applied sciences

MDPI

Article

An Innovative Strategy Based on Secure Element for Cyber–Physical Authentication in Safety-Critical Manufacturing Supply Chain †

Ernesto Gómez-Marín [1,*], Valerio Senni [2], Luis Parrilla [3], Jose L. Tejero López [1], Encarnación Castillo [3] and Davide Martintoni [2]

[1] Infineon Technologies AG, 85579 Neubiberg, Germany
[2] Applied Research & Technology, Collins Aerospace, 00185 Rome, Italy; valerio.senni@collins.com (V.S.); davide.martintoni@collins.com (D.M.)
[3] Departamento de Electrónica y Tecnología de Computadores, Universidad de Granada, 18071 Granada, Spain; luis@ugr.es (L.P.); encas@ugr.es (E.C.)
* Correspondence: ernesto.gomezmarin@gmail.com
† This paper is an extended version of our paper published in 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Barcelona, Spain, 1–3 August 2022.

Abstract: The accurate tracking of every production step and related outcome in a supply chain is a stringent requirement in safety-critical sectors such as civil aviation. In such a framework, trusted traceability and accountability can be reliably and securely managed by means of blockchain-based solutions. Unfortunately, blockchain cannot guarantee the provenance and accuracy of the stored information. To overcome such a limitation, this paper proposes a secure solution to strongly rely on the tracking information of the physical assets in the supply chain. The proposed solution exploits Hardware Security Modules (HSMs) to provide required cryptographic primitives through a Near-Field Communication (NFC) connection. In our approach, each transfer of the assets is authenticated, verified, and recorded in the blockchain through the HSM. Transaction entries are signed, thus providing a guarantee of ownership and authenticity. The proposed infrastructure has been subject of an exhaustive security analysis and proved resilient against counterfeiting attempts, stakeholder repudiations, and misleading information.

Keywords: supply chain; Industry 4.0; blockchain; Hardware Security Module (HSM); Near-Field Communication (NFC); information tracking

check for updates

Citation: Gómez-Marín, E.; Senni, V.; Parrilla, L.; Tejero López, J.L.; Castillo, E.; Martintoni, D. An Innovative Strategy Based on Secure Element for Cyber–Physical Authentication in Safety-Critical Manufacturing Supply Chain. *Appl. Sci.* **2023**, *13*, 10477. https://doi.org/10.3390/app131810477

Academic Editor: Gianluca Lax

Received: 1 August 2023
Revised: 5 September 2023
Accepted: 13 September 2023
Published: 19 September 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In the era of Industry 4.0, a modern and efficient supply chain is key for all company success [1]. A close integration of stakeholders, processes, and resources enables interconnected, automated, and correct decision making, which is vital to maximizing efficiency and boosting overall productivity [2]. With this objective in mind, Supply Chain Management (SCM) integrates the multiple organizational entities and coordinates material, information, and financial flows across the supply chain [3].

However, supply chains are inherently complex, spanning multiple organizations and different physical locations and systems, thereby presenting significant challenges in terms of transparency, traceability, and trust. According to the Organization for Economic Cooperation and Development (OECD), it is estimated that, in 2019, there were USD 19 billion worth of counterfeits in the EU alone, 5.8% of their total imports [4]. Thus, modernizing SCM toward Industry 4.0 is an important and complex research field [5–7].

To approach this challenge, numerous studies strongly advocate avoiding centralized solutions and promoting the use of blockchain in order to provide a trusted and transparent recording of transactions and events of the collaboration between multiple

stakeholders [8–10]. Blockchain, a distributed and immutable ledger, offers a decentralized and transparent platform to record and verify transactions. It eliminates the need for a trusted central authority, enhances data security, and enables real-time access to a shared ledger, fostering trust and collaboration among supply chain participants.

However, its effectiveness is limited when it comes to bridging the gap between the digital realm and the physical world, i.e., consistently reflecting events in the real world [11]. To address this challenge, a trusted entity, known as an "oracle", is required to record data in the real world and to store them into the blockchain system [12]. Nonetheless, ensuring the reliability and accuracy of real-world data coming from oracles to maintain the trust of recorded information in blockchain poses a formidable challenge, commonly referred to as the "oracle problem" [12]. Historically, in a supply chain context, the provenance of physical assets does not have guarantees, thereby limiting the blockhain-based SCM tracking capabilities. Here, the Internet of Things (IoT) emerges as a prominent solution due to its ability to provide real-time information from diverse sources [13].

Multiple works suggest the use of RFID tags as IoT devices to identify the product and combine it with blockchain to store the legitimate data of the product's provenance. However, due to the technology limitation of RFID tag, almost all these solutions require a centralized infrastructure for a secure implementation [14], which makes them unsuitable for integration with a blockchain-based SCM. On the other hand, those few solutions that are decentralized are extremely complicated to implement securely [15,16], or they do not consider the security of the IoT devices interacting with the supply chain physical flow [17]. The reliability of the data recorded in the SCM is extremely relevant in supply chains where the value of an asset is closely related to their origin (e.g., medical drugs, luxury products, safety-critical parts). In this context, there would be high economic rewards in tampering with these data source IoTs to insert malicious track information and therefore to enter counterfeits in the supply chain.

In order to solve these challenges, our scheme does not need a third trusted party or a centralized infrastructure, while making the tags unclonable. To achieve this, our work proposes incorporating NFC [18] tags in the assets tracked by the supply chain and using high-performance asymmetric cryptography, an Elliptic Curve Digital Signature Algorithm (EDCSA) [19]. In this way, there is no need to access sensitive information to identify the tags, ensuring the non-duplicable identity. Additionally, we propose a cryptographically secure mechanism to make blockchain witness each transfer of the asset's ownership to ensure the reliable provenance and path of the product. With this solution, all stakeholders can easily check the unique identity of any asset and securely rely on the information about its origin and each of its owners during its entire life cycle. Finally, thanks to the secure implementation, the proposed system enforces strict data access control to address one of the biggest technological challenges of the blockchain-based supply chain: the privacy [20].

The rest of the paper is structured as follows: Section 2 highlights the motivations driving this research; Section 3 provides an overview of related works and solutions; Section 4 reports the main concepts used for the formulation of the solution; Section 5 presents the approach designed by this research. In Section 6, a specific prototype of the solution is presented, which is finally used in Section 7 to evaluate the overall approach from a security point of view. Section 8 concludes the research and analyzes the future steps.

2. Motivation and Scenario

The state of the art on supply chain advancements are studied across a wide range of products, industries, and markets, such as health products or food tracking. In order to highlight the issues considered in this research, we will focus on a specific and critical scenario in the context of the aerospace industry. In avionic manufacturing, the airplanes' basic components (i.e., actuation, propulsion, navigation, air-quality, etc.) might be manufactured by multiple different companies in a tiered approach [21], which ultimately converges to create a singular, sophisticated product: an airplane. In this scenario, not only does the plane have to pass through several validations and certification processes, but also,

individually, each of the plane's parts is subject to specific regulations with their correlated verification. Passing through the certification process and proving adherence to the quality standards is complex and time-consuming. And still, risks brought by the supply chain are a source of problems more extensive than the design and equipment risks in the aerospace stand-alone devices [22]. For this reason, aerospace assemblers are interested in getting closer and raising the control over the second-tier suppliers to reach better coordination and increase competitivity [23]. In this context, the proposed approach aims to reduce risks and potential errors, mitigate costs, and increase the trust that due diligence is properly executed at all supply chain stages.

Taking into consideration this context and motivation, in the following, we explain the reference use case of the current work. An authorized entity, e.g., a supply chain manager from an airplane assembler, when receiving a part (e.g., an instrument panel), identifies the part and obtains from a database the information regarding the manufacturer, the certificates, and the historical owners of this part. Then, this information can be used to validate whether the asset can be mounted on a plane. Finally, the manufacturer proves adherence to the quality standards in each of the components to a third-party reviewer, like a governmental administrator. Using the STRIDE methodology [24] and the analysts of Hendrik S.B. and Evi H. [25], we identify the seven threats types of the use case in Table 1. These threats are particularly challenging in this scenario due to the nature of the supply chain, where any stakeholder is also considered a possible attacker if it can obtain an economic benefit in some way. For example, an airplane assembler performs a tamper attack to delete part of the life cycle of an asset to insert a cannibalized asset, saving money and still "proving" adherence to the quality standards, or a distributor may make a spoofing attack to duplicate the identity of an asset and insert a counterfeit in the supply chain.

Table 1. High-level threats related to the cyber–physical link.

Threat Type	Identified Threat
Spoofing [24]	An attacker falsifies the identity of an asset. It can be used to insert a counterfeit part in the supply chain linking it to an existing SCM record, or to send illegitimate data or modify data records, respectively.
Tampering [24]	Data records are intentionally inaccurate. An attacker sends false information about the ownership of the asset or its certificates, or because the data records at rest are modified.
Repudiation [24]	An attacker disputes a recorded data's authorship or a legitimate data modifications' authorship.
Information disclosure [24]	An external entity accesses data traffic or data records.
Denial of Service [24]	An attacker makes the SCM inoperable temporally or permanently.
Elevation of Privileges [24]	A stakeholder uses its privileges to access/modify data that this stakeholder should not be allowed or should be allowed only when it physically owns the asset.
System misuse [25]	Several stakeholders collaborate to ignore the verification of the assets in order to include counterfeits, or the validation of the asset is not performed systematically due to lack of concern of the organizations or the employers.

The threat analysis highlights that the link between physical parts and their cyber representation is a potential attack point that can lead to different threats to the supply chain. This emphasizes the necessity of a secure approach for parts hyperlinking and data storage. To mitigate the risks identified in a safety-critical industrial supply chain, the solution should be formulated in a way that does not rely exclusively on the trustworthiness of a single supply partner or an external party. Furthermore, the procedure should be designed as an easy-to-operate technology.

3. Related Work

Various techniques have been proposed to enhance the tracking and tracing capabilities of parts inside the supply chain. In the food industry, the introduction of IoT technologies is exploited to enhance food safety and traceability: QR code technology is proposed in ref. [26] to trace the logistic steps of vegetables; RFID anchors are instead proposed to enhance the traceability of the fish supply chain in ref. [27]. An RFID-enabled supply chain is also explored in ref. [28], where a theoretical model is proposed and evaluated on an aerospace manufacturing process. Those technologies provide promising results regarding the tracking and traceability requirements of physical parts but have a common weakness regarding the authenticity of the hyperlink: both technologies suffer from a clone vulnerability that makes the introduction of counterfeit parts in the supply chain possible.

RFID tags support hash operations, symmetric encryption, or Physically Unclonable Functions (PUFs) [29]. This is the case of the secure protocol Cipurse [30], which uses symmetric cryptography (often Advanced Encryption Standard, AES [31]) to authenticate a tag. Even if this protocol can be applied to NFC [32], it focuses on the secure use of symmetric cryptography inside the tag to keep the tag's secret protected from the majority of attacks. However, the authenticator needs complete or partial knowledge of this secret to perform the authentication, which gives the authenticator the possibility of creating falsifications. The secure management of this secret is a critical point of the symmetric cryptography, which is out of the scope of Cipurse.

There are many works in the state-of-the-art proposing solutions to this problem. In accordance with the survey in ref. [14], almost all the proposed solutions require relying on a centralized entity to identify the clones. This would allow this entity to record fake data about an authentication (tampering attack) or to clone a tag (spoofing attack). The only author in this survey that supports a decentralized solution is Elkhiyaoui [15]. This system uses read/write tags without hardware protection, i.e., everyone can read/write. Every tag contains the ID of the product and the cryptographically protected path of this ID. This solution cannot protect against cloning but proposes a method to detect it. In this method, all partners in the supply chain check between them that the same ID is not used in the two partners' stores. This solution is difficult to apply because it requires not only the cooperation of all the partners in the supply chain but also in the market, e.g., a counterfeit with a cloned ID could be sold to an assembler, and the partner would never detect it if they do not compare their database with the distributor from a different supply chain line that has the original product. Also, another problem is that even if the path in the tag cannot be modified, it can be restored to an old version. So, when a part is in a non-auditable state (i.e., in final user control or discontinued), the distributor can clone its ID and its old path information, include it in the tag of a counterfeit, and sell it like a new and legitimate part.

Apart from that, another more recent work from Saikat M. et al. [33] presents a solution with a self-made blockchain to protect product-related information. In this way, the asset's path information cannot be modified. When a stakeholder receives an asset, it reads from the tag the secret "RFID address" and uses it to identify in the blockchain the product-related information. This secret is also used to send valid transactions to the blockchain and includes more product-related information. The problem with the solution is that there are not any mechanisms used to avoid or detect clones of the RFID tags. Therefore, any stakeholder or an attacker who could scan the part can clone the tag and sell a counterfeit.

Michail S. et al. [17] proposes a mechanism where only authorized entities can identify the tags. Once it is identified, a new block is uploaded to the blockchain, the tag's identification is modified, and the hash of the new identification is uploaded to the blockchain. At the end, the final user can identify the tag using the blockchain and trace its origin and path back. However, anyone with access to the tag can extract the secret credentials and clone it, not only the only authorized entities, because the tag answer is only protected with a random bitwise rotation between 0 and 96.

Nevertheless, the problem of Michail S. et al. [17] is resolved in the solution presented by Srinivas J. et al., LBRAPS [16]. Their protocol achieved mutual authentication and also

the establishment of a session key between the tags (Ts) and the supply chain node (S). The work is quite novel because the tags themselves can authenticate S and the reader (R). Additionally, the solution is secure against diverse attacks like replay attacks. To achieve this, the tag stores its secret IDt, unique for each tag and the identifications of the reader and of the supply chain node, IDr and IDs, respectively. Also, the tag compares each received message's timestamp with the current time to avoid a replay attack. The solution is presented in the scenario of a single organization (department), a single reader, a single supply chain node, and a single tag. Finally, the authors claim that LBRAPS can also be applied in a distributed system, i.e., for various departments, similar to Michail S. et al.'s protocol [17] without giving further details. However, LBRAPS has key differences with Michail S. et al.'s protocol [17] that make it not applicable in the same way in distributed systems. LBRAPS requires the tags to know the IDs and IDr of all the S and R in the system, which is unfeasible and risky for a reduced memory tag. Also, in LBRAPS, the readers need to know the secret IDt of all tags that they are going to communicate with beforehand, which requires a delicate system to distribute these sensible data. These two facts make the solution of Srinivas J. [16] hardly applicable to distributed systems.

On the other side, standard QR codes provide virtually no protection against copying. Efforts have been made to enhance these structures with anti-cloning features such as adding digital watermarks in QR code [34] or including copy detection patterns [35], but all these techniques present an accuracy that varies highly based on printing and scanning calibration, which makes them hard to implement in a real-world scenario. Another possible solution to enhance the link between a physical object and its cyber representation is the usage of physical characteristics that can uniquely identify an item. For example, DustIdentity [36], which proposes a Diamond Unclonable Security Tag, is a coating made out of diamond nanocrystals that can be registered as a unique fingerprint and thus used as an item identifier. This type of solution provides strong identification guarantees but lacks embedded computational capabilities to enhance the supply chain security.

Our research presents a different technological approach to this problem, creating an easy-to-operate and easy-to-implement solution that avoids the need to trust stakeholders or external parties for authentication. In our approach, the tags use high-performance asymmetric cryptography ECDSA, which avoids the possibility of cloning the assets. Also, every ownership transference of the asset is not just recorded in the blockchain but also the blockchain itself verifies the package and the new owner before performing the digital change in ownership, which detects any misuse. This provides complete transparency and highly increases trust in blockchain information. Finally, we implement our solution in a real privacy-preserving blockchain that avoids stakeholders accessing information that is not relevant to them.

4. Background

In this section, some important terms already mentioned previously are going to be described in detail, with the intention of going deeper into the proposal of this work.

- **Blockchain:** blockchain is a peer-to-peer infrastructure proposed by Satosy Nakamoto in 2008 with the name Bitcoin [37]. The peers share a common database that can be extended by adding new blocks containing signed information to the chain, making it perfect for use as a ledger. Six years later, a new blockchain technology was released, called Ethereum [38]. This blockchain technology can be used not only to store bank balances but also to host scripts that can be executed and used to manage data in the system. These scripts are known as smart contracts. Blockchain possesses inherent characteristics that render it exceptionally suitable for certain security applications: All information uploaded—transactions—passes through a consensus mechanism before being accepted in the system; the information, once uploaded, cannot be removed or modified; and all new participants can verify the authenticity of all previously recorded data. This information is publicly available in public blockchains, where everyone can access the infrastructure. However, information confidentiality can be

guaranteed in permissioned blockchains where access to data is limited to authorized organizations. For example, HyperledgerFabric [39] is a framework for permissioned blockchain where data confidentiality can be protected through a certificate-based access control system.

- **Smart contract:** the smart contracts can be seen as stored procedures that regulate the operations on a blockchain system. All the transactions addressed to a smart contract must respect the rules embedded in the smart contract scripts. The compliance is validated through a consensus algorithm by the peers of the blockchain infrastructure, ensuring reliability, accountability, and availability [40]. These scripts are stored in the blockchain itself, guaranteeing code immutability. Mahd Miraz defines it like a trust machine [41]. All the functions processed are signed and stored in the blockchain, providing strong traceability.
- **Hardware Security Modules (HSMs):** HSMs are hardware-based solutions with security-by-design that can perform the essential cryptographic operations. These modules can perform the secure generation, secure storage, and secure operation of asymmetric cryptography (e.g., RSA, ECC). By design, there is no practical way to extract its secret crypto material; therefore, they can only be used to perform crypto-operations (e.g., digital signatures) by accessing its secure APIs.
- **Near-Field Communication (NFC):** NFC is a ISO standard [42] that defines a wireless communication technology working in the 13.56 MHz band. RFID and NFC are two different topics confused in the state of the art. Some papers consider NFC as a standard inside RFID [43] while others consider it as a completely independent standard [44,45]. Nevertheless, the clear advantages of NFC with respect to other wireless technologies is its robustness against eavesdropping due to its very short reading range [45] of up to 10 cm [44] and its popularity, which makes the majority of today's mobile phones support NFC.

5. Proposed Solution

This research exploits the capabilities of passive NFC devices with embedded HSMs that are commonly available in the market (e.g., smart cards). Further on, this class of devices will be identified as a Secure Element (SE). The SE is used to assign a robust digital identity to parts tracked in the SCM. The aim is to design the physical integration of an SE into the overall part, effectively transforming it into a "smart-part".

The SEs are protected with physical security measures that offer tamper protection and detection. For example, the SEs can be protected with a protective mesh and covered with security tape [46]. Moreover, being a secure hardware element designed, produced, and tested by a reliable company following the standard Common Criteria Evaluation Assurance Levels 5+ [47,48], the risk of software attacks or side-channel attacks is reduced significantly.

The SE contains, in a secure partition, a private key that can be used to perform asymmetric crypto operations such as a digital signature. All the operations are performed through secure-by-design APIs, always keeping the crypto material in a secure state.

Once a part is physically tagged with the hardware-based digital identity, the crypto functionalities of the SE can be used to interact with the blockchain-based SCM system. The smart-part can send valid transactions to the blockchain, signing them with its specific private key. The crypto information required for the signature cannot be extracted from the SE; this means that only someone with physical access to the part can trigger these blockchain functionalities, which proves package ownership.

5.1. Integration of SE in the SCM

To demonstrate the integration of the solution, a distributed-ledger infrastructure for supply chain management is properly deployed. The infrastructure used is taken from [49] and the details are out of the scope of this research. In this context, the focus is on a common SCM functionality that provides ownership tracking capabilities of a given part inside

the supply chain. From a high-level point of view, the SCM stores the current owner and exposes services to record ownership changes to follow the part inside the manufacturing process from the suppliers to the final customer. As baseline, an SE is provided with strong private keys, the manufacturing certificates, and a certificate showing part validity (which can be used as oracle certificates [50]).

The SCM is coordinated by a smart contract, which is validated by all the stakeholders and stored in a permissioned blockchain.

Figure 1 presents a funtionality scheme of the interactions between the stakeholders, the SE, and our blockchain SCM system. Notice that the yellow diamonds shall be successful before passing to the next steps, delivering robust tracking capabilities and consistent information. Firstly, the supplier receives and accepts an order for a specific part. Then, the part manufacturing and shipping starts:

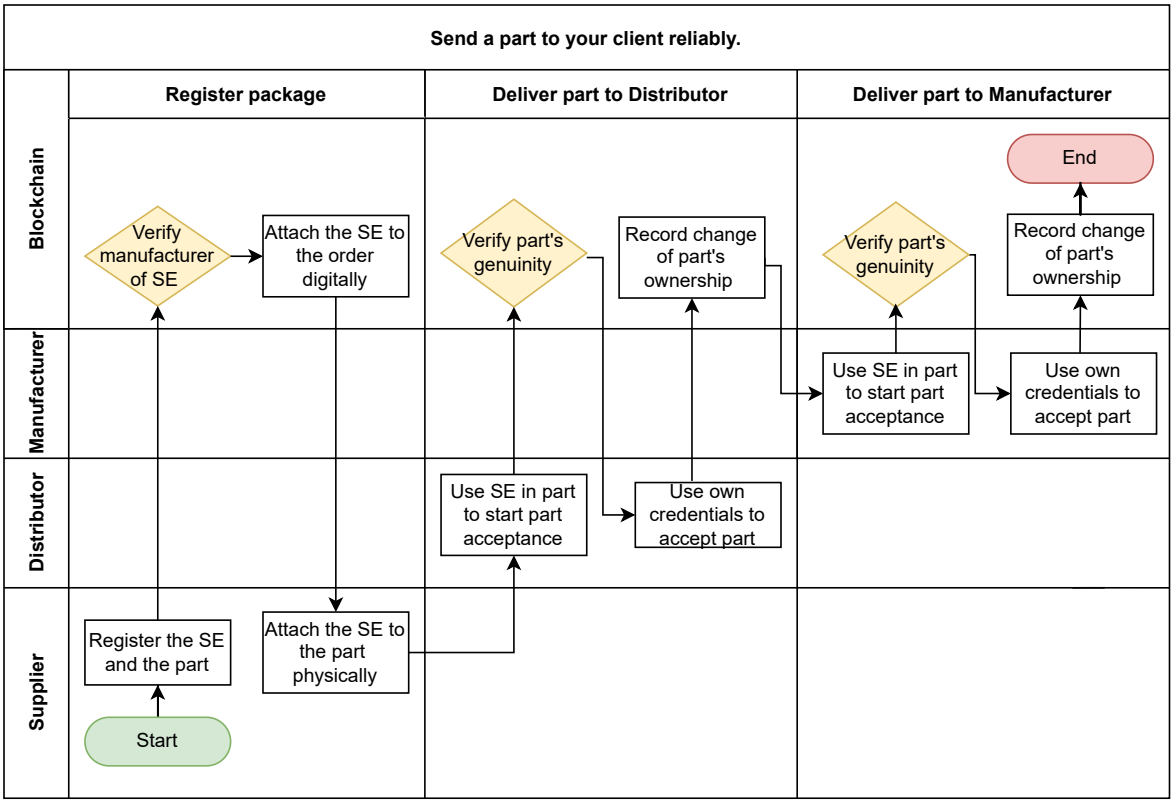

Figure 1. Overview of the proposed interactions.

(A) A supplier physically packages the part to be shipped and prepares it to be traced in the SCM by performing the following:

- The SE is enrolled to the blockchain, registering its identity, the SE's manufacturer certificates, and the physical part that it is linked to.
- The smart contract verifies the certificates to assert the SE trustworthiness.
- After verifying the certificates, the SCM approves the use of this SE as a part tag, stores its public key, and attaches it to the order.
- The SE is finally attached physically to the part, and the tampering security controls are deployed.

(B) The supplier physically and digitally delivers the part to the next actor in the supply chain, the distributor. The digital change in ownership requires the use of two random numbers ("Challenge" and "Challenge-proposed"), as explained in detail in Section 5.2, to avoid prediction attacks and delay attacks defined in Section 7.2.

- The distributor uses the SE attached to the received part to sign a transaction for the blockchain.

- The blockchain verifies that the SE used to sign the transaction is authentic and, consequently, the delivery part.
- The distributor uses their own credentials to send a transaction to the blockchain accepting the part.
- Finally, the smart contract accepts and records the new part owner.

(C) The change in ownership is repeated successively between the supply chain partners until the smart part reaches the final customer.

The scheme shows that only when the distributed ledger verifies the part can it be accepted, and the change in ownership can be recorded permanently in the blockchain. With this system, all the important steps of the product life cycle are verified by consensus and then recorded. This guarantees a correct verification and of the recorded data and that it has not been tampered with. Thus, this approach enables any stakeholder, like the final customer or any other authorized third party, with read access to the smart contract to accurately monitor in real-time the status and the history of a part in the supply chain.

5.2. Change Ownership Detailed

The smart-= part has its identity properly enrolled in the blockchain, so its SE can be used to validate transactions in the system issued by anyone with NFC access to the part. For this reason, the physical owner has to confirm all the transactions performed by the smart part with their own identity. The ownership change of a smart part is the following: the receiving organization employs the SE to propose the ownership change that must be confirmed through a second transaction in the SCM. Therefore, an ownership change is considered valid if (1) it is signed with the part secret key, providing proof of the physical presence of the specific part, and (2) it is confirmed by the receiving organization, providing non-repudiation guarantees on the future owner of the part.

Here follows a detailed explanation of the two-step transaction, which is illustrated in Figure 2. Each part has the following security variables associated:

- Owner: represents the organization in the supply chain currently holding the part.
- Owner-proposed: represents the partner that has to confirm with a second transaction to become the new owner of the part.
- Challenge: random number.
- Challenge-proposed: next random challenge number.

These variables are required to ensure a secure ownership exchange of the part between authorized SCM organizations, avoiding prediction attacks and delay attacks defined in Section 7.2. When a new actor wants to acquire ownership of a part in the supply chain, they proceed by proposing an ownership change as follows (orange arrows in Figure 2):

1. The new owner generates a new secret random number (Secret) to be used as "Challenge-proposed".
2. The actor prepares a non-signed transaction (raw transaction), proposing a change in ownership, ProposedOwnershipChange. The raw transaction contains the part ID, the future owner, the current challenge "Challenge", and the secret random number as the proposed challenge.
3. The raw transaction is sent to the part through NFC and is signed by the SE, which requires physical access to the smart part.
4. The signed transaction is published on the blockchain. The signature confirms that this action was prompted by the current owner of the part. Another consequence of this is that the proposed challenge is publicly disclosed and is not secret any more.
5. The blockchain system validates the transaction by checking (i) that the current challenge number corresponds to the last challenge stored in the SCM for that specific part, "Challenge", and (ii) that the part signature is authentic.
6. Once the transaction is validated, the security variables "Owner-proposed" and "Challenge-proposed" are updated.

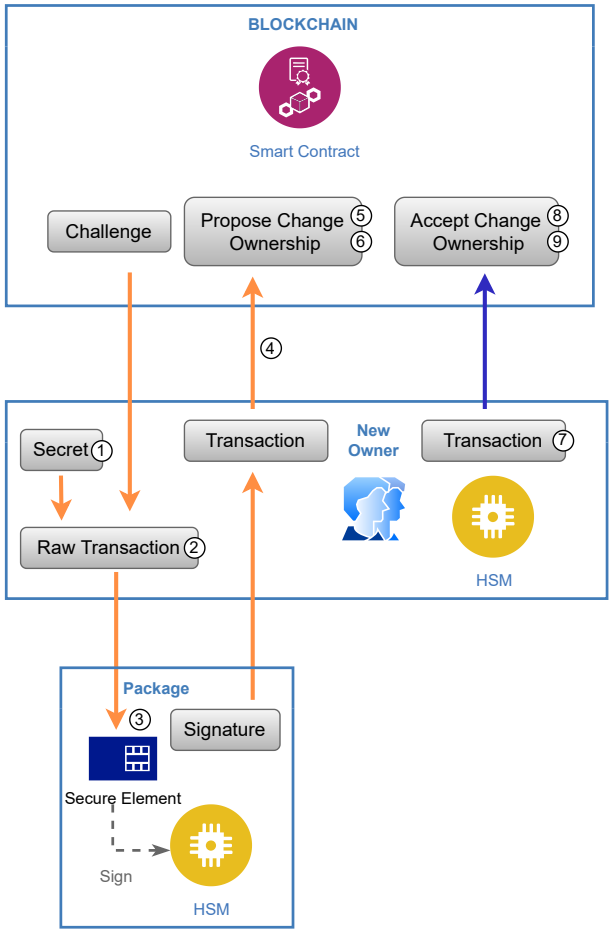

Figure 2. Two-step transaction infrastructure used to change the ownership of a package in the smart contract in the blockchain. The numbers in the figure refer to the enumerated steps in the text.

At this point, any supply chain partner with access to the part could have submitted this transaction. Therefore, the changes produced in the system so far are not binding and must be validated by the receiving organization to have guarantees of robustness and non-repudiation in ownership change. Consequently, the next actor in the supply chain, which is indicated as "owner-proposed" in the security variables, accepts the ownership change with the following steps (blue arrow in Figure 2):

7. The new owner creates a blockchain transaction, AcceptOwnershipChange, attaching the part ID and newly published value currently labeled as "Challenge-proposed".
8. The blockchain verifies (i) that the triggerer is a member of the organization currently stored as "Owner-proposed" and (ii) that the "Challenge" value in the transaction corresponds to what is stored as "Challenge-proposed".
9. Once the transaction is accepted, the security variables are updated to store the proposed values as Owner and Challenge.

The steps presented to propose and accept an ownership are repeated every time the part is sent/received by a partner in the supply chain. With this chain of events, the system can guarantee proper traceability of the part and non-repudiation of the physical ownership by the supply partners.

6. Implementation

The proposed solution was implemented using the permission blockchain framework Hyperledger Fabric (HPL) [39]. Using this framework, we created a blockchain-based SCM system with enhanced access control providing strong confidentiality, data traceability, and non-repudiation guarantees.

In this implementation, we consider four stakeholders: supplier, distribution, manufacturer, and safety certification authority. These entities interact with the SCM using a smart contract with their validated credentials as defined in the permission blockchain HPL. Only using the validated credentials can the information in the blockchain be accessed, or can new information be uploaded, obtaining privacy with respect to the external users.

The smart contract implements the following functions:

- Orderpart: the manufacturer executes Orderpart by sending a transaction to the blockchain. It creates the data structures Contract, Objective&Compliance, and PriceAgreement, which contain the information about the requested order, e.g., qualification data or price.
- AcceptContract: the supplier accepts the order executing AcceptContract, including in the function the Contract identifier.
- SendPart: the supplier executes SendPart to register the SE's public key and link it with the ordered part.
- AcceptDeliveryContract: a distributor with access to the blockchain can accept delivering this order by executing the function AcceptDeliveryContract and providing the Contract identifier.
- ProposedOwnershipChange and AcceptOwnershipChange: these functions are triggered in order to execute a secure ownership change. Their functionality is detailed in Section 5.2.

To avoid the elevation of privileges to modify smart contract data, assertions are placed in each smart contract function to confirm that the triggering user is authenticated with the validated credentials and is part of an organization authorized to execute that specific action. For example, in our scenario, only the manufacturer is allowed to execute Orderpart to order a part from the supplier. If any other organization attempts to trigger the function Orderpart, the validation process of the peers will detect an assertion failure and reject it.

Even if actions identified by the smart contracts are strongly regulated, HLF exposes a query engine, which allows any participant in the blockchain to read the state of the ledger. This action is always permitted and is not regulated by the smart contract. Therefore, in order to enforce the least knowledge principle and to maintain data confidentiality, HLF proposes the Private Data Collections (PDCs) functionality to regulate data read access. Firstly, we identify three data structures with different access rights as shown in Table 2. Then, as shown in Figure 3, the Contract structure is stored directly in the blockchain, and therefore the four stakeholders can read it. Instead, Objective&Compliance and PriceAgreement structures are shared using Private Data Collections (PDCs), which send data peer-to-peer via gossip protocol to only the partner(s) authorized to access it. This information is stored in a private database on the peers of the authorized organizations, and it can be read only through smart contract functions. A hash value of each PDC entry is written on the ledger state as proof of existence and can be inspected by every participant on the blockchain. The hash serves as evidence of the transaction, is used for state validation, and can be used for audit purposes [51]. Notice in Figure 3 that one data structure is openly accessed by every participant in the system (yellow line) while the other data containers have restricted access (orange line).

Finally, to avoid a spoofing attack on the part's identity, it is important to link it to the public key on the SE immovably. In public blockchains, e.g., Bitcoin or Ethereum, the identity of a transaction sender is cryptographically generated by its public key; therefore, each identity is linked with a unique private key, and it is immovable. However, in Hyperledger Fabric, the identity is linked with the public key through a certificate, and, in the case of the part, it is issued by the supplier. Then, the supplier could also issue a second certificate for a part's identity with another SE, which would allow for a package clonation. To avoid this threat, when a part is registered in the SCM, the SE's public key is also stored in the smart contract. Then, in every change in ownership, the identification mechanism of Hyperledger

Fabric has to be modified to assert that the public key of the SE is the same as the stored public key as shown in Figure 4.

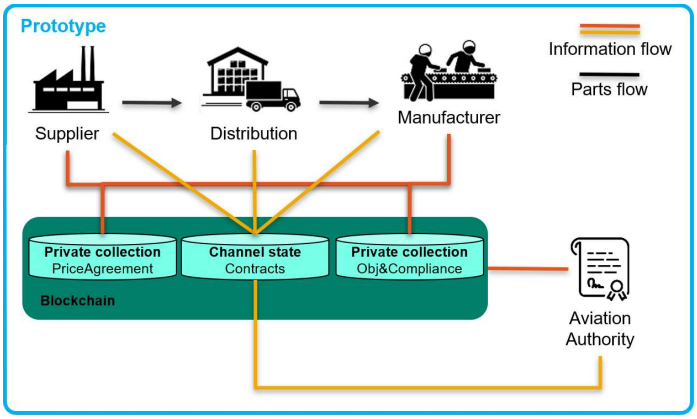

Figure 3. Secure architecture of a modern blockchain-based SCM applied to manufacturing use case.

Table 2. Data assets and protection policies.

Structure	Description	Access Rights
Contracts	Agreement between the manufacturer and the supplier. It contains common data such as name and number of the components, expected delivery date, and all the logistic details	Supplier(R/W), Distribution(R/W), Manufacturer(R/W), Aviation Authority(R)
Obj&Comp.	Each component is linked to objectives or requirements expressed by the manufacturer. The same data structure contains the compliance measurements that the supplier provides to prove adherence to the requirements. Requirements and quality measurements are considered sensitive data since they contain intellectual property and related information.	Supplier(R/W), Manufacturer(R/W), Aviation Authority(R)
PriceAgr.	Each contract has an economical agreement linked to it.	Supplier(R/W), Manufacturer(R/W)

With this solution, we have created a secure and fully functional smart contract that distinguishes between the privileges of users when accepting transactions and delivering information to the stakeholders. Using this same mechanism, other private collections can be created for other uses and more complex data access policies can be defined if necessary. At the same time, this mechanism maintains blockchain's reliability in the private collections since the hash of the private data is stored in the blockchain consortium.

```
publicKeyDer, _ := x509.MarshalPKIXPublicKey(certificate.PublicKey) //Get public key from smart card certificate
publicKeyDerHex := hex.EncodeToString(publicKeyDer)
publicKeyUncompressedFormat := publicKeyDerHex[52:len(publicKeyDerHex)]
fmt.Println("Public key from transaction signature requestor: %s", publicKeyUncompressedFormat)
if (delivery.PackagePublicKey != publicKeyUncompressedFormat){
        return fmt.Errorf("Package is not original (public key not matching)")
}
```

Figure 4. New lines used to identify the parts using their public key instead of their IDs.

To test and validate the capabilities offered by this approach, we used an actual HSM with NFC, and NFC readers, which interact with the smart contract deployed in a privacy-preserving blockchain. To facilitate this process, each participating organization deployed an NFC reader comprising an ACR122U NFC Reader and a Raspberry Pi

4B, as illustrated in the setup in Figure 5. To execute the test, we used a configurable smart-card, Secora^{TM} ID S V1.1 [48], attached to the parts. This smart card possessed the necessary secure functionalities required for our proposed solutions, bringing us closer to market implementation.

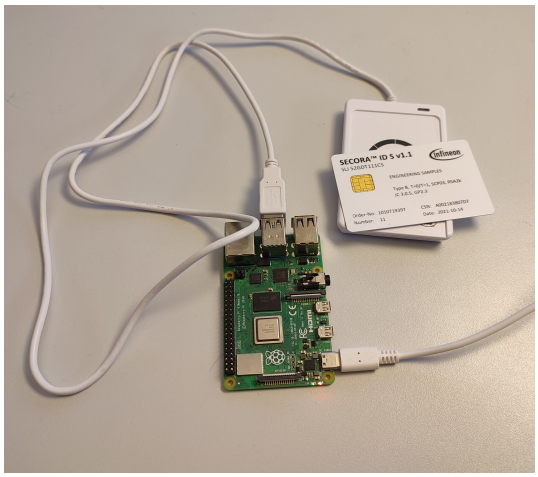

Figure 5. Prototype setup for laboratory evaluation.

Performance Evaluation

The prototype implementation was tested to measure the performances of the SE operations in the proposed architecture. A specific NodeJS [52] client was created to interact with the SE. This client generates the unsigned transaction, hashes it, and sends it to the smart card to be signed. Then, a blockchain verifies the transactions, confirming physical ownership of the part. Due to the internal functionality of Hyperledger Fabric, when sending a transaction, a second signature is needed. The execution of both actions has been tested and measured from a performance point of view on 20 iterations. Table 3 presents the measurements showing the time required for each operation and the overall transaction submission time. Notice that the worst case scenario overhead introduced by adding the two crypto-operations performed by the SE into the Hyperledger client transaction is less than 0.6 seconds (accounting of 17.1% of the total procedure time).

The security/performance trade-offs introduced by this architecture are considered acceptable for this use case, where security is a big concern and there is no real-time requirement, considering the use case where humans are interacting and managing a physical part. Additionally, this process removes the necessity of the handwritten signatures in the supply chain, which saves time and enhance consistency. Finally, it is important to notice that not only do the two parties agree to the part transference, but all the authorized partners are remotely verifying the process and the part's genuineness.

Table 3. HSM performances while interrogated through NodeJS API.

Action	Avg. Time	Min. Time	Max. Time
HSM Sign 1	267.5 ms	264 ms	281 ms
HSM Sign 2	267.7 ms	263 ms	281 ms
Sum of Sign Actions	535.2 ms	527 ms	562 ms
Overall Transaction Time	3290.1 ms	3262 ms	3307 ms
HSM Overhead	535.2 ms	527 ms	562 ms
HSM Overhead (%)	16.3%	16.0%	17.1%

7. Security Analysis

This section explains firstly how our solution can securely mitigate the threats exposed in Section 2. Secondly, it proves the robustness of the system against the attacks found in the state of the art and some new ones self-developed.

7.1. Threat Analysis

The proposed solution has been qualitatively evaluated against the risks identified in Section 2. A summary of the mitigation introduced by the solution with respect to the threats is highlighted in Table 4.

Table 4. Threat analysis.

Threat Type	Mitigation
Spoofing	The use of an HSM to generate and store the private keys of the parts ensures the impossibility of credentials spoofing. Furthermore, identification in the smart contract requires a public key of the SE for the correct functionality. These two facts together ensure the impossibility of cloning the parts.
Tampering	As a result of the proposed scheme, the ownership of a package can only be modified by someone with physical access to the package. This ensures that no false ownership information about the part can be added to the ledger. Also, the data are stored in the blockchain, which prevents any malicious manipulation of the data once uploaded.
Repudiation	All data uploaded to the smart contract are signed, and the decentralized system identifies every contributor before accepting the data. Finally, the peers of the blockchain themselves verify the presence of the real and unique part in the change in ownership process. This means that the information cannot be disputed once it is accepted in the blockchain.
Information disclosure	The solution is implemented over a permissioned blockchain. This means that no entity outside the supply chain can access the data.
Denial of Service	The SCM is based on blockchain with a decentralized peer-to-peer infrastructure. This architecture provides resilience by the design of the system against DoS attacks.
Elevation of Privileges	The solution uses privacy-preserving blockchain, taking advantage of the private collections of Hyplerledger Fabric. With this solution, the stakeholders' part of the supply chain cannot freely access all the information, only those that are relevant to them. Also, the ownership change of the asset requires physical access to the part itself, and the information can never be deleted, which avoids any stakeholder using its privileges to insert fake data in the blockchain.
System misuse	In order to take digital ownership of the package, it is required to verify its authenticity. This operation forces the verification of the asset at every ownership change in the supply chain.

7.2. Attack Analysis

Given that the system mitigates the common threats identified, here is discussed the resilience provided by the proposed solution against the following known attacks.

7.2.1. Key Disclosure

Key Disclosure (KD) is an attack where an internal or outsider attacker can in some way extract the secret variables stored in the tag. The current protocol uses asymmetric cryptography, therefore, the private key is never exposed and always kept protected in the SE.

7.2.2. Replay Attack

In a replay attack, an internal or outsider attacker gathers a legitimate message of the system and replays it later to negatively affect the system. In Hyperledger Fabric, all transactions are protected from replay attacks by using a unique nonce [53]. This means that each transaction can be uploaded to the blockchain only once.

7.2.3. Man-in-the-Middle Attack

In a Man-In-The-Middle (MITM) attack, an outsider attacker intercepts the communications between two parties and relays and possibly alters the messages. Our protocol, unlike other protocols for supply chain tracking, uses NFC. This highly reduces the possibility of an MITM attack as the attacker should be in the 10 cm distance between the tag and the reader. Furthermore, a very unlikely successful MITM could modify the hash sent to the tag or the signature sent back by the SE. This attack would be detected in the part verification function.

7.2.4. Tracking Attack

An outsider attacker can track the part along the supply chain even if they do not belong to the organization based on the responses of the SE. In this proposed solution, the SE performs an ECDSA signature given an external hash. The ECDSA algorithm always gives back a different and unpredictable signature based on a random secret number K internally created by the signer and unique to each message. Therefore, even if an attacker with access to the SE always gives a constant hash to it, the attacker will always retrieve an unpredictable response and will be unable to track the SE.

7.2.5. Prediction Attack

In a prediction attack, an insider or outsider attacker completely or partially knows the future answers of the SE without a KD and, therefore, can create a temporal or a permanent clone of the SE. Most blockchain implementations use a predictable nonce in their transactions (e.g., Ethereum [54] and Hyperledger Fabric). This allows the prediction of the hash of the next transaction to be signed by the SE. With this information, an internal attacker can interrogate the SE to obtain the signature of the next transaction and create a fake part that returns the predicted signature of the next transaction. The next actor in the supply chain would read from the fake part the correct signature and consider it real. This attack is prevented in the proposed protocol by using a secret random number in the "Challenge-proposed" field, which is generated by the next actor, to make the transaction unpredictable and thus the hash be signed by the SE.

7.2.6. Delay Attack

An internal attacker can use the SE when it is in its possession to create messages that will be sent later to negatively affect the system without a KD. The attacker could sign, using the SE, a transaction proposing an ownership change, including themselves as the next owner, but they do not publish it on the blockchain. In the future, without physical access to the part, they send the signed transaction and then proceed to confirm its ownership. This attack is impossible to apply in the proposed protocol since the transaction that changes the ownership requires the "Challenge" variable, which is a random, unrepeatable, and unpredictable value. This value is updated from "Challenge-proposed" every time the part's owner changes, guaranteeing that ownership transactions are ordered and thus cannot be delayed.

7.3. Comparison

Table 5 compares the previously discussed solutions in the state of the art with the proposed protocol. In the table, X means that the protocol cannot provide protection against the attack or not support the property whereas ✓means the opposite. On the other hand, NA indicate that the attack or property is not applicable to the protocol. Notice that, in refs. [15,16,33], the internal partners require access to the keys inside the SE to identify it, and therefore are not resistant

to KD. That means that, at any later moment, they could insert a clone in the supply chain, and they would very rarely be identified as guilty. The protocol [17] fails the key protection by relying on simple bitwise rotation to guarantee key confidentiality. Therefore, none of them are protected against KD. Additionally, none of the analyzed work presents a solution to avoid the stakeholder taking advantage of their privileges and accessing information that is not relevant to them stored in the distributed system.

Table 5. Comparison of decentralized-based SCMs.

Security Protection to:	Elkhiyaoui et al. [15]	Saikat et al. [33]	ULRMAPC [17]	LBRAPS [16]	Own
Key disclosure	X	X	X	X	✓
Replay attack	X	X	✓	✓	✓
MITM attack	✓	X	✓	✓	✓
Tracking attack	✓	X	✓	✓	✓
Prediction attack	X	NA	✓	✓	✓
Delay attack	NA	NA	X	✓	✓
Elevation of privileges	NA	X	X	X	✓
Decentralized	✓	✓	✓	X	✓

8. Conclusions and Future Work

This paper presents a completely decentralized architecture for safety-critical industrial supply chain tracking based on a secure element and blockchain. The technology forces the honest behavior of the stakeholders and provides a strong guarantee of the quality of the product to final users or third-party observers. To achieve this, NFC tags with asymmetric cryptography capabilities are integrated in the parts manufactured and exchanged in the considered supply chain. With a tag, the part receives a digital identity inside the blockchain infrastructure and can trigger transactions. The blockchain-based supply chain manages all the parts' information and cryptographically certifies its owner at every moment. Using a novel scheme, the smart contract forces the stakeholders to honestly verify the parts along any asset transference, and the blockchain itself is witness of the transfer process. The solution is implemented over the Hyperledger Fabric framework, and it uses the "private collection" structures to protect the individual privacy of each stakeholder. As next steps, other functionalities are envisioned, such as the ability to provide the part's physical owner access to certain blockchain privileges or specific data. Additionally, following other tracking solutions, a global navigation satellite system sensor could be integrated in the tag to include information about the position signed by the HSM, though it would present challenges such as the need for an active tag with a power supply.

Author Contributions: Conceptualization, E.G.-M., D.M. and V.S.; methodology, E.G.-M.; software, E.G.-M., D.M. and J.L.T.L.; validation, E.G.-M., D.M. and V.S.; formal analysis, E.G.-M. and D.M.; investigation, E.G.-M., D.M. and J.L.T.L.; writing—original draft preparation, E.G.-M., D.M. and V.S.; writing—review and editing, E.G.-M., D.M., V.S., E.C., L.P. and J.L.T.L.; visualization, E.G.-M., D.M., V.S., E.C., L.P. and J.L.T.L.; project administration, E.G.-M.; supervision E.C. and L.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been founded by the European Union's Horizon 2020 Research and Innovation program under grant agreement No. 871518, a project named, A COmprehensive cyber-intelligence framework for resilient coLLABorative manufacturing Systems, COLLABS [55].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Abdirad, M.; Krishnan, K. Industry 4.0 in logistics and supply chain management: A systematic literature review. *Eng. Manag. J.* **2021**, *33*, 187–201. [CrossRef]
2. Bag, S.; Telukdarie, A.; Pretorius, J.C.; Gupta, S. Industry 4.0 and supply chain sustainability: Framework and future research directions. *Benchmarking Int. J.* **2021**, *28*, 1410–1450. [CrossRef]
3. Stadtler, H. Supply chain management: An overview. In *Supply Chain Management and Advanced Planning: Concepts, Models, Software, and Case Studies;* Springer: Berlin/Heidelberg, Germany, 2014; pp. 3–28.
4. OECD/EUIPO. Global Trade in Fakes: A Worrying Threat; In OECD-iLibrary. 2021. Available online: https://www.oecd.org/publications/global-trade-in-fakes-74c81154-en.htm (accessed on 31 July 2023).
5. Tiwari, S. Supply chain integration and Industry 4.0: A systematic literature review. *Benchmarking Int. J.* **2021**, *28*, 990–1030. [CrossRef]
6. Queiroz, M.M.; Pereira, S.C.F.; Telles, R.; Machado, M.C. Industry 4.0 and digital supply chain capabilities: A framework for understanding digitalisation challenges and opportunities. *Benchmarking Int. J.* **2021**, *28*, 1761–1782. [CrossRef]
7. Fatorachian, H.; Kazemi, H. Impact of Industry 4.0 on supply chain performance. *Prod. Plan. Control* **2021**, *32*, 63–81. [CrossRef]
8. Sunny, J.; Undralla, N.; Pillai, V.M. Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Comput. Ind. Eng.* **2020**, *150*, 106895. [CrossRef]
9. Chang, S.E.; Chen, Y. When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access* **2020**, *8*, 62478–62494. [CrossRef]
10. Queiroz, M.M.; Telles, R.; Bonilla, S.H. Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain. Manag. Int. J.* **2019**, *25*, 241–254. [CrossRef]
11. Wüst, K.; Gervais, A. Do you need a blockchain? In Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.
12. Caldarelli, G. Understanding the blockchain oracle problem: A call for action. *Information* **2020**, *11*, 509. [CrossRef]
13. Aich, S.; Chakraborty, S.; Sain, M.; Lee, H.I.; Kim, H.C. A review on benefits of IoT integrated blockchain based supply chain management implementations across different sectors with case study. In Proceedings of the 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 17–20 February 2019; pp. 138–141.
14. Bu, K.; Weng, M.; Zheng, Y.; Xiao, B.; Liu, X. You Can Clone But You Cannot Hide: A Survey of Clone Prevention and Detection for RFID. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 1682–1700. [CrossRef]
15. Elkhiyaoui, K.; Blass, E.O.; Molva, R. CHECKER: On-site checking in RFID-based supply chains. In Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Tucson, AZ, USA, 16–18 April 2012; pp. 173–184.
16. Jangirala, S.; Das, A.K.; Vasilakos, A.V. Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. *IEEE Trans. Ind. Inform.* **2019**, *16*, 7081–7093. [CrossRef]
17. Sidorov, M.; Ong, M.T.; Sridharan, R.V.; Nakamura, J.; Ohmura, R.; Khor, J.H. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. *IEEE Access* **2019**, *7*, 7273–7285. [CrossRef]
18. Coskun, V.; Ozdenizci, B.; Ok, K. A survey on near field communication (NFC) technology. *Wirel. Pers. Commun.* **2013**, *71*, 2259–2294. [CrossRef]
19. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
20. Dutta, P.; Choi, T.M.; Somani, S.; Butala, R. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *142*, 102067. [CrossRef]
21. Meixell, M.J.; Gargeya, V.B. Global supply chain design: A literature review and critique. *Transp. Res. Part E Logist. Transp. Rev.* **2005**, *41*, 531–550. [CrossRef]
22. Hui, X.; Li, K.; Wang, C.; Zhang, C.; Gu, Z. Risk Management of Aerospace Stand-Alone Device Supply Chain. In Proceedings of the International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC), Beijing, China, 23–25 September 2022; pp. 272–277. [CrossRef]
23. Lanotte, H.; Ferreira, A.; Brisset, P. Lean supply chain and designing a customer-oriented dashboard: The case of an aerospace company. In Proceedings of the IEEE 13th International Colloquium of Logistics and Supply Chain Management (LOGISTIQUA), Fez, Morocco, 2–4 December 2020; pp. 1–7. [CrossRef]
24. Howard, M.; Lipner, S. *The Security Development Lifecycle*; Microsoft Press: Redmond, WA, USA, 2006; Volume 8.
25. Birkel, H.S.; Hartmann, E. Impact of IoT challenges and risks for SCM. *Supply Chain. Manag. Int. J.* **2019**, *24*, 39–61. [CrossRef]
26. Gao, H. Study on the Application of the QRcode Technology in the Farm Product Supply Chain Traceability System. *Appl. Mech. Mater.* **2013**, *321–324*, 3056–3060. [CrossRef]
27. Hsu, Y.C.; Chen, A.P.; Wang, C.H. A RFID-enabled traceability system for the supply chain of live fish. In Proceedings of the IEEE International Conference on Automation and Logistics, Qingdao, China, 1–3 September 2008; pp. 81–86. [CrossRef]
28. Harun, K.; Cheng, K.; Wibbelmann, M. RFID-enabled aerospace manufacturing: Theoretical models, simulation and implementation issues. In Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, Singapore, 8–11 December 2008; pp. 1824–1829. [CrossRef]
29. Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Silicon physical random functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp. 148–160.

30. OSTP Alliance™ Cipurse™ v2 Cryptographic Protocol Revision 2.0. Available online: https://www.cardlogix.com/downloads/support/CIPURSE_V2_Revision_2_0_Document_Overview.pdf (accessed on 31 July 2023).
31. Dworkin, M.; Barker, E.; Nechvatal, J.; Foti, J.; Bassham, L.; Roback, E.; Dray, J. Advanced Encryption Standard (AES). 2001. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (accessed on 31 July 2023).
32. Madlmayr, G.; Langer, J.; Kantner, C.; Scharinger, J. NFC Devices: Security and Privacy. In Proceedings of the 3rd International Conference on Availability, Reliability and Security, Washington, DC, USA, 4–7 March 2008; pp. 642–647. [CrossRef]
33. Mondal, S.; Wijewardena, K.P.; Karuppuswami, S.; Kriti, N.; Kumar, D.; Chahal, P. Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. *IEEE Internet Things J.* **2019**, *6*, 5803–5813. [CrossRef]
34. Biro, A.; Kristo, G.; Remenyi, P. Security Element and Method to Inspect Authenticity of a Print. European Patent EP2815567B1, 14 March 2017.
35. Picard, J.; Landry, P.; Bolay, M. Counterfeit Detection with QR Codes. In Proceedings of the 21st ACM Symposium on Document Engineering, Limerick, Ireland, 24–27 August 2021.
36. Dust Identity. Available online: https://dustidentity.com/products (accessed on 25 July 2022).
37. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 31 July 2023).
38. Ethereum, W. Ethereum Whitepaper. Ethereum. 2014. Available online: https://ethereum.org (accessed on 7 July 2020).
39. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the 13th EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
40. Gupta, R.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717. [CrossRef]
41. Miraz, M.H. Blockchain of things (BCoT): The fusion of blockchain and IoT technologies. In *Advanced Applications of Blockchain Technology*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 141–159.
42. *ISO/IEC 18092:2013*; ISO/IEC JTC 1/SC 6 Telecommunications and Information Exchange between Systems. ISO: Geneve, Switzerland, 2013.
43. Juels, A. RFID security and privacy: A research survey. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 381–394. [CrossRef]
44. Vazquez-Briseno, M.; Hirata, F.I.; Sanchez-Lopez, J.; Jimenez-Garcia, E.; Navarro-Cota, C.; Nieto-Hipolito, J.I. Using RFID/NFC and QR-code in mobile phones to link the physical and the digital world. *Interact. Multimed.* **2012**, *12*, 219–242.
45. Lahtela, A.; Hassinen, M.; Jylha, V. RFID and NFC in healthcare: Safety of hospitals medication care. In Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare, Tampere, Finland, 30 January–1 February 2008; pp. 241–244. [CrossRef]
46. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2020; Chapter 16.
47. *ISO/IEC 15408-5:2022*; Information Security, Cybersecurity and Privacy Protection—Evaluation Criteria for IT Security—Part 5: Pre-Defined Packages of Security Requirements. ISO: Geneve, Switzerland, 2022.
48. Technologies, I. SECORA™ ID Security Solutions. Available online: https://www.infineon.com/cms/en/product/security-smart-card-solutions/secora-security-solutions/secora-id-security-solutions/ (accessed on 18 August 2022).
49. Martintoni, D.; Senni, V.; Gomez Marin, E.; Cabrera Gutierrez, A.J. Sensitive information protection in blockchain-based supply-chain management for aerospace. In Proceedings of the IEEE International Conference on Omni-Layer Intelligent Systems (COINS), Barcelona, Spain, 1–3 August 2022; pp. 1–8.
50. Miličević, K.; Omrčen, L.; Kohler, M.; Lukić, I. Trust model concept for IoT blockchain applications as part of the digital transformation of metrology. *Sensors* **2022**, *22*, 4708. [CrossRef] [PubMed]
51. Foundation, L. HLF Private Collection. 2022. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html (accessed on 29 June 2023).
52. Node.js®. Available online: https://nodejs.org/en/ (accessed on 11 August 2022).
53. Foundation, H. Hyperledger Protocol Specification. Available online: https://hlf.readthedocs.io/en/v0.6/protocol-spec.html (accessed on 31 July 2023).
54. Foundation, E. Transactions. Available online: https://ethereum.org/en/developers/docs/transactions/ (accessed on 31 July 2023).
55. COLLABS-871518 Project Website. Available online: https://www.collabs-project.eu/ (accessed on 31 July 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.