Operations Management Research (2023) 16:1359–1381
https://doi.org/10.1007/s12063-023-00359-y

Supply chain traceability using blockchain

Pedro Azevedo[1] · **Jorge Gomes**[2] · **Mário Romão**[3]

Received: 23 October 2021 / Revised: 20 January 2023 / Accepted: 28 February 2023 / Published online: 1 April 2023

Abstract
In the current global marketplace supply chains can span a huge number of countries, cross many borders and require interoperation of a multitude of organizations. This vastness of supply chains impacts business competitiveness since it adds complexity and can difficult securing traceability, chain of custody and transparency. We propose that assuring chain of custody and traceability via Blockchain (BC) allows organizations to demonstrate product provenance, integrity and compliance. This work proposes that to effect true traceability the more complete approach is to connect both the Supply Chain Actors (SCAs) and products identifications using digital certificates. A Blockchain is used to manage the traceability of products and validation of the identities. Importing, verifying and storing the certificates uses an off-chain data storage solution for products certificates, IDs and data (i.e., WalliD) . To create, validate the certificates and setup the chain of trust a Public Key Infrastructure (PKI) was designed as part of the proposal. Our study follows a Design Science research approach aimed to analyse the requirements and propose a solution to a more complete traceability in supply chains. The results were architectural artifacts, including an Ethereum Smart Contract and a PKI based certificate authentication system. The implementation of these deliverables allow for a supply chain system that can provide decentralized and trustful assurance of the provenance, chain of custody and traceability functionalities for all the Organizations and also for the final consumers.
To exemplify the problem and demonstrate the applicability of the solution, its potential and benefits we applied it to a real food supply chain use case that already uses provenance certificates and stored them in the blockchain using the before mentioned SmartContract to assure and demonstrate the chain of custody and traceability of the food produce.

Keywords Chain of Custody · Provenance · Traceability · Supply chain · Supply chain management · Blockchain · Ethereum · Smart contract

1 Introduction

Blockchain (BC) is a recent technology that was first introduced with the Bitcoin cryptocurrency (Houben and Snyers 2018). However, BC technological capabilities are not only applicable to cryptocurrency and so it has been proposed to be used in other applications. According to Guo and Yu (2022) BC proposes to add several features to any application, namely: decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency. Blockchain is proposed to be a viable method of tracking assets while guaranteeing security and data integrity (Meidute-Kavaliauskiene et al. 2021). The benefits of blockchain-based tracing include the security of information sharing, real-time collection of product data, transparency, and visibility in the supply chain, as well as quality control throughout the entire lifecycle (Agrawal et al. 2021). According to several authors most of these features seem to make a perfect fit to supply chains since they support the key basic objectives: quality, speed, dependability, cost and flexibility (Casey and Wong 2017; Dinh et al. 2017; Kaur and Parashar 2022).

✉ Jorge Gomes
jorge.gomes@ulusofona.pt

Pedro Azevedo
prgazevedo@gmail.com

Mário Romão
mario.romao@iseg.ulisboa.pt

[1] TB.LX, Lisboa, Portugal

[2] Universidade Lusófona, Lisboa, Portugal

[3] Instituto Superior de Economia e Gestão, Universidade de Lisboa, Lisboa, Portugal

1.1 Problem relevance

For supply chain a recent duo of aspects: traceability and provenance have gained more importance. The focus on these aspects aims to allow the industries and customers dependent on supply chain to become assured of the products and processes sustainability (Kshetri 2018; Pal and Kant 2019). While it is common nowadays for logistics operators to accurately track packages at the transportation stages, that type of granularity is either lost or many times not possible at all stages of the supply chains since they have become much more international, complex and interorganizational spanning (Kim and Laskowski 2018).

From literature it is clear that the loss of traceability and provenance information the main factor that affects existing sustainability and compliance certification efforts making it crucial and the focus of research in the context of supply chains (Garcia-Torres et al. 2019). The traceability aspect additionally will also permit the optimization of supply chains which has always been one of the most preeminent topics for businesses as it highly influences a firm's success (Kros et al. 2019). This traceability optimization aspect of the supply chain is then the main driving reason that has led some companies to make trials for Supply Chains using BC for traceability (Berg and Myllymaa 2021; Wang et al. 2019). Examples are; Maersk – tracking global shipping, Alibaba – reduce food fraud, Lockheed Martin – improve cybersecurity, Everledger – implement diamonds and wine certificates, Walmart – monitor pork produce in China, Modum – safe drug delivery, Intel – track seafood supply chain, Bext360 – bring transparency into the coffee bean supply chain (Kshetri 2018).

1.2 Summary of the solution

This article proposes that to effect true and complete traceability the solution is to connect both the Supply Chain Actors (SCAs) and products identifications and provenance certificates. With the proposed approach the chosen BC and the designed Smart Contracts will be used to manage the traceability and validation of the identities while the storage, importing, exporting and verification of production and provenance certificates uses another existing architecture solution off-chain: WalliD[1] (Tavares et al. 2018). To create, validate the certificates and setup the chain of trust, an appropriate PKI (Public Key Infrastructure) with the corresponding CAs (Certificate Authorities) was designed as part of the proposal. To instantiate the problem and apply the solution a real food supply chain example was chosen. The chosen example uses the widely adopted and EU commission sponsored label and quality certificate system: Protected Designation of Origin (PDO). The main advantage of this proposed solution with an aggregated BC and Certificate architecture is that all SCAs (including producers, logistics operators, sellers and the end consumers/buyers) can use the system to view and self-verify the validity of both the traceability and the provenance claims.

In summary this work aims to provide a concrete answer to the supply chain traceability problem for the use case of supply chain certifiable actors, producers, products and consumers. The answer is a complete traceability system that provides both SCAs and the customers the highest level of traceability by assuring provenance, chain of custody and traceability verifiability and visibility to the SCAs and customers. The solution proposal consists of a set of artifacts (architecture diagrams and workflows, Ethereum SC and a PKI infrastructure) that followed the Design Science Research (DSR) methodology. Along the following points, we present a literature review covering various topics related to the scope of our study, like the chosen Blockchain and its impact on supply chains and their actors, the limitations and challenges of supply chains by using BC, the concepts of traceability, provenance, chain of custody, the supply chain agents and the requirements involved on their involvement. Then the research methodology based in the Design Science approach is introduced, and the proof-of-concept results are then analysed and discussed. The proof of concepts includes an architecture and a Use Case functionality for the Protected Designation of Origin for alimentary products (beef). Finally, the conclusions and future work are presented.

2 Literature review

2.1 Blockchain contributes to supply chain management

According to Weber et al (2016) Blockchain can be used as a technology that supports the collaborative process required by a Supply Chain and is proposed as an alternative to having a centralized trusted party. Since then the industry has been alerted to the potential benefits of the use of BC to SC and according to Chang et al. (2020) BC adoption in Supply Chain Management (SCM) is expected to boom over the next 5 years and is one of the BC applications with more growth potential where the market is estimated to grow at a compound annual growth rate of 87%.

2.1.1 Blockchain aspects benefiting supply chains

The mostly stated contributions of blockchain to Supply Chain Management are the traceability and transparency aspects (Moosavi et al. 2021). Already several use cases

[1] WalliD product: https://wallid.io/

have been studied and designed by Francisco and Swanson (2018) to illustrate how blockchain could improve traceability, efficiency, and decrease waste in a food supply chain. Blockchain could also help achieve robust cybersecurity and increase trust as demonstrated by Kshetri 2018 and Ying et al. 2018. There are several BC features that can offer advantages or trade-offs in SCM (Litke et al. 2019): Firstly, scalability may be improved since all actors participate in a common ledger without a single point of interaction. There also may also be a performance increase measurable in a reduced time for assurance of transaction verification compared to centralized and escrow services (e.g., bank payment liquidity or manual verification of a bill of lading) made possible due to automatic execution of contracts. Additionally, the consensus mechanism provides trust to all actors in the chain and offers privacy since although the transactions are verified, the actor's identity might be kept private via the BC specific addressing scheme. Furthermore, the SCM location dependency becomes more flexible by effectively allowing to make transactions autonomous from country regulations and laws. There is also the expectation of reduced cost by allowing faster payments while SCs (Smart Contracts) allow for faster dispute resolution. There are three generic benefits of BC to SC in 3 main topics (Somapa et al. 2018; Wang et al (2019): improvement of SC visibility, ensuring secure information sharing and trust and increased operational effectiveness.

2.1.2 Blockchain benefits to supply chain actors

Perboli et al (2018) used a lean approach to design and evaluate real world use cases that combine BC and SC. In their analysis there are specific benefits to each actor in the supply chain: producer, transporter, distributer, warehouse, final user/customer. For the producer, the value propositions of BC are the improvement of production planning and certification via Enterprise Resource Planning (ERP) integration, introduction of Stock Keeping Unit (SKU) certificates into BC and the reduction of the bullwhip effect since improving supply chain visibility allows for increased production requirements accuracy. For the distributor, the visibility of the whole supply chain allows for better inventory update and the reduction of counterfeit, theft, wrong delivery, product recalls, paperwork and the increase in ease of compliance. For the transporter/carrier, the benefits are the forecast improvement and the time slot reservation by using more real time information on the actual state of the product location and of the processing phase. For the final user, the benefits depend on the segment: Business-to-Business or Business-to-Consumer. Regarding the first, it will benefit more of easier stock management and expiration/recall management while the later will benefit more in better brand value management by providing the consumer better health protection and guarantees with more transparent sustainability or compliance claims.

2.1.3 Blockchain adoption path in supply chains

Dobrovnik et al. (2018) propose an adoption path for BC in supply chains and logistics. They propose that companies should focus first on single use cases to minimize risks of adoption and to start with proof on concepts that require little coordination with third parties and that allow for IT skills to be developed and learn the technology nuances. Specifically, they mention the use case of reconciling multiple companies' internal databases since it is a contained problem that brings major benefits. The second proposed adoption approach it to tackle the transactions across boundaries as, in example, reducing the paperwork by migrating the bills of lading (responsibility ownership documents used in shipping industry) into BC. Thirdly they recommend focusing on replacing functionalities that do not require that end users significantly change their behaviour. As an example, replacing paper certificates in the diamond industry. Finally, the introduction of new business models or new logics of value creation over BC, as for example using new SCs to act to prioritize specific air corridors.

2.1.4 Problems and challenges of SC over BC

A particularly challenging aspect for supply chains over BC has been reported by Weber et al. (2016) and is the latency and latency variance of transaction completion. In a public Ethereum platform the average latency for a modelled supply chain scenario was measured to about 23s. This problem has been reported to be mitigated in a private customized BC with average latency around 2.8 seconds. Another answer to the low performance problem of BC is claimed by Xu et al (2019). Their study focused on providing traceability assurance via improving certificate traceability systems. These systems receive the certificates issued by inspection authorities, that verify the quality and originality of the products, and store and expose them to other interested parties for accountability purposes. The authors proposed and implemented a proof of concept that moved the centralized certificate traceability system to a decentralized system over BC to avoid the risk of tampering by unreliable employees or firms. Their answer to the lower performance problem however is that it is acceptable in that use case since the number of certified suppliers and products is low. Another problem that affects the effectiveness of supply chains over BC is that the number of stakeholders in global supply chains tend to undermine any traditional type or mechanism for enforcing security. Xu et al. (2018) in their work proposed to enhance the security of said supply chains via

the binding of the physical and cyber worlds using digital certificates for both employees, devices and products that are responsible to enter and check the product data in the supply chain.

2.2 SCM traceability conceptual framework

The main problem in SCM when adopting BC is to ensure complete traceability. Many different aspects that provide complete traceability have already been mentioned and it is then important to provide clear definitions and context to their use and relationship to supply chains to have a conceptual framework on how to build a SC with more complete traceability. As mentioned by Keogh (2018), GS1 supply chain industry expert with 35 years of experience in the SC field the concepts of Provenance, Traceability and Chain of Custody (CoC) are often misused but their understanding and differentiation provides a stepwise conceptual framework on how to understand and approach the traceability network.

2.2.1 Provenance

Even before BC was developed it had already been identified that provenance management was a cross-cutting "hard" problem in science, industry and society. In Cheney et al (2009) provenance was defined as the metadata about the origin, context and history of change of origin in associated objects and processes. To assure provenance, there must be some metadata that identifies the item and its geographic characteristic and some functionality that transmits that information along the supply chain. At the time of the rise of the web and search engines it seemed that it was possible to make the claim that all metadata could be indexed, and provenance could be assured. However, several problems with the reality of provenance in SCM were pointed out: provenance was incomplete, unreliable, insecure, heterogeneous, difficult to integrate and non-portable across systems. At the time no real complete solution for provenance assurance was possible although the combination of sematic web and detailed causal graphs was suggested as a path forward. To make evident the difference of applying BC to the provenance problem, Montecchi et al (2019) applied a slogan "It's real, trust me" when proposing a framework that provides traceability, certifiability, trackability, verifiability and most importantly the increase of provenance knowledge. This increase in provenance knowledge comes from providing provenance assurances, namely: origin tracing, authenticity certification, custody tracking and integrity verification. These will in turn benefit firms by reducing business risks (real or perceived) which can be further categorized in physical, performance, social, psychological and financial risks.

2.2.2 Chain of custody

According to GS1 (2017), chain of custody or cumulative tracking in the context of a supply chain is a time-ordered registry of the sequence of parties who take physical custody of an object or collection of objects as it moves through a supply chain network. Chain of custody historically comes from the legal requirement perspective to provide proof of the tracking process. In highly regulated sectors (such as food, arms and drugs) chain of custody is critical and serves as the basis of both provenance and traceability assurance. According to ISEAL Alliance[2] (2016) the key propositions of a chain of custody system are to: identify the origin of a product (final or intermediate), ensure a custodial sequence along the supply chain, ensure that a certified product matches the certification characteristics, link, monitor and protect a claim at a certain stage of the chain with a claim at another point of the chain and finally to improve transparency. ISEAL Alliance (2016) proposes several custody models where the choice of the model depends on the claims the system or the actors wish to make. The models (in decreasing order of connectivity with a certain provenance claim) are identity preservation, segregation, mass balance overview and certificate trading.

2.2.3 Traceability

Has been defined in many different standards (EU Regulation (EC) No 178/2002[3], ISO 9000:2015[4], FAO CODEX Alimentarius CXG 60-2006[5]) and it can be summarized by: "the origin of materials and parts, the processing history, and the distribution and location of the product after delivery". Traceability comes from a business requirement perspective of tracking the movement of products and when origin information is preserved it is said to include provenance information. According to the most recent GS1 Global Traceability Standard, V2.0[6] these traceability concepts (Provenance, Traceability and CoC) when implemented correctly can be used to provide different levels of traceability functionality in supply chains. According to Sermpinis and Sermpinis (2018) there are two types of traceability: forward traceability the ability to find the locality at any point of the supply chain and

[2] ISEAL Alliance - global membership association for credible sustainability standards

[3] EU Regulation (EC) No 178/2002 at: https://bit.ly/35il6Ra

[4] ISO 9000:2015 at: https://www.iso.org/standard/45481.html

[5] FAO CODEX Alimentarius CXG 60-2006 at: https://bit.ly/2meiPUS

[6] Latest GS1 standard at: https://www.gs1.org/standards/traceability/traceability/2-0

backward traceability which is the ability to find the origin of any product given certain search criteria. Providing traceability is important for the food industry as is recommended[7] by the European Parliament in GMOs and GM free products. To provide traceability using BC in supply chains a possible approach is to tokenize the goods and use Smart Contracts (SCs) to model their transformation (Westerkamp et al. 2019). The BC in SCM traceability model has also been considered for risk management when supporting a Hazard Analysis and Critical Control Points System (HACCP) (Rahmadika et al 2018). BC enabled traceability using SCs is also well adapted to the post supply chain and has been proposed in a Product Ownership Management System (POMS) that detects counterfeits via combining the Radio Frequency Identification (RFID) product tags with a Ethereum BC system (Toyoda et al 2017).

2.3 Standards for traceability data

The already mentioned GS1 V2.0 standard proposes to make the bridge between physical products and their digital counterparts. According to GS1, traceability data that can be collected can be defined to answer the following five questions at each point of any business process role. "Who" – is typically identified by a Global Location Number (GLN) code (constituted by Company Prefix, Location Reference and Check Digit). "What" – can be a combination of identifiers based on Global Trade Identification Number (GTIN) with increased traceability granularity: class-level (GTIN), lot-level (GTIN + batch/lot ID - Identification) or instance level (GTIN + serial ID). When in transport process the GTIN may be coupled with the Serial Shipping Container Code (SSCC) – this is a pallet IDs that is created in during packing (by the shipping party) and loses the context and value after receipt by (the receiving party). "Where" – is typically identified by a GLN but can be extended by a GLN extension component to identify internal locations within a site, the Serial GLN (SGLN). "When" can be answered via a time stamp which should include date and time (including time zone and Coordinated Universal Time (UTC) time offset). Finally, "Why" should state the role of the party in the chain with typical roles being: harvesting, manufacturing, shipping, transporting, receiving and selling. Some additional information might be added if shipping is required: Global Shipment Identification Number (GSIN) or Global Identification Number for Consignment (GINC) when a bill of lading requires that the logistic unit has common delivery or shipping.

[7] EU traceability recommendations at: https://ec.europa.eu/food/plant/gmo/traceability_labelling_en

3 Research methodology

The DSR methodology was defined by Hevner et al. (2004) as proactive problem-solving paradigm with the objective to create, apply and evaluate useful artifacts that have as objective to forward the human business and social capabilities in the context of information and management systems. The DSR requires that the result of applying the methodology are artifacts and these can be defined either as constructs, models, methods or instantiations. To carried out the DSR, Hevner et al. (2004) established a set of 7 rules or guidelines: (1) problem relevance, (2) research rigor, (3) design as a research problem, (4) design as an artifact, (5) design evaluation, (6) research contributions and (7) communication of the research (Hevner and Chatterjee 2010). In this study the process of investigation was literature review, definition of problems and requirements, definition of architecture and functionality, interview with use case SCAs, production of artifacts, application of use case and finally an interactive review of artifacts. The produced artifacts were a solution architecture, the Smart Contracts, plus the PKI and digital certification scheme required to support the solution.

3.1 Research objective

This research proposal intends to address the traceability problem by formulating a solution that leverages existing BC functionalities and certificate validation and storage architectures and allows SCAs to gain confidence and verifiable knowledge on a product's traceability in a decentralized manner. To provide context and guide the analysis and design of the solution an alimentary traceability case study has been selected and studied. The research problem then can be formulated as follows: "How to implement a supply chain traceability system using a certificate validation architecture using blockchain?"

3.2 Research problem and questions

The research problem can be summarized as: "How to implement complete traceability and provenance in Supply Chains using Blockchain?"

The research problem was partitioned into more specific research questions in order to facilitate research and design of a solution:

- Question 1 - What are the relevant attributes and functionalities (requirements) that must be considered to implement complete traceability in Supply Chain?
- Question 2 - What would be a feasible and applicable solution architecture using available technologies to implement a certified traceability supply chain system?

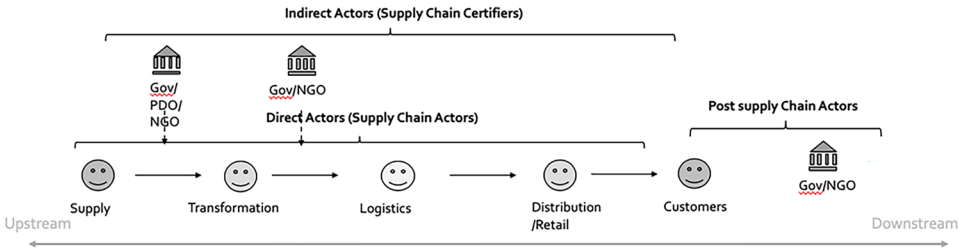


Fig. 1 Supply chain organization

- Question 3 - What are the required components and their functionality to implement the solution architecture?
- Question 4 – What is the required business logic to effectively manage the products ID and data transversally in the SC system?
- Q5 - How to validate the product's ID, relevant data and certificates of provenance?
- Q6 - How can the end user validate the provenance and traceability at the post supply chain?
- Q7 - How can this system apply to an exemplary supply chain that requires traceability and provenance assurance?

3.3 Stakeholder definition

To understand the stakeholders needs in the supply chain traceability problem it is important to understand their identity and context in the supply chain. In Fig. 1 the relevant stakeholders / agents are mapped according to their use and impact on the supply chain: Supply Chain Actors, SC Certifiers, post SC Actors.

The actual supply chain users can be grouped as direct actors where they are involved in the same business use case and are directly responsible in the normal managing of the supply chain (Suppliers, Transformation, Logistics, Distribution/Retail). For the purposes of traceability each SCA has different problems requirements and thus will have different role in managing the SC Products (see Table 1 for a description of the SCA attributes pertaining to traceability). The users/buyers of the products after the retail/seller are considered to belong to the Post Supply Chain. These are either end-user consumers or organizations related to consumer interests (Consumers, Consumer groups/Environmental groups - review and influences public opinion on product attributes and impacts, Governmental agencies - verifies product safety and regulations). There are also groups or organizations that influence the working of the supply chain (require that processes or documentation follow guidelines) but that do not participate directly in the supply chain operation. In what influences the traceability problem and the certificates it is possible to group the supply chain certifiers according to the type of certificate:

- Government: certifies products that are in accordance with governmental regulations.
- PDO: certifies products in accordance with PDO regulations.
- NGO: certifies products in accordance with Non-Governmental Organization regulations.

3.4 Stakeholder requirements

To understand which functionalities are required for SCAs it is important to define their reported weaknesses and limitations. This was performed in the previously presented review of literature. From that review we derived the following list of SCA requirements for the products and the certificate handling. .

3.5 Analysis of requirements

Based on the review of literature the main SCM problems related to traceability that were found are: access control, impersonation, counterfeiting, theft and wrongful delivery, certifying uniqueness of products, visibility, managing product recalls and brand value. According to the review of literature to solve these problems it is crucial to improve the 3 aspects of the defined traceability conceptual framework: provenance (metadata about the origin and associated objects, processes and users), traceability (ability to trace the history, application or location of an object) and the chain of custody (time-ordered sequence of parties with physical custody of an object). The state-of-the-art literature review of SCM over BC provided indications on the required functionalities that are needed to implement more complete traceability namely: (1) Manage the SCA access authorization via a certification mechanism. (2) Bind the physical and digital worlds by restricting access to supply chain product data only to certified actors and devices. (3) Use of a lightweight tokenization of products for representation of the products. (4) Allow the import of certificates and verify the true identity of both SCAs and products using said certificates. (5) Allow for certification data to be univocally linked with the SCAs and product tokens. (6) Allow processing and transfer of ownership procedures while maintaining the identity chain of custody and respective certificate linkages. (7) Reduce supply chain perceived risks in the post supply chain by allowing the customers to view certification information.

Table 1 Supply chain actors' problems and requirements

Actor	Weakness/Limitation	Consequent problems	Aspect to improve	Requirements	Authors
Supply	Ability to prove globally the origin, authenticity and quality of the products and producers	Counterfeiting Loss of brand equity	Provenance	Register valid SC Actor Register products with information and proof of origin	Lu and Xu (2017) Montecchi et al. (2019)
Transformation	Difficulty to monitor the quality and origin of supplies. Limitations in monitoring the product to the final destination.	Contamination Loss of quality Loss of brand equity	Traceability CoC	Register valid SC Actor Transform products while maintaining certificate traceability Register valid SC Actor Register transfer of ownership	Aung and Change (2014) GS1 Standards Document (2012) Sahoo and Halder (2021)
Logistics	Lack of visibility and trust of the transfers of ownership (internal or external).	Delays and theft No attribution of responsibility Interoperability costs	Traceability CoC	Register valid SC Actor Register transfer of ownership Provide visibility to certified product inventory, location, owner	Agrawal et al. (2021) Sahoo and Halder (2021)
Distribution/ Retail	Ability to verify the inventory, origin and authenticity of certified products. Lack of visibility and trust of the transfers of ownership (internal or external).	Counterfeiting Misrepresentation of quantities Customer Legal action Loss of brand image	Traceability CoC		Agrawal et al. (2021) GS1 Global Traceability Standard (2017) Sahoo and Halder (2021)
Final customer	No independent confirmation of the quality, origin and sustainability of products	Health and monetary impacts Distrust in business Concern for environment and sustainability	Provenance Traceability Chain of custody	Provide visibility to supply chain trace and certificates.	Cartier et al (2018) Keogh (2018)

So, the central capability to verify a digital identity and ensure that only that participant, device or product can use that identity is an essential functionality that is required in supply chains that implement traceability. This functionality has 3 parts: (1) being able to verify the digital signature, (2) being able to verify the certificate of a CA has the correct attributes and finally (3) that the participant is the correct owner of the certificate. This traceability functionality was translated into a requirement to setup a PKI involving the SCAs, the product Certificate Authorities (CAs) and that extends to the certified products. According to the literature review it was also possible to summarize the required attributes for a SCM with more complete traceability with verifiable: "user identity" (SCA ID and certificate), "product identity" (Product ID and certificate), "transfer of custody" (two-sided verification of SCA and product IDs), "uniqueness" (ledger of unique product IDs, "location of products" (geographic reference), and "timestamp of operations". From the required functionality and attributes, it was possible to select a supporting applicable technology and derive the corresponding improvement of the traceability aspect (Table 2).

4 Results

4.1 Solution design

Following the literature survey research results, in order to design a solution to provide a supply chain system with complete traceability we must focus on providing solutions to the problems raised by the main three concepts:

- Provenance – provide metadata about the origin, context and history of change of products and producers
- Traceability – provide record of the trace history, application and location of a produce in the SC
- Chain of custody – provide time-ordered sequence of events the parties create when they take physical custody of an object or collection of objects as it moves through a supply chain network.

In table 3 we described the identification of the problems of each concept as it related to SCAs and Products. Following the DSR, the use cases and the architecture are the design artifacts that provide the solutions for the research problems.

4.2 Proposed functionality

According to Weber et al. (2016) BC can be used as the collaborative process execution machine. This is performed in 3 steps. Firstly, translating the process specifications/requirements into Smart Contracts. Secondly using the BC computational infrastructure to organize the collaborative processes. Thirdly using the BC triggers to connect physical and digital world. This proposal adds to that proposal the use digital cryptographic certificates to establish both: SCA and product identity and authenticity inside/post a distributed and untrusted supply chain. The digital representation of supply chain products is supported by a lightweight tokenization of the products and their associated processes in a SC. In this proposal the certificates are only linked to the tokens and to have a minimum increase of BC storage and avoid the cost for the importing and validation of the certificates in the SCM. To implement the previously defined requirements a set of SCM traceability functions/use cases were defined to be implemented in the Ethereum SC (with the Smart Contract business logic). The SCAs can operate the SCM by calling the SC functions[8] (Fig. 2). Architecture workflows for referenced use cases A to G are described in ANNEX 1, use cases H and I are described in ANNEX 2.

4.3 Design aspects

Due to BC's unique capabilities and features several design aspects and trade-offs must be considered when designing a SCM over BC. The decision to use private/consortium vs. public BC systems will depend on the selected industry use case, its requirement for global public access and will have impacts on the decentralization, the scalability and latency/latency variance of transactions. A public BC like Ethereum is globally accessible, fully decentralized and has higher availability due to the number of nodes. One trade-off of a public BC is that its transactions are expected to have higher latency and latency variance so the scalability aspect is not under control of the participating organizations and the BC code will generally follow a standard that is defined by a distributed improvement proposal scheme. As an example, an operation over Ethereum public BC is expected to take tens of seconds or more, varying much on the load on the system and so the latency is not under control of the SCM participants. This latency and latency variance problem can be mitigated to a few seconds per transaction if a private or consortium BC is used. However, a trade-off of that approach would be to lose some of the global access and availability features. In what regards scalability a private or consortium BC can scale its throughput without having to increase the number of nodes since it is possible for example to specifically configure consensus mechanisms that allow for faster transaction validation. For the use case in analysis in this article and for the proposal both public or private BC networks are possible to be used and

[8] Details on the Proposed SCM Functions are available in https://github.com/Supply-Chain-Traceability/SolutionProposal

Table 2 Applicable technology and the corresponding improvement of the traceability aspect

ID	Requirement	Applicable technology – Proposed solution	Problem that it solves	Supported Concept/ Added value
1	SCA registration validation and access control	Public Key Infrastructure (PKI) and SCs – uses certificate to establish and maintain assurance of the identity.	Access control- only allowed SC actors can interact with SCM. Requires registration/ verification of the certificates	Support Traceability
2	SCA sign on operations	Ethereum BC and SC logic– associate EBC addresses to validated identities. Any EBC has to interact by using a signed transaction.	Impersonation - The validated participants are required to sign all operations and make proof of their identity	Support Traceability
3	Register products certificates	SC logic and PKI – associate product identifiers with their certificates	Counterfeiting - only original products information is introduced into the SCM	Assure Provenance
4	Correct transfer of ownership	SC logic - provides 2-sided transfer of ownership.	Theft and wrongful delivery – register of each transfer of ownership is registered	Implement Chain of custody
5	Verify ownership and product certificate validity	SC logic and PKI - to verify the current ownership of a product and if the certificate is valid or has been revoked.	Product ownership and certificate validation - requires a check of ownership and if the certificate is valid.	Implement Traceability and assure provenance
6	Transform products	SC logic - use of SC functions to tracks the transformation of certified products	Certificate and inventory management – requires that transformed products maintain the certification source.	Support traceability, provenance
7	Product certificate retrieval.	JavaScript, SC logic and PKI- use of SCs and an external URL for certificate visibility.	Standards, health, compliance, brand value - requires controlled access to the chain of product certificates.	Implement Provenance visibility

Table 3 Mapping between Problems, solutions and artifacts

Concept	Problems	Solutions	Use Cases to implement
Provenance	Proof of SCA Identity	Identity validation and storage	A - Register SCA
	Proof of product authenticity with origin attributes	Certified Product registry	B - Register Product C/D - Get/Set Product Attributes and Certificates H – Import ID and Certificate
	Provide visibility to supply chain trace and certificates	Provide visibility to specific product certificate and trace data	I/J –Retrieve/Validate ID and Certificates K – View Product Certificate
Traceability	Register changes to the product data (location, owner)	Changes to product are registered via traceable transactions	C - Get/Set Product Attributes F/G - Ownership Transfer to/Receive from
	Transform products while maintaining certificate traceability	Provide access control to view / modify product data	E. Transform Product
	Provide visibility to supply chain trace and certificates	Provide visibility to specific product certificate and trace data	I/J –Retrieve/Validate ID and Certificates K – View Product Certificate
Chain of Custody	Register and view the transfer of ownership (among SCAs)	Provide distributed mechanism for change of custody	F/G - Ownership Transfer to/Receive from
	Provide visibility to supply chain trace and certificates	Provide visibility to specific product certificate and trace data	I/J –Retrieve/Validate ID and Certificates K – View Product Certificate

there is no dependency to any BC public/private flavor. Another design aspect to consider is how to store some or all the SCM data: on-chain or off-chain. When user data is stored on-chain (as a variable in a SC) it is more costly (at least 2x more but can vary depending on the BC) but is potentially more performant since the data is retrieved from BC immediately. If data is stored off-chain the SC can interact with it but is less performant since it requires querying the off-chain system so we should expect a more complex implementation and possibly the addition of latency to the solution. The proposal in this article is to aim to keep as little supply chain data on-chain as possible while retaining the traceability functionalities thus following a light tokenization approach. Reducing BC storage costs is important since it could make the solution too costly and hinder the business adoption. Following this approach, the certificates are stored/retrieved off chain via a store provider and only the information on the validity of SCA and product

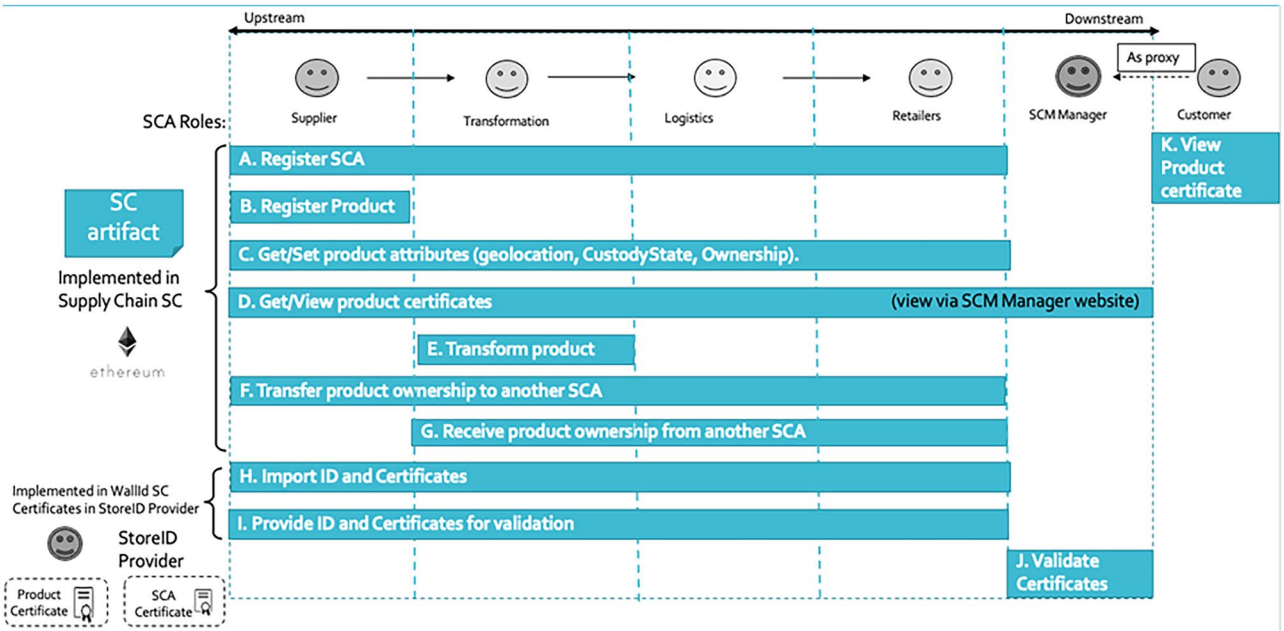


Fig. 2 Proposed functionality

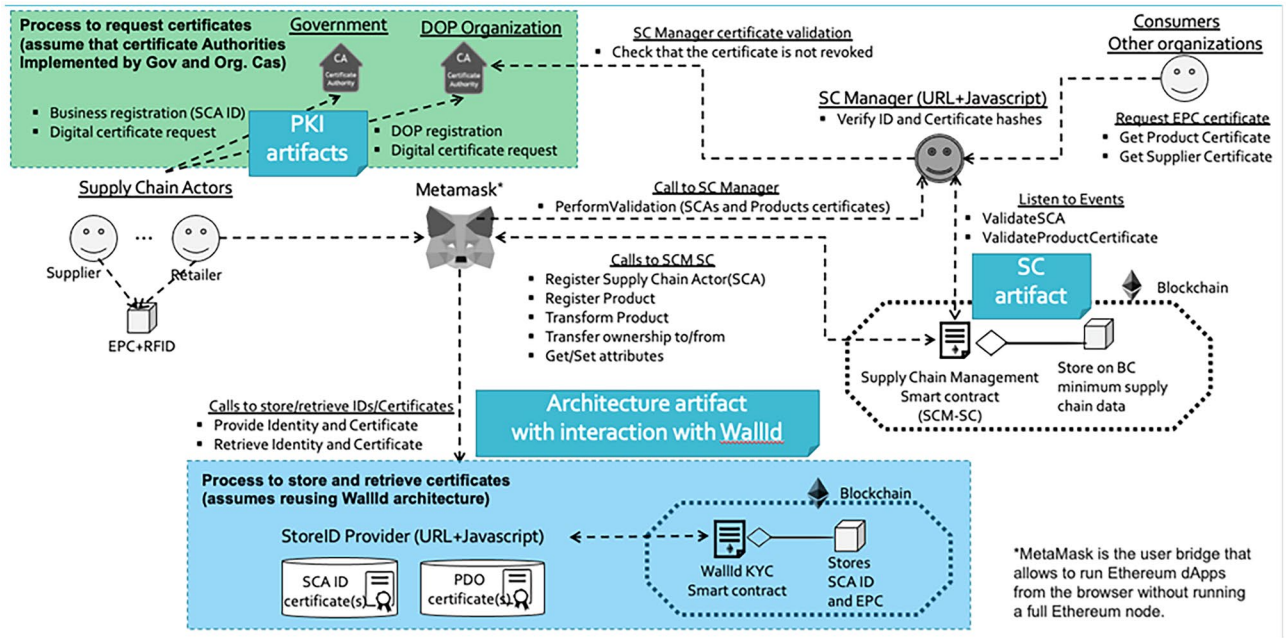


Fig. 3 Proposed architecture

certificates are stored in BC. The SCA addresses and roles and a token representing the product is stored in BC. This token has a universal identifier (Electronic Product Code – EPC) which provides an immediate link to the physical world via Bar codes/QR codes/RFID tags. This EPC will also provide the link to the product certificate which is stored off-chain. The only additional token attributes in BC are the ownership link between EPC and SCA, the custody state (e.g., "owned", "in transfer" or" sold") and the current geographic location of the product. The SCA access is implemented via SC logic by verification of the SCA certificates. The same pattern is used both for SCA and product certificates. An SCA can import both actors or product certificates into certificate storage and afterwards retrieve the certificate to validate the identity (SCA or Product) with the SC Manager. If the deployment is to a private/consortium BC it would be possible to remove the strict enforcing of authentication in the SC via certificates and have other methods of access control such as LDAP[9] (Lightweight Directory Access Protocol) and Kerberos[10] to improve performance and prevent attacks on the BC consensus. It could be argued that private BCs provide better security from the start since only allowed users can use the BC. However, one of the main security risks to any BC is the protection of the private keys and the integrity of the SC code, which is non-dependent on network infrastructure control but on good security practices and hardened and well-maintained SC code. As a preliminary step and to interact with the SCM, a SCA must first create a BC account. A BC account is considered to be the public and private keypair that are connected to the user address and the funds (both stored in the network). To manage the account more easily an interface/wrapper is used, and this is what is generically called a BC Wallet. Interworking with BC with the user wallet can be performed in several ways. For this solution proposal we selected Metamask[11] since it allows to streamline the end-user experience by having an interaction with a responsive website while also allowing the use of both hardware wallets (e.g., Ledger[12] with Metamask) and online wallets (e.g., MyEtherWallet (MEW)[13] with Metamask).

4.4 Proposed architecture

The proposed architecture uses a Ethereum BC SC to implement the already presented use cases. As mentioned, the SCAs interact with the BC using their wallets via Metamask

[9] An application protocol for accessing and maintaining distributed directory information services.

[10] A computer-network authentication protocol that uses tickets to allow nodes to prove their identity.

[11] Metamask documentation. Retrieved from https://bit.ly/2ATNqeE

[12] Ledger is one example of a hardware Ethereum wallet: https://www.ledger.com/

[13] MyEtherWallet is one example of a software Ethereum wallet: https://www.myetherwallet.com/

with calls to the SC code using a JavaScript based interface (Web3 API[14]) (Fig. 3).

The state of the supply chain, all its actors and products are tokenized in Ethereum via the Smart Contract. This proposal uses digital certificates for user and product authentication and so it requires that recognized organizations implement a PKI (to generate digital certificates and provide the chain of trust). In the case of public market products governments and certification organizations are among the best candidates for establishing a PKI for businesses operating on global supply chains. It is possible to have the PKI implemented directly by consortium organizations when the use cases are restricted to specific businesses or industry sectors. This proposal requires that only validated SCAs (the ones which can provide an ID and certificate that match and verifies) can register products into the SC system. The SCA and products certificates are digital certificates that attest of the business identity (e.g., when registering with national government agency) or attest that the product has unique distinguishing and certified characteristics (such as in the case of PDO (Protected Designation of Origin (1992)) where the products and processes are verified and certified by a selected PDO regulator organization. The importing and retrieval aspects of the SCA and product certificates is performed with the reuse of the Know Your Customer (KYC) solution from WalliD adapted for identities such as organizations and products. Details on the Certificate Import and Validation functionality using WalliD KYC (off-chain solution) are described in ANNEX 2.

In this proposal the products in the supply chain are referenced by an industry referencing standard, the EPC – Electronic Product Code which is a unique identifier commonly used in supply chains as described in the case of livestock supply chain by Hartley et al. (2014). The supply chain can operate with products without certification (since it is optional to provide them) but the main business value of this proposal should be for products that require authenticity validation. The validation of certificate hashes for both SCA identity and products is performed off-chain by the Supply Chain Manager entity (that includes the role of "Certificate Validator"). Another deciding factor to have certificate validation off chain has to do because it is not performant to execute crypto hashing (validation function) on chain in the current Ethereum Virtual Machine (EVM). The SC Manager ("Certificate Validator") is also responsible to perform certificate revocation in the cases the SCA or the product must leave the SCM BC. Additionally, SC Manager can also provide a website for SCA actors and consumers to request and view the product certificate given a product EPC. The EPC can then be read from the physical product RFID or QR/Serial code tag using a smartphone with an App our via a specific EPC reader device. After SCA certificate validation the Supply chain management and traceability functionality is provided using the SCA BC addresses via transactions in a trusted and decentralized way with no further validation required. The SCM-SC is deployed in the EVM by the SC Manager which is the owner and ultimate responsible for the security and maintenance of the SC code[15] Details on the proposed Ethereum Smart Contract code is in ANNEX 3.

4.5 Case study - alimentary PDO use case

As already mentioned, an example about alimentary supply chain use case was selected to better understand the requirements and correct application of the proposed solution. The selected use case was the production and transformation of certified livestock produce (bovine meat) of the "Carne Mirandesa" – a type of bovine meat that is PDO certified and only produced in the northeast region of Portugal. This PDO is already currently certified using a combination of paper certificates and products tags or stickers that are shipped with the product. From an interview with a producer and retailer 3 document samples were collected: the certificate that links the Government ID of the animal (SNIRA[16] ID) with the PDO ID and certificate of the brand "Mirandesa" (Geneology ID), the transformation identifier that is shipped with the bovine meat that shows the reference to the animal (SNIRA ID) and the sale point invoice that attests to the purchase of the carcass and served meals with the reference to the batch attested by the a governmental agency (SNIRA ID). The unique identifier that is used across the supply chain is the Electronic Product Code (EPC) that is linked with both the SNIRA ID and the Genealogy ID (EPC-SNIRA ID-Genealogy ID). The product certificate to be generated has then to hold these 3 fields in the X509[17] certificate request as mandatory fields to be certified together with the public key hash of the producer (supplier actor in the SCM). In summary each product will be issued a X509 certificate by the producer. This particular CA chain of trust requires three SCA certificates: one for the root CA (the Government CA), another for the intermediate CA (the PDO association CA) and finally one for the SCA producer. The summaries of the use case data and PKI certificate setup are presented

[14] Web3 API is Ethereum Javascript API that allows to interact with an Ethereum node: https://web3js.readthedocs.io/en/v1.2.4/

[15] A more detailed description of the architecture use cases is available in https://github.com/Supply-Chain-Traceability/SolutionProposal

[16] SNIRA (Sistema Nacional de Informação e Registo Animal) is the national Portuguese Government livestock registry: https://www.ifap.pt/snira

[17] X.509 is a cryptographic standard defined by ITU-T standardization body that defines the format of public key certificates (used in https and electronic signatures): https://tools.ietf.org/html/rfc5280

in ANNEX 4 and ANNEX 5. To streamline the production of X509 certificates the request for product certificates can be automated by an application at the producer side that requires that the producer inputs the triad of X509 attributes that need to be certified (EPC, SNIRA-ID, PDO-ID) and then issues the certificate request and at the CA's side a backend IT system that issues the X509 certificate after the verification processes have been validated. It should also be noted that as a product is processed in the supply chain its EPC code may change from animal EPC (type SGTIN) to carcass EPC (type SSCC) and carton tag EPC (type SGTIN). However even in this case the proposed solution SmartContract code is capable of maintaining reference to the original certified EPC and its owner SCA and support complete certificate traceability. This EPC code change is also described by GS1 in Hartley and Sundermann (2014) where a livestock traceability proof of concept (PoC) was implemented. In that PoC the EPC codes are read from RFID tags but in that case, they were inserted into a centralized SCM application to provide the required traceability metadata while in this proposal the EPC is stored in BC. As in the PoC in this proposal the EPCs can suffer change due to processing the meat thus the requirement for the previously presented "transform product" function in the SCM SmartContract to keep the EPC and certificate link[18].

5 Conclusions and future work

As presented before, we posited and fully described a complex research problem. This complexity stems from two factors, the relative novelty of the technology and the combination of several existing solutions (Ethereum Smart Contracts, Digital Certificates, PKI and WallId certificate storage). This combination allows to propose a solution application for a supply chain when it is imperative to assure the traceability and the authenticity of the products sold over that value chain.

5.1 Research contribution and solution benefits

The research contribution of this work is a solution that aims to answer the research problem of providing complete traceability for a supply chain using blockchain. The main benefit of the solution is that it allows for a group of independent participants to implement a decentralized supply chain system with a complete traceability model for certified products. Another benefit is that via the PKI allow for SCAs themselves to import certificates and customers to view them thus providing trust among participants and the end customers. The proposed architecture simplifies the storage of the certificates by reusing a KYC system (used in banking and credential verification) to both store and validate these certificates. If any certificate fails validation or is revoked (e.g., expiration) it can be added to a CRL (Certificate Revocation List) by the CA (as is usual in PKIs) and the SC Manager simply sets an invalid certificate flag in the SC. If a SCA own certificate is revoked it no longer has access to the chain of trust until it provides a valid certificate. If the product certificate is revoked the product token can still be managed in the SCM but the certificates will be shown as expired or invalid to SCAs and customers (allowing the supply chain to operate while the certificate issue is being resolved). During operation, the SCAs have access via the Blockchain to the ownership status, the operations timestamps, the full chain of certificates and the transfer locations (if added) which can be further processed by SCAs own internal Supply Chain Management systems to interoperate with other IT systems (analytics) and optimize the supply chain.

5.2 Limitations

The main drawbacks of the solution are its dependency on a PKI (for SCAs and products), a centralized and hierarchical trust model and the dependency on a central entity (Supply Chain Manager) for certificate validation. Regarding the dependency on PKI the minimum requirements are its setup by a national or regional or any trusted authority in a privately owned supply chain and that the SCAs must subscribe to an authentication scheme for their identities and products. Regarding the SC Manager this actor is required to deploy the proposed SmartContract into the Ethereum BC and to be the entity responsible to be the "certificate validator". A possible alternative to the use of a centralized PKI (and possibly to replace also the SC Manager) would to use a decentralized approach as has been recently proposed with Self-Sovereign Identities (SSI) and the usage of Decentralized Identifiers (DIDs) as defined by W3C (2022). Instead of digital certificates some previous solutions propose the import of scanned paper certificates. This is the case of "origin Chain" implementation, but this seems a stegap approach since such verification is more complex to implement and may require manual intervention to fix misreading or damage to the paper certificates. A more technology oriented approach would be the use of IoT devices and RFID tags with digital certificates where all authentication and verification is automated with higher granularity and the added security of a physical security token. An alternative for the SCAs certification-based authorization is to replace it with a simpler although less decentralized and autonomous authentication system (e.g., LDAP) but this has the drawback of increased complexity and complexifying the security and management aspects in

[18] For details on use case samples, EPC details, the PKI certificate request and revocation see https://github.com/Supply-Chain-Traceability/SolutionProposal

cases of global SCMs. If only a sectorial industry approach is required and the global decentralization and autonomy is not necessary and it would be more advantageous to operate over a consortium BC, with the benefits of lower latencies/latency variances and centralized SCM control.

5.3 Future work

There remain open points that are left for possible future work and development of a Proof of Concept (PoC). The first open point is that the SC lacks the functionality for all SCAs to add product certificates (currently only suppliers) in the case of transformation of products. Additionally, it is still undefined when to delete product references after the products go to the post supply chain. Some attention should be given also to the issue of certificate validation outside of the BC. One of the possible criticisms of the proposed solution is that of not achieving complete decentralization since due to the centralized PKI and proposing a certificate validation mechanism to be implemented off chain. As previously mentioned it would be very interesting to explore the adoption of SSI and DIDs as a non-centralized approach to the identity and certificate validation problems. For future work, besides the open issues it is left the development and implementation of a PoC that would allow the deployment of a fully-working/testable SCM with this architecture. Also, for future work would be the design of an incentive scheme that would allow for the implementation of the "Certificate Validator" function. This functionality should be possible to implement by third parties in the public Ethereum BC. A future PoC would also require the implementation of a test framework (in JavaScript) to interact with the SC via the Web3 API and the companion browser or possibly IoT software add-ons to facilitate user interaction with the SCM. In addition to real use case validation of the proposal a PoC would allow to measure operating and information storage costs plus the operational feasibility and business competitivity (in terms of required IT infrastructure).

Appendix

ANNEX 1 Architecture workflows

Use case A: Add a new SCA to the supply chain management system (Fig. 4).

A SCA must firstly authenticate himself before being able to interact with the SCM. For this he must register with a trusted entity that makes sure he has the correct credentials and authorization to interact with the SCM. Following the requirement of having a decentralized system and in accordance with the selected use case (PDO alimentary supply chain) the trusted entities were considered to be the Governmental/Organizational agencies. In the case of a centralized SCM (e.g., over private/consortium BC) another central entity could be chosen, and the certificate validator could also become the certificate issuer (CA) (Fig. 4).

Use case B1: Add a new product to supply chain (Fig. 5).
Use case B2: request certificate for product (Fig. 6).
Use case B3– Register a new product in SCM (Fig. 7).
Use case C – Get/Set product attributes (Fig. 8).
Use case D – Get product certificate (Fig. 9).
Use case E– Transform product (Fig. 10).
Use case F/G– Transfer ownership to/from (Fig. 11).

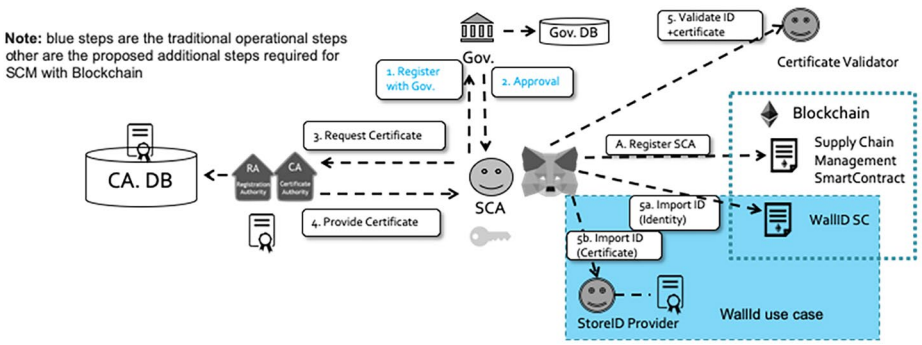


Fig. 4 Use case A – Add a new SCA

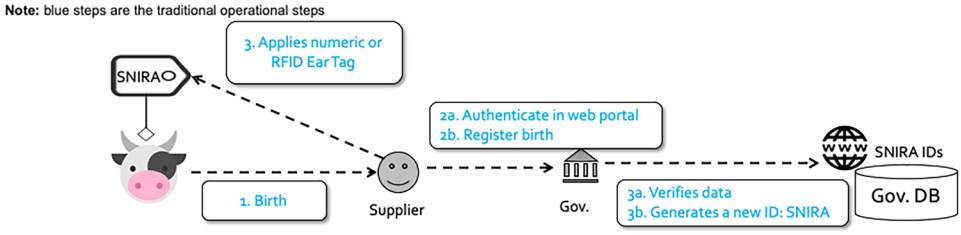


Fig. 5 Use case B1 – Add a new product

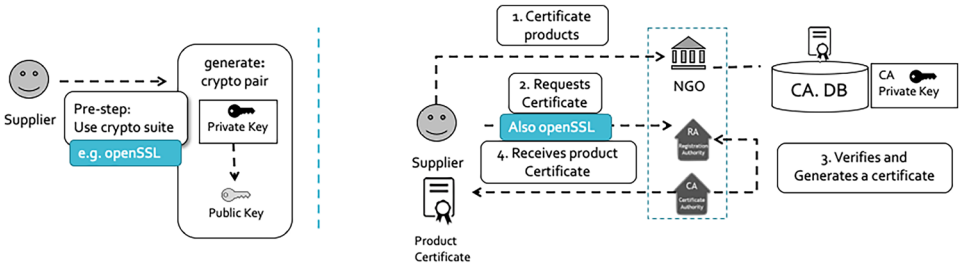


Fig. 6 Use case B2 – Add a new product

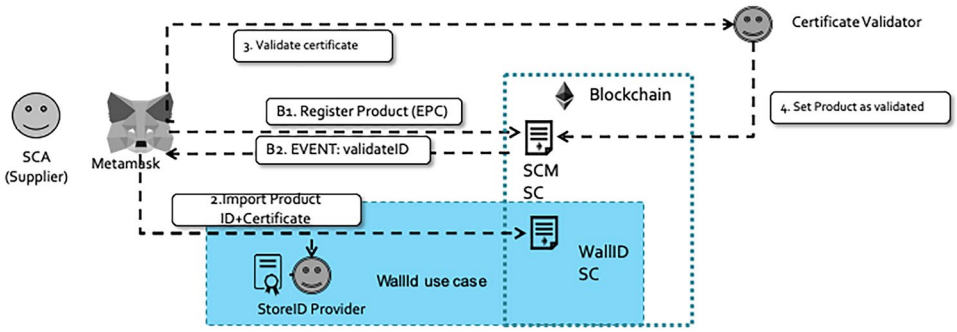


Fig. 7 Use case B3 – Register a new product

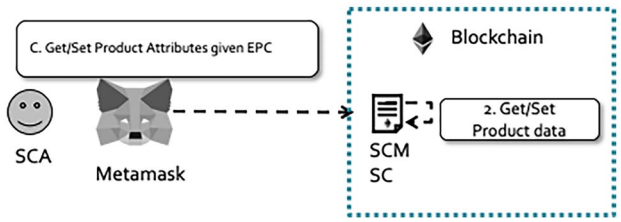


Fig. 8 Use case C – Get/Set product attributes

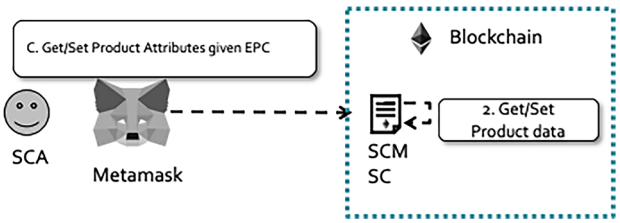


Fig. 10 Use case B3 – Register a new product

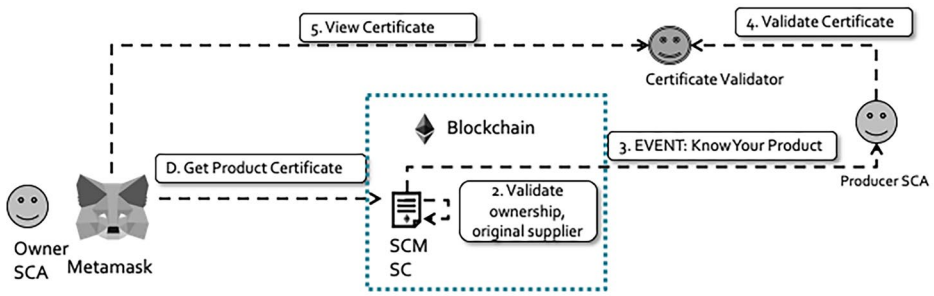


Fig. 9 Use case D – Get product certificate

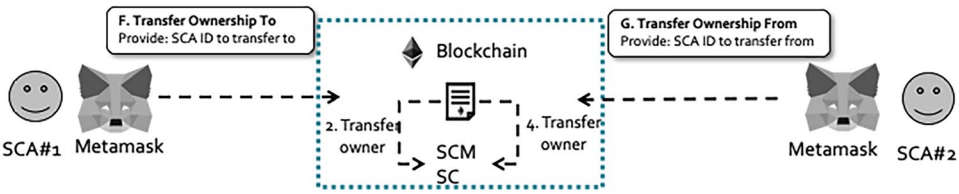


Fig. 11 Use case F/G – Transfer ownership

ANNEX 2 Certificate import and validation

In order to import and validate the certificates the SCM solution interacts with the WalliD architecture for 2 use cases: import of certificates into the WalliD store provider and afterwards certificate retrieval from the store provider. These actions are run in sequence with 2 events: ImportID and following the correct import RequestKYC/RequestKYP. The same pattern is used for both the registration of SCAs and the registration of products.

WallId Import certificate (use case H) (Fig. 12).

WallId Validate certificate (use case I) (Fig. 13).

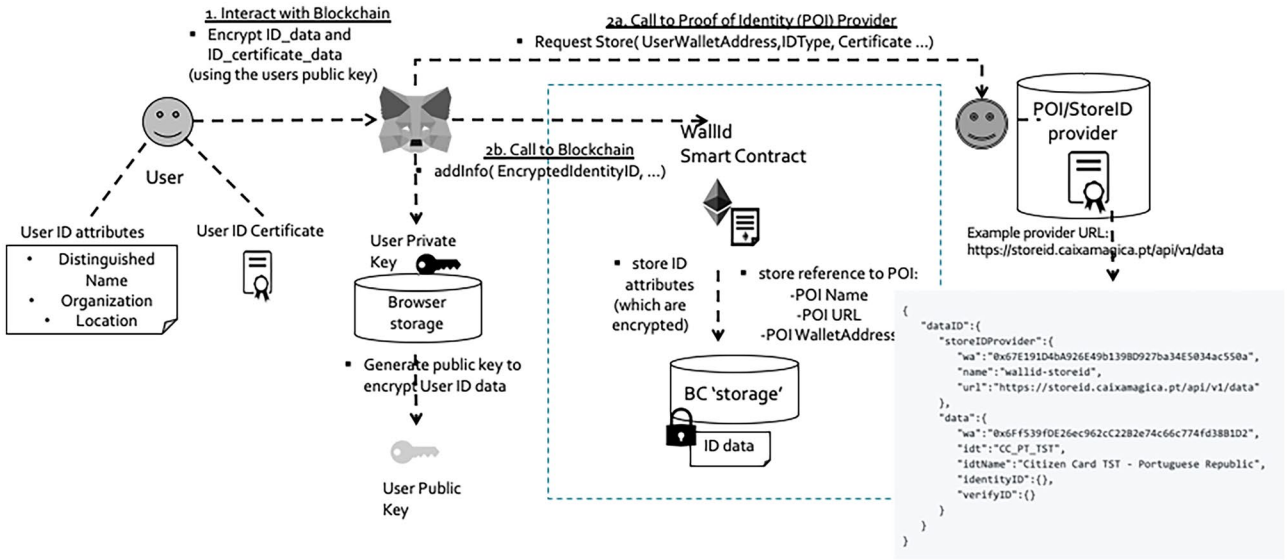


Fig. 12 Import certificate architecture

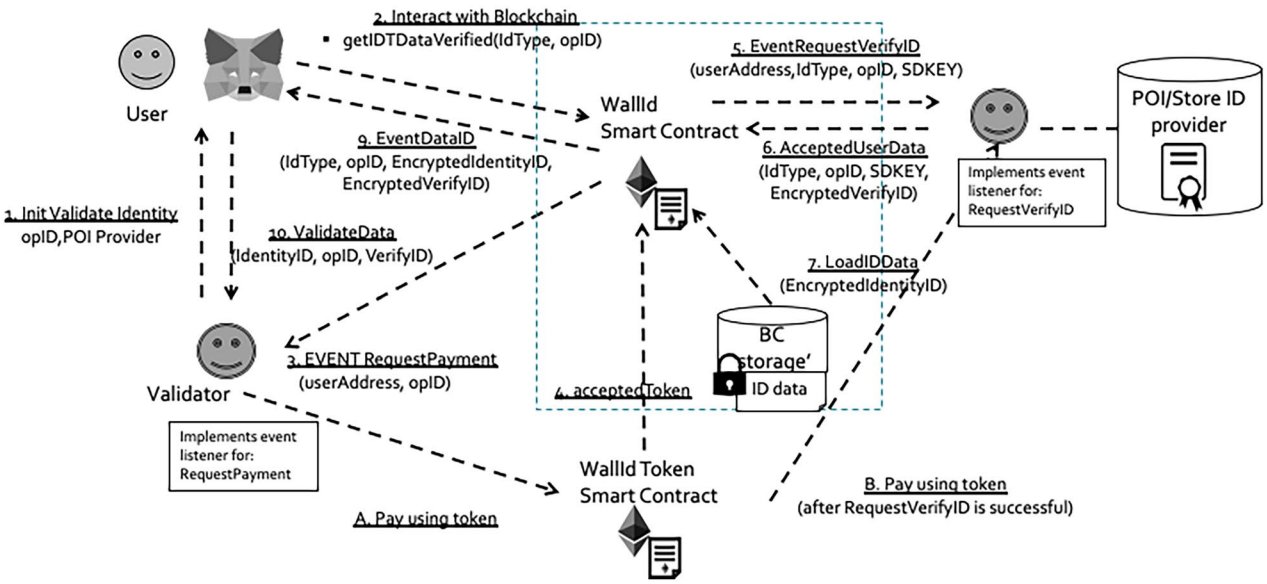


Fig. 13 Validate certificate architecture

ANNEX 3 Ethereum smart contract

The most updated version and complete SC code is available at: https://github.com/prgazevedo/DLT_Masters/tree/master/SCM_SmartContracts. This code compiles for solidity version 0.5.11.

Detail on SCA and Validation (Fig. 14).

Detail on Product registration and transformation (Fig. 15).

Detail on transfer of custody and loss of Product (Fig. 16)

Detail on Get/Set functions (Fig. 17).

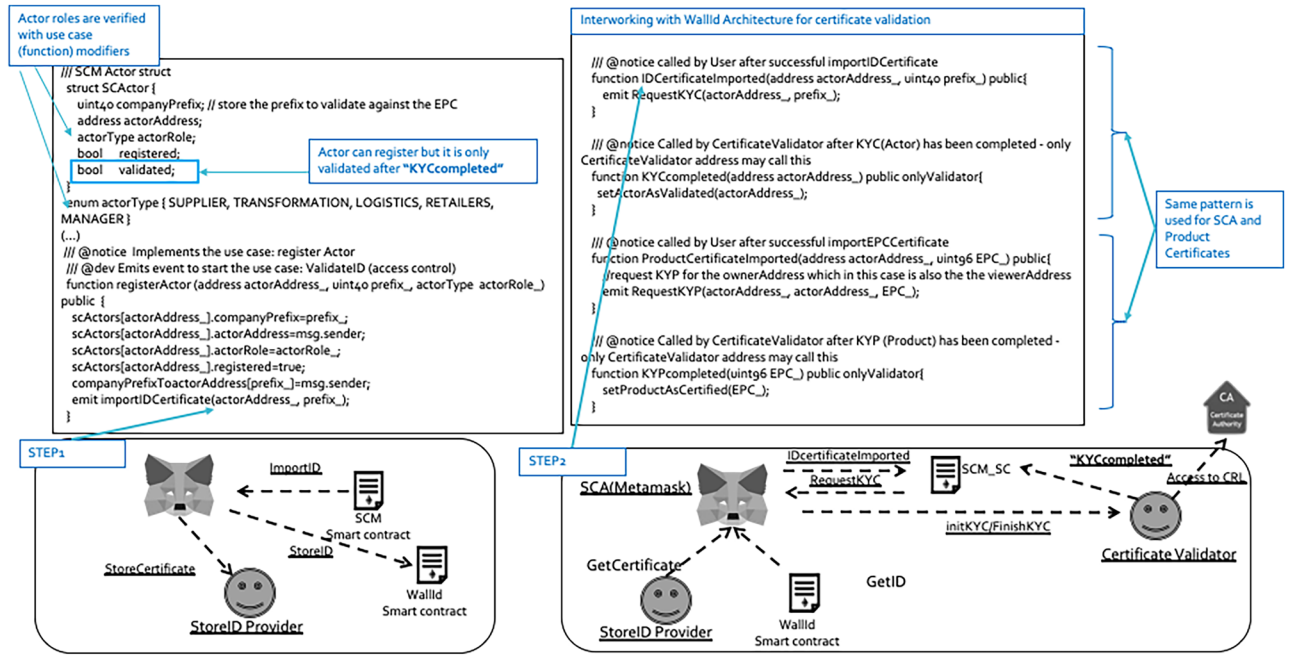


Fig. 14 SCA registration and validation

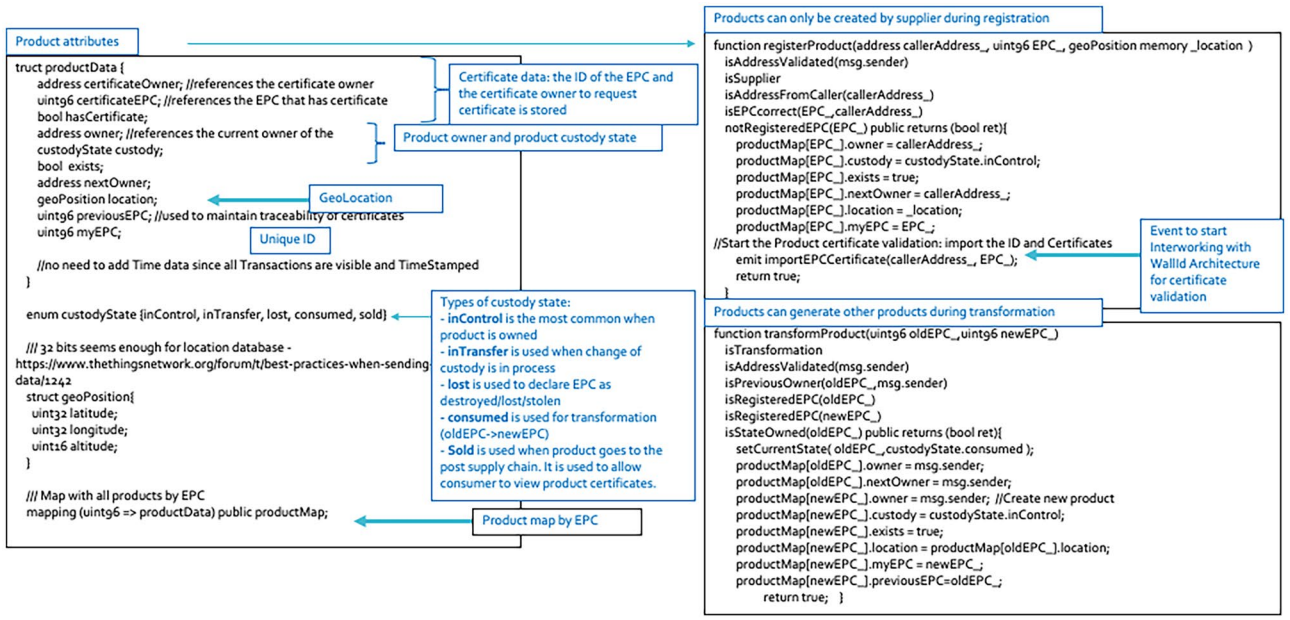


Fig. 15 Product registration and transformation

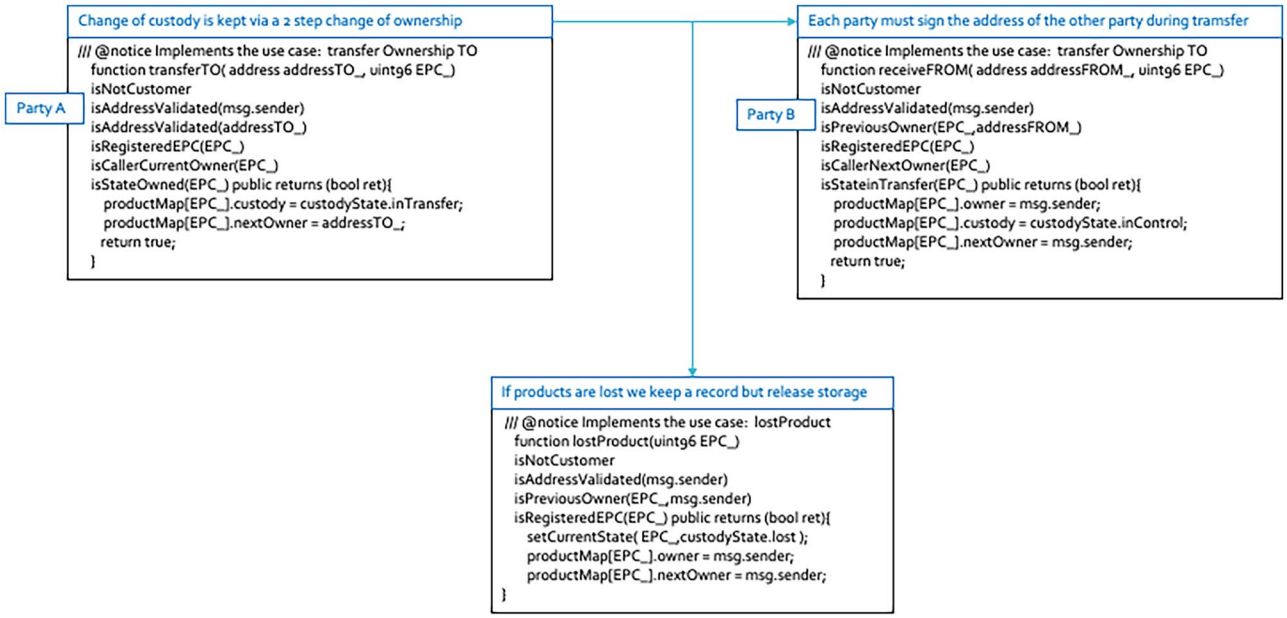


Fig. 16 Transfer of custody

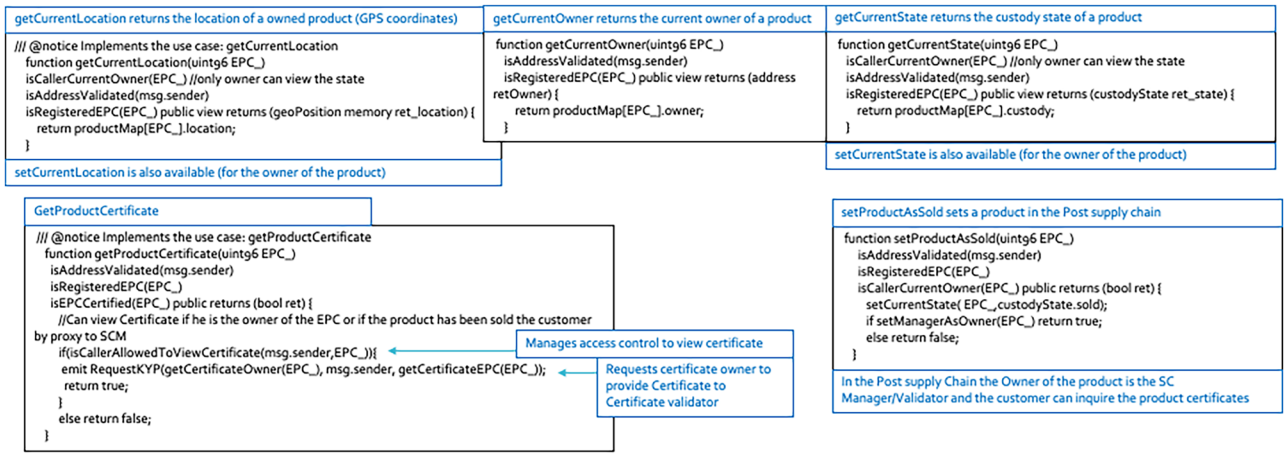


Fig. 17 Get/Set functionality

ANNEX 4 Use case source data

In the next figure is presented the linkage between the livestock (bovine) government assigned ID and the PDO organization assigned certificate ID. These 3 documents presented were collected at the local supply chain exemplify the main data and attributes that are required to establish traceability for this use case (Fig. 18).

The government assigned ID of Bovine (SNIRA ID) is attributed at birth by DGAV and stored in Sistema Nacional de Informação e Registo Animal (SNIRA) by IFAP (more details at https://www.ifap.pt/web/guest/snira-regras). At the same time of birth the genealogy of calf (bull ID and Cow ID) is recorded by the PDO organization (in this case the "Mirandesa" association) and is also recorded in (SNIRA) by IFAP . When the bovine is ready, it is then sent to a certified slaughterhouse where the registry of both SNIRA ID and certificate linkage is assured. At this time the carcass is assigned a EPC code and a physical tag with the ID of the slaughter house (PT-T 18-CE). The carcass is then shipped to the retailers or seller of the end product that can be either a consumer beef produce (in the case of butcher

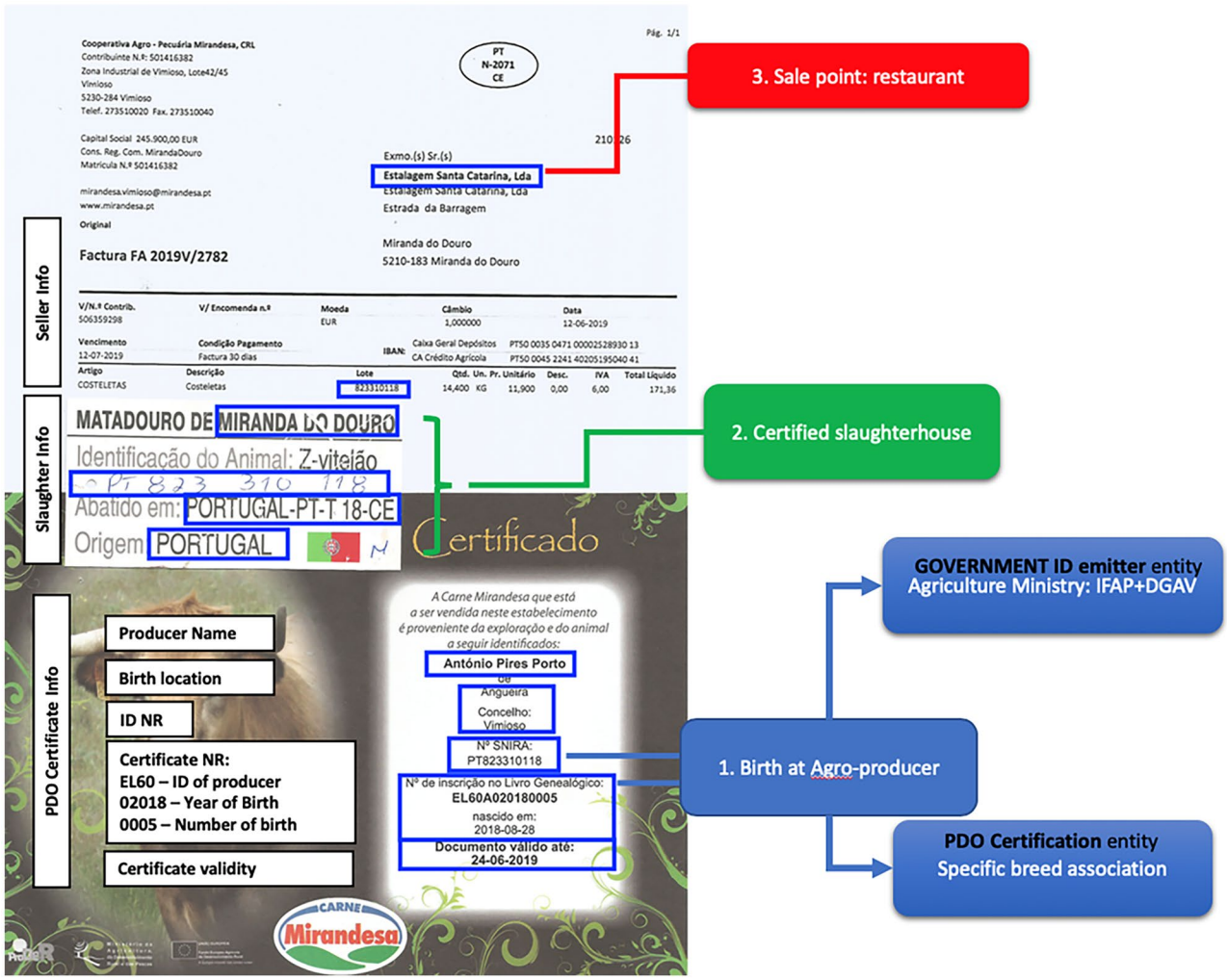


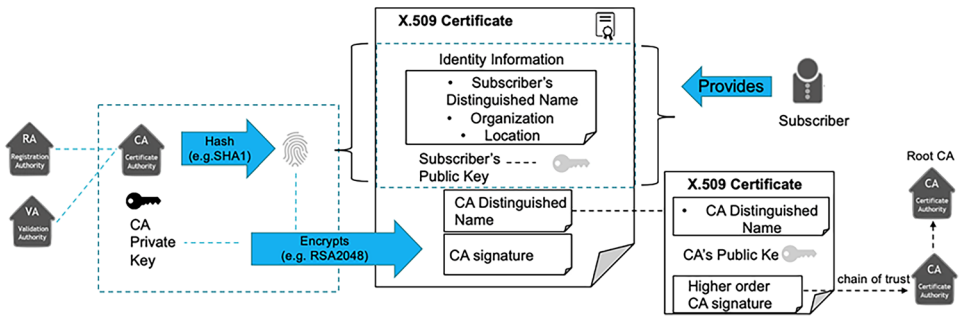
Fig. 18 Use case certificate

or supermarket) or a prepared meal at a restaurant or hotel. Each of the SCAs receive the PDO paper certificate together with the invoice on each carcass.

ANNEX 5 Use Case PKI setup

In a PKI there are 3 main roles and procedures for a certificate: authenticating the identity carried out by the RA (Registration Authority), issuance of certificate carried out by the CA (certification authority) and validation of certificates carried out by the VA (validation authority. A distrusting 3rd party can trust the subscriber when the digital signature is valid and the 3rd party trusts the issuer (CA). A certificate binds the public key with the identity (distinguished name) of an entity (subscriber) (Fig. 19).

Fig. 19 X.509 certificate



In the use case we need to provide products certificates so a PKI needs to be setup. The proposed PKI for the use case shall have 3 levels the root CA, intermediate CA and end user.

The root CA needs to be a most trusted entity, in this case it can be the Portuguese governmental institution IFAP (Instituto de Financiamento da Agricultura e Pescas) which is ruled in Portugal by the Agriculture Ministry. The intermediate CA needs to be a trusted certifier entity that is verified and trusted by the IFAP (Government institution), in this case the intermediate CA is the PDO association and certificer "Mirandesa". The end user shall be the certificate requester/subscriber and in the sample use case is "AgroGranjo" which is the producer/supplier in the supply chain. To establish the PKI each CA must validate and sign certificates in a chain of trust as follows. To implement the PKI and generate the certificates openSSL application was used. The openssl program is a vast library with a big number of commands, each of which often with many options and arguments. Many commands use an external configuration file where the user specifies a configuration file.

To establish the PKI we establishing the root CA, next the intermediate CA and finally the Producer certificate requests.

Product certificate generation

As described in order to univocally associate the PDO certificate with the product identification the digital certificate should include: a EPC global identifier, the governmental identifier and the PDO identifier. A sample EPC global identifier for the use case can be created to a Tag URI: urn:epc:tag:sgtin-96: 2.560123.3456001.823310118 or pure URI: urn:epc:id:sgtin: 560123.3456001.823310118 which is a valid global product identifier that can be used in any supply chain or EPCIS system. For the case of the bovine PDO we must add the SNIRA ID: PT823310118 and the Genealogy ID: EL60A02018005.

The validity of the digital certificate should follow the rules of the physical certificate (e.g., 15 days). To use X509 extensions (as defined in OpenSSL X509 V3) we use a configuration file for the CA authority (the Mirandesa organization issuing PDO certificates on their products). The Producer "Agrogranjo" generates a certificate request using opensslgenrsa-aes256\-out./private/Supplier.key.pem 4096.

In order to create the Product CSR, it is pratical to use a configuration file which includes the EPC Tag URI/SNIRA ID/Genealogy ID as follows (Fig. 20).

Note that to include the product data as a subjectAltName the otherName format is used. This is defined in RFC4043 that requires extra data should be prepended with a OID (as defined by GS1 EPCglobal Certificate Profile Specification. In the case of SNIRA and PDO IDs a private sample generated OID was provided via Windows script. The Producer "Agrogranjo" can create a CSR as follows (Fig. 21).

Now at the Intermediate CA "Mirandesa" we use following procedure to issue the certificate (Fig. 22).

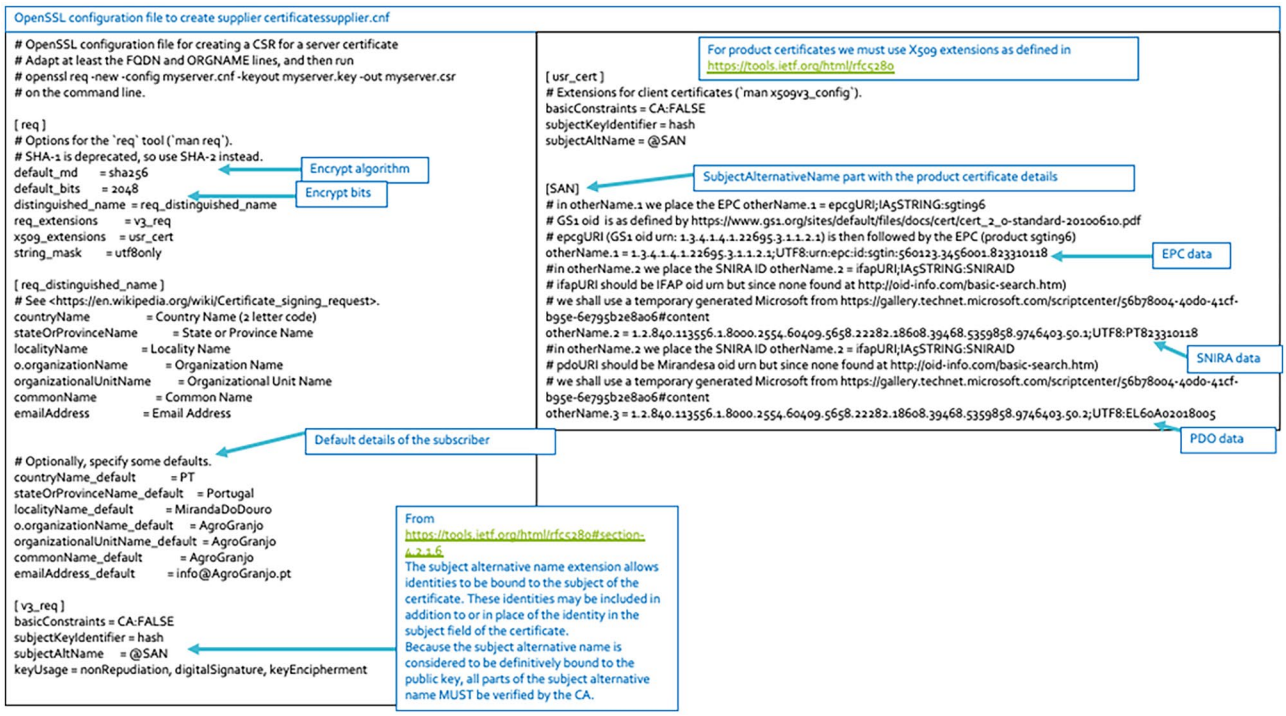


Fig. 20 CSR configuration file

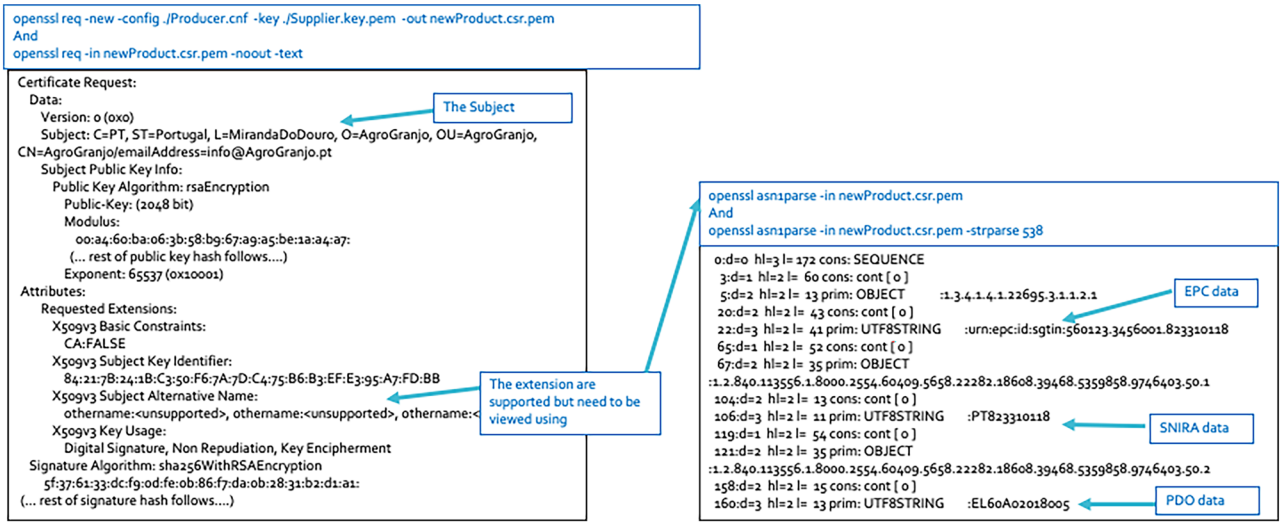


Fig. 21 Certificate Request with Product data

This valid certificate is now ready to be used in the SCM over BC, imported to WalliD provider and supplied to the SCM certificate validator for verification. For revocation of the certification the intermediate CA would create a publicly available CRL – Certificate Revocation List that is then used by the SCM certificate validator to revoke the certificate

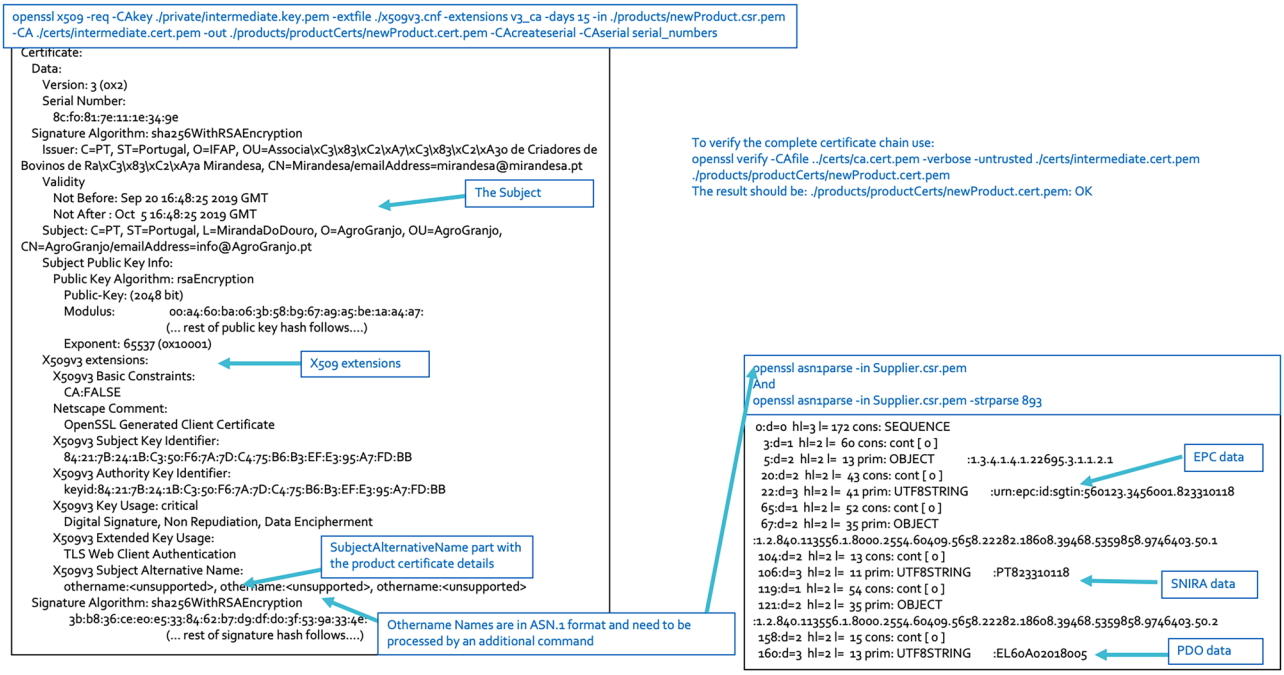


Fig. 22 Product Certificate

Funding Open access funding provided by FCT|FCCN (b-on).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

Agrawal TK, Kumar V, Pal R, Wang L, Chen Y (2021) Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry. Comp Indust Eng 154:107130

Aung MM, Change SS (2014) Traceability in a food supply chain: Safety and quality perspectives. Food Control 39:172–184. https://doi.org/10.1016/j.foodcont.2013.11.007

Berg J, Myllymaa L (2021) Impact of blockchain on sustainable supply chain practices. Master Thesis in Business Administration, Jönköping International Business School, University of Jönköping, Sweden

Cartier LE, Ali SH, Krzemnicki MS (2018) Blockchain, Chain of Custody and Trace Elements: An Overview of Tracking and Traceability Opportunities in the Gem Industry. The J Gemmol 36(3):212–227. https://doi.org/10.15506/JoG.2018.36.3.212

Casey M, Wong P (2017) Global supply chains are about to get better, thanks to blockchain. Harvard Bus Rev 13:1–6

Chang Y, Iakovou E, Shi W (2020) Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art. International J Prod Res 58(7):2082-2099 (2020). https://arxiv.org/ftp/arxiv/papers/1901/1901.02715.pdf

Cheney J, Chong S, Foster N, Seltzer M, Vansummeren S (2009) Provenance: a future history. In proceedings of the 24th ACM SIGPLAN conference on Object oriented programming systems languages and applications (pp. 957-964). ACM. http://nrs.harvard.edu/urn-3:HUL.InstRepos:5346327

Dinh T, Liu R, Zhang M, Chen G, Ooi B, Wang Ji (2017) Untangling Blockchain: A Data Processing View of Blockchain Systems. https://arxiv.org/pdf/1708.05665v1.pdf. [cs.DB]

Dobrovnik M, Herold D, Fürst E, Kummer S (2018) Blockchain for and in Logistics: What to Adopt and Where to Start. Logistics 2(18). https://doi.org/10.3390/logistics2030018

Francisco K, Swanson D (2018) The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. Logistics 2(1):2. https://doi.org/10.3390/logistics2010002

Garcia-Torres S, Albareda L, Rey-Garcia M, Seuring S (2019) Traceability for sustainability – literature review and conceptual framework. Supply Chain Manag: An Int J. https://doi.org/10.1108/SCM-04-2018-0152

GS1 Global Traceability Standard (2012) Business Process and System Requirements for Full Supply Chain Traceabilit. https://www.gs1.org/docs/traceability/Global_Traceability_Standard.pdf

GS1 Global Traceability Standard (2017) GS1's framework for the design of interoperable traceability systems for supply chains. https://www.gs1.org/sites/default/files/docs/traceability/GS1_Global_Traceability_Standard_i2.pdf

Guo H, Yu X (2022) A survey on blockchain technology and its security. Blockchain: Res App 3:100067

Hartley G, Sundermann E (2014) The Efficacy of Using the EPC global Network for Livestock Traceability: A Proof of Concept.: GS1, New Zealand

Hevner A, Chatterjee S (2010) Design Science Research in Information Systems. In: Design Research in Information Systems. Integ Series Inform Syst 22. Boston, MA, Springer

Hevner AR, March ST, Park J, Ram S (2004) Design Science in Information Systems Research. MIS Quarterly 28(1):75–105. https://doi.org/10.2307/25148625

Houben R, Snyers A (2018) Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. Policy Department for Economic, Scientific and Quality of Life Policies. Directorate-Gen Intern Policies

ISEAL Alliance (2016) Chain of custody models and definitions. London, UK. https://www.isealalliance.org/sites/default/files/resource/2017-11/ISEAL_Chain_of_Custody_Models_Guidance_September_2016.pdf

Kaur P, Parashar A (2022) A Systematic Literature Review of Blockchain Technology for Smart Villages. Arch Comput Methods Eng 29:2417–2468. https://doi.org/10.1007/s11831-021-09659-7

Keogh JG (2018) Blockchain, Provenance, Traceability & Chain of Custody. https://bit.ly/2LaJ6x7

Kim HM, Laskowski M (2018) Toward an ontology-driven blockchain design for supply-chain provenance. Intel Syst Account, Finance Manag 25(1):18–27. https://doi.org/10.1002/isaf.1424

Kros J, Liao Y, Kirchoff J, Zemanek J (2019) International Journal of Applied Logistics, 9(1)

Kshetri N (2018) Blockchain's roles in meeting key supply chain management objectives. Int J Inform Manag 39:80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Litke A, Anagnostopoulos D, Varvarigou T (2019) Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. Logistics 3(5). https://doi.org/10.3390/logistics3010005

Lu Q, Xu X (2017) Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. IEEE Software, November/December

Meidute-Kavaliauskiene I, Yıldız B, Çigdem S, Cincikaite R (2021) An Integrated Impact of Blockchain on Supply Chain Applications. Logistics 5(33). https://doi.org/10.3390/logistics5020033

Moosavi J, Naeni L, Fathollahi-Fard A, Fiore U (2021) Blockchain in supply chain management: a review, bibliometric, and network analysis. Environ Sci Pollut Res. https://doi.org/10.1007/s11356-021-13094-3

Montecchi M, Plangger K, Etter M (2019) It's real, trust me! Establishing supply chain provenance using blockchain. Business Horizons 62(3):283–293. https://doi.org/10.1016/j.bushor.2019.01.008

Pal A, Kant K (2019) Using Blockchain for Provenance and Traceability in Internet of Things-Integrated Food Logistics. Computer 52:94–98. https://doi.org/10.1109/MC.2019.2942111

PDO: Protected Designation of Origin (1992) European Comission Geographical indications and quality schemes. https://agriculture.ec.europa.eu/farming/geographical-indications-and-quality-schemes/geographical-indications-and-quality-schemes-explained_en#pdo

Perboli G, Musso S, Rosano M (2018) Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. IEEE Access 6:62018–62028. https://doi.org/10.1109/ACCESS.2018.2875782

Rahmadika S, Kweka BJ, Latt CNZ, Rhee KH (2018) A Preliminary Approach of Blockchain Technology in Supply Chain System. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 156-160), IEEE

Sahoo S, Halder R (2021) Traceability and ownership claimof data on big data marketplace using blockchain technology. J Inform Telecommun 5(1):35–61. https://doi.org/10.1080/24751839.2020.1819634

Sermpinis T, Sermpinis C (2018) Traceability Decentralization in Supply Chain Management Using Blockchain Technologies. arXiv preprint https://arxiv.org/pdf/1810.09203.pdf

Somapa S, Cools M, Dullaert W (2018) Characterizing supply chain visibility - a literature review. Int J Logist Manag. https://doi.org/10.1108/IJLM-06-2016-0150

Tavares M, Guerreiro A, Coutinho C, Veiga F, Campos A (2018) WalliD: Secure your ID in an Ethereum Wallet. In 2018 International Conference on Intelligent Systems (IS) (pp. 714-721). IEEE, Funchal, Portugal

Toyoda K, Mathiopoulos PT, Sasase I, Ohtsuki T (2017) A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access 5:17465–17477. https://doi.org/10.1109/ACCESS.2017.2720760

Wang Y, Singgih M, Wang J, Rit M (2019) Making sense of blockchain technology: How will it transform supply chains? Int J Prod Econ 211:221–236. https://doi.org/10.1016/j.ijpe.2019.02.002

Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J (2016) Untrusted Business Process Monitoring and Execution Using Blockchain. In: La Rosa M., Loos P., Pastor O. (eds) Business Process Management. BPM 2016. Lecture Notes in Computer Science, vol 9850. Springer, Cham

Westerkamp M, Victor F, Kupper A (2019) Tracing manufacturing processes using blockchain-based token compositions. Digital Commun Network 6(2):167–176. https://doi.org/10.1016/j.dcan.2019.01.007

W3C (2022) Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations. https://www.w3.org/TR/did-core/

Xu L, Chen L, Gao Z, Chang Y, Iakovou E, Shi W (2018) Binding the Physical and Cyber Worlds: A Blockchain Approach for Cargo Supply Chain Security Enhancement. In 2018 IEEE International Symposium on Technologies for Homeland Security (pp. 1-5). IEEE. https://doi.org/10.1109/THS.2018.8574184

Xu X, Lu Q, Liu Y, Zhu L, Yao H, Vasilakos AV (2019) Designing blockchain based applications a case study for imported product traceability. Future Gen Comp Syst 92:399–406. https://doi.org/10.1016/j.future.2018.10.010

Ying W, Jia S, Du W (2018) Digital enablement of blockchain: Evidence from HNA group. International J Inform Manag 39:1–4