



Digital Product Passport

A no-nonsense discussion on the blockchain-based perspectives

Ilaria Lunesu; Lodovica Marchesi; Andrea Pinna; **Roberto Tonelli; Andrea Vitaletti**



More questions than answers

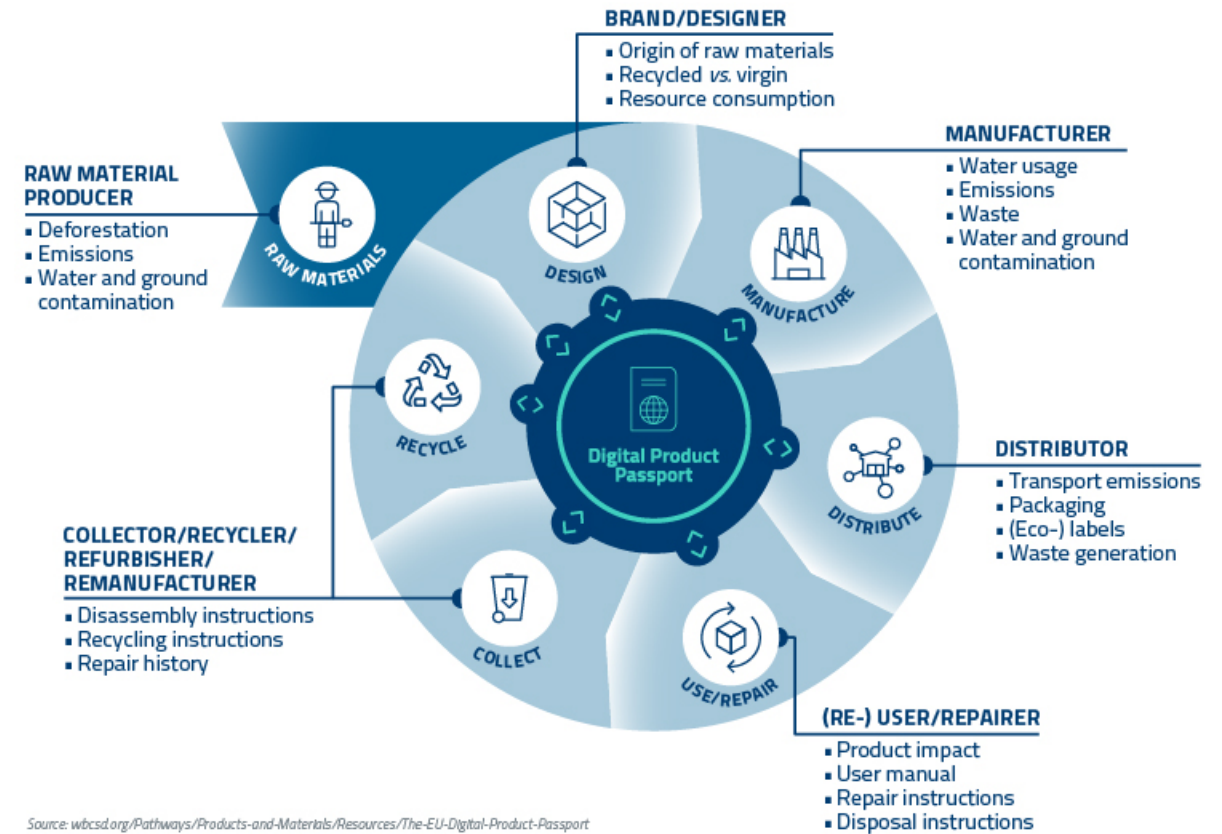
... and this is only a limited number of relevant questions!

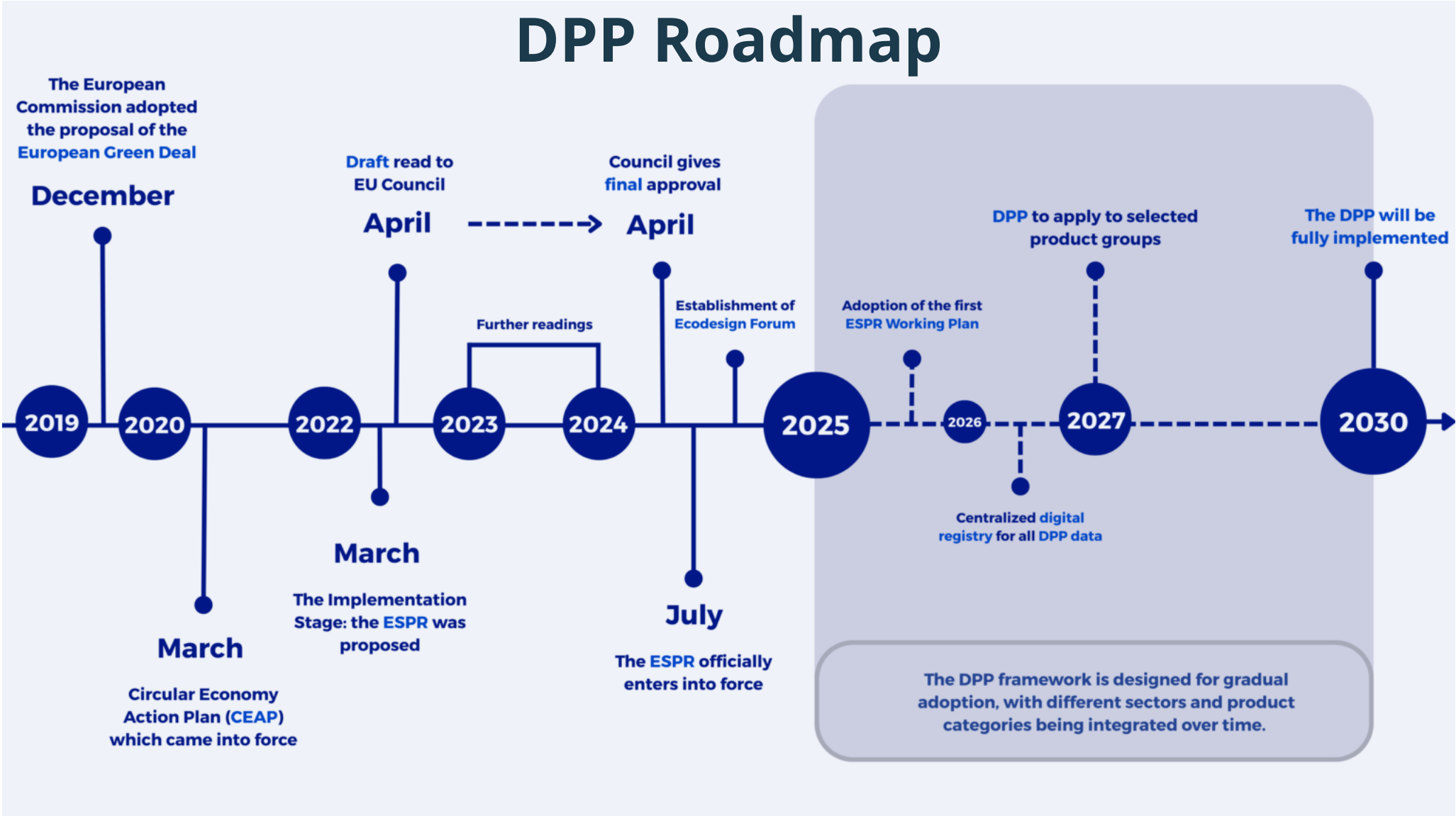
Ecodesign for Sustainable Products Regulation (ESPR)



Digital Product Passport

It is a comprehensive standard (e.g. [GS1 Arch](#), [GS1 GSCN](#)) digital record that tracks a product's lifecycle, materials, origin, and environmental footprint to promote a circular, sustainable economy.







The opportunity

Target Industry / Milestone	Key Timeline & Focus
Batteries	Operational starting February 2027 for industrial and EV batteries under separate battery rules.
Priority Sectors	First wave includes Iron, Steel, Textiles, Apparel, Aluminium, and Furniture (Adoptions spanning 2026–2028).
Secondary Wave	Expected rollout for Tyres, Mattresses, and Electronics by 2027–2029.
Universal Mandate	By 2030, the DPP framework is expected to cover nearly all regulated consumer and industrial goods.



The Blockchain Hypothesis

Proponents claim blockchain is the *only* solution to:

1. Ensure **immutable** historical tracking across a fragmented, global supply chain: changing one entry means breaking the entire chain
2. Establish a **decentralized** trust layer where no single firm or nation controls the data: DPP accessible throughout the product's life (tens of years). No company can guarantee its own database will survive that long.
3. Automatically execute compliance rules via **smart contracts**.



Memento

Blockchain ensures data **integrity**, not data **quality**

If the input data is forged, the blockchain simply records a lie in an immutable, permanent way.



Issue #1: The Physical-Digital Linkage Problem

- **Vulnerabilities of Physical Tags:** e.g. QR Code Copying / destruction
- **The "Garbage In, Garbage Out" (GIGO) Dilemma**
 - Ledgers are digital, products are physical.
 - Cryptographic signatures guarantee *who* wrote the data, not that the *physical reality* matches the entry.

True in all digital solutions



Issue #2: Privacy, Confidentiality, and Trade Secrets

- **The Transparency Paradox**
 - Regulators/consumers demand complete transparency of supply chains.
- **Layered information**
 - Public, Authority, Private
- **Commercial Threats:**
 - Competitors can reverse-engineer manufacturing processes. Public shipping transaction logs reveal supplier pricing, production volumes, and margins.

The Cryptographic Overhead

Using **Zero-Knowledge Proofs (ZKPs)** to hide data while proving compliance is computationally intensive, increases latency, and complicates key management.



Issue #3: Scalability, Latency, and Financial Costs

- **Transaction Volumes & Network Capacity**

- EU markets process **billions** of new physical items each year: tracking every transit, repair, component swap, and recycling event demands high-throughput.
- **Public Blockchains (e.g., Ethereum L1/L2):** Fees are unpredictable and prohibitively high especially for low cost items
- **Private Consortiums:** High throughput and low fees, but are they just centralized databases managed by a cartel of large corporations?



Economic Viability

If the cost of maintaining the digital history exceeds the residual value of the materials being recycled, the circular economy model collapses.



Issue #4: Governance, Standards, and Walled Silos

- **Fragmentation into Silos of Trust**

- There will never be a single, global "DPP Blockchain". Recyclers handling complex e-waste must integrate with dozens of different ledger networks and data schemas.
- Automotive ([Catena-X](#)), Luxury ([Aura](#)), and Tech ([Global Battery Alliance](#) and [Circularise](#)) run separate, incompatible networks.

- **Interoperability still challenging:**

- Cross-chain bridging are prone to hacks (e.g. smart contract vulnerabilities, multi-signature threshold etc.).

- **Centralized Cartels:**

- Private consortia validators might be controlled by market leaders.



Issue #5: GDPR vs. Blockchain Immutability

- **GDPR Article 17:** The "Right to be Forgotten" mandates the erasure of personal data on request. Also right to rectification (Article 16).
 - Who is the data controller?
 - International data transfer
 - National authorities like France's CNIL have long warned that hashes and public keys often remain personal data
- **How Personal Data Leaks Into the Passport:**
 - Ownership transfers of premium goods (e.g., e-bikes, luxury watches) identify buyers.
 - Repair and maintenance logs contain the names, licenses, and locations of technicians.



European Data Protection Board (EDPB's 2025 guidelines)

ANNEX A – RECOMMENDATIONS

Recommendation 1. Architecture – Documentation

108. The EDPB recommends to controller and processors to document:
- Will the data on the blockchain contain personal data?
 - If so, why is a blockchain a necessary and proportionate means for this processing? (i.e. What is the rationale for this choice? What were the eventual alternatives?)
 - What type of blockchain should be used? (i.e. Is a private blockchain sufficient? Can a permissioned blockchain be used? Is a “zero-knowledge” architecture possible?)
 - What technical and organisational measures are used? (i.e. Will personal data be stored off-chain? Which privacy-preserving technologies are used?)

Recommendation 2. Architecture – Off-chain storage

109. The EDPB recommends controllers to store any additional personal data off-chain, beyond the identifiers already present on-chain in transaction metadata, to mitigate data protection risks.

Recommendation 3. Information

110. Data controllers must inform data subjects in clear terms on the rationale of the processing, the existence of their rights and the modalities to exercise them. Suitable times to provide such information are when a data subject is about to commit data to the blockchain and on creation of the blockchain itself. The information should also be available for data subjects to find at other times, e.g. on the controller's website.

Recommendation 4. Minimisation



DPP as a Collection of DIDs + VCs [Garcia et al. 2024]

- DIDs → provide globally unique, resolvable identifiers for products and actors
- VCs → encode certified claims about the product with cryptographic provenance
- Blockchain → anchors DID documents and VC schemas (immutability, auditability)
- Off-chain storage → holds the actual VC payloads (GDPR compliance, data minimization)
- With DIDs, VCs and Verifiable Presentations VPs, persons and companies may easily control which of their own information is presented to others and when and how this is done
- This maps very naturally onto ESPR's requirements.



Paradigm Comparison

Criteria	Centralized Database (EU Registry)	Consortium Blockchain	Public Blockchain (L2)	DIDs + VCs (Decentralized PKI)
Trust Model	Trust in government	Trust in "industry" cartel (IBSI/EBSI)	Math + Miner/Validator set	Cryptographic peer-to- peer
Data Privacy	High (controlled access)	Medium (leaks to rivals)	Extremely low (public)	Excellent (off-chain)
Write Cost	Negligible	Low	High & Unstable	Low
Scalability	High	Medium	Low	High
GIGO Security	Checked at input	Checked by consortium	Unchecked	Checked by peer-to-peer audit



Thank You!

Let's Open the Critical Discussion

@ vitaletti@diag.uniroma1.it

<https://www.diag.uniroma1.it/vitaletti/>