Dossier d’analyse d’intégration blockchain au sein du Digital Product Passport (DPP)

BE THE FUTURE
BE BLOCKCHAIN

Projet subventionné par la Région Wallonne dans le cadre du programme DigitalWallonia4Trust - PRW136

Sommaire

1. Glossaire et abréviation..... 1
2. Introduction et contexte..... 4
3. Résumé exécutif..... 5
4. Rappel du cadre réglementaire..... 6
    4.1. ESPR..... 6
        4.1.1. Objectifs principaux..... 6
        4.1.2. Produits concernés..... 7
        4.1.3. Obligations pour les entreprises..... 7
        4.1.4. Calendrier d'application..... 7
    4.2. Digital Product Passport (DPP)..... 8
5. Enjeux pour la Wallonie et les PME locales..... 9
    5.1. Conformité réglementaire et réduction des risques..... 9
    5.2. Opportunité de différenciation et de compétitivité..... 9
    5.3. Simplification des échanges et interopérabilité..... 9
    5.4. Transformation numérique et montée en compétences..... 10
    5.5. Contribution à la transition écologique et à l'économie circulaire..... 10
    5.6. Positionnement stratégique de la Wallonie dans les initiatives européennes... 10
6. Etat de l'art..... 11
    6.1. Standardisation..... 11
        6.1.1. Normes ISO..... 11
        6.1.1.1. ISO / IEC 15459 (identification unique)..... 11
        6.1.1.2. ISO / IEC 20248 (authenticité des données)..... 11
        6.1.1.3. ISO / IEC 18004 (RFID)..... 12
        6.1.2. AIDC (Automatic Identification and Data Capture)..... 12
        6.1.3. GTIN (Global Trade Item Number)..... 13
        6.1.4. L'URI (Uniform Resource Identifier)..... 13
        6.1.5. La standardisation GS1..... 14
        6.1.6. GS1 Digital Link..... 14
        6.1.7. GS1 DataMatrix..... 15
        6.1.8. Conclusion sur la standardisation :..... 16
    6.2. Revue des initiatives..... 16
        6.2.1. Europe..... 16
        6.2.1.1. Projets CIRPASS :..... 16

6.2.1.2. Global Battery Alliance – Battery Passport : 17
6.2.1.3. GS1 en Europe : 17
6.2.1.4. Initiatives privées 17
6.2.1.5. Belgique 18
6.2.2. International et multi-régions 19
6.2.3. Conclusion sur les initiatives 20
7. Etude de marché 20
7.1. Étude de marché : analyse croisée des entretiens 20
7.2. Un intérêt marqué pour la traçabilité et la conformité 21
7.3. Des outils hétérogènes, souvent cloisonnés 21
7.4. Une gestion complexe des données techniques 21
7.5. Vers une sensibilisation croissante au DPP 21
7.6. Une ouverture mesurée à la blockchain 22
7.7. Des attentes fortes sur l'accompagnement 22
7.8. Conclusion 22
8. Proposition de solution blockchain 22
8.1. Objectifs : dépasser les limites de l'architecture CIRPASS 22
8.2. Principe de conception d'une solution décentralisée 24
8.3. Proposition d'architecture décentralisée pour le DPP 26
8.3.1. Logique fonctionnelle et opérationnelle de la solution décentralisée 27
8.3.2. Schéma fonctionnel 30
8.3.3. Fonctionnalités du Portail européen 33
8.3.4. Portails régionaux ou sectoriels 35
8.4. Plan de déploiement à l'échelle wallonne 35
8.5. Perspectives économiques et compétitives 37
8.6. Conclusion et limites 38
9. Conclusion générale, limites et recommandations 39
10. Bibliographie 41

1. Glossaire et abréviation

- **AIDC (Automatic Identification and Data Capture)** : Ensemble de technologies (codes-barres, RFID, QR codes) permettant l'identification et la traçabilité des produits dans le DPP.
- **AI (Assurance of Information)** : Garantit la qualité, la fiabilité et l'intégrité des données échangées dans le DPP.
- **API (Application Programming Interface)** : Interface logicielle permettant la communication entre le DPP et d'autres systèmes informatiques.
- **CEN (Comité Européen de Normalisation)** : organisme officiel chargé d'élaborer des normes européennes harmonisées dans de nombreux secteurs industriels et de services, afin de faciliter la libre circulation des produits et services au sein du marché unique.
- **CENELEC (Comité Européen de Normalisation Électrotechnique)** : organisme européen spécialisé dans la normalisation du domaine électrotechnique et électronique, couvrant notamment les équipements électriques, l'énergie et les technologies numériques.
- **CEAP (Circular Economy Action Plan)** : Programme de la Commission européenne promouvant l'économie circulaire, dont le DPP est un outil central.
- **CIRPASS (Cross-sectoral Interoperable Registries for Product Asset Sustainability)** : Projet européen visant à définir une architecture commune et interopérable du DPP entre plusieurs secteurs industriels.
- **DAO (Decentralized Autonomous Organization)** : Structure organisationnelle fonctionnant sur la blockchain, gouvernée par des règles codées dans des smart contracts et contrôlée collectivement par ses membres. Une DAO permet de prendre des décisions transparente et décentralisée, sans autorité centrale, grâce à un système de votes généralement lié à la détention de tokens.
- **DID (Decentralized Identifier)** : Standard permettant une identification numérique décentralisée, appliquée à la gestion des identités dans le DPP.
- **DPP (Digital Product Passport)** : Outil numérique centralisant et partageant les informations produit tout au long de son cycle de vie, pour garantir traçabilité et conformité.

- **DPPSD (Digital Product Passport System Demonstrator)** : Projet pilote destiné à tester en conditions réelles l'implémentation du DPP et valider son interopérabilité.
- **DW4T (Digital Wallonia for Trust)** : Initiative wallonne soutenant la mise en œuvre de solutions numériques de confiance, dont le DPP.
- **eIDAS (Electronic Identification, Authentication and Trust Services)** : Cadre réglementaire européen sur l'identification électronique et les services de confiance, appliqué au DPP.
- **EORI (Economic Operator Registration and Identification)** : Numéro unique pour identifier les opérateurs économiques dans l'UE, utilisable dans le DPP.
- **ESPR (Ecodesign for Sustainable Products Regulation)** : Cadre réglementaire européen fixant les exigences d'écoconception et introduisant l'obligation du DPP pour certains produits.
- **EUID (European Unique Identifier)** : Identifiant unique européen pour les entreprises, facilitant leur traçabilité dans le DPP.
- **GLN (Global Location Number)** : Identifiant unique permettant de référencer une entité (entreprise, site, entrepôt) dans le DPP.
- **GTIN (Global Trade Item Number)** : Identifiant unique attribué à un produit via GS1, indispensable à son intégration dans un DPP.
- **IEC (International Electrotechnical Commission)** : Organisme mondial de normalisation dans le domaine électrotechnique, complémentaire de l'ISO.
- **ISO (International Organization for Standardization)** : Organisme mondial de normalisation dont les standards (ex. ISO 9001, ISO 14001) servent de base au DPP.
- **JSON-LD (JavaScript Object Notation for Linked Data)** : Format de données structuré facilitant l'interopérabilité et le partage d'informations dans le DPP.
- **LEI (Legal Entity Identifier)** : Identifiant mondial des entités juridiques, utilisé pour l'interopérabilité des données financières et du DPP.
- **L'Asset Administration Shell (AAS)** : Représentation numérique standardisée d'un actif physique, conçue pour l'interopérabilité et l'échange de données dans le cadre de l'Industrie 4.0 et de l'Internet Industriel des Objets (IIoT).
- **RFID (Radio Frequency Identification)** : Technologie d'identification par radiofréquence, facilitant la capture automatique de données produit dans le cadre du DPP.

- **Sharding** : Le sharding est une technique de partitionnement des données qui consiste à diviser une base de données ou un système en plusieurs fragments appelés shards. Chaque shard contient une portion des données et fonctionne comme une base autonome, mais l'ensemble reste cohérent et accessible comme un tout.
- **Smart Contract** : Programme informatique qui exécute automatiquement des actions prédéfinies lorsque certaines conditions sont remplies, le tout stocké sur une blockchain pour garantir son inaltérabilité et sa transparence.
- **SSCC (Serial Shipping Container Code)** : Identifiant unique des unités logistiques (colis, palettes) utilisé pour le suivi des produits dans le DPP.
- **URI (Uniform Resource Identifier)** : Format d'adresse permettant de référencer et d'accéder aux données du DPP en ligne.
- **VC (Verifiable Credentials)** : Données vérifiables et infalsifiables utilisées pour prouver la conformité ou l'authenticité dans le DPP.

2. Introduction et contexte

Depuis plusieurs années, l'Union européenne intensifie ses efforts pour concilier compétitivité industrielle, innovation et durabilité. La stratégie du Pacte vert pour l'Europe, suivie par une série de règlements structurants, ambitionne de transformer les chaînes de valeur en intégrant pleinement les principes d'économie circulaire et de transparence. Dans cette dynamique, le règlement sur l'écoconception des produits durables (ESPR) constitue une avancée majeure. Il impose progressivement de nouvelles exigences aux fabricants, importateurs et distributeurs, en introduisant notamment le Digital Product Passport (DPP) comme instrument de référence.

Le DPP se présente comme un passeport numérique universel attaché à chaque produit, contenant des informations standardisées et vérifiées sur son origine, ses composants, ses impacts environnementaux, ainsi que ses possibilités de réparation, de réutilisation et de recyclage. Au-delà de son rôle de conformité réglementaire, cet outil ouvre la voie à une gestion beaucoup plus fine du cycle de vie des produits, à une meilleure information des consommateurs et à une coopération renforcée entre acteurs économiques.

Pour la Wallonie, région particulièrement exposée à ces mutations, l'enjeu est considérable. C'est pour accompagner cette transition que la Région wallonne a confié à BE Blockchain, en collaboration avec Agoria et Logistics in Wallonia, la mission de conduire une étude exploratoire autour du DPP. Cette recherche préliminaire s'appuie sur l'état de l'art européen, les premiers retours d'expérience issus du consortium CIRPASS et de ses prolongements (CIRPASS-2), et vise à proposer une architecture idéale intégrant la technologie blockchain, spécifiquement adaptée aux besoins des PME wallonnes, qui constituent l'essentiel du tissu économique régional. L'objectif est de transformer une contrainte réglementaire en véritable levier stratégique pour la compétitivité régionale, en cohérence avec les priorités de DigitalWallonia4Trust, de l'industrie 4.0 et de l'économie circulaire.

Le projet s'inscrit également dans le prolongement du premier programme financé par la Région wallonne, au sein duquel un consortium d'acteurs régionaux avait déjà développé plusieurs démonstrateurs blockchain[1]. Dans cette continuité, il s'agit ici d'explorer le développement plus complet d'un démonstrateur appliqué au DPP, en marge de l'entrée en vigueur prochaine de la réglementation ESPR, afin de préparer les entreprises wallonnes aux nouvelles obligations tout en maximisant les retombées stratégiques et économiques.

[1] https://dw4t.be

3. Résumé exécutif

La mise en place du Digital Product Passport (DPP) dans le cadre de l'ESPR (Ecodesign for Sustainable Products Regulation) représente une transformation systémique des chaînes de valeur industrielles. Ce document propose une synthèse des travaux réalisés en lien avec les expérimentations pilotes menées en Wallonie dans une dynamique collaborative intégrant institutions, entreprises et experts technologiques. L'objectif a été d'évaluer les conditions de mise en œuvre du DPP, d'identifier les freins techniques et organisationnels, et de proposer un cadre d'action adapté à l'écosystème local, tout en respectant les normes européennes émergentes.

À travers une analyse réglementaire, technique et opérationnelle, le rapport met en évidence les enjeux clés liés à l'interopérabilité des données, à l'identification unique des produits (AIDC, GTIN, URI, etc.), et à la gouvernance des informations partagées. Il souligne l'importance d'un alignement étroit entre les standards européens (CIRPASS, GS1 Digital Link, ISO/IEC 15459…) et les réalités terrain. Les retours d'expérience des acteurs industriels locaux révèlent à la fois un intérêt croissant pour le DPP et une complexité de mise en œuvre, notamment autour de l'intégration des systèmes d'information, de la protection des données et de la traçabilité des composants.

La dimension technologique constitue un levier structurant, en particulier par l'intégration de la blockchain comme registre distribué de confiance. Elle répond aux exigences d'intégrité, d'auditabilité et de décentralisation imposées par le DPP. Plusieurs cas d'usage présentés dans le rapport illustrent comment la blockchain permet de créer un lien infalsifiable entre les identifiants produits, les événements de cycle de vie et les certificats de conformité, tout en respectant le RGPD grâce à l'utilisation de technologies telles que les DID (Decentralized Identifiers) et les Verifiable Credentials (VC) combinées à la gestion des accès via des AccessPolicies. Ce positionnement est d'autant plus stratégique que les standards eIDAS 2.0, les wallets d'identité et les registres d'actifs prennent forme au niveau européen.

Ce rapport présente également une cartographie des briques fonctionnelles essentielles à la mise en œuvre d'un DPP interopérable, sécurisé et évolutif. Il met en lumière l'intérêt de développer un démonstrateur souverain capable de servir à la fois les objectifs du CEAP (Circular Economy Action Plan), les exigences réglementaires de l'ESPR, tout en s'appuyant sur les briques établies par le projet CIRPASS. Ce dernier constitue une base de standardisation essentielle, mais les limites identifiées dans ses travaux montrent qu'une extension combinant ces fondations avec des technologies de registre distribué, telles que la blockchain, permettrait d'y répondre plus efficacement. Elle apporterait en effet une réponse crédible aux enjeux de sécurité, de transparence, d'immuabilité, et de privacy by design, renforçant ainsi l'ambition d'innovation numérique du territoire. Cette approche modulaire, orientée vers l'ouverture et la standardisation, permettrait d'impliquer des

industriels de tailles variées dans une transition numérique structurée, résiliente et conforme aux principes de durabilité.

La Wallonie, à travers ses initiatives telles que DW4T (Digital Wallonia for Trust), démontre sa volonté d'occuper une position de précurseur. Les travaux restitués dans ce rapport doivent désormais ouvrir la voie à des expérimentations concrètes, intégrant les briques blockchain, les identifiants uniques, les protocoles de traçabilité et les interfaces utilisateurs nécessaires à un DPP pleinement opérationnel, aligné avec les ambitions européennes de souveraineté numérique et de durabilité.

4. Rappel du cadre réglementaire

L'ESPR (Ecodesign for Sustainable Products Regulation) constitue le nouveau cadre législatif européen visant à renforcer la durabilité des produits mis sur le marché de l'Union. Adopté en juin 2024, il s'inscrit dans la continuité du Green Deal européen et du CEAP (Circular Economy Action Plan), en élargissant l'approche de l'écoconception à un plus grand nombre de catégories de produits. Ce règlement établit une base commune pour améliorer la réparabilité, la réutilisabilité et la recyclabilité des biens, tout en assurant une meilleure transparence des chaînes de valeur. L'ESPR marque ainsi une étape décisive dans la transition vers une économie circulaire et constitue le socle réglementaire sur lequel s'appuie l'introduction progressive du DPP.

4.1. ESPR

Le Règlement sur l'écoconception des produits durables (ESPR – Ecodesign for Sustainable Products Regulation), adopté en juin 2024, constitue l'un des piliers du Green Deal européen et du plan d'action pour l'économie circulaire (CEAP). Il remplace progressivement la directive Écoconception de 2009 et élargit considérablement son champ d'application. L'ESPR établit un cadre horizontal visant à rendre les produits mis sur le marché de l'Union plus durables, réparables, réutilisables et recyclables, tout en renforçant la transparence des chaînes de valeur.

4.1.1. Objectifs principaux

L'ESPR poursuit plusieurs objectifs stratégiques qui s'inscrivent au cœur du Pacte vert européen. Il vise d'abord à réduire l'impact environnemental des produits tout au long de leur cycle de vie, depuis la conception jusqu'au recyclage, en favorisant la réparabilité, la réutilisation et la circularité. Il entend également diminuer la dépendance de l'Union européenne aux matières premières critiques, en optimisant la valorisation des ressources déjà présentes sur le marché et en améliorant la gestion des flux de matières. Par ailleurs, le

règlement constitue un levier de compétitivité et d'innovation en incitant les entreprises à développer de nouveaux modèles d'affaires, à investir dans l'écoconception et à proposer des produits plus durables. Enfin, il renforce la transparence en donnant aux consommateurs, aux acteurs de la filière et aux autorités de contrôle un accès structuré et fiable aux données produits grâce au Digital Product Passport, outil central de suivi et de vérification des informations tout au long de la chaîne de valeur.

4.1.2. Produits concernés

L'ESPR instaure une approche par actes délégués sectoriels. Les premières filières ciblées sont :

- Batteries (entrée en vigueur en 2027, déjà encadrées par le Règlement Batteries).
- Textiles (deuxième semestre 2027).
- Produits électroniques et électroménagers (horizon 2030).
- Produits de construction et mobilier (calendrier progressif en cours de définition).

Ces catégories représentent des secteurs à fort impact environnemental et fortement concernés par les exigences de traçabilité et de circularité.

4.1.3. Obligations pour les entreprises

Concrètement, l'ESPR introduit de nouvelles obligations pour les opérateurs économiques responsables, qu'il s'agisse des fabricants, importateurs ou distributeurs. Ils doivent créer et mettre à jour un passeport numérique pour chaque produit concerné, en y intégrant l'ensemble des informations exigées par la réglementation. Ces acteurs sont également tenus de garantir la qualité, l'exactitude et la disponibilité des données partagées à travers la chaîne de valeur, de manière à renforcer la confiance entre partenaires et à faciliter les contrôles. Les informations contenues dans le DPP doivent par ailleurs être conservées sur une durée minimale définie, pouvant aller jusqu'à dix ans après la mise sur le marché dans certaines catégories de produits, conformément à l'article 12 du règlement. Enfin, le système doit prévoir un accès différencié aux données, afin que chaque partie prenante, consommateurs, recycleurs, autorités de surveillance du marché ou organismes de conformité, puisse disposer du niveau d'information qui lui est pertinent et nécessaire à son rôle.

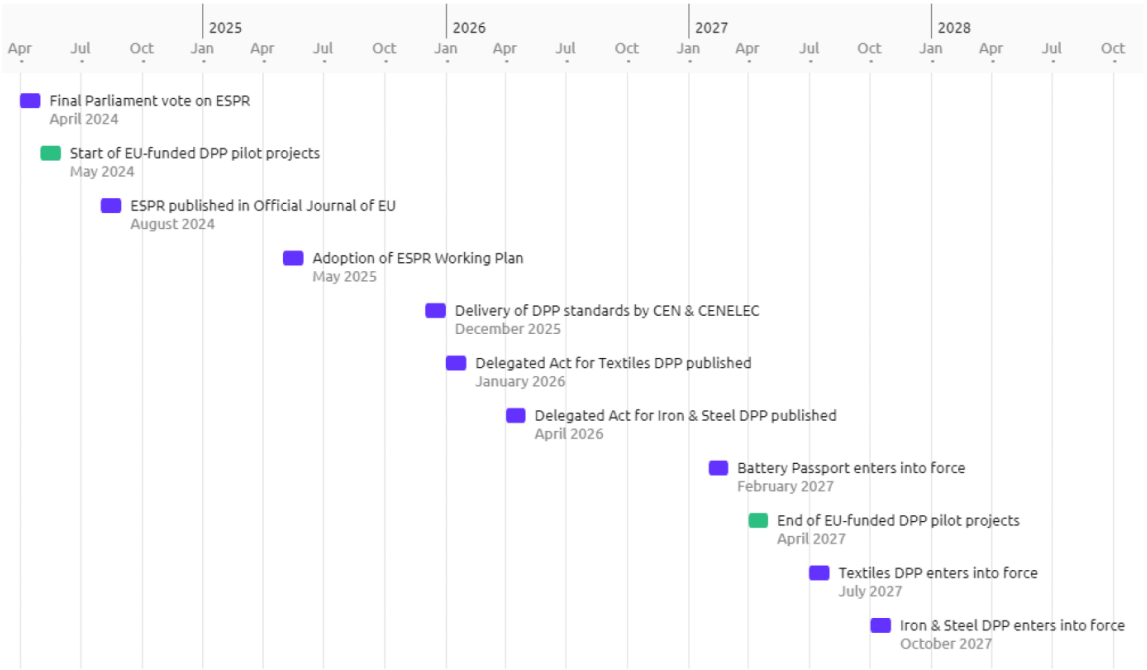
4.1.4. Calendrier d'application

Le règlement ESPR sera déployé progressivement à partir de 2027 par catégorie de produits et avec une suite logique d'extension progressive à d'autres secteurs et produits. Voici un récapitulatif de l'agenda :

- **2024** : adoption officielle du règlement.

- **2025-2026** : élaboration des standards techniques et mise en place de projets pilotes sectoriels (CEN/CENELEC, CIRPASS et autres initiatives).
- **2027** : entrée en vigueur des premiers passeports numériques obligatoires pour les batteries, suivis de près par les textiles.
- **2030** : extension progressive à d'autres catégories de produits (électronique grand public, mobilier, construction).

Cross-sector DPP system roadmap timeline 2024-2027



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

4.2. Digital Product Passport (DPP)

Le Passeport Numérique de Produit (DPP) est un instrument réglementaire central du règlement ESPR, visant à accompagner la transition vers une économie circulaire au sein de l'Union européenne. Il a pour vocation de garantir un accès structuré, sécurisé et interopérable aux informations clés des produits tout au long de leur cycle de vie, tant pour les consommateurs que pour les opérateurs économiques et les autorités.

Concrètement, le DPP intègre un identifiant unique de produit, souvent un GTIN (Global Trade Item Number), ou équivalent, associé à des métadonnées techniques, environnementales et de conformité. Ces informations sont accessibles via un lien numérique (URI), encodé dans un support lisible par machine (QR Code, DataMatrix, RFID), et conforme aux normes GS1 et ISO (ex. ISO/IEC 15459, 20248, 18004).

L'objectif est de favoriser la transparence, la traçabilité et la circularité en assurant la disponibilité d'informations fiables (composition, réparabilité, provenance, empreinte carbone, etc.) au sein d'un écosystème interopérable et harmonisé à l'échelle européenne. Ce dispositif est progressivement déployé par catégorie de produits via des actes délégués, avec une entrée en vigueur attendue à partir de 2027.

5. Enjeux pour la Wallonie et les PME locales

L'introduction du passeport numérique de produit (DPP), dans le cadre de la réglementation européenne ESPR, représente un tournant majeur pour les entreprises wallonnes. Cette obligation réglementaire ne doit pas être perçue comme une contrainte supplémentaire, mais comme une opportunité stratégique pour renforcer la compétitivité des PME dans un contexte de transition écologique, numérique et industrielle.

5.1. Conformité réglementaire et réduction des risques

Le premier enjeu réside dans l'alignement avec la réglementation européenne. Les entreprises qui ne se prépareront pas à temps au DPP s'exposeront à des risques de non-conformité, pouvant entraîner des sanctions financières ou l'exclusion de certains marchés. Pour la Wallonie, dont l'économie est fortement tournée vers l'Europe avec plus de 40 milliards d'euros exportés chaque année, cet enjeu est particulièrement stratégique. L'adoption rapide du DPP n'est pas seulement une obligation réglementaire, elle constitue une condition essentielle pour préserver l'accès sécurisé aux marchés et protéger la réputation de ses entreprises.

5.2. Opportunité de différenciation et de compétitivité

Au-delà de la conformité, le DPP constitue un outil stratégique permettant aux PME d'apporter une transparence accrue sur la traçabilité, la durabilité et la circularité de leurs produits. Les entreprises capables de démontrer la qualité de leurs processus, leur empreinte environnementale réduite ou leur capacité de recyclage, renforceront leur attractivité auprès de clients finaux, de donneurs d'ordre industriels et d'investisseurs. Pour les PME wallonnes, souvent positionnées comme sous-traitants ou fournisseurs de niches, le DPP peut devenir un facteur de différenciation décisif.

5.3. Simplification des échanges et interopérabilité

L'un des défis majeurs pour les PME est de gérer la complexité des données exigées par le DPP (composants, substances, empreinte carbone, réparabilité, etc.). En s'appuyant sur des standards européens harmonisés, le DPP permettra de réduire les coûts administratifs liés à la gestion documentaire et aux audits de conformité. Les solutions numériques

interopérables, intégrées dans des chaînes logistiques ou des plateformes sectorielles, contribueront à alléger la charge pour les PME tout en améliorant la fluidité des échanges.

5.4. Transformation numérique et montée en compétences

L'introduction du DPP agit comme un accélérateur de la transformation numérique des entreprises. Pour les PME wallonnes, il s'agit d'une opportunité de moderniser leurs systèmes d'information, de renforcer la collecte et l'exploitation des données produit, et de s'approprier des technologies innovantes telles que la blockchain, l'intelligence artificielle appliquée à la durabilité, ou encore les jumeaux numériques. Cet effort s'accompagne d'une montée en compétences du personnel, indispensable pour renforcer la résilience et l'agilité des entreprises locales.

5.5. Contribution à la transition écologique et à l'économie circulaire

La Wallonie a placé l'innovation, la durabilité et l'économie circulaire au cœur de sa stratégie de développement économique. Le DPP s'inscrit pleinement dans cette vision, en permettant de mesurer et de valoriser les efforts des entreprises en matière d'empreinte carbone, de réemploi des matériaux, et de recyclabilité des produits. Pour les PME actives dans les secteurs stratégiques régionaux (chimie, construction, logistique, électronique, textile), le DPP constitue un levier concret pour inscrire leurs activités dans un modèle économique durable et reconnu au niveau européen.

5.6. Positionnement stratégique de la Wallonie dans les initiatives européennes

La Wallonie s'inscrit également dans une dynamique proactive à travers son programme **DigitalWallonia4Trust**, qui a déjà permis le développement de premiers démonstrateurs blockchain régionaux. Dans ce prolongement, l'exploration d'un passeport numérique de produit basé sur la blockchain constitue une opportunité stratégique pour proposer une solution allant au-delà des standards proposés dans CIRPASS. Bien que la Wallonie ne soit pas membre direct du consortium CIRPASS, plusieurs entreprises belges y participent activement, renforçant ainsi le lien entre l'écosystème régional et les initiatives européennes. Cette démarche permet à la Région de valoriser son expertise technologique propre, tout en contribuant à façonner des solutions plus résilientes, sécurisées et adaptées aux besoins des PME locales.

6. Etat de l’art

6.1. Standardisation

6.1.1. Normes ISO

L’intégration des normes ISO/IEC constitue un fondement essentiel de l’architecture du Passeport Numérique de Produit, garantissant son interopérabilité, sa fiabilité et sa conformité aux exigences européennes. La norme ISO/IEC 15459 assure une identification unique, globale et non ambiguë des produits et entités, pilier central pour relier chaque article à son DPP. En complément, la norme ISO/IEC 20248 permet de garantir l’authenticité des données échangées à travers les supports AIDC (codes-barres, RFID), grâce à une signature numérique intégrée vérifiable hors ligne. Enfin, la norme ISO/IEC 18004 définit les spécifications techniques des codes à barres 2D incluant les QR Codes, assurant via les standards GS1 (GTIN, GLN, etc.), une compatibilité avec les dispositifs d’identification et de lecture déployée dans l’industrie et l’accessibilité sécurisée aux URI du DPP via les dispositifs de lecture optique standards. Ensemble, ces normes forment une base technique robuste pour l’identification, la traçabilité et l’intégrité des données produits dans l’écosystème DPP.

6.1.1.1. ISO / IEC 15459 (identification unique)

La norme ISO/IEC 15459 constitue un socle fondamental pour l’identification unique dans le cadre du DPP. Elle définit les principes et les structures permettant d’assigner un identifiant global, unique et non ambigu aux objets physiques (produits, composants, équipements) et entités logistiques, garantissant ainsi l’interopérabilité au sein des chaînes d’approvisionnement internationales.

Cette norme est particulièrement pertinente dans le contexte de l’AIDC (Automatic Identification and Data Capture), puisqu’elle permet de lier de manière fiable un produit à ses données numériques via un identifiant stable. Elle est d’autant plus cruciale que le DPP repose sur la capacité à suivre et authentifier chaque objet individuellement, y compris dans des environnements complexes et multi-acteurs.

Conformément aux exigences du règlement ESPR, l’ISO/IEC 15459 est souvent combinée à d’autres standards comme le GTIN, le GLN ou les structures GS1 Digital Link, renforçant la traçabilité et la transparence sur l’ensemble du cycle de vie des produits.

6.1.1.2. ISO / IEC 20248 (authenticité des données)

La norme ISO/IEC 20248 joue un rôle central dans l’intégrité et l’authenticité des données transmises via des supports AIDC (Automatic Identification and Data Capture), en particulier dans le cadre du DPP. Elle spécifie une structure de données signée numériquement,

capable d'être incorporée dans des codes à barres ou des étiquettes RFID, permettant à tout lecteur conforme de vérifier l'origine et la véracité des données sans connexion à un serveur distant.

Cette capacité d'auto-vérification décentralisée est particulièrement adaptée aux exigences du règlement ESPR, notamment pour lutter contre la fraude, garantir la fiabilité des informations produits, et renforcer la confiance entre les parties prenantes (fabricants, autorités, consommateurs).

Dans l'écosystème du DPP, ISO/IEC 20248 peut être utilisée en complément d'identifiants uniques (ex. ISO/IEC 15459) pour associer des métadonnées vérifiables à chaque produit, tout au long de son cycle de vie.

6.1.1.3. ISO / IEC 18004 (RFID)

La norme ISO/IEC 18004 définit les caractéristiques techniques des systèmes RFID (Radio Frequency Identification) pour l'identification automatique des objets. Elle spécifie les interfaces air (ou lien de communication) entre le lecteur et l'étiquette RFID pour différentes bandes de fréquence (LF, HF, UHF), assurant ainsi l'interopérabilité des dispositifs AIDC.

Dans le cadre du DPP, cette norme constitue une référence essentielle pour la lecture et l'écriture de données sans contact. L'ESPR autorise l'usage de supports RFID (en complément ou en alternative aux QR Codes/Data Matrix), à condition qu'ils soient conformes aux normes ISO reconnues et interopérables à l'échelle européenne.

L'utilisation d'étiquettes RFID conformes à ISO/IEC 18004 permet de garantir une traçabilité robuste, même en environnement industriel, sans ligne de visée, et facilite la gestion logistique tout au long du cycle de vie du produit.

6.1.2. AIDC (Automatic Identification and Data Capture)

L'AIDC regroupe un ensemble de technologies destinées à l'identification automatique d'objets, de produits ou d'actifs, et à la capture de données associées. Ces technologies sont centrales dans l'écosystème du DPP, car elles permettent de garantir la fiabilité, l'interopérabilité et l'automatisation du transfert d'informations tout au long du cycle de vie des produits.

L'approche AIDC repose sur l'utilisation de supports lisibles par des machines, tels que les codes-barres, les codes 2D (QR Code, DataMatrix) ou les étiquettes RFID, combinés à des dispositifs de lecture optique ou radio. Ces supports embarquent des identifiants produits (GTIN, GLN…) et des métadonnées codées selon des normes ISO ou GS1, permettant d'assurer une cohérence internationale dans les systèmes d'information logistique, de traçabilité, ou de conformité réglementaire.

En lien avec les exigences de l'ESPR, l'AIDC permet de lier efficacement les objets physiques aux passeports numériques hébergés sur le web, via des identifiants standardisés. Cette architecture garantit une compatibilité avec les infrastructures existantes et un accès universel aux informations produits, via tout lecteur conforme.

Les technologies AIDC sont ainsi devenues un pilier technique incontournable pour la mise en œuvre des DPP, assurant une lecture automatisée, fiable et sécurisée des identifiants dans toutes les phases de la chaîne de valeur, de la production à la distribution, jusqu'au recyclage.

6.1.3. GTIN (Global Trade Item Number)

Le GTIN (Global Trade Item Number) est un identifiant globalement reconnu et standardisé par GS1, conçu pour l'identification unique des articles commerciaux. Il joue un rôle central dans l'architecture du DPP, en tant qu'identifiant de référence permettant de relier un produit physique à ses données numériques de manière univoque et interopérable au niveau international. Le GTIN peut également être enrichi grâce aux AI (Application Identifiers), des préfixes standardisés définis par GS1 permettant d'ajouter des informations complémentaires telle que le numéro du lot (AI 10), le numéro de série (AI 21) ou encore la date d'expiration (AI 17). Ces éléments sont souvent encapsulés dans les QR code ou dans les structures GS1 Digital Link, offrant une lecture directe et une sémantique riche aux données du produit.

Le GTIN s'inscrit dans l'écosystème des normes ISO/IEC 15459, garantissant ainsi sa compatibilité avec les systèmes AIDC. Ce cadre normatif assure une interopérabilité renforcée et permet d'adapter les exigences à chaque catégorie de produits définie par actes délégués. Dans la logique du DPP, le GTIN est souvent encodé dans un QR Code conforme à ISO/IEC 18004, offrant un accès direct, sécurisé et sémantiquement enrichi aux informations du produit.

6.1.4. L'URI (Uniform Resource Identifier)

L'URI est un identifiant normalisé qui permet d'accéder de manière unique, pérenne et interopérable à une ressource numérique, ici, aux données essentielles du DPP. Dans le cadre du règlement ESPR, les URI jouent un rôle central : elles lient les identifiants physiques (comme le GTIN, le GLN ou le numéro de série) aux données numériques accessibles via le web, tout en assurant la compatibilité avec les systèmes d'identification automatique (AIDC).

En utilisant une URI conforme à la spécification GS1 Digital Link, comme nous le verrons au point 6.1.6, chaque produit peut être associé à un lien structuré lisible par un navigateur ou une machine. Cette URI encapsule à la fois l'identifiant du produit et les métadonnées associées, rendant l'accès aux informations produit fluide, sécurisé, et conforme aux exigences de transparence de l'Union européenne.

6.1.5. La standardisation GS1

L'organisation GS1 est un organisme international à but non lucratif, reconnu pour avoir développé et maintenu les systèmes d'identification les plus largement utilisés dans le commerce mondial, tels que le GTIN, le GLN, le SSCC et les codes à barres. Dans le cadre du DPP, la Commission européenne a identifié GS1 comme l'un des piliers techniques les plus aptes à fournir une infrastructure d'identification unique, interopérable et normalisée à l'échelle mondiale.

Les standards GS1 sont déjà déployés dans plus de 150 pays et couvrent l'ensemble de la chaîne de valeur : fabricants, importateurs, distributeurs, prestataires logistiques et même consommateurs. Leur adoption garantit la compatibilité avec les systèmes d'AIDC (Automatic Identification and Data Capture), tout en assurant une cohérence avec les exigences de traçabilité, d'accès aux données produit et de portabilité posées par l'ESPR. En conséquence, les identifiants GS1 (notamment le GTIN, le GLN ou le Digital Link) constituent la colonne vertébrale du système d'identification recommandé pour la mise en œuvre du DPP.

6.1.6. GS1 Digital Link

Le GS1 Digital Link est une structure normalisée de type URI (Uniform Resource Identifier) développée par GS1 pour permettre à un identifiant tel qu'un GTIN de devenir un lien web cliquable. Il permet d'associer à un produit non seulement son identifiant unique, mais aussi l'ensemble de ses données numériques, conformément aux exigences du DPP.

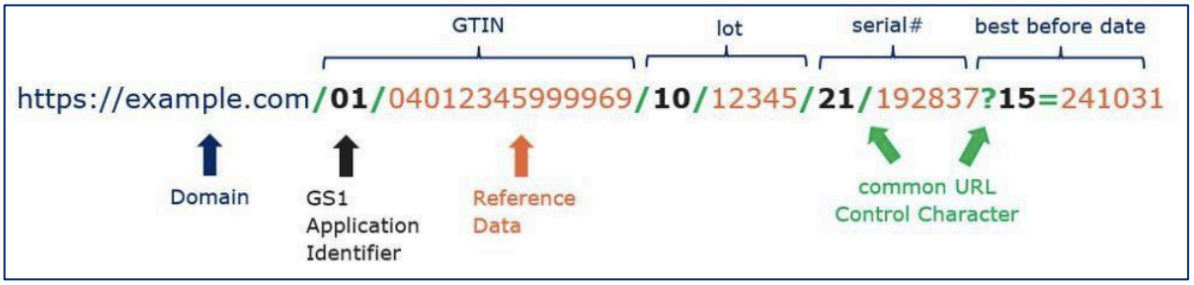
Dans le contexte du règlement ESPR, le GS1 Digital Link constitue la méthode privilégiée pour encoder les identifiants produits dans un QR Code conforme à la norme ISO/IEC 18004. Cette approche rend les données directement accessibles aux consommateurs, autorités et partenaires commerciaux, tout en garantissant leur sécurité et leur interopérabilité.

Dans ce cadre, chaque identifiant produit est encodé sous forme d'Application Identifier (AI), ce qui permet d'enrichir le GTIN avec des informations complémentaires normalisées. Parmi les plus courants figurent le numéro de lot (AI 10), le numéro de série (AI 21) ou encore la date d'expiration (AI 17, au format YYMMDD selon les standards GS1). Cette structuration garantit une lecture uniforme et interopérable des données tout au long de la chaîne de valeur.

Exemple de structure URI recommandée :

https://id.gs1.org/01/GTIN/21/SERIAL
ou

https://domainefabricant.com/01/GTIN/21/SERIAL



[2]

Chaque segment de l'URI correspond à un Application Identifier (AI) GS1 :

01 = AI indiquant le GTIN utilisé dans le cadre du Digital Link GS1
10 (optionnel) = Numéro de lot
21 = Numéro de série
15 (optionnel) = Date d'expiration (au format YYMMDD selon les standards GS1)

Ce format d'URI permet de lier dynamiquement un produit physique à son passeport numérique hébergé dans une base de données sécurisée, tout en assurant la compatibilité avec les systèmes existants de traçabilité, d'inventaire ou de douane.

L'approche GS1 Digital Link renforce la portabilité des données et la résilience du système, tout en permettant aux DPP d'être consultés via n'importe quel lecteur optique ou smartphone compatible, sans recourir à un système propriétaire.

6.1.7. GS1 DataMatrix

Le GS1 DataMatrix est un symbole de code 2D normalisé, conforme à la norme ISO/IEC 16022, qui permet d'encoder des identifiants GS1 (comme le GTIN, le numéro de lot, ou le numéro de série) ainsi que des données supplémentaires en format structuré.

Dans le cadre du DPP, il constitue une alternative reconnue au QR Code, offrant une densité de données élevée et une meilleure lisibilité sur des surfaces réduites, notamment pour les produits de petite taille ou les applications industrielles.

En complément du QR code, l'utilisation du GS1 DataMatrix est reconnue comme option conforme dans le DPP dans les spécifications techniques établies par le consortium CIRPASS et les lignes directives GS1. Ce format permet ainsi un accès direct aux données du DPP, tout en assurant la compatibilité avec les systèmes de lecture existants dans les chaînes logistiques, notamment dans les filières des batteries, du textile ou de l'électronique.

---

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

Son adoption dans le DPP est particulièrement pertinente lorsque les contraintes d'impression, la sécurité ou la robustesse des lectures optiques sont déterminantes.

6.1.8. Conclusion sur la standardisation :

Les normes ISO/IEC, les standards GS1 et les technologies AIDC forment un socle cohérent, interopérable et sécurisé pour la mise en œuvre du Passeport Numérique de Produit (DPP). Leur articulation permet d'assurer l'identification univoque des produits (via ISO/IEC 15459), la garantie de l'authenticité des données (via ISO/IEC 20248), ainsi que la compatibilité des supports de lecture (via ISO/IEC 18004, RFID, DataMatrix...).

Concrètement, lorsqu'un code AIDC conforme est scanné (QR Code, DataMatrix ou étiquette RFID), le système peut automatiquement récupérer :

- l'identifiant unique du produit (GTIN)
- l'URI GS1 Digital Link, menant vers la fiche numérique sécurisée du produit
- ainsi que les attributs obligatoires ou contextuels définis pour chaque catégorie de produit : numéro de lot, numéro de série, date d'expiration, version, etc.

Ces éléments sont encapsulés dans des formats standardisés, garantissant une lecture fluide, sécurisée et interopérable par n'importe quel acteur de la chaîne de valeur. Ce fonctionnement assure la conformité au règlement ESPR, tout en facilitant la traçabilité, la vérification d'authenticité et l'accès aux données produit, même hors ligne.

6.2. Revue des initiatives

Le paysage des initiatives liées au DPP est aujourd'hui extrêmement fragmenté. On observe à la fois des approches normatives (GS1, CEN/CENELEC, ISO), des projets sectoriels pilotes (batteries, textile, électronique, construction) et des solutions technologiques de marché (start-ups, consortiums industriels, plateformes SaaS). Ces initiatives peuvent être regroupées selon leur situation géographique, leur secteur d'application et leur choix technologique (recours ou non à la blockchain).

6.2.1. Europe

6.2.1.1. Projets CIRPASS :

Le projet CIRPASS (Cross-sectoral Interoperable Registries for Digital Product Passports) constitue l'un des travaux les plus structurants sur le DPP. Mené jusqu'en mars 2024, CIRPASS 1 visait à établir une définition inter-sectorielle claire du DPP, un modèle de données commun, ainsi qu'un protocole d'échange ouvert pour faciliter l'interopérabilité entre secteurs (électronique, textiles, batteries). Plusieurs roadmaps et prototypes ont été

développés, permettant de tester des dispositifs pilotes et de bâtir une approche harmonisée.

Le prolongement CIRPASS-2 s'inscrit dans le programme Digital Europe. Il vise la phase pilote à large échelle, notamment avec des DPP validés dans les chaînes de valeur du textile, des batteries et de l'électronique, en préparation à l'application progressive du règlement ESPR dès 2027. CIRPASS-2 consolide la dimension opérationnelle, interopérable et sectorielle du passeport produit tout en assurant un socle technique et normatif partagé.

6.2.1.2. Global Battery Alliance – Battery Passport :

Le Battery Passport est porté par une alliance mondiale (GBA, basée à Bruxelles mais active à l'échelle internationale) et constitue le projet phare aligné avec la réglementation européenne sur les batteries. L'objectif est d'assurer un suivi harmonisé du cycle de vie, de l'empreinte carbone et de la circularité des batteries. La gouvernance est technologiquement neutre, mais plusieurs implémenteurs (ex. Circulor, Minespider) explorent la blockchain comme registre d'authenticité.

6.2.1.3. GS1 en Europe :

GS1 fournit un référentiel normatif via GS1 Digital Link et l'identification unique des produits (GTIN). L'approche repose sur des standards ouverts interopérables, adoptés par de nombreux projets pilotes DPP. Elle ne prescrit pas l'usage de la blockchain mais garantit l'unicité et la persistance des identifiants.

6.2.1.4. Initiatives privées

Dans l'espace européen, de nombreux projets traduisent la diversité des approches technologiques et sectorielles autour du passeport numérique produit. En France, plusieurs solutions se distinguent. Keeex, par exemple, mise sur des mécanismes cryptographiques (horodatage, signature, intégrité) pour assurer la fiabilité des données, tout en restant en dehors des logiques blockchain. À l'inverse, Tilkal a développé une infrastructure de traçabilité inter-entreprises reposant sur une blockchain permissionnée, avec des cas d'usage dans l'agroalimentaire, le textile ou l'électronique. Arianee illustre une orientation plus radicalement ouverte : ce protocole open source, basé sur Ethereum, ambitionne de standardiser l'identité numérique des produits dans le secteur du luxe et de la distribution. TextileGenesis, quant à lui, s'est progressivement éloigné de la blockchain pour adopter une logique SaaS fondée sur des certificats et des jetons de volumes de matière, répondant ainsi à une exigence de simplicité d'usage pour les industriels du textile.

Aux Pays-Bas, l'innovation se cristallise autour de Circularise, qui associe blockchain permissionnée et preuves à divulgation nulle de connaissance (ZKP) pour concilier confidentialité des données industrielles et transparence des chaînes d'approvisionnement. Dans la construction, Madaster privilégie une approche centralisée à travers ses passeports

de matériaux, intégrés dans une logique de réemploi et de circularité sans recours à la blockchain.

En Allemagne, en Autriche et en Suisse, les initiatives reflètent une articulation étroite entre industrie, normalisation et innovation numérique. Catena-X, écosystème automobile de référence, déploie des passeports numériques intégrés à Gaia-X et à l'Asset Administration Shell, sans s'appuyer sur des registres distribués. Spherity, en revanche, explore les identités décentralisées (DID) et les Verifiable Credentials, avec un ancrage blockchain partiel, tandis que Narravero propose une alternative SaaS orientée PME. Dans le luxe, l'Aura Blockchain Consortium (Suisse/Luxembourg), regroupant LVMH, Prada ou Cartier, a choisi une blockchain privée de type Ethereum/Quorum pour garantir l'authenticité des produits haut de gamme.

Les pays d'Europe du Nord privilégient des solutions SaaS et cloud, à l'image de TrusTrace en Suède, qui structure la traçabilité textile via la collecte de preuves documentaires, ou Whatt.io qui combine NFC et infrastructure blockchain pour gérer la propriété et l'authenticité des biens. Au Royaume-Uni, Provenance, pionnier du DPP, illustre une trajectoire hybride : après avoir expérimenté la blockchain, la solution repose désormais sur des données vérifiables et des architectures hybrides. iPoint-systems, pour sa part, propose une suite logicielle de conformité ESG et substances, sans composante blockchain. En Europe du Sud, l'Italie concentre plusieurs initiatives notables : Certilogo s'appuie sur l'intelligence artificielle pour l'authentification dans la mode, tandis que The ID Factory propose une plateforme textile interopérable, ouverte à des intégrations blockchain. Dans le bâtiment, Cobuilder développe des solutions basées sur les jumeaux numériques et l'Asset Administration Shell, en cohérence avec les standards européens émergents.

Dans leur ensemble, ces initiatives européennes traduisent une tension structurante : d'un côté, des architectures SaaS centralisées, rapides à mettre en œuvre et plus accessibles pour les PME ; de l'autre, des expérimentations blockchain, souvent ciblées sur des filières où la confiance, l'authenticité et la traçabilité intersectorielle sont particulièrement critiques (textile, luxe, agroalimentaire, électronique).

6.2.1.5. Belgique

La Belgique se positionne comme un terrain fertile pour l'expérimentation de passeports numériques, avec des initiatives variées qui reflètent à la fois la dynamique entrepreneuriale locale et l'intégration aux projets européens. Dans le secteur de l'économie circulaire, TripleR.io, en Fandre, a lancé *mattressID*, un dispositif destiné au suivi et au recyclage des matelas. En combinant QR codes et puces RFID, la solution permet de tracer la composition et le cycle de vie de chaque produit, facilitant ainsi leur collecte et leur réemploi. Son architecture repose sur un modèle cloud centralisé, simple à déployer, et s'inscrit déjà dans

des programmes pilotes européens, ce qui en fait un exemple concret d'application sectorielle alignée avec les priorités de circularité.

En parallèle, certaines initiatives belges explorent des approches plus décentralisées. Crypto Kastaar, implanté également en Flandre, développe un passeport numérique pour les bières, accessible via QR ou NFC. L'originalité de cette initiative réside dans son inscription dans une logique Web3, avec ancrage des données sur une blockchain publique. Cette orientation traduit une volonté d'expérimenter de nouveaux modèles de confiance et de transparence, particulièrement adaptés à des filières où l'authenticité et l'image de marque constituent des leviers commerciaux.

Sur le plan institutionnel, GS1 Belu, basé à Bruxelles, joue un rôle structurant dans l'accompagnement des entreprises belges. À travers ses ateliers et ressources, l'organisation aide les PME à se préparer à l'implémentation du DPP en s'appuyant sur les standards internationaux *GS1 Digital Link*. L'approche est volontairement technologie-agnostique et non blockchain, centrée sur l'interopérabilité et la simplification des processus pour les acteurs économiques locaux. Enfin, l'écosystème se complète avec Twintag, une jeune entreprise flamande qui propose une plateforme SaaS flexible pour créer des passeports numériques adaptés à divers secteurs tels que le textile, la logistique ou l'électronique. Reposant sur une architecture centralisée mais extensible, la solution s'intègre déjà dans plusieurs pilotes européens, illustrant une orientation vers l'industrialisation rapide et l'usage transverse.

Dans leur ensemble, ces initiatives belges révèlent une complémentarité intéressante : d'un côté, des projets pragmatiques et normatifs qui visent à assurer l'adoption large par les PME ; de l'autre, des expérimentations Web3 qui explorent le potentiel de la blockchain pour renforcer l'authenticité et la traçabilité. Cette diversité constitue un atout stratégique pour la Belgique, qui peut ainsi contribuer activement à la définition des futurs standards européens tout en offrant aux acteurs locaux des options adaptées à différents niveaux de maturité technologique et sectorielle.

6.2.2. International et multi-régions

Au-delà de l'Europe, le mouvement du DPP s'illustre par des projets transcontinentaux, souvent portés par de grands groupes technologiques ou des consortiums internationaux. Aux États-Unis, EON développe une plateforme centralisée de passeports numériques pour la mode et les biens durables, intégrant des services de revente et de réparation. Digimarc mise sur l'identification par filigrane numérique, alignée sur les standards GS1, avec des applications concrètes dans le recyclage plastique. Au Canada, OPTEL déploie la suite Optchain, interopérable avec des *data spaces* et capable, selon les cas, d'intégrer des registres distribués.

Certaines initiatives explorent plus directement la blockchain publique. VeChain, en partenariat avec DNV, a conçu le projet *My Story*, qui permet d'assurer la traçabilité et l'authenticité de produits agroalimentaires et de luxe grâce à sa blockchain VeChainThor. La fondation IOTA a développé des prototypes de DPP pour le plastique et l'électronique, utilisant son registre distribué Tangle et intégrant identités décentralisées et Verifiable Credentials. Enfin, le partenariat entre Circularise et Marubeni au Japon illustre l'exportation de solutions européennes vers l'Asie, avec l'utilisation de ZKP pour protéger la confidentialité des données tout en favorisant la transparence sur la composition des matériaux.

Ces projets internationaux témoignent d'une forte dynamique d'expérimentation, où la blockchain occupe une place plus centrale qu'en Europe. Toutefois, ils reflètent également la difficulté de trouver un équilibre entre transparence, confidentialité et interopérabilité globale. Là où l'Europe privilégie une approche normative et sectorielle pilotée par le cadre réglementaire de l'ESPR, les initiatives nord-américaines et asiatiques explorent des modèles de marché, cherchant à démontrer rapidement la valeur ajoutée du passeport produit dans des secteurs comme le luxe, l'agroalimentaire, le textile ou l'électronique.

6.2.3. Conclusion sur les initiatives

Le paysage des initiatives DPP en 2025 illustre la coexistence d'architectures décentralisées et centralisées. Certaines solutions s'appuient sur la blockchain afin de fournir immuabilité et attestations vérifiables, tandis que d'autres privilégient standards ouverts et simplicité d'intégration. CIRPASS, Battery Pass et GS1 structurent l'harmonisation technique et réglementaire, tandis que des fournisseurs publics et privés accélèrent les déploiements sectoriels. La Belgique bénéficie d'initiatives locales et d'un ancrage européen fort, offrant un terrain favorable à l'implémentation pragmatique du DPP pour les PME.

7. Etude de marché

7.1. Étude de marché : analyse croisée des entretiens

Dans le cadre de la mission DPP en Wallonie, cinq entretiens semi-directifs ont été réalisés auprès d'acteurs industriels régionaux issus de différents secteurs (pharma, cosmétique, dispositifs médicaux, mobilier, agroalimentaire, etc.). L'objectif était d'identifier leurs pratiques actuelles de gestion de données produit, leurs attentes vis-à-vis d'un DPP, les freins rencontrés, ainsi que leur perception des solutions numériques émergentes, dont la blockchain. Ces retours d'expérience permettent de dresser un état des lieux structuré et représentatif du tissu économique wallon, en amont de la mise en place d'une solution DPP à plus grande échelle.

7.2. Un intérêt marqué pour la traçabilité et la conformité

Toutes les entreprises interrogées expriment un besoin croissant de garantir la traçabilité, la qualité et la conformité des produits. Cette exigence est d'autant plus forte que les secteurs concernés relèvent majoritairement de l'agroalimentaire, du pharmaceutique, du cosmétique ou du dispositif médical. Dans ces secteurs fortement réglementés, les systèmes d'information existants visent à répondre à des obligations normatives (ISO 9001, HACCP, etc.), mais peinent à assurer une vision fluide, transversale et à jour des données produit.

7.3. Des outils hétérogènes, souvent cloisonnés

L'écosystème numérique des entreprises est majoritairement fragmenté. ERP, fichiers Excel, bases de données Access, logiciels de gestion documentaire ou qualité sont utilisés en parallèle, sans véritable interopérabilité. Plusieurs répondants évoquent des difficultés à faire communiquer leurs outils internes ou à intégrer les partenaires externes dans les chaînes d'information. La duplication manuelle de données reste fréquente, occasionnant des erreurs et une perte de temps importante.

7.4. Une gestion complexe des données techniques

Les informations techniques produit (fiches, spécifications, composants, étiquetage, documentation réglementaire) sont éparpillées entre plusieurs systèmes, souvent non mis à jour. Certaines entreprises conservent encore des archives papier. L'absence de référentiel unique ou de gouvernance claire complexifie l'accès aux données fiables. Les changements de version, les multiples formats et la multiplicité des contributeurs freinent la consolidation d'une vue unique produit.

7.5. Vers une sensibilisation croissante au DPP

Si la notion même de DPP est encore peu connue, toutes les entreprises manifestent un intérêt pour un système structuré permettant de centraliser, tracer et partager des données produit tout au long du cycle de vie. Le DPP est perçu comme un levier pour répondre aux obligations de l'ESPR, mais aussi comme un outil interne de pilotage de la qualité, de réduction des non-conformités, et d'amélioration de la maintenance ou du service client. Certains entrevoient déjà des cas d'usage dans leur chaîne de valeur.

7.6. Une ouverture mesurée à la blockchain

La technologie blockchain n'est pas familière à la majorité des interlocuteurs, mais plusieurs d'entre eux en comprennent les avantages théoriques : immutabilité, horodatage, sécurisation, traçabilité décentralisée. Toutefois, son image reste associée à la

crypto-finance et à la complexité technique. Pour être adoptée, la blockchain devra être invisible à l'utilisateur final, intégrée aux outils métier et démontrer une valeur ajoutée claire (ex. : preuves de conformité, simplification des audits, interopérabilité).

7.7. Des attentes fortes sur l'accompagnement

Les entreprises expriment un besoin d'accompagnement fort : aide au diagnostic, cartographie des données, aide à la structuration des référentiels, assistance à la sélection de standards (GTIN, URI, JSON-LD…), formation, etc. L'intégration d'un DPP, et a fortiori de la blockchain, suppose une montée en maturité numérique. La lisibilité des initiatives pilotes, la clarification du rôle des autorités publiques, et la démonstration de cas concrets seront déterminants pour lever les réticences.

7.8. Conclusion

Les entretiens réalisés montrent que les entreprises wallonnes sont confrontées à des enjeux de traçabilité, de qualité, de conformité documentaire et d'intégration des systèmes. Le DPP apparaît comme une réponse prometteuse à ces défis, à condition qu'il soit simple, interopérable et soutenu par un accompagnement adapté. La blockchain peut y contribuer, mais elle devra rester au service de l'usage, sans complexifier les processus. Le contexte réglementaire (ESPR), combiné à l'émergence de projets structurants comme le DPPSP, crée une dynamique propice à l'expérimentation.

8. Proposition de solution blockchain

8.1. Objectifs : dépasser les limites de l'architecture CIRPASS

Les travaux du projet CIRPASS ont constitué une avancée majeure dans la définition d'une architecture de référence pour le DPP, en intégrant les cadres normatifs européens (ESPR, CEN/CENELEC, ISO, GS1) et en proposant une approche modulaire et interopérable. Cette architecture, fondée sur des registres de données centralisés ou fédérés, répond à de nombreux impératifs de gouvernance, de standardisation et de conformité. Elle a cependant mis en évidence un ensemble de limites structurelles qui, à terme, pourraient freiner la résilience et l'adoption généralisée du DPP par les entreprises européennes, et en particulier par les PME.

Le diagnostic CIRPASS souligne notamment trois vulnérabilités majeures. Premièrement, la dépendance vis-à-vis d'un Digital Product Passport Service Provider (DPPSP) centralisé introduit un risque de "single point of failure", tant sur le plan technique (pannes, attaques,

perte de disponibilité) que sur le plan institutionnel (risques de censure, d'exclusion de certains acteurs ou de distorsion concurrentielle). Deuxièmement, l'architecture actuelle repose sur une forte confiance institutionnelle dans les intermédiaires qui hébergent et valident les données, sans garantie de mécanismes techniques robustes contre la falsification, la suppression ou la manipulation ex-post des informations. Troisièmement, malgré l'usage recommandé de standards comme le GS1 Digital Link, l'interopérabilité réelle entre secteurs, chaînes de valeur et juridictions internationales demeure conditionnée à des accords politiques et techniques encore instables.

Dans ce contexte, il devient légitime d'explorer une alternative dite « solution idéale », qui conserve les acquis normatifs de CIRPASS tout en s'appuyant sur les atouts des technologies décentralisées. L'hypothèse que nous posons est la suivante : un DPP adossé à la blockchain et à un cloud décentralisé permettrait de renforcer la résilience, la confiance et la transparence du système, tout en offrant une traçabilité immuable des contributions des différents acteurs.

La démarche que nous proposons est donc progressive et complémentaire. Elle consiste à repartir des briques conceptuelles posées par CIRPASS, ontologies, user stories, scénarios d'identification (GTIN, GS1 DataMatrix, URI), recommandations de sécurité et d'accès, pour les transposer dans un modèle distribué où la blockchain assure le rôle de registre de confiance et où les données opérationnelles sont hébergées dans un stockage distribué redondant (par exemple via des solutions européennes telles que Alephium ou ThreeFold). Dans ce modèle, chaque enregistrement, mise à jour ou révocation d'un DPP est notarisé sur la blockchain, garantissant l'immutabilité et l'auditabilité, tandis que les données volumineuses restent accessibles via des API conformes aux standards européens.

Cette approche décentralisée permet de répondre à plusieurs enjeux identifiés par CIRPASS et la Commission européenne :

- Résilience et disponibilité : élimination du point de défaillance unique (single point of failure) grâce notamment au sharding et à la redondance distribuée (via un cloud décentralisé).
- Résistance à la censure : impossibilité pour un opérateur unique d'altérer ou de supprimer un DPP sans laisser de traces.
- Responsabilisation des acteurs : enregistrement immuable des contributions de chaque opérateur, lié à son identité numérique (DID, Verifiable Credentials).
- Interopérabilité normative : compatibilité avec les standards GS1 Digital Link et ISO/IEC 15459 pour l'identification, garantissant que la blockchain n'est pas un silo mais une couche de confiance.
- Sécurité et confidentialité : contrôle granulaire des droits d'accès aux sections du DPP via des mécanismes cryptographiques (délégation, chiffrement sélectif).

En définitive, cette solution « idéale » ne cherche pas à remplacer l'architecture CIRPASS, mais à l'étendre pour répondre aux limites inhérentes à tout système centralisé. Elle s'inscrit

dans la logique des recommandations européennes, qui préconisent à la fois la neutralité technologique et la recherche de modèles innovants garantissant la confiance et la souveraineté numérique européenne.

8.2. Principe de conception d'une solution décentralisée

CIRPASS conçoit le DPP comme un système fédéré orchestré par des DPP Service Providers (DPPSP), avec des fonctions clés de résolution, d'accès aux données, d'authentification et de gouvernance. Les risques majeurs identifiés sont la centralisation de la disponibilité, la censure potentielle, l'altération ou la perte de données, l'hétérogénéité des identifiants et la non-interopérabilité sémantique entre secteurs. Les options de redirection et de portail de recherche européen adressent la résilience de l'accès mais laissent subsister un point de défaillance sur l'opérateur du service de résolution, et déplacent la confiance vers la gouvernance du DPPSP et la conformité de ses logs.

Il faut séparer ce qui relève de la preuve, de l'indexation et de la gouvernance d'accès, de ce qui relève de l'hébergement des données métier, tout en maintenant l'alignement sur GS1 Digital Link et les ontologies CIRPASS. La blockchain est pertinente pour l'indexation, l'horodatage, le contrôle d'accès et la piste d'audit. Le stockage métier reste off-chain, mais sous des garanties de redondance et d'immutabilité contrôlée.

La proposition d'une architecture DPP décentralisée repose donc sur une série de principes de conception qui traduisent les enseignements des travaux CIRPASS tout en tirant parti des apports de la blockchain et du cloud décentralisé. Ces principes visent à assurer la conformité réglementaire, l'interopérabilité avec les standards existants et la robustesse technique face aux risques identifiés :

Minimalisme on-chain
La blockchain ne doit pas être surchargée de données. Seuls les éléments critiques y sont inscrits : index d'objets, preuves cryptographiques, événements d'audit, politiques d'accès et horodatages. Les données sensibles, personnelles ou volumineuses n'ont pas vocation à être placées directement sur la chaîne, afin de respecter les contraintes de confidentialité, de coût et de scalabilité. La couche on-chain joue donc un rôle d'ancrage et de notarisation immuable, garantissant l'authenticité et la traçabilité.

Stockage off-chain vérifiable
Les informations contenues dans le passeport produit sont idéalement conservées dans un environnement de stockage décentralisé offrant redondance opérationnelle et mécanismes de réplication. Les hash de ces données sont ancrés sur la blockchain pour garantir leur intégrité, et chaque modification est associée à un schéma de versioning attesté. Une distinction est opérée entre données publiques (accessibles à tous : composition, réparabilité, indicateurs environnementaux) et données permissionnées (accessibles

uniquement à certains acteurs via des politiques d'accès chiffrées). Ce modèle concilie transparence et protection des informations stratégiques ou confidentielles.

Identité vérifiable
L'authentification des acteurs et la gestion des rôles reposent sur des identifiants décentralisés (DIDs) et des Verifiable Credentials (VC). Ceux-ci sont liés à des identifiants d'entreprise reconnus à l'échelle européenne, tels que l'EORI, le numéro de TVA, l'EUID ou le LEI, afin d'assurer une interopérabilité et une reconnaissance officielle. Cette approche s'inscrit dans le cadre réglementaire de l'eIDAS 2.0 et permet d'attribuer à chaque action enregistrée une responsabilité claire et juridiquement traçable.

Alignement avec GS1 et CIRPASS
L'identification des produits s'appuie sur les standards GS1, en particulier le GTIN et le GS1 Digital Link, encodés dans des supports AIDC (DataMatrix ou QR code). Les données exposées suivent un format sémantique basé sur le JSON-LD, aligné avec les ontologies de haut niveau définies par CIRPASS et complété par des vocabulaires sectoriels spécifiques. Cette homogénéité sémantique garantit la compatibilité entre secteurs et facilite l'intégration avec d'autres initiatives européennes, telles que Gaia-X ou les passeports sectoriels (textiles, batteries, électronique).

Gouvernance multi-parties
La résolution et l'exploration des données sont assurées par un réseau de nœuds fonctionnant sous gouvernance partagée, de manière à éviter tout monopole technique ou institutionnel. Deux options sont envisageables : d'une part, un portail officiel opéré par la Commission européenne, qui interprète les données on-chain et fournit un point d'accès de référence ; d'autre part, un déploiement décentralisé de l'explorateur et du code applicatif sur des clouds distribués (IPFS, Arweave, ThreeFold), avec renoncement explicite des droits administratifs par le déployeur, à l'image de ce qui existe déjà dans certains protocoles décentralisés. Une approche hybride, combinant un portail officiel pour la conformité et des explorateurs indépendants pour la résilience et la transparence, apparaît comme la plus robuste. Ainsi nous pourrions avoir un portail européen central et une multitude de portails régionaux qui récupèrent et filtres les données du protocole en fonction de leurs intérêts.

Défense en profondeur
Afin de prévenir les abus, plusieurs mécanismes de protection sont combinés : attestations de liens dans la chaîne de valeur (par exemple, une entreprise ne peut ajouter des informations que si elle prouve un lien contractuel avec le produit), dépôts remboursables pour toute tentative de mise à jour (limitant le spam), listes de rôles autorisés définies au niveau du smart contract, et outils de modération automatisés. En cas de litige ou de signalement par un utilisateur, une procédure d'escalade est prévue vers l'autorité compétente, sans jamais compromettre l'immutabilité de l'historique.

Principes complémentaires
Trois principes transversaux complètent ce socle :

– Interopérabilité by design, en garantissant la compatibilité avec les API et ontologies proposées par CIRPASS, ainsi qu'avec les standards ISO, GS1 et CEN/CENELEC.
– Sustainability by design, en privilégiant des solutions techniques sobres en énergie, telles que les blockchains de type Proof-of-Stake ou les stockages décentralisés à faible empreinte environnementale.
– Resilience & fallback, en imposant une double URI (fabricant et copie immuable sur l'explorateur européen), afin d'assurer la disponibilité du passeport même en cas de disparition du domaine d'origine.

En suivant ces principes, la solution décentralisée proposée répond de manière optimale aux critères et aux limites identifiés par CIRPASS. Elle s'inscrit dans un effort de standardisation et d'interopérabilité au niveau protocolaire, garantissant une cohérence avec les cadres normatifs européens et internationaux. En parallèle, elle conserve une souplesse fonctionnelle permettant aux opérateurs économiques d'ajouter, au-delà des obligations légales, des informations volontaires et différenciantes autour du DPP. Ce double mouvement, rigueur normative d'un côté, liberté d'innovation de l'autre, contribue à faire du passeport numérique non seulement un outil de conformité, mais également un vecteur de compétitivité et de création de valeur pour les entreprises.

8.3. Proposition d'architecture décentralisée pour le DPP

Pour rappel, les travaux du projet CIRPASS ont mis en évidence plusieurs limites inhérentes aux modèles centralisés actuellement envisagés pour le DPP. En particulier, la dépendance vis-à-vis d'un DPPSP unique engendre un risque de centralisation excessif : un point de défaillance unique pour la disponibilité des données, la possibilité pour l'opérateur d'exclure arbitrairement des participants, ou encore des risques de censure et d'altération des informations.

Comme explicité précédemment, afin de dépasser ces contraintes, nous proposons une solution fondée sur la blockchain et le cloud décentralisé, garantissant résilience, résistance à la censure et immutabilité des données. Le principe repose sur une architecture hybride qui sépare les fonctions d'indexation, de preuve et de gouvernance des accès (gérées on-chain) de l'hébergement des données métier (stockées off-chain avec des garanties de redondance et d'intégrité). Cette approche respecte les standards GS1 et CIRPASS, tout en répondant aux risques identifiés.

8.3.1. Logique fonctionnelle et opérationnelle de la solution décentralisée

La solution proposée s'articule autour de composants fonctionnels interdépendants qui garantissent l'identité, l'indexation, le stockage, l'accès et la gouvernance des DPP. À travers ces composants, un cycle opérationnel clair encadre la création, la mise à jour et la

consultation du DPP, tout en respectant les standards européens et en répondant aux risques identifiés par CIRPASS.

Le **premier composant**, dédié à l'identité et à la confiance, repose sur les identifiants décentralisés (DIDs) et les Verifiable Credentials (VCs). Ces derniers attestent des rôles des acteurs (fabricant, importateur, recycleur, organisme d'évaluation de conformité) et sont liés à des identifiants reconnus en Europe (EORI, numéro de TVA, l'EUID ou le LEI). Ce mécanisme, conforme à eIDAS 2.0, garantit que chaque action est juridiquement traçable et que les relations de supply chain sont certifiées via un registre d'attestations avec possibilité de révocation.

Le **deuxième composant** assure la fonction d'ancrage et de traçabilité. Il établit le lien entre l'écosystème d'identité (DIDs/VCs) et l'infrastructure de preuve sur blockchain. Cette couche ne stocke pas les données métiers elles-mêmes, mais indexe leurs représentations et enregistre les preuves nécessaires pour garantir intégrité, authenticité et gouvernance d'accès. Elle se structure autour de cinq éléments complémentaires en plus d'un portail d'accès européen :

- **ProductPointer**
  Le ProductPointer est l'URI persistante et officielle du DPP, générée par le Portail européen. À la différence du GS1 Digital Link, lorsqu'il est hébergé sur le domaine du fabricant et donc dépendant de son maintien, le ProductPointer fournit une adresse neutre et immuable (tout comme GS1). Lorsqu'il est suivi, l'utilisateur est redirigé vers la page DPP du Portail, qui interroge la blockchain afin d'afficher les données du DPPContract correspondant.
  Le ProductPointer est intégré dans le DataMatrix ou QR code du produit, en complément du Digital Link GS1. L'association des deux assure la compatibilité avec les standards GS1 tout en apportant une redondance résiliente : même si le domaine du fabricant disparaît, l'accès via le Portail demeure garanti.

- **DPPContract**
  Le DPPContract constitue le smart contract autoritatif du passeport numérique sur la blockchain. Il centralise la logique d'orchestration et référence les différents éléments qui composent le DPP :
  - Un ou plusieurs ResourceManifests (contenant les métadonnées et pointeurs vers les ressources off-chain stockées sur un cloud décentralisé).
  - Les AccessPolicies qui définissent les règles d'accès aux données permissionnées,
  - l'EventLog qui enregistre le cycle de vie et les événements associés au produit.
  Le DPPContract inclut également les identifiants de référence (notamment le GTIN) et associe chaque opération à un acteur identifié via DID/VC. Toute consultation effectuée par le Portail ou par un résolveur tiers s'appuie sur ce contrat, qui fait office de point de vérité technique.

- **ResourceManifest**
  Le ResourceManifest décrit et référence les ressources liées à un DPP. Pour chaque ressource, il précise son type (informations réglementaires, certificats de conformité, données environnementales, instructions de maintenance, etc.), sa version, son hash d'intégrité, sa politique d'accès (publique ou restreinte), sa durée de rétention et des métadonnées contextuelles (catégorie de produit, langue, licence). Les fichiers eux-mêmes, généralement des structures JSON-LD ou des documents complémentaires comme des certificats, sont stockés dans un environnement off-chain distribué et répliqué. L'ancrage des hash dans le DPPContract permet de vérifier leur authenticité et d'assurer un versioning transparent et traçable.

- **AccessPolicy (on-chain)**
  L'AccessPolicy fixe les règles de gouvernance applicables aux données permissionnées. Il s'agit de politiques chiffrées qui conditionnent l'accès à certaines sections du DPP en fonction des rôles ou habilitations attestés par des VCs. Ainsi, seules les autorités compétentes, les organismes notifiés ou les partenaires de la supply chain peuvent consulter ou enrichir les sections qui leur sont réservées. Ces règles peuvent être mises en œuvre via des schémas de délégation de clés ou de chiffrement attributaire, garantissant un partage sélectif sans compromettre la transparence globale du passeport produit.

- **EventLog (on-chain)**
  L'EventLog est le journal immuable et append-only qui retrace l'ensemble du cycle de vie du DPP. Chaque action, création, mise à jour, transfert de responsabilité, rappel produit, correction ou marquage de fin de vie, y est inscrite de façon horodatée et liée au DID de l'acteur concerné. Ce mécanisme assure l'imputabilité et l'auditabilité de toutes les opérations, en conformité avec les exigences réglementaires et les attentes en matière de contrôle.

Pour finir, **le troisième composant** concerne l'hébergement des données métiers du DPP. À la différence du registre on-chain, qui se limite à l'indexation et aux preuves d'intégrité, ce composant gère les informations complètes relatives au produit et à son cycle de vie. L'architecture proposée reste volontairement agnostique sur le plan technologique : elle permet de référencer des ressources situées dans différents environnements, qu'il s'agisse de clouds décentralisés, de solutions centralisées classiques ou encore d'un hébergement institutionnel opéré par la Commission européenne.

La logique du protocole consiste donc à pointer vers un système de stockage sans en imposer la nature, de sorte que chaque acteur puisse choisir la solution la plus adaptée à ses contraintes techniques, économiques ou réglementaires. Néanmoins, la recommandation privilégiée est l'utilisation d'un cloud décentralisé, qui offre les meilleures garanties en matière de gouvernance, d'impartialité ainsi que d'immutabilité et de pérennité. Dans ce modèle, les données ne peuvent pas être altérées, et dans tous les cas de figure,

chaque action reste systématiquement enregistrée sur la blockchain (que ce soit pour un cloud centralisé ou décentralisé).

Les ressources off-chain comprennent notamment la fiche produit structurée en format JSON-LD, qui constitue le socle du DPP et agrège l'ensemble des ResourceManifests qui lui sont liés. Elles intègrent également les certificats de conformité et les rapports réglementaires, ainsi que les données environnementales et de réparabilité. À ces éléments peuvent s'ajouter les notices techniques et les instructions relatives à la fin de vie du produit, et, le cas échéant, des fichiers multimédias complémentaires tels que des schémas, des images ou des vidéos explicatives destinés à enrichir la compréhension et l'utilisation du produit.

Afin d'assurer la pérennité et la résilience, plusieurs principes structurent ce composant :

- Redondance : chaque ressource doit être stockée en plusieurs copies, idéalement au moins trois, afin de limiter les risques de perte de données en cas de panne ou de défaillance d'un opérateur.
- Tolérance aux pannes : le protocole prévoit que si une copie disparaît, une nouvelle copie soit automatiquement régénérée afin de maintenir le seuil minimal de disponibilité.
- Adressage par contenu : chaque ressource est identifiée par un hash cryptographique (empreinte numérique unique), ce qui permet de vérifier à tout moment qu'elle n'a pas été altérée.
- Interopérabilité : les systèmes de stockage référencés doivent être accessibles via des URI (Uniform Resource Identifiers), garantissant une compatibilité avec les API et les résolveurs du DPP.
- Neutralité technologique : les acteurs peuvent recourir à différents modèles, qu'il s'agisse d'un cloud public, d'une solution décentralisée ou d'un hébergement institutionnel, à condition que les principes de réplication, de traçabilité et de vérifiabilité soient respectés.

Une alternative envisageable réside dans la mise en place d'une solution d'hébergement institutionnelle opérée directement par la Commission européenne. Une telle option offrirait aux acteurs économiques une modalité de stockage plus traditionnelle et moins complexe à adopter que des infrastructures totalement décentralisées, ce qui pourrait faciliter l'adhésion stratégique des PME et des filières industrielles.

Toutefois, cette approche ne doit pas exclure la possibilité d'une interconnexion de solutions variées. On pourrait imaginer une simplification de la gestion du stockage via une intégration orchestrée depuis le Portail européen, permettant de paramétrer et de sélectionner une solution en fonction des besoins spécifiques de chaque acteur, sans exiger une expertise technique approfondie sur chaque type de cloud. Avec la combinaison d'initiatives telles que Gaia-X au point de vue de l'interopérabilité, il serait ainsi possible de développer des offres packagées dédiées au DPP, prêtes à l'emploi et facilement déployables aussi bien sur des

environnements centralisés que sur des solutions décentralisées, assurant un équilibre entre facilité d'adoption, interopérabilité et résilience.

Quel que soit le mode choisi, le lien entre la donnée stockée et le registre on-chain est assuré par le ResourceManifest, qui enregistre le hash, le type, la version et la politique d'accès. Ce mécanisme permet de concilier la souplesse dans le choix du stockage et l'exigence d'une intégrité vérifiable par tous.

En résumé, le troisième composant confère au DPP sa dimension documentaire et opérationnelle : il héberge l'ensemble des informations nécessaires à la traçabilité et à la conformité, tout en reposant sur des garanties de réplication, de vérifiabilité et d'immutabilité, renforcées par la recommandation d'un stockage décentralisé.

Enfin, le **Portail européen** pourrait constituer l'interface officielle de référence du DPP. Il assure la génération et l'enregistrement des identifiants on-chain, garantit la résolution des liens, notamment en cas d'indisponibilité du domaine du fabricant, et propose un moteur de recherche transversal couvrant l'ensemble des DPP. Au-delà de cette fonction technique, il joue également un rôle de conformité et de supervision, en hébergeant les formulaires réglementaires de saisie et en veillant à l'intégrité des accès comme des journaux d'événements. Le détail de son fonctionnement et de sa gouvernance fera toutefois l'objet d'une section spécifique du dossier.

8.3.2. Schéma fonctionnel

Le cycle fonctionnel d'un DPP débute avec l'attribution d'un identifiant de produit par GS1 pour le fabricant qui est le premier opérateur économique. Le fabricant sollicite un GTIN, qui devient la clé d'ancrage de son passeport numérique. Cet identifiant, normalisé et interopérable, est indispensable pour assurer la continuité avec les standards existants.

Une fois le GTIN obtenu, le fabricant doit créer son identité numérique dans l'écosystème du DPP. Cette étape s'effectue via le Portail européen (ou toute autre plateforme se connectant aux APIs blockchain), qui joue le rôle de point d'entrée institutionnel. Le fabricant y génère un identifiant décentralisé (DID), inscrit sur la blockchain sous la forme d'un smart contract dédié. Ce DID est associé aux identifiants officiels déjà reconnus dans le cadre européen (numéro de TVA, EUID, LEI, EORI), constituant ainsi une identité d'entreprise conforme au règlement eIDAS 2.0. Le dispositif fonctionne comme une procédure de Know Your Business (KYB), permettant de regrouper et de certifier les informations juridiques et administratives de chaque opérateur économique.

À partir de cette identité, le fabricant peut procéder à la création de son DPP toujours via le Portail. Cette opération déploie sur la blockchain un smart contract spécifique, le DPPContract. Ce dernier contient le GTIN et les informations minimales requises par la réglementation, qui peuvent être inscrites on-chain sous forme de métadonnées publiques

ou d'input data. Toutefois, pour des raisons de scalabilité et de protection des données, la majorité des informations détaillées sont gérées via des ResourceManifests.

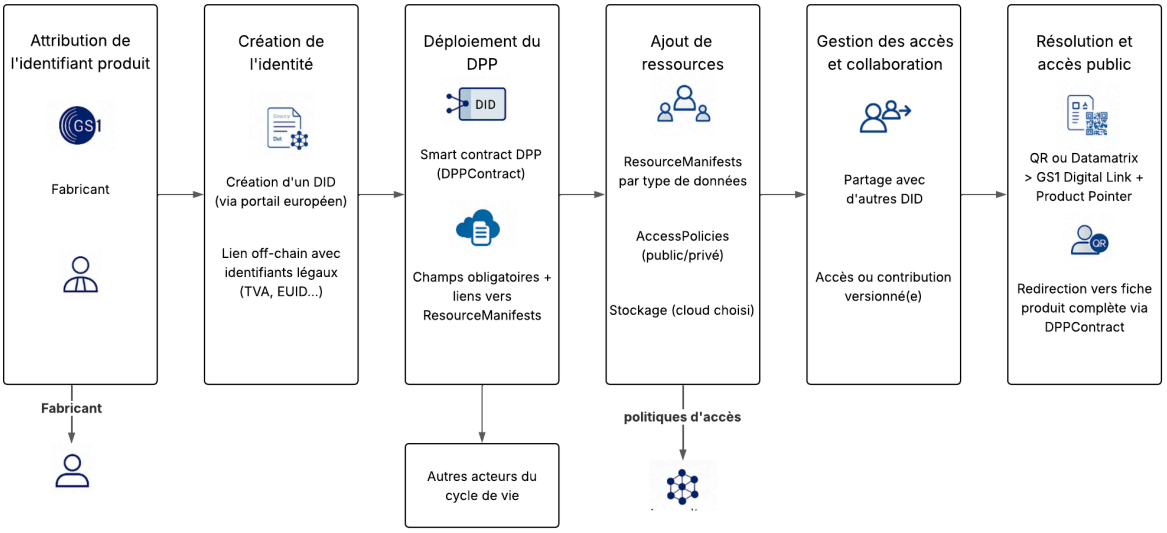
Les ResourceManifests sont créés et mis à jour via le Portail européen. Ils regroupent les données métiers du DPP et permettent de préciser, pour chaque ressource, si elle est publique ou privée. Les informations publiques incluent, par exemple, la composition, la réparabilité ou les performances environnementales. Les informations sensibles, telles que certains certificats de conformité ou des données de supply chain, peuvent être restreintes grâce à des politiques d'accès (AccessPolicies) définies par le fabricant ou par d'autres opérateurs impliqués. Ces politiques utilisent les DIDs et VC des acteurs pour attribuer ou limiter les droits d'accès.

Le stockage des ressources est laissé au choix de chaque opérateur. Par défaut, le Portail européen peut proposer une solution institutionnelle, garantissant neutralité et simplicité d'adoption. Néanmoins, les acteurs ont également la possibilité de recourir à des clouds centralisés ou à des solutions décentralisées, offrant une résilience accrue et une meilleure garantie d'immutabilité. Dans ce modèle hybride, chaque opérateur est responsable du choix et de la gestion de son système de stockage, tout en assurant l'intégrité des données par l'ancrage de hash sur la blockchain.

Une fois le DPP créé, les informations de base sont encodées dans le support AIDC afin de générer les codes barres à apposer sur les produits. Lors du scan du code, deux URI apparaissent. Le premier est le GS1 Digital Link, hébergé sur le domaine du fabricant, garantissant la compatibilité avec l'écosystème GS1. Le second est le ProductPointer, généré par le Portail européen, qui constitue l'URI persistante du DPP. Ce lien redirige vers la page officielle du DPP sur le Portail, laquelle interroge le DPPContract on-chain et restitue les ResourceManifests correspondants.

L'ensemble du dispositif garantit ainsi que chaque DPP est rattaché à une identité fiable (DID/VC), qu'il dispose d'un ancrage immuable (DPPContract), qu'il est enrichi de ressources versionnées, vérifiables et permissionnées (ResourceManifests), et qu'il reste accessible en toutes circonstances grâce au mécanisme de double URI (Digital Link GS1 et ProductPointer européen). Ce workflow assure la cohérence entre standards existants et innovation blockchain, tout en offrant la flexibilité nécessaire pour répondre aux contraintes et aux besoins des différents acteurs de la chaîne de valeur.

Voici un schéma permettant de visualiser le flux :



1. **Attribution de l'identifiant produit**
   Fabricant → obtient un GTIN auprès de GS1.

2. **Création de l'identité**
   Fabricant → se connecte au Portail européen → génération d'un DID (inscrit on-chain via un smart contract DID) → association via un JSON stocké off-chain aux identifiants légaux (TVA, EUID, LEI, EORI).

3. **Déploiement du DPP**
   Fabricant → crée un smart contract DPP (DPPContract) lié au GTIN.
   – Ce contrat contient les champs de base obligatoires par catégorie de produit (légaux et publics).

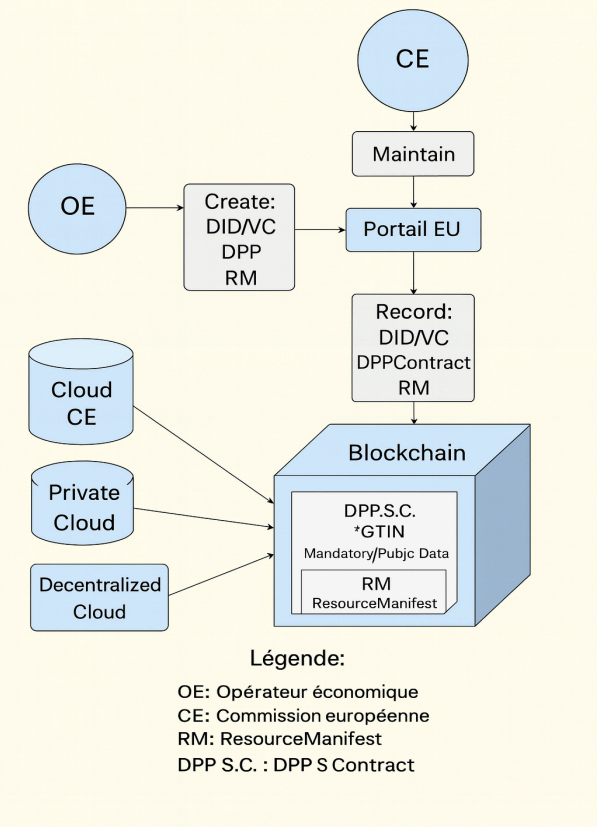
4. **Ajout de ressources**
   Fabricant (et autres acteurs du cycle de vie) → crée des ResourceManifests, chacun décrivant un ensemble de données (certificats, informations environnementales, notices techniques, etc.), et lie les documents qui seront stockés off-chain.
   – Définition des AccessPolicies (public ou privé, délégation d'accès à certains DID).
   – Stockage des données dans un environnement choisi (Commission, cloud centralisé, cloud décentralisé)

5. **Gestion des accès et collaborations**
   – Fabricant peut inviter d'autres DID à consulter ou enrichir certaines données.
   – D'autres opérateurs peuvent aussi solliciter l'accès en lecture et/ou écriture à des données reprises dans un ResourceManifest.
   – Chaque contribution est versionnée, horodatée et attribuée au DID de l'acteur.

6. **Résolution et accès public**
   – Dans l'AIDC (QR/DataMatrix), deux liens apparaissent :

• GS1 Digital Link (nom de domaine fabricant ou GS1)
• ProductPointer (Portail européen) → qui récupère les données du DPPContract.
– Le portail lit le DPPContract, récupère les ResourceManifests et affiche la fiche produit en fonction du niveau d'accès de l'utilisateur identifié.

Voici un schéma fonctionnel afin de compléter la compréhension du système :



8.3.3. Fonctionnalités du Portail européen

Le Portail européen constitue l'interface centrale et officielle du système DPP. Il joue un rôle pivot dans l'orchestration des différents composants (identité, registre on-chain, stockage off-chain et accès). Son objectif est de garantir une expérience utilisateur homogène tout en respectant les standards techniques et réglementaires définis au niveau européen.

Concrètement, il propose les fonctionnalités suivantes :

- **Création et gestion des comptes opérateurs économiques** : chaque acteur (fabricant, importateur, distributeur, recycleur, organisme notifié) s'enregistre sur le portail et procède à une vérification d'identité organisationnelle (Know Your Business, KYB). Cette procédure s'appuie sur des identifiants officiels (EORI, EUID, TVA, LEI) et

débouche sur la génération d'un DID (Decentralized Identifier) et de Verifiable Credentials (VCs) attestant du rôle.

- **Administration des produits et DPP** : le portail permet à un opérateur économique de déclarer de nouveaux produits (sur base d'un GTIN délivré par GS1), puis de créer leur DPP. Un même opérateur peut détenir plusieurs rôles selon le DPP considéré (par exemple fabricant pour un produit, importateur pour un autre, ou encore réparateur ou recycleur dans une autre chaîne de valeur). Le portail ne se limite pas à la création : il permet également d'enrichir des DPP existants en y ajoutant de nouveaux ResourceManifest. Ces enrichissements interviennent soit parce que l'opérateur a reçu un accès explicite (via une AccessPolicy), soit parce qu'il a sollicité l'accès à certaines sections d'un DPP.

- **Choix du mode de stockage** : au moment de la création ou de la mise à jour du DPP, l'opérateur sélectionne un mode d'hébergement pour ses données (cloud centralisé, cloud décentralisé ou solution institutionnelle). Le portail assure la configuration des liens vers les ResourceManifests et simplifie l'intégration, sans exiger une expertise technique poussée.

- **Gestion des accès et politiques de permission** : via des interfaces ergonomiques, l'opérateur définit les AccessPolicies associées à ses données. Il peut déclarer certaines informations comme publiques (accessibles à tous) ou restreindre leur consultation à des acteurs disposant de VCs spécifiques (par ex. autorités de surveillance, partenaires supply chain).

- **Génération du ProductPointer** : à chaque DPP correspond une URI persistante, le ProductPointer, créée et garantie par le portail. Elle est encodée dans le DataMatrix ou QR code aux côtés du GS1 Digital Link.

- **Ajout et mise à jour des ResourceManifests** : les opérateurs peuvent enrichir un DPP en ajoutant de nouveaux blocs (certificats de conformité, données environnementales, notices techniques). Chaque ajout est versionné, horodaté et référencé dans l'EventLog du smart contract.

- **Gestion des signalements et supervision** : le portail intègre un mécanisme de remontée d'anomalies (signalements par d'autres acteurs ou par des consommateurs). Ces signalements sont archivés et peuvent déclencher une procédure de modération ou de contrôle par les autorités compétentes.

Ces fonctionnalités font du portail européen non seulement une interface d'administration des DPP, mais également un instrument de conformité et de supervision, garantissant l'alignement avec le règlement ESPR et les standards techniques issus des travaux CIRPASS.

8.3.4. Portails régionaux ou sectoriels

En complément du Portail européen, des instances décentralisées peuvent être créées par les États membres, des regroupements sectoriels ou des entreprises spécialisées. Ces portails régionaux ou sectoriels s'appuient sur les API exposées par le protocole afin de récupérer les données, les filtrer et les mettre en forme selon des besoins spécifiques. Ainsi, chaque État membre pourrait disposer de son propre portail miroir, permettant d'adapter la restitution aux priorités nationales, tandis que des portails sectoriels offriraient une valorisation ciblée (par exemple pour le textile, la chimie ou la construction). Cette approche favorise à la fois l'interopérabilité et l'appropriation locale des données, tout en laissant à la Commission européenne le rôle de garant de l'intégrité et de la cohérence globale du système.

Dans ce cadre, la **Wallonie** pourrait développer un portail régional dédié, en miroir du Portail européen, interconnecté directement au protocole. Ce portail wallon remplirait plusieurs fonctions :

- proposer une interface localisée en lien avec les priorités régionales (économie circulaire, traçabilité, industrie 4.0) ;
- fournir des services adaptés aux PME wallonnes, comme des connecteurs simples vers leurs ERP ou outils de gestion, ou encore des formulaires no-code pour créer et enrichir des DPP sans expertise technique approfondie ;
- offrir une visibilité aux filières régionales (textiles techniques, batteries, chimie, bois, construction) en regroupant et valorisant les données pertinentes pour ces secteurs ;
- servir d'outil de support et de médiation, en relayant les informations réglementaires européennes et en accompagnant les entreprises dans leur mise en conformité.

Ainsi, le portail wallon constituerait une déclinaison locale du Portail européen, garantissant l'interopérabilité technique et sémantique tout en renforçant l'appropriation par les acteurs économiques de la région.

8.4. Plan de déploiement à l'échelle wallonne

Au jour d'aujourd'hui, le Portail européen et la solution présentée sont hypothétiques et n'existent encore que dans ce document. La Wallonie a donc l'opportunité de prendre une position de pionnier en mettant en œuvre un prototype régional de la solution proposée, sous la forme d'une sandbox. Ce portail wallon constituerait le premier démonstrateur opérationnel d'un DPP décentralisé, testé à l'échelle régionale mais pensé dès l'origine pour être fédératif et interopérable avec le futur dispositif européen.

Ce prototype pourrait remplir plusieurs fonctions clés en fonction du budget déployé :

- **Onboarding des entreprises :** permettre aux PME wallonnes de créer une identité numérique (DID/VC) et de l'associer à leurs identifiants légaux (TVA, EUID, LEI, EORI). Cette étape s'appuierait sur des processus de Know Your Business simplifiés pour abaisser la barrière d'entrée.

- **Création et gestion de DPP pilotes :** les fabricants pourraient, à partir de GTIN fournis par GS1 Belgium & Luxembourg, créer des DPP pour des produits réels. Ces DPP incluraient à la fois les informations réglementaires obligatoires et des enrichissements via des ResourceManifests, selon que les données sont publiques ou permissionnées.

- **Expérimentation des choix de stockage :** la sandbox offrirait plusieurs options de stockage (cloud régional, solutions décentralisées, hébergement institutionnel), permettant de tester la simplicité d'usage, les coûts et la robustesse en fonction des besoins des acteurs.

- **Gestion des accès et des rôles :** le portail wallon permettrait de simuler les différentes positions dans la chaîne de valeur (fabricant, importateur, distributeur, recycleur, autorité) et de tester en conditions réelles la définition des AccessPolicies et l'échange sélectif d'informations.

- **Interopérabilité et connecteurs :** la sandbox intégrerait des API ouvertes et des connecteurs simplifiés pour ERP, PLM ou MES utilisés par les PME. Les DPP créés respecteraient les standards GS1 Digital Link, JSON-LD et les ontologies CIRPASS, assurant une interopérabilité immédiate avec les autres initiatives européennes.

- **Valorisation sectorielle et régionale :** le portail offrirait des tableaux de bord et vues sectorielles adaptés aux filières stratégiques wallonnes (textiles techniques, batteries, chimie, construction, bois), facilitant l'exploitation des données par les entreprises, les fédérations et les autorités.

L'objectif de cette sandbox n'est pas simplement d'expérimenter, mais de placer stratégiquement la Wallonie au cœur de l'innovation européenne autour du DPP, en démontrant la faisabilité d'une solution unique et fédératrice. À terme, ce portail wallon pourrait évoluer vers un portail miroir interconnecté au futur Portail européen, mais avec l'avantage d'avoir servi de prototype de référence. Une telle démarche suppose évidemment une collaboration étroite et précoce avec les initiatives européennes existantes, notamment le projet CIRPASS, avec lequel la Wallonie est déjà en contact.

8.5. Perspectives économiques et compétitives

Le développement d'un prototype régional de DPP en Wallonie offre des perspectives économiques et compétitives considérables. Loin de se limiter à une réponse à la contrainte réglementaire, il peut devenir un catalyseur d'innovation et un levier de différenciation pour les filières industrielles régionales.

Renforcer la compétitivité des PME
Les PME wallonnes, qui constituent la majorité du tissu industriel, disposent rarement des ressources pour anticiper des réglementations complexes. En mettant à leur disposition une infrastructure prête à l'emploi, accompagnée de connecteurs simplifiés et d'outils *no-code*, la Région leur permet de se conformer aux futures obligations de l'ESPR tout en réduisant les coûts de mise en œuvre. Cette anticipation leur donnera un avantage compétitif par rapport à des concurrents d'autres régions européennes qui n'auront pas bénéficié d'un tel accompagnement.

Positionner la Wallonie comme territoire pilote
En développant une sandbox régionale opérationnelle, la Wallonie se positionne comme un territoire pilote au sein de l'Union européenne. Elle démontre sa capacité à expérimenter, à fédérer et à proposer une solution cohérente qui pourra être intégrée dans le futur Portail européen. Cette position renforce sa visibilité auprès des instances européennes et augmente les chances de capter des financements dédiés aux projets de standardisation et d'industrialisation du DPP.

Stimuler l'écosystème d'innovation locale
La mise en place du prototype nécessitera la mobilisation d'acteurs régionaux spécialisés en blockchain, en cloud, en sécurité et en standards GS1. Cela stimulera l'écosystème numérique wallon, créant des opportunités pour les start-ups, les centres de recherche et les prestataires technologiques. Les compétences acquises dans ce cadre pourront être exportées vers d'autres projets européens, positionnant la Wallonie comme un fournisseur de solutions et non uniquement comme un utilisateur.

Créer de nouvelles opportunités de marché
Le DPP ouvre la voie à des modèles économiques innovants : services de vérification de conformité, plateformes de reconditionnement et de recyclage, marchés secondaires basés sur la traçabilité des produits, valorisation des données environnementales dans le cadre de la finance durable. Les entreprises wallonnes qui adopteront tôt le DPP pourront exploiter ces opportunités et développer de nouveaux relais de croissance.

Accroître la souveraineté numérique et industrielle
En hébergeant un portail régional et en expérimentant avec des solutions de stockage hybrides (centralisé, décentralisé, institutionnel), la Wallonie s'assure de garder le contrôle sur ses données industrielles stratégiques. Elle limite ainsi sa dépendance à des

infrastructures étrangères et consolide sa souveraineté numérique, tout en contribuant à la résilience des chaînes de valeur européennes.

En résumé, la mise en place d'une sandbox DPP en Wallonie n'est pas seulement un projet de conformité réglementaire : c'est un projet stratégique qui renforce la compétitivité des PME, positionne la Région comme leader européen de l'innovation DPP, stimule son écosystème numérique et ouvre la voie à de nouveaux modèles économiques fondés sur la transparence, la circularité et la confiance numérique.

8.6. Conclusion et limites

La proposition de solution d'une architecture décentralisée pour le DPP, s'inscrit dans la continuité des travaux de CIRPASS tout en cherchant à dépasser certaines limites structurelles des modèles centralisés. En s'appuyant sur la blockchain pour l'indexation, la preuve et la gouvernance des accès, et sur un cloud distribué pour l'hébergement des données métiers, elle offre un cadre qui conjugue conformité aux standards européens, résilience technique, interopérabilité sémantique et responsabilisation des acteurs.

Cette vision permet de répondre à plusieurs enjeux clés identifiés par la Commission européenne : assurer la disponibilité et l'intégrité des données, prévenir la censure ou l'exclusion arbitraire, et renforcer la confiance grâce à l'immutabilité des contributions. En outre, elle ouvre des perspectives économiques nouvelles, en transformant le DPP d'une contrainte réglementaire en levier de compétitivité, en particulier pour les PME wallonnes qui pourraient bénéficier d'un portail régional pionnier.

Cependant, cette approche comporte également des limites et défis importants :

- **Complexité technique et coûts d'adoption** : l'implémentation d'une solution décentralisée suppose des compétences en blockchain, en sécurité cryptographique et en gestion du stockage distribué, qui ne sont pas encore largement répandues dans les PME. Des interfaces simplifiées et un accompagnement seront indispensables pour garantir l'adhésion.

- **Acceptabilité institutionnelle** : la mise en œuvre d'un registre de confiance distribué suppose un accord sur la gouvernance multi-parties, incluant Commission européenne, États membres, industriels et organismes tiers. L'acceptation d'un modèle partiellement décentralisé pourrait susciter des résistances de la part d'acteurs habitués à des architectures plus centralisées.

- **Interopérabilité internationale** : si le modèle est aligné avec GS1 et les ontologies CIRPASS, il reste à garantir sa compatibilité avec des cadres réglementaires et techniques extérieurs à l'Union européenne (par exemple aux États-Unis ou en Asie).

Le risque de fragmentation normative n'est pas totalement écarté.

- **Questions de souveraineté et de confiance dans les infrastructures** : si des solutions décentralisées sont privilégiées, il conviendra de s'assurer qu'elles reposent sur des opérateurs et des réseaux compatibles avec les objectifs de souveraineté numérique européenne. Le choix des infrastructures (blockchain, stockage, identités) doit éviter toute dépendance critique à des acteurs non européens.

- **Équilibre entre transparence et confidentialité** : le DPP doit fournir un haut niveau de transparence pour les consommateurs et les autorités, tout en protégeant des données industrielles sensibles. Le bon calibrage des AccessPolicies, entre ouverture et restriction, sera un défi central pour éviter à la fois la sur-exposition et l'opacité.

- **Trajectoire d'évolution** : cette proposition est aujourd'hui hypothétique et doit encore être testée dans des environnements réels. Le développement d'une sandbox régionale en Wallonie constitue une première étape pragmatique, mais la montée en puissance à l'échelle européenne nécessitera des ajustements techniques, réglementaires et organisationnels.

En définitive, cette solution ne se présente pas comme une alternative exclusive au modèle CIRPASS, mais comme une extension fédératrice qui anticipe les besoins de résilience, de transparence et de confiance numérique. Elle positionne la Wallonie comme un territoire d'expérimentation privilégié, capable d'apporter une contribution déterminante à l'élaboration de la future infrastructure européenne du DPP.

9. Conclusion générale, limites et recommandations

La mise en œuvre du Digital Product Passport (DPP) dans le cadre du règlement ESPR constitue une étape majeure pour la transformation durable de l'industrie européenne. En plaçant la traçabilité et la transparence au cœur du cycle de vie des produits, le DPP permet d'assurer une documentation complète et vérifiable, de la fabrication jusqu'à la fin de vie, tout en soutenant les objectifs de circularité et de durabilité définis par la Commission européenne. Les expérimentations menées en Wallonie, dans le cadre du programme DigitalWallonia4Trust, ont fourni un terrain concret pour tester les processus, identifier les verrous techniques et organisationnels, et valider les standards d'interopérabilité requis pour une adoption à l'échelle européenne.

L'un des enseignements majeurs de cette étude réside dans la valeur stratégique apportée par la blockchain. En tant qu'infrastructure décentralisée, elle garantit l'immuabilité des

journaux d'événements, la traçabilité certifiée des cycles de vie, ainsi que la gestion sécurisée des identifiants (DID, VC). Couplée aux standards européens tels que GTIN, URI, JSON-LD ou eIDAS, elle offre une interopérabilité native et un niveau élevé de confiance pour tous les acteurs. Les ResourceManifests modulaires et l'utilisation de smart contracts permettent d'automatiser certaines validations, tout en conservant une gouvernance distribuée. Cette approche renforce la crédibilité du DPP et offre un cadre technique robuste pour la coordination entre industriels, autorités publiques et consommateurs, tout en anticipant les évolutions réglementaires et technologiques.

Recommandations

Pour maximiser l'efficacité et l'acceptation du DPP, il est recommandé de déployer une architecture hybride et fédérée, combinant stockage off-chain, registres blockchain et portails d'accès sécurisés. La gouvernance de cette infrastructure doit être partagée entre industriels, pouvoirs publics et experts techniques, et prévoir un mécanisme de validation collective pour toute modification du protocole. Une approche de type DAO (Decentralized Autonomous Organization) permettrait ainsi de concilier la sécurité, la transparence et la flexibilité, tout en assurant la capacité du système à évoluer avec les besoins des utilisateurs et les innovations technologiques. La modularité et l'ouverture de la solution favorisent également l'intégration progressive des PME et des plateformes régionales, garantissant une adoption progressive à l'échelle européenne.

Limites

Malgré ses avantages, la blockchain présente certaines limites. Son immuabilité peut restreindre l'adaptabilité des systèmes si aucun mécanisme de gouvernance n'est prévu pour les évolutions futures. La complexité technique de la mise en œuvre et la nécessité de synchroniser l'ensemble des parties prenantes peuvent ralentir le déploiement opérationnel. En outre, la dépendance à des standards spécifiques, bien que nécessaire pour l'interopérabilité, impose un cadre contraignant qui doit être anticipé et géré. L'usage complémentaire du référentiel CIRPASS, combiné à la blockchain, permet d'atténuer certains de ces risques en offrant un socle solide tout en introduisant des mécanismes d'évolution graduelle.

Enfin, cette approche démontre que le DPP peut constituer un accélérateur d'écosystèmes vertueux et un levier stratégique pour la compétitivité industrielle européenne. Chaque produit peut ainsi être documenté, accessible et vérifiable tout au long de son cycle de vie, dans un langage commun et standardisé. En combinant innovation technologique, adoption des standards européens et gouvernance distribuée, l'Europe dispose d'un socle solide pour déployer un DPP efficace, évolutif et durable, au service des industriels, des autorités et des consommateurs.

En cohérence avec les ambitions régionales et industrielles, la Wallonie pourrait constituer le cadre idéal pour expérimenter cette solution dans un projet pilote interopérable, réunissant les écosystèmes publics, industriels et technologiques. Il revient désormais à l'ensemble des

acteurs concernés de concrétiser cette promesse européenne, en assurant la coordination et la mise en œuvre des standards et mécanismes définis.

10. Bibliographie

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

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

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

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

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

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

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

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

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

CIRPASS Consortium. D5.1 Digital Product Passport Prototypes, 2024. Disponible sur : 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. Disponible sur : https://doi.org/10.5281/zenodo.10925636

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

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

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

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

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

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

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

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

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

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

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

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

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

Madaster. Material Passport resources (consulté 2025). Disponible sur : https://www.madaster.com

Spherity. Battery Passport SSI resources (consulté 2025). Disponible sur : https://spherity.com

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

Narravero. Product Passport SaaS (consulté 2025). Disponible sur : https://narravero.com

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

Aura Blockchain Consortium. Official materials (consulté 2025). Disponible sur : https://aurablockchain.com

TrusTrace. DPP Playbook and resources (consulté 2025). Disponible sur : https://trustrace.com

whatt.io. Product Passport Solutions (consulté 2025). Disponible sur : https://www.whatt.io

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

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

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

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

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

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

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

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

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

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

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