Preprints.org

Article

Not peer-reviewed version

Collaborative Smart Production Supply Chains with Blockchain Based Digital Product Passports

Fatemeh Stodt , Nicolai Maisch , Philipp Ruf , Armin Lechler , Oliver Riedel , Christoph Reich *

Posted Date: 21 February 2024

doi: 10.20944/preprints202402.1194.v1

Keywords: digital product passport; blockchain; GAIA-X; traceability; interoperability; privacy and security; circular economy; smart industries

Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

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.

Article

Collaborative Smart Production Supply Chains with Blockchain Based Digital Product Passports

Fatemeh Stodt [1,‡], Nicolai Maisch [2,‡], Philipp Ruf [1,‡], Armin Lechler [2], Oliver Riedel [2] and Christoph Reich [1,*]

[1] Institute for Data Science, Hochschule Furtwangen University, Cloud Computing and IT-Security (IDACUS), 78120 Furtwangen im Schwarzwald, Germany; philipp.ruf@hs-furtwangen.de (P.R.); fatemeh-stodt@hs-furtwangen.de (F.S.); christoph.reich@hs-furtwangen.de (C.R.)

[2] Institute for Control Engineering of Machine Tools and Manufacturing Units (IWS), University of Stuttgart, 70174 Stuttgart, Germany; nicolai.maisch@isw.uni-stuttgart.de (N.M.); armin.lechler@isw.uni-stuttgart.de (A.L.); oliver.riedel@isw.uni-stuttgart.de (O.R.)

* Correspondence: christoph.reich@hs-furtwangen.de

‡ These authors contributed equally to this work.

Abstract: In recent years, the manufacturing sector has benefited from a variety of technological innovations regarding automation and utilization of artificial intelligence on the shopfloor. During the manufacturing processes of a product, a variety of meta data can be derived from each working step and considered during subsequent stages of its liefycle like shipment, utilization or recycling. With upcoming regulations decided by the European Union, manufacturers must begin to react to the demand of a comprehensive circular economies by introducing technical solutions like Digital Product Passports (DPP). By associating the specific conditions of all stages in the life of a product within a digital identity, e.g., the DPP, transparency and efficiency can be increased. The Gaia-X service landscape aims at realizing federated data infrastructures, enabling robust and transparent services while considering data sovereignty. In this work, a modular and generic multi-tenant framework for utilizing DPPs within cross-company ecosystems is presented with respect to the manufacturing sector. In applying the *Secret Network*-blockchain for implementing the automation of DPP management processes, premises for Gaia-X compliance and therefore strengthened trust-anchors are realized. By considering details of ecosystems, as well as most interesting security threats to the proposed architecture, a holistic view of applying DPPs in the context of smart production supply chains is shown. In presenting a simple but vivid use case of the production and compilation of car wheels, the fundamental benefits of the work on hand are underlined, once more.

Keywords: digital product passport; blockchain; GAIA-X; traceability; interoperability; privacy and security; circular economy; smart industries

1. Introduction

As part of the European Green Deal [1], regulations are being prepared for making traceable documentation of industrial and consumer goods mandatory. The aim is to facilitate the circular economy and improve overall product transparency within the European market. One intended way to achieve this goal is through mandatory digital proof of product characteristics and traceable information about the manufacturing process [2]. One of the first concrete legal requirements will be a Digital Product Passport (DPP) for automotive and industrial batteries, containing, for example, operational and performance data, a carbon footprint, maintenance and recycling information [3]. This is intended to serve as a model for implementation in other product classes of resource-intensive sectors such as construction or electronics [1]. In general, the DPP can be seen as a set of different components, which are characterized by static meta-information objects such as their fundamental design- and production procedures, as well as unique values [4]. Other key findings when considering

© 2024 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

existing systems [5] include unidirectional dataflows, as only suppliers and manufacturers create new product data. A DPP can also be interpreted as a data set that summarizes the components, materials and chemical substances, as well as information on repairability, spare parts or proper disposal regarding a specific product [5]. Current research focuses on sector-specific applications and content of DPPs instead of discussing fundamental requirements, technical architectures and integration into collaborative ecosystems [6]. In order to enable DPPs and thus strengthen the concept of an circular economy, there is a need to evaluate standards of representing product information, integrate data aggregation into business processes and enable the trustworthy exchange of collected information between trading partners. In 2020, an EU data strategy was affirmed, focusing on the regulation of two aspects in any modern digital service-landscape, e.g., services regarding the provision and processing of data, as well as trustable cloud resources [7]. In this context, the Gaia-X project aims at providing use-cases and technical concepts and architectures for Europe's next-generation data infrastructure ecosystem with focus on enabling data sovereignty, while effectively benefiting from exploiting regulated services of the common federation.

As there are usually many different stakeholders involved in production processes, there is an obvious need of collaboratively work on the DPP throughout the supply- and manufacturing-chain. The prerequisite for this is that every participant in the value chain can trust the integrity of the information it contains. However, proposed solutions for DPPs are most often stored centrally, which naturally allows subsequent manipulation as the information is in full control of a central authority. To make DPPs more trustworthy and traceable throughout the supply chain, a methodology of tracking changes to the data they contain while being tamper-proof, is required. One way to avoid centralised storage by a single party is to use Blockchain (BC) technology. In a BC, data is stored decentral and secured end-to-end using cryptographic methods. If an attempt is made to change data retrospectively, this fraud is made transparent by the algorithms used [8]. This mechanism prevents the falsification of content as soon as it is stored in a BC. The use of a BC is therefore suitable for the collaborative documentation of product features in a supply chain. Some BC implementations, e.g. [9], enable the formalisation of functional logic on the BC through smart contracts. These are based on "if, then" logic and change the state of the BC when they are called and executed [10]. This enables custom applications within an BC ecosystem, allowing their participants to interact with each other while the data used is stored in a decentralized and tamper-proof manner. In general, the functionality of a DPP can be mapped in such logic, where the pre-defined rule-set is exploited for aggregation and retrieval of information without being subject to the control of individual participants.

The contribution of this work is multi-layered, as it is clarifying requirements on DPPs in cross-company manufacturing scenarios with increased security demands. In proposing a generic BC-based architecture for configuring such product-specific passports, the secure implementation of many use-cases is made possible. By considering the architecture's security and discussing it's appropriateness in the context of a carbon-footprint scenario, a holistic view of DPPs is given in the context of collaborative smart production supply chains. In this work, a concept of how a BC can be implemented for enabling traceable DPPs is worked out and discussed with respect to the manufacturing industry. In order to gain a holistic understanding of the technological requirements on a DPP, Section 2 presents work related to the approach on hand with respect to impacting security- and technology considerations in the manufacturing sector. A general discussion of enabling the concept of DPP lifecycles in the domain of smart-manufacturing is carried out in Section 4. In addition, the utilization of presented methodologies is overviewed in Section 3 with respect to a novel, secure and BC-enabled DPP implementation, as well as an potential application within the GAIA-X ecosystem. By evaluating the shown concepts and security considerations on use cases with cross-company product-lifecycles in Section 5, a holistic view on the potential of BC-enabled DPP activity is given. Finally, the work on hand is concluded and discussed with respect to an outlook of future work in Section 6.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

2. Related Work and State-of-the-Art

Since the work on hand is based on a combination of approaches originating from different domains, the aim of this section is to give an holistic overview of existing solutions regarding DPP-specific requirements, the feasibility of potential technologies for implementing a respective framework, as well as considering surfacing security considerations. This multi-disciplinary approach is furthermore observed in the context of the main objective in the EU regulations regarding DPPs, which is to promote the so-called *R-strategies*, e.g., enabling the reuse, repair, refurbish, remanufacture and recycle of the regulated product classes [6]. According to [11] an implementation of such strategies which act as an replacement for current product End-of-Life (EoL) concepts, could save 80-90% of raw materials and energy consumption, leading to an estimated 25-30% decrease of product prices, which remains to be proven.

The concept of a DPP is also closely related to Digital Twin (DT)s, material passports and life-cycle record files. The key difference is that a DPP provides information whenever and on-demand, rather than just at the pre-defined end of a cycle [11]. Although there are various approaches of implementing lifecycle-related data structures for considering cross-tenant tracking systems [5], an common and EU-wide standard of defining DPPs is still to come. As the overall methodology of defining and applying DPP is still in a conceptual phase, technologies like BC and the Asset administration Shell (AAS) are widely applied [11], but in no way required or . The common objective of all of these technologies is information modelling for multi-tenant ecosystems [5]. Studies such as [12] discuss the various whitepapers and living documents to provide a holistic and comprehensive view of current approaches and methodologies related to DPP.

The Gaia-X project aims at creating future data platforms with focus on data privacy, as well as on the compliance of data-at-rest policies, e.g., the location in which data is stored [7]. Even within an organization, the traditional exchange of data is not always standardized, e.g., there are often *information silos* per business process or department, whereas the concept of data sovereignty aims at enforcing context-based usage constraints, definable by the respective data owners. By designing a trusted infrastructure ecosystem for standardizing service descriptions, management-capabilities and audition of federated services, a framework for managing and controlling the their overall compliance with regulations, on-boarding processes, certification, etc., is foreseen. On the other hand, the data ecosystem is focusing on securing the accountable processes with respect to a sovereign and certifiable data exchanges among different actors, utilizing the concept of data spaces which are implemented in the infrastructure services for providing or consuming information. Since the final technical service landscape of Gaia-X, and therefore the common requirements for participation, is still to be defined and standardized, there are many additional aspects to consider when designing DPP-enabling solutions in the context of the Gaia-X ecosystem. Although the work on hand is discussing a DPP-enabling framework for enabling such federated or cross-company scenarios in the broadest sense, a Gaia-X affiliation is not required at all. In addition, the approach in hand is solely utilizing BC technology for DPP-related operations, which in turn also contributes to decreasing the complexity of the overall system's setup.

2.1. Implications of DPP for Manufacturing

As there is a variety of possible scenarios which may increase the motivation of manufacturers to take part in the Circular Economy (CE), a literature review of requirements on DPPs in [11] resulted in four main-categories, e.g., *product-, utilization-, value-chain-, & sustainability-information*, and 21 sub-categories, showcasing how to potentially apply concepts in the machinery sector. Beginning with the mostly non-changeable *product information* ranging from details of physical models to certifications of standards applied during the manufacturing process. Another sub-category concerns the *utilization information* which is dynamically gathered and adjusted during the product life-cycle, e.g., different service-related data as for example energy consumption, as well as service manuals or information about spare parts. The data defined in the *value chain information* increases transparency along

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

stakeholders and enables a certain degree of automation when processing a DPP-enabled product with respect to the *R-strategies*. When gathering *sustainability information* with respect to a product, it may be an added value to apply DT technology for calculating and illustrating conclusion about the products sustainability e.g., ecological, social or circular events. Although the work on hand is considering many aspects of such an DPP design, the focus is on an approach of securing the overall DPP ecosystem and usage by presenting a BC-enabled concept.

In [13], an adaptable DPP-specific framework was proposed in an CE-enabling context, considering different technologies regarding the collection, curation, sharing, as well as leveraging of product-specific data. With respect to Internet of Things (IoT) and other *smart devices*, the collection of data may be considered in an DT implementation, where efficient monitoring can be included, too. Another aspect to take notice of is the processing of personal data, as for example the consideration of biometric information provided by personal devices for authentication, as well as enabling Machine Learning (ML)-based approaches by interconnecting databases, the detection and collection of user-specific and identifying data respectively. Next to common techniques for the curation of data by, as for example reducing background-noise or applying filters, the format for sharing information between process or organizations must be considered, too. By now, there is also a wide utilization of the BC technology as configurable processing and maintenance mechanisms are provided while a combination with 'foreign' technologies remains possible. With respect to approaches regarding *data leverage*, the term 'Piggybacking' is used for describing the utilization of business data in productive data pipelines for CE purposes. Although a concept of an adaptable and BC-enabled DPP system is presented in the work on hand, the overall focus is on the framework's dynamism and accountability in the manufacturing domain, instead of solving user-specific privacy consideration.

In [5], multiple approaches of implementing DPP-alike systems for different purposes and scenarios were analyzed. Therein, the intention of an DPP is considered as the consistent 'track-and-trace' of information with respect to a product's origin, composition, repair, dismantling options and EoL handling. In addition, such a implementation must be compatible across all involved actors. The considered DPP examples were also categorized according to their regulations, as for example the European Union (EU) *energy labeling* framework where a product is extended with a product-identifying sticker on market introduction. This already implemented approach is shaped due to other politically driven impacts as for example the referencing of European Product Registry for Energy Labelling (EPREL) data, which is mandatory to register since 2021 for a variety of energy-related products on entering the market and where energy consumption and technical aspects can be requested on-demand during usage. In extreme cases, there are also obligations where information must be provided by suppliers of products containing substances of very high concern to the European Chemicals Agency (ECHA) [5]. On the other hand, there are benefits of implementing DPP in a variety of scenarios, which is why there are some approaches of proving voluntary regulations. One of the most prominent is the material passport in building industry with focus on recycling materials when the product EoL is reached. There are other voluntary regulations, as in the case of the Cradel-to-Cradel (C2C) passport where a 3D-model depicts the kind of materials and their exact locations within large cargo-ships for recycling purposes when the boat's EoL is reached. In addition to being capable of handling the depiction of each of such approach-specific DPP information, e.g., product type-specific decisions for *r*-strategies, technical specifications like energy consumption, or location-specific material utilization, the generic architecture which is proposed in the work on hand also considers a variety of security mechanisms.

In [4], efforts for clarifying requirements on DPPs were undertaken with respect to the depiction of different lifecycle stages, performed operations and design decisions of an DPP structure, as well as it's possible utilization. Next to common advice such as investigating co-contractors components and analyzing previously developed components, the assessment of the product's replaceability in terms of material and components are basic practices when designing the data management within an DPP system. In [6], a holistic analysis of requirements on DPP-enabling systems is presented. In general,

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

a DPP is a unique document and may contain life-cycle data like the composition of a product, e.g., manufacturing processes, materials, phsyical- and chemical properties, Substances of Concern (SoC), etc., specific usage data as for example repairs or replaced components, as well as information and how to treat product components when their EoL is reached. With identifying different requirement categories fro DPPenabling systems, e.g., considerations regarding legal questions, functionality, security, interoperability, modifiability, accessibility, availability, as well as portability. Since many of the requirements apply to the approach in the work on hand, specific attention was payed to them during the architecture's design decisions, e.g., the selection of the respective BC technology, as well as pre-defined interaction specifications.

In general, there are also many additional commonalities of the information which is contained in an DPP. As the digital nameplate [14] sets the focus on static features like the manufacturer's address, name, product name and type, serial & batch number and others, there are also references to CE certification possible. For example, in Germany it is required to state the electronic voltage, current and frequency range, connection types, as well as special power supply information physically on the product. On the other hand, specific product properties [15] like the geometric or physical model containing technical data and documentation, while an behavioral model is referencing configurations, operational data, simulation models or maintenance.

2.2. Impacting Approaches and Technologies

It is becoming obvious, that the concept of applying an DPP-alike methodology has originated out of an evolution of best practices and semi-standards over the last years. Next to the heavy utilization of AAS implementations with respect to dynamic inventory management, the concepts of DT and digital nameplates are closely related to DPPs.

Digital nameplate [14] solves the problem of providing product-specific information which is directly located at a specific product and can be utilized by everyone, as they are usually applied in the form of an Quick Response (QR)-code printed on stickers, engraved metal plates or more technological solutions like Radio Frequency IDentification (RFID). A digital nameplate contains all labels which are required by law, as well as info regarding the life-cycle phases with the overall purposes of saving time and cost due to digital management, high availability and a standard-free depiction, while reducing the need for paper documentation and enhancing sustainability. With respect to a referenceable digitial identification, the concepts of Decentralized IDentifier (DID) are a promising technology for enabling DPP-based systems [6], as they are represented by an specifically structured Universal Resource Identifier (URI) [14]. Providing such verifiable credentials for a specific product will also contribute to CE scenarios while enabling cross-sectoral use-cases when participants settle upon such standardized formats. Another side-effect is the ability of providing a reference to the complete product documentation while enabling automation of information retrieval processes, their utilization in customer-specific applications, as well as the seamless communication of manufacturer and customer processes. When combining a digital nameplate system with Enterprise Resource Planning (ERP)-connectivity, error-free inventory-control is possible. When making heavy use of AAS, as proposed in [14], all information about a product and how it is connected to processes in the company may be persisted within that technology, which is shielded by organization-internal web-apps referable by the QR codes. In the context of Gaia-X, concepts like the DID are playing a vital role for creating and identifying actors and services. Although they are not specifically considered in the work on hand, they are most likely implied when conformity with Gaia-X is a requirement. In general, the work on hand can easily be extended for utilization of physical enablers like QR codes burned into the product.

In current literature and projects with association to the manufacturing domain, the AAS is the database-type of choice [5,11,15] and is sometimes called itself a DT implementation as all available product data can be placed there. The many opportunities and challenges of AAS implementations with respect to a holistic traceability for supply-chain management were discussed in [16]. The end-to-end

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

traceability of an object, e.g., service or product, is a vital instrument for validating the compliance of partners across the supply-chain, dynamic object-configurations or tackling disruptions . When for example applying the Reference Architectural Model for Industrie 4.0 (RAMI)4.0 model, differentAAS submodels can relate to different life-cycle stages of an unique asset. There are many opportunities of using AAS, as for example standardized data interfaces which enables participation across product-specific systems, as well as machine-readable data for improving automated processing steps during specific lifecycle stages. On the other hand, challenges like data non-sovereignity, inconsitences on exchange between different AAS instances, lack of consistent (global) asset identification and many others remain due to non-existing standards. In [15], a mapping between DT and AAS models is considered for implementing a virtual industrial IoT simulation system. Therein, the AAS is enabling the interoperability of an systems which spreads across companies through standardized digital representation of industrial application assets. In a way, the AAS is considered as DT-embodiment of industrial applications, e.g., exploiting concepts like object encapsulating, information integration, data interaction, re-/configuration, decision support, also enabling scenarios as for example digital nameplates. Although the work on hand does not specifically make use of an AAS, the BC technology is considered in the work on hand as trust anchor, enabling global identification of assets, while conformity with Gaia-X addresses a sovereign data exchange between organizations.

2.3. Use-Case: Carbon Footprint in Manufacturing

Since the work on hand is discussing the proposed architecture with respect to the use-case of carbon footprints within DPPs in Section 5, this section is paying special attention to existing work in this domain. By specifically considering and overviewing the information from the digital nameplate required by [17] and integrating them into the DPP [18], a more holistic view on this realistic scenario can be gained.

In [19], a scenario specifying the likely content of DPPs in industrial application is presented. Therefore, two main components are presented, a *digital nameplate* with administrational information of the product and manufacturer, as well as a *carbon footprint* with information about CO_2-equivalents that have accumulated during the production and the transport of the asset. While the digital nameplate fulfils import regulations, e.g. the CE mark, the carbon footprint provides information on the sustainability of the product, which is in line with the objectives of the European Green Deal regulations. The basis for the specific content of these two components are standardised information collections, such as [18], which specifies an information model for the content required for a digital nameplate industrial machines products. The standardisation and digitization of nameplates can simplify the collaboration within supply chains by increasing the scope of product information, leading to enhanced interoperability between participants across the supply chain. The content must comply with existing international conventions and standards for nameplates and regulations such as the EU Machine Directive [17]. The digital nameplate contains general information about the product, the manufacturer, as well as the regulations fulfilled. Therefore, the information from the digital nameplate required by [17] were primarily integrated into the DPP [18], as depicted in the following enumeration:

1. *URIOfTheProduct*: The product needs to be unambiguously identifiable using a globally URI.
2. *ManufacturerName*: The legally valid designation of the natural or judicial person directly responsible for the design, production, packaging and labeling of a product with respect to bringing it into circulation.
3. *ManufacturerProductDesignation*: Brief product description (e.g. "industrial robot").
4. *ContactInformation*: Contact to the manufacturer or an authorised service provider.
5. *ManufacturerProductType*: Characteristic of different products in a product family or special variants, e.g., an International Registration Data Identifier (IRDI) reference to a product class using [20].
6. *YearOfConstruction*: The year in which the asset was completed.
7. *Markings*: Collection of product markings and all label-specific information, e.g., the "CE" mark including the date of issue and the label file.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

A standard for the required content for a carbon footprint, as it is also utilized in the work on hand, is presented in [21]. Therein, the carbon footprint is calculated from the sum of the emissions from the production of an asset and its transport. For this, the CO_2-equivalents and the calculation method must be specified. Due to the different calculation methods used for the Product Carbon Footprint (PCF) and the Transprt Carbon Footprint (TCF), the two aspects contain different information, which is documented. According to [21], the information used for the carbon footprint of the production of an asset can be summarized as follows:

1. *ProductCarbonFootprintCalculationMethod*: This describes a standard or a method for determining the greenhouse gas emissions of a product (from a list of various standards for calculation).
2. *ProductCarbonFootprintCO2equivalent*: This summarizes all greenhouse gas emissions of a product according to the quantification requirements of standard (e.g. 17.2 kg).
3. *ProductCarbonFootprintReferenceValueForCalculation*: This describes the quantity unit of the product to which the PCF information on the CO2 footprint refers to (e.g. per piece).
4. *ProductCarbonFootprintQuantityOfMeasureForCalculation*: This describes the quantity of the product to which the PCF information on the CO2 footprint refers to (e.g. 5 pieces).
5. *ProductCarbonFootprintGoodsAddressHandover*: This indicates the place of hand-over of the goods.
6. *ProductCarbonFootprintLifeCyclePhase*: Here the life cycle stages of the product according to the quantification requirements of the standard to which the PCF carbon footprint statement refers to is categorised (e.g. raw material supply).

In order to assess the carbon footprint of the asset's transportation, the following information is collected in addition to the equivalents of points 1-5 from the PCF [21]:

1. *TransportCarbonFootprintProcess*: Processes in a transport service to determine the sum of all direct or indirect greenhouse gas emissions from fuel supply and vehicle operation (e.g. Tank-to-Wheel).
2. *TransportCarbonFootprintGoodsTransportAddressTakeover*: This indicates the place of receipt of the goods.

2.4. Security Considerations

There are many existing frameworks and approaches with varying technology stacks and security requirements which are able to fulfill the core-requirements on a DPP system. In [22], a threat analysis of a framework for the rapid implementation of cross-company scenarios was carried out with respect to BC-enabled use-cases in the manufacturing domain. Therein, a central management platform was considered as communication mechanism for decoupling different shopfloors or tenants and dynamically compiling and configuring different constellations of predefined containers from the ecosystem's repository. By analysing the framework's dataflows and assessing observed threats to the overall infrastructure, staff, as well as the business side of an organization, a high-level view of the system's security considerations was presented. Although there are many commonalities of the overall system with the work on hand, there are major differences in the requirements on a DPP-enabling application, as well as the technical differences in managing the ecosystem. In [23], a holistic enumeration and analysis of many major security incidents in the industrial sector is given while considering details of the adversarial tactics which were applied to the exploited vulnerabilities. When assessing systems where digital actions are based on physical resources or conversely, or humans are included in-the-loop, additional attention must be payed to security as not only is the attack vector is increasing, safety of personnel and the environment must be considered, too. Although this remains true for a DPP system in the manufacturing sector as the one discussed in the work on hand, only the digital security is considered since the physical environment, where the operational technology is executed, is almost always dependent on the use-case.

Whenever multi-tenant systems like the ones required to fulfill the concept of DPPs are designed, the trustworthiness and management of digital identities comes into play. Since such a problem formulation is also part of the BC paradigm in general, this choice of technology may offer an elegant

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

solution for solving applications within the federated system. In [24], many of the aforementioned aspects are considered in a review on digital wallets and cloud service identity management. With comparing self-sovereign identity to centralized, user-centric, federated and service-based identity management to different security requirements, e.g., assumptions about storage security, effectiveness of management, sharing- and storing-security, as well as their aggregation, the management of future ecosystems is depicted. Although the work on hand is not considering the assessment of a service's criticality regarding it's management of identities, the participation in the framework presented in the work on hand requires a type of digital wallet in the broadest sense, anyhow.

3. Methodology of Blockchain-based DPP

The BC technology, with its decentralized nature and immutability is a key-point to development of DPPs. The inherent attributes of BC, such as transparency, traceability, and security, make it an ideal platform for managing product information across complex supply chains. However, DPPs in terms of data privacy and confidentiality, require a careful consideration of the respective BC platform used. In the context of DPPs, privacy emerges as a paramount requirement. While transparency and traceability are essential, protecting sensitive product data and proprietary information within the supply chain is equally critical. This unique requirement necessitates a BC solution that is also able to balance transparency with privacy.

3.1. Key Features Required for Implementing DPPs in Blockchain

There are several requirements for the privacy preserving BC and DPP eco-systems [25], which must be considered when planning for a specific implementation:

- Privacy and Confidentiality: The cornerstone of any DPP system is the assurance of privacy and confidentiality. This is particularly critical for protecting sensitive data such as proprietary manufacturing processes and product compositions, which could be of high value to competitors. By ensuring data security and business confidentiality within the supply chain, DPPs can safeguard critical business information, thereby maintaining competitive advantage and trust.
- Scalability and Efficiency: As DPP systems are expected to handle high volumes of transactions and data, scalability and efficiency become paramount. This requirement is crucial for extensive supply chains, where delays or prohibitive costs can be detrimental. The ability of the DPP system to scale efficiently ensures the smooth operation and growth of the system as the product and user bases expand, without compromising on performance or cost-effectiveness.
- Interoperability: The diverse nature of supply chains means that DPP systems must seamlessly integrate with various existing systems and protocols used by different participants. Interoperability is key to creating a cohesive ecosystem where various stakeholders, regardless of their underlying technology platforms, can effectively interact with the DPP. This feature ensures that the DPP system can be universally adopted and utilized, enhancing its utility and reach.
- Decentralization and Trust: The BC's inherent feature of decentralization plays a vital role in DPP implementation. By preventing any single entity from exerting control over the DPP, a decentralized approach enhances trust among all participants. This trust is fundamental in fostering collaboration and transparency, ensuring that the DPP system is equitable and democratic.
- Smart Contract Capability: Automation is another critical aspect, achievable through smart contract capabilities. Smart contracts allow for the automation of processes, enforcement of rules, and reduction of manual interventions and errors. In the realm of DPPs, this translates to enhanced efficiency, accuracy, and reliability of operations, making the system more resilient and responsive to the needs of its users.
- Data Integrity and Security: Ensuring the integrity and security of DPP data is non-negotiable. The data must be accurate, consistent, and safeguarded against unauthorized access and tampering.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

Maintaining the credibility and reliability of DPP information is essential for all stakeholders involved, as it forms the basis of trust and decision-making within the supply chain.

- There are sector-independent requirements on DPP systems [6], as legal obligations, e.g., the compliance with regulations like ESPR, the EU 'right to repair' EPR or the General Data Protection Regulation GDPR. There is an obvious need for functional sustainability and security mechanisms, e.g., ensuring nonrepudiation, data verification, data sovereignity and the security of data storages. With clear semantics and standardized data schemas, the interoperability may be enabled, while the overall accessibility must be considered in policies and onboarding proceedings. In addition to availability, e.g., appropriate information availability including real-time data, the portability of DPPs in a variety of different software systems ensures wide applicability.
- There are requirements with respect to an efficient DPP-based supply-chain management, where the identification of all required resources for a specific scenario, as well as impacting factors are gathered and ecologically friendly materials are found. Therefore, the most feasible production chain process, as well as product-delivery, services, maintenance materials, etc., must be defined.
- There are supply-chain traceability requirements [16], which are based on events. While object-events are describing what happens to an object, as well as aggregation and transformation events, where objects are represented or combined or transaction events in which the object is involved in the process of describing ownership. Therein, data elements should includethe what, who, when, where and why of an tracebility event.

3.2. Overview of Candidate BC Platforms

Our selection process for the blockchain technology is based on [26]. They compare many platforms like Ethereum, Hyperledger Fabric, R3 Corda, Quorum, Ripple, VeChain, EOSIO, Tezos, and Stellar according to scalability, consensus, centralized, accessibility, cost and communication model. Considering the balance of the features: flexibility, enterprise-readiness, and specific industry requirements, Ethereum and Hyperledger Fabric, R3 Corda, Quorum and Secret network are selected as more versatile and adaptable choices for a wider range of industrial integration needs.

- Ethereum: Known for its robust smart contract platform and widespread adoption [27]. Limitations include lower privacy and scalability issues.
- Hyperledger Fabric: A permissioned BC offering higher control over transactions and data privacy [28]. Less decentralized, potentially limiting trust in a public supply chain context.
- R3 Corda: Designed for financial services, emphasizing privacy and security [29]. May lack some flexibility needed for broader supply chain applications.
- Secret Network: Offers encrypted data processing, balancing privacy with transparency [30]. Strong in privacy, scalability, and smart contract capabilities.
- Quorum: A permissioned version of Ethereum, improving privacy while maintaining Ethereum's strengths [31]. Balances privacy and decentralization, but privacy may not be as robust as Secret Network.

In Table 1, a comparative analysis of various blockchain platforms is presented, focusing on key aspects such as privacy, scalability, interoperability, decentralization, smart contract capabilities, and data integrity. Most important the consensus processes of each platform are highlighted, providing insight into the fundamental frameworks that control these systems. Ethereum (ETH) utilizes Proof of Stake (PoS) [32], a mechanism that selects validators in proportion to their holdings, thus reducing energy consumption compared to Proof of Work systems. Fabric employs Practical Byzantine Fault Tolerance (PBFT) [33], which offers efficient processing and high fault tolerance. R3 Corda operates on a Notary-Based system [34], centralizing trust to a lesser degree to ensure data integrity. Secret Network adopts Cosmos Tendermint [35], which is a Byzantine Fault Tolerant (BFT) consensus algorithm known for its speed and security. Lastly, Quorum uses Istanbul Byzantine Fault Tolerance (IBFT) [36], a variation of the Byzantine Fault Tolerance mechanism, customized for permissioned blockchain networks. These diverse mechanisms underpin the functional and operational differences

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

of each platform, catering to varied requirements in the context of Data Privacy and Protection (DPP) implementation.

Table 1. Comparative Analysis of Blockchain Platforms for DPP Implementation.

Feature/Blockchain	ETH	Fabric	R3 Corda	Secret Net.	Quorum
Privacy & Confidentiality	×	✓	✓	✓	-
Scalability & Efficiency	×	✓	×	✓	✓
Interoperability	✓	✓	✓	✓	✓
Decentralization & Trust	✓	×	×	✓	✓
Smart Contract Capability	✓	✓	✓	✓	✓
Data Integrity & Security	✓	✓	✓	✓	✓
Consensus Mechanism	PoS	PBFT	Notary-Based BFT		IBFT

Based on the overview shown in Table, the Secret Network stands out as the most suitable BC platform for implementing DPPs, primarily due to its unique combination of privacy, scalability, and smart contract capabilities. A distinctive feature of the Secret Network is its ability to issue viewing keys that safeguard privacy by allowing only authorized users to access the content of a block. While other platforms like Ethereum and Hyperledger Fabric offer their own advantages, they fall short in critical areas such as privacy and scalability, which are essential for the effective implementation of DPPs in supply chains. The viewing key functionality further solidifies the Secret Network's position as the premier choice for applications demanding stringent privacy controls, such as those found in supply chain scenarios.

3.3. Integration of Blockchain and Gaia-X

Gaia-X, envisioned as a federated data infrastructure, plays a pivotal role in enhancing trust in digital ecosystems. Its architecture, grounded in European values of transparency, openness and data sovereignty is offering a robust foundation for companies seeking to deploy DPPs. The integration of Gaia-X with the Secret Network, a BC known for its privacy-preserving features, presents a unique solution for managing digital product passports, as also depicted in Figure 1.

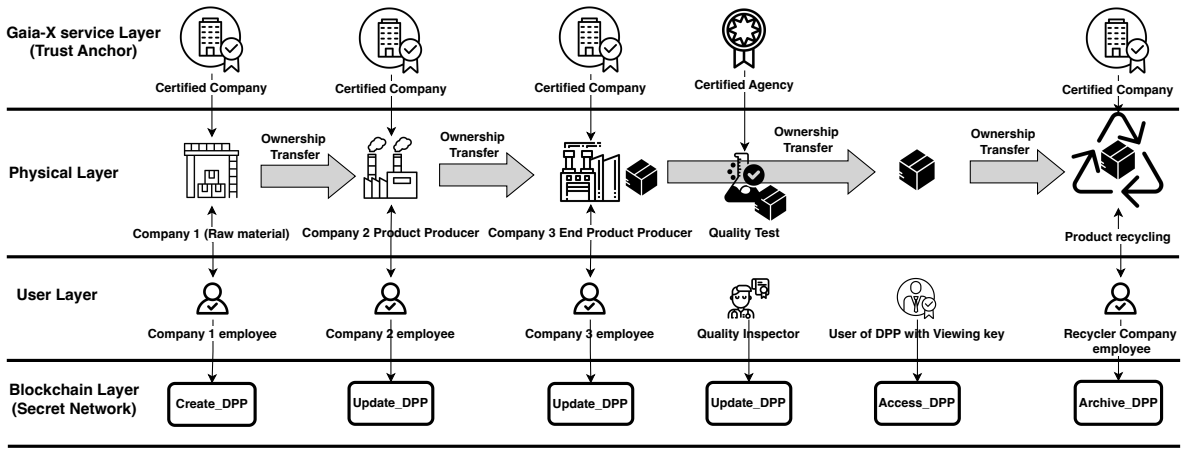

Figure 1. High-level depiction of the Proposed DPP Management Architecture using the Secret Network.

While the Secret Network provides a secure and private ledger for storing sensitive product data, Gaia-X ensures that the overarching data infrastructure aligns with regulatory standards and ethical guidelines, particularly relevant in the European Union's stringent data protection landscape. In practice, a company issuing a DPP on the Secret Network would rely on Gaia-X as the framework

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

to manage data handling processes and trust mechanisms. This model ensures that while the product data is stored securely and privately on the BC, all operations align with the broader data sovereignty principles and industry standards, fostering trust among consumers, regulators, and partners. However, this integration is not without challenges. Technical complexities in harmonizing BC technology with Gaia-X principles, scalability concerns, and maintaining a balance between transparency and privacy are critical areas to address. Ongoing collaboration between BC developers, policy makers, and industry stakeholders is essential to navigate these challenges effectively.

3.4. Proposed Architecture for Blockchian-Enabled DPP

The proposed architecture for implementing a BC-based DPP system is a confluence of advanced distributed ledger technology and Europe's Gaia-X framework for data sovereignty as it shows in Algorithm 1, which is referencing functions described in the following subsection 3.4.3. It is envisioned as a holistic, interoperable ecosystem that leverages the strengths of BC to provide a secure, transparent, and immutable record of product information, while Gaia-X acts as the custodian of trust, ensuring compliance with stringent EU regulations and standards.

Algorithm 1 Overall DPP Management Process for Creation, Storage, and Retrieval Process.

```
Initialize blockchain and Gaia-X services
Establish secure communication channels
Define Security policies
Call Create_DPP function as needed
Call Update_DPP function as needed
Call Access_DPP function as needed
Call Archive_DPP function as needed
while system is active do
    Listen for incoming data, user credentials, and access requests
    Maintain continuous security monitoring and incident response handling
end while
```

The algorithm outlined in Algorithm 1 serves as the backbone of our blockchain-based Data Product Platform, orchestrating the initialization, management, and secure operation of both blockchain and Gaia-X services. It ensures the efficient creation, update, access, and removal of DPPs, while rigorously maintaining access control and continuous security monitoring, in compliance with the European Union's stringent data sovereignty and privacy standards.

3.4.1. Components and Functionality

At the heart of the architecture lies the Product Information Module, a repository that encapsulates required facet of a product's existence. Each product is endowed with a unique identifier, that paves the way for traceability throughout its lifecycle. The module is a rich tapestry of data, from the physical and technical specifics that inform about the product's design and materials, to the usage and historical data that narrates the product's journey from creation to consumer. This historical ledger not only enhances the product's value through transparency but also serves as a crucial tool for assessing its longevity and maintenance needs.

Complementing the detailed history is the environmental impact assessment, a feature that quantifies the product's ecological footprint and underlines the commitment to sustainable practices. As the product approaches the end of its utility, the module offers a blueprint for its responsible disposal, feeding into a circular economy that values reuse and recycling.

3.4.2. Integrating Gaia-X for Trust and Compliance

Integral to this architecture is the Gaia-X Trust Layer, which imbues the system with a level of regulatory compliance and data authenticity that is unmatched. It ensures that all stakeholders can fully trust the DPP data, as it adheres to the EU's data protection and privacy standards. Moreover,

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

Gaia-X facilitates a seamless exchange of data across different platforms and entities, embodying the vision of a unified digital single market.

3.4.3. Blockchain: The Backbone of DPP Security

The architecture of the DPP begins with a foundational phase of system initialization. This phase involves setting up the BC environment, where the *Secret Network* is chosen for its advanced privacy features, crucial for handling sensitive product data. Simultaneously, integration with Gaia-X services is established, ensuring that the DPP system aligns with European data infrastructure standards, particularly focusing on data sovereignty and interoperability. This dual-setup forms the bedrock of the system, offering a balanced blend of security, privacy, and regulatory compliance.

A key component of this phase is the establishment of secure communication channels. These channels are fortified with robust encryption protocols, essential for safeguarding data transmissions within the system and preventing unauthorized access. In parallel, a security policies framework is implemented. This framework defines policies, laying the groundwork for secure and efficient interactions with the DPP system.

The architecture encapsulates four primary functions for DPP management: creation, updating, access, and removal. Each function is designed to handle specific aspects of DPP lifecycle management while ensuring data security and integrity.

The Create_DPP function is shown in Algorithm 2 and initiates the DPP lifecycle. It generates a unique product identifier for each new product, a critical feature for ensuring traceability. Product data is then encrypted using advanced encryption standards, creating a secure layer of privacy for sensitive information. This encrypted data, along with the product identifier, is incorporated into a smart contract. Before being stored on the BC, the smart contract undergoes a thorough Gaia-X compliance check, reinforcing the system's adherence to European data standards.

Algorithm 2 Create DPP Contract.

```
function CREATE_DPP(product_data)
    Generate unique_product_identifier
    Encrypt product_data using advanced encryption standards
    Create smart_contract with product_data and unique_product_identifier
    Validate smart_contract using Gaia-X compliance checks
    Store smart_contract on blockchain
    return unique_product_identifier
end function
```

The Update_DPP function is shown in Algorithm 3 and allows for modifications to existing DPPs. It involves retrieving the relevant smart contract using the product's unique identifier, verifying user credentials against security policies, and updating the product data. The updated data is re-encrypted and stored back on the BC, with all actions logged for audit purposes.

Algorithm 3 Update DPP Contract.

```
function UPDATE_DPP(unique_product_identifier, updated_data)
    Retrieve smart_contract from blockchain using unique_product_identifier
    Validate user credentials and permissions using security policies
    Decrypt existing product_data from smart_contract
    Merge updated_data with existing product_data
    Re-encrypt merged product_data
    Update smart_contract on blockchain with new product_data
    Log update event and user information for audit purposes
end function
```

The Access_DPP function is shown in Algorithm 4 and handles requests for accessing product data. It involves validating user credentials as per security policies, retrieving and decrypting the

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

required product data from the smart contract, and providing access to the data. This function is meticulously designed to ensure compliance with Gaia-X privacy policies, maintaining the highest standard of data confidentiality.

Algorithm 4 Access Control for DPP Contract.

```
function ACCESS_DPP(unique_product_identifier, user_credentials)
    Validate user credentials using security policies
    Retrieve smart_contract from blockchain using unique_product_identifier
    Decrypt product_data from smart_contract
    Validate data access against Gaia-X privacy policies
    Provide user with access to decrypted product_data
    Log access event and user information for security monitoring
end function
```

Lastly, the Archive_DPP function is shown in Algorithm 5 and facilitates the smart contract deletion of a DPP from the BC. It validates user credentials, retrieves the associated smart contract, and performs the invalidation of the contract in a manner compliant with data retention laws. This process is carefully logged for auditing and compliance.

Algorithm 5 Retrieval Process for DPP.

```
function ARCHIVE_DPP(unique_product_identifier)
    Validate user credentials and permissions using security policies
    Retrieve smart_contract from blockchain using unique_product_identifier
    Invalidate or delete smart_contract from BC
    archive event and user information for audit purposes
end function
```

This proposed system is engineered for continuous operation. It remains vigilant for incoming data, user credentials, and access requests. Depending on the nature of the incoming requests, the system dynamically calls the appropriate function, ensuring seamless management of DPPs. Integral to the architecture is a robust security monitoring system, actively detecting and responding to potential threats. This continuous monitoring, coupled with a proactive incident response mechanism, fortifies the system's resilience and reliability.

3.5. Security Evaluation

In the proposed architecture for the BC-based DPP system, security is paramount. It is critical to evaluate the security measures to ensure the integrity, confidentiality, and availability of data within the DPP. This section discusses the security assessment conducted to gauge the robustness of the DPP architecture against potential threats and vulnerabilities identified in the threat model assessment (Table 2) and visualized in the Data Flow Diagram (Figure 2).

3.5.1. Threat Modeling and Risk Assessment

In order to gain insights in the state of the architectures security considerations, a threat model was created as an first step. This involved identifying potential threat actors, cataloging various types of threats and specific malicious behaviour, such as phishing, credential theft, policy bypass, with the aim of unauthorized access to the system's exploitable vulnerabilities. Each identified threat was then evaluated for its likelihood and potential impact, allowing for a prioritized risk assessment. The preliminary outcome of this exercise is detailed in Table 2, which outlines the asset-specific threats, their impacts, as well as the corresponding mitigation strategies.

In Figure 2, we present a high-level Data Flow Diagram (DFD) that illustrates the interactions within the proposed architecture. The process begins with users interacting with the system, either by retrieving product information or submitting data requests. These interactions are closely monitored

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

for security, with a focus on data access patterns and login attempts, and the information gathered is directed to the Security Monitoring system. This component aggregates data on user login attempts, policy alterations from the Security Policies, and compliance breaches from the Gaia-X framework, an external component depicted on the rightmost side of the diagram.

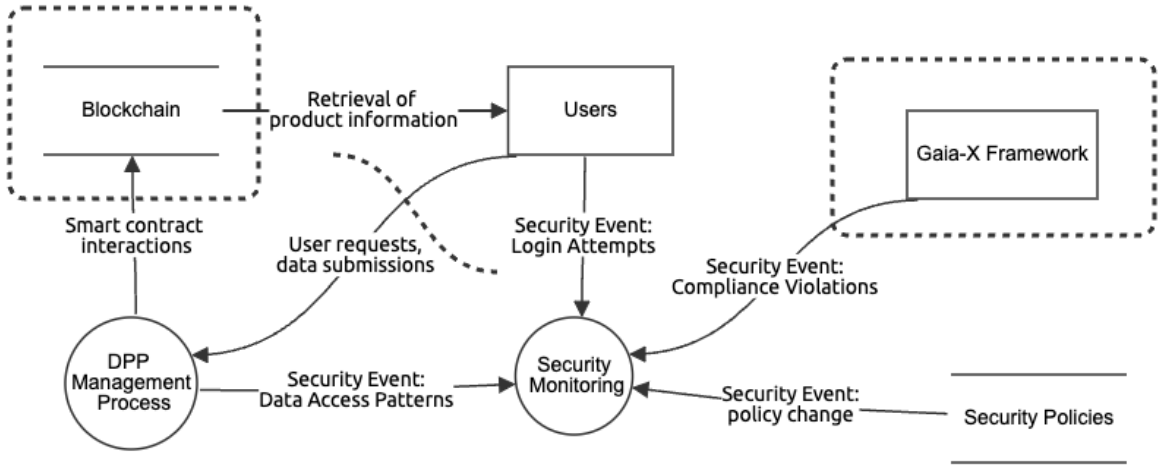

Figure 2. High-Level depiction of Data Flows in the proposed Architecture.

The DPP Management Process, connected to the blockchain, manages smart contract activities related to data privacy and security. This indicates the utilization of blockchain technology for enforcing or logging data protection regulations, thus providing a tamper-proof and verifiable record of transactions for compliance and audit purposes.

Table 2. Threat Model Assessment and Mitigation Strategies.

Asset Name	Threat Type	Impact	Mitigation Strategies
Users	Phishing, Credential theft	Critical	Secure session management, security by design with viewing key
Security Policies	Policy Bypass, Misconfiguration	High	Least privilege, Regular access reviews, Automated policy enforcement
DPP Management Process	Unauthorized Access, Data Manipulation	Critical	security by design with Secret Network
Gaia-X Service Initialization	unauthorized access during setup	High	Secure bootstrapping, Encryption at rest and in transit
Blockchain Operations	Smart Contract Vulnerabilities	Critical	Smart contract audits, Input validation and sanitization
Security Monitoring	Inadequate Detection	Critical	Continuous threat intelligence
Data Transfers	MITM Attacks, Data Interception	High	TLS, Certificate pinning, Regular certificate rotation

Table 2 presents an assessment of the key threats to this architecture and their respective mitigation strategies. This table categorizes each threat's impact on various assets and outlines tailored countermeasures. A notable aspect of this approach is the emphasis on proactive security enhancement, as illustrated by the 'security by design' principle. This is evident in strategies such as incorporating viewing keys for secure user session management and leveraging the Secret Network for the DPP Management Process. The classification of threats, such as assigning a 'Critical' rating to phishing attacks targeting 'Users' and smart contract vulnerabilities in 'Blockchain Operations',

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

reflects a comprehensive risk assessment approach. It guides the implementation of specific mitigation strategies, such as continuous threat intelligence for 'Security Monitoring' and robust encryption methods for 'Gaia-X Service Initialization'. These strategies form a multi-layered defense framework, ensuring robust protection against both internal and external threats.

3.5.2. Security Measures and Controls

The proposed architecture incorporates a layered security approach, encompassing both technological and procedural controls high-level in Table 2. By implementing such control strategies, identified threats from the threat modeling and risk assessment phase can be countered. The most impacting aspects are overviewed in the following enumeration.

- Encryption and Data Protection: Advanced encryption standards are employed to protect data at rest and in transit, a critical measure for maintaining the confidentiality and integrity of DPP data as it traverses networks and is stored within the blockchain.
- Access Control Mechanisms: Utilizing Role-Based Access Control (RBAC) and fine-grained permission policies, the system ensures that only authorized users can access or modify the DPP data. Secure session management and viewing keys are dynamically managed and thoroughly audited to prevent unauthorized data exposure.
- Smart Contract Security: Smart contracts, which enforce the business logic of the DPP on the blockchain, are rigorously tested for vulnerabilities. Smart contract audits, along with input validation and sanitization, are performed to identify and remediate security flaws.
- Gaia-X Compliance: The Gaia-X framework incorporates a regulatory compliance layer rooted in security-by-design principles. This framework ensures adherence to European regulations by implementing stringent data protection and privacy standards, such as secure bootstrapping and regular audits to safeguard data integrity.

The security monitoring processes are designed to address the threats of inadequate detection and compliance violations, with continuous threat intelligence and automated policy enforcement ensuring the system's resilience against evolving cybersecurity threats. Additionally, secure design with the Secret Network and encryption measures like TLS, certificate pinning, and regular certificate rotation are employed to protect against unauthorized access, data manipulation, and data interception during data transfers.

4. Enabling Digital Product Passports in Manufacturing

This section describes how the presented DPPs in the form of an smart contract is utilised in a manufacturing supply chain. First, a supply chain process is abstracted and the participants are generically classified. It then shows how the introduced SC functionalities are used in general business cases.

In order to bring the functionality of collaborative DPPs into a BC using smart contracts, the interactions between participants in an industrial supply chain need to be abstracted. The concept developed should be applicable to all industrially manufactured goods. Since different products go through very different production processes and supply chains, a specification of defined participants (e.g. raw material supplier, component supplier and Original Equipment Manufacturer (OEM)) or domain-specific production processes limits the scope of the DPP. Thus, the concept follows a generic approach and does not consider pre-defined roles.

[37] presents a standard to categorise the two basic participants in a generic supply chain process: suppliers, which are providing goods, and customers, receiving goods after purchase. Extending this, the participants' processes and interactions are described by the Supply-chain operations reference (SCOR) model [38]. The model extends the interaction of one buyer and one seller to an entire supply chain with an arbitrary number of trading steps and categorises not only the internal processes of organisations but also the fundamental interactions between the organisations in order to depict the activities in a functioning supply chain (Figure 3). These are [38]:

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

- *Source*: This process describes all activities realted to the ordering and receipt of goods and services.
- *Return (Customer point of view)*: The customer may identify the need to return a delivered product. The identifying, the scheduling and the execution of returning goods are summarised in this process.
- *Make*: This process describes all activities that add value to a product, such as the conversion of materials or the creation of a service.
- *Deliver*: Every activity associated with the creation and fulfliment of customer orders are described by this process, such as scheduling, shipment or invoicing the customer.
- *Return (Supplier point of view)*: This process describes all activities associated with the return of formerly delivered goods.
- *Enable*: This process describes management processes (e.g., regularity compliance, performance measurements).
- *Plan*: "Plan" processes include all activities that contribute to planning the supply chain (e.g., balancing requirements, planning capabilities).

Since *Enable* and *Plan* relate to the management of the supply chain and have no direct influence on the product as such, the work on hand is considering the remaining activities and is focusing on the abstraction of the interactions which are related to the DPP itself.

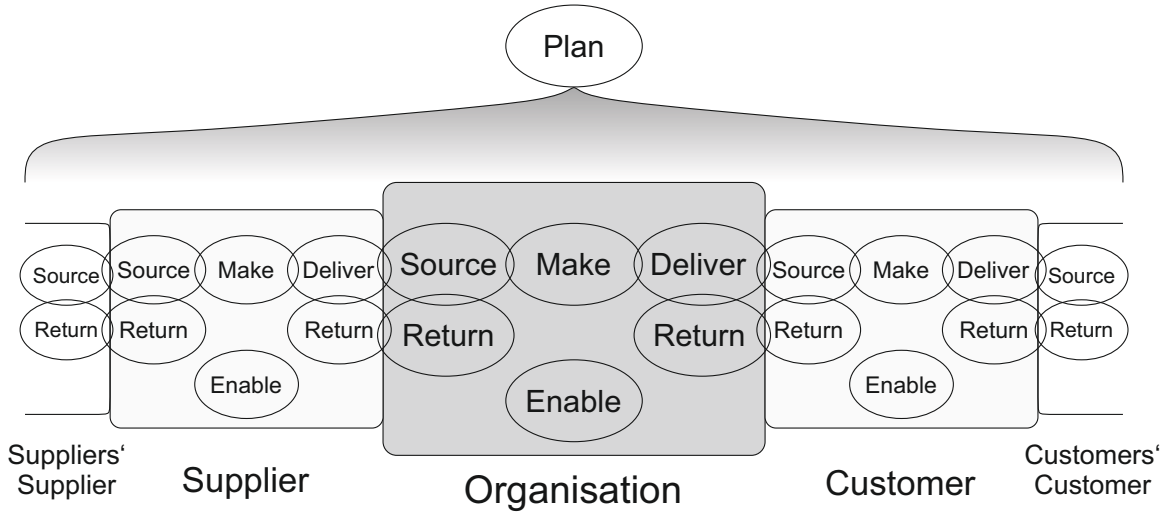

Figure 3. Fundamental Supply Chain Processes of SCOR.

4.1. Overview of a supply chain process

The supplier of a product is producing an asset and creates an according initial DPP representation, which is stored on the BC by executing Algorithm 2. Changes to the asset (e.g., milling, moulding, assembling) are documented in the DPP by updating the smart contract with Algorithm 3. The properties that are added to the DPP are always depending on the specific use-case (e.g., determining the carbon footprint of a product) and the corresponding regulations. There can be any number of references to other product passports in the DPP, for instance to preliminary products.

Each asset has an owner who is also referenced in the DPP. If an asset is sold, the customer is noted as the new owner of the asset by updating the smart contract, which results in a new state in the smart contract of the DPP. As the owner of the DPP, you can also always give partners certain access authorisations to the smart contract by running Algorithm 4. Figure 4 provides an overview of the participants in a supply chain process (supplier and customer) and their relationships to the DPP and the represented product. The participants' business functions are also depicted.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

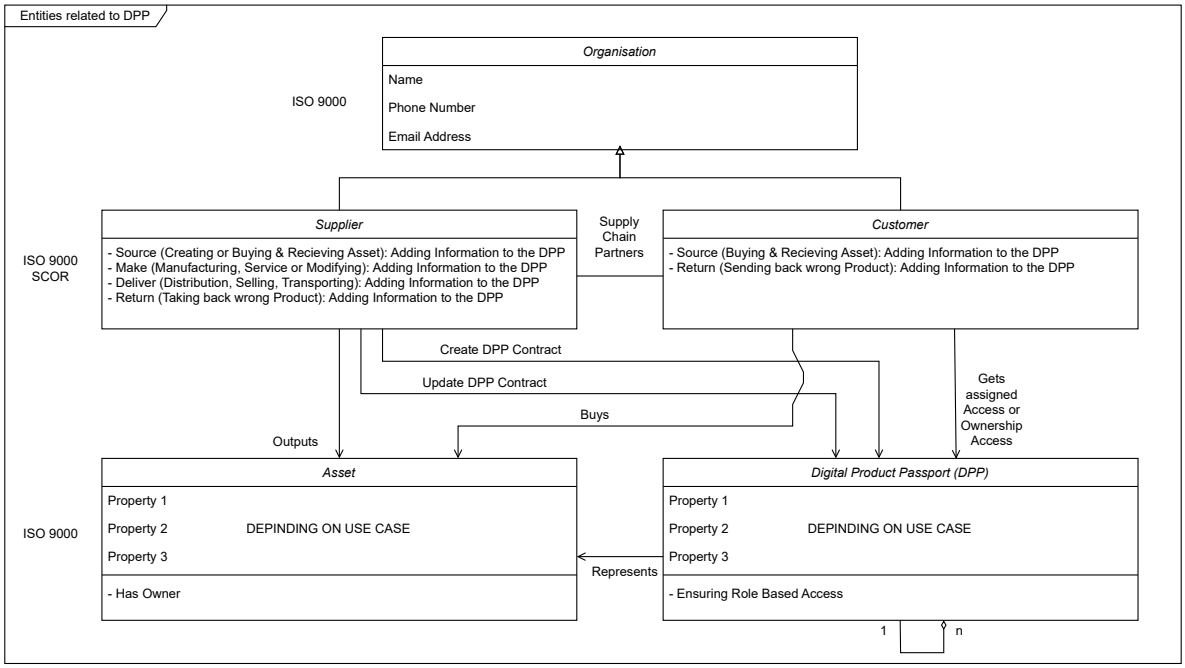

Figure 4. UML Class Diagram of Entities related to a DPP.

4.2. Source Asset

When a new asset is created, an associated DPP is created in the form of a smart contract. The supplier creates the technical framework (e.g., the encryption) and adds required information to the smart contract by using Algorithm 2. However, if an asset has been purchased and there is only a change in ownership, there is no need of creating a new smart contract. In this case updating the smart contract by the former owner is sufficient (Algorithm 4). When invoking an existing smart contract your BC-compiler will give feedback about a positive or negative invoking process. After invoking the smart contract the new owner can then update all information inside the DPP. Another option is the linking of a purchased asset to an existing asset. In this case the DPP of the existing asset is updated with a reference to the added asset. All of these options are shown in Figure 5. It should be noted that in this sequence diagram, the supplier is the customer of a previous step.

4.3. Make Asset

During the production assets are processed in various ways. Every piece of information that is generated during the processing steps can be added to the DPP by using Algorithm 3 with respective input data (Figure 6). The write access to the smart contract lies solely with the current manufacturer. However, the information actually aggregated to the DPP depends on sector specific requirements and the demands of possible customers. When added information to the DPP the manufacturer can lookup the new changes to the smart contract.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

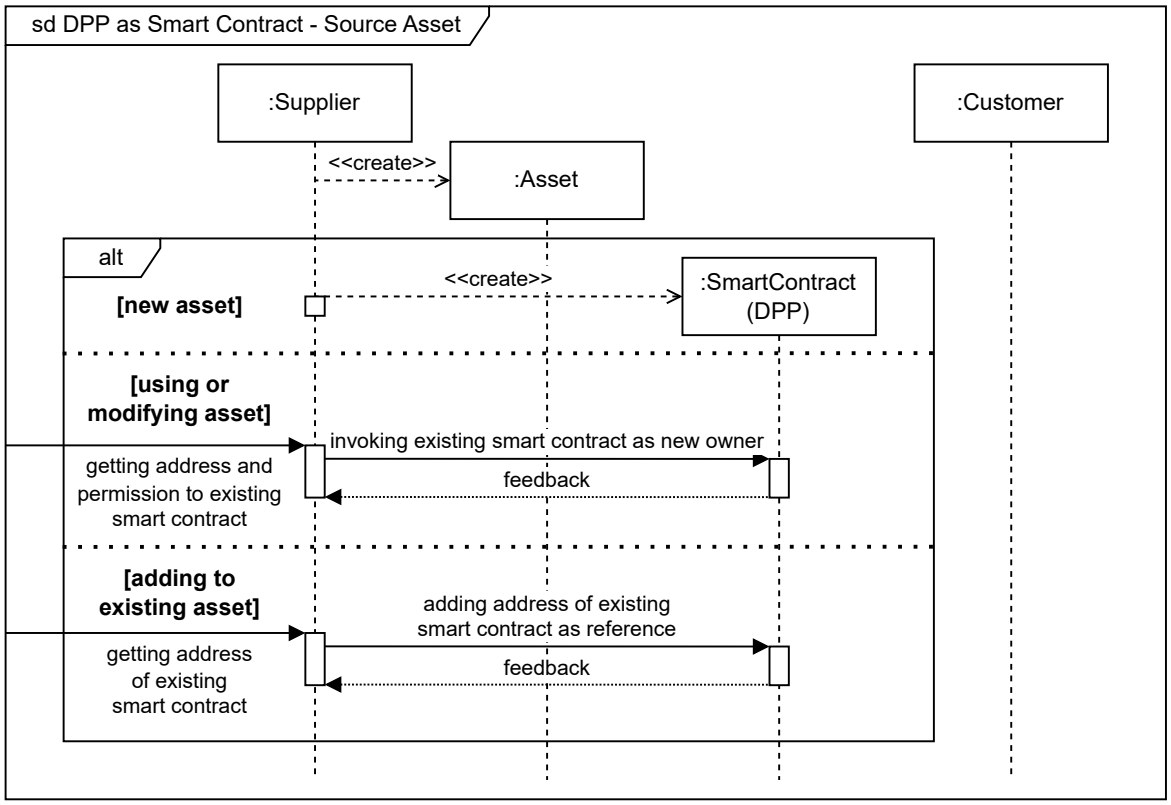

Figure 5. Sequence Diagram of Sourcing an Asset.

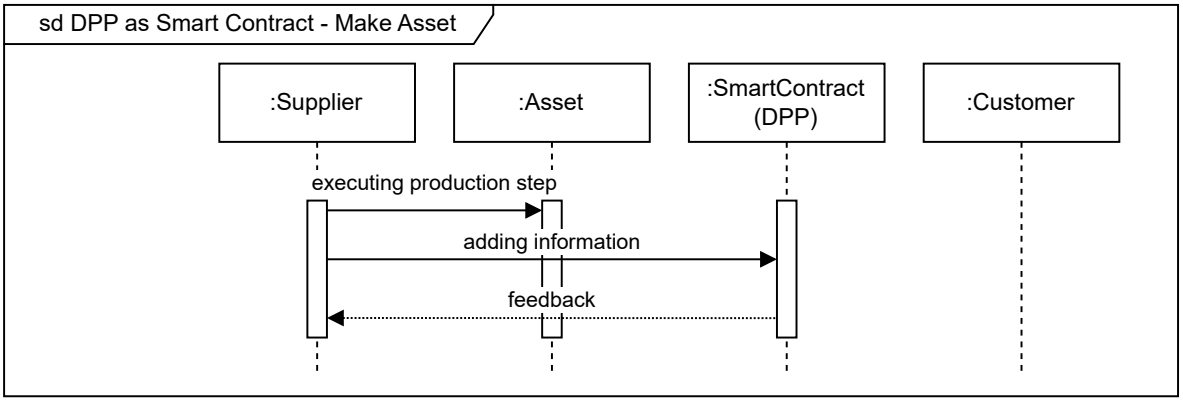

Figure 6. Sequence Diagram of Making an Asset.

4.4. Deliver Asset

During the sales phase, the supplier can give the customer a view access to the information of the DPP, so that the customer can obtain the greatest possible transparency about the product. This requires the submission of the customers BC credentials first. If the customer purchases the asset, he is declared as the new owner of the asset in the DPP by using Algrithm 4 and is now permitted for write access to the DPP. At this point in time, the supplier has no longer any access to newly added information. However, the supplier does not lose access to historical information in the DPP at the time of purchasing. The delivering process ends with sending the actual asset to the customer as depicted in Figure 7.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

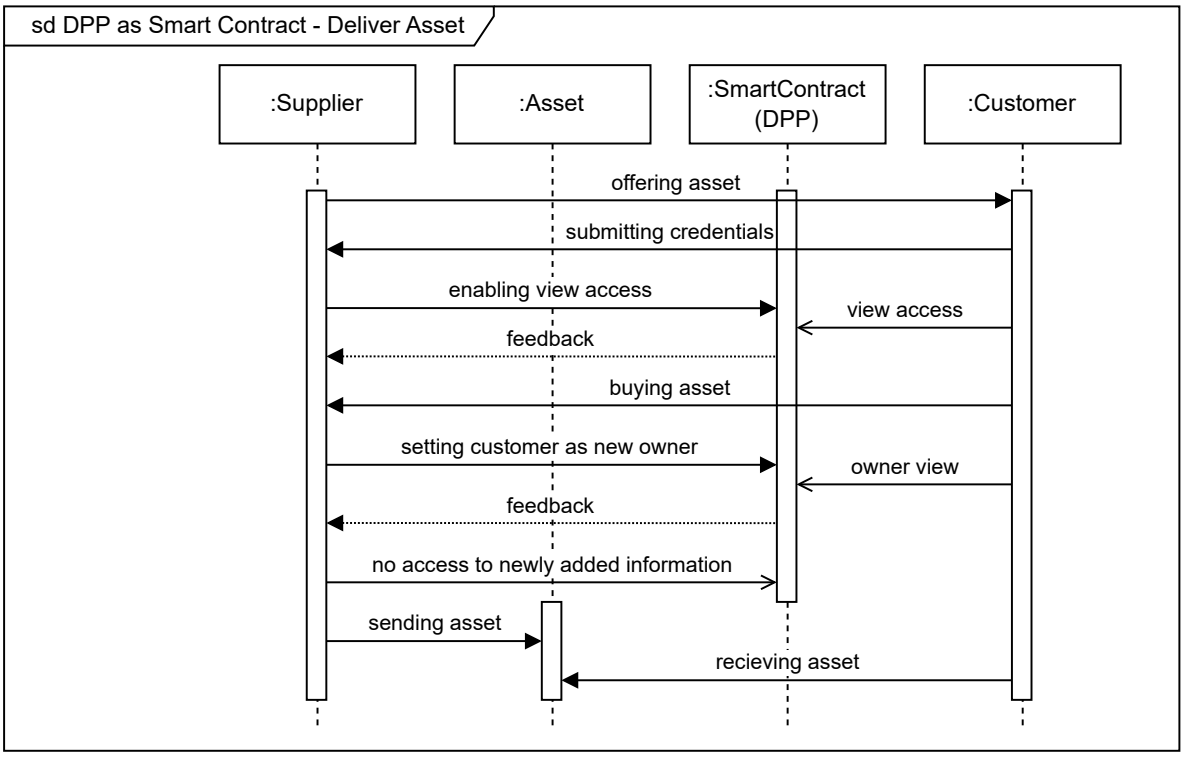

Figure 7. Sequence Diagram of Delivering an Asset.

4.5. Return Asset

The customer identifies a problem with the delivered asset and sends it back to the supplier, who accepts it and confirms the return. The supplier is given back full access rights to the DPP (Algorithm 4), as depicted in Figure 8.

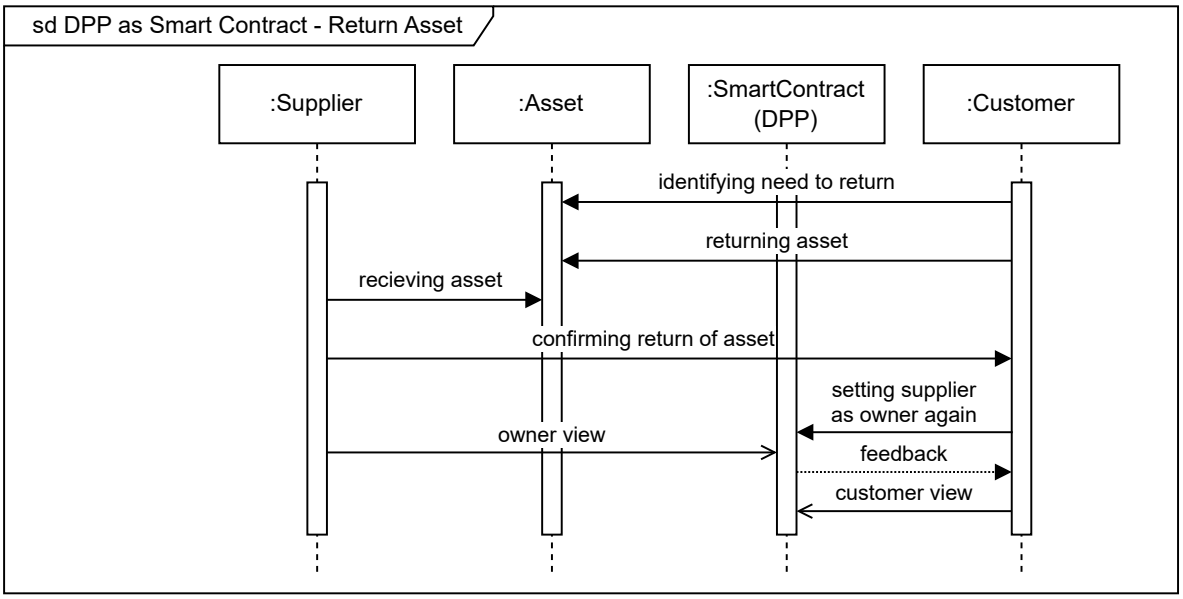

Figure 8. Sequence Diagram of Returning an Asset.

5. Evaluation by Cross-Company Product Life-Cycle Use Case

In the following, the discussion of a use case showcasing how a BC-based DPP can support the measures of the European Union ([1–3]) for the traceability of industrial supply chains is carried out.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

This shows the utilisation of the presented method in a practical sample case. The use case is oriented along the scenario of the DPP with basic and organisational information about the product and the manufacturer by a digital nameplate [18] to fit existing regulations (such as the CE marking) and carbon footprint information in order to promote sustainability of industrial products [21]. The product is accompanied by the DPP throughout the entire supply chain. Information of every executed step regarding these two topic areas are aggregated into the DPP enabled by the smart contract. The DPP therefor serves as consistent and tamper-proof documentation of the aggregated product information, as depicted in Figure 9.

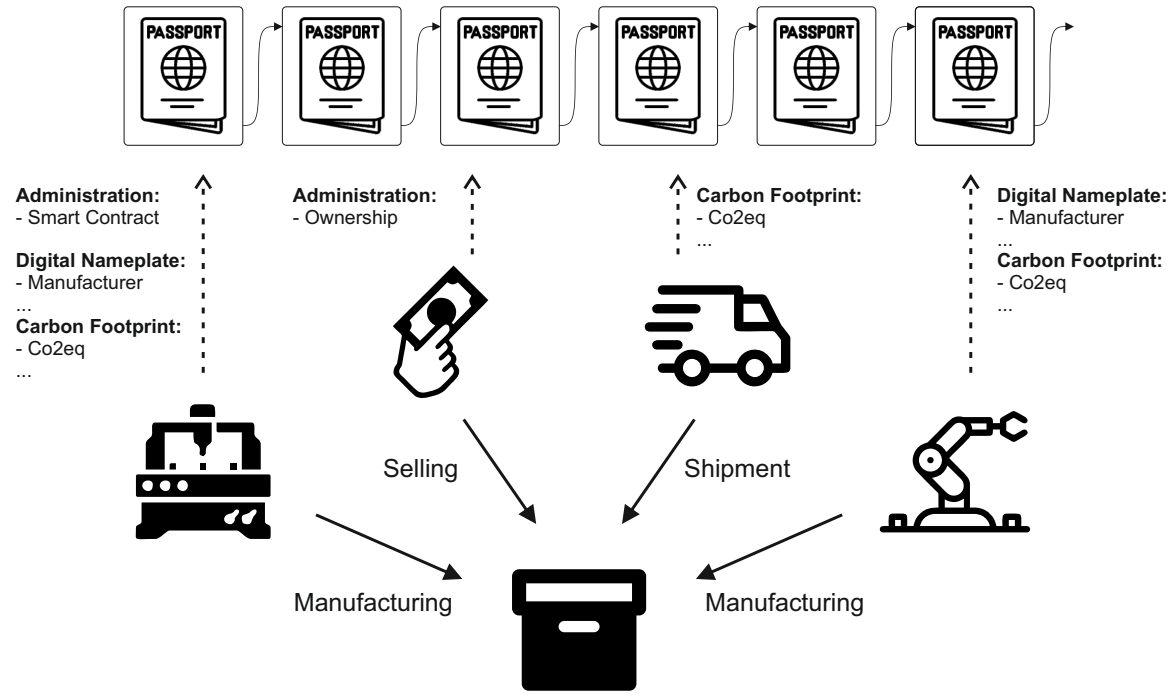

Figure 9. Overview over the life cycle product data aggregation to the DPP.

5.1. Exemplary Application of the DPP

To illustrate the use case, an example asset is the production of a car wheel. In this scenario, a company is receiving a tyre and a rim for further assembling a car wheel. However, the rim must first pass through a further processing step. In the first step, the company receives the supplies and invokes the existing DPP smart contracts as the new owner. The company now has full control over newly added information on the supplier parts. In addition, the company creates the new smart contract of the future wheel and adds general information of the digital nameplate, as illustrated in Figure 10.

The further manufacturing step is then carried out on the rim. The company documents additional CO_2 equivalents generated by the manufacturing step in the existing smart contract of the rim. After the assembly of the processed rim and the tyre, the company adds information on the carbon footprint to the DPP smart contract of the wheel. The existing smart contracts are also referenced, as the new wheel consists of these two parts, as illustrated in Figure 11.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

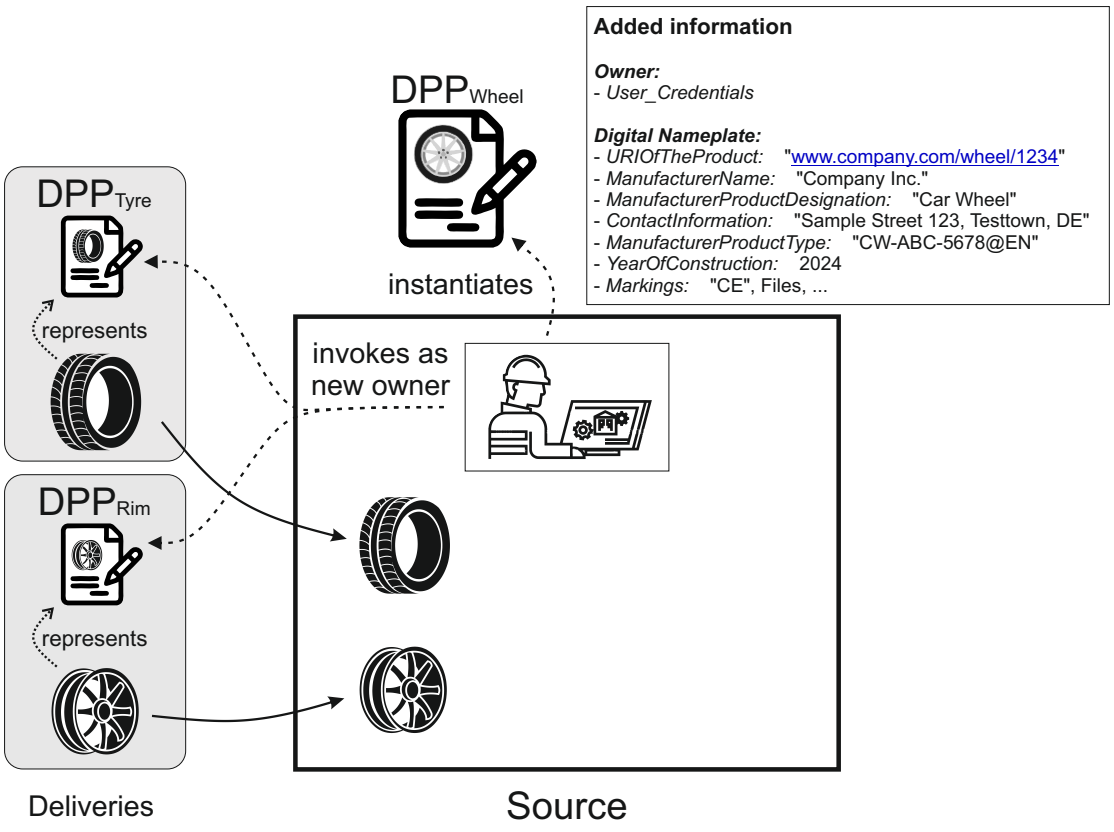

Figure 10. Sourcing of a car wheel supply chain process with information flow to the DPPs.

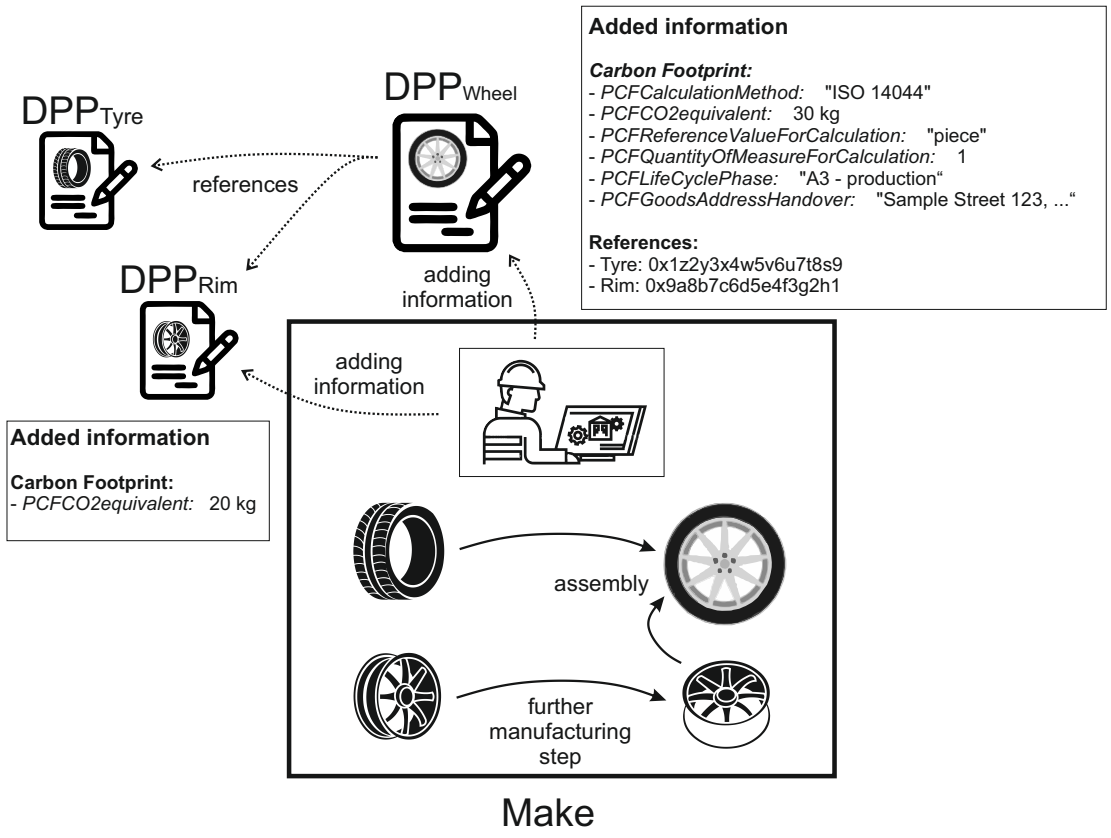

Figure 11. Making of a car wheel supply chain process with information flow to the DPPs.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

Finally, the finished wheel is packaged and shipped to the customer. The carbon footprint caused by the transport of the asset is also added to the DPP. The customer of the wheel is entered as the new owner of the smart contract after the purchase, as illustrated in Figure 12. The manufacturing company has now handed over control of the DPP and cannot make any subsequent changes. However, all information entered can be clearly traced back to it through the documentation on the BC. This ensures that even if the customer makes subsequent changes, it is clear who added this information over time. The asset and its information regarding the nameplate and carbon footprint can be clearly traced using this method.

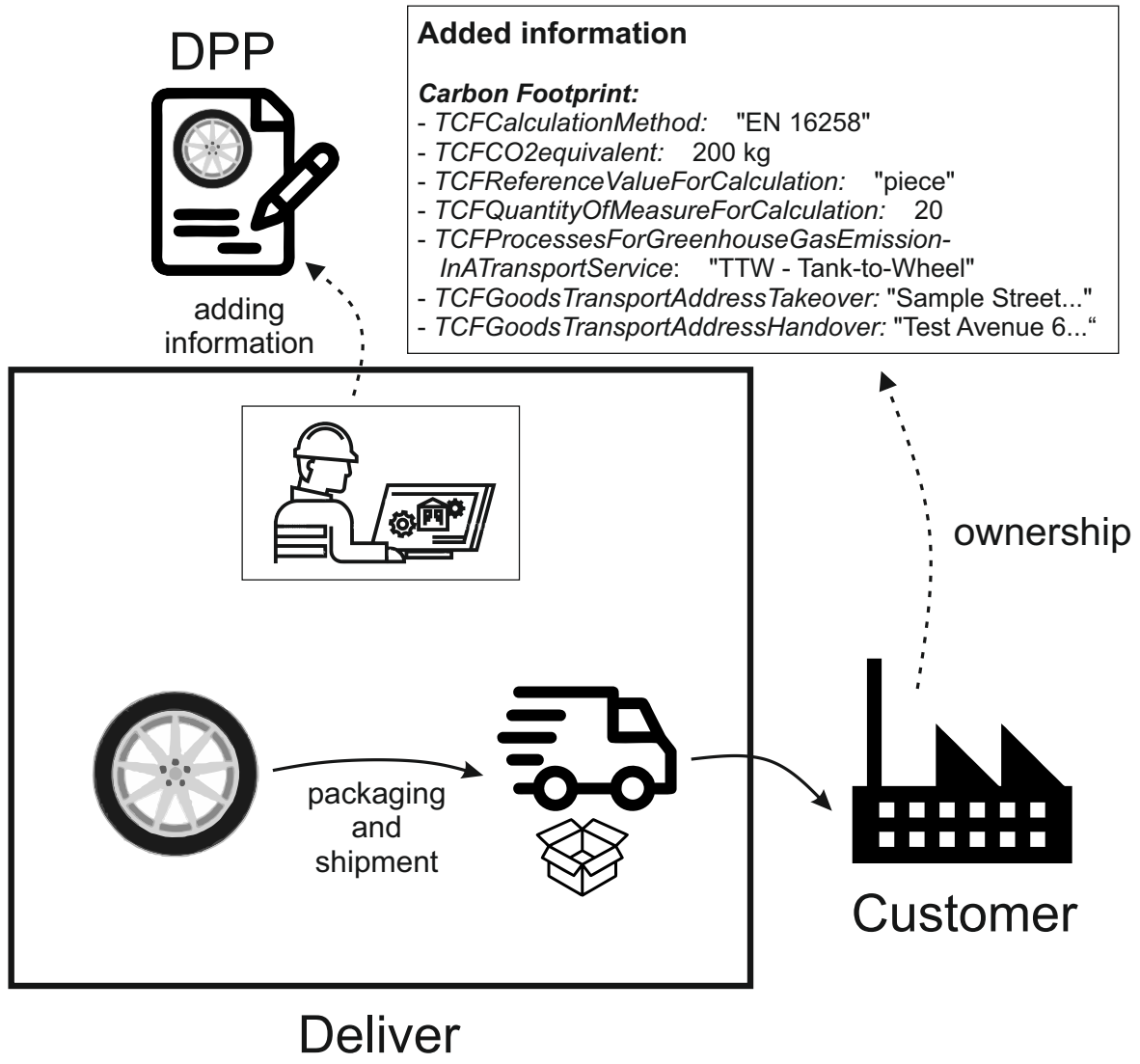

Figure 12. Delivering of a car wheel supply chain process with information flow to the DPPs.

5.2. Evaluation

This section critically evaluates the proposed Blockchain (BC)-based Digital Product Passport (DPP) system, particularly focusing on its application to the car wheel supply chain. The evaluation will consider the system's problem-solving functionality, architectural merits, and security aspects, specifically in the context of the Wheel-DPP scenario.

5.2.1. Elegance of Technology Combinations

In the Wheel-DPP scenario, the integration of *secret network* technology with the Gaia-X framework demonstrates a sophisticated blend of decentralization, transparency, and immutability of BC. This

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

is particularly relevant in the seamless tracking and validation of digital nameplates and carbon footprints of car wheel components. Smart contracts automate and enforce data access and usage policies, ensuring integrity and compliance throughout the car wheel's lifecycle, from sourcing to delivery.

5.2.2. Resource Consumption

Resource consumption is a critical factor in the evaluation of distributed system's feasibility or appropriateness. The DPP architecture is designed for efficiency, utilizing on-chain and off-chain data storage to balance the cost with performance. The on-chain components are minimized to essential transactional data, thereby reducing the bloat and associated costs of BC operation, while the off-chain components are secured via cryptographic guarantees, maintaining integrity with lower resource consumption. In addition, there is commonly only an occasional need of interaction with the DPP ecosystem, as also depicted in Figure 1.

5.2.3. Generic & Extensible Architecture

The architecture of the DPP system is both generic and extensible, capable of adapting to various industrial sectors and use-cases without the need for significant redesign. In addition, a standardized interface is provided for DPP management, while allowing for custom smart contracts and extensions to cater to domain-specific requirements. This flexibility ensures that the system can evolve alongside technological advancements and changing regulatory landscapes.

5.2.4. Gaia-X Conformity

The adherence to Gaia-X standards is particularly significant in the Wheel-DPP scenario. It ensures that data privacy and security are maintained throughout the car wheel's supply chain. The system's transparency, portability, and interoperability principles align with Gaia-X, ensuring that each step, from sourcing to delivery, adheres to European data sovereignty standards.

5.2.5. Threat Surface Minimization

In the Wheel-DPP scenario, the threat surface is significantly reduced through the implementation of privacy-preserving designs and the inherent security features of BC. Continuous verification of transactions and the elimination of single points of failure are vital in protecting against unauthorized access and data breaches, especially in the complex interactions involving multiple stakeholders in the car wheel supply chain. Regular audits and security assessments ensure the robustness of smart contracts and the overall system against vulnerabilities. A critical aspect of this scenario is the immutable nature of BC. This immutability is instrumental in reducing risks related to data tampering and fraud. Once information about a product's digital nameplate or carbon footprint is logged into the DPP, altering this information without detection becomes virtually impossible. This feature is not just a technical marvel but a fundamental aspect in fostering a culture of accountability and transparency in supply chains. Conclusion and Future Outlook

6. Conclusion and Future Work

In this work, a BC-enabled architecture for designing scenarios across multiple industrial sectors was discussed in the face of prevailing EU regulations, which make the utilization of so-called DPPs mandatory for specific products in the near future. Special attention was given to the monitoring and operation of collaborative smart production supply chains with respect to the different life-cycle stages of a product, enabling traceability and accountability. Based on the vivid and real-world use-case of *digital nameplates* and *carbon footprints* in the industrial sector, possible content and parameters of DPPs were illustrated on the basis of the proposed architecture. The adoption of BC-based DPPs in industrial supply chains, as exemplified by the car wheel supply chain scenario, aligns effectively with the EU's

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

objectives for sustainable and traceable supply chains. It is to be noted that the approach on hand is content-agnostic and therefore enables manufacturers with the freedom to decide on the content of an DPP, as it is assumed that product and industry-specific requirements and regulations are known by the respective organizations. Once a participant in the supply chain has entered information to the system, future attempts to overwrite this information, as for example the product specifications of a supplier, are mitigated by the tamper-resistant nature of the BC technology. As security-related DPP requirements [6] like non-repudiation, data verification, data sovereignty and secure data storage can also be fulfilled by existing BC frameworks, application within the proposed architecture is no coincidence. The utilized *Secret Network* BC technology not only provides smart contract functionality, scalability and ensuring of data integrity, but also enables assigning custom access authorisations by making so-called *viewing keys* available to an allowed party. In addition to the presented benefits of BC within the approach on hand, this technology can enable a collaborative ecosystem in which information is exchanged and processed via theDPP in a secure, trustworthy and straight-forward manner while being conform with Gaia-X procedures.

With respect to DPP systems, there are many gaps identified [6] which are tackled by design decisions in the work on hand, as for example the energy and resource utilization of DPP systems or their level of data privacy.

Looking forward, the continual evolution of BC technology and its integration with other emerging technologies will be pivotal in addressing the dynamic needs of industrial supply chains and regulatory frameworks. In terms of interoperability, the system may potentially benefit from a utilization of AAS as information model for exchanging the DPP data.

In conclusion, the proposed DPP system presents a robust solution that meets the specified requirements of resource efficiency, architectural soundness, and security compliance. The architecure's design addresses current and emerging threats more effectively than traditional systems, offering a forward-looking approach to digital product passport management in line with Gaia-X standards. A detailed long-term study of real-world use-cases utilizing this implementation still remains to be done.

Author Contributions: Conceptualization, F.S. and M.N. and P.R.; methodology, F.S. and M.N. and P.R.; validation,F.S. and M.N. and P.R.; formal analysis, F.S. and M.N. and P.R. and C.R.; investigation, F.S. and M.N. and P.R.; writing—original draft preparation, F.S. and M.N. and P.R.; writing—review and editing, F.S. and M.N. and P.R. and C.R.; visualization, F.S. and M.N. and P.R.; supervision, C.R. and A.L. and O.R.; project administration, C.R.; funding acquisition, C.R.; Data curation, N/A; Resources, N/A; Software, N/A, All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Federal Ministry of Education and Research (BMBF) under reference number COSMIC-X 02J21D144, and supervised by Projektträger Karlsruhe (PTKA).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not Applicable

Acknowledgments: The authors would like to thank all project partners of COSMIC-X. In Addition, the authors acknowledge comments by Samed Ajdinović from the ISW on parts of this work.

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

References

1. European Commission. The European Green Deal: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 11.12.2019.
2. European Commission. A new Circular Economy Action Plan: For a cleaner and more competitive Europe: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2020.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

3. European Parlament and EU Council. REGULATION (EU) 2023/1542 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC, 12.07.2023.
4. Donetskaya, J.V.; Gatchin, Y.A. Development of requirements for the content of a digital passport and design solutions. In Proceedings of the Journal of Physics: Conference Series. IOP Publishing, 2021, Vol. 1828, p. 012102.
5. Adisorn, T.; Tholen, L.; Götz, T. Towards a digital product passport fit for contributing to a circular economy. *Energies* **2021**, *14*, 2289.
6. Jansen, M.; Meisen, T.; Plociennik, C.; Berg, H.; Pomp, A.; Windholz, W. Stop Guessing in the Dark: Identified Requirements for Digital Product Passport Systems in: Systems 11, 123, 2023.
7. Braud, A.; Fromentoux, G.; Radier, B.; Le Grand, O. The road to European digital sovereignty with Gaia-X and IDSA. *IEEE network* **2021**, *35*, 4–5.
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
9. Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2014.
10. Introduction to smart contracts, 31.07.2023.
11. Stratmann, L.; Hoeborn, G.; Pahl, C.; Schuh, G. Classification of product data for a Digital Product Passport in the manufacturing industry **2023**.
12. Jansen, M.; Gerstenberger, B.; Bitter-Krahe, J.; Berg, H.; Sebestyén, J.; Schneider, J. *Current approaches to the digital product passport for a circular economy*; Wuppertal Institute for Climate, Environment and Energy, 2022.
13. Voulgaridis, K.; Lagkas, T.; Angelopoulos, C.M.; Boulogeorgos, A.A.A.; Argyriou, V.; Sarigiannidis, P. Digital product passports as enablers of digital circular economy: a framework based on technological perspective. *Authorea Preprints* **2023**.
14. ZVEI Recommendation: "The Digital Nameplate" - CONSISTENT, SUSTAINABLE, FUTURE-PROOF, NETWORKED, 2020. https://www.zvei.org/en/press-media/publications/zvei-recommendation-the-digital-nameplate; accessed 01-01-2024.
15. Ye, X.; Xu, W.; Liu, J.; Zhong, Y.; Liu, Q.; Zhou, Z.; Song, W.S.; Hong, S.H. Implementing Digital Twin and Asset Administration Shell Models for a Simulated Sorting Production System. *IFAC-PapersOnLine* **2023**, *56*, 11880–11887.
16. Künster, N.; Dietrich, F.; Palm, D. Opportunities And Challenges Of The Asset Administration Shell For Holistic Traceability In Supply Chain Management. 02 2023. https://doi.org/10.15488/13481.
17. European Parlament and EU Council. DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), 17.05.2006.
18. Digital Nameplate for Industrial Equipment: Submodel Template of the Asset Administration Shell: Specification IDTA 02006-2-0.
19. Garrels, K.; Grüner, S.; Schönfeld, M.; Jänicke, L.; Lamboley, P.; Martinez, B.; Gayko, J.; Holst, J.C.; Käbisch, S.; Klasen, W.; et al. ZVEI-Show-Case PCF@Control Cabinet: Product Carbon Footprint Calculation of a Control Cabinet using the Asset Administration Shell: White Paper, Mai 2022.
20. ECLASS e.V.. Einführung in den Standard. https://eclass.eu/eclass-standard/einfuehrung, 2024.
21. IDTA Carbon Footprint: Working Draft.
22. Ruf, P.; Stodt, J.; Reich, C. Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud. In Proceedings of the 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021, pp. 192–199. https://doi.org/10.1109/WorldS451998.2021.9514058.
23. Makrakis, G.M.; Kolias, C.; Kambourakis, G.; Rieger, C.; Benjamin, J. Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *Ieee Access* **2021**, *9*, 165295–165325.
24. Stodt, F.; Reich, C. A Review on Digital Wallets and Federated Service for Future of Cloud Services Identity Management. 06 2023.
25. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* **2019**, *52*, 1–34.
26. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652.
27. Buterin, V. Ethereum: platform review. *Opportunities and Challenges for Private and Consortium Blockchains* **2016**, *45*.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 21 February 2024 doi:10.20944/preprints202402.1194.v1

28. Nasir, Q.; Qasse, I.A.; Abu Talib, M.; Nassif, A.B.; et al. Performance analysis of hyperledger fabric platforms. *Security and Communication Networks* **2018**, *2018*.
29. Valenta, M.; Sandner, P. Comparison of ethereum, hyperledger fabric and corda. *Frankfurt School Blockchain Center* **2017**, *8*, 1–8.
30. Woetzel, C. Secret network: A privacy-preserving secret contract & decentralized application platform **2016**.
31. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv preprint arXiv:1809.03421* **2018**.
32. Thin, W.Y.M.M.; Dong, N.; Bai, G.; Dong, J.S. Formal analysis of a proof-of-stake blockchain. In Proceedings of the 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS). IEEE, 2018, pp. 197–200.
33. Yu, G.; Wu, B.; Niu, X. Improved blockchain consensus mechanism based on PBFT algorithm. In Proceedings of the 2020 2nd International Conference on Advances in Computer Technology, Information Science and Communications (CTISC). IEEE, 2020, pp. 14–21.
34. Xiong, A.; Liu, G.; Zhu, Q.; Jing, A.; Loke, S.W. A notary group-based cross-chain mechanism. *Digital Communications and Networks* **2022**, *8*, 1059–1067.
35. Kwon, J.; Buchman, E. Cosmos whitepaper. *A Netw. Distrib. Ledgers* **2019**, *27*.
36. Moniz, H. The Istanbul BFT consensus algorithm. *arXiv preprint arXiv:2002.03613* **2020**.
37. DIN Deutsches Institut für Normung e.V.. DIN EN ISO 9000 - Qualitätsmanagementsysteme: Grundlagen und Begriffe, Nov 2015.
38. Council, A.S.C. APICS Supply Chain Operations Reference Model: SCOR Version 12.0, 2017.

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.