Dwivedi, Ashutosh Dhar; Tadayoni, Reza

Conference Paper

Designing Decentralized Digital Product Passports: A Path to Circular Economy Implementation

ITS 33rd European Conference 2025: "Digital innovation and transformation in uncertain times", Edinburgh, UK, 29th June – 1st July 2025

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Dwivedi, Ashutosh Dhar; Tadayoni, Reza (2025) : Designing Decentralized Digital Product Passports: A Path to Circular Economy Implementation, ITS 33rd European Conference 2025: "Digital innovation and transformation in uncertain times", Edinburgh, UK, 29th June – 1st July 2025, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/331267

Designing Decentralized Digital Product Passports: A Path to Circular Economy Implementation

Ashutosh Dhar Dwivedi, and Reza Tadayoni
Department of Electronic Systems, Aalborg University, Denmark
{*addw,reza*}*@es.aau.dk*

Abstract: The global transition towards a circular economy demands the creation of advanced digital tools that enable transparency, trust, and sustainability across product lifecycles. Decentralized Digital Product Passports (DPP) are emerging as a transformative solution to address these challenges. This paper investigates digital product passports based on distributed ledger and Internet of Things (IoT) technologies. The framework aims to securely record, store, and share product-related data, such as material composition, environmental impact, and usage history, in a tamper-proof and decentralized manner. Using the immutable nature of distributed ledgers and integrating real-time IoT data collection, the DPP framework aligns stakeholder actions with circular economy objectives, including improved resource efficiency, increased product reuse, and optimized recycling processes.

1. Introduction

The global economy is undergoing a fundamental transformation from a traditional linear model—characterized by "take, make, dispose"—to a more sustainable, circular paradigm wherein materials and products are kept in use for as long as possible, and waste is designed out of the system. This shift, widely known as the Circular Economy (CE), aims not only to reduce environmental impact but also to drive innovation, create resilient supply chains, and unlock new economic opportunities by transforming end-of-life materials into valuable inputs for new products. However, realizing the promise of a truly circular system requires transparent, reliable information flow across all stages of a product's lifecycle: from raw-material extraction and manufacturing through distribution, use, and eventual recycling or remanufacturing.

To meet this information challenge, the European Union (EU) has introduced the *Digital Product Passport* (DPP) as a key instrument under its forthcoming Ecodesign for Sustainable Products Regulation (ESPR). The DPP is envisioned as a secure, interoperable digital record—accessible via QR code, NFC tag, or web portal—that encapsulates exhaustive data on a product's material composition, manufacturing footprint, reparability, durability, and end-of-life pathways. By equipping stakeholders (including manufacturers, recyclers, regulators, and consumers) with fine-grained, authenticated data, the DPP creates the transparency needed to inform repair, reuse, and recycling decisions, thereby closing the loop on material flows and supporting the European Green Deal's ambitions for climate neutrality and resource efficiency.

Despite its transformative potential, deploying DPPs at scale presents several nontrivial challenges. First, product data originate in heterogeneous systems—enterprise ERPs, manufacturing execution systems, lab information management systems, and third-party supplier databases—each with distinct schemas and security regimes. Achieving seamless *interoperability* therefore requires standardized data models, robust APIs, and alignment with international metadata standards. Second, many payloads stored in a DPP (e.g., proprietary design files, detailed performance logs or commercial terms) are commercially sensitive; a practical DPP framework must balance *selective transparency* with confidentiality through fine-grained access controls, encryption, and off-chain storage. Third, the sheer volume and velocity of product-lifecycle data—particularly if enhanced by Internet of Things (IoT)–based condition monitoring—demands an architecture that can scale elastically while maintaining performance and low latency for real-time queries. Finally, DPPs must accommodate the diverse requirements of stakeholders ranging from multinational OEMs to small repair shops and individual consumers, each with unique regulatory, technical, and usability constraints.

A systematic and concept-driven methodology is applied to develop a robust DPP framework, integrating blockchain and IoT technologies in alignment with the principles of circular economy. The key steps in the methodology are as follows.

- **Literature Review:** A detailed review of academic and industry literature to explore existing frameworks,

technologies, and best practices related to blockchain [2], IoT, and digital product passports. This step builds a strong foundation for understanding the technical, legal, and social factors critical to DPP implementation.

- **Requirement Analysis and Stakeholder Mapping:** Using insights from the literature review, stakeholder requirements are analyzed. Key stakeholders, such as manufacturers, recyclers, regulators, and consumers, are mapped to assess their preferences for data sharing, centralization needs, and goals. This ensures that the DPP framework balances decentralization, selective data sharing, and regulatory compliance, meeting the needs of diverse participants.
- **Architectural Design and Protocol Specification:** A hybrid blockchain needs to be explored with on-chain and off-chain components. On-chain elements ensure immutable, transparent data storage, while off-chain databases securely manage sensitive information. Protocols securely link on-chain and off-chain records, enabling granular control over data access and sharing. The architecture supports scalability, interoperability, and security for various applications.
- **IoT Integration for Real-Time Data Collection:** IoT devices and sensors are integrated to automate real-time collection of key product lifecycle data, including material composition, environmental impact, and usage history. Secure communication protocols ensure data is accurately transmitted to the blockchain or off-chain storage. This integration enhances traceability and accountability while supporting resource management.

The remainder of this paper is structured as follows. Section 2 reviews recent developments and frameworks in *Digital Product Passports*, with a focus on blockchain technologies, IoT-enabled lifecycle tracking, and their role in circular economy transitions. Section 3 outlines our *requirement analysis and stakeholder mapping*, identifying key expectations, barriers, and technological enablers relevant to DPP deployment. Section 4 presents the *architectural design and protocol specification* of our hybrid on-chain/off-chain DPP platform, emphasizing scalability, interoperability, and data governance.

2. Literature Review

Recent years have seen a surge of interest in Digital Product Passports (DPPs) as both a technical and regulatory instrument to support circular economy and Industry 5.0 objectives. Below we survey work on domain-specific DPP frameworks, cross-industry requirement analyses, governance and sustainability perspectives, and enabling technology standards.

2.1. Domain-Specific DPP Frameworks

In the healthcare context, Stodt *et al.* [1] propose a blockchain-enabled DPP architecture for Internet of Medical Things (IoMT) devices. Their design uses smart contracts and role-based access control to immutably record manufacturing data, software updates, and usage logs, demonstrating how DPPs can enforce traceability and regulatory compliance in sensitive settings.

Çetin *et al.* [2] develop a DPP prototype tailored to the construction sector, integrating BIM metadata with IoT sensor feeds. They show how real-time structural performance metrics and material provenance can be embedded in a passport format to facilitate asset reuse and end-of-life deconstruction planning.

Berger *et al.* [3] address battery value chains by designing a DPP that tracks cell chemistry, usage cycles, and remanufacturing status. Their evaluation highlights the importance of standardized data schemas for second-life repurposing and regulatory reporting.

2.2. Cross-Industry Requirements and Design Principles

Plociennik *et al.* [4] present a systematic requirements analysis for DPP systems, emphasizing modularity, lifecycle traceability, and multi-stakeholder interoperability. They distill a common set of functional and non-functional requirements—such as tamper-proof logging, version control, and extensible data models—that underlie diverse DPP implementations.

Jansen *et al.* [5] complement this with a stakeholder-centric study, mapping user needs to technical capabilities. Through interviews and use-case mapping across electronics, textiles, and automotive, they prioritize features like real-time update propagation, API-first architectures, and embedded compliance checks.

Pourjafarian *et al.* [6] propose a multi-stakeholder DPP architecture based on the Asset Administration Shell (AAS) standard. Their work demonstrates how AAS submodels can encapsulate passport data semantically, enabling plug-and-play integration with Industry 4.0 assets and services.

Timms and King [7] apply a system-of-systems lens to DPP implementation, analyzing complexities such as cross-domain interoperability, lifecycle versioning, and governance fragmentation. They call for unified ontologies and federation layers to tame DPP heterogeneity.

2.3. Governance, Sustainability, and Policy Perspectives

Ducuing and Reich [8] delve into DPP governance, discussing data ownership, consent management, and regulatory interoperability. They argue for a pragmatic blend of decentralization with selective central authority—e.g., national agencies issuing credentialed attestations—so as to satisfy both GDPR and product safety mandates.

Panza *et al.* [9] emphasize embedding social and absolute sustainability metrics within DPPs. By linking cradle-to-grave environmental impact data and social compliance indicators directly into the passport, they show how DPPs can drive transparent supply chain decarbonization.

Becker [10] reviews the EU's Ecodesign for Sustainable Products Regulation (ESPR) and identifies how DPPs can operationalize requirements on traceability, reparability, and recyclability. His work underscores the need for policy-aligned data models and audit trails.

Lövdahl *et al.* [11] analyze European instruments—such as the Product Environmental Footprint (PEF) and extended producer responsibility directives—and assess their influence on corporate readiness to adopt DPPs. They find that harmonized standards are essential for cross-border passport exchange.

Ospital *et al.* [12] investigate DPP use in the fashion industry, exploring how consumer-facing passports can enhance transparency in materials sourcing and labor practices. Their study reveals positive shifts in brand trust but highlights user experience challenges.

King *et al.* [13] propose a conceptual ecosystem model for DPPs, delineating stakeholder roles (issuers, stewards, verifiers, consumers) and system dependencies. Their framework guides strategic alignment and value-chain orchestration.

2.4. Positioning DPPs Within Circular Economy Frameworks

Voulgaridis *et al.* [14] introduce a layered DPP meta-model structured around data collection, curation, and usage tiers. They map enabling technologies—IoT for sensing, blockchain for immutability, AI/cloud for analytics—and tie these to Industry 5.0 principles of modularity and human–machine collaboration.

Psarommatis and May [15] position DPPs as strategic levers for sustainable manufacturing, showing through simulation how passport-driven feedback loops improve material efficiency and reduce waste across product cohorts.

Panzieri *et al.* [16] (Greiner *et al.*) discuss blockchain consortium models for DPP interoperability, highlighting trade-offs between public transparency and enterprise privacy.

Together, these works form a rich, multidisciplinary tapestry—spanning technical architectures, governance regimes, sectoral pilots, and policy analysis—that establishes the DPP as a mature socio-technical instrument for circularity, compliance, and competitive advantage.

3. Requirement Analysis and Stakeholder Mapping

A robust Digital Product Passport (DPP) system must reconcile the diverse requirements of manufacturers, suppliers, recyclers, regulators, and consumers. Drawing on insights from the CE-RISE stakeholder mapping initiative [17], this section analyzes these stakeholder needs and highlights how emerging technologies—particularly blockchain and IoT—can address or exacerbate implementation challenges.

3.1. Stakeholder Mapping

Manufacturers and component suppliers prioritize data confidentiality, traceability of raw materials, and seamless integration with existing ERP systems. They require DPPs to capture environmental footprint data, compliance certifications, and bill-of-materials (BOM) information while maintaining commercial secrecy. Blockchain can enable immutable provenance records, but must be complemented with off-chain data storage and selective disclosure to prevent IP leakage.

Reuse and repair organizations seek information on repairability, disassembly procedures, and spare parts availability. Their main challenge is accessing detailed product specifications and histories across brands and formats. IoT-enabled DPPs can provide real-time diagnostics and service logs, but variability in data formats across manufacturers remains a barrier.

Refurbishers and remanufacturers demand granular access to usage data, component lifespans, and firmware histories to assess upgradeability and residual value. They face difficulties sourcing reliable data from previous product owners or OEMs. Blockchain-based audit trails and IoT telemetry can enhance data integrity but raise concerns over retrofitting and standardization.

Recyclers emphasize composition data—such as the location and quantity of critical raw materials (CRMs), presence of hazardous substances, and embedded battery details. Limited access to this information reduces the quality of material recovery. Here, a blockchain-backed DPP can anchor certified composition claims, and IoT sensors can assist in real-time detection (e.g., RFID tags for battery presence).

Regulators and market surveillance authorities require standardized, interoperable formats to verify compliance with EU directives (e.g., ESPR, PEF, CSRD). They value data authenticity, verifiability, and auditability. Blockchain provides legal-grade timestamping and non-repudiation, while IoT ensures timely updates. However, alignment across decentralized DPP networks and legal interoperability remain unresolved issues.

Consumers express growing interest in repairability, carbon footprint, and ethical sourcing data, but expect simplicity and clarity in access and visualization. They prefer QR/NFC interfaces and visual summaries like icons and scores. IoT integration can enable dynamic product updates, but privacy and data overload concerns persist.

3.2. Cross-Cutting Challenges and Technological Enablers

The CE-RISE consultation [17] identifies several recurring challenges in implementing DPPs:

- **Data Sensitivity and Sharing Resistance:** Many stakeholders hesitate to share data for fear of competitive disadvantage. Blockchain can address trust through cryptographic proofs and access control, while IoT can automate collection—but both require robust data governance.
- **Standardization and Interoperability:** Lack of harmonized formats across sectors hinders integration. While IoT devices can generate standardized telemetry, blockchain networks often fragment without a unifying protocol layer.
- **Scalability and Cost:** IoT deployments can overwhelm networks with real-time data, and public blockchains impose transaction costs. Hybrid architectures (e.g., using sidechains or permissioned ledgers with cloud off-loading) are essential to scale.
- **Data Availability and Completeness:** Many products lack a unique digital identity or data record from origin to end-of-life. Blockchain-linked DIDs and digital twins offer a solution but require upfront commitment and cross-industry collaboration.
- **Ease of Access and Usability:** Especially for consumers, DPPs must be intuitive and accessible. Blockchain and IoT must work behind the scenes, with front-ends providing seamless access through apps or web portals.
- **Privacy and Compliance:** Ensuring GDPR compliance while maintaining traceability is complex. Selective disclosure via zero-knowledge proofs and encrypted IoT payloads can enable compliance but increase design complexity.

4. Architectural Design and Protocol Specification:

The architectural integration of blockchain in Digital Product Passport (DPP) systems is driven by the need to establish trust, transparency, and verifiability among heterogeneous stakeholders without relying on a central authority. In the context of circular economy applications, where product information must persist across extended supply chains and life cycles, distributed ledger technologies (DLTs) provide a secure, tamper-resistant, and auditable backbone. However, classical blockchain designs are incompatible with privacy mandates such as the General Data Protection Regulation (GDPR), which emphasizes the right to data erasure, purpose limitation, and data minimization. To reconcile these goals, we adopt a hybrid architecture that carefully separates public verifiability from private data management.

In our design, only cryptographic commitments—such as SHA-256 hashes or Merkle roots—are recorded on-chain. These commitments serve as immutable fingerprints of the original data, which is stored off-chain in encrypted form using decentralized file systems (e.g., IPFS, Filecoin) or compliant cloud infrastructure. Product lifecycle data, such as environmental performance, bill-of-materials, repair history, and ownership transitions, is indexed off-chain and made selectively accessible via role-based access control and attribute-based encryption. By storing only hash pointers on the blockchain, the architecture allows the physical deletion or overwriting of off-chain data without affecting the integrity of the ledger. This decoupling of data and proof enables compliance with GDPR's "right to be forgotten" while maintaining verifiability.

To manage access, each stakeholder (manufacturer, regulator, recycler, consumer) is assigned a Decentralized Identifier (DID) in accordance with W3C standards. These DIDs are associated with verifiable credentials (VCs) that define their roles and permissions. When a stakeholder requests access to product data, smart contracts verify their credentials and release only the authorized decryption keys or file pointers. This mechanism ensures granular

access control, enabling compliance with privacy regulations without compromising transparency for legitimate actors.

Furthermore, smart contracts deployed on the blockchain encode key lifecycle rules and compliance logic. For example, they can automatically trigger alerts when a product enters a restricted regulatory zone, enforce extended producer responsibility (EPR) obligations, or verify the origin of recycled materials in secondary manufacturing processes. These rules are cryptographically enforced and auditable, reducing administrative overhead and enhancing accountability.

Table 1 summarizes how the proposed architecture addresses critical system requirements while maintaining alignment with legal and ethical constraints.

Table 1. Hybrid Blockchain Architecture: Alignment with DPP Requirements and Privacy

Requirement	**Solution within Hybrid Architecture**
Tamper-proof data lineage	Hashes of off-chain data are stored on blockchain, ensuring immutability and proof of authenticity
GDPR compliance (*right to erasure*)	Deletion of encrypted off-chain data while keeping hash on-chain allows verifiable deletion
Access control and confidentiality	Decentralized Identity (DID) and Verifiable Credentials (VCs) enable selective disclosure of encrypted data
Traceability across life cycle stages	On-chain state transitions linked to off-chain documents via immutable references
Scalability and storage efficiency	Large payloads stored off-chain prevent blockchain bloat and reduce transaction fees
Policy automation and compliance	Smart contracts encode circular economy rules and automate enforcement at runtime
Multi-stakeholder interoperability	Standardized interfaces (e.g., DIDComm, JSON-LD, VC schema) support plug-and-play integration

By separating concerns between the blockchain (as a layer of trust and verification) and off-chain components (as storage and privacy domains), the architecture strikes a functional balance between data transparency, system scalability, and regulatory compliance. This hybrid approach preserves the auditability and permanence of product histories while enabling legal deletion, fine-grained control over visibility, and data minimization—key tenets for real-world deployment of DPP frameworks across global supply chains.

4.1. Tamper-Proof Data Lineage

Establishing tamper-proof data lineage is critical for Digital Product Passport (DPP) systems, where stakeholders require guarantees that lifecycle data—ranging from material origin to recycling events—has not been modified or falsified. In decentralized environments involving competing actors (e.g., OEMs, recyclers, regulators), cryptographic guarantees of data authenticity and temporal ordering form the cornerstone of system integrity.

To achieve this, our architecture uses blockchain's append-only ledger properties in conjunction with cryptographic hash functions. Each off-chain data object, denoted as d_i (e.g., a repair log or emissions report), is processed through a secure hash algorithm (e.g., SHA-256), producing a fixed-length digest:

$$h_i = H(d_i)$$

Here, H represents a collision-resistant cryptographic hash function such that it is computationally infeasible to find two inputs $d_i \neq d_j$ for which $H(d_i) = H(d_j)$. These digests h_i are published to the blockchain as transaction payloads or stored within a Merkle tree structure for batch efficiency.

For a collection of n such data objects $\{d_1, d_2, \ldots, d_n\}$, we construct a Merkle tree $\mathscr{M}$, whose root R summarizes the entire dataset:

$$R = \text{MerkleRoot}(h_1, h_2, \ldots, h_n)$$

This root R is then stored immutably on-chain. When a verifier later requests proof of inclusion for a particular document d_k, a Merkle proof π_k is generated that reconstructs the path from h_k to R using sibling hashes. The verifier can check:

$$\text{VerifyMerkleProof}(h_k, \pi_k, R) \rightarrow \texttt{True}$$

This structure guarantees that no participant can retroactively alter d_k or substitute it with another without invalidating the root hash R, which is irrevocably recorded on the blockchain.

Time-Stamping and Sequencing: Each data hash or Merkle root is embedded in a blockchain transaction T_j with an associated block height b_j and timestamp t_j, collectively providing a temporal anchor:

$$T_j = \langle R_j, b_j, t_j \rangle$$

This enables not only integrity but also sequencing of lifecycle events (e.g., `ManufacturedBefore Certified`, `UsedBefore Recycled`), which is particularly relevant in compliance checks and product recalls. Since blockchain consensus protocols enforce strict ordering of blocks, the timestamp t_j serves as a verifiable lower bound on data existence.

Binding Data to Identity: Each hash commitment is signed digitally using the private key of the submitting entity, ensuring origin authentication. Let $\text{Sign}_{sk_i}(h_j)$ denote the digital signature on hash h_j using stakeholder i's private key sk_i. The signature is recorded as:

$$\sigma_j = \text{Sign}_{sk_i}(h_j)$$

and stored alongside h_j on-chain. This enables any party with access to the public key pk_i to verify the source of the data:

$$\text{Verify}_{pk_i}(h_j, \sigma_j) \rightarrow \texttt{True}$$

In the DPP context, this binds each data object to a known actor—e.g., manufacturer, recycler, or auditor—without central coordination.

Implications for the Circular Economy: Tamper-proof lineage underpins all higher-level assurances in circular economy use cases. For example, verifying that a component contains certified recycled content requires not only the presence of a claim but its cryptographic linkage to an immutable historical record. Similarly, warranty claims or reuse eligibility depend on confirmed usage records, which must be provably unaltered.

Illustrative Example Consider a washing machine with identifier `ProductID` $= P12345$. Its repair log d_{repair} is stored off-chain and hashed to yield h_{repair}. The manufacturer digitally signs the hash:

$$\sigma_{\text{repair}} = \text{Sign}_{sk_{\text{OEM}}}(h_{\text{repair}})$$

The tuple $(h_{\text{repair}}, \sigma_{\text{repair}})$ is committed to the blockchain via a smart contract that emits an event with timestamp t_r. If a regulator or customer wants to verify the authenticity of the repair record, they retrieve d_{repair} from the storage, recompute the hash, and check against the on-chain tuple:

$$H(d_{\text{repair}}) \stackrel{?}{=} h_{\text{repair}} \quad \text{and} \quad \text{Verify}_{pk_{\text{OEM}}}(h_{\text{repair}}, \sigma_{\text{repair}}) \rightarrow \texttt{True}$$

Thus, both the content and provenance of the repair entry are verifiably intact.

In simple terms, our system ensures that once any product-related information—such as repair records, environmental data, or ownership changes—is added to the passport, it cannot be secretly changed or deleted. This is done using mathematical fingerprints (called hashes) and storing them on a secure, distributed ledger (blockchain). Even though the actual documents are stored elsewhere (off-chain), anyone can later verify that what they see now is exactly what was originally recorded. This tamper-proof trail builds trust between all actors in the supply chain, including manufacturers, regulators, and recyclers, without needing a central authority.

4.2. GDPR Compliance and Privacy Preservation

The General Data Protection Regulation (GDPR) is a foundational legal framework that governs how personal data must be handled across the European Union. Among its core principles are the rights to access, rectify, and erase personal data (Articles 15–17), as well as the obligations of data minimization, lawful processing, and purpose limitation (Article 5). In designing Digital Product Passports (DPPs) for circular economy applications, we must ensure that these legal obligations are met—particularly in a system built on blockchain, where data is immutable and replicated.

To address this tension, our architecture incorporates privacy-preserving design choices that allow for verifiable, auditable data management without storing sensitive content directly on-chain. The following components constitute our approach to ensuring GDPR compliance within a decentralized DPP framework.

1. **Hybrid Storage with Erasable Off-Chain Data**

   In our system, sensitive product lifecycle data—such as ownership logs, usage telemetry, or repair records—is stored off-chain in encrypted format. Only the cryptographic hash of each data item is stored on-chain. This design allows the physical deletion of the actual data while retaining a tamper-proof reference.

   For instance, consider a smart washing machine whose DPP includes encrypted logs of energy consumption and past repairs. These logs are stored off-chain in a GDPR-compliant storage service. A hash of each log file (e.g., $h_i = H(d_i)$) is stored immutably on the blockchain. If the user exercises their right to erasure, the encrypted data d_i is deleted from storage. The blockchain reference h_i remains but can no longer be used to access or reconstruct the deleted content.

2. **Consent-Aware Storage and Purpose Limitation**

   Each data entry includes metadata specifying the legal basis for collection and processing (e.g., user consent, warranty fulfillment) and its permitted use duration. For example, a diagnostic report on the washing machine's motor failure may be retained for five years under a service agreement, after which access is automatically revoked.

   This enforcement is achieved through access policies encoded in smart contracts or access-control APIs, which interpret metadata flags to restrict or revoke retrieval privileges based on time or consent status.

3. **Granular Access Control via Decentralized Identity (DID)**

   Access to off-chain data is protected using Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Each authorized actor—e.g., the washing machine's manufacturer, repair technician, or recycling agency—receives a cryptographic identity and permission tokens. When requesting data, their credentials are verified before decryption keys are released.

   This ensures that only parties with appropriate authorization can access specific portions of the DPP—e.g., a recycler can view component composition, but not user activity logs.

4. **Zero-Knowledge Proofs for Private Verification**

   To balance privacy with transparency, our architecture supports zero-knowledge proofs (ZKPs). These cryptographic tools allow stakeholders to prove that certain conditions are satisfied—such as a product containing at least 30% recycled plastic—without revealing the full underlying dataset.

   Understanding ZKPs: A simple analogy is a customer proving they are over 18 without showing their ID. Similarly, the washing machine manufacturer may prove that the product complies with environmental standards without disclosing proprietary material ratios. ZKPs preserve trade secrets while supporting trusted claims across the supply chain.

5. **Case Example: Deleting User Data After Ownership Transfer**

   Imagine a user owns a smart washing machine that collects usage logs for energy optimization. These logs are encrypted and stored off-chain; only their hashes are stored on-chain. After five years, the user sells the machine and requests deletion of all usage data.

   The system deletes the encrypted records while the blockchain hash remains. The hash alone does not expose personal data and no longer maps to any valid file. Any attempt to verify or access the log fails, fulfilling the user's right to be forgotten while preserving auditability.

To protect privacy and comply with GDPR, our system stores sensitive product data—like usage history or service records—in secure locations outside the blockchain. Only digital fingerprints of that data are placed on the blockchain. This means the data can be deleted when necessary, while the blockchain still provides proof that something existed at a certain time. For example, if you sold your washing machine and asked for your energy data to be erased, we can remove the stored file while keeping a secure log that proves the system once had that data. This ensures that manufacturers and consumers both benefit from trust and transparency without compromising privacy.

4.3. Access Control and Confidentiality

In Digital Product Passport (DPP) systems, data is generated and used by a wide range of actors—including manufacturers, recyclers, regulators, and consumers—each of whom should see only the information they are authorized to access. This principle of "need-to-know" access is essential not only for protecting commercially

sensitive or personal information, but also for reducing cybersecurity risk and aligning with legal requirements such as GDPR's data minimization clause.

To enforce these access boundaries in a decentralized architecture, we employ cryptographic identity mechanisms and granular permission models rooted in the use of Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and encrypted off-chain data.

1. **Decentralized Identity (DID) for Stakeholder Authentication**

   Each actor in the DPP ecosystem is assigned a Decentralized Identifier (DID), a W3C-standardized identifier that is unique, verifiable, and under the control of the subject. Unlike centralized user accounts, DIDs are self-sovereign and stored on a distributed ledger. Associated with each DID are one or more public keys used for cryptographic operations such as signing and verifying access requests.

   For instance, the manufacturer of a washing machine receives a DID (e.g., `did:example:manufacturer123`), as does the authorized recycling facility and the current owner of the product.

2. **Verifiable Credentials for Role-Based Access**

   DIDs alone do not encode access privileges. Therefore, we use Verifiable Credentials (VCs) to attach attributes—such as "certified recycler" or "end-user"—to each identity. These credentials are digitally signed by trusted issuers (e.g., regulators, OEMs) and stored locally or on secure identity wallets.

   When a stakeholder attempts to retrieve data from the DPP, their credential is presented alongside their DID and verified using the issuer's public key. For example, a repair technician holding a VC indicating "authorized service agent" may be granted access to component-level maintenance logs, while a general consumer would be restricted to product energy ratings and warranty status.

3. **Encrypted Off-Chain Storage for Data Confidentiality**

   All sensitive product data—including usage telemetry, repair logs, and material composition—is stored off-chain in encrypted form. Encryption is performed using symmetric or attribute-based encryption (ABE) schemes, depending on the complexity of the access policies.

   In the case of the washing machine, suppose its repair log d_{repair} is encrypted with a symmetric key k, which is then encrypted using the public keys of the manufacturer and authorized repair technician. This ensures that only these two parties can decrypt and access the repair history, even if the encrypted data is exposed.

4. **Access Enforcement via Smart Contracts or Gatekeeping APIs**

   Access policies are enforced by smart contracts on the blockchain or via secure access-control gateways. These contracts verify whether a presented credential (e.g., "certified recycler") satisfies the policy tied to a specific data resource (e.g., composition of electronic modules). If the policy is satisfied, the encrypted data location and decryption key (or access token) are released.

   For instance, when the washing machine reaches end-of-life and is scanned at a recycling center, the center presents its credentials. A smart contract verifies the role, grants access to the DPP's composition submodel, and enables the center to recover valuable components without revealing consumer data.

5. **Case Example: Controlled Access Across the Product Lifecycle**

   Consider a washing machine that records maintenance history, energy consumption patterns, and component data. The manufacturer has access to all data, the repair technician is allowed to view only the maintenance logs, and the recycling facility can access the bill of materials (BoM) without seeing any personal usage logs.

   As the product passes from one actor to another, each stakeholder uses their DID and VCs to access relevant information. Unauthorized users cannot decrypt any data, and even those with access see only what they are explicitly allowed to. No centralized server is required to manage these permissions, and no raw data is placed on-chain, preserving both confidentiality and compliance.

These mechanisms create a flexible and secure access model that supports multiple actors and regulatory environments without compromising user or business confidentiality. Stakeholders gain just enough visibility to perform their roles—no more, no less—based on cryptographic credentials and decentralized logic.

Only authorized actors are ever able to decrypt and use the data, and this is done without any central authority managing permissions or issuing access keys on demand. Everything is governed through cryptographic proofs and roles that are distributed and verifiable, which makes the system robust, fair, and secure across the entire product lifecycle.

4.4. Traceability Across Life Cycle Stages

A core goal of Digital Product Passports (DPPs) is to create end-to-end traceability of a product—from raw material extraction to manufacturing, usage, repair, resale, and eventual recycling. Traceability ensures that stakeholders across the value chain can access verifiable and time-aligned records of how a product has evolved and moved through its lifecycle. This is essential for enforcing environmental compliance, planning disassembly, enabling second-life applications, and verifying repair or warranty claims.

Our architecture achieves traceability by linking off-chain events to immutable on-chain records using timestamped hash commitments, stakeholder signatures, and lifecycle state transitions governed by smart contracts.

1. **Lifecycle State Modeling**

   Each product in the DPP system is modeled as a finite-state machine (FSM), where each lifecycle stage—e.g., `Manufactured`, `Sold`, `Repaired`, `Transferred`, `Recycled`—represents a discrete state. Transitions between states are triggered by verifiable events logged on-chain.

   For example, when a smart washing machine is produced, the manufacturer emits an on-chain event `Manufacture(P12345, t_0)`, where `P12345` is the product ID and `t_0` is the timestamp. When the product is sold or repaired, new events are appended with corresponding proofs and signer identities.

2. **Hash-Linked Event Anchoring**

   Each off-chain lifecycle event is hashed and anchored to the blockchain. Let d_i denote an event record (e.g., repair invoice, ownership transfer contract), and $h_i = H(d_i)$ its hash. This hash is stored on-chain as part of a transition log:

   $$T_i = \langle \texttt{EventType}, h_i, \texttt{ActorID}, \texttt{t\_i} \rangle$$

   This makes it possible to later verify that a particular document existed and was associated with the correct actor at the time of the event. The record's integrity and sequencing are guaranteed by the blockchain's append-only structure.

3. **Temporal Traceability via Blockchain Timestamps**

   Since each transaction is embedded in a block with a consensus-driven timestamp, all product events are inherently ordered. This allows auditors or supply chain participants to reconstruct a chronological history of the product:

   $$\texttt{Manufactured} \rightarrow \texttt{Sold} \rightarrow \texttt{Used} \rightarrow \texttt{Repaired} \rightarrow \texttt{Recycled}$$

   For the washing machine case, the manufacturer might register the initial product data, a repair shop logs maintenance at `t_3`, and the recycling agency logs final processing at `t_7`. These events form a verifiable chain of custody.

4. **Stakeholder Attribution via Signatures**

   Every transition is signed digitally by the actor responsible for it using their private key. This ensures that each change in lifecycle state is traceable to a specific stakeholder identity (authenticated by DID) and prevents disputes over responsibility.

   For example, when a recycling agency declares that the washing machine has been processed and its components recovered, they sign a statement with their private key. This signed hash is stored on-chain, and anyone can verify its origin using the agency's public key.

5. **Case Example: Product Journey from Manufacturing to Recycling**

   Consider the full life of a smart washing machine with ID `WM-2025-001`. The manufacturer logs its birth by submitting product metadata and issuing a certificate of compliance. The first owner activates the machine, and the system begins collecting encrypted usage logs off-chain. Two years later, the product is repaired and this event is hashed and logged. Eventually, the product is sold second-hand, and the ownership transfer is registered. Finally, at end-of-life, the machine is recycled, with material recovery details submitted by a certified recycling center.

   Each of these lifecycle steps is anchored to the blockchain, forming an auditable trace of what happened, when, and by whom. The actual data—such as service logs or material composition—is retrieved off-chain when needed, but its authenticity and timing are always verifiable on-chain.

By combining event logging, digital signatures, cryptographic hashing, and time-based ordering, our architecture enables complete traceability without storing large or sensitive data directly on the blockchain. This design supports environmental reporting, warranty verification, take-back schemes, and second-life reuse, while ensuring each record can be independently verified by stakeholders across the product's lifetime. No matter how many hands the product passes through, every key action leaves a secure, traceable, and immutable record that builds trust across the circular economy.

4.5. Scalability and Storage Efficiency

A Digital Product Passport (DPP) system must accommodate massive volumes of data generated across diverse sectors and throughout long product lifecycles. These data include not only static attributes like material composition and certifications, but also dynamic and time-dependent records such as repair logs, energy usage statistics, and ownership transfers. At scale, this generates a significant storage and bandwidth burden—especially when thousands or millions of products are deployed and tracked simultaneously.

Blockchain systems, by design, are inefficient for storing large payloads. Storing all DPP data directly on-chain would lead to rapid ledger bloat, prohibitively high transaction costs, and degraded network performance. To address these limitations, our architecture separates data persistence from data verification using a lightweight, content-addressed, off-chain storage model.

1. **Off-Chain Storage for Payload Data**

   All large or sensitive data elements—such as firmware logs, recycling certificates, or sensor telemetry—are stored off-chain in decentralized or cloud-based storage systems. These systems may include InterPlanetary File System (IPFS), Filecoin, Amazon S3, or EU-compliant GDPR cloud providers, depending on the use case and compliance requirements.

   For example, a smart washing machine generates encrypted maintenance logs every month. These logs are stored off-chain and referenced via unique content hashes. The blockchain stores only a pointer—i.e., a cryptographic hash of the file—to verify that the content has not been tampered with.

2. **Content Addressing with Cryptographic Hashes**

   Each data file d_i is hashed using a secure one-way function H, producing a digest $h_i = H(d_i)$ that uniquely identifies the content. This digest serves as a content address and is stored immutably on the blockchain. Because even a single-bit change in d_i will produce a new hash, this allows any party to later verify whether a retrieved file is original and untampered.

   Content addressing enables data deduplication and caching. If a large number of washing machines share identical component specifications, those files are stored only once, reducing overall storage load.

3. **Merkle Trees for Batch Anchoring**

   To further reduce blockchain transaction volume, data hashes are aggregated into Merkle trees. A Merkle root R summarizes a batch of product data records $\{h_1, h_2, ..., h_n\}$. Only the root R is published on-chain, while the individual records remain off-chain. Verifiers can later reconstruct inclusion proofs for any record using minimal auxiliary data.

   This strategy significantly reduces gas fees and ledger size while preserving verifiability.

4. **Elastic Scalability via Distributed Infrastructure**

   Off-chain storage systems can scale horizontally, supporting parallel data ingestion and retrieval across geographies. Cloud storage providers offer redundancy, load balancing, and automated failover. IPFS nodes can replicate popular content for faster access.

   The blockchain layer is used only for anchoring trust—not for bulk storage—making the system suitable for long-term use across millions of products with modest infrastructure cost.

5. **Case Example: Monthly Logs at Scale**

   Suppose 10,000 smart washing machines generate monthly diagnostic logs of 100 KB each. Directly storing these on-chain would require 1 GB per month—unsustainable in most public or consortium blockchains. Instead, we store logs in IPFS, compute their hashes, and batch-anchor them to the blockchain via a single Merkle root per month. The result is a verifiable and scalable system with minimal on-chain footprint.

By decoupling data storage from verification and anchoring only essential commitments on-chain, our architecture achieves both integrity and efficiency. This ensures that DPP systems can scale elastically with real-world data volumes, support long-lived product histories, and operate cost-effectively without sacrificing transparency or compliance.

4.6. Policy Automation and Compliance

Regulatory frameworks such as the Ecodesign for Sustainable Products Regulation (ESPR), Extended Producer Responsibility (EPR), and the Right to Repair impose detailed compliance obligations on product manufacturers, sellers, and recyclers. These include requirements for material traceability, repairability documentation, recovery targets, and product certification. In conventional systems, enforcing these rules relies on manual audits, third-party attestations, or complex enterprise systems—approaches that are costly, opaque, and prone to error.

To streamline compliance and reduce administrative overhead, our DPP architecture integrates smart contracts—self-executing code deployed on the blockchain—to encode policy rules and enforce them automatically. These rules can evaluate conditions, verify signatures, track deadlines, and emit proofs of compliance that are visible and verifiable by all stakeholders.

1. **Encoding Rules as Smart Contracts**

   Each policy requirement—such as verifying recycled content, checking repair eligibility, or confirming take-back compliance—is modeled as a set of conditions encoded in a smart contract. These contracts are deployed on-chain and invoked during relevant product lifecycle transitions.

   For example, a contract might require that a product be accompanied by a recycling certificate before it can be marked as `Recycled`. The smart contract checks that a valid hash of the certificate is logged on-chain, signed by an authorized recycling agent.

2. **Role-Based Execution**

   Policy enforcement depends on the actor performing the action. Using Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), the system determines whether an entity is authorized to trigger a contract function. Unauthorized users are prevented from manipulating product states or falsely declaring compliance.

   For instance, only certified recyclers are permitted to trigger the `CompleteRecycling()` function for a product passport. Their credential is verified automatically through the contract, ensuring role-compliant behavior.

3. **Threshold Checks and Boolean Logic**

   Smart contracts can encode quantitative conditions—such as material composition thresholds or repair counts—based on input data hashes and external proofs. For example, a rule may enforce that a washing machine model must contain at least 30% recycled plastic to be eligible for sale in a particular region.

   The manufacturer provides a zero-knowledge proof (ZKP) of compliance, and the contract accepts or rejects the product registration accordingly.

4. **Time-Based Triggers and Expiry Control**

   Many regulatory conditions have time constraints—such as service intervals, warranty periods, or data retention deadlines. Smart contracts can enforce these by comparing timestamps on-chain.

   As a use case, consider a washing machine under a 5-year warranty. The smart contract can track the original sale date and automatically reject warranty repair claims submitted after expiration, ensuring policy consistency.

5. **Case Example: Enforcing Take-Back Compliance**

   At end-of-life, the washing machine must be returned to an authorized recycler. The system includes a smart contract that verifies: (a) the product is marked as `Decommissioned`, (b) the recycling agent holds the correct credential, and (c) a recycling report is submitted and hashed on-chain. Only when these conditions are met does the contract emit a compliance certificate and update the DPP status.

   This automation replaces manual audit procedures with decentralized, tamper-proof, and real-time enforcement, increasing efficiency and reducing compliance risks.

By embedding policy logic into verifiable smart contracts, our DPP framework transitions compliance from a manual, trust-based process to an automated, rule-based protocol. This enhances regulatory transparency, minimizes overhead, and builds confidence among all actors—ensuring that circular economy and sustainability goals are not only declared but demonstrably enforced.

4.7. Multi-Stakeholder Interoperability and Standardized Interfaces

Digital Product Passports (DPPs) operate across highly diverse ecosystems involving manufacturers, regulators, logistics providers, recyclers, consumers, retailers, and third-party certifiers. Each actor may use distinct information systems, ontologies, and communication protocols. Therefore, interoperability—both semantic and technical—is essential to ensure that product data can be created, updated, verified, and interpreted consistently across organizational and national boundaries.

Our DPP architecture promotes interoperability by adopting standardized data formats, schemas, and interfaces that support seamless data exchange, decentralized identity management, and role-based access across platforms.

1. **W3C DIDs and Verifiable Credentials (VCs)**

   Identity and access across actors are based on W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). These are interoperable standards widely adopted in digital identity frameworks, allowing organizations and individuals to issue, receive, and verify cryptographically secure identity assertions without centralized registries.

   For example, the washing machine's manufacturer, distributor, and repair technician each use a DID. The repair technician possesses a VC stating they are "authorized service personnel," which can be verified by any other stakeholder regardless of their internal systems.

2. **Structured Data Formats: JSON-LD and RDF**

   Product metadata, lifecycle events, and credentials are encoded using JSON-LD (JSON for Linked Data), which allows for machine-readable, context-aware semantics. This format supports schema extensibility and compatibility with Resource Description Framework (RDF) standards, enabling systems to interpret and query data across organizational boundaries.

   A DPP submodel describing energy consumption of the washing machine can include fields like `"energyRating": "A++"` and `"compliance": "EN50564"`, embedded within a JSON-LD context to define their meaning unambiguously.

3. **Domain-Specific Standards: Asset Administration Shell (AAS)**

   For industrial integration, particularly within Industry 4.0 and manufacturing systems, we align with the Asset Administration Shell (AAS) standard. AAS allows each product or component to carry digital twins with submodels (e.g., material composition, usage history, repair instructions) that can be shared across factories, ERP systems, and DPP platforms.

   A washing machine might expose a digital twin via an AAS interface containing submodels for components (drum, motor, PCB), warranty, and recyclability, each using a structured ontology.

4. **Standardized APIs for Read/Write Interactions**

   Interoperability is also supported at the protocol level through standardized RESTful and GraphQL APIs. These APIs allow stakeholders to query DPP data, submit updates, request verifications, or trigger contract logic in a secure and modular way.

   For instance, a regulator may send an API query to check whether a batch of products meets EU energy efficiency thresholds. The system responds with ZKP-backed confirmations using common query templates.

5. **Case Example: Cross-Border Product Update**

   Suppose a washing machine model is manufactured in Germany, sold in Denmark, serviced in Sweden, and recycled in Finland. Each country has different IT systems and regulatory frameworks. Using DIDs, JSON-LD payloads, and standard APIs, every actor can contribute verifiable information to the same DPP instance, without prior coordination or shared infrastructure. Each update is semantically understood and technically interoperable.

By integrating identity standards, linked data formats, domain ontologies, and modular APIs, our architecture ensures that stakeholders can collaborate across legal, linguistic, and technical boundaries. This not only supports scalability but is vital for implementing a circular economy infrastructure that spans jurisdictions and industries.

5. IoT Integration for Real-Time Data Collection

While traditional product information systems rely on static, manually curated records, the integration of Internet of Things (IoT) devices into Digital Product Passports (DPPs) enables real-time, automated, and trustworthy updates throughout a product's lifecycle. This capability is especially valuable in dynamic or long-lived products where conditions such as usage intensity, component degradation, environmental exposure, or repair events evolve over time.

Our architecture integrates IoT data streams directly into the DPP framework to enhance visibility, support predictive maintenance, and ensure traceable, machine-generated event reporting across all lifecycle stages.

1. **Sensor-Driven Data Acquisition**

   IoT devices embedded in or attached to a product continuously or periodically measure parameters relevant to its operational or environmental context. In the case of a smart washing machine, internal sensors may monitor vibration profiles, water consumption, temperature cycles, fault codes, and power efficiency.

   Each measurement is timestamped and transmitted to a secure data pipeline where it is formatted and filtered before entering the DPP system.

2. **Secure Communication and Data Signing**

   To ensure trustworthiness, each data packet transmitted from the IoT device is digitally signed using the device's private key. This prevents spoofing and ensures authenticity even if the data passes through untrusted networks.

   The receiving system (e.g., manufacturer server or gateway node) verifies the signature using the device's registered public key, then hashes the data and stores the original payload in an encrypted off-chain store.

3. **Event Triggering and Lifecycle Updates**

   Certain IoT events can act as lifecycle triggers. For example, an abnormal vibration pattern may indicate a pending mechanical failure, triggering a maintenance alert. If a repair is confirmed, the corresponding event is logged, signed, and anchored to the blockchain with a hash reference.

   This automation ensures that lifecycle records—such as `Repaired` or `Under Diagnosis`—are not just manually asserted but are supported by real sensor data.

4. **Granular Traceability and Verification**

   Since IoT data is timestamped, signed, and linked to specific sensors, it provides a tamper-evident trace of how the product was used. For instance, a recycling center might check the number of operational cycles a washing machine completed to determine whether its components qualify for reuse or refurbishment.

   Using blockchain-anchored hashes, the veracity and timeline of usage data can be verified without exposing raw telemetry—preserving both privacy and integrity.

5. **Edge Processing and Bandwidth Optimization**

   To avoid overwhelming the network and storage systems with raw data, lightweight preprocessing is performed at the edge. This includes statistical summaries (e.g., max/min/mean cycle durations), anomaly detection, and compression. Only validated or policy-relevant events are retained for DPP updates.

   This makes the system scalable to fleets of millions of devices without compromising responsiveness or cost efficiency.

6. **Case Example: Lifecycle Visibility in a Smart Washing Machine**

   Consider a smart washing machine model `WM-2025-001` equipped with embedded sensors. Over its life, the machine records 842 wash cycles, triggers two predictive maintenance alerts, and sends telemetry showing a 5% drop in spin efficiency. Each event is signed and securely pushed to the backend. Key events—such as a technician's visit to replace a drum bearing—are linked to these alerts and recorded on-chain.

   Later, at the point of resale or recycling, this sensor-backed history informs stakeholders about the product's wear, energy performance, and service record, enabling confident reuse, warranty validation, or disassembly planning.

By embedding IoT into the DPP ecosystem, we ensure that lifecycle data is not only up to date but rooted in objective, machine-generated evidence. This reduces fraud, increases automation, and enhances the value of passports across regulatory, commercial, and consumer-facing applications—enabling truly data-driven circular economy practices.

Conclusion

This paper presents a comprehensive architectural framework for designing decentralized Digital Product Passports (DPPs) that align with the goals of circular economy, regulatory compliance, and scalable industry adoption. By combining blockchain, off-chain storage, privacy-preserving cryptographic techniques, and IoT-based data acquisition, our design addresses the core challenges of traceability, trust, data sovereignty, and interoperability.

The hybrid architecture we propose ensures tamper-evident lifecycle records while preserving privacy and GDPR compliance through off-chain encrypted storage and selective disclosure mechanisms. Smart contracts enable real-time enforcement of environmental and legal policies, eliminating manual verification burdens and increasing system transparency. IoT integration allows dynamic and accurate recording of product events, transforming DPPs from static data carriers into living, auditable systems that reflect real-world usage.

Crucially, the framework accommodates a diverse ecosystem of stakeholders—manufacturers, consumers, recyclers, regulators—through standardized interfaces such as Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and linked-data formats like JSON-LD and AAS. This ensures that data remains verifiable, usable, and exchangeable across organizational and jurisdictional boundaries.

Taken together, the system design provides a viable blueprint for implementing next-generation product traceability platforms that are decentralized, privacy-respecting, scalable, and regulation-ready. Future work may explore large-scale pilots in specific product domains (e.g., white goods, electronics, batteries), formal verification of smart contracts, and the use of machine learning on aggregated passport data to support predictive sustainability analytics.

With the right technological foundation, Digital Product Passports can serve not only as compliance tools, but as strategic enablers of circular business models, sustainable innovation, and consumer trust in global supply chains.

References

1. F. Stodt, P. Ruf, C. Reich, Blockchain-enabled digital product passports for enhancing security and lifecycle management in healthcare devices, in: 2024 8th Cyber Security in Networking Conference (CSNet), 2024, pp. 44–51. doi:10.1109/CSNet64211.2024.10851725.
2. S. Çetin, D. Raghu, M. Honic, A. Straub, V. Gruis, Data requirements and availabilities for material passports: A digitally enabled framework for improving the circularity of existing buildings, Sustainable Production and Consumption 40 (2023) 422–437. doi:10.1016/j.spc.2023.01.024.
3. K. Berger, R. J. Baumgartner, M. Weinzerl, J. Bachler, J.-P. Schöggl, Factors of digital product passport adoption to enable circular information flows along the battery value chain, in: Procedia CIRP, Vol. 116, 2023, pp. 528–533.
4. C. Plociennik, M. Pourjafarian, A. Nazeri, W. Windholz, J. Rickert, T. Hagedorn, T. Vogelgesang, Requirements for a digital product passport to boost the circular economy, in: INFORMATIK 2022, 2022.
5. M. Jansen, T. Meisen, C. Plociennik, H. Berg, A. Pomp, W. Windholz, Stop guessing in the dark: Identified requirements for digital product passport systems, Systems 11 (3) (2023). doi:10.3390/systems11030124.
6. M. Pourjafarian, C. Plociennik, A. Nazeri, J. Rickert, T. Hagedorn, W. Windholz, A multi-stakeholder digital product passport based on the asset administration shell, in: 2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA), 2023, pp. 1–8. doi:10.1109/ETFA57862.2023.10267163.
7. P. D. Timms, M. R. N. King, Complexity in the delivery of product passports: A system of systems approach to passport lifecycles, in: 2023 18th Annual System of Systems Engineering Conference (SoSE), 2023, pp. 1–8. doi:10.1109/SoSE58292.2023.10192532.
8. C. Ducuing, R. H. Reich, Data governance: Digital product passports as a case study, Competition and Regulation in Network Industries 24 (1) (2023) 3–23. doi:10.1177/17835917231152417.
9. L. Panza, G. Bruno, F. Lombardi, Integrating absolute sustainability and social sustainability in the digital product passport to promote industry 5.0, Sustainability 15 (16) (2023). doi:10.3390/su151610240.
10. T. Becker, Ecodesign for sustainable products and the eu digital product passport, Zeitschrift für Stoffrecht 19 (3) (2022) 177–188.
11. J. Lövdahl, S. I. Hallstedt, J. Schulte, Implications of eu instruments on company capabilities to design more sustainable solutions—product environmental footprint and digital product passport, in: Proceedings of the Design Society: 24th International Conference on Engineering Design (ICED23), 2023, pp. 2245–2254.
12. P. Ospital, D. H. Masson, C. Beler, J. Legardeur, A digital product passport to support product transparency and circularity, Global Fashion Conference 2022 (2022).
URL https://hal.science/hal-04082837
13. M. R. N. King, P. D. Timms, S. Mountney, A proposed universal definition of a digital product passport ecosystem (dppe): Worldviews, discrete capabilities, stakeholder requirements and concerns, Journal of Cleaner Production 384 (2023) 135538. doi:10.1016/j.jclepro.2022.135538.
14. K. Voulgaridis, T. Lagkas, C. M. Angelopoulos, A.-A. A. Boulogeorgos, V. Argyriou, P. Sarigiannidis, Digital product passports as enablers of digital circular economy: a framework based on technological perspective, Telecommunication Systems 85 (4) (2024) 699–715. doi:10.1007/s11235-024-01104-x.

15. F. Psarommatis, G. May, Digital product passport: A pathway to circularity and sustainability in modern manufacturing, Sustainability 16 (1) (2024). doi:10.3390/su16010326.
16. M. Greiner, K. Seidenfad, C. Langewisch, A. R. Hofmann, U. Lechner, The digital product passport: Enabling interoperable information flows through blockchain consortia for sustainability, in: Proceedings of the International Conference on Industry 4.0 and Circular Systems (I4CS), Springer, 2024, pp. 377–396, greiner *et al.* discuss blockchain-consortium models for DPP interoperability, highlighting trade-offs between public transparency and enterprise privacy. doi:10.1007/978-3-031-XXXX-X_23.
URL https://doi.org/10.1007/978-3-031-XXXX-X_23
17. CE-RISE Consortium, Mapping dpp knowledge gap and stakeholder needs, deliverable 1.1, Horizon Europe Project CE-RISE (2024).
URL https://www.ce-rise.eu