Analysis file for blockchain integration within the Digital Product Passport (DPP)

AI-translated version from french to english

BE THE FUTURE
BE BLOCKCHAIN

Project subsidized by the Walloon Region under the DigitalWallonia4Trust program - PRW136

Table of Content

1. Glossary and Abbreviations..... 1
2. Introduction and Context..... 4
3. Executive Summary..... 5
4. Regulatory Framework Review..... 6
    4.1. ESPR..... 6
        4.1.1. Main Objectives..... 6
        4.1.2. Products Concerned..... 7
        4.1.3. Obligations for Companies..... 7
        4.1.4. Application Timeline..... 7
    4.2. Digital Product Passport (DPP)..... 8
5. Challenges for Wallonia and Local SMEs..... 9
    5.1. Regulatory Compliance and Risk Reduction..... 9
    5.2. Opportunity for Differentiation and Competitiveness..... 9
    5.3. Simplification of Exchanges and Interoperability..... 9
    5.4. Digital Transformation and Upskilling..... 9
    5.5. Contribution to Ecological Transition and the Circular Economy..... 10
    5.6. Strategic Positioning of Wallonia in European Initiatives..... 10
6. State of the Art..... 10
    6.1. Standardization..... 10
        6.1.1. ISO Standards..... 10
        6.1.1.1. ISO / IEC 15459 (Unique Identification)..... 11
        6.1.1.2. ISO / IEC 20248 (Data Authenticity)..... 11
        6.1.1.3. ISO / IEC 18004 (RFID)..... 11
        6.1.2. AIDC (Automatic Identification and Data Capture)..... 12
        6.1.3. GTIN (Global Trade Item Number)..... 12
        6.1.4. L'URI (Uniform Resource Identifier)..... 13
        6.1.5. GS1 Standardization..... 13
        6.1.6. GS1 Digital Link..... 13
        6.1.7. GS1 DataMatrix..... 15
        6.1.8. Conclusion on Standardization:..... 15
    6.2. Review of Initiatives..... 16
        6.2.1. Europe..... 16
        6.2.1.1. CIRPASS Projects :..... 16
        6.2.1.2. Global Battery Alliance – Battery Passport :..... 16

6.2.1.3. GS1 in Europe :.....16
6.2.1.4. Private Initiatives.....17
6.2.1.5. Belgium.....18
6.2.2. International and multi-Region.....19
6.2.3. Conclusion on Initiatives.....19
7. Market Study.....20
7.1. Market Study: Cross-Analysis of Interviews.....20
7.2. A Strong Interest in Traceability and Compliance.....20
7.3. Heterogeneous, Often Siloed Tools.....20
7.4. Complex Management of Technical Data.....20
7.5. Towards Growing Awareness of the DPP.....21
7.6. A Measured Openness to Blockchain.....21
7.7. Strong Expectations for Support.....21
7.8. Conclusion.....21
8. Blockchain Solution Proposal.....22
8.1. Objectives: Going Beyond the Limits of the CIRPASS Architecture.....22
8.2. Design Principle of a Decentralized Solution.....23
8.3. Proposal for a Decentralized Architecture for the DPP.....25
8.3.1. Functional and Operational Logic of the Decentralized Solution.....26
8.3.2. Functional Diagram.....29
8.3.3. European Portal Functionalities.....32
8.3.4. Regional or Sectoral Portals.....33
8.4. Deployment Plan at the Walloon Scale.....33
8.5. Economic and Competitive Perspectives.....35
8.6. Conclusion and Limitations.....36
9. General Conclusion, Limitations, and Recommendations.....37
Recommendations.....37
Limitations.....38
10. Bibliography.....39

1. Glossary and Abbreviations

- **AIDC (Automatic Identification and Data Capture):** Set of technologies (barcodes, RFID, QR codes) enabling the identification and traceability of products in the DPP.
- **AI (Assurance of Information):** Guarantees the quality, reliability, and integrity of data exchanged in the DPP.
- **API (Application Programming Interface):** Software interface allowing communication between the DPP and other IT systems.
- **CEN (European Committee for Standardization):** Official body responsible for developing harmonized European standards in many industrial and service sectors, to facilitate the free movement of products and services within the single market.
- **CENELEC (European Committee for Electrotechnical Standardization):** European body specializing in the standardization of the electrotechnical and electronic fields, covering notably electrical equipment, energy, and digital technologies.
- **CEAP (Circular Economy Action Plan):** European Commission program promoting the circular economy, of which the DPP is a central tool.
- **CIRPASS (Cross-sectoral Interoperable Registries for Product Asset Sustainability):** European project aiming to define a common and interoperable DPP architecture across several industrial sectors.
- **DAO (Decentralized Autonomous Organization):** Organizational structure operating on the blockchain, governed by rules coded in smart contracts and collectively controlled by its members. A DAO enables transparent and decentralized decision-making, without a central authority, through a voting system generally linked to token ownership.
- **DID (Decentralized Identifier):** Standard allowing decentralized digital identification, applied to identity management in the DPP.
- **DPP (Digital Product Passport):** Digital tool centralizing and sharing product information throughout its lifecycle, to guarantee traceability and compliance.
- **DPPSD (Digital Product Passport System Demonstrator):** Pilot project intended to test the implementation of the DPP under real-world conditions and validate its interoperability.

- **DW4T (Digital Wallonia for Trust):** Walloon initiative supporting the implementation of trusted digital solutions, including the DPP.
- **eIDAS (Electronic Identification, Authentication and Trust Services):** European regulatory framework on electronic identification and trust services, applied to the DPP.
- **EORI (Economic Operator Registration and Identification):** Unique number to identify economic operators in the EU, usable in the DPP.
- **ESPR (Ecodesign for Sustainable Products Regulation):** European regulatory framework setting ecodesign requirements and introducing the obligation of the DPP for certain products.
- **EUID (European Unique Identifier):** Unique European identifier for companies, facilitating their traceability in the DPP.
- **GLN (Global Location Number):** Unique identifier allowing an entity (company, site, warehouse) to be referenced in the DPP.
- **GTIN (Global Trade Item Number):** Unique identifier assigned to a product via GS1, essential for its integration into a DPP.
- **IEC (International Electrotechnical Commission):** Global standardization body in the electrotechnical field, complementing ISO.
- **ISO (International Organization for Standardization):** Global standardization body whose standards (e.g., ISO 9001, ISO 14001) serve as the basis for the DPP.
- **JSON-LD (JavaScript Object Notation for Linked Data):** Structured data format facilitating interoperability and information sharing in the DPP.
- **LEI (Legal Entity Identifier):** Global identifier for legal entities, used for the interoperability of financial data and the DPP.
- **The Asset Administration Shell (AAS):** Standardized digital representation of a physical asset, designed for interoperability and data exchange within the framework of Industry 4.0 and the Industrial Internet of Things (IIoT).
- **RFID (Radio Frequency Identification):** Radio frequency identification technology, facilitating the automatic capture of product data in the context of the DPP.
- **Sharding:** Sharding is a data partitioning technique that consists of dividing a database or system into several fragments called shards. Each shard contains a portion of the data and functions as an autonomous database, but the whole remains coherent and accessible as a unit.

- **Smart Contract:** Computer program that automatically executes predefined actions when certain conditions are met, all stored on a blockchain to guarantee its immutability and transparency.
- **SSCC (Serial Shipping Container Code):** Unique identifier for logistical units (parcels, pallets) used for product tracking in the DPP.
- **URI (Uniform Resource Identifier):** Address format allowing online referencing and access to DPP data.
- **VC (Verifiable Credentials):** Verifiable and unforgeable data used to prove compliance or authenticity in the DPP.

2. Introduction and Context

For several years, the European Union has been stepping up its efforts to reconcile industrial competitiveness, innovation, and sustainability. The European Green Deal strategy, followed by a series of structuring regulations, aims to transform value chains by fully integrating the principles of circular economy and transparency. In this dynamic, the Ecodesign for Sustainable Products Regulation (ESPR) constitutes a major step forward. It progressively imposes new requirements on manufacturers, importers, and distributors, notably by introducing the Digital Product Passport (DPP) as a reference instrument.

The DPP is presented as a universal digital passport attached to each product, containing standardized and verified information on its origin, components, environmental impacts, as well as its possibilities for repair, reuse, and recycling. Beyond its role in regulatory compliance, this tool opens the way to much finer management of product lifecycle, better consumer information, and reinforced cooperation between economic actors.

For Wallonia, a region particularly exposed to these changes, the stakes are considerable. It is to support this transition that the Walloon Region entrusted BE Blockchain, in collaboration with Agoria and Logistics in Wallonia, with the mission of conducting an exploratory study around the DPP. This preliminary research is based on the European state of the art, the initial feedback from the CIRPASS consortium and its extensions (CIRPASS-2), and aims to propose an ideal architecture integrating blockchain technology, specifically adapted to the needs of Walloon SMEs, which constitute the essential part of the regional economic fabric. The objective is to transform a regulatory constraint into a true strategic lever for regional competitiveness, in line with the priorities of DigitalWallonia4Trust, Industry 4.0, and the circular economy.

The project is also part of the continuation of the first program financed by the Walloon Region, within which a consortium of regional actors had already developed several blockchain demonstrators. In this continuity, the objective here is to explore the more complete development of a demonstrator applied to the DPP, alongside the upcoming entry into force of the ESPR regulation, in order to prepare Walloon companies for the new obligations while maximizing the strategic and economic benefits.

.

3. Executive Summary

The implementation of the Digital Product Passport (DPP) within the framework of the ESPR (Ecodesign for Sustainable Products Regulation) represents a systemic transformation of industrial value chains. This document proposes a synthesis of the work carried out in connection with the pilot experiments conducted in Wallonia in a collaborative dynamic integrating institutions, companies, and technological experts. The objective was to evaluate the conditions for implementing the DPP, identify the technical and organizational barriers, and propose a framework for action adapted to the local ecosystem, while respecting emerging European standards.

Through a regulatory, technical, and operational analysis, the report highlights the key challenges related to data interoperability, unique product identification (AIDC, GTIN, URI, etc.), and the governance of shared information. It emphasizes the importance of close alignment between European standards (CIRPASS, GS1 Digital Link, ISO/IEC 15459…) and on-the-ground realities. Feedback from local industrial actors reveals both a growing interest in the DPP and a complexity of implementation, particularly around the integration of information systems, data protection, and component traceability.

The technological dimension constitutes a structuring lever, particularly through the integration of blockchain as a distributed trust registry. It meets the integrity, auditability, and decentralization requirements imposed by the DPP. Several use cases presented in the report illustrate how blockchain allows for the creation of an unforgeable link between product identifiers, lifecycle events, and compliance certificates, while respecting the GDPR through the use of technologies such as DIDs (Decentralized Identifiers) and Verifiable Credentials (VC) combined with access management via AccessPolicies. This positioning is all the more strategic as eIDAS 2.0 standards, identity wallets, and asset registries take shape at the European level.

This report also presents a mapping of the essential functional building blocks for the implementation of an interoperable, secure, and scalable DPP. It highlights the interest of developing a sovereign demonstrator capable of serving both the objectives of the CEAP (Circular Economy Action Plan) and the regulatory requirements of the ESPR, while relying on the building blocks established by the CIRPASS project. The latter constitutes an essential standardization base, but the limitations identified in its work show that an extension combining these foundations with distributed ledger technologies, such as blockchain, would allow for a more effective response. It would indeed provide a credible answer to the challenges of security, transparency, immutability, and privacy by design, thereby reinforcing the territory's ambition for digital innovation. This modular approach, oriented towards openness and standardization, would allow industrial players of various sizes to be involved in a structured, resilient, and durable digital transition in accordance with sustainability principles.

Wallonia, through its initiatives such as DW4T (Digital Wallonia for Trust), demonstrates its desire to occupy a pioneering position. The work presented in this report must now pave the way for concrete experiments, integrating the blockchain building blocks, unique identifiers, traceability protocols, and user interfaces necessary for a fully operational DPP, aligned with European ambitions for digital sovereignty and sustainability.

4. Regulatory Framework Review

The ESPR (Ecodesign for Sustainable Products Regulation) constitutes the new European legislative framework aiming to strengthen the sustainability of products placed on the Union market. Adopted in June 2024, it is part of the continuity of the European Green Deal and the CEAP (Circular Economy Action Plan), by extending the ecodesign approach to a greater number of product categories. This regulation establishes a common basis for improving the repairability, reusability, and recyclability of goods, while ensuring greater transparency in value chains. The ESPR thus marks a decisive step in the transition towards a circular economy and constitutes the regulatory foundation on which the progressive introduction of the DPP is based.

4.1. ESPR

The Ecodesign for Sustainable Products Regulation (ESPR), adopted in June 2024, constitutes one of the pillars of the European Green Deal and the action plan for the circular economy (CEAP). It gradually replaces the 2009 Ecodesign Directive and considerably broadens its scope. The ESPR establishes a horizontal framework aimed at making products placed on the Union market more sustainable, repairable, reusable, and recyclable, while strengthening the transparency of value chains.

4.1.1. Main Objectives

The ESPR pursues several strategic objectives that are at the heart of the European Green Deal. Firstly, it aims to reduce the environmental impact of products throughout their lifecycle, from design to recycling, by promoting repairability, reuse, and circularity. It also intends to reduce the European Union's dependence on critical raw materials, by optimizing the recovery of resources already present on the market and improving the management of material flows. Furthermore, the regulation constitutes a lever for competitiveness and innovation by encouraging companies to develop new business models, invest in ecodesign, and offer more sustainable products. Finally, it reinforces transparency by giving consumers, industry players, and control authorities structured and reliable access to product data

thanks to the Digital Product Passport, a central tool for monitoring and verifying information throughout the value chain.

4.1.2. Products Concerned

The ESPR introduces an approach based on sectoral delegated acts. The first targeted sectors are:

- Batteries (entry into force in 2027, already governed by the Batteries Regulation).
- Textiles (second half of 2027).
- Electronic and household appliances (horizon 2030).
- Construction products and furniture (progressive timetable currently being defined).

These categories represent sectors with a high environmental impact and are strongly concerned by traceability and circularity requirements.

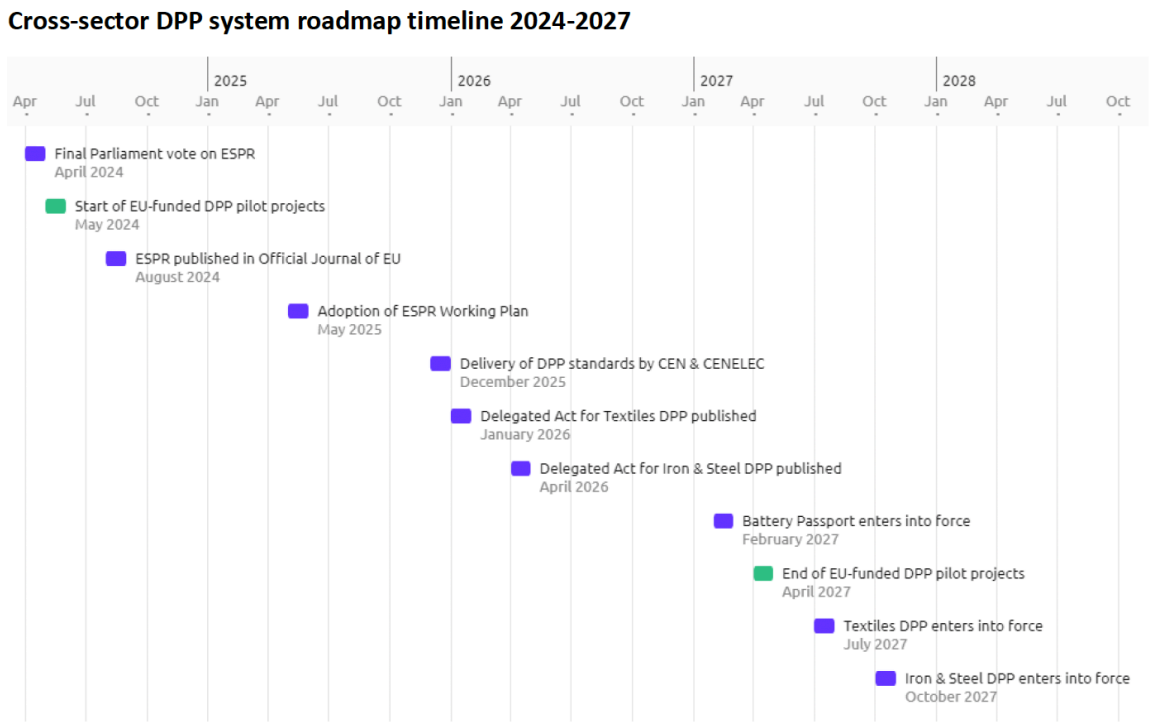
4.1.3. Obligations for Companies

Concretely, the ESPR introduces new obligations for responsible economic operators, whether they are manufacturers, importers, or distributors. They must create and update a digital passport for each product concerned, incorporating all the information required by the regulation. These actors are also required to guarantee the quality, accuracy, and availability of data shared across the value chain, in order to strengthen trust between partners and facilitate controls. The information contained in the DPP must also be kept for a minimum defined period, which can be up to ten years after being placed on the market in certain product categories, in accordance with Article 12 of the regulation. Finally, the system must provide for differentiated access to data, so that each stakeholder, consumers, recyclers, market surveillance authorities, or compliance bodies, can have the level of information that is relevant and necessary for their role.

4.1.4. Application Timeline

The ESPR regulation will be progressively deployed from 2027 by product category and with a logical sequence of progressive extension to other sectors and products. Here is a summary of the agenda:

- 2024: official adoption of the regulation.
- 2025-2026: development of technical standards and implementation of sectoral pilot projects (CEN/CENELEC, CIRPASS and other initiatives).
- 2027: entry into force of the first mandatory digital passports for batteries, closely followed by textiles.
- 2030: progressive extension to other product categories (consumer electronics, furniture, construction).



DPP - CIRPASS_Cross-sector_and_sector-specific_DPP_roadmaps_1.2_2024-03-27_1527

4.2. Digital Product Passport (DPP)

The Digital Product Passport (DPP) is a central regulatory instrument of the ESPR regulation, aiming to support the transition towards a circular economy within the European Union. Its purpose is to guarantee structured, secure, and interoperable access to key product information throughout its lifecycle, for consumers as well as for economic operators and authorities.

Concretely, the DPP integrates a unique product identifier, often a GTIN (Global Trade Item Number), or equivalent, associated with technical, environmental, and compliance metadata. This information is accessible via a digital link (URI), encoded in a machine-readable medium (QR Code, DataMatrix, RFID), and compliant with GS1 and ISO standards (e.g., ISO/IEC 15459, 20248, 18004).

The objective is to promote transparency, traceability, and circularity by ensuring the availability of reliable information (composition, repairability, provenance, carbon footprint, etc.) within an interoperable and harmonized ecosystem at the European level. This system is gradually deployed by product category via delegated acts, with entry into force expected from 2027.

5. Challenges for Wallonia and Local SMEs

The introduction of the Digital Product Passport (DPP), under the European ESPR regulation, represents a major turning point for Walloon companies. This regulatory obligation should not be perceived as an additional constraint, but as a strategic opportunity to strengthen the competitiveness of SMEs in a context of ecological, digital, and industrial transition.

5.1. Regulatory Compliance and Risk Reduction

The first challenge lies in alignment with European regulation. Companies that do not prepare for the DPP in time will expose themselves to risks of non-compliance, which could lead to financial penalties or exclusion from certain markets. For Wallonia, whose economy is strongly oriented towards Europe with more than 40 billion euros exported each year, this challenge is particularly strategic. The rapid adoption of the DPP is not only a regulatory obligation, it is an essential condition for preserving secure access to markets and protecting the reputation of its companies.

5.2. Opportunity for Differentiation and Competitiveness

Beyond compliance, the DPP constitutes a strategic tool allowing SMEs to bring increased transparency to the traceability, sustainability, and circularity of their products. Companies capable of demonstrating the quality of their processes, their reduced environmental footprint, or their recycling capacity will strengthen their attractiveness to end customers, industrial contractors, and investors. For Walloon SMEs, often positioned as subcontractors or niche suppliers, the DPP can become a decisive differentiation factor.

5.3. Simplification of Exchanges and Interoperability

One of the major challenges for SMEs is managing the complexity of the data required by the DPP (components, substances, carbon footprint, repairability, etc.). By relying on harmonized European standards, the DPP will help reduce administrative costs related to document management and compliance audits. Interoperable digital solutions, integrated into logistics chains or sectoral platforms, will help lighten the burden on SMEs while improving the fluidity of exchanges.

5.4. Digital Transformation and Upskilling

The introduction of the DPP acts as an accelerator of companies' digital transformation. For Walloon SMEs, this is an opportunity to modernize their information systems, strengthen the collection and exploitation of product data, and adopt innovative technologies such as blockchain, artificial intelligence applied to sustainability, or digital twins. This effort is

accompanied by upskilling of personnel, essential for strengthening the resilience and agility of local companies.

5.5. Contribution to Ecological Transition and the Circular Economy

Wallonia has placed innovation, sustainability, and the circular economy at the heart of its economic development strategy. The DPP fully aligns with this vision, by making it possible to measure and enhance the efforts of companies in terms of carbon footprint, material reuse, and product recyclability. For SMEs active in strategic regional sectors (chemistry, construction, logistics, electronics, textile), the DPP constitutes a concrete lever for integrating their activities into a sustainable and European-recognized economic model.

5.6. Strategic Positioning of Wallonia in European Initiatives

Wallonia is also part of a proactive dynamic through its DigitalWallonia4Trust program, which has already enabled the development of initial regional blockchain demonstrators. In this continuation, the exploration of a digital product passport based on blockchain constitutes a strategic opportunity to propose a solution that goes beyond the standards proposed in CIRPASS. Although Wallonia is not a direct member of the CIRPASS consortium, several Belgian companies actively participate in it, thus strengthening the link between the regional ecosystem and European initiatives. This approach allows the Region to enhance its own technological expertise, while contributing to shaping more resilient, secure solutions adapted to the needs of local SMEs.

6. State of the Art

6.1. Standardization

6.1.1. ISO Standards

The integration of ISO/IEC standards constitutes an essential foundation for the architecture of the Digital Product Passport, guaranteeing its interoperability, reliability, and compliance with European requirements. The ISO/IEC 15459 standard ensures unique, global, and unambiguous identification of products and entities, a central pillar for linking each item to its DPP. In addition, the ISO/IEC 20248 standard makes it possible to guarantee the authenticity of data exchanged through AIDC media (barcodes, RFID), thanks to an integrated digital signature verifiable offline. Finally, the ISO/IEC 18004 standard defines the technical specifications for 2D barcodes including QR Codes, ensuring via GS1 standards

(GTIN, GLN, etc.), compatibility with identification and reading devices deployed in the industry and secure accessibility to DPP URIs via standard optical reading devices. Together, these standards form a robust technical basis for the identification, traceability, and integrity of product data in the DPP ecosystem.

6.1.1.1. ISO / IEC 15459 (Unique Identification)

The ISO/IEC 15459 standard constitutes a fundamental basis for unique identification within the framework of the DPP. It defines the principles and structures allowing a global, unique, and unambiguous identifier to be assigned to physical objects (products, components, equipment) and logistical entities, thus guaranteeing interoperability within international supply chains.

This standard is particularly relevant in the context of AIDC (Automatic Identification and Data Capture), as it allows a product to be reliably linked to its digital data via a stable identifier. It is all the more crucial because the DPP relies on the ability to track and authenticate each object individually, including in complex and multi-actor environments.

In accordance with the requirements of the ESPR regulation, ISO/IEC 15459 is often combined with other standards such as GTIN, GLN, or GS1 Digital Link structures, reinforcing traceability and transparency throughout the entire product lifecycle.

6.1.1.2. ISO / IEC 20248 (Data Authenticity)

The ISO/IEC 20248 standard plays a central role in the integrity and authenticity of data transmitted via AIDC (Automatic Identification and Data Capture) media, particularly within the framework of the DPP. It specifies a digitally signed data structure, capable of being incorporated into barcodes or RFID tags, allowing any compliant reader to verify the origin and veracity of the data without connecting to a remote server.

This decentralized self-verification capacity is particularly suited to the requirements of the ESPR regulation, notably to combat fraud, guarantee the reliability of product information, and strengthen trust between stakeholders (manufacturers, authorities, consumers).

In the DPP ecosystem, ISO/IEC 20248 can be used in addition to unique identifiers (e.g., ISO/IEC 15459) to associate verifiable metadata with each product, throughout its lifecycle.

6.1.1.3. ISO / IEC 18004 (RFID)

The ISO/IEC 18004 standard defines the technical characteristics of RFID (Radio Frequency Identification) systems for the automatic identification of objects. It specifies the air interfaces (or communication link) between the reader and the RFID tag for different frequency bands (LF, HF, UHF), thus ensuring the interoperability of AIDC devices.

Within the framework of the DPP, this standard constitutes an essential reference for contact-less data reading and writing. The ESPR authorizes the use of RFID media (in addition or as an alternative to QR Codes/Data Matrix), provided they comply with recognized and interoperable ISO standards at the European level.

The use of RFID tags compliant with ISO/IEC 18004 helps ensure robust traceability, even in an industrial environment, without line of sight, and facilitates logistics management throughout the product lifecycle.

6.1.2. AIDC (Automatic Identification and Data Capture)

AIDC encompasses a set of technologies intended for the automatic identification of objects, products, or assets, and the capture of associated data. These technologies are central to the DPP ecosystem, as they allow for ensuring the reliability, interoperability, and automation of information transfer throughout the product lifecycle.

The AIDC approach relies on the use of machine-readable media, such as barcodes, 2D codes (QR Code, DataMatrix), or RFID tags, combined with optical or radio reading devices. These media embed product identifiers (GTIN, GLN, etc.) and metadata coded according to ISO or GS1 standards, making it possible to ensure international coherence in logistics, traceability, or regulatory compliance information systems.

In connection with the ESPR requirements, AIDC makes it possible to effectively link physical objects to digital passports hosted on the web, via standardized identifiers. This architecture guarantees compatibility with existing infrastructures and universal access to product information, via any compliant reader.

AIDC technologies have thus become an essential technical pillar for the implementation of DPPs, ensuring automated, reliable, and secure reading of identifiers in all phases of the value chain, from production to distribution, up to recycling.

6.1.3. GTIN (Global Trade Item Number)

The GTIN (Global Trade Item Number) is a globally recognized and standardized identifier by GS1, designed for the unique identification of commercial items. It plays a central role in the DPP architecture, as a reference identifier allowing a physical product to be linked to its digital data in an unequivocal and internationally interoperable manner. The GTIN can also be enriched thanks to AIs (Application Identifiers), standardized prefixes defined by GS1 allowing additional information to be added such as the batch number (AI 10), the serial number (AI 21), or the expiration date (AI 17). These elements are often encapsulated in QR codes or in GS1 Digital Link structures, offering direct reading and rich semantics to product data.

The GTIN is part of the ISO/IEC 15459 standards ecosystem, thereby guaranteeing its compatibility with AIDC systems. This normative framework ensures reinforced interoperability and allows the requirements to be adapted to each product category defined by delegated acts. In the logic of the DPP, the GTIN is often encoded in a QR Code compliant with ISO/IEC 18004, offering direct, secure, and semantically enriched access to product information.

6.1.4. L'URI (Uniform Resource Identifier)

The URI is a standardized identifier that allows unique, sustainable, and interoperable access to a digital resource, here, to the essential data of the DPP. Within the framework of the ESPR regulation, URIs play a central role: they link physical identifiers (such as GTIN, GLN, or serial number) to digital data accessible via the web, while ensuring compatibility with automatic identification systems (AIDC).

By using a URI compliant with the GS1 Digital Link specification, as we will see in section 6.1.6, each product can be associated with a structured link readable by a browser or a machine. This URI encapsulates both the product identifier and the associated metadata, making access to product information fluid, secure, and compliant with the transparency requirements of the European Union.

6.1.5. GS1 Standardization

The GS1 organization is an international non-profit organization, recognized for having developed and maintained the most widely used identification systems in global commerce, such as GTIN, GLN, SSCC, and barcodes. Within the framework of the DPP, the European Commission has identified GS1 as one of the technical pillars most capable of providing a unique, interoperable, and standardized identification infrastructure on a global scale.

GS1 standards are already deployed in more than 150 countries and cover the entire value chain: manufacturers, importers, distributors, logistics providers, and even consumers. Their adoption guarantees compatibility with AIDC (Automatic Identification and Data Capture) systems, while ensuring consistency with the requirements for traceability, access to product data, and portability set by the ESPR. Consequently, GS1 identifiers (notably GTIN, GLN, or Digital Link) constitute the backbone of the recommended identification system for the implementation of the DPP.

6.1.6. GS1 Digital Link

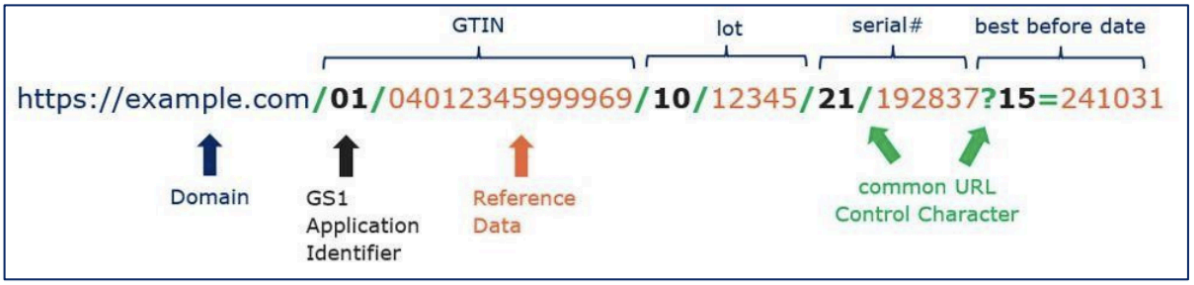
The GS1 Digital Link is a standardized URI (Uniform Resource Identifier) structure developed by GS1 to allow an identifier such as a GTIN to become a clickable web link. It allows a product to be associated not only with its unique identifier, but also with all of its digital data, in accordance with the requirements of the DPP.

In the context of the ESPR regulation, the GS1 Digital Link constitutes the preferred method for encoding product identifiers in a QR Code compliant with the ISO/IEC 18004 standard. This approach makes the data directly accessible to consumers, authorities, and commercial partners, while guaranteeing its security and interoperability.

In this framework, each product identifier is encoded in the form of an Application Identifier (AI), which allows the GTIN to be enriched with standardized complementary information. Among the most common are the batch number (AI 10), the serial number (AI 21), or the expiration date (AI 17, in YYMMDD format according to GS1 standards). This structuring guarantees uniform and interoperable reading of data throughout the value chain.

Example of recommended URI structure :

https://id.gs1.org/01/GTIN/21/SERIAL
or
https://domainefabricant.com/01/GTIN/21/SERIAL



[1]

Each segment of the URI corresponds to a GS1 Application Identifier (AI):

01 = AI indicating the GTIN used in the context of the GS1 Digital Link
10 (optional) = Batch number 21 = Serial number
15 (optional) = Expiration date (in YYMMDD format according to GS1 standards)

This URI format allows a physical product to be dynamically linked to its digital passport hosted in a secure database, while ensuring compatibility with existing traceability, inventory, or customs systems.

The GS1 Digital Link approach reinforces data portability and system resilience, while allowing DPPs to be consulted via any compatible optical reader or smartphone, without resorting to a proprietary system.

[1] GS1 Standards enabling the EU digital product passport 2025. Available online: https://gs1.eu/wp-content/uploads/2024/12/GS1-Standards-Enabling-DPP.pdf

6.1.7. GS1 DataMatrix

The GS1 DataMatrix is a standardized 2D code symbol, compliant with the ISO/IEC 16022 standard, which allows encoding GS1 identifiers (such as GTIN, batch number, or serial number) as well as additional data in a structured format.

Within the framework of the DPP, it constitutes a recognized alternative to the QR Code, offering high data density and better readability on reduced surfaces, particularly for small products or industrial applications.

In addition to the QR code, the use of GS1 DataMatrix is recognized as a compliant option in the DPP in the technical specifications established by the CIRPASS consortium and the GS1 guidelines. This format thus allows direct access to DPP data, while ensuring compatibility with existing reading systems in logistics chains, particularly in the battery, textile, or electronics sectors.

Its adoption in the DPP is particularly relevant when printing constraints, security, or the robustness of optical readings are decisive.

6.1.8. Conclusion on Standardization:

ISO/IEC standards, GS1 standards, and AIDC technologies form a coherent, interoperable, and secure basis for the implementation of the Digital Product Passport (DPP). Their articulation makes it possible to ensure the unambiguous identification of products (via ISO/IEC 15459), the guarantee of data authenticity (via ISO/IEC 20248), as well as the compatibility of reading media (via ISO/IEC 18004, RFID, DataMatrix...).

Concretely, when a compliant AIDC code is scanned (QR Code, DataMatrix, or RFID tag), the system can automatically retrieve:

- the unique product identifier (GTIN)
- the GS1 Digital Link URI, leading to the product's secure digital record
- as well as the mandatory or contextual attributes defined for each product category: batch number, serial number, expiration date, version, etc.

These elements are encapsulated in standardized formats, guaranteeing fluid, secure, and interoperable reading by any actor in the value chain. This operation ensures compliance with the ESPR regulation, while facilitating traceability, authenticity verification, and access to product data, even offline.

6.2. Review of Initiatives

The landscape of DPP-related initiatives is currently extremely fragmented. We observe both normative approaches (GS1, CEN/CENELEC, ISO), pilot sectoral projects (batteries, textile, electronics, construction), and market technological solutions (start-ups, industrial consortia, SaaS platforms). These initiatives can be grouped according to their geographical location, their application sector, and their technological choice (use or non-use of blockchain).

6.2.1. Europe

6.2.1.1. CIRPASS Projects :

The CIRPASS project (Cross-sectoral Interoperable Registries for Digital Product Passports) constitutes one of the most structuring works on the DPP. Conducted until March 2024, CIRPASS 1 aimed to establish a clear cross-sectoral definition of the DPP, a common data model, as well as an open exchange protocol to facilitate interoperability between sectors (electronics, textiles, batteries). Several roadmaps and prototypes have been developed, allowing pilot devices to be tested and a harmonized approach to be built.

The CIRPASS-2 extension is part of the Digital Europe program. It targets the large-scale pilot phase, notably with DPPs validated in the textile, battery, and electronics value chains, in preparation for the progressive application of the ESPR regulation from 2027. CIRPASS-2 consolidates the operational, interoperable, and sectoral dimension of the product passport while ensuring a shared technical and normative foundation.

6.2.1.2. Global Battery Alliance – Battery Passport :

The Battery Passport is led by a global alliance (GBA, based in Brussels but active internationally) and constitutes the flagship project aligned with the European regulation on batteries. The objective is to ensure harmonized monitoring of the lifecycle, carbon footprint, and circularity of batteries. Governance is technologically neutral, but several implementers (e.g., Circulor, Minespider) are exploring blockchain as a registry of authenticity.

6.2.1.3. GS1 in Europe :

GS1 provides a normative repository via GS1 Digital Link and unique product identification (GTIN). The approach relies on open, interoperable standards, adopted by numerous DPP pilot projects. It does not prescribe the use of blockchain but guarantees the uniqueness and persistence of identifiers.

6.2.1.4. Private Initiatives

In the European space, numerous projects reflect the diversity of technological and sectoral approaches around the digital product passport. In France, several solutions stand out. Keeex, for example, relies on cryptographic mechanisms (timestamping, signature, integrity) to ensure data reliability, while remaining outside of blockchain logic. Conversely, Tilkal has developed an inter-company traceability infrastructure based on a permissioned blockchain, with use cases in the agri-food, textile, or electronics sectors. Arianee illustrates a more radically open orientation: this open-source protocol, based on Ethereum, aims to standardize the digital identity of products in the luxury and distribution sector. TextileGenesis, for its part, has gradually moved away from blockchain to adopt an SaaS logic based on certificates and material volume tokens, thus meeting a requirement for simplicity of use for textile industrialists.

In the Netherlands, innovation crystallizes around Circularise, which combines permissioned blockchain and zero-knowledge proofs (ZKP) to reconcile the confidentiality of industrial data and the transparency of supply chains. In construction, Madaster favors a centralized approach through its material passports, integrated into a logic of reuse and circularity without resorting to blockchain.

In Germany, Austria, and Switzerland, initiatives reflect a close articulation between industry, standardization, and digital innovation. Catena-X, a reference automotive ecosystem, deploys digital passports integrated into Gaia-X and the Asset Administration Shell, without relying on distributed ledgers. Spherity, on the other hand, explores decentralized identities (DID) and Verifiable Credentials, with a partial blockchain anchor, while Narravero proposes an SaaS alternative oriented towards SMEs. In luxury, the Aura Blockchain Consortium (Switzerland/Luxembourg), bringing together LVMH, Prada, and Cartier, chose a private blockchain of the Ethereum/Quorum type to guarantee the authenticity of high-end products.

Northern European countries favor SaaS and cloud solutions, such as TrusTrace in Sweden, which structures textile traceability via the collection of documentary proofs, or Whatt.io which combines NFC and blockchain infrastructure to manage the ownership and authenticity of goods. In the United Kingdom, Provenance, a pioneer of the DPP, illustrates a hybrid trajectory: after experimenting with blockchain, the solution now relies on verifiable data and hybrid architectures. iPoint-systems, for its part, offers an ESG and substance compliance software suite, without a blockchain component. In Southern Europe, Italy concentrates several notable initiatives: Certilogo relies on artificial intelligence for authentication in fashion, while The ID Factory offers an interoperable textile platform, open to blockchain integrations. In construction, Cobuilder develops solutions based on digital twins and the Asset Administration Shell, in line with emerging European standards.

Taken as a whole, these European initiatives reflect a structuring tension: on the one hand, centralized SaaS architectures, quick to implement and more accessible for SMEs; on the

other hand, blockchain experiments, often targeting sectors where trust, authenticity, and cross-sectoral traceability are particularly critical (textile, luxury, agri-food, electronics).

6.2.1.5. Belgium

Belgium is positioning itself as a fertile ground for experimenting with digital passports, with varied initiatives that reflect both the local entrepreneurial dynamic and integration into European projects. In the circular economy sector, TripleR.io, in Flanders, launched mattressID, a system intended for the monitoring and recycling of mattresses. By combining QR codes and RFID chips, the solution makes it possible to trace the composition and lifecycle of each product, thus facilitating their collection and reuse. Its architecture relies on a centralized cloud model, simple to deploy, and is already part of European pilot programs, making it a concrete example of a sectoral application aligned with circularity priorities.

In parallel, certain Belgian initiatives are exploring more decentralized approaches. Crypto Kastaar, also established in Flanders, is developing a digital passport for beers, accessible via QR or NFC. The originality of this initiative lies in its inclusion in a Web3 logic, with data anchoring on a public blockchain. This orientation reflects a desire to experiment with new models of trust and transparency, particularly suited to sectors where authenticity and brand image constitute commercial levers.

On the institutional level, GS1 Belu, based in Brussels, plays a structuring role in supporting Belgian companies. Through its workshops and resources, the organization helps SMEs prepare for the implementation of the DPP by relying on the international GS1 Digital Link standards. The approach is deliberately technology-agnostic and non-blockchain, focused on interoperability and the simplification of processes for local economic actors. Finally, the ecosystem is completed with Twintag, a young Flemish company that offers a flexible SaaS platform for creating digital passports adapted to various sectors such as textile, logistics, or electronics. Based on a centralized but extensible architecture, the solution is already integrated into several European pilots, illustrating an orientation towards rapid industrialization and transverse use.

Taken as a whole, these Belgian initiatives reveal an interesting complementarity: on the one hand, pragmatic and normative projects that aim to ensure broad adoption by SMEs; on the other hand, Web3 experiments that explore the potential of blockchain to strengthen authenticity and traceability. This diversity constitutes a strategic asset for Belgium, which can thus actively contribute to the definition of future European standards while offering local actors options adapted to different levels of technological and sectoral maturity.

6.2.2. International and multi-Region

Beyond Europe, the DPP movement is illustrated by transcontinental projects, often driven by large technology groups or international consortia. In the United States, EON is developing a centralized platform of digital passports for fashion and durable goods, integrating resale and repair services. Digimarc focuses on digital watermark identification, aligned with GS1 standards, with concrete applications in plastic recycling. In Canada, OPTEL deploys the Optchain suite, interoperable with data spaces and capable, depending on the case, of integrating distributed ledgers.

Certain initiatives more directly explore public blockchain. VeChain, in partnership with DNV, designed the My Story project, which ensures the traceability and authenticity of agri-food and luxury products thanks to its VeChainThor blockchain. The IOTA foundation has developed DPP prototypes for plastic and electronics, using its Tangle distributed ledger and integrating decentralized identities and Verifiable Credentials. Finally, the partnership between Circularise and Marubeni in Japan illustrates the export of European solutions to Asia, with the use of ZKP to protect the confidentiality of data while promoting transparency on the composition of materials.

These international projects testify to a strong experimentation dynamic, where blockchain occupies a more central place than in Europe. However, they also reflect the difficulty of finding a balance between transparency, confidentiality, and global interoperability. Where Europe favors a normative and sectoral approach driven by the ESPR regulatory framework, North American and Asian initiatives explore market models, seeking to quickly demonstrate the added value of the product passport in sectors such as luxury, agri-food, textile, or electronics.

6.2.3. Conclusion on Initiatives

The landscape of DPP initiatives in 2025 illustrates the coexistence of decentralized and centralized architectures. Some solutions rely on blockchain to provide immutability and verifiable attestations, while others favor open standards and simplicity of integration. CIRPASS, Battery Pass, and GS1 structure technical and regulatory harmonization, while public and private providers accelerate sectoral deployments. Belgium benefits from local initiatives and a strong European anchor, offering favorable ground for the pragmatic implementation of the DPP for SMEs.

7. Market Study

7.1. Market Study: Cross-Analysis of Interviews

Within the framework of the DPP mission in Wallonia, five semi-structured interviews were conducted with regional industrial actors from different sectors (pharma, cosmetics, medical devices, furniture, agri-food, etc.). The objective was to identify their current product data management practices, their expectations regarding a DPP, the barriers encountered, as well as their perception of emerging digital solutions, including blockchain. This feedback allows for a structured and representative inventory of the Walloon economic fabric, upstream of the implementation of a larger-scale DPP solution.

7.2. A Strong Interest in Traceability and Compliance

All the companies interviewed express a growing need to guarantee the traceability, quality, and compliance of products. This requirement is all the stronger since the sectors concerned mainly relate to agri-food, pharmaceuticals, cosmetics, or medical devices. In these highly regulated sectors, existing information systems aim to meet normative obligations (ISO 9001, HACCP, etc.), but struggle to ensure a fluid, transverse, and up-to-date vision of product data.

7.3. Heterogeneous, Often Siloed Tools

The digital ecosystem of companies is largely fragmented. ERP, Excel files, Access databases, document management software, or quality software are used in parallel, without real interoperability. Several respondents mention difficulties in getting their internal tools to communicate or integrating external partners into the information chains. Manual duplication of data remains frequent, causing errors and a significant loss of time.

7.4. Complex Management of Technical Data

Technical product information (data sheets, specifications, components, labeling, regulatory documentation) is scattered across several systems, often not updated. Some companies still keep paper archives. The absence of a unique repository or clear governance complicates access to reliable data. Version changes, multiple formats, and the multiplicity of contributors hinder the consolidation of a single product view.

7.5. Towards Growing Awareness of the DPP

While the notion of the DPP itself is still little known, all companies show interest in a structured system allowing for the centralization, tracing, and sharing of product data throughout the lifecycle. The DPP is perceived as a lever for responding to the obligations of the ESPR, but also as an internal tool for quality monitoring, reduction of non-conformities, and improvement of maintenance or customer service. Some already foresee use cases in their value chain.

7.6. A Measured Openness to Blockchain

Blockchain technology is not familiar to the majority of interlocutors, but several of them understand its theoretical advantages: immutability, timestamping, security, decentralized traceability. However, its image remains associated with crypto-finance and technical complexity. To be adopted, blockchain must be invisible to the end user, integrated into business tools, and demonstrate clear added value (e.g., proofs of compliance, simplification of audits, interoperability).

7.7. Strong Expectations for Support

Companies express a need for strong support: help with diagnosis, data mapping, assistance with structuring repositories, assistance with selecting standards (GTIN, URI, JSON-LD, etc.), training, etc. The integration of a DPP, and even more so blockchain, presupposes an increase in digital maturity. The readability of pilot initiatives, the clarification of the role of public authorities, and the demonstration of concrete cases will be decisive in overcoming reluctance.

7.8. Conclusion

The interviews conducted show that Walloon companies are facing challenges related to traceability, quality, documentary compliance, and system integration. The DPP appears to be a promising response to these challenges, provided it is simple, interoperable, and supported by appropriate assistance. Blockchain can contribute to this, but it must remain at the service of use, without complicating processes. The regulatory context (ESPR), combined with the emergence of structuring projects like the DPPSP, creates a dynamic conducive to experimentation.

8. Blockchain Solution Proposal

8.1. Objectives: Going Beyond the Limits of the CIRPASS Architecture

The work of the CIRPASS project constituted a major step forward in defining a reference architecture for the DPP, by integrating European normative frameworks (ESPR, CEN/CENELEC, ISO, GS1) and proposing a modular and interoperable approach. This architecture, based on centralized or federated data registries, meets many governance, standardization, and compliance imperatives. However, it highlighted a set of structural limitations which, in the long term, could hinder the resilience and generalized adoption of the DPP by European companies, and particularly by SMEs.

The CIRPASS diagnosis notably highlights three major vulnerabilities. Firstly, dependence on a centralized Digital Product Passport Service Provider (DPPSP) introduces a risk of a "single point of failure," both technically (failures, attacks, loss of availability) and institutionally (risks of censorship, exclusion of certain actors, or competitive distortion). Secondly, the current architecture relies on strong institutional trust in the intermediaries who host and validate the data, without guaranteeing robust technical mechanisms against ex-post falsification, deletion, or manipulation of information. Thirdly, despite the recommended use of standards like GS1 Digital Link, real interoperability between sectors, value chains, and international jurisdictions remains conditioned by political and technical agreements that are still unstable.

In this context, it becomes legitimate to explore an alternative called the "ideal solution," which preserves the normative achievements of CIRPASS while relying on the assets of decentralized technologies. The hypothesis we put forward is the following: a DPP backed by blockchain and a decentralized cloud would strengthen the resilience, trust, and transparency of the system, while offering immutable traceability of the contributions of different actors.

The approach we propose is therefore progressive and complementary. It consists of starting from the conceptual building blocks laid out by CIRPASS—ontologies, user stories, identification scenarios (GTIN, GS1 DataMatrix, URI), security, and access recommendations—to transpose them into a distributed model where blockchain ensures the role of a trust registry and where operational data is hosted in redundant distributed storage (for example, via European solutions such as Alephium or ThreeFold). In this model, every registration, update, or revocation of a DPP is notarized on the blockchain, guaranteeing immutability and auditability, while voluminous data remains accessible via APIs compliant with European standards.

This decentralized approach allows for addressing several challenges identified by CIRPASS and the European Commission:

- Resilience and availability: elimination of the single point of failure thanks notably to sharding and distributed redundancy (via a decentralized cloud).
- Resistance to censorship: impossibility for a single operator to alter or delete a DPP without leaving a trace.
- Accountability of actors: immutable recording of the contributions of each operator, linked to their digital identity (DID, Verifiable Credentials).
- Normative interoperability: compatibility with GS1 Digital Link and ISO/IEC 15459 standards for identification, guaranteeing that the blockchain is not a silo but a layer of trust.
- Security and confidentiality: granular control of access rights to DPP sections via cryptographic mechanisms (delegation, selective encryption).

Ultimately, this “ideal” solution does not seek to replace the CIRPASS architecture, but to extend it to address the limitations inherent in any centralized system. It aligns with the logic of European recommendations, which advocate both technological neutrality and the search for innovative models guaranteeing trust and European digital sovereignty.

8.2. Design Principle of a Decentralized Solution

CIRPASS conceives the DPP as a federated system orchestrated by DPP Service Providers (DPPSPs), with key functions of resolution, data access, authentication, and governance. The major risks identified are the centralization of availability, potential censorship, alteration or loss of data, heterogeneity of identifiers, and semantic non-interoperability between sectors. The options for redirection and a European search portal address access resilience but leave a point of failure with the resolution service operator, and shift trust to the DPPSP's governance and the compliance of its logs.

It is necessary to separate what relates to proof, indexing, and access governance from what relates to the hosting of business data, while maintaining alignment with GS1 Digital Link and CIRPASS ontologies. Blockchain is relevant for indexing, timestamping, access control, and the audit trail. Business storage remains off-chain, but under guarantees of redundancy and controlled immutability.

The proposal for a decentralized DPP architecture is therefore based on a series of design principles that translate the lessons learned from the CIRPASS work while taking advantage of the contributions of blockchain and the decentralized cloud. These principles aim to ensure regulatory compliance, interoperability with existing standards, and technical robustness against identified risks:

- **On-chain Minimalism** The blockchain must not be overloaded with data. Only critical elements are recorded there: object index, cryptographic proofs, audit events, access policies, and timestamps. Sensitive, personal, or voluminous data is not intended to be placed directly on the chain, in order to respect confidentiality, cost, and scalability

constraints. The on-chain layer therefore plays a role of anchoring and immutable notarization, guaranteeing authenticity and traceability.

- **Verifiable Off-chain Storage** The information contained in the product passport is ideally kept in a decentralized storage environment offering operational redundancy and replication mechanisms. The hashes of this data are anchored on the blockchain to guarantee their integrity, and each modification is associated with an attested versioning scheme. A distinction is made between public data (accessible to all: composition, repairability, environmental indicators) and permissioned data (accessible only to certain actors via encrypted access policies). This model reconciles transparency and protection of strategic or confidential information.

- **Verifiable Identity** Actor authentication and role management rely on Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). These are linked to company identifiers recognized at the European level, such as EORI, VAT number, EUID, or LEI, to ensure interoperability and official recognition. This approach falls within the eIDAS 2.0 regulatory framework and allows clear and legally traceable responsibility to be assigned to each recorded action.

- **Alignment with GS1 and CIRPASS** Product identification relies on GS1 standards, particularly GTIN and GS1 Digital Link, encoded in AIDC media (DataMatrix or QR code). The exposed data follows a semantic format based on JSON-LD, aligned with the high-level ontologies defined by CIRPASS and supplemented by specific sectoral vocabularies. This semantic homogeneity guarantees compatibility between sectors and facilitates integration with other European initiatives, such as Gaia-X or sectoral passports (textiles, batteries, electronics).

- **Multi-Party Governance** Data resolution and exploration are ensured by a network of nodes operating under shared governance, in order to avoid any technical or institutional monopoly. Two options are conceivable: on the one hand, an official portal operated by the European Commission, which interprets the on-chain data and provides a reference access point; on the other hand, a decentralized deployment of the explorer and the application code on distributed clouds (IPFS, Arweave, ThreeFold), with explicit relinquishment of administrative rights by the deployer, similar to what already exists in certain decentralized protocols. A hybrid approach, combining an official portal for compliance and independent explorers for resilience and transparency, appears to be the most robust. Thus, we could have a central European portal and a multitude of regional portals that retrieve and filter protocol data according to their interests.

- **Defense in Depth** In order to prevent abuse, several protection mechanisms are combined: attestations of links in the value chain (for example, a company can only

add information if it proves a contractual link with the product), refundable deposits for any update attempt (limiting spam), lists of authorized roles defined at the smart contract level, and automated moderation tools. In the event of a dispute or reporting by a user, an escalation procedure is provided to the competent authority, without ever compromising the immutability of the history.

- **Complementary Principles** Three transversal principles complete this foundation:
  - **Interoperability by design**, by guaranteeing compatibility with the APIs and ontologies proposed by CIRPASS, as well as with ISO, GS1, and CEN/CENELEC standards.
  - **Sustainability by design**, by favoring energy-efficient technical solutions, such as Proof-of-Stake type blockchains or decentralized storage with a low environmental footprint.
  - **Resilience & fallback**, by imposing a double URI (manufacturer and immutable copy on the European explorer), to ensure the availability of the passport even if the original domain disappears.

By following these principles, the proposed decentralized solution optimally meets the criteria and limitations identified by CIRPASS. It is part of a standardization and interoperability effort at the protocol level, guaranteeing coherence with European and international normative frameworks. In parallel, it retains a functional flexibility allowing economic operators to add, beyond legal obligations, voluntary and differentiating information around the DPP. This double movement—normative rigor on one side, freedom of innovation on the other—contributes to making the digital passport not only a compliance tool but also a vector of competitiveness and value creation for companies.

8.3. Proposal for a Decentralized Architecture for the DPP

As a reminder, the work of the CIRPASS project highlighted several limitations inherent in the centralized models currently envisaged for the DPP. In particular, dependence on a single DPPSP generates a risk of excessive centralization: a single point of failure for data availability, the possibility for the operator to arbitrarily exclude participants, or risks of censorship and alteration of information.

As previously explained, in order to overcome these constraints, we propose a solution based on blockchain and decentralized cloud, guaranteeing resilience, resistance to censorship, and data immutability. The principle is based on a hybrid architecture that separates the functions of indexing, proof, and access governance (managed on-chain) from the hosting of business data (stored off-chain with guarantees of redundancy and integrity). This approach respects GS1 and CIRPASS standards, while addressing the identified risks.

8.3.1. Functional and Operational Logic of the Decentralized Solution

The proposed solution is structured around interdependent functional components that guarantee the identity, indexing, storage, access, and governance of DPPs. Through these components, a clear operational cycle frames the creation, updating, and consultation of the DPP, while respecting European standards and addressing the risks identified by CIRPASS.

The first component, dedicated to identity and trust, relies on Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). The latter attest to the roles of the actors (manufacturer, importer, recycler, conformity assessment body) and are linked to identifiers recognized in Europe (EORI, VAT number, EUID, or LEI). This mechanism, compliant with eIDAS 2.0, guarantees that each action is legally traceable and that supply chain relationships are certified via an attestation registry with the possibility of revocation.

The second component ensures the anchoring and traceability function. It establishes the link between the identity ecosystem (DIDs/VCs) and the blockchain proof infrastructure. This layer does not store the business data itself, but indexes its representations and records the proofs necessary to guarantee integrity, authenticity, and access governance. It is structured around five complementary elements in addition to a European access portal:

- **ProductPointer** The ProductPointer is the persistent and official URI of the DPP, generated by the European Portal. Unlike the GS1 Digital Link, which is hosted on the manufacturer's domain and therefore dependent on its maintenance, the ProductPointer provides a neutral and immutable address (just like GS1). When followed, the user is redirected to the DPP page of the Portal, which queries the blockchain to display the data of the corresponding DPPContract. The ProductPointer is integrated into the product's DataMatrix or QR code, in addition to the GS1 Digital Link. The association of the two ensures compatibility with GS1 standards while providing resilient redundancy: even if the manufacturer's domain disappears, access via the Portal remains guaranteed.
- **DPPContract** The DPPContract constitutes the authoritative smart contract of the digital passport on the blockchain. It centralizes the orchestration logic and references the different elements that make up the DPP:
    - One or more ResourceManifests (containing metadata and pointers to off-chain resources stored on a decentralized cloud).
    - AccessPolicies which define the rules for accessing permissioned data.
    - the EventLog which records the lifecycle and events associated with the product. The DPPContract also includes reference identifiers (notably GTIN) and associates each operation with an actor identified via DID/VC. Any consultation carried out by the Portal or by a third-party resolver relies on this contract, which serves as the technical point of truth.

- **ResourceManifest** The ResourceManifest describes and references the resources linked to a DPP. For each resource, it specifies its type (regulatory information, compliance certificates, environmental data, maintenance instructions, etc.), its version, its integrity hash, its access policy (public or restricted), its retention period, and contextual metadata (product category, language, license). The files themselves, generally JSON-LD structures or complementary documents such as certificates, are stored in a distributed and replicated off-chain environment. Anchoring the hashes in the DPPContract makes it possible to verify their authenticity and ensure transparent and traceable versioning.
- **AccessPolicy (on-chain)** The AccessPolicy sets the governance rules applicable to permissioned data. These are encrypted policies that condition access to certain sections of the DPP based on the roles or authorizations attested by VCs. Thus, only the competent authorities, notified bodies, or supply chain partners can consult or enrich the sections reserved for them. These rules can be implemented via key delegation or attribute encryption schemes, guaranteeing selective sharing without compromising the overall transparency of the product passport.
- **EventLog (on-chain)** The EventLog is the immutable and append-only journal that traces the entire lifecycle of the DPP. Every action—creation, update, transfer of responsibility, product recall, correction, or end-of-life marking—is recorded there with a timestamp and linked to the DID of the actor concerned. This mechanism ensures the accountability and auditability of all operations, in compliance with regulatory requirements and control expectations.

Finally, the third component concerns the hosting of the DPP's business data. Unlike the on-chain registry, which is limited to indexing and proofs of integrity, this component manages the complete information relating to the product and its lifecycle. The proposed architecture remains voluntarily technologically agnostic: it allows referencing resources located in different environments, whether they are decentralized clouds, classic centralized solutions, or even institutional hosting operated by the European Commission.

The logic of the protocol therefore consists of pointing to a storage system without imposing its nature, so that each actor can choose the solution best suited to their technical, economic, or regulatory constraints. Nevertheless, the preferred recommendation is the use of a decentralized cloud, which offers the best guarantees in terms of governance, impartiality, as well as immutability and durability. In this model, data cannot be altered, and in all cases, every action remains systematically recorded on the blockchain (whether for a centralized or decentralized cloud).

The off-chain resources notably include the product record structured in JSON-LD format, which constitutes the foundation of the DPP and aggregates all the ResourceManifests linked to it. They also integrate compliance certificates and regulatory reports, as well as environmental and repairability data. Technical notices and instructions relating to the end of life of the product can be added to these elements, and, where applicable, complementary

multimedia files such as diagrams, images, or explanatory videos intended to enrich the understanding and use of the product.

To ensure durability and resilience, several principles structure this component:

- **Redundancy:** each resource must be stored in multiple copies, ideally at least three, in order to limit the risks of data loss in the event of a failure or default of an operator.
- **Fault tolerance:** the protocol provides that if a copy disappears, a new copy is automatically regenerated in order to maintain the minimal threshold of availability.
- **Content addressing:** each resource is identified by a cryptographic hash (unique digital fingerprint), which makes it possible to verify at any time that it has not been altered.
- **Interoperability:** the referenced storage systems must be accessible via URIs (Uniform Resource Identifiers), guaranteeing compatibility with DPP APIs and resolvers.
- **Technological neutrality:** actors can resort to different models, whether it is a public cloud, a decentralized solution, or institutional hosting, provided that the principles of replication, traceability, and verifiability are respected.

A conceivable alternative lies in the establishment of an institutional hosting solution operated directly by the European Commission. Such an option would offer economic actors a more traditional and less complex storage modality to adopt than totally decentralized infrastructures, which could facilitate the strategic adhesion of SMEs and industrial sectors.

However, this approach must not exclude the possibility of interconnecting various solutions. One could imagine a simplification of storage management via orchestrated integration from the European Portal, allowing a solution to be configured and selected according to the specific needs of each actor, without requiring in-depth technical expertise on each type of cloud. With the combination of initiatives such as Gaia-X from the point of view of interoperability, it would thus be possible to develop packaged offers dedicated to the DPP, ready to use and easily deployable both on centralized environments and on decentralized solutions, ensuring a balance between ease of adoption, interoperability, and resilience.

Regardless of the chosen mode, the link between the stored data and the on-chain registry is ensured by the ResourceManifest, which records the hash, type, version, and access policy. This mechanism makes it possible to reconcile flexibility in the choice of storage and the requirement for verifiable integrity by all.

In summary, the third component gives the DPP its documentary and operational dimension: it hosts all the information necessary for traceability and compliance, while relying on guarantees of replication, verifiability, and immutability, reinforced by the recommendation of decentralized storage.

Finally, the European Portal could constitute the official reference interface of the DPP. It ensures the generation and registration of on-chain identifiers, guarantees the resolution of links, particularly in the event of unavailability of the manufacturer's domain, and offers a transverse search engine covering all DPPs. Beyond this technical function, it also plays a compliance and supervision role, by hosting the regulatory entry forms and ensuring the integrity of accesses and event logs. The detail of its operation and governance will, however, be the subject of a specific section of the file.

8.3.2. Functional Diagram

The functional cycle of a DPP begins with the assignment of a product identifier by GS1 for the manufacturer who is the first economic operator. The manufacturer requests a GTIN, which becomes the anchoring key for their digital passport. This standardized and interoperable identifier is essential to ensure continuity with existing standards.

Once the GTIN is obtained, the manufacturer must create their digital identity in the DPP ecosystem. This step is carried out via the European Portal (or any other platform connecting to the blockchain APIs), which plays the role of the institutional entry point. The manufacturer generates a Decentralized Identifier (DID) there, recorded on the blockchain in the form of a dedicated smart contract. This DID is associated with the official identifiers already recognized in the European framework (VAT number, EUID, LEI, EORI), thus constituting a company identity compliant with the eIDAS 2.0 regulation. The system functions as a Know Your Business (KYB) procedure, making it possible to group and certify the legal and administrative information of each economic operator.

Based on this identity, the manufacturer can proceed with the creation of their DPP, still via the Portal. This operation deploys a specific smart contract on the blockchain, the DPPContract. The latter contains the GTIN and the minimal information required by the regulation, which can be recorded on-chain in the form of public metadata or input data. However, for reasons of scalability and data protection, the majority of detailed information is managed via ResourceManifests.

ResourceManifests are created and updated via the European Portal. They group the DPP's business data and make it possible to specify, for each resource, whether it is public or private. Public information includes, for example, composition, repairability, or environmental performance. Sensitive information, such as certain compliance certificates or supply chain data, can be restricted through Access Policies (AccessPolicies) defined by the manufacturer or by other involved operators. These policies use the DIDs and VCs of the actors to assign or limit access rights.

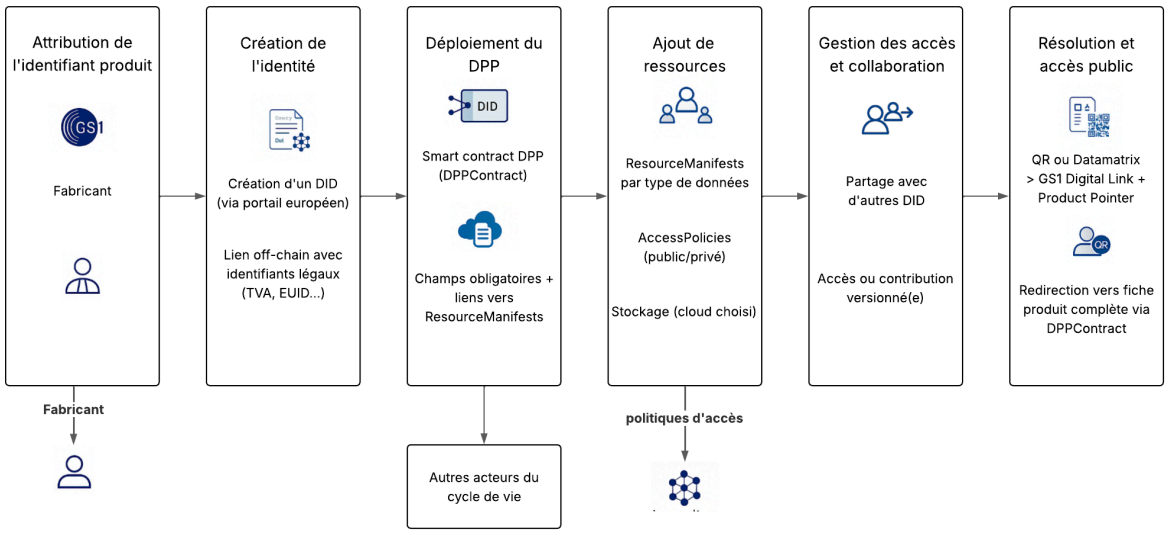
The storage of resources is left to the choice of each operator. By default, the European Portal can offer an institutional solution, guaranteeing neutrality and simplicity of adoption. Nevertheless, actors also have the possibility of resorting to centralized clouds or

decentralized solutions, offering increased resilience and a better guarantee of immutability. In this hybrid model, each operator is responsible for the choice and management of their storage system, while ensuring data integrity by anchoring hashes on the blockchain.

Once the DPP is created, the basic information is encoded in the AIDC medium to generate the barcodes to be affixed to the products. When the code is scanned, two URIs appear. The first is the GS1 Digital Link, hosted on the manufacturer's domain, guaranteeing compatibility with the GS1 ecosystem. The second is the ProductPointer, generated by the European Portal, which constitutes the persistent URI of the DPP. This link redirects to the official DPP page on the Portal, which queries the on-chain DPPContract and returns the corresponding ResourceManifests.

The entire system thus guarantees that each DPP is attached to a reliable identity (DID/VC), that it has an immutable anchor (DPPContract), that it is enriched with versioned, verifiable, and permissioned resources (ResourceManifests), and that it remains accessible in all circumstances thanks to the double URI mechanism (GS1 Digital Link and European ProductPointer). This workflow ensures coherence between existing standards and blockchain innovation, while offering the necessary flexibility to meet the constraints and needs of the different actors in the value chain.

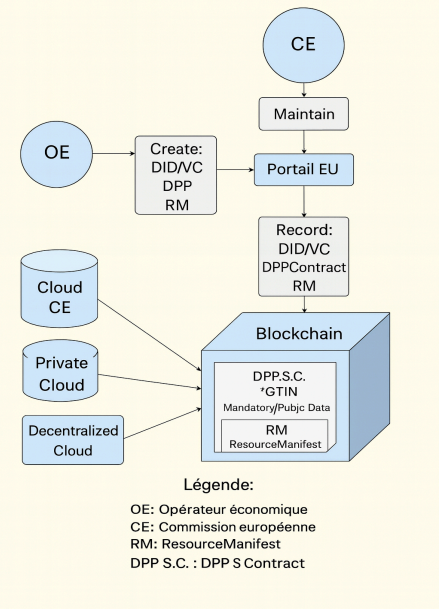
Here is a diagram to visualize the flow:



1. **Product Identifier Assignment** Manufacturer → obtains a GTIN from GS1.
2. **Identity Creation** Manufacturer → connects to the European Portal → generation of a DID (recorded on-chain via a dedicated DID smart contract) → association via an off-chain stored JSON to legal identifiers (VAT, EUID, LEI, EORI).

3. **DPP Deployment** Manufacturer → creates a DPP smart contract (DPPContract) linked to the GTIN.
    - This contract contains the mandatory base fields per product category (legal and public).
4. **Resource Addition** Manufacturer (and other lifecycle actors) → creates ResourceManifests, each describing a set of data (certificates, environmental information, technical notices, etc.), and links the documents that will be stored off-chain.
    - Definition of AccessPolicies (public or private, delegation of access to certain DIDs).
    - Data storage in a chosen environment (Commission, centralized cloud, decentralized cloud).
5. **Access and Collaboration Management**
    - Manufacturer can invite other DIDs to consult or enrich certain data.
    - Other operators can also request read and/or write access to data included in a ResourceManifest.
    - Each contribution is versioned, timestamped, and attributed to the actor's DID.
6. **Resolution and Public Access**
    - In the AIDC (QR/DataMatrix), two links appear:
        - GS1 Digital Link (manufacturer or GS1 domain name)
        - ProductPointer (European Portal) → which retrieves data from the DPPContract.
    - The portal reads the DPPContract, retrieves the ResourceManifests, and displays the product record based on the identified user's access level.

Here is a functional diagram to complete the understanding of the system:



8.3.3. European Portal Functionalities

The European Portal constitutes the central and official interface of the DPP system. It plays a pivotal role in orchestrating the different components (identity, on-chain registry, off-chain storage, and access). Its objective is to guarantee a homogeneous user experience while respecting the technical and regulatory standards defined at the European level.

Concretely, it offers the following functionalities:

- **Creation and management of economic operator accounts:** each actor (manufacturer, importer, distributor, recycler, notified body) registers on the portal and carries out an organizational identity verification (Know Your Business, KYB). This procedure relies on official identifiers (EORI, EUID, VAT, LEI) and leads to the generation of a DID (Decentralized Identifier) and Verifiable Credentials (VCs) attesting to the role.
- **Administration of products and DPPs:** the portal allows an economic operator to declare new products (based on a GTIN issued by GS1), then to create their DPP. The same operator can hold several roles depending on the DPP considered (for example, manufacturer for one product, importer for another, or even repairer or recycler in another value chain). The portal is not limited to creation: it also allows enriching existing DPPs by adding new ResourceManifests. These enrichments occur either because the operator has received explicit access (via an AccessPolicy), or because they have requested access to certain sections of a DPP.
- **Choice of storage mode:** when creating or updating the DPP, the operator selects a hosting mode for their data (centralized cloud, decentralized cloud, or institutional solution). The portal ensures the configuration of links to the ResourceManifests and simplifies integration, without requiring in-depth technical expertise.
- **Access and permission policy management:** via ergonomic interfaces, the operator defines the AccessPolicies associated with their data. They can declare certain information as public (accessible to all) or restrict its consultation to actors with specific VCs (e.g., surveillance authorities, supply chain partners).
- **Generation of the ProductPointer:** each DPP corresponds to a persistent URI, the ProductPointer, created and guaranteed by the portal. It is encoded in the DataMatrix or QR code alongside the GS1 Digital Link.
- **Addition and updating of ResourceManifests:** operators can enrich a DPP by adding new blocks (compliance certificates, environmental data, technical notices). Each addition is versioned, timestamped, and referenced in the smart contract's EventLog.
- **Management of reports and supervision:** the portal integrates a mechanism for reporting anomalies (reports by other actors or by consumers). These reports are archived and can trigger a moderation or control procedure by the competent authorities.

These functionalities make the European portal not only a DPP administration interface but also an instrument for compliance and supervision, ensuring alignment with the ESPR regulation and the technical standards resulting from the CIRPASS work.

8.3.4. Regional or Sectoral Portals

In addition to the European Portal, decentralized instances can be created by Member States, sectoral groupings, or specialized companies. These regional or sectoral portals rely on the APIs exposed by the protocol to retrieve, filter, and format data according to specific needs. Thus, each Member State could have its own mirror portal, allowing the presentation to be adapted to national priorities, while sectoral portals would offer targeted valorization (for example for textile, chemistry, or construction). This approach favors both interoperability and local appropriation of data, while leaving the European Commission the role of guarantor of the overall integrity and coherence of the system.

In this context, Wallonia could develop a dedicated regional portal, mirroring the European Portal, interconnected directly to the protocol. This Walloon portal would fulfill several functions:

- propose a localized interface in line with regional priorities (circular economy, traceability, Industry 4.0);
- provide services adapted to Walloon SMEs, such as simple connectors to their ERP or management tools, or no-code forms to create and enrich DPPs without in-depth technical expertise;
- offer visibility to regional sectors (technical textiles, batteries, chemistry, wood, construction) by grouping and enhancing the data relevant to these sectors;
- serve as a support and mediation tool, relaying European regulatory information and assisting companies in their compliance.

Thus, the Walloon portal would constitute a local declination of the European Portal, guaranteeing technical and semantic interoperability while strengthening appropriation by the economic actors of the region.

8.4. Deployment Plan at the Walloon Scale

As of today, the European Portal and the solution presented are hypothetical and exist only in this document. Wallonia therefore has the opportunity to take a pioneering position by implementing a regional prototype of the proposed solution, in the form of a sandbox. This Walloon portal would constitute the first operational demonstrator of a decentralized DPP, tested at the regional level but designed from the outset to be federative and interoperable with the future European system.

This prototype could fulfill several key functions depending on the budget deployed:

- **Company Onboarding:** allowing Walloon SMEs to create a digital identity (DID/VC) and associate it with their legal identifiers (VAT, EUID, LEI, EORI). This step would rely on simplified Know Your Business processes to lower the barrier to entry.

- **Creation and management of pilot DPPs:** manufacturers could, based on GTINs provided by GS1 Belgium & Luxembourg, create DPPs for real products. These DPPs would include both mandatory regulatory information and enrichments via ResourceManifests, depending on whether the data is public or permissioned.

- **Experimentation with storage choices:** the sandbox would offer several storage options (regional cloud, decentralized solutions, institutional hosting), allowing testing of simplicity of use, costs, and robustness according to the needs of the actors.

- **Management of access and roles:** the Walloon portal would allow simulating the different positions in the value chain (manufacturer, importer, distributor, recycler, authority) and testing in real conditions the definition of AccessPolicies and the selective exchange of information.

- **Interoperability and connectors:** the sandbox would integrate open APIs and simplified connectors for ERP, PLM, or MES used by SMEs. The created DPPs would comply with GS1 Digital Link, JSON-LD standards, and CIRPASS ontologies, ensuring immediate interoperability with other European initiatives.

- **Sectoral and regional valorization:** the portal would offer dashboards and sectoral views adapted to Walloon strategic sectors (technical textiles, batteries, chemistry, construction, wood), facilitating the exploitation of data by companies, federations, and authorities.

The objective of this sandbox is not just to experiment, but to strategically position Wallonia at the heart of European innovation around the DPP, by demonstrating the feasibility of a unique and unifying solution. Ultimately, this Walloon portal could evolve into a mirror portal interconnected with the future European Portal, but with the advantage of having served as a reference prototype. Such an approach obviously requires close and early collaboration with existing European initiatives, notably the CIRPASS project, with which Wallonia is already in contact.

8.5. Economic and Competitive Perspectives

The development of a regional DPP prototype in Wallonia offers considerable economic and competitive perspectives. Far from being limited to a response to regulatory constraint, it can become a catalyst for innovation and a lever for differentiation for regional industrial sectors.

- **Strengthening the Competitiveness of SMEs** Walloon SMEs, which constitute the majority of the industrial fabric, rarely have the resources to anticipate complex regulations. By providing them with a ready-to-use infrastructure, accompanied by simplified connectors and no-code tools, the Region allows them to comply with future ESPR obligations while reducing implementation costs. This anticipation will give them a competitive advantage over competitors from other European regions who have not benefited from such support.

- **Positioning Wallonia as a Pilot Territory** By developing an operational regional sandbox, Wallonia is positioning itself as a pilot territory within the European Union. It demonstrates its ability to experiment, federate, and propose a coherent solution that can be integrated into the future European Portal. This position strengthens its visibility with European bodies and increases the chances of capturing funding dedicated to DPP standardization and industrialization projects.

- **Stimulating the Local Innovation Ecosystem** The implementation of the prototype will require the mobilization of regional actors specializing in blockchain, cloud, security, and GS1 standards. This will stimulate the Walloon digital ecosystem, creating opportunities for start-ups, research centers, and technology providers. The skills acquired in this context can be exported to other European projects, positioning Wallonia as a solution provider and not only as a user.

- **Creating New Market Opportunities** The DPP opens the way to innovative economic models: compliance verification services, reconditioning and recycling platforms, secondary markets based on product traceability, valorization of environmental data within the framework of sustainable finance. Walloon companies that adopt the DPP early will be able to exploit these opportunities and develop new growth drivers.

- **Increasing Digital and Industrial Sovereignty** By hosting a regional portal and experimenting with hybrid storage solutions (centralized, decentralized, institutional), Wallonia ensures that it maintains control over its strategic industrial data. It thus limits its dependence on foreign infrastructures and consolidates its digital sovereignty, while contributing to the resilience of European value chains.

In summary, the implementation of a DPP sandbox in Wallonia is not only a regulatory compliance project: it is a strategic project that strengthens the competitiveness of SMEs,

positions the Region as a European leader in DPP innovation, stimulates its digital ecosystem, and opens the way to new economic models based on transparency, circularity, and digital trust.

8.6. Conclusion and Limitations

The solution proposal for a decentralized architecture for the DPP (Digital Product Passport) falls within the continuity of the CIRPASS work while seeking to overcome certain structural limitations of centralized models. By relying on blockchain for indexing, proof, and access governance, and on a distributed cloud for hosting business data, it offers a framework that combines compliance with European standards, technical resilience, semantic interoperability, and the accountability of stakeholders.

This vision makes it possible to address several key challenges identified by the European Commission: ensuring data availability and integrity, preventing arbitrary censorship or exclusion, and strengthening trust through the immutability of contributions. Furthermore, it opens up new economic perspectives, transforming the DPP from a regulatory constraint into a lever for competitiveness, particularly for Walloon SMEs which could benefit from a pioneering regional portal.

However, this approach also involves significant limitations and challenges:

- **Technical complexity and adoption costs:** The implementation of a decentralized solution requires expertise in blockchain, cryptographic security, and distributed storage management, which is not yet widely spread among SMEs. Simplified interfaces and support will be essential to ensure adherence.

- **Institutional acceptability:** The implementation of a distributed trust registry presupposes an agreement on multi-party governance, including the European Commission, Member States, industrial players, and third-party organizations. The acceptance of a partially decentralized model could provoke resistance from actors accustomed to more centralized architectures.

- **International interoperability:** While the model is aligned with GS1 and the CIRPASS ontologies, its compatibility with regulatory and technical frameworks outside the European Union (for example, in the United States or Asia) still needs to be guaranteed. The risk of normative fragmentation is not entirely ruled out.

- **Sovereignty and trust in infrastructure issues:** If decentralized solutions are favoured, it will be necessary to ensure that they rely on operators and networks compatible with the objectives of European digital sovereignty. The choice of infrastructure (blockchain, storage, identities) must avoid any critical dependence on non-European actors.

- **Balance between transparency and confidentiality:** The DPP must provide a high level of transparency for consumers and authorities, while protecting sensitive industrial data. The correct calibration of the Access Policies, balancing openness and restriction, will be a central challenge to avoid both over-exposure and opacity.

- **Evolutionary path:** This proposal is currently hypothetical and still needs to be tested in real environments. The development of a regional sandbox in Wallonia constitutes a pragmatic first step, but scaling up to the European level will require technical, regulatory, and organizational adjustments.

Ultimately, this solution is not presented as an exclusive alternative to the CIRPASS model, but as a federating extension that anticipates the needs for resilience, transparency, and digital trust. It positions Wallonia as a privileged experimentation territory, capable of making a determining contribution to the development of the future European DPP infrastructure.

9. General Conclusion, Limitations, and Recommendations

The implementation of the Digital Product Passport (DPP) within the framework of the ESPR (Ecodesign for Sustainable Products Regulation) constitutes a major step for the sustainable transformation of European industry. By placing traceability and transparency at the heart of the product lifecycle, the DPP ensures comprehensive and verifiable documentation, from manufacturing to end-of-life, while supporting the circularity and sustainability objectives defined by the European Commission. The experiments conducted in Wallonia, within the DigitalWallonia4Trust program, have provided a concrete field for testing processes, identifying technical and organizational hurdles, and validating the interoperability standards required for European-scale adoption.

One of the major lessons learned from this study lies in the strategic value provided by the blockchain. As a decentralized infrastructure, it guarantees the immutability of event logs, certified lifecycle traceability, and the secure management of identifiers (DID, VC). Coupled with European standards such as GTIN, URI, JSON-LD, or eIDAS, it offers native interoperability and a high level of trust for all stakeholders. The modular Resource Manifests and the use of smart contracts allow for the automation of certain validations while maintaining distributed governance. This approach reinforces the credibility of the DPP and offers a robust technical framework for coordination among industrial players, public authorities, and consumers, while anticipating regulatory and technological developments.

Recommendations

To maximize the effectiveness and acceptance of the DPP, it is recommended to deploy a hybrid and federated architecture, combining off-chain storage, blockchain registries, and secure access portals. The governance of this infrastructure must be shared among industrial players, public authorities, and technical experts, and include a collective validation mechanism for any protocol modification. A DAO (Decentralized Autonomous Organization) approach would thus allow for the conciliation of security, transparency, and flexibility, while ensuring the system's ability to evolve with user needs and technological innovations. The modularity and openness of the solution also favour the gradual integration of SMEs and regional platforms, guaranteeing progressive adoption across Europe.

Limitations

Despite its advantages, the blockchain presents certain limitations. Its immutability can restrict the system's adaptability if no governance mechanism is planned for future evolutions. The technical complexity of implementation and the necessity of synchronizing all stakeholders can slow down operational deployment. Furthermore, the dependence on specific standards, while necessary for interoperability, imposes a constraining framework that must be anticipated and managed. The complementary use of the CIRPASS repository, combined with the blockchain, helps mitigate some of these risks by offering a solid foundation while introducing mechanisms for gradual evolution.

Finally, this approach demonstrates that the DPP can constitute an accelerator for virtuous ecosystems and a strategic lever for European industrial competitiveness. Each product can thus be documented, accessible, and verifiable throughout its lifecycle, in a common and standardized language. By combining technological innovation, adoption of European standards, and distributed governance, Europe has a solid foundation for deploying an effective, scalable, and sustainable DPP, serving industrial players, authorities, and consumers.

In coherence with regional and industrial ambitions, Wallonia could constitute the ideal framework to experiment with this solution in an interoperable pilot project, bringing together public, industrial, and technological ecosystems. It is now up to all concerned stakeholders to realize this European promise by ensuring the coordination and implementation of the defined standards and mechanisms.

10. Bibliography

GS1 Standards enabling the EU digital product passport 2025. Available online: https://gs1.eu/wp-content/uploads/2024/12/GS1-Standards-Enabling-DPP.pdf

CIRPASS-2 Consortium. D4.1 Reference Architecture, v1.0, 2025. Available online : https://doi.org/10.5281/zenodo.15388412

CIRPASS Consortium. Risks and Mitigations, v1.0, 2024. Available online : https://doi.org/10.5281/zenodo.10933985

CIRPASS-2 Consortium. Options for Redirection to the Mandatory DPP Backup, 2024. Available online : https://doi.org/10.5281/zenodo.15007842

CIRPASS-2 Consortium. Options for EU Web Portal Search, 2024. Available online : https://doi.org/10.5281/zenodo.15007842

CIRPASS Consortium. D3.3 Identification Schemes, v1.3, 2024. Available online : https://doi.org/10.5281/zenodo.10925703

CIRPASS-2 Consortium. D3.2 Upper-level Regulatory Sectoral Ontologies and Vocabularies, v1.1, 2025. Available online : https://doi.org/10.5281/zenodo.14900882

CIRPASS Consortium. Cross-sector and sector-specific DPP Roadmaps, v1.2, 2024. Available online : https://doi.org/10.5281/zenodo.10996459

CIRPASS Consortium. D3.4 DPP System Roadmap, V2.0, 2024. Available online : https://doi.org/10.5281/zenodo.11096973

CIRPASS Consortium. D5.1 Digital Product Passport Prototypes, 2024. Available online : https://doi.org/10.5281/zenodo.11393742

CIRPASS Consortium. D2.1 Mapping of legal and voluntary requirements and screening of emerging DPP-related pilots, 2023. Available online : https://doi.org/10.5281/zenodo.10925636

CIRPASS Consortium. Standardisation gaps and roadmap, 2024. Available online : https://doi.org/10.5281/zenodo.11316405

Global Battery Alliance. Battery Passport overview and materials, 2024–2025. Available online : https://www.globalbattery.org

Règlement (UE) 2023/1542 relatif aux batteries et aux déchets de batteries. Available online : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023R1542

GS1 in Europe. Digital Product Passport Architecture, mars 2022. Available online : https://www.gs1.eu/digital-product-passport

Vlaanderen Circulair. Cas d'usage TripleR.io mattressID (consulté 2025). Available online : https://triplr.io

Crypto Kastaar. Digital Product Passport (consulté 2025). Available online : https://www.cryptokastaar.com/digitalproductpassport

GS1 Belu. Digital Product Passport resources (consulté 2025). Available online : https://www.gs1belu.org

Twintag. Digital Product Passport use cases (consulté 2025). Available online : https://twintag.com

KeeeX. Le passeport numérique des produits, 2024. Available online : https://keeex.me/fr/blog/2024/09/02/le-passeport-numerique-des-produits

Tilkal. Traçabilité blockchain et passeports produits (consulté 2025). Available online : https://www.tilkal.com

Arianee. Documentation protocole et cas d'usage (consulté 2025). Available online : https://www.arianee.org

TextileGenesis by Lectra. Solution de traçabilité textile (consulté 2025). Available online : https://www.textilegenesis.com

Circularise. Smart Questioning resources and white papers (consulté 2025). Available online : https://www.circularise.com

Madaster. Material Passport resources (consulté 2025). Available online : https://www.madaster.com

Spherity. Battery Passport SSI resources (consulté 2025). Available online : https://spherity.com

Catena-X. Data space architecture and assets (consulté 2025). Available online : https://catena-x.net

Narravero. Product Passport SaaS (consulté 2025). Available online : https://narravero.com

Battery Pass Consortium. Content and guidance, 2023–2025. Available online : https://www.battery-pass.eu

Aura Blockchain Consortium. Official materials (consulté 2025). Available online : https://aurablockchain.com

TrusTrace. DPP Playbook and resources (consulté 2025). Available online : https://trustrace.com

whatt.io. Product Passport Solutions (consulté 2025). Available online : https://www.whatt.io

Provenance. Transparency and product passports resources (consulté 2025). Available online : https://www.provenance.org

iPoint-systems. DPP resources (consulté 2025). Available online : https://www.ipoint-systems.com

Certilogo (eBay). Digital ID and authentication resources (consulté 2025). Available online : https://www.certilogo.com

The ID Factory. DPP resources (consulté 2025). Available online : https://www.theidfactory.com

Cobuilder. Data dictionaries and AAS resources (consulté 2025). Available online : https://cobuilder.com

EON. Digital IDs for circular fashion (consulté 2025). Available online : https://www.eon.xyz

Digimarc Product Cloud. Watermarking and DPP integrations (consulté 2025). Available online : https://www.digimarc.com

OPTEL. Optchain and DPP module (consulté 2025). Available online : https://www.optelgroup.com

VeChain & DNV. My Story (consulté 2025). Available online : https://www.vechain.org

IOTA Foundation. Digital Product Passport Showcase (consulté 2025). Available online : https://www.iota.org/learn/showcases/dpp

Circularise & Marubeni. Partnership announcements (consulté 2025). Available online : https://www.marubeni.com