, D. (2021). Review and analysis of blockchain projects in supply chain management, Procedia Computer Science, 180, 724-733.

Pournader, M., Shi, Y., Seuring, S., and Koh, S. L. (2020). Blockchain applications in supply chains, transport and logistics: a systematic review of the literature, International Journal of Production Research, 58 (7), 2063-2081.

Hackius, N., and Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat?, In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), 23, 3-18.

Tijan, E., Aksentijević, S., Ivanić, K., and Jardas, M. (2019). Blockchain technology implementation in logistics, Sustainability, 11 (4), 1185.

Sun, W., Zhu, X., Zhou, T., Su, Y., and Mo, B. (2019). Application of blockchain and RFID in anti-counterfeiting traceability of liquor, 2019 IEEE 5th International Conference on Computer and Communications.

Toyoda, K., Mathiopoulos, P. T., Sasase, I., and Ohtsuki, T. (2017). A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain, IEEE Access, 5, 17465-17477.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., and Khandelwal, V. (2008). Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications, 2008 IEEE International Conference on RFID, 58-64.

Hori, Y., Hagiwara, M., Kang, H., Kobara, K., and Katashita, T. (2015). Device-specific information generation device, device-specific information generation system and device-specific information generation method, Japanese Patent P2015-154291A. [in Japanese].

Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., and Wilczynski, A. (2019). Towards a supply chain management system for counterfeit mitigation using blockchain and PUF, arXiv preprint arXiv:1908.09585.

Negka, L., Gketsios, G., Anagnostopoulos, N. A., Spathoulas, G., Kakarountas, A., and Katzenbeisser, S. (2019). Employing blockchain and physical unclonable functions for counterfeit IoT devices detection, Proceedings of the International Conference on Omni-Layer Intelligent Systems, 172-178.

Dodis, Y., Reyzin, L., and Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, In International conference on the theory and applications of cryptographic techniques, 523-540.

Koike, M. (2010). Authenticity verification system, information generation device, authenticity verification device, information generation program, and authenticity verification program, Japanese Patent P2010-81039A. [in Japanese].

Remix (2021). Ethereum IDE, Retrieved March 5, 2021, from https://remix.ethereum.org/.

Etherscan (2021). Ethereum average gas price chart, Retrieved March 5, 2021, from https://etherscan.io/chart/gasprice.

CoinGecko (2021). Ethereum price, ETH price index, chart, and info, Retrieved March 5, 2021, from https://www.coingecko.com/en/coins/ethereum.