Physically Unclonable Functions (PUFs): A New Frontier in Supply Chain Product and Asset Tracking

Jack Davies[1] and Yingli Wang[2]

[1] Researcher, nChain, email: j.davies@nchain.com

[2] Reader in Logistics and Operations Management, Cardiff Business School, Cardiff University, email: WangY14@cardiff.ac.uk

Keywords

Physically Unclonable Functions; PUF, product tracking, supply chain visibility, blockchain

Abstract

We introduce and explore the early implications of an innovative technological development known as Physically Unclonable Functions (PUFs). We review the main technological developments of product and asset tracking in the supply chain management field ranging from barcode, radio frequency identification (RFID) tags and the Internet of Things (IoTs). We then introduce the PUF: its definition, technical attributes and why it brings unique advantages to product tracking. Several use cases are explored demonstrating how PUFs may add value to supply chains, particularly when combined with emerging technologies such as blockchain. We conclude by discussing potential issues for managers in trying to adopt PUF technology and its limitations.

1. Introduction

Product and asset tracking is an essential part of any effective operations and supply chain management. Knowing the location, identity, and state of physical objects at both the point and time of action provides much-needed supply chain visibility to companies. Having the location visibility of raw materials, work-in-progress, and finished products helps retailers and manufacturers in elimination of counterfeit products, effective inventory control, agile response to changes in demand and supply chain planning.

Supply chain visibility is also critical for product recalls in case there are quality and safety issues. Product tracking plays an important role in closed-loop product or asset life cycle management, powering the emerging concept of circular economy (Ellen MacArthur Foundation, 2016).

It worth noting that there are two terms often associated with supply chain visibility. *Tracking* is the term often used to describe the determination of the identity and state of a product in the forward direction—from supplier to manufacturer to the end user. *Tracing* is used to infer the product's path and history from downstream to upstream of the supply chain (Musa et al., 2014). Tracking history provides a record for traceability.

In recent years, demand for true end-to-end visibility and traceability continues to gain momentum driven by increasing consumer demand for transparency and the need for security, accuracy and auditability (GS1 2020). Product tracking has evolved from manual analogue

processes to the use of quick response (QR) code, radio frequency identification (RFID) and Internet of Things (IoTs) technologies. Coupled with systems such as satellite navigation systems and telematics, one can track goods in real time.

Existing tracking technologies have their limitations. For instance, QR code and barcodes are the most established tracking technology but require manual scanning. RFID tracking tags are not suitable for certain types of products. Many connected IoT devices have less secure software and are vulnerable to malware. Millions of insecure IoT devices are connected to the internet and have become the 'botnet of things', presenting 'a serious challenge to cyber security for a considerable time to come' (National Crime Agency, 2017, p.8).

It is in this context, we propose to introduce a new frontier in product and asset tracking, known as Physically Unclonable Functions (PUF). PUF has the potential to address the aforementioned limitations of existing technologies. A PUF is like a fingerprint or biometric for a physical object where each instantiation of that object has its own unique PUF response.

A PUF exploits inherent randomness introduced during manufacturing to give a physical entity a unique fingerprint or trust anchor (Gao et al., 2020). Before introducing PUFs, we shall firstly discuss the current state of developments in supply chain product and asset tracking. We will then further define PUF technology, how it functions and why it brings unique advantages to product tracking. This will be followed by a discussion of several supply chain use cases, in particular by using PUF devices in conjunction with a blockchain for data integrity and product identity management. Finally, we will explore potential issues for managers in trying to adopt this technology and its limitations.

2. Current state of product and asset tracking

In this section, we briefly describe some of the well-established tracking technologies in supply chain management.

2.1 Barcodes

When an item or product travels through the supply chain—taking an example of a type of prepacked item—its whole journey involves raw material suppliers, producers, logistics companies, distributors and retailers, before finally reaching consumers. At each stage, there needs to be a record of its certain attributes for safety and quality control purposes—often imposed by legal requirements. Historically record keeping and updating was manual and paper based, often slow and incurring errors.

Barcode emerged to address this record keeping problem in the 1970s. Barcodes are made up of black stripes of varying thickness and a 12-digit number that encodes numerical data that a machine could read (Eastman 2015). By tracking and automating inventory, barcode lowered the cost of having a wide variety of products and made it possible to run a diversified complex supply chain operation possible that can sell a large number of product lines—each product line given a universal product code (UPC). Nowadays, barcodes have been used almost everywhere, including manufacturing, transportation, government and health care.

Two-dimensional (2D) barcodes appeared at the end of 1980s (Gao et al., 2007). Unlike 1D barcodes, 2-D barcodes are able to meet the needs of encoding alphanumeric data, including letters, numbers, and punctuation marks, and can hold much more data in a small area to support information distribution and detection. Taking an example of GS1 QR Code, its

numeric capacity is up to 7089 and alphanumeric capacity up to 4296 (GS1 2021), whilst the maximum capacity of 1D barcode is only 28-bits. Given its larger capacity, higher reliability and ease of production, 2D barcode has gained popularity since the 1990s in areas of document management, fraud prevention, inventory tracking, ID cards, parts marking or product tagging (Kato et al., 2010; Lin et al., 2014).

Despite the advantages of 1D and 2D barcodes, one major weakness is the need for manual scanning. Another disadvantage, particularly associated with 1D barcode is that item-level tracking is difficult, as barcodes are mostly used to track a product line, rather than individual products of the same product line.

2.2 Radio Frequency Identification (RFID)

RFID is an automatic identification solution that streamlines identification and data acquisition. Its origin dates to the 1920s and with wider uptake in practice only occurring in the 2000s (Vena et al., 2016).

RFID systems consist of an RFID tag (typically many tags) and an interrogator or reader. The interrogator emits a field of electromagnetic waves from an antenna, which are absorbed by the tag. The absorbed energy is used to power the tag's microchip and a signal that includes the tag identification number is sent back to the interrogator which then transmit the data to a database that is used to assess the information captured (Perret 2014).

RFID's major advantages over barcode lie in that many tags can be read simultaneously without line-of-sight as items are moving (Williams 2016). RFID technology can provide a unique identity to a specific item, allowing for efficient item tracking-and-tracing.

RFID can be categorised into active or passive RFID depending on whether tags require a power source. The former are the most widespread tags in supply chain for tracking of stock, sales, and orders. The latter is more expensive and often used when the required reading range is greater than 10 meters. Active tags are mainly used for monitoring physical parameters—such as temperature, humidity, movement—used for cold chain control in refrigerated trucks.

It is worth noting that RFID does not necessarily eliminate the use of barcode—which has cost advantages and is simple to use. Often the two can be used together. Today RFID is not universally adopted in the supply chain, largely due to cost and performance. Implementing RFID systems is significantly more expensive and complex than a barcoding system. Properties of some materials—for example water or metal—may be an obstacle to RFID application at a given radio frequency, as they may corrupt data transmission either by absorption or by ambient reflection of the signals.

2.3 Internet of Things (IoTs)

RFID may be considered an early form of IoTs. But, IoT has developed and extends beyond the scope of RFID alone. IoT is the term used for networks of uniquely identifiable physical objects—*things*—that are embedded with low-cost sensors and actuators for data collection, monitoring, decision-making and process optimisation. IoTs may interact and operate with or without conscious human intervention.

Currently IoTs' main deployment in supply chains is for product tracking and monitoring. Example applications include inventory management and control, management of trailers, containers and other heavy assets, and shipment tracking.

One example of innovative IoT use is that of the German carmaker, Daimler, which launched the *car2go* service, which uses IoT functionality to monitor and manage cars remotely, allowing customers to use shared cars. IoTs also power innovations in retailing, for instance the *checkout-less* store launched by Amazon.

As with RFID, major adoption barriers relate to the high cost of IoT infrastructure, security, and privacy concerns. While IoTs continue to gain popularity, the rising number of IoT devices pose significant security risks. Many have less secure software, can be reprogrammed to become the *botnet of things* and used to deliver distributed denial of service (DDOS) attacks (Paffenroth and Zhou 2019).

3. Physically Unclonable Functions (PUFs)

3.1 What is a PUF?

PUFs are a class of physical devices that can be used to provide unique digital fingerprints for devices. They act like physical random functions, which use the tangible underlying properties and characteristics of a device to generate a distinct and universal attribute (Gao et al., 2020).

A PUF-based fingerprint for a physical device can be used to identify and authenticate its use in complex systems such as supply chains, allowing for other data related to the device to become anchored to a robust, trustworthy identifier.

The advent of PUF technology addressed a long-standing problem in cryptography and device security: namely the need to store sensitive keys in non-volatile memory. Prior to the introduction of PUF in early 2000s, many electronic systems needed to store important keys used for encryption, access-control, and other important processes in physical memory. This presents a significant vulnerability to physical or invasive attacks on electronics—such as IoTs—that store digital keys in non-volatile memory where a malicious attacker aims to extract or copy the keys from the device using a range of practical physical attacks (Yao et al., 2019).

In order to mitigate risks these devices can implement protective measures, such as by using secure memory, erasable read-only memory (EEPROM)—authenticated and/or encrypted storage (Herder et al., 2014)—but this serves to increase the overall costs of the system and adds inefficiency. The primary advantage of using a PUF is that it does not require a key to be stored in-memory on the device. Instead, PUFs employ a challenge-response mechanism to generate keys on-the-fly based on the underlying physical properties of the device itself. The keys generated using a PUF are therefore bound to that specific device because they depend on the unique characteristics of that particular PUF instance.

PUFs rely on measurable random variations in the physical properties of devices caused during manufacturing. These differences occur on the micro- and nanoscales, which means they are infeasible to control or predict, such that even original equipment manufacturers (OEMs) cannot meaningfully influence the physical characteristics of PUF devices. We call this property of PUFs *manufacturer-resistance* and it forms a core assumption underpinning their security as key-generators for devices. These variations ensure that each PUF, and its corresponding challenge-response behaviour, can be considered unique.

This property means that PUFs are extremely well-suited to providing digital fingerprints for physical objects, because they are unique and inherently bound to the device or object rather than being assigned to it from an external source. The intrinsic nature of the challenge-response behaviour of a PUF also means that they are highly tamper-proof. Any attempt to modify a PUF device physically or by invasive means will result in the alteration of its low-level physical parameters and thus a change in its challenge-response behaviour, which can be easily detected.

The basic mode for interacting with a PUF is to input a challenge to the device, which the PUF maps to a response. A challenge and its corresponding response for a given PUF is known as a challenge-response pair (CRP), and the deterministic mapping from the challenge to the response depends on the internal physical characteristics of the PUF. In this sense, a PUF can be considered much like a physical one-way function, generating an unpredictable yet deterministic response to a given challenge.

As shown in Figure 1, inputting identical challenges to the same PUF will yield the same response, but inputting them into different PUFs will yield different responses. The form of both the challenges and responses for a PUF device will depend on both the specific type of PUF chosen and how it has been implemented. For example, in an optical PUF (Pappu, 2001), the challenge is the angle of incidence of a light source on the PUF—a small optical medium in this case—and the response is a unique speckle pattern caused by the interaction of the light beam with randomly distributed bubbles in the optical medium.

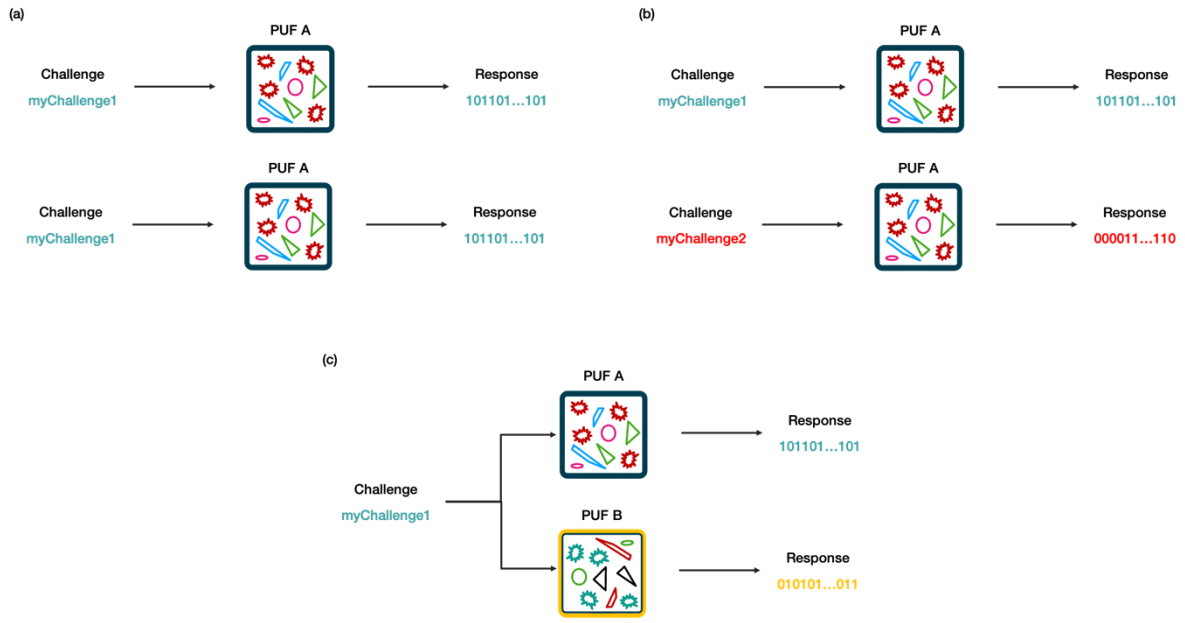

***Figure 1**. The basic properties of PUFs; (a) presenting a given PUF with the same challenge will produce the same response, (b) presenting a given PUF with two different challenges will produce different responses, and (c) presenting two different PUFs with the same challenge will produce different responses.*

3.2 Weak and Strong PUFs

The field of research related to PUFs is nascent and growing rapidly. A wide range of differing PUF implementations have surfaced over the last two decades, which has led to their classification into two categories: *weak* PUFs and *strong* PUFs (Herder et al., 2014). The distinction between these classes of PUF device is based on the number of CRPs that the PUF can provide--also known as the PUF *CRP space*. The size of the PUF CRP space for a particular implementation will tend to determine its utility for different applications.

Weak PUFs are characterised by having a small CRP space, often providing just one or a few CRPs. This characterization also means that the challenge-response interface of a weak PUF should be protected, with access controls such that only an authorised user can probe the device with a challenge and obtain a response. These types of PUFs are generally used to generate a single root key for a device, used for simple device identification, or from which further derived keys can be used in cryptographic applications, such as encrypting on-device memory or generating message authentication codes (MACs).

Strong PUFs are distinguished by having a much larger CRP space. Strong PUFs are typically able to yield so many CRPs that it is considered infeasible for an attacker to be able to enumerate the entire CRP space even with direct access to the device. This characteristic means that some strong PUFs can be implemented with an unrestricted challenge-response interface, although this is not often done in practice, and a sub-class of controlled PUFs (CPUFs) have been proposed to mitigate attacks.

A vast CRP space makes strong PUFs highly applicable for use in device authentication protocols—such as for implementing key cards—where it is desirable that the device can be presented with fresh challenges on many different occasions. However, designing strong PUFs that are both secure and practical is non-trivial and is an on-going challenge for industry.

3.3 Example: The Static Random-Access Memory (SRAM) PUF

Weak PUFs are generally more practical and inexpensive to produce, which has led to their widespread use in many fields. For example, a weak PUF based on static random-access memory (SRAM), known as the SRAM PUF (Holcomb et al., 2009) is widely deployed for device identification and security applications.

The SRAM PUF makes use of sub-micron variations in SRAM cells that occur during their manufacture, whereby the resulting electrical properties of transistors in these cells are unpredictable. Small differences in transistor voltages become observable when power is supplied to an SRAM cell and it preferentially takes one of two binary states (see Figure 2). This means that a region of SRAM memory will have a distinct fingerprint based on which cells assume start-up values of ‘0’ or ‘1’ within the region. The digital fingerprint obtained from the behaviour of a collection of SRAM cells—a response on the order of one kilobyte—can be used to derive a root key for the PUF, which can in turn be used to identify the device and perform cryptographic processes.

In practice, the SRAM PUF employs additional techniques to ensure the uniqueness and reliability of the PUF key generated from a silicon chip (Intrinsic ID, 2017). These steps include error-correction, whereby an enrolment phase is introduced to ensure that the same PUF key can be reconstructed each time the chip is powered on. In the context of an SRAM PUF, the challenge corresponds to the memory address(es) of the SRAM region, and the response corresponds to the binary start-up state of each cell.

SRAM PUFs are widely used in the field because they can be implemented in virtually any silicon device containing static memory, whilst also being simple to implement in flexible environments such as field-programmable gate arrays (FPGAs). In other examples, SRAM PUFs have been implemented by applying a software module to existing hardware, effectively allowing an existing device to become an SRAM PUF at will.

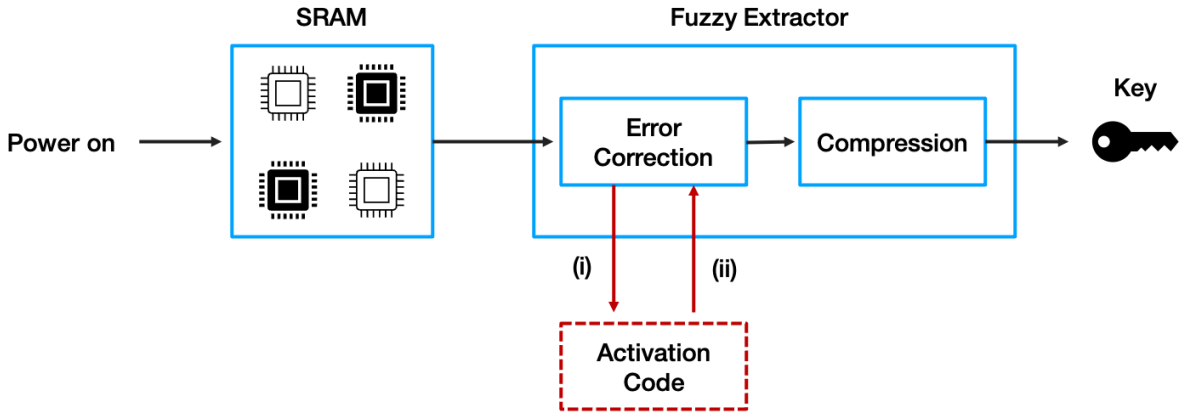

***Figure 2**. A schematic diagram of an SRAM PUF comprising a region of SRAM memory cells and PUF logic in the form of a fuzzy extractor that performs error correction and compression on the raw SRAM fingerprint. The fuzzy extractor utilises an activation code (AC) to ensure the same key will be derived from the SRAM PUF. The code is generated during an enrolment phase (i) and is utilised during any key reconstruction phase (ii) at a later time when the key is be regenerated.*

4. Applications of PUFs in the Supply Chain

PUFs sit at the interface between the physical and digital worlds; they provide a means of extracting robust digital identity from inherent physical uniqueness. This makes PUF technology a strong candidate for use in digital supply chain tracking, where a key requirement is the ability to bridge the physical objects and digital systems.

We can consider PUFs to be a natural successor to barcodes, QR codes, and RFID tags in the context of supply chain tracking and transparency. The key benefit that PUFs provide over these existing technologies is that they are highly tamper-proof and infeasible to copy because they leverage an intrinsic form of digital identity. This benefit is in stark contrast to the incumbent techniques used for supply chain visibility, which merely assign digital identifiers to physical objects, making them vulnerable to physical attacks such as impersonation or modification. This characteristic is crucial for trustworthy supply chain tracking, as it can ensure that tracking data is logged for only the intended device(s). There is greater confidence that the device in question has not been modified, counterfeited or replaced.

4.1 Anti-counterfeiting

Measures to mitigate counterfeiting attempts are key to many industries, and typically require a high degree of supply chain visibility and traceability. Effective anti-counterfeiting measures require the ability to both identify physical items in the supply chain and to detect when counterfeiting has occurred to a particular item. Traditional identity measures such as barcodes and RFID tags meet the first requirement, but only in a limited capacity given that the

identifying information or tag are vulnerable to modification and cloning attacks (Ai et al. 2020). These techniques also fail to fulfil the second requirement in a meaningful capacity, as the integrity of a barcode or RFID tag does not imply the integrity of the item itself.

PUFs can address both shortcomings--the use of an intrinsic identifier as opposed to an applied identifier ensures that can confidently identify a device or object without risk of cloning, while the tamper-proof property of PUF devices ensures that any attempt to modify the device during its movement through the supply chain will be detected.

A simple scheme has been suggested (see Aniello et al., 2019) whereby the PUF response is verified at each delivery point in the supply chain to provide counterfeit-detection. Aniello et al., (2020) demonstrate that a particularly promising area for PUF is in the integrated circuit (IC) supply chain. Electronic components in IC supply chains are items where PUFs can be easily and cheaply implanted by integrating PUF circuitry inside the component circuitry, ensuring that tamper-evident PUFs cannot be removed and replaced. PUFs can be used not just for identification *and* authentication. The authentication can be repeated after a system is assembled or resold, protecting against counterfeit ICs being inserted throughout a system's lifecycle (Bauer and Hamlet 2014).

4.2 IoT security

The increasing use of IoT devices in the supply chain is a driver for increased supply chain visibility. Tracking data can be reported automatically through IoT connected devices. The problem of authenticating IoT devices efficiently in such networks is a challenge, especially given devices with low computational resources.

PUFs have been proposed as tool to allow for lightweight authentication of IoT devices (Braeken, 2018). PUFs have received significant attention in the industrial sectors for addressing the security concerns of a vast quantity of IoT devices (Shamsoshoara et al., 2020).

These applications represent another facet to the use of PUFs in the supply chain; namely as a way to augment other transformative technologies like IoT that are already being adopted to aid supply chain tracking and visibility.

4.3 Field-Programmable Gate Array (FPGA)s and Intellectual Property Protection

FPGAs are configurable integrated circuits that allow for the user to design the circuit post-manufacturing, which have become widely deployed in a variety of computing applications due to their flexibility and re-programmability. Intellectual property (IP) rights for the designers of bespoke FPGA circuits have become a critical concern in recent years.

The nature of FGPAs makes them highly vulnerable to cloning, allowing an attacker to effectively copy a proprietary FPGA design and circumvent paying the requisite licensing fees. The problem can be solved in part by using encryption, but the inability to store an encryption key in non-volatile memory on an FPGA has motivated the use of PUFs embedded within the FPGA to fully resolve the issue. For instance, the scheme proposed in (Guajardo et al., 2007) employs PUFs to enforce that (i) certain FPGA designs to be restricted to running on specific hardware, and (ii) a given hardware can only run authorised FPGA designs.

This example exemplifies another role of PUFs in enforcing property rights within integrated circuit supply chains in particular.

One particular use case could be supplier vetting and IP management. Typically, when manufacturing companies select, vet, and engage new suppliers, those suppliers are required to go through complex due diligence and IP protection negotiations at the point of contract. As a result, the process can be lengthy, leading to increased time, cost, and risk for all parties. The use of PUFs can effectively protect supplier IP, streamline the supplier engagement process, and build trust among integrated circuit supply chain actors (Islam et al., 2019).

5. Combining PUFs and Blockchains

The integration of PUF devices and blockchains has been explored in a number of recent works (Aniello et al., 2020; Negka et al., 2019; Mohanty et al., 2020), with many focusing on supply chains as a driving theme (see Figure 3). This combination of emergent technologies can lay the groundwork for a more holistic approach to supply chain visibility.

Introducing the blockchain into supply chain management can facilitate increased transparency and trust in tracking data if it is logged or notarised on-chain. In particular, the deployment of a public distributed ledger in a supply chain tracking system can enable strong guarantees of data integrity.

In this case, the key benefit an assurance of tracking data integrity from the blockchain network—independent of the supply chain tracking system itself. Moreover, the public blockchain acts as a distributed time-stamping service for data, such as identity-mappings or access controls for IoT devices. This aspect may be advantageous in turning real-time tracking data into a long-term resource for traceability, where historical activity within the supply chain can be reliably traced backwards in time without the risk of the tracking data changing.

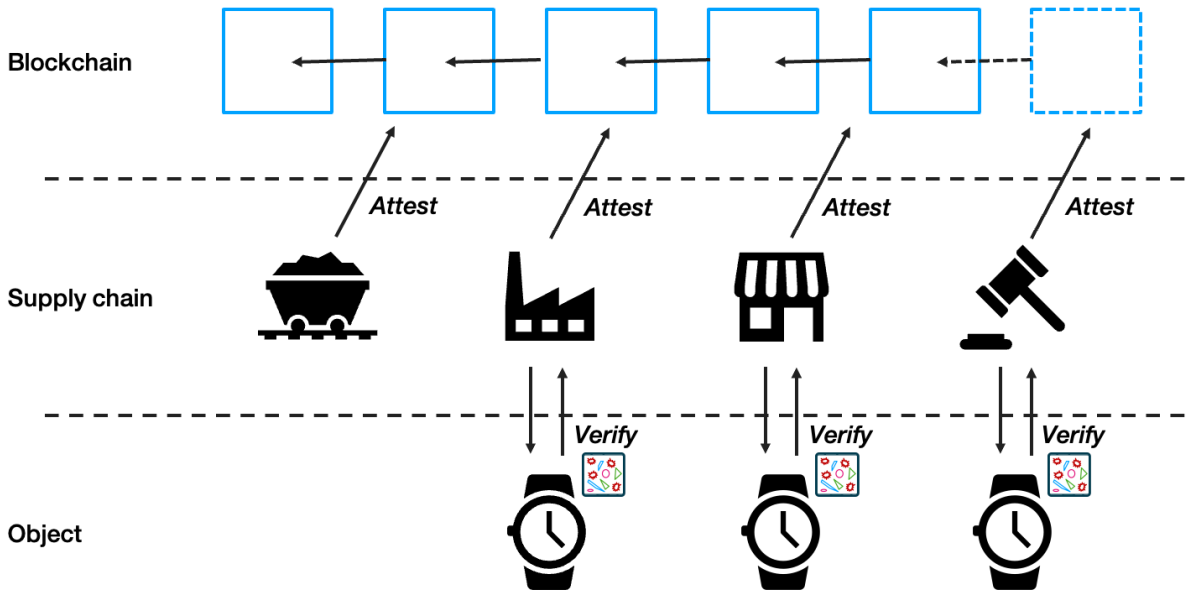

***Figure 3**. An outline showing the combination of PUF and blockchain technologies for increasing supply chain visibility. At each point in the supply chain, with time flowing from left to right, a physical good (e.g., a watch) equipped with a PUF can used to verify its authenticity, and data about the product or proof that the verification has occurred can be logged on the blockchain.*

A further aspect whereby the supply chain may benefit from combining PUFs and blockchain is in fostering *accountability* amongst suppliers and other participants (Aniello et al., 2019). In particular, inherent technical features of the blockchain, such as digital signatures, can be leveraged to add accountability (Guardtime, 2016). Digital signatures, which are used extensively across many different blockchain architectures, are submissible as legal evidence in many jurisdictions, including the UK (Electronic Communications Act, 2000).

Accountability may therefore be improved within a supply chain if its participants and stakeholders are required to provide digital signatures on tracking data, whose integrity can also be ensured by publishing the signatures on the blockchain. The use of PUFs can improve the situation still by linking digital signatures to hardware devices, which could be used to prove that a supplier logged tracking information using standard-issue, certified or approved equipment.

As a new frontier in asset-tracking, the combination PUF devices and blockchain technology provide complementary capabilities. PUFs represent innovations in device identity and authenticity, while the blockchain embodies a new standard in data traceability and integrity. PUFs are an enabling technology for tracking data and blockchain is an enabling technology for tracing it. These properties dovetail to meet requirements of a mature supply chain management paradigm.

6. Discussion and Conclusion

Although PUFs show great potential in supply chain tracking, their deployment is not without challenges.

As a maturing technology the main technical challenges for some PUF implementations include reliability, practicality, and evolving mathematical and physical attacks. For example, some strong PUFs have been shown to be vulnerable to modelling attacks whereby the challenge-response behaviour of the PUF can be mimicked (e.g. using machine learning) by observing many CRPs in certain implementations.

While weak PUFs face fewer attack vectors in general, the need for robust error-correction methods presents an additional implementation challenge, and the small CRP spaces of these PUFs can limit the scope of their applications. Countermeasures that tackle those issues are in place and new measures being actively explored (Gao et al., 2020; Braeken 2018).

Another issue is that a failure of the PUF circuit is likely to lead to inaccuracies in the counterfeit detection process – a problem intrinsic of any tag-based tracking mechanisms.

A significant limitation of PUFs in the supply chain is that their practical application for anti-counterfeiting is presently suited to electronic devices with existing integrated circuits, but requires more thought for other types of non-electronic physical good such as watches or diamonds. In these cases, we require a practical—or at least cost-effective—PUF implementation whereby the PUF is suitably embedded within the physical good. Other concerns include privacy and cost of implementation.

However, in the case of non-electronic products, we can conceive of the use of PUF devices in other aspects of supply chain management to improve visibility indirectly. For instance, PUFs may facilitate more trustworthy monitoring of the supply chain by securing IoT devices and sensors already used to track non-electronic products, where PUFs may improve the identity-

management of such devices. In addition, PUFs may be applied to electronic devices such as scanners used for collecting data about non-electronic devices in the supply chain, such that we can ensure data has been collected and recorded using the correct equipment and methodology. In both aspects, introducing a blockchain for data integrity and identity-management can improve the value proposition for supply chain visibility.

In summary, we have discussed the classical technologies utilised for product and asset tracking in supply chain and introduced PUFs as a new frontier that has several advantages over the existing methods. We articulated a few application areas where PUFs could create value for supply chain tracking, and where their utility may be enhanced when used in conjunction with a blockchain.

Though we are yet to see a wide deployment of PUF devices across diverse supply chains, in particular outside of IC supply chains, new PUF architectures and applications are continually being developed. We therefore need to keep abreast of ongoing developments in the field in order to fully utilise their potential.

References

Ai, X., Chen, H., Lin, K., Wang, Z. and Yu, J., 2020. Nowhere to Hide: Efficiently Identifying Probabilistic Cloning Attacks in Large-Scale RFID Systems. *IEEE Transactions on Information Forensics and Security*, 16, pp.714-727.

Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M. and Wilczynski, A., 2020. Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF. *International Journal of Information Security*, pp.1-16.

Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M., & Wilczynski, A. (2019). Towards a Supply Chain Management System for Counterfeit Mitigation using Blockchain and PUF. *ArXiv, abs/1908.09585*.

Bauer, T. and Hamlet, J., 2014. Physical unclonable functions: A primer. IEEE Security & Privacy, 12(6), pp.97-101.

Braeken, A. PUF Based Authentication Protocol for IoT. *Symmetry* **2018**, *10*, 352. https://doi.org/10.3390/sym10080352

Eastman, J. 2015, Brief history of barcode scanning, in OSA Century of Optics, p.128-133

Ellen MacArthur Foundation, 2016, Intelligent assets: unlocking the circular economy potential, available from https://www.ellenmacarthurfoundation.org/publications/intelligent-assets, date accessed 11/10/2020.

Gao, J.Z., Prakash, L. and Jagatesan, R., 2007, Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution. In *31st Annual International Computer Software and Applications Conference (COMPSAC 2007)* (Vol. 2, pp. 49-56). IEEE.

Gao, Y., Al-Sarawi, S.F. and Abbott, D., 2020. Physical unclonable functions. *Nature Electronics*, *3*(2), pp.81-91.

GS1, 2020. Trend Research 2020-2021: navigating the next normal, available from https://www.gs1.org/articles/trend-research-2020-2021-navigating-next-normal?it_medium=carousel&it_campaign=TrendResearch2020-2021, date published 2/12/2020, date accessed 07/01/2021.

GS1, 2021, Two-dimensional (2D) barcodes, available from https://www.gs1.org/barcodes/2d, date accessed 11/01/2021.

Guajardo J., Kumar S.S., Schrijen GJ., Tuyls P. (2007) FPGA Intrinsic PUFs and Their Use for IP Protection. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74735-2_5

Herder, C., Yu, M.D., Koushanfar, F. and Devadas, S., 2014. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, *102*(8), pp.1126-1141.

Holcomb, D. E., Burleson, W. P. & Fu, K. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Trans. Comput.* **58**, 1198–1210 (2009).

Intrinsic ID, 2017, SRAM PUF : The Secure Silicon Fingerprint, available from https://www.intrinsic-id.com/wp-content/uploads/2020/08/sram-puf-secure-silicon-fingerprint-white-paper.pdf, date accessed 18/02/2021.

Islam, M.N. and Kundu, S., 2019. Enabling ic traceability via blockchain pegged to embedded puf. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, *24*(3), pp.1-23.

Kato, H., Tan, K.T. and Chai, D., 2010. *Barcodes for mobile devices*. Cambridge University Press.

Lin, Y.C., Cheung, W.F. and Siao, F.C., 2014. Developing mobile 2D barcode/RFID-based maintenance management system. *Automation in construction*, *37*, pp.110-121.

Mohanty, S.P., Yanambaka, V.P., Kougianos, E. and Puthal, D., 2020. PUFchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE). *IEEE Consumer Electronics Magazine*, *9*(2), pp.8-16.

Musa, A., Gunasekaran, A. and Yusuf, Y., 2014. Supply chain product visibility: Methods, systems and impacts. *Expert Systems with Applications*, *41*(1), pp.176-194.

National Crime Agency (2017). The cyber threat to UK business: 2016/2017 report. National Crime Agency and National Cyber Security Centre. [online] Available at: http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file [accessed 22 May 2018].

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

Paffenroth, R. C., & Zhou, C. (2019). Modern Machine Learning for Cyber-Defense and Distributed Denial-of-Service Attacks. IEEE Engineering Management Review, 47(4), 80-85

Pappu, S.R. 2001, Physical One-Way Functions. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA.

Perret, E., 2014. *Radio frequency identification and sensors: from RFID to chipless RFID*. John Wiley & Sons.

Shamsoshoara, A., Korenda, A., Afghah, F. and Zeadally, S., 2020. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Computer Networks, 183, p.107593.

Electronic Communications Act 2000. [online] Available at: <https://www.legislation.gov.uk/ukpga/2000/7> [Accessed 11 March 2021].

Vena, A., Perret, E. and Tedjini, S., 2016, Introduction to RFID technologies, in Vena et al ed, Chipless RFID based on RF Encoding Particle, Elsevier, 2016, Pages 1-26, ISBN 9781785481079

Guardtime. 2016. Internet of Things Authentication: A Blockchain solution using SRAM Physical Unclonable Functions. [online] Available at: <https://www.intrinsic-id.com/wp-content/uploads/2017/05/gt_KSI-PUF-web-1611.pdf> [Accessed 11 March 2021].

Williams, H. 2016, RFID in logistics, in Wang and Pettit ed, E-logistics: managing your digital supply chains for competitive advantage, Kogan Page, London, pp. 270-299

Yao, F., & Venkataramani, G. (2019). Architecting Non-Volatile Main Memory to Guard Against Persistence-based Attacks. *ArXiv, abs/1902.03518*.