PUF-based Smart Tags for Supply Chain Management

Alberto Falcone
University of Calabria
Rende, Cosenza, Italy
alberto.falcone@dimes.unical.it

Carmelo Felicetti
University of Calabria
Rende, Cosenza, Italy
carmelo.felicetti@unical.it

Alfredo Garro
University of Calabria
Rende, Cosenza, Italy
alfredo.garro@unical.it

Antonino Rullo
University of Calabria
Rende, Cosenza, Italy
n.rullo@dimes.unical.it

Domenico Saccà
University of Calabria
Rende, Cosenza, Italy
sacca@unical.it

ABSTRACT

Counterfeiting represents one of the most widespread phenomena at a global level that indiscriminately affects all product sectors, from fashion to food, from medicines to digital media. The fight against counterfeiting remains a significant challenge for industries. Most of the current supply chains rely on centralized authorities or intermediaries that are not sufficient robust to guarantee anti-counterfeiting and traceability of goods.

This paper aims at mitigating these issues by introducing a blockchain-based supply chain for traceability and anti-counterfeiting of goods through *Physically Unclonable Function (PUF)* and *Elliptic-Curve Cryptography (ECC)*-based devices, where goods are uniquely identified and tracked along the supply chain so as to trace and detect possible counterfeit. Moreover, the proposed blockchain-based supply chain is decentralized, highly available, and guarantees the integrity of the data stored in it. To assess the validity of the solution two application scenarios have been defined followed by a robustness analysis related to the individual parts that make up the solution.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; **Peer-to-peer architectures**; • **Applied computing** → **Supply chain management**; • **Security and privacy** → *Distributed systems security*.

KEYWORDS

Blockchain, Anti-counterfeiting, Physically Unclonable Function (PUF), Supply Chain Management, Elliptic-Curve Cryptography (ECC)

ACM Reference Format:
Alberto Falcone, Carmelo Felicetti, Alfredo Garro, Antonino Rullo, and Domenico Saccà. 2021. PUF-based Smart Tags for Supply Chain Management. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3465481.3469195

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3469195

1 INTRODUCTION

Counterfeit goods market is an increasingly serious problem affecting producers and customers all over the world. The phenomenon of globalization and e-commerce have contributed to greatly amplify this problem, generating lost revenue for companies. According to the *Counterfeit and Piracy Watch List*, drawn up by the European Commission in 2020, counterfeiting constitutes 3.3% of world trade [6]. Indeed, from a predominantly physical phenomenon, counterfeiting has passed to an almost uncontrollable sphere in which it is necessary to have ad-hoc and effective strategies, architectures, devices, and laws to counter this phenomenon. This aspect becomes crucial when goods are used in critical domains, such as military, food, and medicine, because counterfeited parts can lead to serious security risks and potentially loss for human lives [2, 11]. Counterfeiting is often perceived as a "victimless" crime, in which nobody gets hurt. However, aside from the economic impact, there are serious implications of counterfeit market trading; indeed, some counterfeit products are sold with the customer awareness who intentionally decides to buy products that are of poor quality and failing to meet the minimum safety and security standards; in other cases the costumer is not aware that s/he is buying a counterfeit product with even more negative consequences. In both cases, through reverse engineering approaches, it is possible to make identical copies of the original goods, which are sold as authentic, in order to deceive the final customer and/or regulation authorities. Another aspect that fuels the counterfeiting market comes from goods produced in surplus by third party contractors, which continue to make a certain product even after the contract with the owner has expired. Finally, there are goods that are equally sold instead of being discarded due to the failure of quality controls. Non-authentic goods combined with the inability of retailers and consumers to identify non-genuine products is the main reason that fuels the proliferation of counterfeit products, especially in the luxury supply chain.

To tackle the problem of counterfeiting, it is necessary to have an integrated platform capable of recording every step among the involved companies along the entire supply chain. The availability of such a platform would be an effective means of providing actors involved in the supply chain with precise information on what

companies are doing along the chain to make products. Furthermore, it could ensure that recorded transactions are truthful and not tampered in order to verify the originality of the products.

The implementation of such a platform requires a decentralized infrastructure along the supply chain that allows monitoring of products between producers and consumers. The infrastructure itself should be a distributed peer-to-peer network across parties in the supply chain, without any centralized control that could represent a single point of failure or a performance bottleneck. An emerging technology that lends itself well to implement such a platform is the blockchain [25]. In short, blockchain is a shared and immutable distributed system. It is defined as a digital register whose entries are grouped into blocks, concatenated in chronological order, and whose integrity is guaranteed by the use of cryptography. Although its size is destined to grow over time, it is immutable as data once written can no longer be modified or deleted, unless the entire network is invalidated.

Many blockchain-based supply chain management systems have been proposed in literature and industry to address the abovementioned issues. In [7], authors introduce and present the concept of blockchain and its current applications in logistics and supply networks.

In [18], authors present a blockchain-based system for products anti-counterfeiting. Manufacturers can exploit the proposed system to provide genuine products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance.

In [1], authors propose a decentralized supply chain (block-supply) based on blockchain and Near-Field Communication (NFC) technologies. Experiments conducted by the authors show that the proposed block-supply chain is able to track-and-trace products and detect modification, cloning, and tag reapplication attacks. Authors also introduced a new scalable and secure consensus protocol, which is efficient for large networks.

Toyoda et al. in [23] propose a blockchain-based *Product Ownership Management System (POMS)* that use RFID (Radio-Frequency IDentification) tags to prevent counterfeits in the post supply chain. Authors introduce a novel protocol that enables each party, including supply chain partners and customers, to transfer and prove the ownership of RFID tag-attached products. Authors performed different experiments on the proposed protocol by implementing it on the Ethereum platform.

However, approaches based on the use of RFID tags are vulnerable to cloning attacks, which makes this technology unsuitable for protection against counterfeiting attempts [12, 13]

In this paper a blockchain-based supply chain for traceability and anti-counterfeiting of products through PUF (*Physically Unclonable Fuction*)/EEC(*Elliptic-Curve Cryptography*)-based devices is proposed with the aim to mitigate the traceability and anti-counterfeiting issues discussed above.

The remainder of the paper is organised as follows. After a background on Blockchain and Physically Unclonable Function (PUF) devices (Section 2), Section 3 presents the architecture of the proposed solution based on PUF, blockchain and Smart Contract technologies. Section 4 presents some application scenarios concerning the adoption of the proposed supply chain, whereas its security characteristics are analysed in Section 5. Finally, conclusions and future works are presented in Section 6.

2 BACKGROUND

This section provides a brief overview of the Blockchain technology along with an introduction on the Physically Unclonable Function (PUF) devices.

2.1 Blockchain

Blockchain was introduced in 2009 with the invention of an electronic cash (e-cash) system, called *Bitcoin* [25]. Blockchain can be defined as a Distributed Ledger Technology (DLT) that records transactions among parties in a secure and permanent way [27]. A blockchain is structured as a chain of data blocks, where a generic block b_i is linked to the previous one b_{i-1} through a hash of characters. Block contain a set of transactions, are shared among several peers, and cannot be altered without the consent of the entire network.

Consensus is what gives the blockchain robustness: any updates made to the blockchain are confirmed based on rigorous criteria defined by the consensus protocol, i.e., changes are accepted by all peers when a consensus is reached among a subset of the network. To achieve consensus, different algorithms have been proposed in the literature, such as *Proof-of-work (PoW)*, *Proof-of-stake (PoS)*, *Delegated proof-of-stake*, and *Proof-of-Importance (PoI)* [19]. All consensus algorithms ensure that all peers agree on the final state of the data on the blockchain network and firmly agree that it is true.

These characteristics allow keeping the history of any digital asset without the need of any intermediary to act as a trusted third party to verify, record, and coordinate transactions. This means that there is no central controller in the network, and all participants interact to each other directly.

Although the concept of blockchain was defined as a tool for a cryptocurrency, its use is more general and it can be exploited to create decentralized applications in any other domain, such as industrial, economical, political, humanitarian, and legal. Specifically, the Blockchain technology can be broken down into three categories, i.e., *blockchain 1.0*, *2.0*, and *3.0*, which differ on the managed data, scopes of use, and on what actions can be performed by users.

Blockchain 1.0 began in 2009 with the invention of the Bitcoin cryptocurrency. This first generation of blockchain is mainly used for the management of cryptographic currencies.

Blockchain 2.0 started with the introduction of smart contracts, computer programs intended to automatically execute certain actions when specific blockchain events take place, according to the terms of an agreement. *Ethereum*, *Hyperledger* and other blockchain platforms are considered part of Blockchain 2.0 [24].

The feature which characterizes *Blockchain 3.0* is the capability to run decentralized applications, rather than acting only as decentralized database storage. This feature determines full integration with other technological paradigms related to the Industry 4.0, such as Internet of Things and Artificial Intelligence. In this paper we exploit the potential of blockchain 3.0 for building a framework for the management of supply chains.

2.2 Physically Unclonable Functions

A Physically Unclonable Function (*PUF*) is a hardware primitive that for a given input and conditions (challenge) produces a hardware-based fingerprint (response) that serves as a unique identifier for a device, which cannot be replicated (unclonable) [8]. A PUF is based on unique physical variations which occur naturally during the manufacturing process of semiconductor devices, where small variations and imperfections in the materials introduce random modifications to the operating parameters of the circuits that are impossible to avoid, no matter how controlled the process is.

The PUF technology has many advantages, including its relatively low cost, its inherent security deriving from the impossibility to predict a response, and its stability over time.

Rather than integrate within it a single cryptographic key, PUFs implement a challenge-response authentication mechanism to evaluate its physical microstructure. When a physical input is applied to the structure, it reacts in an unpredictable way due to the complex interaction of the provided input with the physical microstructure of the device. The challenge-response authentication phase consists of two steps, *Enrolment* and *Verification*. In first step, when an entity has to be enrolled, a verifier retrieves the challenge-response data from the entity's PUF and stores it in a database along with the ID of the entity. In the *Verification* step, when an enrolled entity needs to be authenticated, the verifier retrieves the challenge-response data from the database using the entity ID. A random challenge-response pair is retrieved from the database and sent to the entity, which calculates the response using its PUF. Subsequently, the calculated response is sent to the verifier for verification. If the response matches the one stored in the database, the authentication ends successfully and the challenge-response pair is removed from the database to prevent replay attacks. Otherwise, authentication fails.

In theory, a PUF should generate the same response for a given challenge. However, conditions such as temperature, voltage, and current variations may lead to different responses [9].

3 A SOLUTION FOR SUPPLY CHAIN MANAGEMENT BASED ON SMART TAGS

Today's global consumer supply chain has made it possible to trade goods on a planetary scale. However, the biggest challenge for the consumer industry is to ensure safety, reduce counterfeits and at the same time keep operating costs low [17]. The introduction of blockchain technology has already had a deep impact in the financial industry [5, 21]. As this technology matures, it now seems able to address the challenges that the consumer industry have been facing for some time, such as tracing products along the entire production chain, managing fraud, counterfeiting and meeting new consumer trends.

In this paper, blockchain and PUF technologies are combined to provide a novel supply chain framework for traceability and anti-counterfeiting of products that uses PUF-based devices as smart tags associated to the products and the blockchain as a distributed ledger for registering all transactions involving the products.

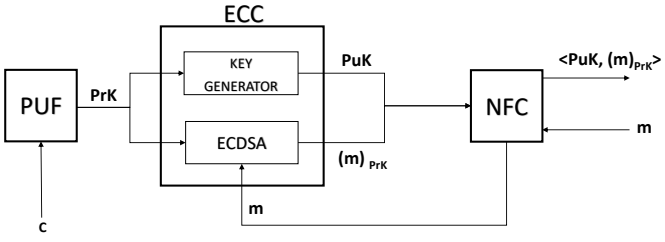

Figure 1: Smart tag architecture.

3.1 Smart Tag

The architecture of the proposed smart tag, depicted in Figure 1, consists of three components: (1) PUF, (2) ECC and (3) NFC. The PUF component is exploited to generate a digital fingerprint for the smart tag in the form of a string of bits; the ECC component uses the fingerprint as a private key to generate a public key, and for signing incoming messages; the NFC (Near Field Communication) component interfaces the smart tag with the external world. The proposed smart tag schema uses the NFC technology as it is available on cell phones enabling them to act as RFID readers, thus providing a product authentication mechanism at the consumer level.

3.1.1 PUF Component. It represents the hardware primitive which produces unpredictable and instantiation dependent outcomes. A silicon PUF is implemented on a silicon chip and uses the intrinsic random variations of the chip manufacturing process to generate a device-unique response (see Section 2.2). This is an advantage for PUF implementation as these variations generate a random output which can be utilized as a unique key/secret to support cryptographic algorithms and services including encryption/decryption, authentication, and digital signature. Except during the cryptographic operation, the PUF key value never exists in digital form within the circuitry of the security integrated circuit (IC). Further, since the key is derived and produced on-demand from physical characteristics of electronics transistors and instantaneously erased once used, it is never present in the non-volatile memory of the device. The structure of the circuits with which the PUFs are built and their sensitivity level make these devices not vulnerable to invasive investigation techniques, modifying their behavior to the point of irreparably manipulating the output when an attempt to intercept confidential information is made.

When the tag receives an input message `m` through the NFC component, a trigger signal enables the hardwired challenge `c` to be given as input to the PUF. As a result of the input `c` a response is pulled out of the PUF component, and used as private key (the digital fingerprint) of the smart tag. Notice that no challenge other than `c` is used in order for a tag to keep the same identity throughout its lifecycle.

3.1.2 ECC Component. The ECC component is used for authentication purposes. The Elliptic Curve Cryptography (ECC) consists of a series of public-key cryptosystems based on the structures of the elliptic curves over finite fields and on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [14]. ECC is

ideal for devices with limited resources, as it provides the same level of security as other cryptographic frameworks, but keeping storage and computational requirements low. Indeed, ECC uses smaller keys and signatures than RSA for the same level of security and provides very fast key generation, fast key agreement, and fast signatures [3].

The ECC component includes a module for generating the public key (Key Generator), and a module for signing input messages (ECDSA). These two modules are enabled when an authentication task has to be performed, i.e., when a verifier wants to authenticate the good the smart tag is associated with.

The authentication protocol works as follows. The verifier (another device or a human by means of a smartphone) submits a message m to the device. The Key Generator module takes as input the private key PrK (returned by PUF activation, see Subsection 3.1.1), and computes a public key $PuK = G \cdot PrK$, where G is the *base point* of the elliptic curve. The input m and the private key PrK are the input of the ECDSA module, which returns the signature $(m)_{PrK}$, that is m signed with the private key PrK. Finally, the pair $<PuK, (m)_{PrK}>$ is returned through the the NFC component to the verifier, which authenticates the tag by simply verifying the tag signature using its public key.

The key generation in the ECC cryptography is as simple as securely generating a random integer in a certain range: any number within the range $[1, n-1]$ is a valid private key, where n is the *order* of the elliptic curve, and the public key PuK is a point on the elliptic curve. An effective random number generator is thus at the basis of the secure functioning of any ECC-based cryptosystem, since predictable generators may be exploited by attackers to infer the private key. This is relevant, in particular, in light of the security vulnerabilities that were identified in pseudorandom generators used by many systems [26]. In this architecture we use the PUF component to generate the private key. Since a PUF is a hardware primitive able to produce unpredictable outcomes, any issue that could arise by using a pseudorandom number generator is avoided.

3.2 A supply chain framework based on Blockchain and Smart Tags

In product supply chains, understanding how products are made and delivered are critical issues. Nowadays, supply chains are global networks that typically include manufacturers, suppliers, logistics companies, and retailers that work together to make and deliver goods to consumers.

As modern supply chains continue to evolve, they also become more complex and disparate. Typically, traditional supply chains use document-based systems that make product tracking a time-expensive task. The lack of traceability and transparency represents a challenge for companies because it leads to delays, errors and increased costs. Therefore, a modern supply chain must provide participants (e.g., producer, distributor, and consumer) with a unified view of the data, so that they can independently verify transactions, such as production and transportation updates.

Given the the main components illustrated in sections 2.1 and 3.1, a blockchain-based supply chain framework for traceability and anti-counterfeiting of products that uses PUF/ECC-based devices used as smart tags associated to products is proposed, thus enabling supply chain actors to track and trace their entire production and delivery process with increased automation efficiency. As depicted in Figure 2, the framework represents a network that allows a company to track its suppliers to produce and distribute products to final consumers. The proposed supply chain and its underlying process are composed of four steps involving different people, information, and resources.

The supply chain begins with *Raw Materials* step, where the raw materials are sourced from logistics service providers. The data related to the raw materials (e.g., price, date, location, quality, and certifications) is registered in the blockchain. In the *Production* step, the row materials are then brought to a production line that refines and transforms them into a finished product. Upon the product is ready, a smart tag is physically coupled to the product to uniquely identify it, allowing for other data related to the product to become anchored to a robust, trustworthy identifier. The smart tag has the potential of addressing the aforementioned challenges of existing technologies in industry regarding safety, tracking, and counterfeiting. The information of both the smart tag and the product is recorded in the blockchain, including the public key of the smart tag.

The *Distribution* step encompasses all the steps from processing customer inquiries to selecting distribution strategies and transportation options. Finished products, as required by consumers, have to meet expectations through the company's delivery distribution channels and logistics services (e.g., road, air and rail). Data related to every delivery phase is recorded in the blockchain. In this way, a company can monitor products along the entire supply chain.

The *Consumer* step regards any organization or individuals who purchase and use products. The purchased products shall be incorporated into another product, which in turn sells to other consumers. Consumers use their smartphone to authenticate the smart tag in order to verify whether the product is original and not counterfeit (see Section 3.1). In addition, they can access the blockchain to retrieve additional information about the product (see Section 2.1).

4 APPLICATION SCENARIOS

The proposed supply chain framework based on blockchain and smart tags can be specialized in different application scenarios; in this section two interesting scenarios are considered:

- *Uncoupled Batch*: batch of *n* products is associated with *n* tags without direct coupling between products and tags;
- *Coupled Batch*: Each product of the batch is associated with a tag.

The first scenario represents a simple specialization of the platform that involves a very reduced logistical complexity but with the drawback that a product can be replaced with another one of lower quality. This inconvenient can be mitigated by using suitable trusting mechanism. The second scenario completely removes the possibility of replacing a product through the coupling between the product and its tag. The drawback is a significant increase in the logistical complexity and particularly suitable for luxury goods.

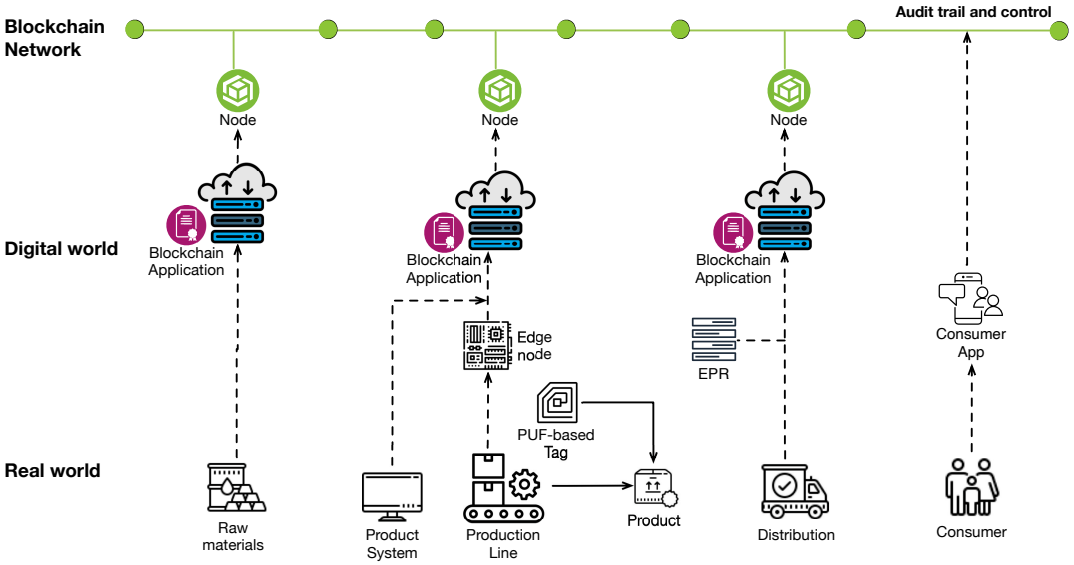

Figure 2: The proposed Blockchain-based supply chain for traceability and anti-counterfeiting of products through PUF.

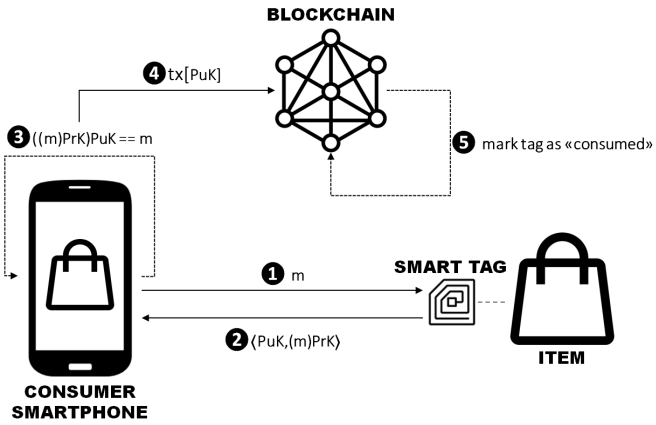

Figure 3: Authentication phase in anti-counterfeiting of goods scenario

4.1 Uncoupled Batch Scenario

The framework proposed in Section 3.2 can be applied as a tool against the anti-counterfeiting of consumer goods.

Given a batch of n consumer goods (products) and n tags, during the enrollment phase, the producer enrols the n tags for the batch by asking each tag to generate its public key that are eventually registered on the blockchain together with a batch description .

The authentication phase enables the customer to authenticate the item s/he is going to buy by approaching its smartphone to the tag, so as to enforce the authentication protocol described in Section 3.1.2. This entails the following steps: the customer submits a message $\mathtt{m}$ to the tag; the tag challenges the PUF with the hard wired challenge $\mathtt{c}$ to regenerate its public-private key pair $\langle \mathtt{PuK}, \mathtt{PrK} \rangle$, and returns the pair $\langle \mathtt{PuK}, (\mathtt{m})_{\mathtt{PrK}} \rangle$ to the customer; at this point the customer checks whether $((\mathtt{m})_{\mathtt{PrK}})_{\mathtt{PuK}}$ equals $\mathtt{m}$, and if successful, s/he can complete the authentication process by verifying on the blockchain that the tag's public key has been enrolled. This is done by issuing a transaction on the blockchain containing the public key $\mathtt{PuK}$: if the tag has not been already used in the past, then the tag's public key is flagged as "consumed", making the tag inoperable for future usage, otherwise the consumer receive an alert message. This way, if the same tag is reused for non-original items, these will be detected as counterfeit. A graphical representation of the actions that make up the operating scheme just described is shown in Figure 3.

This mechanism brings benefits to both the manufacturer and the end user: the manufacturer is allowed to know exactly how many items are currently on the market, and when they are purchased by the end users; on the other hand, the end user is guaranteed to have purchased a genuine product. We stress that a tag that has been consumed for a batch can be later used for tracking another batch.

4.2 Coupled Batch Scenario

Given a batch of n (luxury) goods (products) and n tags, in this scenario each smart tag is coupled with a good, thus the enrolment phase becomes more complex: not only the public key of the tag is registered on the blockchain but also some "unique" features of the associated good. A possible solution is to take some pictures or video of the object, store them in a repository and include their hash together with the public key of the tag.

In the authentication phase, in addition to authenticate the good tag by approaching its smartphone to the tag as in the uncoupled batch scenario, the customer is asked to recognize the features characterizing the good that have been stored in the repository with hash registered in the blockchain. A simple solution is that an ad-hoc app displays the pictures or videos to the consumer. An

interesting issue to be investigated in the future is to use Unsupervised Machine Learning techniques, e.g., following the promising approaches for facial recognition, video surveillance, handwritten character recognition, voice recognition, etc. [22].

5 ROBUSTNESS ANALYSIS

In order to assess the degree of robustness of the proposed solution, an analysis of the weaknesses relating to the individual elements that make up the architecture was conducted. In particular, to consider potential existing vulnerabilities, the cases described in the following were analyzed from a functional point of view.

5.1 Robustness of the smart tag

The proposed tag design does not provide for the use of any memory, thus allowing for the protection against non-volatile memory readout, invasive volatile memory probing attacks [20], and the side-channel attack [10, 15, 16] in which the adversary is able to learn a noisy version of the memory with the aim of inferring secret data. Rather, the challenge c is hard wired which enables the PUF to dynamically regenerate the response every time it is required (see Section 3.1). This reduces the exposure of private data, as it only exists when needed for a cryptographic operation.

Since a tampering attempt to the PUF modifies its behavior, physical inspection of this component cannot be exploited (intrinsic anti-tamper system). The proposed smart tag directly communicates only when in proximity of other devices, thus attacks typically carried in an Internet environment like man-in-the-middle (i.e. relaying or altering the communications between devices) and eavesdropping cannot be accomplished.

5.2 Robustness of the authentication protocol

The classical authentication approach [4] which exploits the PUF technology is based on a challenge-response mechanism: (*i*) during a preliminary enrollment phase a device P registers its challenge-response pairs at a dependable repository R; (*ii*) when the authenticator V wants to verify P's identity, it asks R a P's challenge-response pair and submits the challenge to P; (*iii*) P responds with the corresponding response generated using its internal PUF; (*iv*) finally, V authenticates P if the received response corresponds to the one obtained from R. Besides the complex enrollment phase that may involve difficulties in certain application scenarios, a severe drawback of this authentication scheme is that challenge-response pairs (CRPs) must be stored at a trusted third party, which represents a point of failure due the risk of information leakage. In fact, attackers may steal CRPs with the aim of impersonating a smart tag.

In the proposed authentication protocol (see Section 3), CRPs are not required to be enrolled at trusted third parties, which leaves no room for impersonation attacks. Rather, the verifier directly interacts with the smart tag without the need of involving third parties during the authentication protocol.

5.3 Robustness of the supply chain management framework

A classical issue that arises in a blockchain-based system is the so called *double spending*. In the scenarios discussed in Section 4, once a tag has been bought and thus flagged as "consumed", the buyer cannot falsely attempt another sale, as it would be detected (unless s/he decouple the tag from the item). Furthermore, as the PUF input (i.e., the challenge c) is hardwired, the identity of a smart tag can not be changed over time, and thus a recycled tag can not be re-enrolled as a legitimate one. This way, a counterfeiter cannot introduce multiple forged tags by pretending those to be legitimate new ones, and then attempting a future sale.

Our proposed method makes the tampering with the smart tag very costly due to the presence of the embedded PUF. Various PUF tampering techniques are costly and would have to be performed on a per chip basis to obtain multiple clones.

To make sure a tag is not decoupled from its item before authentication tasks are performed, it should be adopted some anti-tampering mechanisms according to which any decoupling attempt would cause damage to the tag circuit, in order to make it inoperable for future usage. However, a discussion of such a mechanism goes beyond the scope of this paper. Rather, an alternative solution consists in using photos and/or video recordings to collect the characteristics of the items into a dependable repository. The public key of the items, along with the hashes of the video/photo material, are registered on the blockchain. The buyer can finally access the repository in order to check the authenticity of the inspected item.

6 CONCLUSION

This paper presented a blockchain-based supply chain designed to track and mitigate possible counterfeits of goods. The solution provides high availability and strong tolerance against data integrity attacks. The proposed supply chain rely on *Physically Unclonable Function (PUF)* and *Elliptic-Curve Cryptography (ECC)*-based devices to uniquely identify and track goods along the supply chain so as to mitigate the above-presented issues.

Two application scenarios have been defined to assess the validity of the solution followed by a robustness analysis to evaluate the solution against specific threats.

As a possible direction for the future research, the proposed solution will be improved in order to mitigate failure events due to the possible (but already quite unlikely) generation of private keys with a value out of the range allowed by the ECC algorithm. A further contribution will be given on evaluating complex malicious attacks, such as Denial-of-Service and Machine Learning attacks.

ACKNOWLEDGMENTS

This work has been partially funded by the PON-MIUR Projects: ARS01_00587 "SecureOpenNet: Distributed Ledgers for Secure Open Communities – SON" and ARS01_00401 "DEMETRA: DEvelopment of MatErial and TRAcking technologies for the safety of food". Carmelo Felicetti doctoral scholarship is supported by Regione Calabria, within the Project POR Calabria - FSE/FESR 2014-2020 – PhD Students and Research Grant - POR Calabria 2014-2020 - Actions 10.5.6.

REFERENCES

[1] Naif Alzahrani and Nirupama Bulusu. 2018. Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. 30–35.

[2] Erwin A Blackstone, Joseph P Fuhr Jr, and Steve Pociask. 2014. The health and economic effects of counterfeit drugs. *American health & drug benefits* 7, 4 (2014), 216.

[3] Daniel RL Brown. 2010. Sec 2: Recommended elliptic curve domain parameters. *Standars for Efficient Cryptography* (2010).

[4] Urbi Chatterjee, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. 2017. A PUF-based secure communication protocol for IoT. *ACM Transactions on Embedded Computing Systems (TECS)* 16, 3 (2017), 1–25.

[5] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2, 6-10 (2016), 71.

[6] Commission Staff Working Document. 2020. *Counterfeit and Piracy Watch List.* https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159183.pdf Accessed 17 May 2021.

[7] Davor Dujak and Domagoj Sajter. 2019. Blockchain applications in supply chain. In *SMART supply network*. Springer, 21–46.

[8] Basel Halak. 2018. *Physically Unclonable Functions: Design Principles and Evaluation Metrics.* Springer International Publishing, Cham, 17–52. https://doi.org/10.1007/978-3-319-76804-5_2

[9] Basel Halak. 2018. Security attacks on physically unclonable functions and possible countermeasures. In *Physically Unclonable Functions*. Springer, 131–182.

[10] J Alex Halderman, Seth D Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A Calandrino, Ariel J Feldman, Jacob Appelbaum, and Edward W Felten. 2009. Lest we remember: cold-boot attacks on encryption keys. *Commun. ACM* 52, 5 (2009), 91–98.

[11] Bryan T Horvath. 2017. *Not all parts are created equal: The impact of counterfeit parts in the air force supply chain.* Technical Report. Air War College, Air University Maxwell AFB United States.

[12] Jun Huang, Xiang Li, Cong-Cong Xing, Wei Wang, Kun Hua, and Song Guo. 2015. DTD: A novel double-track approach to clone detection for RFID-enabled supply chains. *IEEE Transactions on Emerging Topics in Computing* 5, 1 (2015), 134–140.

[13] Rajat Jain, Dev Kumar Chaudhary, and Sanjiv Kumar. 2018. Analysis of vulnerabilities in radio frequency identification (RFID) systems. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 453–457.

[14] Neal Koblitz. 1987. Elliptic curve cryptosystems. *Mathematics of computation* 48, 177 (1987), 203–209.

[15] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential Power Analysis. In *Advances in Cryptology — CRYPTO' 99*, Michael Wiener (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 388–397.

[16] François Koeune and François-Xavier Standaert. 2005. *A Tutorial on Physical Security and Side-Channel Attacks.* Springer-Verlag, Berlin, Heidelberg, 78,Äi108.

[17] Nir Kshetri. 2018. Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management* 39 (2018), 80–89.

[18] Jinhua Ma, Shih-Ya Lin, Xin Chen, Hung-Min Sun, Yeh-Cheng Chen, and Huaxiong Wang. 2020. A blockchain-based application system for product anti-counterfeiting. *IEEE Access* 8 (2020), 77642–77652.

[19] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. 2017. A review on consensus algorithm of blockchain. In *2017 IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE, 2567–2572.

[20] Sergei P. Skorobogatov. 2005. Semi-invasive attacks – A new approach to hardware security analysis. (2005).

[21] Alex Tapscott and Don Tapscott. 2017. How blockchain is changing finance. *Harvard Business Review* 1, 9 (2017), 2–5.

[22] Tony Thomas, Athira P Vijayaraghavan, and Sabu Emmanuel. 2020. Neural networks and face recognition. In *Machine Learning Approaches in Cyber Security Analytics*. Springer, 143–155. https://doi.org/10.1007/978-981-15-1706-8_8

[23] Kentaroh Toyoda, P Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki. 2017. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE access* 5 (2017), 17465–17477.

[24] Martin von Haller Gronbaek. 2016. Blockchain 2.0, smart contracts and challenges. *Comput. Law, SCL Mag* (2016), 1–5.

[25] Dejan Vujičić, Dijana Jagodić, and Siniša Ranđić. 2018. Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh)*. IEEE, 1–6.

[26] Scott Yilek, Eric Rescorla, Hovav Shacham, Brandon Enright, and Stefan Savage. 2009. When private keys are public: Results from the 2008 Debian OpenSSL vulnerability. In *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement*. 15–27.

[27] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services* 14, 4 (2018), 352–375.