Article

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: 10 May 2024

doi: 10.20944/preprints202402.1194.v2

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

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 (ISW), 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: For the purpose of improve the sustainability of products sold in the EU, Digital Product Passports is a mandatory solution. These passports would systematically gather information about products, such as detailing the materials involved to aid recycling and remanufacturing efforts, or recording the emissions produced throughout the manufacturing process. The overall goal is the establishment of a circular economy in the EU. Current research on Digital Product Passports is focused on collating content for sector-specific applications. However, achieving sustainability goals through Digital Product Passports will require new methods and technical solutions for digital collaboration between supply chain participants, especially in the manufacturing sector. Collaborative work on Digital Product Passports requires trust and traceability in data and access management to ensure privacy over the data contained. One way to enable this securely and confidentially is through the use of blockchain technology, in which stored data cannot be concealed, which is key to the traceability of digital product data documentation. This paper therefore presents a concept for the implementation of generically applicable cross-industry blockchain-based digital product passports. To this end, generic supply chain processes have been abstracted and condensed into the architecture of smart contracts. Great attention is paid to the establishment of traceability as well as privacy through the selection of the blockchain technology *Secret Network* in combination with *Gaia-X* functionalities. An illustrative use case for digital product passports in manufacturing is used to demonstrate the applicability of the presented concept. In this use case information about the digital nameplate and carbon footprint is exchanged securely and confidentially in a multi-tenant supply chain network based on the Industry 4.0 infomation model of the *Asset Administration Shell*.

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

1. Introduction

To achieve climate neutrality by 2050, the European Union (EU) aims to transform the economy as part of the European Green Deal [1]. The goal is to establish a circular economy that decouples economic growth from natural resource consumption. To drive this forward, regulations are being prepared that will require industries to provide traceable documentation of industrial and consumer goods. This is intended to allow subsequent reparation or remanufacturing processes by providing more information about the recycled assets, as well as to increase the overall transparency of the products [2]. In some sectors, such as battery manufacturing and construction or electronics, a mandatory Digital Product Passport (DPP) is intended to address these requirements, containing product characteristics and traceable information about the manufacturing process. For instance, starting in 2027, automotive and industrial batteries sold within the EU are required to have a DPP that includes operational and performance data, carbon footprint, maintenance, and recycling information [3].

 doi:10.20944/preprints202402.1194.v2

Research tends to focus on sector-specific applications and the content of DPPs, rather than discussing fundamental requirements, technical architectures and integration into collaborative ecosystems [4]. An example of this is the *Battery Pass Consortium's* specification of the DPP for batteries [5]. However, the EU notes that for such collaborative work on product data documentation throughout the entire supply chain and across company boundaries, new digital methods need to be developed to enable efficient administrative processes and build trust [1,2]. Collaboration on shared data requires trust between partners, in the technologies used, and in the integrity and traceability of the data. Proper traceability is essential for implementing cross-company DPPs. This ensures the authenticity of the data contained within the DPP and protects it against tampering by anyone earlier in the supply chain.

A potential solution is the adoption of Blockchain (BC) technology, which, due to its decentralized storage and inherent cryptographic features, renders it impossible to alter DPP information undetected. Additionally, once data is recorded on the blockchain, it becomes immutable, preventing any tampering with the contained data and ensuring vital traceability. Some BC implementations, such as Ethereum [6] to mention the most prominent, allow 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 by adding new information when they are called and executed from the real world [7]. This enables interaction with the BC, as any real-world data can be stored in a decentralised and secure BC environment. Despite the secure traceability and decentralisation, privacy of the information contained in the BC can be ensured by using encryption technologies and BCs with built-in privacy functionalities.

In the manufacturing industry, smart contracts and BC technology can be used as tools to exchange information about manufactured products in a trusted manner. In particular, the use of BC technology as a trusted and collaborative documentation platform promises to simplify storage processes when providing data from DPPs across supply chains. Figure 1 illustrates the fundamental idea of a blockchain as a collaborative documentation platform. Participants who interact with the product enter the information generated into the BC-based DPP using smart contracts. This results in consistent and traceable documentation of the collected product data, which ensures trust due to its decentralised nature and the inherent mechanisms of the BC. This requires both a holistic analysis of supply chains first and the mapping of generic processes into smart contracts, alongside being aware of their efficient executability by manufacturing companies across supply chains. It also requires technical solutions for data exchange security measures and DPP management functions to be executed by companies within the supply chain.

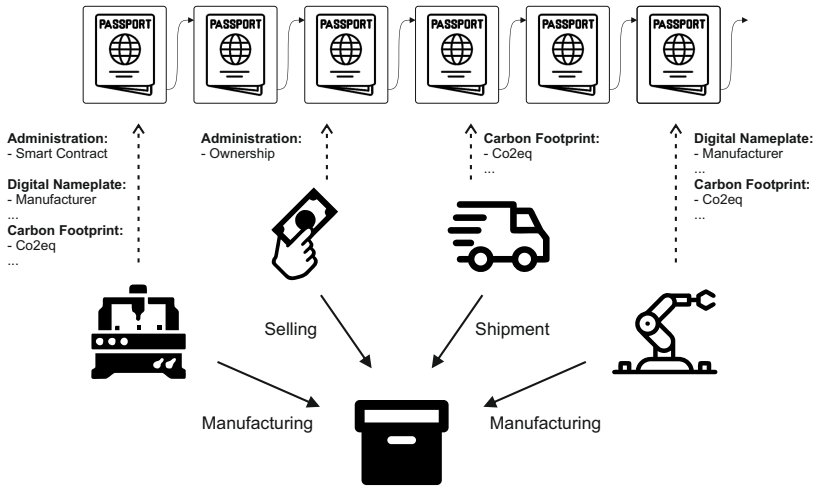

Figure 1. Overview over the collaborative lifecycle product data aggregation to the DPP

This paper contributes to filling the gap of secure and traceable collaborative methods for working on DPPs by proposing a novel framework that leverages BC technology to integrate DPP smart contract methods into manufacturing supply chains. The work underscores the potential of BC technology

 doi:10.20944/preprints202402.1194.v2

to serve as a foundational technology for creating trusted, collaborative documentation platforms. By employing decentralised storage and cryptographic mechanisms, BC ensures that DPP information remains immutable and traceable, thereby addressing key challenges of transparency, trust, and data integrity in cross-company supply chains. Furthermore, it guarantees that access to the information of a DPP can be managed and kept private while maintaining traceability.

Furthermore, our contribution includes:

- Analysis of supply chains to understand the integration points and requirements for DPP management using BC.
- The development and mapping of generic processes into smart contracts, ensuring their privacy across the supply chain.
- Proposals for secure data exchange and manage DPP functions within the supply chain, fostering trust and collaboration among stakeholders.

Therefore, this paper describes the following parts: First, the fundamentals of DPPs and BC technology are introduced to evaluate general benefits and requirements of passports implemented by this technology (Section 2). Afterwards approaches to establishing product data documentation throughout an entire supply chain and other implementations of DPPs are discussed (Section 3). This includes an introduction to widely used standards for DPP content. Section 4 presents an in-depth analysis of supply chains and the adaptability of smart contracts to the requirements of business interactions. It also presents DPP management functions that can be used to establish trust in the content of the DPP. The paper then illustrates the application of the presented concept to a use case that documents general product information and a carbon footprint of industrially manufactured products. After a security evaluation of the concepts based on the presented use case in Section 5 the work on hand is concluded and discussed with respect to an outlook of future work in Section 6.

2. Fundamentals

2.1. Digital Product Passports (DPPs)

The following outlines the background and principles of DPPs, identifies the general requirements and summarises the relevant regulations, focusing on the EU market. The main objective of DPPs is to promote the circular economy. Collecting product information in DPPs is one step towards achieving the so-called *R-strategies*, which aim to reuse, repair, refurbish, remanufacture, and recycle regulated product classes [4]. The circular economy contradicts current product end-of-life concepts, which typically involve disposing of products after their utilisation phase [8]. Implementing the R-strategies could save up to 80-90% of raw materials and reduce energy consumption, potentially resulting in a 25-30% decrease in product prices [9].

While previous market regulations focused primarily on product labelling, DPPs are intended to be a continuous and traceable collection of information throughout a product's life cycle, from production and use to repair or reuse [10]. Examples of product labelling include EU *Energy Labelling* framework, where a label identifying the product is affixed to the product when it is placed on the market [11]. In addition, the mandatory registration of a range of energy-related products in the EU's European Product Registry for Energy Labelling (EPREL) database, where energy consumption and technical aspects can be queried on demand during use [12]. Such obligations extend to cases where suppliers of products containing substances of very high concern must provide information to the European Chemicals Agency (ECHA) [13].

Although the concept of DPPs is related to these approaches, they go beyond the provision of product data in large registries at specific cycle endpoints and are more concerned with their documentation in a collaborative digital twin over the entire life cycle [8,14]. It is important to ensure that they are compatible across all stakeholders in order to enable multi-tenant tracking systems. However, the establishment of a common EU-wide standard for defining DPPs remains pending [10].

 doi:10.20944/preprints202402.1194.v2

Donetskaya et al. made efforts to elucidate the requirements for DPPs, concentrating on defining the different stages of the life cycle, operational procedures, design choices integral to DPP frameworks, and their possible applications [15]. Standard practices, such as investigating co-contractor components and analyzing previously developed components, are supplemented by evaluating the product's replaceability in terms of materials and components when designing data management within a DPP system. In general, a DPP serves as a unique document containing life cycle data such as product composition, manufacturing processes, materials, physical and chemical properties, state of charge, substances of concern, usage data like repairs or replaced components, and instructions on how to handle product components at their End-of-Life (EoL) [4]. The identification of various requirement categories from DPP-enabling systems, including considerations regarding legal aspects , functionality, security, interoperability, modifiability, accessibility, availability, and portability, underscores the multifaceted nature of these systems [16]. The development of DPP must therefore take into account both the content of the sectoral product classes and the syntactic structure and possibilities for cooperation with regard to functional and safety-related aspects.

Stratmann et al. provided meta-requirements for the content of DPPs identifying four main categories: *product*, *utilisation*, *value chain*, and *sustainability information*, along with 21 sub-categories, illustrating potential applications in the machinery sector [8]. Beginning with *product information*, which largely remains static and encompasses details ranging from physical models to certifications of manufacturing standards applied. Another sub-category pertains to *utilisation information*, dynamically gathered and adjusted throughout the product life cycle. This includes various service-related data such as energy consumption, service manuals, and spare parts information. *Value chain information* plays a crucial role in enhancing transparency among stakeholders and facilitating automation in processing DPP-enabled products, particularly concerning *R-strategies*. Gathering *sustainability information* offers added value, with digital twin technology potentially aiding in calculating and illustrating the product's ecological, social, or circular impact.

2.2. Blockchain Technology

BC technology is a decentralised, distributed ledger that records transactions across multiple node in network in a way that ensures each transaction is secure, transparent, and immutable [17]. This process involves grouping transactions into blocks, where each block is connected to the one preceding it, thereby forming a chain. Each block is validated by the network through a consensus mechanism [18], such as Proof of Work (PoW) or Proof of Stake (PoS), ensuring that each transaction is verified and agreed upon by multiple parties. This structure prevents tampering, as altering any single record would require changing all subsequent blocks and achieving consensus again, making BCs a robust and trustworthy way to record and share data across a network without the need for a central authority. This innovative technology is foundational to cryptocurrencies, such as *Bitcoin* [19], and has rapidly expanded its influence into various sectors including supply chain management, healthcare, finance and beyond. Its ability to ensure transparency, security, and integrity of data without centralised control makes it a cornerstone in the digital transformation of numerous industries [20]. The essence of BC technology is encapsulated in three core characteristics:

- Decentralisation: Unlike traditional data systems which rely on a central authority, BC operates on a decentralised model. This means that control and decision-making are distributed across all participants in the network, enhancing security, resilience, and inclusivity [21].
- Immutability: A BC consists of blocks of calculations that contain mathematical references to the preceding blocks. Therefore, once data is recorded in a block, it cannot be altered without changing all subsequent blocks and achieving consensus among network participants [22]. This is secured through cryptographic hashing, ensuring that once a transaction is recorded, it becomes tamper-evident, safeguarding data integrity.

 doi:10.20944/preprints202402.1194.v2

- Transparency and Security: Through mechanisms like public and private keys, transactions are visible to all network participants, yet sensitive information is encrypted and protected from unauthorised access [23].

Two fundamental technologies underpin the operation and reliability of BCs:

- Cryptography: The integrity of the BC is maintained through cryptographic hashes, such as *SHA-256* in *Bitcoin* [19]. These hashes create a unique and unalterable fingerprint for each block, linking them in a secure chain that guards against tampering.
- Consensus Mechanisms: The crucial element of BC's decentralised nature is the process of reaching consensus among network participants [24]. Mechanisms like PoW and PoS ensure all participants agree on the ledger's state without needing a central authority. PoW requires computational work to validate transactions and mint new blocks, while PoS selects validators in proportion to their holdings, offering a more energy-efficient alternative. Validators are financially remunerated for carrying out calculations to achieve the consensus. As a result, transactions always come with transaction costs.

The BC ecosystem is diverse, comprising [25]:

- Public BC: Networks like *Bitcoin* and *Ethereum* are open to anyone, ensuring security and transparency at the cost of scalability and energy efficiency.
- Private BC: Networks such as *Hyperledger Fabric* utilize permissioned access control, focusing on scalability and privacy. These often use consensus algorithms like Practical Byzantine Fault Tolerance (PBFT) to achieve faster transaction times and data confidentiality.
- Consortium BC: A hybrid model where control is shared among a consortium of organisations, like *R3 Corda*, which uses a notary node for consensus, striking a balance between decentralisation and efficiency.
- Hybrid BC: *Dragonchain* provides flexibility in keeping some data private while broadcasting other data to a public BC, using a combination of consensus mechanisms to serve varied business needs.

By leveraging the inherent characteristics of BC, such as immutability and decentralisation, data storage systems can achieve noteworthy levels of security and integrity [26]. This makes BC an ideal technology for applications requiring secure, tamper-proof storage and access mechanisms, from financial transactions to sensitive machine data records.

2.2.1. Smart Contract

Within the domain of BC technology, smart contracts are programs to control or document events and actions according to pre-defined contractual terms [27]. They are embedded directly into BC networks and are immutable once deployed.

Their application is instrumental for several reasons [28]: firstly, they automate the execution of agreements by automatically enforcing the terms of an agreement once pre-defined conditions are met. Secondly, by harnessing BC's inherent security and decentralisation, smart contracts ensure data integrity and prevent unauthorised access. Thirdly, the reduction of transaction costs and increased process efficiency, owing to the bypassing of intermediaries, streamline operations significantly. Lastly, the inherent transparency of smart contracts fosters trust among participants, as all parties have access to the contract terms and the assurance of execution based on consensus. In most BCs (e.g., Ethereum [6]), the contract's execution and operational data and terms are fully visible to the public, which increases transparency but significantly reduces privacy.

2.2.2. Overview of Blockchain Platforms

The survey [24] compares different BC technologies based on their scalability, consensus mechanism, centralisation, accessibility, cost, and communication model. Considering the balance of the

 doi:10.20944/preprints202402.1194.v2

features *flexibility*, *enterprise-readiness* and *specific industry requirements*, *Ethereum*, *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: Ethereum enables the development of Decentralized Application (dApp)s and smart contracts [29] by using its built-in Solidit scripting language. The network's transition from PoW to PoS aims to address scalability and energy efficiency. The platform includes a widely used built-in smart contract functionality.
- Hyperledger Fabric: Known for its modular and configurable architecture, Fabric allows for the creation of permissioned BC networks with a high degree of control over transactions and privacy [30]. Its support for chaincode in various programming languages and the ability to create private channels make it ideal for DPPs in environments where data privacy and permissioned access are paramount.
- R3 Corda: Tailored for the financial industry, Corda's design focuses on privacy and security, offering features like transaction finality and privacy through its notary architecture [31]. Its ability to interoperate with existing legal frameworks and focus on regulated industries makes it suitable for DPPs in sectors where compliance and legal conformity are critical.
- Secret Network: Secret Network is a BC designed to prioritize privacy, offering unique features that enable smart contracts to execute in a way that the data remains encrypted [32]. This capacity allows for the creation and management of private transactions and private dApps compared to those on traditional BCs where all transactions and smart contract interactions are public by default. However, it's important to note that Secret Network isn't a "private BC" in the sense that it's restricted to a select group of users or entities, like a corporate BC would be. Instead, it's a public BC with privacy-enhancing features. This means anyone can participate in the network, send transactions, or deploy smart contracts, but the content of those transactions and contracts can be kept hidden from other users, depending on how they're designed. So called *Viewing Keys* can be issued to authorise access to data stored in the BC by the respective owner.
- Quorum: As an enterprise-focused fork of Ethereum, Quorum's attempt to tailor Ethereum for enterprise use by enhancing privacy raises significant concerns [33]. Its modifications, aimed at balancing privacy with Ethereum's interoperability, may actually compromise the principles of decentralisation and transparency central to BC technology. This approach, while intended to attract dApps requiring both privacy and Ethereum's features, could fall short of addressing stringent privacy demands, potentially undermining the platform's utility and security.

2.3. Blockchain-Based DPP

The selection of BC technology for the development of DPPs is predicated on its inherent qualities decentralisation, immutability, transparency, traceability, and robust security. These attributes are pivotal for ensuring the integrity and accessibility of product information throughout complex supply chains. However, the unique challenges presented by DPPs, especially concerning data privacy and confidentiality, necessitate a nuanced approach in the choice of BC platforms [34]. It is critical to employ a BC solution that not only fosters transparency and traceability but also adeptly safeguards sensitive data and proprietary information. This dual requirement leads to the selection of BC platforms that offer a balanced approach to transparency and privacy, ensuring that DPPs can fulfill their role without compromising sensitive information within the supply chain.

2.3.1. Key Features Required for Implementing DPPs in Blockchain

There are several requirements for the privacy preserving BC and DPP eco-systems [35], 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 propri-

 doi:10.20944/preprints202402.1194.v2

etary manufacturing processes and product compositions, which could be of high value to competitors [36].

- Scalability and Efficiency: As DPP systems are expected to handle high volumes of transactions and data, scalability and efficiency become paramount [10]. 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 [37].
- Decentralisation and Trust: The BC's inherent feature of decentralisation plays a vital role in DPP implementation [4]. By preventing any single entity from exerting control over the DPP, a decentralised approach enhances trust among all participants [38].
- Smart Contract Capability: 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 [39].
- Data Integrity and Security: Ensuring the integrity and security of DPP data is non-negotiable [40]. The data must be accurate, consistent, and safeguarded against unauthorised access and tampering [41]. 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.
- Sector-independency: DPP systems should be independent of sectors, regulations, and individual customer needs. With clear semantics and standardised data schemas, the interoperability may be enabled, while the overall accessibility must be considered in policies and onboarding proceedings.
- DPP-based supply chain management efficiency: There are requirements with respect to an efficient DPP-based supply chain management [42], where the identification of all required resources for a specific scenario, as well as impacting factors are gathered.
- Supply chain traceability: Supply chain traceability requirements are based on events. Object-events describe 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 [43]. Data elements should include the what, who, when, where and why of a traceability event. The BC technology used must enable these requirements.

2.3.2. Overview of Candidate BC Platforms

In Table 1, a comparative analysis of various BC platforms is presented, focusing on key aspects such as privacy, scalability, interoperability, decentralisation, smart contract capabilities, and data integrity.

Table 1. Comparative Analysis of Blockchain Platforms for DPP Implementation

Feature/Blockchain	ETH	Fabric	R3 Corda	Secret Net.	Quorum
Privacy & Confidentiality	×	✓	✓	✓	-
Scalability & Efficiency	×	✓	×	✓	✓
Interoperability	✓	✓	✓	✓	✓
Decentralisation & 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

 doi:10.20944/preprints202402.1194.v2

keys that safeguard privacy by allowing only authorised 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 or 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. Related Work and State-of-the-Art

The following section provides an overview of the state of the art of product data documentation in manufacturing. First, the most prominent industrial digital twin of the Asset administration Shell (AAS) and its typical content with respect to a DPP is presented. Next, *Gaia-X*, a much-discussed approach that enables collaborative data processing in industry and IT while taking security measures into account, is explained. This is followed by an explanation of how BC technology can be used to complement the security measures for DPPs. Finally, approaches to implementing DPPs found in the literature, some of which also use BC technology, are presented in order to draw conclusions for the concept of a DPP presented in this paper.

3.1. The AAS: A Digital Twin for Manufacturing

In contemporary literature and projects within the manufacturing and DPP domain, the AAS emerges as the preferred database type [8,10,44]. The AAS is a standardised and machine-readable information model used to construct a digital twin that incorporates all available product data [45]. Key features of the AAS are the globally unique identification of each asset through a Universal Resource Identifier (URI) and the subdivision of technical and life cycle content into submodels. The AAS's ability to provide globally unique identification and an interoperable usable digital twin for a product makes it a viable candidate for use as a DPP. One prominent submodel is the Digital Nameplate as the central entity for providing product data documentation in manufacturing, as described in [46]. It predominantly emphasises static features such as the manufacturer's address, name, product name and type, serial and batch numbers, it also allows for references to Conformité Européenne (CE) certification, as required by the *EU Machinery Directive* [47].

Garrels et al. provide a scenario that outlines the likely contents of DPPs in industrial applications [48]. This scenario comprises two primary components: a Digital Nameplate containing administrative information about the product and manufacturer, and a carbon footprint detailing the CO_2-equivalents generated during the production and transportation of the asset. The digital nameplate serves to fulfill essential regulations, such as the CE mark, while the carbon footprint offers insights into the product's sustainability, aligning with the objectives of the European Green Deal regulations. The standardised content of the Digital Nameplate is [49]:

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 [50].
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.

The carbon footprint of a product is calculated from the sum of the emissions from the production and its transport. For this, the CO_2-equivalents and the calculation method must be specified. Due

 doi:10.20944/preprints202402.1194.v2

to the different calculation methods used for Product Carbon Footprint (PCF) and Transprt Carbon Footprint (TCF), the two aspects contain different information, which is documented in [51]:

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 [51]:

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.

3.2. Gaia-X as a Tool for Collaboratively Working on Product Data

The *Gaia-X* project endeavors to establish future data platforms prioritizing data privacy and compliance with data-at-rest policies, such as determining the location of stored data [52]. Even within organisations, data exchange is often unstandardised, leading to "information silos" within different business processes or departments [53]. The concept of data sovereignty seeks to impose context-based usage constraints defined by the respective data owners [54]. *Gaia-X* focuses on securing accountable processes for sovereign and certifiable data exchanges among various actors, utilizing data spaces implemented in infrastructure services for information provisioning and consumption. An example use case of Gaia-X is providing standard software for authorisation and authentication in digital ecosystems [55]. These standardised data exchange rules can be utilised for DPP access management functionalities and combined with the security benefits of BC technology. In practice, a company issuing a DPP on the Secret Network would rely on Gaia-X as the framework to manage data handling processes and trust mechanisms.

3.3. Enhancing Security for DPP Systems through Blockchain Technology

In the context of DPP systems, the study conducted in [56] offers a profound insight into the specific vulnerabilities, attack vectors, and potential impacts that are quintessential to BC-enabled use cases in the manufacturing domain. The research meticulously evaluates the data flow within a central management platform designed for swift cross-company implementation, highlighting threats to infrastructure, personnel, and business operations as a pivotal aspect of security considerations. Similarly, Makrakis et al. provides a comprehensive enumeration and analysis of significant security incidents within the industrial sector, focusing on adversarial tactics and vulnerabilities where digital and physical domains intersect, thus underlining the expanded attack vector and the criticality of ensuring personnel and environmental safety [57].

These findings directly inform the security framework for DPP systems, underscoring the need for tailored security measures that address unique system vulnerabilities. The DPP system, leveraging BC technology, necessitates rigorous data integrity and access control mechanisms to safeguard against the identified risks.

 doi:10.20944/preprints202402.1194.v2

Building upon these examples, we propose a structured framework that categorizes security considerations into four main aspects: data security, identity management, network security, and physical security. Each category encompasses specific risks and mitigation strategies, tailored to the DPP system. For instance, data security focuses on protecting the integrity and confidentiality of data through advanced cryptographic techniques, while identity management explores the use of use of Gaia-X authentication and authorisation methods to secure user access and interactions within the DPP ecosystem. Network security measures are designed to defend against cyber threats at the infrastructure level, and physical security ensures the safeguarding of physical assets and operational technology integral to the DPP system.

Emerging technologies such apply security policies and advanced cryptographic methods offer solutions to enhance the security of DPP systems. These technologies are pivotal in addressing the security challenges identified, providing robust mechanisms for secure data exchange and user authentication within the DPP framework.

The application of these security considerations to specific use cases within the manufacturing sector reveals unique challenges and solutions. For example, in scenarios where DPP systems interface with operational technology, the integration of physical security measures becomes paramount to mitigate risks to safety and environmental integrity.

A multi-layered security approach is advocated to address both digital and physical aspects of security comprehensively. This approach encompasses the deployment of operational technology and the critical importance of physical safeguards, aligning with the expanded scope of security considerations in DPP systems. The management and trustworthiness of digital identities are crucial in DPP systems. The review paper [58], offers valuable insights into various identity management approaches, including self-sovereign and federated models, their security requirements, and their applicability to DPP systems. This discussion underscores the importance of secure identity management in enabling secure and efficient user interactions within the DPP ecosystem. Lastly, a comparative analysis of different security frameworks or models applicable to DPP systems highlights the pros and cons of each approach. This analysis aids in justifying the selection of a security framework that best aligns with the unique requirements and challenges of the DPP system, ensuring a balanced approach to security and usability.

3.4. State of the Art: Digital Product Passports

The inception of DPP represents a pivotal shift towards realizing the principles of the Circular Economy, propelled by the integration of Distributed Ledger Technology (DLT) and smart contracts. These innovations promise to revolutionize transparency, traceability, and the management of sustainable product life cycles. Our review synthesizes critical research and initiatives, tracing the evolution of DPPs and assessing their impact on diverse stakeholders.

Despite the considerable advancements, existing frameworks exhibit significant deficits in fully achieving the Circular Economy's objectives. This section delineates these gaps, focusing on the deficiencies related to DPP content, collaborative methodologies without BC, and the overarching need for privacy enhancement in BC applications.

3.4.1. Deficits in DPP Content and Collaboration Methods

Nowacki et al. provide an initial framework for DPP development across sectors, emphasizing the role of DLT and smart contracts in standardizing DPPs and enhancing product transparency [59]. However, their exploration reveals a glaring omission of collaboration methods within the DPP context, a critical element for fostering a truly interconnected Circular Economy ecosystem. Moreover, while acknowledging the potential of DPPs in facilitating circular practices through secure data exchanges, they highlight significant challenges in privacy and security, alongside the pressing need for regulatory standardisation. These challenges underscore the inadequacy of current approaches in addressing the comprehensive needs of DPP stakeholders. Adisorn et al. critique DPP design options

 doi:10.20944/preprints202402.1194.v2

and their implications for stakeholders, championing DPPs that empower informed sustainability decisions [10]. They identify a critical gap in data generation and the lack of sector-specific adaptations, underlining the urgent need for extensive research to refine DPP solutions for effective Circular Economy contributions.

3.4.2. Blockchain Integration without Comprehensive Privacy Support

The application of DLT within the Circular Economy, demonstrated through a prototype by Falco et al., illustrates the potential of technology in enhancing product and material traceability [60]. Despite showcasing DLT's capability, the initiative admits to the technical complexities and the essentiality of industry-wide collaboration, without fully addressing the privacy concerns inherent in BC applications. Saleheen et al. explores the integration of BC with DPPs in the textile sector, emphasizing standardised, transparent information sharing for supply chain collaboration and consumer trust [61]. The research underscores the potential of BC-enhanced DPPs yet falls short of proposing solutions that ensure user privacy throughout the product life cycle. Lastly, Voulgaridis et al. aim to integrate DPPs with IoT technologies, providing a roadmap for data traceability in sustainability efforts [39]. However, their framework, while ambitious, lacks a clear strategy for addressing privacy concerns, a critical element for widespread adoption and technological maturity.

Table 2. Comparative Analysis of Studies on Digital Product Passports

Study	Method Used	Blockchain	Area of Applying DPP	Privacy Preserving	Secure	Scalable	Decentralised
[59]	Framework Development	Yes	Various Sectors	Not Specified	Yes	Yes	Yes
[10]	Mixed Methods (Desk Research and Stakeholder Workshops)	Not Specified	Sustainable Development, Circular Economy	Not Specified	Not Specified	Not Specified	Not Specified
[61]	Qualitative Exploratory Design (Interviews)	Yes	Textile Industry	Not Specified	Yes	Not Specified	Yes
[60]	Technical Solution Development	Yes	Recycling, Circular Economy	Not Specified	Yes	Yes	Yes
[39]	Systematic Literature Review	Not Specified	Digital Circular Economy	Not Specified	Not Specified	Not Specified	Not Specified
Ours	Technical Solution Development	Yes	Digital Circular Economy in industry	Yes	Yes	Yes	Yes

3.4.3. Addressing the Gaps: The Need for Privacy-Enhanced DPPs

Table 2 shows comparison of related works. The comparative analysis of studies on DPPs highlights a consistent trend: while there's a collective momentum towards leveraging technology for sustainable product life cycle management, significant gaps remain. These include a lack of effective collaboration methods, incomplete integration of BC technology without addressing privacy concerns, and the absence of a unified approach to regulatory standardisation.

Our contribution to the field of DPPs lies in recognizing and addressing these gaps. We advocate for the integration of the Secret Network within DPP architectures to ensure privacy by design. Unlike

 doi:10.20944/preprints202402.1194.v2

existing BC solutions, the Secret Network offers privacy-preserving smart contracts, enabling encrypted data processing and storage. This innovation is pivotal for DPPs, ensuring that while transparency and traceability are maintained, sensitive data remains protected, addressing a critical deficiency in current DPP implementations.

In summary, the exploration of the state of the art in DPP research underscores the imperative for innovative technologies to be seamlessly integrated with Circular Economy practices. However, for DPPs to truly effectuate sustainable product life cycle management, the identified gaps particularly in collaborative methodologies, BC integration without privacy, and regulatory standardisation must be bridged. Our research posits the integration of privacy-enhancing technologies, such as the Secret Network, as a cornerstone for future DPP solutions, aiming to reconcile the need for transparency with the indispensable requirement for privacy.

4. Blockchain-Enabled DPPs in Manufacturing

In the following, a concept for a BC-based DPP is presented. The aim is to create a technical framework for collaborative processing of DPPs that can be used to document product data in a traceable way to facilitate the circular economy and to store sustainability information about products. Centrally managed systems can be used to provide collaborative platforms and store the relevant information about products [10,60]. However, a central system requires agreement on one provider across the entire supply chain. This provider would also have to guarantee the existence of the DPP at any point in the life cycle of a product, even years after the first sale. In addition, the provider of the central DPP service could view, lose or manipulate the data at any time, as they have control and access to the data and need to manage it properly. The use of decentral BC technology is therefore suitable for the DPP use case, as data on a BC is tamper-proof due to its inherent mathematical and cryptographic functions, and does not require a centralised service provider with full control over the data. In addition, the data cannot be lost, so users of the system throughout the supply chain can be sure that the data it contains is correct, or can trace who changed what data and when.

BC technology itself has its natural strengths in the immutability of the information it contains. If the chosen BC is public, it can be accessed and viewed by anyone. In order to enable a practical BC-based system for DPPs, a solution must be found to the fact that participants in a supply chain have no interest in making all of their product data generally accessible for economically understandable reasons. The approaches mentioned above [59], [62] solve this problem by using private BCs to manage access to the information. However, this works against the general accessibility and the advantages of decentralised systems that make traceability possible in the first place. Another important aspect of the presented concept is therefore the creation of information privacy through the use of the basic technologies *Secret Network* and *Gaia-X* and a role-based access control of the DPP.

To meet the collaborative and practical functional requirements of a system for establishing DPPs, ways must be found to interact appropriately with the BC used. The technical barriers and complexity of the system must be as low as possible to enable all participants in a supply chain to work with BC-based DPPs. In addition, the functionalities developed must be generically applicable to all functional and life cycle phase-dependent differentiated use cases in all sectors of the manufacturing sector, to avoid excluding certain cases. 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 business roles.

Smart contracts are suitable for the application in DPPs due to their clear functional rules, as the functionalities of a smart contract are generally visible and cannot be falsified. To achieve this, methods must be found to integrate smart contracts into supply chain processes that are as generic as possible. Through such a system, all supply chain participants in the production of a product can work on

 doi:10.20944/preprints202402.1194.v2

a collaborative DPP to secure the information needed to meet circular economy and sustainability requirements in a decentralised BC (Figure 1).

4.1. Systemic Requirements for Generic DPPs in Manufacturing Supply Chains

Smart contracts are the formalisation of business rules into code that is executed through the BC. In order to create smart contracts for DPPs, it is essential to understand the supply chain processes and derive the required functionality. This section therefore presents a framework for distilling supply chain interactions, which is intended to serve as a functional basis for the development of a generic smart contract for a DPP. In order to develop this interaction framework, it is also necessary to identify the stakeholders and entities involved in supply chain interactions.

4.1.1. Abstraction of Supply Chain Business Processes

[63] 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 [64]. The model extends the combination of one buyer and one seller to an entire supply chain with an arbitrary number of trading steps and categorises the fundamental interactions between the organisations in order to depict the activities in a functioning supply chain (Figure 2). These are [64]:

- *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.

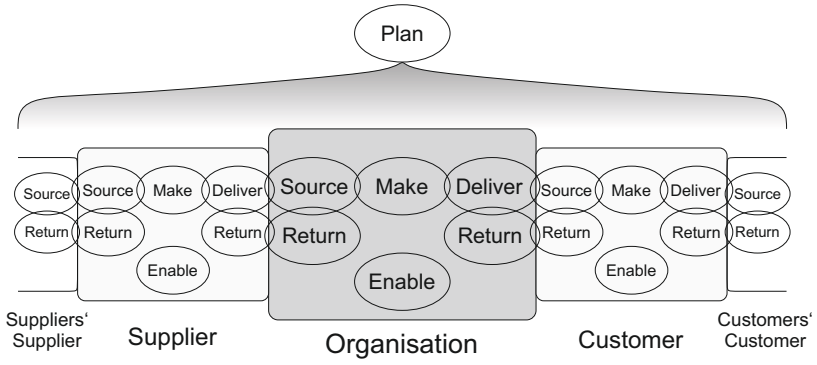

Figure 2. Fundamental Supply Chain Processes of SCOR

 doi:10.20944/preprints202402.1194.v2

4.1.2. Integration of Supply Chain Functionalities into Smart Contract-Based DPPs

Both [63] and [64] abstract interactions within supply chains as interactions between a supplier and a customer. The phase of the supply chain in which the interaction takes place (from primary to final product) and the type of company involved (e.g., raw material supplier or OEM) are irrelevant. The approaches can therefore be used as the basis for a generic framework for classifying supply chain interactions. According to [64], suppliers and customers can be assigned the universal supply chain interactions related to the traded product (Figure 3, *Supplier & Customer*). The supplier must first *source* an asset, can then process the asset (*make*) and *deliver* it. The customer must also *source* the asset after it has been delivered and, if necessary, *return* it. In this case, the customer must also become active again (*return*).

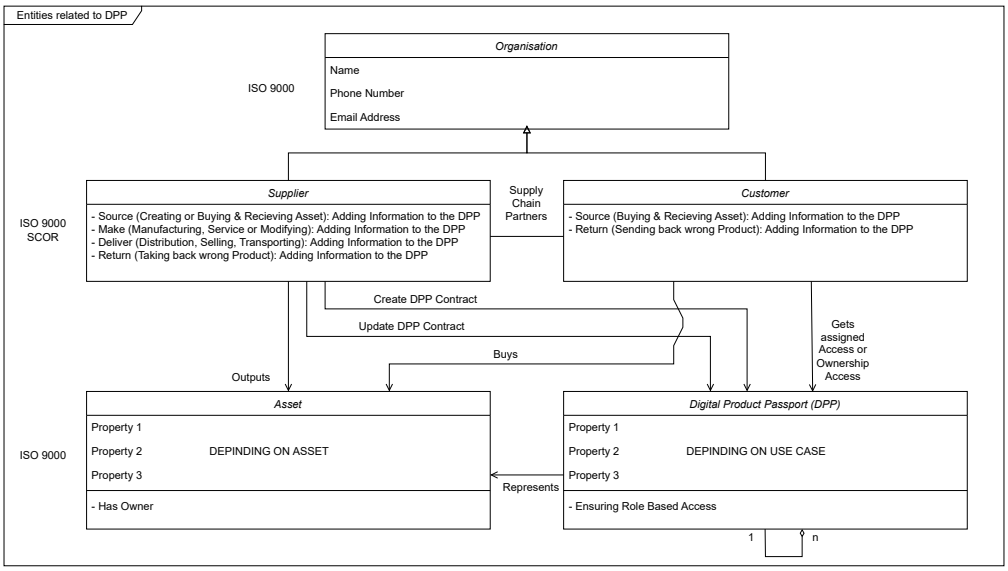

Figure 3. UML Class Diagram of Entities related to a DPP

The characteristics and relations of the asset and the DPP are displayed in the bottom part of Figure 3. The asset itself has an arbitrary set of product-specific properties and a defined owner at each point in its life cycle. To integrate the DPP into this framework, the DPP must also have an owner who, like the asset, has full control over access to the current state of the DPP. This task of role-based access control is accomplished by implementing the DPP in a smart contract. When the DPP is sold, the proposed smart contract creates a new state in which the owner of the DPP has changed. Furthermore, it is the responsibility of the supplier to decide which content properties should be stored in the DPP, as they are responsible for collecting the correct information in the same way as for certifications such as the *CE* label or a carbon footprint. The properties contained in the DPP will therefore change depending on which verifications or regulations the supplier wishes to address. The advantage of implementing the DPP in a smart contract over a centralised collection in a file, for example, is the clear traceability of changes that have been made. A property that has been tampered with by the supplier, e.g., an information about a purchased part from a previous manufacturer, can therefore be immediately identified by the customer. To indicate that the product has preliminary products, there can be any number of references to other product passports in the DPP.

4.1.3. DPP Interactions in Manufacturing: Source Asset

In the following, the above-mentioned interactions within the supply chain derived from [63] and [64] will be presented in more detail. Figure 4 depicts the processes and interactions regarding the asset and the associated DPP during *sourcing* in a UML sequence diagram. The figure distinguishes between sourcing the product from scratch and adopting an existing supplied product within the

 doi:10.20944/preprints202402.1194.v2

company. When a new asset is physically created, an associated DPP is created in the form of a smart contract, which leads to an update of the BC. 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. When invoking an existing smart contract the 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.

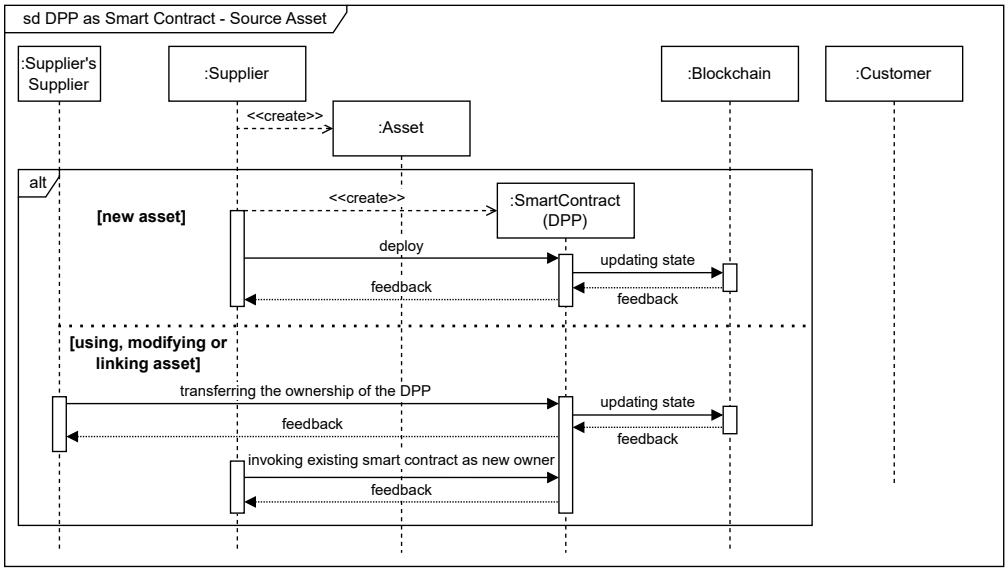

Figure 4. Sequence Diagram of Sourcing an Asset

4.1.4. DPP Interactions in Manufacturing: Make Asset

During the production assets are processed in various ways, that lead to physical changes of the asset. Every piece of information that is generated during the processing steps can be added to the DPP with respective input data. When the smart contract is executed, the BC is updated and feedback is returned on the success or failure of the execution. 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. This processes regarding the supplier, the asset and the smart contract are depicted in Figure 5.

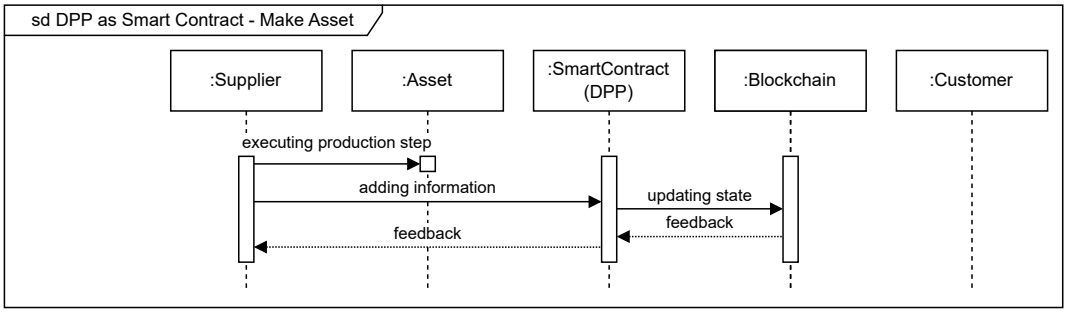

Figure 5. Sequence Diagram of Making an Asset

4.1.5. DPP Interactions in Manufacturing: Deliver Asset

This section and Figure 6 describe the processes associated with the DIP in the *deliver* interaction. During the sales phase, the supplier should be able to 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 customer's credentials first. If the customer purchases the asset, he is declared as the new owner of the asset in the DPP by updating the state of the BC. At this stage, he

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2024 doi:10.20944/preprints202402.1194.v2

only has write access to the DPP. The supplier, however, no longer has any access to newly added information. Nevertheless, the supplier does not lose access to historical information in the DPP at the time of purchase. The delivery process ends with sending the actual asset physically to the customer.

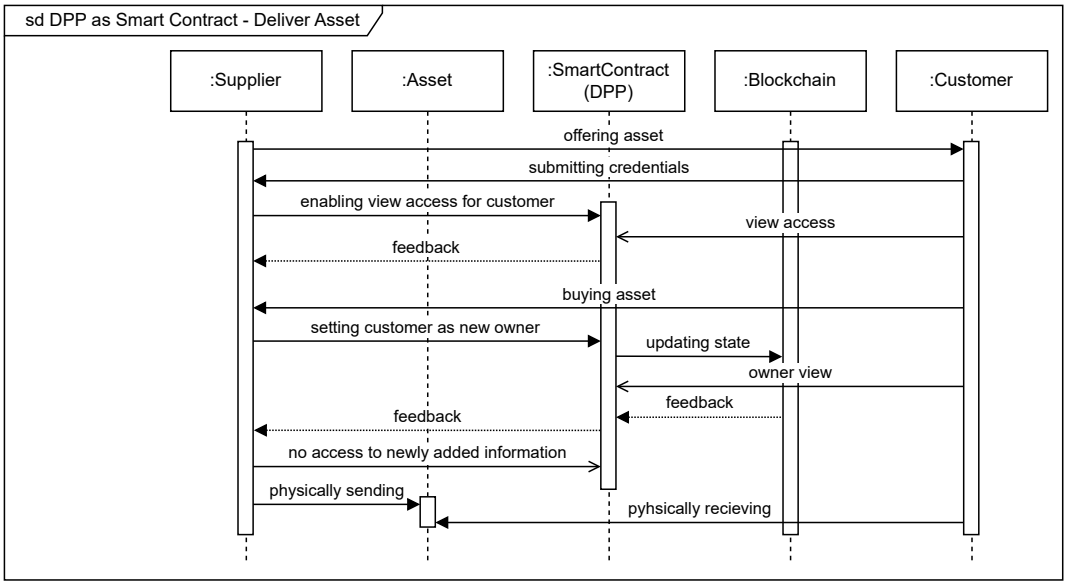

Figure 6. Sequence Diagram of Delivering an Asset

4.1.6. DPP Interactions in Manufacturing: Return Asset

This section outlines the processes undertaken by supply chain partners in the return of assets. 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's access rights to the DPP are fully restored by updating the status of the BC. These steps are described in Figure 7.

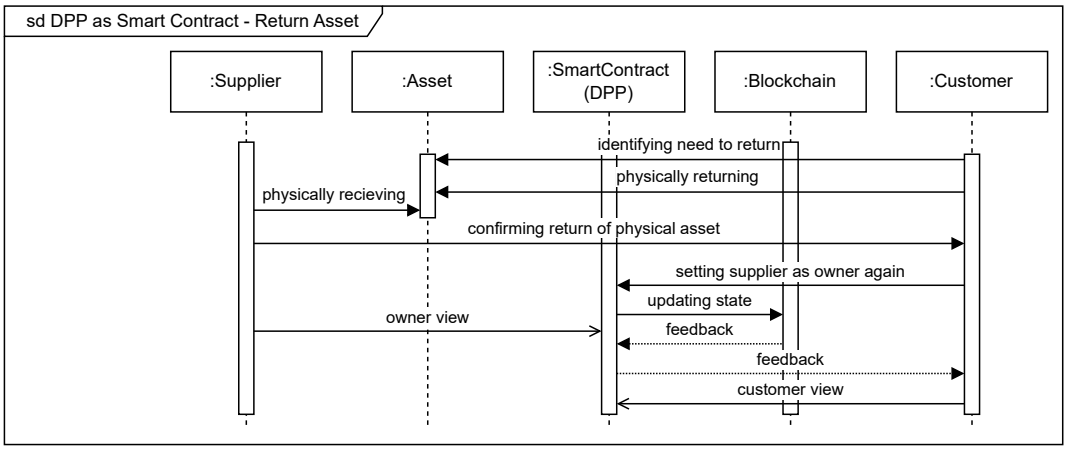

Figure 7. Sequence Diagram of Returning an Asset

4.2. Proposed System Architecture for BC-Based DPPs

This section presents a concept that implements the requirements and functionalities derived from the analysis of supply chains into BC-based smart contracts. To achieve this goal, management functions for handling smart contracts are presented to work collaboratively on DPPs. Analysing the described interactions and processes within supply chains regarding DPPs, it can be determined that the required interactions with a smart contract are as follows:

- **Creating a smart contract** when a product is first created (Figure 4).

 doi:10.20944/preprints202402.1194.v2

- **updating the smart contract** when an asset is modified (Figure 5).
- **setting a new owner of the smart contract** when an asset is sold or returned (Figures 6 and 7).
- **enabling view access** to the DPP to a potential customer.

The frameworks described [63,64] do not take into account the potential end of a product's life cycle. Thus, an additional feature for managing smart contract-based DPPs is added:

- **Closing a smart contract** for further modifications at the end of an asset's lifetime.

By establishing these five smart contract functionalities, all possible cases within supply chains can be generically covered. Other requirements of the DPP system are the interoperable usability of the information it contains and the globally unique identifiability of the asset it represents. In addition to traceability, the privacy of the data contained must be guaranteed, as well as secure mechanisms for access management.

4.2.1. Design Considerations

At the heart of the presented architecture is the product information of the DPP in the form of an AAS, which serves as a repository for the aggregated information to fulfil the content requirements and regulations. As described in [45], each AAS is provided with a globally unique identifier. By storing an identifiable AAS on the BC, information about an asset is secured immutably and tamper-proof throughout its life cycle. The AAS is usually serialised in the structured format JSON. The advantage of the standardised information model of the AAS is the interoperability it guarantees and the large number of standardised submodels for describing different thematic aspects of the asset (e.g., the *Digital Nameplate* [49] or the *Carbon Footprint* [51]). Another advantage of the AAS is the encapsulation of information from different composite products through references in the AASs [65].

Choosing Secret Network for our DPP platform was a strategic decision, underscored by its unique viewing key feature alongside scalability and performance. Secret Network differentiates itself with the capacity to execute smart contracts that process encrypted data, maintaining the confidentiality of sensitive information. This is crucial for DPP platforms, which requires robust privacy to protect proprietary data in supply chains without compromising on transparency and traceability. The viewing key functionality ensures that access to this encrypted data is strictly controlled, providing access only to authorised parties. This, combined with Secret Network's efficient handling of high transaction volumes, makes it the optimal choice for deploying a DPP platform that prioritizes privacy, security, and operational efficiency.

Integrating BC with Gaia-X for DPP initiative merges the privacy and security of BC technology with the data sovereignty and compliance framework of Gaia-X. This combination ensures that sensitive product data is managed securely on the BC while adhering to European standards for data privacy and transparency. Gaia-X's principles guide the handling and exchange of data, aligning with stringent regulatory requirements. The synergy between BC's secure ledger and Gaia-X's infrastructure enhances trust and compliance, addressing the complexities of digital ecosystems, as described in Section 3.2. This strategic integration aims to navigate the challenges of data privacy and sovereignty, offering a compliant and trusted DPP solution.

In a functional perspective the proposed architecture encapsulates the identified five primary functions for DPP management: **creation**, **updating**, **transferring ownership**, **enabling view access**, and **closing** a smart contract for further modifications on the BC using unique product identifier. Each function is designed to handle specific aspects of DPP life cycle management while ensuring data security and integrity. Figure 8 shows a high-level depiction of the proposed DPP management architecture, enabling all the required steps to the DPP. This figure demonstrates the collaboration between the physical layer, where the traded asset is located, and the documented product life cycle within the BC layer. The aggregation of Gaia-X serves to ensure the privacy and security of product information and users.

 doi:10.20944/preprints202402.1194.v2

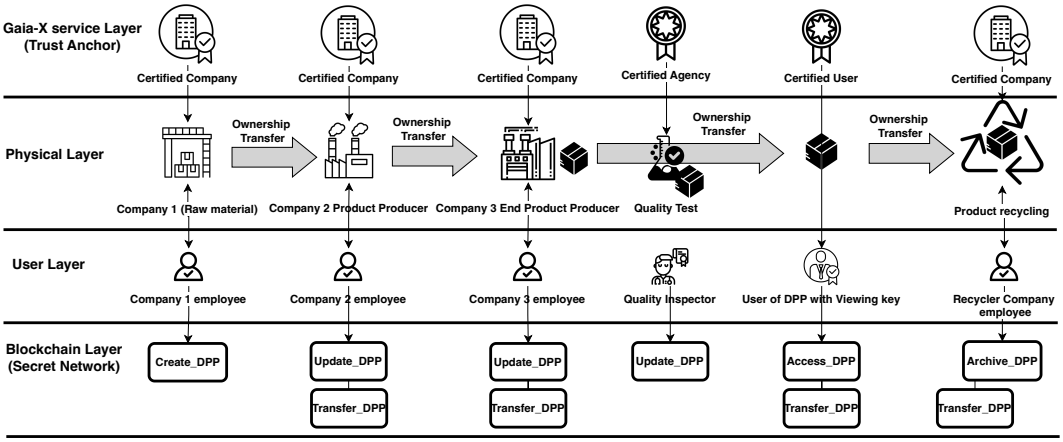

Figure 8. High-level depiction of the Proposed DPP Management Architecture using the Secret Network

4.2.2. DPP Management Functions: Creating the DPP

The *Create_DPP* function, as depicted in Algorithm 1, not only initiates the DPP life cycle by generating a unique product identifier but also integrates a secure mechanism for future updates. Upon creating the DPP, product data is encrypted and embedded within a smart contract, ensuring traceability and privacy. This smart contract, designed for dynamic interaction, allows the system to append updates as new transactions linked by the product's unique identifier, without altering the original data. Following encryption, the DPP undergoes Gaia-X compliance verification before storage on the BC.

Algorithm 1 Create DPP

```
function CREATE_DPP(product_data)

    Generate unique_product_identifier for each product

    Encrypt product_data

    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
```

4.2.3. DPP Management Functions: Updating the DPP

The *Update_DPP* function, detailed in Algorithm 2, is designed to enhance existing DPPs by appending new information to the product's BC passport. This process begins with the retrieval of the relevant smart contract using the product's unique identifier and the verification of user credentials according to established security policies. Instead of replacing the existing data, the update mechanism adds to it, preserving the historical integrity of the product data. The newly appended data is securely re-encrypted and stored on the BC, ensuring that all modifications are immutably logged for comprehensive audit trails. This approach underscores the data consistency and traceability across the product life cycle.

 doi:10.20944/preprints202402.1194.v2

Algorithm 2 Update DPP

```
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

end function
```

4.2.4. DPP Management Functions: Transferring the Ownership of the DPP

The *Transfer_DPP* function is designed to set a customer as the new owner of the DPP. Analogous to Algorithm 2, the owner retrieves the smart contract using the product's unique identifier. The user's credentials and permissions are then also checked against the security policies. The smart contract owner is then updated using the customer's credentials. After this the event data is logged (Algorithm 3). This process transfers control over future entries to the smart contract to the responsibility of the new owner.

Algorithm 3 Transferring the Ownership of the DPP

```
function TRANSFER_DPP(unique_product_identifier, user_credentials, customer_user_credentials)

    Retrieve smart_contract from blockchain using unique_product_identifier

    Validate user credentials and permissions using security policies

    Update owner of smart_contract on blockchain with new customer_user_credentials

end function
```

4.2.5. DPP Management Functions: Enabling View Access to the DPP

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 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

```
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 via viewing key

    Validate data access against Gaia-X privacy policies

    Provide user with access to decrypted product_data

end function
```

4.2.6. DPP Management Functions: Closing the DPP

Finally, the Closing_DPP function is shown in Algorithm 5. Once executed, no more information can be added to 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.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2024 doi:10.20944/preprints202402.1194.v2

Algorithm 5 Closing the DPP

```
function CLOSING_DPP(unique_product_identifier, user_credentials)

    Validate user_credentials and permissions using security policies

    Retrieve smart_contract from blockchain using unique_product_identifier

    Archive the given unique_product_identifier from BC

    if credentials and permissions are valid then

        Proceed with archiving process

    else

        Deny the operation and log an unauthorized access attempt

    end if

end function
```

4.3. Exemplary Application of the Concept to an Industrial Use Case

In the following, the developed concept is applied to an exemplary use case to clearly demonstrate its functionality. The presented 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 [49] to fit existing regulations (such as the *CE* marking) and carbon footprint information in order to promote sustainability of industrial products [51]. Information of every executed step regarding these two topic areas are aggregated into the DPP enabled by the smart contract.

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 after being set as the owner by the supplier by using Algorithm 3. The company now has full control over newly added information on the parts. In addition, the company creates the new smart contract of the future wheel (Algorithm 1) and adds general information of the digital nameplate (Algorithm 2), as illustrated in Figure 9.

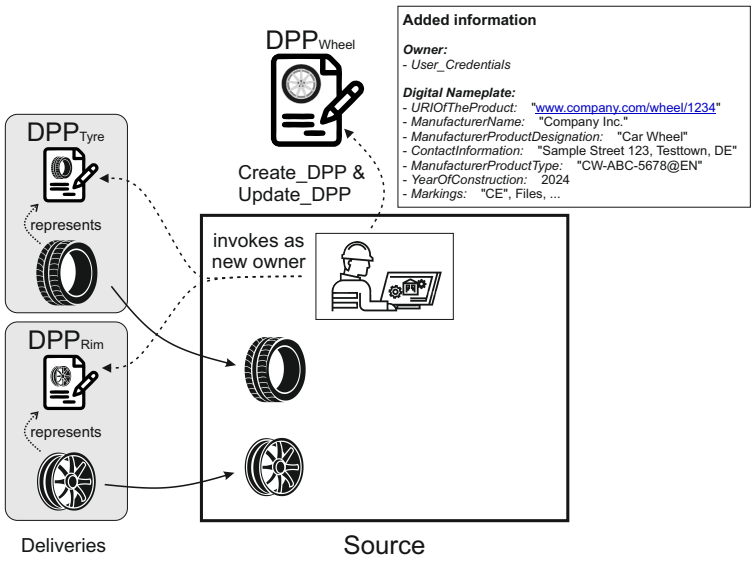

Figure 9. Sourcing of a car wheel supply chain process with information flow to the DPPs

The further manufacturing step is then carried out on the rim, as illustrated in Figure 10. 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

 doi:10.20944/preprints202402.1194.v2

also referenced by their unique identification, as the new wheel consists of these two parts. All of these actions are achieved by updating the smart contract, and thus the BC, as outlined in Algorithm 2.

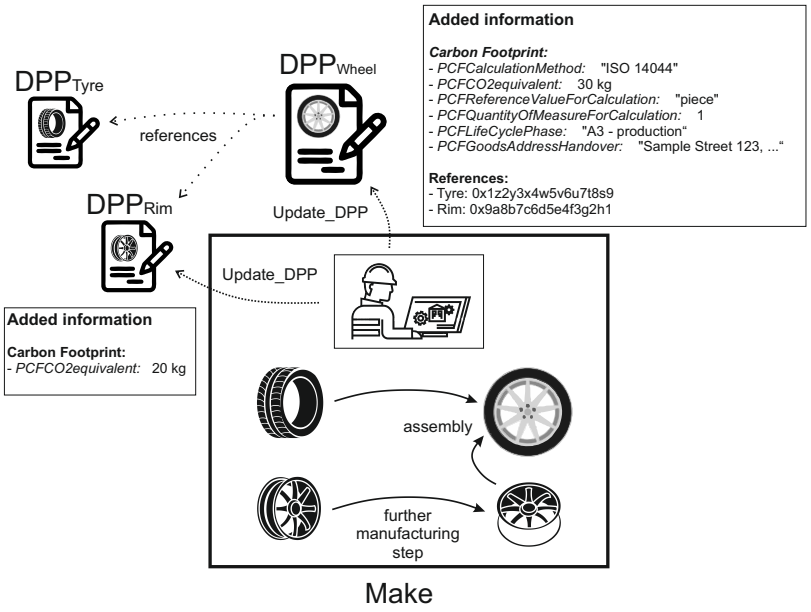

Figure 10. Making of a car wheel supply chain process with information flow to the DPPs

Finally, the finished wheel is packaged and shipped to the customer, illustrated in Figure 11. The carbon footprint caused by the transport of the asset is also added to the DPP by using Algorithm 2. The customer of the wheel is set as the new owner of the smart contract after the purchase by using Algorithm 3. 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.

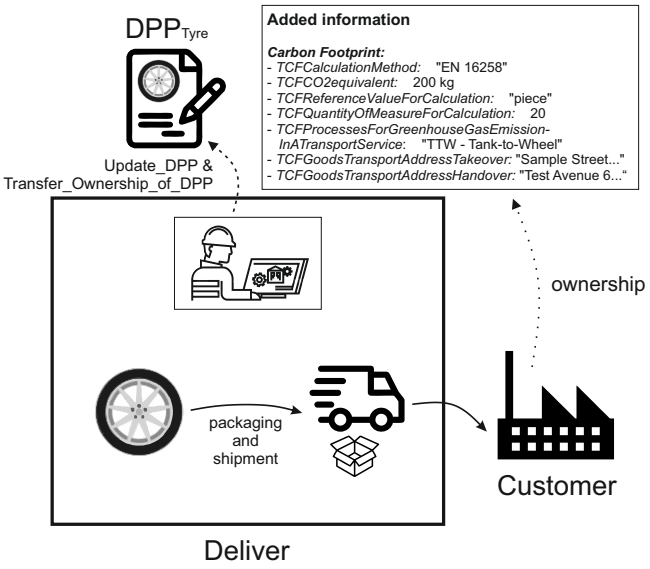

Figure 11. Delivering of a car wheel supply chain process with information flow to the DPPs

 doi:10.20944/preprints202402.1194.v2

5. Evaluation

In this section, we delve into the critical evaluation of security considerations within the BC-based DPP system, aligning our discourse with the requirnment elucidated in Section 2.3.1. Our aim is to illuminate the specific security measures implemented within the DPP system, present a structured framework for addressing these security considerations, and expound on explicit evaluation metrics and approaches for a comprehensive security assessment.

5.1. Integration of Security in DPP Architecture:

The architectural design of the DPP system is inherently security-focused, integrating BC technology to harness its decentralisation, trust, and immutability features for enhanced security. This integration facilitates a robust framework wherein:

- Decentralisation and Trust: Leveraging the decentralised architecture of BC markedly diminishes the likelihood of single points of failure, thereby bolstering the network's resilience against adversarial actions. The employment of smart contracts enhances trust through the transparent and efficient application of rules. By integrating Secret Network technology within the Gaia-X framework, a nuanced fusion of decentralisation, transparency, and the immutable nature of BC is achieved. This architecture capitalizes on the intrinsic decentralisation of BC to cultivate trust among all parties involved in the supply chain.
- Data Integrity and Security: DPP architecture seamlessly integrates on-chain and off-chain data storage solutions, significantly advancing data integrity and security while efficiently managing resource consumption. By selectively utilizing on-chain storage for crucial transactional data, it leverages BC's inherent immutability, thereby safeguarding against tampering and ensuring the utmost data integrity and bolstered security. For more extensive data sets, it employs off-chain storage, which is secured through advanced cryptographic measures to maintain integrity and operational efficiency. This strategic approach not only alleviates the issues of BC bloat and its related costs but also establishes a comprehensive framework for the protection of sensitive information.

5.2. Structured Security Framework:

To systematically address the security considerations of the DPP system, we adopt a comprehensive framework comprising:

5.2.1. Security Evaluation Metrics and Approaches:

Our security assessment of the DPP system is underpinned by a set of predefined metrics and approaches:

- Compliance Adherence: This metric assesses the DPP system's compliance with relevant standards and regulations, ensuring data privacy and sovereignty as per Gaia-X framework requirements.
- Threat Model Coverage: Evaluates the comprehensiveness of the threat model and the efficacy of corresponding mitigation strategies in addressing identified security risks.
- Smart Contract Audit Findings: Focuses on identifying and rectifying vulnerabilities within the smart contracts that govern the DPP system's BC operations.
- System Resilience: Assessed through rigorous penetration testing and simulated attack scenarios to ascertain the system's ability to withstand and recover from potential security breaches.

5.2.2. Threat Modeling and Risk Assessment:

Employing tools such as Threat Dragon alongside [66] the STRIDE methodology [67], we meticulously identify and assess potential threats, facilitating the development of a prioritised threat model in Figure 12 which guides our mitigation strategy implementation in Table 3. This process involved

 doi:10.20944/preprints202402.1194.v2

identifying potential threat actors and various malicious behaviors, such as phishing and credential theft, to pinpoint where attackers might exploit system vulnerabilities.

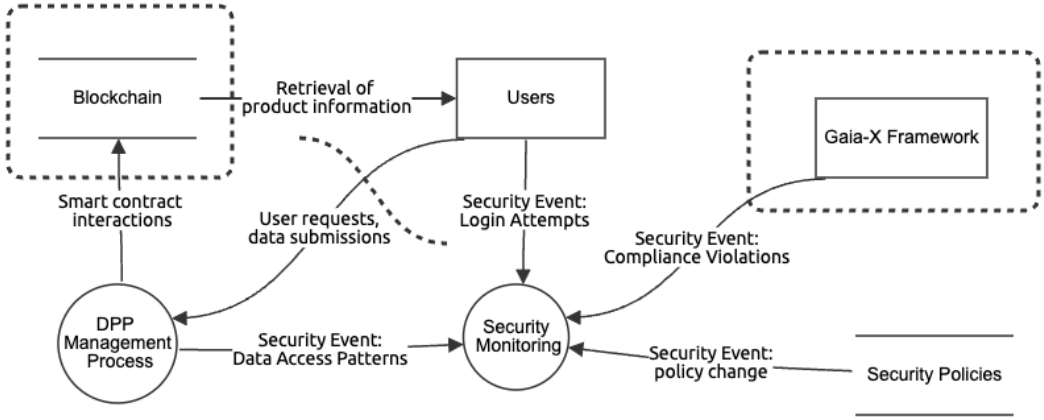

Figure 12. High-Level depiction of Data Flows in the proposed Architecture

In Figure 12, 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 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. The DPP Management Process, connected to the BC, manages smart contract activities related to data privacy and security. This indicates the utilisation of BC technology for enforcing or logging data protection regulations, thus providing a tamper-proof and verifiable record of transactions for compliance and audit purposes.

Table 3. 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	Unauthorised Access, Data Manipulation	Critical	security by design with Secret Network
Gaia-X Service Initialisation	unauthorised access during setup	High	Secure bootstrapping, Encryption at rest and in transit
Blockchain Operations	Smart Contract Vulnerabilities	Critical	Smart contract audits, Input validation and sanitisation
Security Monitoring	Inadequate Detection	Critical	Continuous threat intelligence
Data Transfers	MITM Attacks, Data Interception	High	TLS, Certificate pinning, Regular certificate rotation

Table 3 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', reflects a com-

 doi:10.20944/preprints202402.1194.v2

prehensive 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 Initialisation'. These strategies form a multi-layered defense framework, ensuring robust protection against both internal and external threats.

5.2.3. Security Measures and Controls

The proposed architecture incorporates a layered security approach, encompassing both technological and procedural controls high-level in Table 3. 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 BC.
- Access Control Mechanisms: Utilizing Role-Based Access Control (RBAC) and fine-grained permission policies, the system ensures that only authorised users can access or modify the DPP data. Secure session management and viewing keys are dynamically managed and thoroughly audited to prevent unauthorised data exposure.
- Smart Contract Security: Smart contracts, which enforce the business logic of the DPP on the BC, are rigorously tested for vulnerabilities. Smart contract audits, along with input validation and sanitisation, 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 unauthorised access, data manipulation, and data interception during data transfers.

6. Conclusions and Future Work

This paper presents a concept and architecture for a BC-based DPP, addressing the need for secure collaborative methods for working on digital product data documentation across the entire supply chain. The advantage of the presented concept is the technical possibility for the recipient of a product to trust that the content in the DPP have not been falsified while maintaining the privacy of the DPP's information. The achievement of the EU's objectives regarding the R-strategies can only be achieved by establishing trust in the correctness of the DPPs, because remanufacturing or recycling processes can only be carried out if the communicated information is certain and trustworthy. By combining Gaia-X authentication tools with smart contracts, an architecture has been created that allows secure access to product information on the BC while respecting privacy. The utilised *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.

By aligning the functionalities of the smart contract with generic processes in supply chains, a generally applicable framework was presented that enables different manufacturers within a supply chain to read and write data to the DPP depending on the life cycle phase. The information contained in the smart contract is fully traceable for customers and other authorised stakeholders, making forgeries and manipulations detectable. To demonstrate the functionality of the presented concept, an exemplary application was explained. The example consisted of a production process of a car wheel

 doi:10.20944/preprints202402.1194.v2

and the aggregation of information from the digital nameplate and the carbon footprint during the manufacturing and assembling processes into the BC-based DPP. Relevant security aspects were taken into account and evaluated.

In addition to the specification of sector-specific content for DPPs such as [5,68], future work could focus on linking real production machines and the data they provide with the BC network so that the data required for the DPP is aggregated automatically, as presented in [37]. To achieve this, Operation Technology (OT) technologies from production systems such as Programmable Logic Controller (PLC) data or OPC UA must be linked syntactically and semantically with the digital twin of products, as presented in [69]. Automatic adaptation of the information models used to regulations and technical requirements would also improve the usability of DPPs [70].

Author Contributions: Conceptualization, F.S. and N.M. and P.R.; methodology, F.S. and N.M. and P.R.; validation,F.S. and N.M. and P.R.; formal analysis, F.S. and N.M. and P.R. and C.R.; investigation, F.S. and N.M. and P.R.; writing—original draft preparation, F.S. and N.M. and P.R.; writing—review and editing, F.S. and N.M. and P.R. and C.R.; visualization, F.S. and N.M. 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.
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. 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.
5. Aschermayr, D.; Kadner, S.; Risch, L.; Simböck, J.; Braunfels, A.S.; Dixon, B.; Herrmann, S.; Kleine Jäger, J.; Kühl, C.; Schenk, S.; Teuber, A.; Vahle, T. Battery Passport Content Guidance: Achieving compliance with the EU Battery Regulation and increasing sustainability and circularity.
6. Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2014.
7. Introduction to smart contracts. https://ethereum.org/en/smart-contracts/, 31.07.2023.
8. Stratmann, L.; Hoeborn, G.; Pahl, C.; Schuh, G. Classification of product data for a Digital Product Passport in the manufacturing industry **2023**.
9. Zier, M.; Stenzel, P.; Kotzur, L.; Stolten, D. A review of decarbonization options for the glass industry. *Energy Convers. Manag. X* **2021**, *10*, 100083.
10. Adisorn, T.; Tholen, L.; Götz, T. Towards a digital product passport fit for contributing to a circular economy. *Energies* **2021**, *14*, 2289.
11. ESCAP, U. Beginners' manual on digital marketing and e-commerce **2022**.
12. Union, E. EPREL - European Product Registry for Energy Labelling. 2024, https://eprel.ec.europa.eu/screen/home, 2024.

 doi:10.20944/preprints202402.1194.v2

13. Agency, E.C. Understanding REACH, 2024.
14. Michael, J.; Grote, E.M.; Pfeifer, S.A.; Rasor, R.; Henke, C.; Trächtler, A.; Kaiser, L. Towards the Concept of a Digital Green Twin for a Sustainable Product Lifecycle. International Conference on Water Energy Food and Sustainability. Springer, 2021, pp. 548–557.
15. Donetskaya, J.V.; Gatchin, Y.A. Development of requirements for the content of a digital passport and design solutions. Journal of Physics: Conference Series. IOP Publishing, 2021, Vol. 1828, p. 012102.
16. Walden, J.; Steinbrecher, A.; Marinkovic, M. Digital product passports as enabler of the circular economy. *Chem. Ing. Tech.* **2021**, *93*, 1717–1727.
17. Swan, M. *Blockchain: Blueprint for a new economy*; " O'Reilly Media, Inc.", 2015.
18. Zhang, C.; Wu, C.; Wang, X. Overview of blockchain consensus mechanism. Proceedings of the 2020 2nd International Conference on Big Data Engineering, 2020, pp. 7–12.
19. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
20. Nguyen, G.T.; Kim, K. A survey about consensus algorithms used in blockchain. *J. Inf. Process. Syst.* **2018**, *14*.
21. Mishra, D.K.; Ghadi, M.J.; Azizivahed, A.; Li, L.; Zhang, J. A review on resilience studies in active distribution systems. *Renew. Sustain. Energy Rev.* **2021**, *135*, 110201.
22. Stančić, H.; Bralić, V. Digital archives relying on blockchain: Overcoming the limitations of data immutability. *Computers* **2021**, *10*, 91.
23. Xu, P.; Lee, J.; Barth, J.R.; Richey, R.G. Blockchain as supply chain technology: Considering transparency and security. *Int. J. Phys. Distrib. Logist. Manag.* **2021**, *51*, 305–324.
24. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652.
25. Zeba, S.; Suman, P.; Tyagi, K. Types of blockchain. In *Distributed Computing to Blockchain*; Elsevier, 2023; pp. 55–68.
26. Li, R.; Song, T.; Mei, B.; Li, H.; Cheng, X.; Sun, L. Blockchain for large-scale internet of things data storage and protection. *IEEE Trans. Serv. Comput.* **2018**, *12*, 762–771.
27. Wang, S.; Yuan, Y.; Wang, X.; Li, J.; Qin, R.; Wang, F.Y. An overview of smart contract: Architecture, applications, and future trends. 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018, pp. 108–113.
28. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857.
29. Buterin, V. Ethereum: Platform review. *Oppor. Challenges Priv. Consort. Blockchains* **2016**, *45*.
30. Nasir, Q.; Qasse, I.A.; Abu Talib, M.; Nassif, A.B.; others. Performance analysis of hyperledger fabric platforms. *Secur. Commun. Networks* **2018**, *2018*.
31. Valenta, M.; Sandner, P. Comparison of ethereum, hyperledger fabric and corda. *Frankf. Sch. Blockchain Cent.* **2017**, *8*, 1–8.
32. Woetzel, C. Secret network: A privacy-preserving secret contract & decentralized application platform **2016**.
33. Baliga, A.; Subhod, I.; Kamat, P.; Chatterjee, S. Performance evaluation of the quorum blockchain platform. *arXiv preprint arXiv:1809.03421* **2018**.
34. Stodt, F.; Kamel, M.B.; Reich, C.; Theoleyre, F.; Ligeti, P. Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture. *IEEE Access* **2024**, *12*, 26747–26758.
35. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34.
36. Berger, K.; Rusch, M.; Pohlmann, A.; Popowicz, M.; Geiger, B.C.; Gursch, H.; Schöggl, J.P.; Baumgartner, R.J. Confidentiality-preserving data exchange to enable sustainable product management via digital product passports-a conceptualization. *Procedia CIRP* **2023**, *116*, 354–359.
37. Ajdinović, S.; Strljic, M.; Lechler, A.; Riedel, O. Interoperable Digital Product Passports: An Event-Based Approach to Aggregate Production Data to Improve Sustainability and Transparency in the Manufacturing Industry. 2024 IEEE/SICE International Symposium on System Integration (SII). IEEE, 2024, pp. 729–734.
38. Stodt, F.; Reich, C.; Sikora, A.; Welte, D. Trust management system for hybrid industrial blockchains. 2023 IEEE 21st International Conference on Industrial Informatics (INDIN). IEEE, 2023, pp. 1–6.
39. 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. *Telecommunication Systems* **2024**, pp. 1–17.

 doi:10.20944/preprints202402.1194.v2

40. Jensen, S.F.; Kristensen, J.H.; Adamsen, S.; Christensen, A.; Waehrens, B.V. Digital product passports for a circular economy: Data needs for product life cycle decision-making. *Sustain. Prod. Consum.* **2023**, *37*, 242–255.
41. Stodt, J.; Schönle, D.; Reich, C.; Ghovanlooy Ghajar, F.; Welte, D.; Sikora, A. Security audit of a blockchain-based industrial application platform. *Algorithms* **2021**, *14*, 121.
42. Psarommatis, F.; May, G. Digital Product Passport: A Pathway to Circularity and Sustainability in Modern Manufacturing. *Sustainability* **2024**, *16*, 396.
43. Künster, N.; Dietrich, F.; Palm, D. Opportunities And Challenges Of The Asset Administration Shell For Holistic Traceability In Supply Chain Management. 2023, doi:10.15488/13481.
44. 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.
45. Federal Ministry for Economic Affairs and Climate Action. Details of the Asset Administration Shell: Part 1 - The exchange of information between partners in the value chain of Industrie 4.0: Specification, 2022.
46. 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.
47. 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.
48. Garrels, K.; Grüner, S.; Schönfeld, M.; Jänicke, L.; Lamboley, P.; Martinez, B.; Gayko, J.; Holst, J.C.; Käbisch, S.; Klasen, W.; Löffler, M.; Löwen, U.; Rossi, G.; Stephan, G.; Wegener, D.; Vojanec, B.; Schork, S. ZVEI-Show-Case PCF@Control Cabinet: Product Carbon Footprint Calculation of a Control Cabinet using the Asset Administration Shell: White Paper, Mai 2022.
49. Digital Nameplate for Industrial Equipment: Submodel Template of the Asset Administration Shell: Specification IDTA 02006-2-0.
50. ECLASS e.V.. An introduction to the standard. https://eclass.eu/en/eclass-standard/introduction, 2024.
51. Industrial Digital Twin Association e.V.. IDTA Carbon Footprint: Working Draft. https://github.com/admin-shell-io/submodel-templates/blob/main/development/Carbon
52. Braud, A.; Fromentoux, G.; Radier, B.; Le Grand, O. The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Netw.* **2021**, *35*, 4–5.
53. Mazumdar, S. How to Reduce Information Silos While Blockchain-ifying Recycling Focused Supply Chain Solutions? The 56th Hawaii international conference on system sciences. HICSS 2023. Hawaii International Conference on System Sciences (HICSS), 2023, pp. 459–468.
54. Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P. Data sovereignty: A review. *Big Data Soc.* **2021**, *8*, 2053951720982012.
55. eco Association of the Internet Industry. Software Requirements Specification for Gaia-X Federation Services: Authentication/Authorization: IDM.AA, 2021.
56. Ruf, P.; Stodt, J.; Reich, C. Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud. 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021, pp. 192–199, doi:10.1109/WorldS451998.2021.9514058.
57. 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.
58. Stodt, F.; Reich, C. A Review on Digital Wallets and Federated Service for Future of Cloud Services Identity Management. Service Computation 2023: The Fifteenth International Conference on Advanced Service Computing, June 26, 2023 to June 30, 2023, Nice, France, 2023, pp. 16–20.
59. Nowacki, S.; Sisik, G.M.; Angelopoulos, C.M. Digital Product Passports: Use Cases Framework and Technical Architecture Using DLT and Smart Contracts. 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). IEEE, 2023, pp. 373–380.
60. Falco, F. Distributed ledger technology in the circular economy: Enable traceability and transparency of recyclable products with a digital product passport platform. PhD thesis, FH Vorarlberg (Fachhochschule Vorarlberg).

 doi:10.20944/preprints202402.1194.v2

61. Saleheen, A.; Afrid, S. Potential of decentralised blockchains for the digital product passport: Need for traceability and transparency in textile industries, 2023.
62. Nguyen, H.; Do, L. The adoption of blockchain in food retail supply chain: Case: IBM food trust blockchain and the food retail supply chain in Malta **2018**.
63. DIN Deutsches Institut für Normung e.V.. DIN EN ISO 9000 - Quality management systems - Fundamentals and vocabulary, Nov 2015.
64. Council, A.S.C. APICS Supply Chain Operations Reference Model: SCOR Version 12.0, 2017.
65. Federal Ministry for Economic Affairs and Climate Action. Relationships between I4.0 Components – Composite Components and Smart Production: Continuation of the Development of the Reference Model for the I4.0 SG Models and Standards: Working Paper, 2017.
66. Shi, Z.; Graffi, K.; Starobinski, D.; Matyunin, N. Threat modeling tools: A taxonomy. *IEEE Secur. Priv.* **2021**, *20*, 29–39.
67. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2017, pp. 1–6.
68. Heinrich, M.; Lang, W. Materials Passports - Best Practice: Innovative Solutions for a Transition to a circular Economy in the Built Environment, 2019. https://www.bamb2020.eu/wp-content/uploads/2019/02/BAMB_MaterialsPassports_BestPractice.pdf
69. Kämper, B.; Both, M.; Maisch, N.; Müller, J. Mapping of an abstract PLC information model into different fields of application: CLIMA 2022 conference, 2022: CLIMA 2022 The 14th REHVA HVAC World Congress **2022**, doi:10.34641/clima.2022.341.
70. Ajdinović, S.; Maisch, N.; Dzubba, M.; Lechler, A.; Riedel, O. Defining Scalable Data Models for Operational Data Integration in Manufacturing Processes within the Digital Product Passport Framework through OPC UA and Asset Administration Shell [Manuscript submitted for publication]. *Proceedings for FAIM 2024* **2024**.