EU Blockchain
Observatory and Forum

Digital Product Passports: A Blockchain-based Perspective

About this report

This is the fourth of a series of reports that will be published addressing selected topics following European Commission priorities. The aim is to reflect on the latest trends and developments and discuss the future of blockchain in Europe and globally.

This report has been produced by the EU Blockchain Observatory and Forum team. Any mistakes, omissions, or oversights are solely the authors' responsibility.

The EU Blockchain Observatory and Forum team:

- Dr Ioannis Vlachos, Tonia Damvakeraki (Netcompany – Intrasoft)

The EUBOF team would like to extend its gratitude for their interviews to

Mesbah Sabur – founder and CEO of Circularise

Douglas Johnson-Poensgen – CEO of Circulor

Carsten Stöcker – founder and CEO of Spherity

Leandro Nunes – chief revenue officer of nChain

Laura Kajtazi – project and regulatory affairs manager at IOTA Foundation, and

Andrea D'Intino, from DYNE.

We are thankful for the review and feedback from our Expert Panel members:

- Luca Boldrin (Infocert),
- Jim Mason (Sybal),
- Donal O'Regan (Fujitsu)
- Daniel Szego (EU Blockchain Observatory& Forum Expert), and
- Koen Vingerhoets (Fujitsu).

Note

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this report.

Disclaimer

Digital Product Passports: A Blockchain-based Perspective

Table of Contents

Table of Abbreviations

Abbreviation	Explanation
DPP	Digital product passport
ESPR	Ecodesign for Sustainable Products Regulation
CO2	Carbon dioxide
CEAP	Circular Economy Action Plan
NFT	Non-fungible token
EBSI	European Blockchain Services Infrastructure
ODI	Organisation digital identity
SDLC	Secure software development life cycle
SSI	Self-sovereign identity
VC	Verifiable credentials
DID	Decentralised identifier
API	Application programming interface
MPC	Multi-party computation
IoT	Internet of things
AI	Artificial intelligence
ESG	Environmental, social and governance
NIST	National Institute for Standards and Technology
PoW	Proof of work
eIDAS	Electronic identification and trust services for electronic transactions in the internal market

Chapter 1: Digital Product Passports and Related Regulations

1.1 Introduction to the Digital Product Passport[1]

The European Digital Product Passport Regulation (DPP) is a component of the European Union's broader endeavours to foster sustainability and propel the objectives of the European Green Deal. Embedded within the Ecodesign for Sustainable Products Regulation (ESPR), it aims to facilitate a 55% reduction in CO_2 emissions by 2030 compared to 1990 levels. Additionally, it aspires for Europe to become the first climate-neutral continent by 2050.

The digital product passport serves as distributed, decentralised network of interoperable platforms, each platform being crafted to the needs of its community of users and sector, intended to offer consumers and businesses enhanced transparency and insights into the environmental and sustainability features of products available in the EU market. It aims to promote the adoption of more sustainable practices in product lifecycle management, facilitating improved repairability and recycling for all products distributed within the EU. The digital product passport initiative is part of the Ecodesign for Sustainable Products Regulation (ESPR, 2022) and one of the key actions under the EU's Circular Economy Action Plan (CEAP, 2020). Similarly, the EU Batteries Regulation, also under the CEAP, is driving the initiative for digital battery passports, like digital product passports. DPP for the first product groups is expected to come into effect in 2027, which does not leave long for businesses to prepare.[2,3]

The Digital Product Passport (DPP) is key to the EU's transition to a circular economy and will provide information about products' environmental sustainability. It aims to improve traceability and transparency along the entire value chain of a product and to improve the management and sharing of product-related data that are critical to ensuring their sustainable use, prolonged life, and circularity.

DPPs will be mandatory for all product categories subject to the delegated acts specified in the Ecodesign for Sustainable Products Regulation (ESPR).

The current section provides an overview of the concept of the digital product passport, as well as its objectives, benefits, and potential implications and challenges (especially concerning the circular economy).

1.1.2 Aims & objectives of the EU Digital Product Passport

This concept aims to create a comprehensive digital representation or passport system that can track every detail about any single product's lifecycle. The DPP concept, as established by the EU, is an inclusive programme that does not just cover electronic devices but also software or online services – providing in-depth knowledge about their environmental and social impact on users. It aims to inspire sustainability across industries by educating everybody who plays a role regarding these products.

The key objectives of the EU DPP, underlying its role in promoting sustainability and circularity in the digital sector are listed below.

1. **Enhancing transparency:** The DPP provides the means to consumers and businesses to have access to product data related to its environmental performance, including carbon footprint, resource usage, and

[1] CIRPASS (2023). Source
[2] Ecodesign Directive (2022). Source
[3] Circular Economy Action Plan (2020). Source

recyclability. Therefore, DPPs provide the required transparency about a product to enable buyers to make informed decisions, as well as incentivise the development of greener digital products.

2. **Facilitating circularity:** The DPP promotes a circular economy by documenting the lifecycle of a product from start to end. At the same time, it encourages product repair, reuse, and recycling. This is achieved by providing transparent and detailed information on product durability, availability of spare parts, and recycling options. This shift towards a circular model results in the reduction of waste and promotes resource efficiency.

3. **Ensuring data security and privacy:** The DPP also promotes cybersecurity and facilitates data protection, thus ensuring that digital products comply with EU standards and regulations. In turn, cybersecurity and data security strengthen consumer trust in the digital economy and protect sensitive information throughout a product's lifecycle.

1.1.3 Benefits of the EU Digital Product Passport

There are several benefits from the use of the EU DPP for various stakeholders:

Consumer empowerment: The DPP empowers consumers to make environmentally conscious choices by providing them with clear and reliable information. Consumers can compare products based on their sustainability credentials, encouraging companies to adopt greener practices.

Business competitiveness: By encouraging sustainable design, production, and disposal practices, the DPP drives innovation and competitiveness among businesses. Companies that prioritise sustainability will gain a competitive advantage, meeting the growing demand for environmentally friendly products.

Environmental protection: The passport aims to reduce the environmental impact of digital products by promoting resource efficiency, waste reduction, and the adoption of eco-friendly materials. This leads to a more sustainable use of resources and a significant reduction in electronic waste.

Policy alignment and harmonisation: The EU DPP supports the EU's broader policy objectives, including the European Green Deal and the Circular Economy Action Plan. It fosters harmonisation across member states, establishing a common framework for sustainable digital product development and regulation.

1.1.4 Potential Implications and Challenges

While the EU DPP is a promising solution, it also raises certain implications and challenges that must be addressed:

1. **Standardisation and interoperability:** Achieving standardised and interoperable digital product passports across a wide range of industries and Member States poses a considerable challenge. Cooperation among stakeholders, including industry players, policymakers, and technology experts, is crucial to ensure seamless implementation.

2. **Data management and privacy:** Collecting, managing, and sharing data across the entire lifecycle of digital products necessitates robust data management systems. Protecting consumer privacy and ensuring data security will be essential considerations in implementing the passport.

3. **International collaboration:** To maximise the effectiveness of the passport, international collaboration and alignment with global standards are vital. Engaging with international partners and harmonising efforts will facilitate the adoption of the passport beyond EU borders.

Although the implementation of the DPP requirement across European Union countries has not yet been enacted, it is expected to happen soon, facilitated by the approval of the proposal for Ecodesign for Sustainable Product Regulation by the European Commission in March 2022. Currently, the EU is planning the implementation of product passports in three industries by 2026: apparel, batteries, construction products, and consumer electronics. In the following sub-sections, we investigate the existing EU strategies for these industries.

1.1.1 EU Strategy for Sustainable and Circular Textiles[4]

The EU Strategy for Sustainable and Circular Textiles represents a comprehensive and forward-thinking approach to transforming the textile industry into a sustainable and circular sector. Recognising the environmental and social challenges associated with textile production and consumption, this strategy sets out a roadmap for fostering sustainable practices, promoting resource efficiency, and ensuring the responsible management of textiles throughout their lifecycle. This overview will delve into the key objectives, strategies, and potential impacts of the EU Strategy for Sustainable and Circular Textiles.

The EU Strategy for Sustainable and Circular Textiles and digital product passports are interrelated and complementary tools that can accelerate the transition to a sustainable textile industry. Digital product passports, as comprehensive digital records, provide transparent and traceable information about the environmental and social aspects of textile products throughout their lifecycle. By integrating digital product passports into the EU Strategy for Sustainable and Circular Textiles, policymakers can enhance the traceability and transparency of textile supply chains, enabling consumers and businesses to make informed choices based on reliable data. Digital product passports can provide real-time information on a product's sustainability credentials, including its materials, production processes, and end-of-life options. This integration can support the implementation of the strategy by facilitating sustainable sourcing, promoting circular business models, and empowering consumers to engage in sustainable and circular textile practices. The combination of the EU Strategy for Sustainable and Circular Textiles and digital product passports provide a comprehensive approach to transforming the textile industry by promoting transparency, accountability, and sustainable consumption.

1.1.2 EU Battery Regulation[5]

The EU Battery Regulation represents a crucial policy initiative aimed at addressing the environmental and social challenges associated with batteries and their use. As the demand for batteries grows rapidly, driven by the increasing use of electric vehicles and renewable energy storage, the regulation sets out to ensure the sustainable and responsible production, use, and end-of-life management of batteries within the European Union. This overview will delve into the key objectives, principles, implementation strategies, and potential impacts of the EU Battery Regulation.

The EU Battery Regulation and digital product passports are closely related and mutually supportive tools that can enhance the sustainability and traceability of batteries within the European Union. The EU Battery Regulation is a piece of legislation proposed by the European Commission to ensure that batteries marketed in the EU meet the highest sustainability standards. It aims to improve the environmental performance of batteries throughout their entire life cycle, from design to end-of-life. The regulation covers aspects like the

[4] EU Strategy for sustainable and circular textiles (2022). Source

[5] EU Battery Regulation (2023). Source

use of recycled materials in batteries, carbon footprint, performance, and durability requirements, and the end-of-life handling of batteries to promote recycling and reduce waste. Digital product passports are part of the EU's broader initiative to foster a circular economy. A digital product passport is essentially a digital record containing information about a product's characteristics, origin, composition, repair and dismantling possibilities, and handling at the end of life.

The concept of a digital product passport is not limited to batteries but is applicable to various products to enhance product sustainability, traceability, and circularity. Digital product passports provide a comprehensive digital record of a battery's lifecycle, capturing crucial information about its design, materials, energy efficiency, and end-of-life management.

Integrating digital product passports into the EU Battery Regulation can strengthen its effectiveness by facilitating the monitoring, enforcement, and transparency of battery-related requirements. By leveraging digital technologies, digital product passports can enable (depending on how quickly or automated it is) real-time tracking of a battery's environmental performance, allowing manufacturers and authorities to monitor compliance with sustainability standards. Additionally, digital product passports provide consumers with valuable information, empowering them to make informed decisions by considering a battery's sustainability attributes. This integration promotes a circular economy by supporting the traceability and recycling of batteries, fostering responsible sourcing, and advancing the development of innovative and sustainable battery technologies. The combination of the EU Battery Regulation and digital product passports establishes a comprehensive framework for promoting sustainability, circularity, and transparency in the battery sector.

1.1.3 EC Recommendation on improving the rate of return of used and wasted mobile phones, tablets, and laptops[6]

On 6 October, the EC issued a recommendation to EU Member States for improving and incentivising the return of used and wasted mobile phones, tablets, laptops, and their chargers. This recommendation aims to support national authorities to ensure maximum collection rates and subsequent re-use, repair, refurbishment, and recovery of these small electronic devices.

The rate of small electronic device collection within the EU remains low. For instance, the collection rate for mobile phones is reported to be below 5%, with an estimated stock of 700 million unused and discarded mobile phones stored in households across the EU.

These devices contain valuable materials, particularly critical raw materials. A single smartphone contains rare earths in the magnet, cobalt in the battery, indium in the screen, and tantalum, gallium, and precious metals in the printed circuit board.

Boosting the repair, reuse, and recycling of small electronics will facilitate the transition to a circular economy, bolster the security of critical raw materials and energy supply, and enhance the EU's strategic autonomy.

The recommendation focuses on:

> **Providing financial incentives** such as discounts, vouchers, deposit-return schemes, or monetary rewards. These incentives should target small consumer electronics that are no longer functional but are still retained in households, as well as functional electronics that people no longer use but can be

[6] EC recommendation on improving the rate of return of used and waste mobile phones, tablets and laptops (2023). Source

resold, reused, or repaired. Consumers should be empowered to make informed decisions, including the ability to assess the value of a device.

Increasing the use of postal services for returning used and discarded mobile phones, tablets, and laptops. This can be achieved by offering pre-paid envelopes or labels to consumers for returning their devices.

Facilitating partnerships between reuse organisations and take-back scheme operators, along with setting targets for reuse and preparation for reuse.

Enhancing awareness and improving the accessibility and visibility of collection points for small electronics. Information regarding nearby take-back points can be integrated into user-friendly maps, search tools, and applications. At these collection points, individuals should also be informed about the proper management and deletion of personal data stored on their devices.

1.2 Main Principles and Requirements for DPPs

Digital product passports have emerged as increasingly vital in our digital era, offering critical insights into a product's journey, circularity and reusability, regulatory compliance, environmental footprint, etc. While precise criteria and guidelines can vary, contingent on the context and industry, there are several **key principles** and **prerequisites** to developing authentic digital product passports.

The push for establishing **universal standards** is critical to ensuring DPPs' effectiveness on a global scale. By achieving worldwide acceptance and standardisation, it fosters a unified approach, facilitating seamless data exchange among various stakeholders. This harmonisation is not only about interoperability but also about elevating DPPs to a globally recognised and used tool, highlighting the need for a cohesive framework endorsed by international standardisation bodies. (Standardisation)

For DPPs to truly serve their purpose, they must encapsulate comprehensive product information, spanning the entirety of a product's lifecycle—from raw material sourcing to disposal or recycling. This level of detail encompasses the product's design, materials, manufacturing processes, and performance characteristics, providing a full spectrum of data. (Comprehensive Product Information)

Moreover, these passports should detail the ecological impact, energy consumption, and emissions throughout the product's life, leveraging standardised methodologies like life cycle assessment (LCA) for accurate and meaningful data. This lifecycle data is invaluable in promoting transparency and informed decision-making. (Lifecycle Data)

Traceability is another cornerstone of DPPs, enabling the tracking of materials and components to verify a product's provenance and authenticity. This traceability is essential in combatting counterfeiting and enhancing supply chain visibility. (Traceability)

Interoperability is also paramount, ensuring DPPs can be easily integrated into existing digital infrastructures across various domains, from supply chain management to e-commerce and regulatory compliance systems. This facilitates a broader adoption and use of DPPs across industries. (Interoperability)

Data security and privacy must be maintained, with stringent protocols to protect sensitive information while adhering to data privacy regulations. Access and editability to certain data should be restricted to authorised entities, ensuring consistency, confidentiality, and compliance. (Data Security & Privacy)

User experience is crucial; DPPs should be designed with intuitive interfaces, incorporating visual aids and user-friendly formats to aid understanding and accessibility for all users, including those with disabilities. This inclusivity extends to complying with web accessibility standards, making DPPs universally accessible. (User Friendliness & Accessibility)

Real-time updates are essential for maintaining the accuracy of DPPs, reflecting any changes in materials or manufacturing processes. This dynamic nature of DPPs ensures their relevance throughout the product's lifecycle. (Real-Time-Updates)

Incorporating environmental and sustainability metrics within DPPs empowers stakeholders to make choices on the basis of environmental considerations, aligning with global efforts towards sustainability. On blockchain, these metrics can be calculated in a trustless fashion, i.e., with the use of smart contracts, making the data immutable. (Environmental & Sustainability Metrics)

Ensuring DPPs are in harmony with existing and emerging regulatory requirements and standards, such as those set by the European Union, is essential for legal compliance and market accessibility. Furthermore, DPPs should be adaptable to various international markets and regulatory frameworks, enhancing global trade and providing consumers worldwide with access to comprehensive product data. (Regulatory Compliance & International Compatibility)

Educational initiatives are crucial in helping consumers navigate and leverage DPPs for informed decision-making, while stakeholder collaboration across the spectrum of manufacturers, suppliers, and regulatory bodies ensures a well-rounded and effective implementation of DPPs. (Consumer Education & Stakeholder Collaboration)

Lastly, scalability is vital as the adoption of DPPs grows, ensuring the system can accommodate an increasing array of products and information. (Scalability)

Embracing these principles and requirements will reinforce the role of digital product passports as indispensable tools for promoting product authenticity, environmental sustainability, and informed decision-making.

Chapter 2: From Theory to Practice

Below we present an overview of national and European-funded projects leveraging blockchain technology for applying DPP in different industries.

2.1 TRACE4EU

2.1.1 Sector targeted & objectives

Trace4EU aims to create an umbrella architecture based on existing EBSI services. The architecture builds the basis for the implementation of traceability application scenarios. The pilot will be aligned with the EU Digital Wallet and related qualified trust services. Furthermore, by including organisational digital identity (ODI), TRACE4EU ensures that the pilot evaluates scenarios that are relevant to citizens, businesses, and governments such as secure e-commerce and business-to-business transactions.

The project is focused on the traceability of products to ensure the **trustworthy proof of origin of European products** e.g. seafood, agrifood, halloumi, and batteries (seafood and agrifood sector and batteries). It is worth noting here that the EU DPP excludes food products from its scope.

Additionally, TRACE4EU will develop and test solutions for the secure traceability of transactions and documents to make processes in decentralised ecosystems evident to 3rd parties, including their long-term preservation. This traceability addresses the tracking requirements of physical products, documents, and data but also product owners on trusted business-to-business interactions. This process includes the physical (pre-) products and materials that will be shipped and further processed in factories or manufacturing plants as well as the arrival of products to consumers. The traceability of the involved data and documents ensures the non-repudiation of digital transactions as well as secure data sharing cross-border.

As a result, TRACE4EU will provide technical pilots to fulfil the requirements on burden of proof and cybersecurity in decentralised ecosystems using EBSI.

TRACE4EU promotes recommendations for developing the EBSI ecosystem through engagement with pan-European stakeholders and has the potential to significantly influence traditional industries, assisting them in becoming more efficient, productive, competitive, and resilient. Upcoming traceability implementations will also improve transparency in the European area for citizens, who will be able to track commodities and documents more effectively and proactively.

One issue for consideration is the accessibility of non-EU actors and value chains.

2.1.2 How blockchain technology is used

TRACE4EU uses blockchain technology to create an umbrella architecture based on existing European Blockchain Services Infrastructure (EBSI) services. This architecture forms the foundation for implementing traceability application scenarios.

More specifically, for this project, blockchain is used to maintain a secure, transparent, and immutable record of the product's journey from production to the end consumer. By leveraging blockchain, Trace4EU can provide

verifiable traceability that is resistant to fraud and manipulation, enhancing consumer trust in the products' origins and sustainability.

Furthermore, the project also develops solutions for the secure traceability of transactions and documents. This is critical for making processes in decentralised ecosystems evident against third parties, including their long-term preservation. Blockchain's immutable ledger ensures that all transactions and related documents are securely recorded, providing non-repudiation of digital transactions and secure data sharing across borders.

TRACE4EU includes the concept of ODI to ensure that the pilot evaluates scenarios relevant to various stakeholders. This involves the use of blockchain for managing digital identities, making it possible to authenticate the entities involved in the product lifecycle securely. The blockchain-based ODI facilitates trust in business-to-business interactions by verifying the identity of the product owners and the authenticity of the products and transactions.

2.1.3 Strong Points

The pilot project is aligned with the EU Digital Wallet and related qualified trust services. This alignment signifies that TRACE4EU evaluates scenarios that are relevant not only to businesses and governments but also to citizens, such as secure e-commerce and business-to-business transactions. The integration with the EU Digital Wallet indicates a broader application of blockchain technology, extending the benefits of secure and transparent transactions to a wider range of societal and economic activities.

TRACE4EU promotes recommendations for developing the EBSI ecosystem through engagement with pan-European stakeholders. This engagement aims to assist traditional industries in becoming more efficient, productive, competitive, and resilient. The use of blockchain technology in this context is not just about enhancing traceability and security but also about improving transparency in the European area, enabling citizens to track commodities and documents more effectively and proactively.

2.2 BATTERY PASS[7]

2.2.1 Sector targeted & objectives

The digital battery passport will be a core tool in enabling the sustainable scaling of **battery value chains** globally. While decarbonisation and dematerialisation are overarching goals of the European Green Deal, more ambitious action from both business and politics is required. The battery passport is a lighthouse example of using innovation to achieve these goals, support legal implementation, and empower companies to make informed decisions on their supply chains and products. A group of partners from industry, science, and beyond (including the German Federal Ministry for Economic Affairs and Climate Action) recognised the opportunity to form Battery Pass, a consortium of leading experts to jointly advance the implementation of the battery passport based on requirements of the emerging EU battery regulation and beyond. By setting the necessary foundations and bringing together different stakeholders and initiatives, Battery Pass aims to contribute to this

[7] Battery Pass (thebatterypass.eu)

complex challenge, which starts with batteries but will go far beyond as a first step towards the broader implementation of digital product passports in the future.

The European Battery Passport aims to develop timely (due to burdensome and incoming requirements for batteries) and holistic guidance on all relevant aspects of the battery passport as mandated by the EU Battery Regulation and beyond, by balancing sustainability objectives against industry feasibility. Furthermore, it is expected that existing battery passport initiatives will join forces, to ensure compatibility and symbiotic scaling as well as exchange and aligning with all major ecosystem participants to achieve maximum impact through commonly accepted multi-stakeholder views. Engagement with stakeholders and key players beyond the EU is going to support the process.

2.2.2 How blockchain technology is used

The battery passport platform relies heavily on multi-party private permissioned blockchain technology. Unlike public blockchains, which are open to anyone, private permissioned blockchains limit access to a specific group of participants, ensuring the security and privacy of data. Within the battery passport context, the blockchain functions as a secure, transparent, and unchangeable ledger for monitoring the origin and lifecycle of battery materials.

Here's an overview of how it operates.

Participants: Essential stakeholders within the battery supply chain are granted entry to the private permissioned blockchain. These stakeholders encompass miners, processors, manufacturers, recyclers, and others. Each participant possesses a distinct identifier and role within the network.

Data Recording: Participants input pertinent data onto the blockchain, including details regarding the origin, processing, manufacturing, and recycling of battery materials. Each data entry is time-stamped and linked to the preceding entry, establishing a secure and traceable record.

Data Validation: The platform employs a consensus mechanism to validate the accuracy and authenticity of the data. This ensures that only verified and precise information is appended to the blockchain.

Traceability: Through interconnected data entries, the blockchain constructs an immutable and transparent record of the battery's origin and lifecycle. Authorised participants can access this information to confirm the responsible sourcing and management of battery materials.

2.2.3 Strong Points

Sustainable batteries are a key element for environmentally, socially, and climate-friendly electromobility. With the digital battery pass, we are getting a big step closer to this goal. Important data, such as the climate footprint or information on the conditions of raw material extraction, repairability, and recyclability, will be securely stored in it and exchanged between the economic actors along the battery value chain – from raw material extraction to reuse and recycling. This creates transparency around the electric car battery.

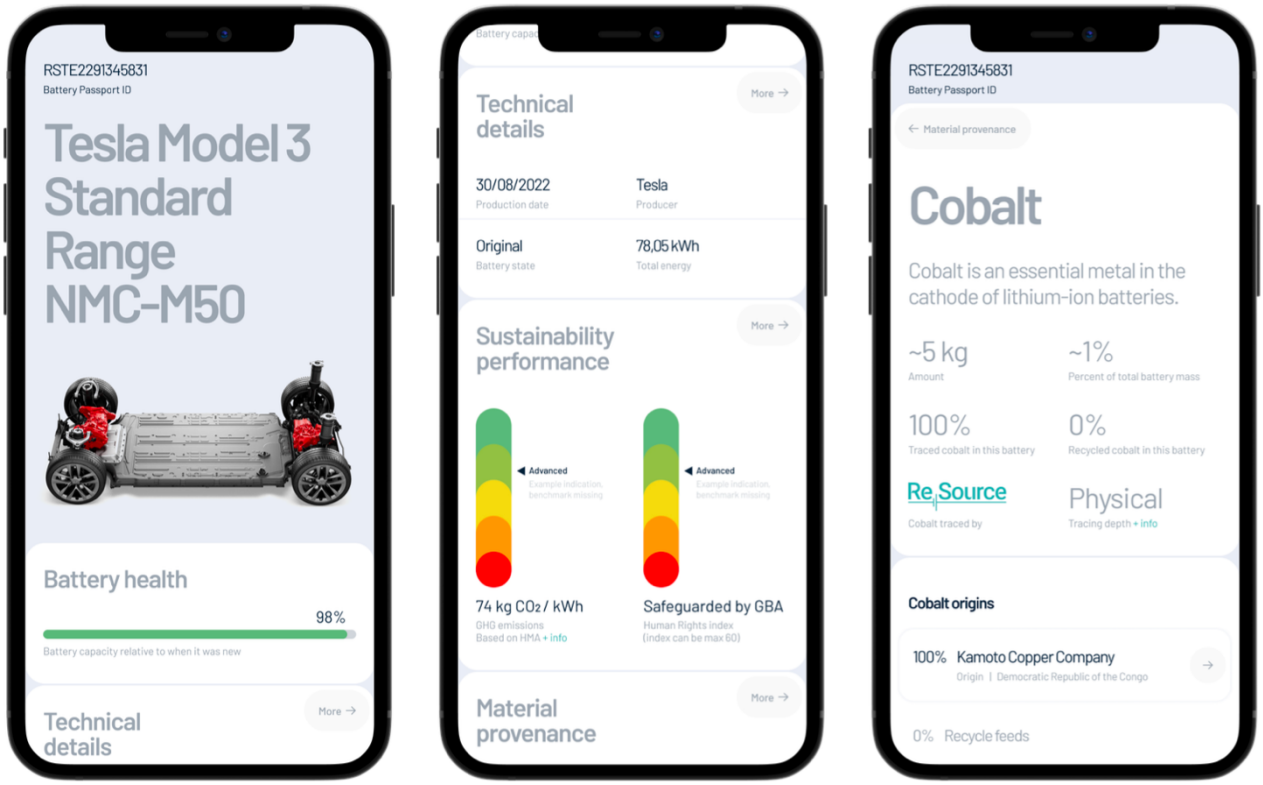
Data-enabled lifecycle management of vehicle batteries is central to strengthening the effectiveness of the EU battery and automotive industry. It will not only accelerate the scaling of the number of electric vehicles but will also ensure a productive and environmentally sound use of valuable vehicle traction batteries. This will help

EU nations and companies to achieve their climate targets, generate high-quality jobs, and reduce import dependencies.

2.3 RE|SOURCE[8]

2.3.1 Sector targeted and objectives

Re|Source is the initiative of a consortium of multiple industry players, which means there is no single authority that has control. This is particularly important, since ReSource needs sensitive data – like production yields or human rights scores – about the companies for the platform to work, while many of those companies are competitors. Entrusting that sensitive information to a single entity could 'break the industry' and be an impediment for companies to use Re|Source.



2.3.2 How blockchain technology is used

Blockchain enables decentralisation by ensuring that no single entity has access to all information. Instead, companies run their node and can keep their information on-premises, without it being shared or accessible to anyone else. Re|Source performs calculations with that sensitive information and only shares the necessary

[8] https://resource-platform.eu/

outcomes of those calculations, without sharing the underlying data itself. This approach ensures that sensitive information is safeguarded while still allowing for collaboration and the necessary transparency in the supply chain.

Electrification of mobility plays an essential role in the transition to clean energy. The demand for electric vehicle EV batteries has skyrocketed over the past few years and will only continue to increase. However, this growth comes at a price. There are about eight different metals in a standard lithium-ion battery, like cobalt, nickel, and lithium. Unfortunately, some of those metals are sourced from mines that operate under bad social conditions, and mining them is not sustainable for the environment. The supply chains of those metals are complex and can have similar issues.[9]

Re|Source will be a platform for the EV industry to provide physical tracking of battery metals and manage sustainability risks in battery supply chains. It will provide proof of provenance and sustainability performance of battery metals in compliance with both regulatory and commercial requirements. It will be developed by a founding consortium of CMOC, the Eurasian Resources Group, and Glencore 116 in partnership with blockchain solutions expert Kryha and industry leaders such as the Cobalt Institute, the Responsible Minerals Initiative, Tesla, and Umicore.

Re|Source's provenance and sustainability insights can be used by a battery manufacturer to issue a digital product passport for a specific battery, which is required for upcoming regulatory compliance. Earlier this year, Re|Source issued such a battery passport for the very first time, in collaboration with the Global Battery Alliance and a consortium of supply chain partners. Using blockchain technology as a basis for a platform like Re|Source and issuing battery passports has four main advantages: decentralisation, accountability, confidentiality, and verifiability.

One crucial aspect of digital product passports for EV batteries is the product's material provenance and the material processors involved. Only when this information is known can the passport's necessary supply chain due diligence be conducted, and details like a product's carbon footprint be calculated. To hold supply chain actors accountable, it is critical to be able to prove this provenance of material.

2.3.3 Strong Points

The material provenance information in the battery passport can be accounted for using Re|Source's **blockchain-based traceability solution**. It creates a digital twin of each unit of physical material in the form of a non-fungible token (NFT) issued on the blockchain. Using NFTs makes these physical units noninterchangeable with each other, as they are unique to their origin (providing proof of provenance). These NFTs take the same route as the physical material, following each step throughout the supply chain. This journey is captured in the NFT, which allows downstream battery producers who ultimately own these NFTs to prove the provenance of the material in their batteries. This mechanism ensures accountability and verifiable proof of provenance.[10]

Re|Source needs lots of data from the companies that use the platform to issue battery passports that are compliant with future regulations. These data can be commercially sensitive and contain trade secrets. They are not something companies like sharing, especially since many of those companies are competitors, too.

[9] Supply Due Diligence is a major topic, looking at human rights including labour and environmental rights e.g. Corporate Sustainability Due Diligence Directive, Source

[10] It is important to stress here, that this might be a problem in terms of 1) the fact that according to the Battery Regulation, a battery passport must be identifiable by a QR code (not an NFT); and 2) it is not certain that these forms of identifiers be interoperable with other types of DPPs.

Also, any information stored on the blockchain is publicly available. To lower the barrier for these companies to share truthful data, Re|Source uses a combination of confidentiality-preserving solutions. First, the data Re|Source stores on-chain never hold actual information, only auditable zero-knowledge proofs that link to data off-chain. Second, companies can use Re|Source's disclosure settings to decide what data they would like to share with whom. If needed for the passport, Re|Source can still derive certain necessary information from undisclosed data through zero-knowledge proof mechanisms.

These data confidentiality solutions do not prevent untruthful data from being uploaded to Re|Source, but using blockchain does allow auditing or verifying the data by third parties. Blockchain is an immutable record of what happened when, where, and by whom. The ability to verify data retroactively is important, since it allows companies to be held accountable, which in return reduces the risk of untruthful data entering the system.

All material provenance data and sustainability performance data in the Re|Source battery passport can be verified and traced back to its origin through the underlying blockchain technology. This makes these battery passports more reliable and valuable to both the end consumer and the organisation issuing them.

Blockchain technology offers numerous benefits for the implementation and issuance of product passports for EV batteries. With these advantages, the Re|Source battery passport is poised to change the way the supply chain of EV batteries is tracked and managed, paving the way for a cleaner, more sustainable future.[11]

[11] Ensuring interoperability with other battery passports as well as with passports from other sectors (e.g. construction products), is critical.

Chapter 3: Blockchain and DPPs

This section presents the way DPPs and blockchain could play major roles in creating a more sustainable future. It involves interviews with industry executives describing the way blockchain technology supports the objectives of DPP.

3.1 Introduction

A digital product passport (DPP) is a concept used to provide comprehensive and immutable[12] information about a product throughout its life cycle from manufacturing to disposal. Blockchain technology can be a valuable tool in the implementation of DPPs due to its key features such as decentralisation, transparency, security, and immutability. Blockchain technology can work seamlessly for digital product passports, and it offers several benefits.

Blockchain is a distributed ledger technology, which means there is no central authority and no single point of control. Each network participant (node) keeps a copy of the entire ledger. For a DPP, this means that information about a product can be stored and updated across a network of participants (manufacturers, suppliers, distributors, consumers, regulators) without relying on a central entity, making it resistant to censorship and single points of failure. (Decentralisation and Disintermediation)

All transactions and data recorded on a blockchain are visible to all participants in the network. This transparency builds trust among stakeholders as they can independently verify the authenticity and history of a product. Consumers can access information about the product's origin, manufacturing processes, materials used, and environmental impact, increasing their confidence in the product. (Transparency and Trust)

Once the data is stored on the blockchain, it is very difficult to change or delete it. This immutability ensures that the information stored in the DPP is tamper-proof and can be trusted for product certification and compliance. This is particularly valuable for maintaining accurate product history, including certifications, recalls, and durability information. (Persistence)

Blockchain uses cryptographic techniques to protect data and transactions. This ensures that data can only be accessed and updated by authorised participants. This security feature is crucial to protect sensitive product data, especially in industries with strict regulatory requirements, such as pharmaceuticals or food. (Security)

The technology enables the creation of a transparent and verifiable chain of origin for products. Each stage of the product and its life cycle can be recorded, and this information can be easily traced back to the source. In the event of a product recall or quality issue, blockchain helps identify problematic products quickly and efficiently. (Traceability)

The key advantages of using blockchain for digital product passports, therefore, include **improved transparency**, **less fraud**, **improved compliance**, **sustainability**, **supply chain efficiency**, and **consumer empowerment**.

Blockchain technology provides a clear and verifiable record of product and travel information, making it easier for consumers to make informed choices based on the origin, sustainability, and authenticity of a product (improved transparency).

[12] Immutability is not a pre-requisite for the EU DPP; there are concerns regarding static vs dynamic data, due to the complexity of the supply chain sector.

Blockchain security measures reduce the risk of counterfeiting or fraud in the supply chain and protect both consumers and producers. For industries that need to abide by regulatory requirements, blockchain-based DPPs can streamline compliance processes and provide regulators with real-time access to information (decreased cases of fraud and improved compliance).

Blockchain can track the environmental impact of products, help consumers make more sustainable choices, and encourage manufacturers to improve their environmental friendliness (sustainability).

The transparency and traceability provided by blockchain can improve supply chain efficiency by reducing errors, delays, and disputes while consumers gain more control over their choices, by having detailed product information, which can increase demand for products that align with their values (supply chain efficiency & consumer empowerment).

Blockchain technology can enhance the concept of digital product passports by providing secure, transparent, and immutable information about a product and its life cycle. This technology can benefit consumers, manufacturers, regulators, and the environment by increasing trust, reducing fraud, and improving supply chain efficiency.

On the other hand, there are also some challenges and limitations that need to be tackled for the successful implementation and operation of the system, concerning scalability, privacy and security, compatibility with international standards, compliance with the regulatory framework, interoperability, stakeholder collaboration, etc.

Blockchain networks, especially those that use proof-of-work (PoW) consensus mechanisms, can face scalability issues, leading to slower transaction times and higher costs. This can be a significant barrier when trying to track large numbers of products in real time, potentially limiting the practicality of DPPs for widespread use.

Ensuring the privacy and security of sensitive data within a DPP is very important, especially given the immutable nature of blockchain. Balancing transparency and privacy are challenging, as stakeholders demand confidentiality for certain data while regulatory and operational needs require transparency.

Different blockchains and DPP platforms may have incompatible standards and technologies, hindering the seamless exchange of data. Without interoperability, the potential of DPPs to streamline global supply chains and product lifecycle management could be significantly reduced.

Navigating the complex and evolving regulatory landscape related to digital identities, data privacy, and blockchain technology can be challenging. Compliance is essential for widespread adoption, requiring DPP solutions to be flexible and adaptable to meet global and local regulatory standards.

Achieving widespread adoption of DPPs requires buy-in from all stakeholders in the product lifecycle, including manufacturers, suppliers, regulators, and consumers. Overcoming inertia and the status quo necessitates demonstrating clear benefits, ease of integration, and interoperability with existing systems.

Developing, deploying, and managing blockchain-based DPPs involves significant technical complexity and potential cost implications. There needs to be a clear return on investment for businesses to undertake the initial costs and ongoing management of such systems.

The value of a DPP is highly dependent on the accuracy and integrity of the data it contains. Ensuring that only verified and accurate data is entered into the blockchain is crucial. Incorrect or fraudulent data can

undermine the trust and utility of the entire DPP system, necessitating robust mechanisms for data verification and validation.

Addressing these challenges requires a multi-faceted approach, involving technological innovation, regulatory engagement, stakeholder collaboration, and ongoing education and advocacy. Successfully overcoming these obstacles can unlock the full potential of blockchain-based digital product passports, paving the way for more transparent, efficient, and sustainable product lifecycles.

3.1.1 How can a DPP be implemented on Blockchain

Implementing a digital product passport on the blockchain requires careful consideration of the trade-offs between different approaches to **tokenisation**, **data storage**, and **trust** enhancement. A hybrid approach that combines the strengths of various methodologies may offer the most balanced solution, ensuring that the DPP is both practical and robust. Adopting standards for interoperability and ensuring compliance with regulatory requirements are also crucial for the success and adoption of DPPs on the blockchain. An overview is presented in the table below.

Digital product Passport Representation	
Approach	
Tokenisation: Tokenising a product involves creating a digital representation of the product or its attributes on the blockchain. This could be achieved using non-fungible tokens (NFTs) for unique items or fungible tokens for parts or materials that are not unique but are part of the product's lifecycle.	**Advantages:** Provides a clear immutable record of product ownership and product history Facilitates the transfer and tracking of products in a secure manner
	Disadvantages: • Scalability issues could arise with blockchain platforms, impacting transaction speed and costs. • Environmental concerns due to the energy consumption of certain blockchain networks.
Verifiable Credentials allow secure and verifiable sharing of attributes or qualifications of a product. This method leverages decentralised identifiers (DIDs) to ensure the authenticity and integrity of the data shared.	**Advantages:** • Enhances privacy by allowing selective disclosure of informatic • Reduces the risk of counterfeit products through secure verification mechanisms.

	Disadvantages: • Complexity in implementation and management of credentials • Dependency on the wider adoption of DIDs and verifiable credential standards		
Storage Solutions			
Fully on-chain storage: storing all data directly on the blockchain ensures data immutability and transparency.	**Advantages:** • High data integrity and security. • Easier to implement smart contracts that interact with the data.		
	Disadvantages: • High costs for data storage on the blockchain. • Scalability issues due to the size of the blockchain.		
Hybrid Storage: Combining on-chain storage for critical data with decentralised storage solutions (e.g. IPFS, Filecoin) for larger datasets.	**Advantages:** • Cost-effective storage solution. • Maintains the benefits of on-chain storage for critical data points while leveraging efficient off-chain storage for bulk data.		
	Disadvantages: • Increased complexity in managing data across different storage solutions. • Potential latency in accessing off-chain stored data.		
Enhancing Trustworthiness			
Single point of trust: Registering data to the blockchain inherently involves trust in the entity that inputs the data. To mitigate this, several techniques can be employed →	**Multiple Reviewers:** Using a consortium or multi-signature approach, where multiple parties must verify the accuracy of the data before it is added to the blockchain.	**Oracles:** Employing oracles to fetch and verify data from external sources. This helps ensure data relevance and accuracy.	**Decentralised Oracles:** Further decentralising the process by using a network of oracles to reduce the risk of manipulation or error in data fetching and verification.

In the following sections, we present a few DPP use cases, deployed by various organisations.

3.2 Circularise

Circularise is a supply chain traceability software scale-up that provides a platform for companies to create and manage digital product passports (DPPs). DPPs are a digital record of a product's lifecycle, including information about its materials, sustainability impact, and ownership.

Circularise uses blockchain technology to secure and verify the data in DPPs. This makes DPPs tamper-proof and ensures that the information they contain is accurate and reliable. Circularise is committed to using a decentralised approach to DPPs. This means that the data in DPPs is not owned or controlled by any single party, which helps to build trust and transparency in the supply chain. They are also working on using other decentralised technologies, such as NFTs, DIDs, and VCs, to enhance the functionality of DPPs. These technologies could be used to improve traceability, authentication, and data sharing.

Some of the key challenges identified in the process of the adoption of DPPs include:

- There is limited understanding of the technology.
- There are no clear regulatory requirements for DPPs.
- Connecting DPP systems to make them interoperable is difficult.

The best practice approach for implementing a DPP according to Circularise includes a clear definition of the goals of each DPP implementation, alignment with other members of the value chain on data sharing, ensuring internal systems readiness, and development of clear business cases for DPPs. Furthermore, it is essential to manage expectations of return on investment (ROI) of DPPs as well as fast adaptation to changes to maintain innovation potential.

The full interview with Mesbah Sabur – Founder and CEO of Circularise is available in the Appendix.

3.3 Circulor

Circulor is a technology company that specialises in supply chain traceability and sustainability. Circulor uses blockchain technology to create DPPs (digital product passports), which are tamper-proof records of a product's journey from raw materials to end-of-life.

There are several benefits to using decentralised architecture for DPPs, including improved data integrity, increased security, enhanced transparency, improved resilience, reduced dependency, and increased performance.

The main technological and regulatory barriers to the application of blockchain technology for DPPs include scalability, interoperability, data standardisation, and the lack of a regulatory framework.

The use of NFTs (non-fungible tokens), DIDs (decentralised identifiers), VCs (verifiable credentials), and other decentralised technologies for the implementation of DPPs has the potential to provide significant benefits but also comes with some challenges.

Key lessons learned from following a blockchain-based approach for DPPs include the importance of collaboration, standardisation, regulatory compliance, and education.

Best practices for implementing a DPP include defining clear objectives, involving all stakeholders, ensuring data accuracy and integrity, addressing privacy and security concerns, using appropriate technology, and testing and iterating.

The full interview with Douglas Johnson-Poensgen – CEO of Circulor is available in the Appendix.

3.4 Spherity

Spherity is a company that aims to address various compliance challenges in the modern world, including health, fraud, and environmental issues. The focus is on creating digital product passports (DPPs) using blockchain technology and decentralised principles to enhance transparency, trust, and compliance.

Spherity aims to revolutionise compliance by providing a digital backbone for scalable and automated business transactions. They focus on establishing provenance and authorisation chains to automate compliance at the individual transaction level.

The company employs advanced cybersecurity features, adhering to NIST zero trust architecture, Gaia-X design principles, and the US National Cybersecurity Strategy to protect API endpoints from malicious actors. Spherity has successfully launched its first supply chain security product, CARO, in the US pharma market, partnering with industry leaders like AstraZeneca, Bristol Myers Squibb, Johnson & Johnson, Novartis, and Sandoz. The company is also uniquely positioned in Europe with enterprise and object identity wallets focused on developing secure, compliant, and interoperable digital product passport (DPP) solutions to meet emerging EU regulations in various industries.

Spherity uses blockchain technology to address the challenges of creating DPPs, emphasising transparency, security, and data placement. They use blockchain for public data while preserving confidentiality for sensitive information.

The advantages of decentralised architecture for DPPs include enhanced security, tamper-proof registries, off-chain provenance and authorisation chains, increased trust, compliance controls, decentralised look-up for business confidentiality, and more.

There are several barriers to implementing DPPs, including the need for ecosystem development, education, business case support, standardisation, adoption roadmap, trust framework, and project timelines.

DIDs and VCs are seen as crucial for DPPs, providing secure identity management and verifiable assertions. They enable trust, compliance, interoperability, and enhanced security within the ecosystem. Attribute-based access control (ABAC) is recommended to enhance cybersecurity, particularly for API endpoints. It provides fine-grained access control, reducing the risk of unauthorised access. VCs and authorisation mechanisms help automate compliance with laws and regulations, reducing manual work in compliance departments. AI-driven dynamic risk scoring is suggested for DPP claims, allowing businesses to assess the trustworthiness of product claims based on credentials and non-conformance events.

NFTs are discouraged for DPP applications due to potential conflicts with business confidentiality requirements and lack of standardisation for regulatory and compliance use cases.

User managed access (UMA) is mentioned as a framework for secure data sharing, but challenges related to centralised access policy configuration are highlighted. Blockchain technology may assist in improving UMA solutions.

Confidential computing, especially multi-party computation (MPC), is recommended for privacy-preserving data sharing. It allows multiple parties to compute over encrypted data while maintaining privacy and security.

Overall, Spherity's approach involves leveraging blockchain, DIDs, VCs, and other decentralised technologies to enhance compliance, security, and trust in digital product passports, while also acknowledging existing challenges and emerging solutions in the field.

The full interview with Carsten Stöcker – Founder and CEO is available in the Appendix.

3.5 nChain

nChain is a company founded in 2015 with a focus on making blockchain technology accessible to individuals, businesses, and governments. They describe themselves as the 'DNA of blockchain' and emphasise the efficient exchange of value.

nChain leverages blockchain technology to address the challenges of creating digital product passports (DPPs). DPPs involve multiple parties in a supply chain sharing data, and blockchain eliminates the need for direct trust between parties by providing a neutral, immutable infrastructure for data sharing. It simplifies the data-sharing process, enhances efficiency, and eliminates intermediaries.

Decentralized architecture is favoured for DPPs because it allows for secure, efficient, and trusted data sharing across an ecosystem of organisations. It complements centralized systems by enabling them to connect to the ecosystem for improved data sharing.

Challenges faced include the complexity of selecting the right blockchain solutions, the need for standards to ensure interoperability, supportability, and consistency, and the integration of various technologies like IoT and AI. Education and regulation surrounding blockchain use are also crucial.

NFTs, DIDs, and VCs, have various advantages, including accountability, compliance with labour regulations, verifiability, inclusion, user control, privacy, and confidentiality. Combining them effectively can enhance the DPP ecosystem.

Blockchain-based DPPs require **cooperation between ecosystem participants**, strong governance models, common standards, and business commitment. Each supply chain is unique, and technology solutions need to be flexible. Success depends on an ecosystem willing to bring about change.

Best practice examples include use cases that buy in from key stakeholders and have a common goal. They address common pain points, ensure specific value delivery to each party, and consider regulatory compliance as an accelerator. Finally, they tailor solutions to the unique needs of the industry and build a common infrastructure for data sharing.

For example, the SeafoodChain by Unisot, is a blockchain-based solution that addresses the needs of different stakeholders in the seafood supply chain, ensuring global traceability and compliance with industry standards.

The full interview of Leandro Nunes – Chief Revenue Officer is available in the Appendix.

3.6 IOTA

IOTA is an open, feeless, scalable data and value distributed ledger technology (DLT)-based transfer protocol. It aims to overcome the limitations of traditional blockchains like Bitcoin and provide a scalable and sustainable DLT for applications and digital economies.

IOTA's core technology is the Tangle, a directed acyclic graph functioning as a consensus algorithm. Users must confirm previous transactions to complete their own IOTA transactions. Currently, the IOTA network is managed by coordinator nodes operated by the IOTA Foundation. These nodes determine which transactions and data are included in the ledger. Currently, IOTA is working on the Coordicide project (IOTA 2.0) to remove the need for coordinators and achieve full decentralisation.

Stardust is an infrastructure layer for smart contract chains and multi-asset ledgers. Shimmer is a network deployed to test Stardust's features before its implementation on the IOTA mainnet.

DPPs collect information about a product throughout its life cycle. IOTA's Tangle can ensure the auditability and immutability of DPP data in a decentralised environment. IOTA's DPP implementation includes DIDs and VCs for identity management and data integrity. These components enable authorised and competent entities to contribute to the DPP. NFTs can be used for ownership-based access management in DPPs, but they may pose data privacy challenges. Tokenisation, combined with IOTA smart contracts, can incentivise sustainable behaviour.

Decentralisation enhances trust, security, and reliability in DPPs by eliminating central authorities and single points of failure. Standardisation, interoperability, and uncertain regulation are barriers to implementing blockchain technology for DPPs.

IOTA has developed a decentralised blueprint for digital product passports in collaboration with Digimarc. It also created a digital product passport for consumer electronics in partnership with the Technical University of Catalonia. Phase 2B involves further development and testing, including the involvement of real economic operators.

IOTA aims to continue its work on the European Blockchain Pre-Commercial Procurement in Phase 2B, focusing on field testing, real-world stakeholders, and integration with the European Blockchain Services Infrastructure (EBSI).

The full interview with Laura Kajtazi – Project and Regulatory Affairs Manager is available in the Appendix.

3.7 Chromaway

ChromaWay is one of the five contractors participating in Phase 2A of the European Blockchain Pre-Commercial Procurement initiative. Currently, ChromaWay is engaged in the development and demonstration of the Relational Blockchain Nebula (RBN), showcasing its potential to facilitate widespread blockchain adoption within the European Union.

Blockchain technology is recognised for its indispensable role in enabling transparent and secure tracking, particularly in environments where data integrity is paramount. In the context of a circular textile economy, a multitude of stakeholders with diverse interests exists:

- Designers prioritise the verification of material integrity for production.
- Regulators aim to ensure compliance with production standards.
- Consumers demand authenticity verification and a transparent product history.
- Recycling facilities necessitate accurate information regarding textile content.
- Manufacturers aspire to standardise competitor practices and obtain precise raw material data.

Acknowledging these varied interests, a neutral and transparent data source is advantageous for all parties involved. By leveraging multiple block producers and allowing node verification, data accuracy is ensured. Nevertheless, traditional blockchain limitations, such as high transaction costs and computational requirements, impede widespread adoption.

ChromaWay's relational blockchain nebula (RBN) addresses these challenges through innovative consensus mechanisms and a hybrid database blockchain architecture.

Digital product passports (DPP), powered by ChromaWay's relational blockchain nebula, encapsulate comprehensive product lifecycle information within the blockchain.

1. Production: Upon successful quality control, garments receive a DPP entry denoted as 'PRODUCED', outlining production specifics.
2. Shipment to retailer: Garments attain 'SHIPPED' status upon transfer to retail or warehousing, with subsequent entries such as 'DISPATCHED TO CUSTOMER'.
3. Retail handling: Upon receipt at inventory, garments are marked as 'RECEIVED BY RETAILER', facilitating flaw detection and potential recycling or return to the factory.
4. Consumer usage: Garments labelled as 'SOLD' upon purchase may be returned, incentivising recycling through tokens redeemable for discounts.
5. Recycling phase: Garments deemed unsuitable for reuse receive 'RECYCLED', 'UPCYCLED', or 'DESTROYED' status upon recycling or disposal.

This streamlined system, wherein each stakeholder minimally interacts with the RBN and the DPP, establishes a robust data trail, thereby enhancing efficiency and sustainability while fostering circular economies.

ChromaWay remains steadfast in its commitment to developing blockchain solutions that drive the European Union's transition towards a circular economy, ensuring long-term prosperity for all stakeholders involved.

3.8 Billon

Billon is a technology company with a self-developed, ultra-efficient, data-centric blockchain protocol. The platform fully supports Web 3.0 and provides high performance as well as energy efficiency. It processes data, documents, identity, tokens, and money on the same rails, leading to improvements in processes, security, and automation. Billon's solution is a revolution in data management and has been tested and verified by globally recognised companies. The company was founded in the UK in 2015, based on an earlier R&D project in Poland. Its promising blockchain protocol has been supported by several R&D grants, including from the EU's Horizon2020 programme. In 2022, the European Commission selected Billon as one of three suppliers for the pre-commercial solution development and field testing of the Europe-wide blockchain within the European Blockchain Services Infrastructure (EBSI) programme. Billon's partners include leading companies such as the Reserve Bank Innovation Hub (RBiH), FIS Global, Raiffeisen Bank International, Tauron, and BIK, Findings.co, Sycope.

Billon's unified blockchain system's document management capabilities can be used to manage the complexity of tracing the life-cycle of material goods from raw material extraction through goods creation, logistics, and storage, and finally to trace usage and recycling disposal. While it can be applied to any product, the focus will be on two specific cases: plastic waste and car batteries. The digital product passport is a blockchain-based end-to-end provenance and traceability solution that allows companies to digitally record and share information about the product to prove the product's origin and sustainability. The solution provides easy access to transparent product information for supply chain participants supporting objectives of circular economy goals set by the EU.

The objective of the digital product passport is to gather comprehensive data on products, beginning from the materials used in their production, through various stages of the supply chain, and continuing throughout the customer journey. This initiative facilitates the collection, tracking, reporting, and immediate access to a product's history at any given time within the blockchain ecosystem, renowned for its transparency and data immutability. It aims to digitise and advance the recycling process for market sectors including food, textiles, plastics, construction, electronics, and more, which are poised to integrate circular economy principles into their product life cycles.

Billon's solution is ideally equipped to establish the origins and track the movement of materials, as well as to monitor environmental impact and identify waste within the economy.

3.9 Interfacer by DYNE

While the global movement around fab cities, fab labs, and the maker scene is growing, there is a digital infrastructure missing that would enable a data-based circular economy in both the global and local sphere.

A fab city is an innovative urban model that re-localises production to the city and its bioregional context, by empowering communities with the technology to build their own sustainable, innovative, and regenerative urban futures.

The project aims to help fab cities produce everything they consume on the basis of collaboratively developed and globally shared data as commons on the web. It promotes a green, resilient, and digitally based mode of production and consumption that enables the greatest possible sovereignty, empowerment, and participation of citizens all over the world.

Within the Interfacer Project, Dyne.org focused on the core component of this technology stack, the Interfacer Platform (aka Fab City OS Core), an innovative federated solution, tackling the challenges facing open-source hardware projects by mapping out the entire product lifecycle.

Interfacer is a software stack aiming to offer modular and highly customisable components that each fab city, fab lab, and like-minded organisations, can adopt, activate, and configure based on their own needs. The challenges to be tackled involve:

- Accelerating the growth of the network by facilitating the onboarding process
- Reducing the required technical knowledge
- Ensuring compatibility, coherence, and scalability by promoting the same data exchange standards, protocols, principles, and frameworks.
- Offering community support and further development along the way.

A digital product passport is structured product-related information, including data on sustainability, to facilitate circular value retention and extraction activities such as reuse, remanufacturing, and repairing.

Stored in a distributed ledger, it will guarantee reliable and authentic information, which may be able to reduce production costs and bureaucracy.

DPP will also record any flows on the design and development data to promote global collaboration, providing stronger motivation and opportunities for new contributors. The DPP will add valuable data for recycling, disassembly, and repair to improve sustainability and green practices.

The W3C DID standard defines a way to create and manage decentralised identifiers (DIDs) for entities such as people, organisations, devices, etc., on a blockchain or other decentralised system. It empowers digital sovereignty and federated cooperation.

Fab City OS core presents a revolutionary economic model, called ‘creative flows’, supporting the sharing, tracking, and tracing of open hardware in a standardised form. This enhances collaboration and promotes fair agreements directly between users in a secure network. Globally connected productive communities are empowered to discover, remix, and improve designs and technologies like never before.

Creative flows, making use of blockchain technology, facilitate fair revenue distribution based on contributions and agreements. Fab City OS will transform the traditional economic model, offering a decentralised and equitable solution.

The full interview with Andrea D'Intino from DYNE is available in the Appendix.

CHAPTER 4: BEST PRACTICES AND LESSONS LEARNED

EU's strategy for a circular economy, fuelled by its digital transition and the establishment of data spaces, seeks to unify, and normalise data accessibility. The digital product passport (DPP) has been developed as a bespoke solution to fulfil these requirements. Initially focused on the battery, textile, and construction sectors, it is expected that more rigorous standards will soon be applied across additional sectors.

Implementing digital product passports is poised to significantly hasten the journey toward an eco-friendly and circular economy. Nonetheless, there might be apprehensions concerning the security implications of a centralised data repository. This is precisely where solutions based on a decentralised, blockchain-based ecosystem come into play. They promise a secure, transparent, and effective methodology, safeguarding the interests of both businesses and consumers. Such systems allow enterprises to comply with regulatory mandates while leveraging the economic and marketing benefits associated with possessing a DPP.

The initiative to explore and apply DPPs is a major stride towards fostering an environmentally sustainable society and promoting the circular economy concept. Through the use of blockchain's decentralised feature, DPPs ensure a transparent, secure, and efficient mechanism for monitoring and managing the lifecycle of products – from their inception to recycling or disposal. This approach not only maintains the integrity of products but also provides consumers with valuable insights into the origins and eco-friendliness of their acquisitions.

An issue that has come up several times during the preparation of the current document has been the vital importance of multi-stakeholder collaboration. The successful deployment of blockchain-enabled DPPs relies on collective effort and data sharing among suppliers, manufacturers, regulators, and consumers. Moreover, to achieve interoperability across diverse systems and sectors, standardising data formats and protocols is crucial, enabling the smooth exchange of information.

Compliance with prevailing regulatory standards, especially those related to data privacy, security, and ownership, is crucial. This underscores the necessity for ongoing engagement with regulatory entities to ensure DPP solutions meet all legal requirements, reflecting the dynamic nature of digital products and blockchain technology regulations.

The broader acceptance of DPPs depends on creating an ecosystem informed about their use. Therefore, targeted educational and awareness programs are essential to dispel misconceptions about blockchain and DPPs, cultivating a culture of trust and openness among stakeholders.

It is imperative to identify and tackle the obstacles hindering the adoption of blockchain and DPPs. This includes making the technology more user-friendly, improving the economic feasibility of DPP implementation, and developing clear business cases to communicate the benefits of DPPs beyond mere compliance and sustainability.

Future strategies for DPP adoption must incorporate continuous innovation and adaptability. As technology and regulatory landscapes evolve, so too should DPP implementation tactics, with a focus on scalability to accommodate increasing product volumes and data as adoption expands.

In conclusion, while blockchain provides a solid foundation for DPPs, its deployment faces challenges such as scalability, energy consumption, and the complexity of establishing a decentralised infrastructure. However, the potential for innovation remains vast, including the use of smart contracts to promote sustainable practices and zero-knowledge proofs to reconcile transparency with privacy concerns.

Reference

Blümke, J. and Hof, H.J., 2023. Binding the Battery to the Pass: An Approach to Trustworthy Product Life Cycle Data by Using Certificates Based on PUFs. *International Journal on Advances in Security*, *16*(1&2), pp.44-53.

Navarro, L., Esteban, J.C., Miralles, M.F. and Griso, D.F., 2022. Digital transformation of the circular economy: Digital product passports for transparency, verifiability, accountability. *Manuscript submitted for publication*.

Panza, L., Bruno, G. and Lombardi, F., 2023. Integrating absolute sustainability and social sustainability in the digital product passport to promote industry 5.0. *Sustainability*, *15*(16), p.12552.

Saari, L., Heilala, J., Heikkilä, T., Kääriäinen, J., Pulkkinen, A. and Rantala, T., 2022. Digital Product Passport Promotes Sustainable Manufacturing.

Saleheen, A. and Afrid, S., 2023. Potential of decentralised blockchains for the digital product passport: Need for traceability and transparency in textile industries.

Stodt, F., Maisch, N., Ruf, P., Lechler, A., Riedel, O. and Reich, C., 2024. Collaborative Smart Production Supply Chains with Blockchain Based Digital Product Passports.

Voulgaridis, K., Lagkas, T., Angelopoulos, C.M., Boulogeorgos, A.A.A., Argyriou, V. and Sarigiannidis, P., 2024. Digital product passports as enablers of digital circular economy: a framework based on technological perspective. *Telecommunication Systems*, pp.1-17.

Wu, L., Lu, W., Peng, Z. and Webster, C., 2023. A blockchain non-fungible token-enabled 'passport'for construction waste material cross-jurisdictional trading. *Automation in Construction*, *149*, p.104783.

Web Sources

- DPP in a nutshell – CIRPASS (cirpassproject.eu)
- Ecodesign for Sustainable Products Regulation - European Commission (europa.eu)
- Circular economy action plan - European Commission (europa.eu)
- Textiles strategy - European Commission (europa.eu)
- Batteries - European Commission (europa.eu)
- EUR-Lex - 32023H2585 - EN - EUR-Lex (europa.eu)
- https://www.intesigroup.com/en/news/trace4eu/
- https://thebatterypass.eu/
- https://re-source.tech/resource-first-battery-passport-pilots/
- Corporate sustainability due diligence - European Commission (europa.eu)
- Circularise
- Circulor
- Spherity
- nChain
- Digital Product Passport (iota.org)

- ChromaWay
- Billon
- Interfacer Platform

Appendix: Interviews with DPP providers

Circularise

Interview with Mesbah Sabur – Founder and CEO

Could you please briefly introduce Circularise?

Circularise is a supply chain traceability software scale-up, providing a platform for companies to create and manage digital product passports, with the overall goal of facilitating the transition to more circular material flows.

The company was founded in 2016 to address the problem of ineffective waste processing, by facilitating more efficient and reliable information transfer between members of supply chains. This is achieved by creating digital product passports which contain information useful to members of the value chain such as material composition and sustainability impact metrics.

Our USP lies in our selective data sharing technology, which allows companies to reliably share the key information required by members of the supply chain, while keeping their sensitive information secure. Our technology puts the owner of the original information in full control of who they share the information with.

By including a reliable record of information with a product, consumers can make more informed buying decisions, they know how best to care for and repair their products, and what to do with a product at the end of its life. This allows businesses to set up repair, refurbishment, remanufacture, and product-as-a-service offerings, thereby creating a more circular economy.

How is Circularise leveraging blockchain technology to address the challenges of creating DPPs?

The reliability of the data in a digital product passport is key to their overall success. If the information in a digital product passport is not accurate and comparable, then it is not useful. Blockchain ensures that the information entered cannot be tampered with, so when primary data is added, it cannot be altered. An immutable history of a product makes it clear who added what data about a product, with the confidence that it has not been wrongfully altered.

This is why we use blockchain in the background of our platform. When a company creates a DPP on the Circularise platform, they create a unique digital record (a.k.a. a token) which represents the physical asset. They can then include information about the product relevant to their operations.

When they send the product to their customer, the DPP is sent along with it. So the ownership of the digital record reflects the ownership of the physical product. Each company is then responsible for adding information about their operations and impact on the product to the DPP, to create a reliable history of the product's lifecycle.

At every stage, companies can make use of our selective data sharing technology to ensure that only the parties they approve see certain insights. As the claims made are linked to primary data sources (such as ERP or production machine data) which can also be verified by third-party audits, the claims made can be trusted by the other parties in the value chain.

The information from each stage of the supply chain can then be collated to paint an overall picture of the composition and environmental impact of the product. Knowing that the insight is based on real data which cannot be tampered with, not from estimates or unverified sources.

Based on your experience, are there any relevant benefits from using a decentralized architecture for DPPs compared to a centralized one?

Opting for decentralisation fundamentally comes down to trust in the system. Decentralisation means that participants in the network do not have to trust a centralised party or group, to own and be the administrator

of their data. A centralised system (blockchain or otherwise) means that companies have to trust that the centralised party has no incentive to edit or disclose their data.

A decentralised blockchain on the other hand, has public verifiability that the information cannot be tampered with. This is because in a public distributed ledger, the system is built to prevent information from being deleted, and all entries in the system are public, so anyone can check the history of the record, so trust does not have to be placed in any private party or committee.

Centralisation also creates data silos, making it difficult to get information flowing between parties which are not part of the private network. If a variety of companies try to create their own centralised ecosystems, it makes it very difficult for companies which need to interact with a range of different centralised systems. Whereas decentralisation by its very nature makes it easier to facilitate interoperability between systems.

There will be times when in simple ecosystems where parties trust one another, it will make sense to choose the easy option of a centralised database for DPPs. But in many complex supply chains where universal trust is not present, a decentralised approach is the only scalable and reliable option.

Decentralisation vs centralisation is also not as black and white as it may seem, different parts of a system can be centralised while others are decentralised. From our point of view, it is currently not beneficial to pursue a fully decentralised system (e.g., a DAO-like approach). It introduces too many challenges for significantly diminishing returns. But there are certain aspects of the full system which make sense being decentralised. For example, transactions, e.g., “create a DPP”, are performed on a centralised system, but anchored to a decentralised blockchain for verifiability of the correctness of the transaction.

What are the main technological and/or regulatory barriers for the application of blockchain technology for DPPs?

Understanding of the technology is one of the main barriers to the adoption of DPPs and blockchain in general. They are both new concepts, only just reaching technical readiness and scalability, and the majority market will not move until a technology becomes the norm or it is a legal requirement.

The use of blockchain for DPPs is also not prescribed in current regulations. Many EU proposals, frameworks, and strategies reference the need for decentralisation and interoperability but do not say that blockchain is strictly necessary. It is not yet clear how strict the EU will be with regard to specific system architecture, and it is unlikely they will get involved in deciding the specific applications to be used which will allow companies to create DPPs. Having said that, more specifications for the backend structure of DPPs are required from regulations (i.e., systems need to be public, permissionless, cannot use proof of work, etc.) in order to bring in a level of standardisation and quality for DPP ecosystems.

Connecting systems together to make a DPP ecosystem interoperable and scalable is a key challenge. If DPP providers which operate in closed, private systems become prominent, then a web of integrations and APIs will be required for the system to run, creating many points of potential failure in the system. Ideally, an open protocol will be established (similar to email), so that systems can easily communicate with each other, even if they are using different applications. But this will also require widespread collaboration between companies to establish an open standard.

What are you views about the use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and/or other decentralized technologies for the implementation of DPPs? What are their respective advantages and disadvantages?

NFTs can be used for DPPs but are limited to product-level traceability. You can implement batch-level traceability using NFTs, but that would be an implementation without double spending prevention. With double spend prevention, ERC-1155-like tokens are more suitable. Each token then represents a batch and the amount represents the weight/amount of the batch. This is more suitable for batch-level DPPs, which enable the most value for the circular economy.

Having said that, using such tokens to enable DPPs on a public blockchain introduces privacy and confidentiality issues that would prevent certain industries from adopting the technology. Our focus is more on using zero knowledge proofs to bring the best of both worlds:

- public verifiability of the correctness of data
- data is not publicly available

DIDs seem to be the best approach for a more decentralised authentication layer of the DPP architecture. However, in our experience we have not seen many organisations that are ready to adopt DIDs currently.

VCs are great in principle, but last time we checked they weren't easily fitting the zero knowledge proof paradigm, which we believe is the way forward. Also, while ZKP is being worked on for VCs, it's mainly useful for proving static claims. IT does not lend itself well to transactional claims like within a chain of custody.

What are the key lessons learned from following a blockchain-based approach for the DPPs?

- The knowledge gap many executives have makes discussing the use of blockchain difficult. Particularly when different DPP solutions using different types of blockchain in different ways need to be compared it makes it difficult to communicate key differences and considerations.
- There are also very few companies who are prepared to prioritise full decentralisation, as some level of centralisation comes with greater convenience. It is often best to focus on the outcomes of what a certain system design will practically mean for a company, rather than trying to explain the system details themselves.
- Having all information present on a public chain is also not a viable solution, as trade secrets must be protected by selectively sharing information, as opposed to having full transparency.
- Creating entirely new systems for digital product passports is also not feasible as the barrier to implementation is too high. DPPs will need to be integrated with existing systems to automate information transfer and alignment with existing business operations.
- Even with our selective data sharing technology, our cryptography team must very carefully consider what information will be stored on-chain. As data can never be deleted, we must be extra cautious to protect from future risks. This is why we use zero-knowledge proofs, so that on-chain data are perfectly hiding the underlying (sensitive) data.

Based on your experience, what are the best practices for implementing a DPP?

It is then useful to run an exercise to determine what information is desired from others, what should be shared, and what must be shared for regulatory compliance. Once this is mapped out, including where the information is stored, businesses can then consider how to connect the dots.

First, internal systems must be in order, ensuring all the required data is collected, reliable, in a standard format, and stored in a system which can be easily connected with other systems.

There must first be a clear goal for implementing digital product passports. Businesses must also align with the other key members of the value chain on what information companies are prepared to share with each other. It is also important to establish a clear set of goals and definitions with the supply chain, so that new systems, business models, and initiatives can be established effectively. This alignment and collaboration within the value chain is a key factor to a successful DPP initiative.

To ensure that this innovation is economically sustainable, there must also be a clear business case for scaling DPPs after an initial pilot. This could be to mitigate the risks of greenwashing, establish a service model, capture the value of waste, establish a directed buy agreement, reduce time spent on information transfer activities, or some other value adding activity.

One issue is that many of these business cases require scaled implementation of DPPs before there is an ROI, so if a company tries to measure success early in an incremental innovation process, it will appear

unsuccessful. To mitigate this, expectations must be clearly managed by measuring the success of DPP implementation over a longer time frame, or a disruptive innovation approach must be taken to embrace rapid change.

Circulor

Interview with Douglas Johnson-Poensgen – CEO

Could you please briefly introduce Circulor?

Circulor is a technology company that specializes in supply chain traceability and sustainability. Our platform uses a combination of blockchain and other advanced technologies to track and verify the origins and movements of raw materials, components and finished products through complex supply chains. Circulor's goal is to help companies and organizations ensure the ethical and sustainable sourcing of raw materials, such as minerals used in electronics and batteries, as well as to support efforts to reduce carbon emissions and promote circularity in the economy. We work with a variety of industries, including automotive, electronics, and aerospace, to provide transparency and accountability in their supply chains. Overall, Circulor is dedicated to using technology to make global supply chains more sustainable, ethical, and transparent, and are a leader in this field.

How is Circulor leveraging blockchain technology to address the challenges of creating DPPs?

One of the key challenges faced by companies when implementing DPPs (Digital Product Passports) is ensuring the integrity of the data captured throughout the product's lifecycle. To address this challenge, Circulor has leveraged blockchain technology to create an immutable record of all product-related data that cannot be altered or tampered with.

Blockchain technology is a distributed ledger system that allows for the creation of a secure, transparent, and immutable record of all transactions. Circulor's blockchain-based DPP solution ensures that all data related to the product's lifecycle is recorded in a tamper-proof and transparent manner. The use of blockchain technology ensures that the data recorded is immutable, meaning it cannot be modified, deleted, or altered in any way.

Circulor's DPP solution is based on the Hyperledger Fabric blockchain framework, which is an enterprise-grade blockchain platform that provides high levels of scalability, security, and performance. The Hyperledger Fabric framework is designed specifically for enterprise use cases and provides a range of features that make it ideal for creating DPPs, such as private channels, smart contracts, and energy efficient consensus mechanisms.

Circulor's DPP solution provides a comprehensive view of a product's lifecycle, from the raw materials used to manufacture the product, to the final product itself. All data related to the product's lifecycle, including information such as the origin of the raw materials, the manufacturing process, and the distribution and sale of the product is managed in the Circulor platform. For performance reasons only data fingerprint (hash value) of each recorded transaction is stored on the blockchain. The use of blockchain technology provides greater transparency and accountability throughout the supply chain. All parties involved in the supply chain can access the Circulor platform and can view the data recorded, providing a transparent and auditable record of the product's journey. This can help to improve trust between suppliers, manufacturers, and consumers, as it provides greater visibility into the product's origin, quality, and sustainability.

In conclusion, Circulor's use of blockchain technology to create DPPs provides a secure and transparent solution for tracking and tracing products throughout the supply chain. The use of blockchain technology ensures that all data recorded is tamper-proof and transparent, providing a comprehensive view of a product's lifecycle. This can help to improve trust and accountability throughout the supply chain and provide consumers with greater confidence in the products they purchase.

Based on your experience, are there any relevant benefits from using a decentralized architecture for DPPs compared to a centralized one?

There are several relevant benefits to using a decentralized architecture for DPPs compared to a centralized one. A decentralized architecture for DPPs refers to a system where data is distributed across a network of nodes or computers rather than being stored in a central location. Here are some of the key benefits of using a decentralized architecture for DPPs.

- Improved Data Integrity: Decentralized architectures can improve data integrity as data is stored across multiple nodes, making it more difficult for any single node to corrupt the data. Decentralized architectures can also leverage consensus mechanisms to ensure that any changes made to the data are agreed upon by the network, further enhancing data integrity.
- Increased Security: Decentralized architectures can increase security as data is distributed across a network of nodes, making it more difficult for hackers to gain access to the data. Additionally, decentralized architectures can use cryptography and other security measures to protect the data stored on the network.
- Enhanced Transparency: Decentralized architectures can enhance transparency as data is accessible to all network participants, providing a transparent and auditable record of the product's journey. This can help to improve trust and accountability throughout the supply chain.
- Improved Resilience: Decentralized architectures can improve resilience as data is stored across a network of nodes, meaning that even if one node fails, the data can still be accessed from other nodes. This can help to ensure that data remains accessible and available even in the event of a network failure or outage.
- Reduced Dependency: Decentralized architectures can reduce dependency on a single centralized entity for storing and managing data, providing greater autonomy to network participants. This can help to reduce the risk of a single point of failure and promote a more decentralized and distributed supply chain ecosystem.
- Increased performance: Given the fact that there will be millions of DPPs available in the future, a single network node wouldn't be able to manage the amount of network requests, hence a distributes architecture is mandatory for DPPs in the future.

In summary, using a decentralized architecture for DPPs can provide several benefits over a centralized architecture, including improved data integrity, increased security, enhanced transparency, improved resilience, and reduced dependency.

What are the main technological and/or regulatory barriers for the application of blockchain technology for DPPs?

While blockchain technology offers significant benefits for the implementation of DPPs, there are still some technological and regulatory barriers that need to be addressed. Here are some of the main technological and regulatory barriers for the application of blockchain technology for DPPs.

- Scalability: One of the technological barriers for the application of blockchain technology for DPPs is scalability. As the number of products and transactions on the blockchain increases, compute and storage costs will increase. Organisations might not want to process and store data that are unrelated to them.
- Interoperability: One of the technological challenges is interoperability. As there are multiple blockchain platforms available, there is a need to ensure that they can all work together seamlessly. This can be a challenge as different blockchain platforms have different architectures, protocols, and consensus mechanisms.
- Data Standardization: A significant challenge for the implementation of DPPs is the lack of data standardization. Without standardization, it can be difficult to ensure that all data recorded on the blockchain is consistent and can be compared across different products and supply chains. This can limit the value of DPPs in terms of improving transparency and traceability.

- Regulatory Framework: The regulatory framework for blockchain technology is still evolving, and there are concerns around data privacy, security, and ownership. Regulators are still trying to understand how blockchain technology can be used and how to regulate it. This can create uncertainty for companies looking to implement DPPs.

In summary, while blockchain technology offers significant benefits for the implementation of DPPs, there are still some technological and regulatory barriers that need to be addressed. These include scalability, interoperability, data standardization, the regulatory framework, and cost. Addressing these barriers will be crucial to unlocking the full potential of blockchain technology for DPPs.

What are you views about the use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and/or other decentralized technologies for the implementation of DPPs? What are their respective advantages and disadvantages?

The use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and other web3 technologies for the implementation of DPPs has the potential to provide significant benefits, but also comes with some challenges. Here are some of the advantages and disadvantages of each of these technologies.

- NFTs: NFTs, or non-fungible tokens, can be used to create a unique digital record of a product that can be tracked and verified on the blockchain. The advantage of using NFTs for DPPs is that they provide a secure and immutable record of a product's journey through the supply chain. Additionally, NFTs can be used to verify the authenticity and provenance of a product. However, the disadvantage of using NFTs is that they can be expensive to create and maintain, particularly for large volumes of products.
- DIDs: Decentralized Identifiers (DIDs) are a type of digital identifier that allows individuals or entities to create a unique, decentralized identity on the blockchain. DIDs can be used to provide a secure and decentralized way to track and verify the identity of individuals or entities involved in the supply chain. The advantage of using DIDs for DPPs is that they provide a way to ensure that only authorized parties have access to the data stored on the blockchain. However, the disadvantage of using DIDs is that they can be complex to implement and require significant technical expertise.
- VCs: Verifiable Credentials (VCs) are a type of digital credential that can be used to provide proof of identity, qualifications, and other attributes. VCs can be used to provide a secure and verifiable record of an individual's or entity's qualifications, which can be used to verify their eligibility to participate in the supply chain. The advantage of using VCs for DPPs is that they provide a way to ensure that only authorized parties have access to the data stored on the blockchain. However, the disadvantage of using VCs is that they can be complex to implement and require significant technical expertise. However, in the frame federate data spaces like CATENA-X that based on GAIA-X Trust Framework those web3 technology is easier accessible since some parts of the implementation for that are available as open source.

In summary, the use of NFTs, DIDs, VCs, and other web3 technologies for the implementation of DPPs has the potential to provide significant benefits, but also comes with some challenges. The key advantages of these technologies are that they provide a secure and immutable record of a product's journey through the supply chain and can be used to verify the identity and qualifications of individuals or entities involved in the supply chain. However, the main disadvantage is that these technologies can be complex and expensive to implement and require significant technical expertise.

What are the key lessons learned from following a blockchain-based approach for the DPPs?

Key lessons learned from following a blockchain-based approach for DPPs are as follows:

- Collaboration is crucial: The success of a blockchain-based DPP depends on the collaboration between all parties involved in the supply chain. This includes suppliers, manufacturers, distributors, retailers, and consumers. Each party needs to be willing to share data and work together to ensure the integrity and transparency of the supply chain. As a neutral and independent provider, our solution facilitates this collaboration.

- Standardization of data formats and protocols is critical for the successful implementation of blockchain-based DPPs. Standardization can help ensure that data can be easily shared and compared across different supply chains and can help reduce the costs and complexity of implementing DPPs.
- Regulatory compliance is essential: Blockchain-based DPPs must comply with all relevant regulations, particularly around data privacy, security, and ownership. Companies implementing DPPs must work closely with regulators to ensure that their solutions are compliant with all relevant laws and regulations.
- Education and awareness are important for the successful adoption of blockchain-based DPPs. All parties involved in the supply chain need to understand the benefits of DPPs and how they work. This can help build trust and increase adoption.

Based on your experience, what are the best practices for implementing a DPP?

Best practices based on our experience are the following.

- Define clear objectives: Before implementing a DPP, it's important to define clear objectives and goals for the project. This includes understanding what problem the DPP is trying to solve, what data needs to be collected, and how the DPP will be used to improve the supply chain.
- Involve all stakeholders: The success of a DPP depends on the involvement and cooperation of all stakeholders in the supply chain. This includes suppliers, manufacturers, distributors, retailers, and consumers. Engaging with all stakeholders and getting their buy-in is crucial for the successful implementation of a DPP.
- Ensuring the accuracy and integrity of data are critical for the success of a DPP. Data should be collected in a standardized format and verified at each stage of the supply chain to ensure its accuracy and integrity. Implementing mechanisms such as smart contracts and digital signatures can help ensure the authenticity and integrity of the data.
- Privacy and security concerns are a major issue for DPPs. Sensitive data should be protected using cryptography and access controls. Data privacy regulations should also be considered, and all stakeholders should be aware of their responsibilities in handling sensitive data.
- Use appropriate technology: Beside blockchain technology other technologies such as IoT sensors and AI can also be used to collect and analyse data.
- Test and iterate: DPPs should be tested and iterated upon to ensure their effectiveness. This involves collecting feedback from stakeholders and adjusting the DPP as necessary.

Spherity

Interview with Carsten Stöcker – Founder and CEO

Could you please briefly introduce Spherity?

In today's world, individuals and businesses face a multitude of health, fraud, and environmental challenges. To address these issues, policymakers are introducing stringent compliance regulations like supply chain policies, product passports, customs, ESG, and circular economy principles. However, the lack of digital evidence and infrastructure has led to massive fraud, counterfeit products, and widespread greenwashing.

Spherity aims to revolutionise compliance by providing a digital backbone for scalable and automated business transactions. Our solution establishes provenance and authorization chains, automating compliance at the level of individual transactions. By ensuring verifiable provenance, we help our customers create safer, more sustainable, compliant, ethical, and reliable value chains.

Leveraging advanced cybersecurity and authorization features, we protect API endpoints from malicious actors, adhering to NIST Zero Trust Architecture, Gaia-X design principles, and US National Cyber-security Strategy.

We have successfully launched our first supply chain security product, CARO, in the US pharma market, partnering with industry leaders like AstraZeneca, Bristol Myers Squibb, Johnson & Johnson, Novartis, and Sandoz.

In Europe, Spherity is uniquely positioned with enterprise and object identity wallets. We focus on developing secure, compliant, and interoperable Digital Product Passport (DPP) solutions to meet emerging EU regulations. Our solutions easily integrate with legacy infrastructure and support different trust domains, catering to industries such as batteries, textiles, toys, and bed mattresses.

How is Spherity leveraging blockchain technology to address the challenges of creating DPPs?

Spherity is leveraging blockchain technology to address the challenges of creating Digital Product Passports (DPPs) by focusing on the transparency challenge, implementing controls in software development, and employing strategic data placement. By understanding the potential risks associated with blockchain, Spherity can harness the technology to build DPPs that offer increased efficiency and trust while preserving business confidentiality.

The transparency challenge in blockchain technology arises from the inherent exposure of information due to replicated transaction storage and execution. Spherity recognizes that this challenge can be more problematic than anticipated and extends to both private and business data. Therefore, the company takes a careful approach to maintaining confidentiality by focusing on the tamper-proof registries feature of blockchain for public data only. This allows Spherity to create DPPs that benefit from blockchain's immutability without compromising sensitive information.

In software development, Spherity emphasizes the importance of security and compliance controls, especially when incorporating decentralized digital identity and W3C verifiable credentials. By following the Secure Software Development Life Cycle (SDLC) and considering compliance requirements from various regulations, Spherity ensures that the DPPs are secure, reliable, and adhere to necessary legal frameworks. The adoption of decentralized identity technology and verifiable credentials allows for more efficient implementation of existing controls and the potential for new controls to enhance the security of SSI systems.

Spherity also addresses the non-functional requirements and features of blockchain technology by considering transparency, electronic signatures, data integrity/authentication, confidentiality, attributability, tamper-proof timestamps, authentication, and authorization. By paying attention to these aspects, the company can provide a robust and secure foundation for DPPs that take full advantage of blockchain's capabilities.

To further mitigate privacy risks, Spherity employs a strategic data placement architecture for blockchain use cases. This approach involves placing registry data on-chain and keeping company master data, company transaction data, transaction data assets, core process transaction data, customer data, and data subject to transparency obligations off-chain. By doing so, Spherity ensures that sensitive information is protected while still benefiting from the inherent advantages of blockchain technology.

Spherity is leveraging blockchain technology and Self-Sovereign Identity (SSI) principles to create Digital Product Passports (DPPs) that address the transparency challenge, implement robust controls in software development, and strategically manage data placement. By utilizing SSI for verifiable credentials, Spherity is able to establish provenance chains about product assertions, as well as authorization chains for granting access to DPPs. This approach provides a secure and efficient method for verifying the authenticity of products and ensuring the security for the involved parties.

Additionally, blockchain technology plays a vital role in enabling decentralized service endpoint look-up for supply chain actors. When a product identifier is scanned, the blockchain can be used to look up the DPP API service endpoint, allowing seamless access to relevant product information. This decentralized nature of blockchain-based look-up ensures that any actor can access the registry via its local blockchain node, eliminating the need for a centralized look-up registry. Consequently, this approach mitigates the risk of correlation by a central authority, enhancing both business confidentiality and security.

Our compliance-focused approach ensures that Spherity's DPPs meet the complex demands of today's digital landscape, providing a robust foundation for establishing provenance and authorization chains, while harnessing the decentralized capabilities of blockchain technology to drive innovation and improve business processes.

Based on your experience, are there any relevant benefits from using a decentralized architecture for DPPs compared to a centralized one?

There are several benefits to using a decentralized architecture for Digital Product Passports (DPPs) compared to a centralized one.

- Enhanced security: Decentralized systems, like blockchains, distribute data across multiple nodes, making them less vulnerable to hacking, data corruption, or system failures.
- Tamper-proof registries: Decentralized architectures make use of tamper-proof registries, which provide a reliable and secure way to store and manage information, such as DID registries, revocation registries, look-up registries, and trust registries. Each of these registries comes with its own publicly accessible transaction history and audit log, which makes it possible to verify the accuracy and authenticity of the stored data. This feature ensures transparency, trustworthiness, and immutability, and enables stakeholders to trace the provenance of data and transactions, further enhancing the overall security and confidence in the system.
- Off-chain provenance and authorization chains: Decentralized architectures enable the separation of on-chain and off-chain data. This allows for the establishment of off-chain provenance chains to track product assertions, as well as authorization chains for access to DPPs. By utilizing SSI and verifiable credentials, these chains can provide secure and trusted information without compromising confidentiality or overloading the blockchain. This separation of data also allows for better scalability, as off-chain data storage can be optimized without impacting the overall performance of the decentralized system.
- Increased trust: Decentralized architectures often rely on consensus mechanisms and cryptographic techniques. This creates a higher level of trust among participating parties, as the data's authenticity and integrity are independently verifiable by all ecosystem actors. However, this also requires the implementation of a robust trust framework and formal conformance program as well.

- Compliance controls: Decentralized systems can more effectively address regulatory and compliance requirements through the use of SSI, verifiable credentials, and blockchain technology. These mechanisms can help ensure the transparency, traceability, and consistency of compliance controls in the software development process and throughout the product's life cycle. This decentralized approach also enables a more efficient implementation of existing controls while providing new ones to enhance security and trust.
- Decentralized look-up for business confidentiality: Decentralized architectures enable the use of decentralized look-up registries, accessible via local blockchain nodes, which eliminates the need for a centralized registry. This approach reduces the risk of centralized surveillance and correlation, as any actor can access the look-up registry through its local blockchain node.

What are the main technological and/or regulatory barriers for the application of blockchain technology for DPPs?

The technology behind decentralized digital product passports (DPPs) is fundamentally an ecosystem technology, which means that its true value can only be realized when it is widely adopted by an early majority of supply chain actors. If only a few players adopt the technology, it will not deliver the intended benefits, as the effectiveness of DPPs is directly proportional to the level of adoption of the underlying trust framework. Consequently, it is crucial to have a structured ecosystem development and adoption approach that garners support from the majority of ecosystem actors. This collaborative and coordinated effort helps to ensure the successful implementation and widespread use of DPPs, ultimately unlocking their full potential in enhancing transparency, traceability, and trust throughout the supply chain.

The main technological and regulatory barriers for the implementation of Digital Product Passports (DPPs) include the following.

- Incomplete ecosystem can hinder the economic justification and viability of DPP technology.
- Limited education and understanding of technology, processes, value proposition and trust framework.
- Lack of business case support for DPP implementation, the project may face resistance and struggle to gain traction.
- Over-complication of use case scenarios: Overengineering the complexity of DPP use case scenarios can lead to project failures, as it creates a significant barrier to adoption and successful execution.
- Unmet need for digital backbone and DPPs for policy enforcement: When existing policies, such as those related to the EU Green Deal, require a digital backbone and DPPs for automated enforcement at scale, the lack of such infrastructure can hinder the success and adoption of DPPs.
- Standardization is crucial for DPP adoption but challenging due to rapidly evolving technology and competing blockchain networks.
- Absence of a joint adoption roadmap and strategy: Without a clear and mutually supported adoption strategy among all involved parties, the project risks fragmentation and failure.
- Absence of a trust framework and conformance program for decentralized digital product passports (DPPs) can lead to compromised authenticity and integrity, undermining their main purpose of enhancing transparency and traceability in supply chains.
- Lengthy project timelines for DPPs can deter early adopters due to concerns about stranded investments and rapidly evolving technology, leading to hesitance and slowed progress in the ecosystem.
- Lack of Ecosystem leadership hinders the success of DPPs, as most organizations focus on short-term ROI rather than fostering a collaborative approach to drive widespread adoption and development of the technology.

It shall be recognized that these barriers apply to both blockchain- and non-blockchain-enabled DPP projects.

What are you views about the use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and/or other decentralized technologies for the implementation of DPPs? What are their respective advantages and disadvantages?

Unlocking Business Benefits with DIDs and VCs: Enhancing Trust, and Compliance in Digital Product Passports

Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) play a crucial role in the successful implementation of Digital Product Passports (DPPs). DIDs provide a secure and decentralized mechanism for uniquely identifying entities within the DPP ecosystem, such as supply chain actors, products, or assets. They enable greater privacy, security, and control for identity management, mitigating the risks associated with centralized identity systems.

Verifiable Credentials (VCs), on the other hand, are digital representations of claims or assertions made by one entity about another. They are cryptographically secure, tamper-evident, and can be independently verified by any party. In the context of DPPs, VCs can be used to represent various aspects of a product's life cycle, such as its provenance, quality, environmental impact, and compliance with regulations or standards.

Verifiable Credentials (VCs), when combined with a trust framework, a conformance program, credential chaining, and authorized issuers, can effectively establish provenance and authorization chains for DPP applications. This comprehensive approach ensures secure, trusted, and transparent data management, enhancing the overall integrity and reliability of the system in which they operate.

Together, DIDs and VCs form the foundation for establishing trust and transparency within the DPP ecosystem. They enable participants to create and share secure, verifiable, and privacy-preserving records of product-related information throughout the supply chain. This, in turn, allows for more efficient and automated policy enforcement, compliance monitoring, and traceability of products.

Empowering Cross-Domain Provenance Assertions: Harnessing DIDs and VCs for Trust and Interoperability

DIDs and VCs provide a versatile solution for working across multiple trust domains, bridging diverse sectors and regulatory environments. By enabling seamless interactions between eIDAS TSPs, TÜV, GS1, GLEIF, national governments, and domain-specific trust domains such as Carbon Credits or Supply Chain Security, DIDs and VCs create a robust and interoperable framework for identity, credential management and provenance graphs.

This empowers organizations to establish and maintain trust with various stakeholders, fostering secure and efficient collaboration across different domains. As a result, businesses can confidently navigate complex ecosystems, ensuring compliance and leveraging the unique benefits of each trust domain to enhance their overall value proposition.

Data Storage and Data Spaces: Scaling Value of Your Data with Next Level Data Sharing

Decentralized data storage offers businesses numerous advantages, including enhanced security, greater control, and improved business confidentiality. We recommend integrating DIDs/VCs with data spaces, federated catalogues, metadata repositories, and standardized control planes for access policy decisions and enforcement in accordance with Zero Trust Architecture (ZTA) Principles.

This approach enables the discovery, request, and provision of credential graphs for verifiable product provenance assertions. Additionally, authorization credentials can be utilized for attribute-based access management (ABAC) on the control plane layer. Projects such as Gaia-X, Catena-X, Manufacturing-X, and SIMPL are actively developing solutions to harness the benefits of decentralized data storage for businesses.

Cyber-security: Enhancing Business Security with ABAC and Robust API Endpoint Protection

Cybersecurity and API endpoint security are of paramount importance for businesses in today's digital landscape. The increasing number of cyber threats and data breaches emphasize the need for robust security measures to protect sensitive information and maintain trust with customers and partners. API endpoints, as critical points of data exchange, are particularly vulnerable and require strong security protocols. Authorization credentials and Attribute-Based Access Control (ABAC) contribute to improved API endpoint security by providing a fine-grained, context-aware access control mechanism.

With ABAC, access decisions are based on attributes of the requester, the resource, the environment, and the action being performed, ensuring that only authorized users with appropriate permissions can access the data. This comprehensive approach to access control reduces the risk of unauthorized access and enhances the overall security posture of an organization's API infrastructure for DPP solutions.

Automating Compliance with the Law: Establishing Audit Trails for Authorization Events

ABAC can also help drive compliance with the law by granting access only to authorized ecosystem actors and generating an audit trail of third-party access requests, such as export compliance credentials or licenses to operate in a given industry. Without such authorization mechanisms, organizations may face increased manual work in compliance departments, potentially leading to inefficiencies and increased risk of non-compliance.

Boosting Trust & Efficiency: AI-enabled Risk Scoring for DPP Claims Across Trust Domains

Leveraging credentials and credential graphs from multiple trust domains within a DPP allows businesses to conduct risk-scoring or trustworthiness scoring of product claims more effectively. By incorporating diverse sources of verified information, businesses can establish a comprehensive understanding of a product's lifecycle, provenance, and compliance with various standards. This holistic approach enables the creation of a dynamic risk-scoring system that assesses the trustworthiness of product claims based on the reliability and credibility of the associated credentials, non-conformance events in the supply chain and issuing entities.

The business benefits of this risk-scoring approach include improved decision-making, streamlined compliance monitoring, and enhanced supply chain transparency. By analysing product claims through artificial intelligence (AI), businesses can better identify potential risks, monitor adherence to regulations, and make more informed choices regarding their supply chain partners. Ultimately, the implementation of risk scoring for DPP claims fosters trust and confidence among stakeholders, contributing to a more resilient and efficient ecosystem. AI-driven dynamic risk scoring is an emerging capability in the DPP Domain that is expected to gain more momentum with the amount of operational DPP data.

Avoid the Hype Driven by Unregulated Industries: Steering Clear of NFTs for DPP Applications

We advise against using NFTs for digital product passports and supply chain use cases since they involve on-chain ownership assertions that conflict with business confidentiality requirements in industrial and regulatory contexts.

Although future privacy-preserving blockchain technology might address this challenge, it is currently at a low technology readiness level. Furthermore, NFTs lack standardization for regulatory and compliance use cases, with their adoption primarily occurring in unregulated industries.

Empower SMEs & Protect Business Confidentiality: Decentralized UMA for Secure Data Sharing

User Managed Access (UMA) is a security framework that empowers users to have control over the sharing and access of their digital resources, particularly when the data owner and data provider are distinct roles. For instance, in the case of vehicle telematic data or electronic health records, a private individual may be the data owner while a centralized platform operator provides the data. Another example includes a digital product passport (DPP) operator serving small and medium-sized enterprises (SME).

An issue with existing UMA solutions is that access policies must be configured on a centralized platform, which may inadvertently reveal sensitive information, such as the business partners with whom one engages. This unintentional leakage of data presents a challenge when preserving privacy is crucial. Blockchain technology shows potential in facilitating UMA solutions, particularly when combined with privacy-preserving technology. However, this approach is still in its early stages, with research ongoing and a low technology readiness level at present. A decentralized version of UMA is being researched in the IDunion project.

Path to Next Level Business Confidentiality & Security: Multi-party Computation for Encrypted Data Sharing

Confidential Computing, particularly Multi-party Computation (MPC), is a cryptographic technique with immense potential for enabling privacy-preserving data sharing. MPC allows multiple parties to collaboratively compute a function over their inputs while keeping those inputs private.

Data can be stored on a shared MPC infrastructure, and when requesters seek access, they send a request to the data owners. In response, data owners generate a search token, allowing requesters to execute their queries on encrypted MPC data.

The value proposition of MPC for searching encrypted data is that it ensures a third party cannot gain any knowledge about the encrypted search request, maintaining privacy and security throughout the process. However, the application of this technology for industrial use case ecosystems is currently at a low level of technology readiness.

nChain

Interview with Leandro Nunes – Chief revenue Officer

Could you please briefly introduce nChain?

Since our founding in 2015, nChain has been focused on a singular objective: making the world-changing potential of blockchain technology accessible to more individuals, businesses, and governments. We are the DNA of Blockchain. The DNA of blockchain is the efficient exchange of value.

Innovative and forward-thinking organisations around the globe are looking to unlock the power of blockchain-enhanced data, and we are working tirelessly to provide solutions and support that minimise the gap between blockchain interest and realised value. Over the last few years, our work in critical areas including scaling open public blockchains, supply chain solutions, identity solutions, loyalty programmes, micropayments, and automated exchanges have demonstrated that we understand and can fulfil the large, and still underappreciated, potential of blockchain technology. Our research and development teams have developed one of the largest portfolios of research related to blockchain technology.

How is nChain leveraging blockchain technology to address the challenges of creating DPPs?

Blockchain technology holds the potential to revolutionise numerous business operations by streamlining and simplifying complex processes. Amongst these, DPP stands out as it requires the contribution of multiple parties within a supply chain sharing data at various stages of a product's lifecycle. Traditional data sharing in this way is costly, inefficient and error prone. Furthermore, establishing direct connections and trust between parties isn't always feasible, adding yet another layer of complexity. A successful DPP implementation requires a neutral entity or equivalent infrastructure to facilitate data sharing. This eliminates the need for parties to directly trust each other. Instead, parties place their trust in the neutral platform. This is where blockchain technology proves to be a game-changer. By providing a neutral, immutable infrastructure, blockchain enables all participants to share data throughout a product's lifecycle. This eradicates the need for establishing direct connections or repeated data verification, thereby ensuring data integrity and authenticity.

Blockchain's distinctive features, such as its distributed architecture, cryptographic security measures, and consensus protocols, foster interoperability. This means participants from around the globe can transact, exchange data, and collaborate in a trusted and secure environment. The technology effectively eliminates the need for intermediaries and geographical constraints, thereby simplifying the data sharing process and enhancing the efficiency of business operations.

nChain delivers products and solutions together with our partner UNISOT, a Web3 supply chain traceability platform that provides global interoperability and specialises in supply chain applications including SeafoodChain and a DPP application aligning to EU standards. Using the public blockchain as a global data layer enables supply chain actors to securely connect and open their data silos and get economically incentivised to share information. This means global traceability and transparency. We believe that only infrastructure that can provide efficient value exchange, peer-to-peer, at scale and solve the inefficiencies across every level of the supply chain.

Based on your experience, are there any relevant benefits from using a decentralized architecture for DPPs compared to a centralized one?

Decentralized architecture offers profound advantages for DPPs, primarily due to the intrinsic need for interconnectedness among its diverse systems. At its core, a product lifecycle is shaped by a multiplicity of contributors, each operating with their own unique systems and protocols. The exchange and trust of data between these parties is of paramount importance.

It's worth acknowledging that contemporary systems, like EDI, have been in use for over six decades. In that time, technology and architectural designs have undergone monumental transformations. The demand for trust, interoperability, security, efficiency, and speed has magnified significantly compared to sixty years ago, driving the necessity to modernize our architectural frameworks.

Centralized architectures, while essential for the internal operations of individual organizations, are inherently designed to function within the organization's boundaries, limiting their ability to share data with unverified or unknown third parties. This presents a challenge in the context of DPPs, where multiple organizations need to collaborate, share and work on the same set of data. The current process, which involves repeatedly sending data to different parties, validating it, and establishing connections, is susceptible to errors.

Decentralized architecture emerges as a solution by providing the infrastructure to share verifiable data across an ecosystem of organizations, extending beyond their individual perimeters. This new architecture supplements existing centralized systems, enabling them to connect to the ecosystem for secure, efficient, and trusted data sharing.

So, the key advantage of decentralized architecture lies in its potential benefits for the collective ecosystem rather than a single organization. Our experiences suggest that the way forward is to enhance existing centralized systems with decentralized features, allowing the entire ecosystem to benefit from improved security, efficiency, and speed in data sharing.

What are the main technological and/or regulatory barriers for the application of blockchain technology for DPPs?

One of the primary challenges for the application of blockchain for Distributed Product Portfolios (DPPs) is the disparate market landscape. Given the intricacies of blockchain technology, it can be daunting for organizations to identify and select the optimal solutions that will facilitate their DPP objectives effectively.

To address this, we at nChain advocate for the establishment of standards to ensure interoperability, supportability, and consistency for all parties interested in leveraging DPPs. The market boasts a multitude of diverse solutions, and regulatory bodies should not restrict entities from opting for their preferred choices. Instead, clear standards can provide a unified direction.

Creating a robust DPP system involves integrating various technologies, including IoT devices and AI, all tailored to the specific product or industry in question. Data standards can help ensure consistency across these different technologies, thus enhancing the effectiveness of blockchain utilization. For blockchain technology to be truly effective, it requires high-quality, consistent data, which could unlock considerable value by facilitating the sharing of trusted data without necessitating the context of each transaction.

Furthermore, there's a pressing need for enhanced education across the market and among regulatory bodies to foster a better understanding of blockchain technology. It's important to note that not all use cases apply blockchain in the same manner, nor are all public blockchains slow, restricted in scale, or plagued by volatile and expensive gas fees.

Factors such as financial speculation in cryptocurrencies, performance and scalability issues, and inadequate understanding of governance management have contributed to low adoption rates and a siloed approach to the implementation of this technology. Improved regulation surrounding the use of blockchain and increased education for regulators regarding the technology could help lower these barriers.

Regulations related to competition and data sharing also need revisiting to ensure that competitive organizations can collaborate when necessary. As critical stakeholders in DPP, public sector organizations, governments, and regulators need to develop their capabilities in this technology to drive broader adoption.

What are you views about the use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and/or other decentralized technologies for the implementation of DPPs? What are their respective advantages and disadvantages?

While DIDs and VCs are closely associated and specifically for an identity of a product or entity, NFTs provide for a different use case potentially as a mechanism for trade and engagement with consumers. The 3 technologies can be used in combination effectively. To leverage decentralized ID capabilities (DIDs, VCs) has significant advantages.

- Accountability - each organization that is part of a product lifecycle can have a DDD. As each organization transact and provide data in DPP, the identity of the organization can be verified using decentralized identity capabilities, thereby creating greater accountability for every transaction.
- Labour regulations compliance - organizations can use the same decentralized ID capabilities for their workforce so that every employee in the supply chain has a digital ID with their own VCs along with government issued identity VCs. This will enable organizations to be more accountable and transparent for each item they produce, who produces it and when the item goes to recycling, this can also demonstrate the data shared can be trusted.
- Verifiability – with DID and VC capabilities, an entity can share data specifically about the product. They control what they share, and the data is signed and verifiable that the data came from a specific entity/individual. This is particularly interesting for smaller/artisanal organizations where individual association with a product would enhance the value of a product and bring about direct, more equitable benefits to the individual. It could also be applied to carbon emissions and reporting.
- Inclusion – By providing the smallholders and individuals with a digital ID, they can be paid directly, rather than through middlemen and be able to collect benefits directly; they can also be rewarded for the right behaviour directly from organisations and consumers e.g., farming organically and regularly providing verifiable data.
- User control/Privacy/Confidentiality – by combining the decentralized identity capabilities in DPP, this provides strong abilities to manage confidentiality of information and user control. Unisot's solution already has a module enables decentralized ID. Every smallholder to large enterprise in a supply chain should have the ability to manage the identity of their products, their workforce and thus the confidentiality and privacy associated.

There are also disadvantages with using decentralized identity capabilities in the supply chain. It adds a level of complexity to both the user and the relevant processes. Not every transaction would require identity verification. Thus, a risk-based approach needs to be taken to understand which transactions would benefit from such capabilities and how to deploy them in use cases that drives value.

While nChain is known for its significant expertise in public blockchain technology with proven capabilities in DPP, NFTs and supply chain use cases, nChain will also be launching DIDs capabilities.

For IoT devices, cars and other devices where they are acting on behalf of an entity, decentralized ID capabilities provide the ability to directly associate a person with the device and the transaction that it conducts, bringing greater accountability to the transaction e.g., car buys a part, the owner of the car has provided VCs in advance that they own and authorize such a transaction. Accountability will become even more important as AI and other forms of machine learning become more advanced.

What are the key lessons learned from following a blockchain-based approach for the DPPs?

Blockchain-based approaches for DPP require a degree of cooperation for those who are part of the ecosystem. It requires multiple, potentially fully independent, parties to work together. While parties along the supply chain of a product must share data, there are often strong competitive dynamics, anti-competitive regulations and other issues at play that limit collaboration. Strong governance models and common standards are needed to facilitate this. Many blockchain-based supply chain pilots have failed to gain momentum and adoption not because of the underlying blockchain technology itself but because the projects often lack leadership, and business commitment due to the lack of business value, appropriate governance, regulatory framework and legal framework to bring about change that impact an ecosystem beyond a single entity. Blockchain technology can be transformational but to be effective, it must be driven by an ecosystem willing to bring about change.

Additionally, every product is different. Every supply chain, be it seafood or wind farming, has its own uniqueness and complexity. Technology solutions will need to be flexible and there are likely going to be multiple solutions that would cater to specific requirements of particular industries. Blockchain alone would not deliver the right applications catering to those industries. The blockchain approach for DPP is about building a common infrastructure – akin to the internet, road network or power grid. If organizations understand that blockchain forms the foundation of data sharing of which their individual industry and organizational specific applications sits on top of, then the blockchain based approach could deliver real benefits to the ecosystem.

Based on your experience, what are the best practices for implementing a DPP?

In our experience, we suggest starting with use cases that have alignment and buy in from key stakeholders. There needs to be a common goal and set of data that needs to be shared by all parties involved. There needs to be a common pain point – regulatory compliance, meeting targets etc. that all parties can agree upon to collaborate. The DPP needs to deliver specific value to each party so that they are incentivized to implement the DPP and use it. The need for organizations to be compliant with regulations often accelerate the deployment and adoption of such capabilities.

Seafood from Unisot is a good example of a solution on blockchain that addresses the different needs of different stakeholders in the seafood supply chain. Seafood (IS-SF) is compatible with seafood industry standards and procedures such as GS7 Global Traceability Standard (GTS) and ISO 72877/72875 "Traceability of finfish products" Standards provide a common language to identify, capture and share seafood supply chain data, ensuring important information is accessible and accurate. This module provides the tools required to obtain E2E global traceability from fish-eggs to consumer to recycling.

IOTA

Interview with Laura Kajtazi – Project and Regulatory Affairs Manager

Could you please briefly introduce IOTA?

IOTA is an open, feeless, scalable data and value distributed ledger technology (DLT)-based transfer protocol. IOTA is designed to overcome the limitations of traditional Blockchains such as Bitcoin. It aims to provide a scalable and sustainable DLT for applications and digital economies and as a result enable digital autonomy for everyone and everything. The IOTA core is a technology called the Tangle, which is a Directed Acyclic Graph functioning as a consensus algorithm that requires users to confirm previous transactions to complete their own IOTA transactions.

Currently, the IOTA protocol is at an Intermediate stage. Thereby, the IOTA network is managed by coordinator nodes, operated by the IOTA Foundation. Coordinators determine which transactions and data are included in the ledger, which is the list of token balances for all users. To be fully decentralized, IOTA is working on the Coordicide project, which aims to provide a new protocol (IOTA 2.0) that removes the coordinator need. As part of the evolution towards IOTA 2.0, is Stardust, an infrastructure layer for smart contract chains and multi-asset ledgers. To test the features of Stardust, the Shimmer network has been deployed as a staging environment before Stardust can be fully implemented as an upgrade on the IOTA mainnet.

How is IOTA leveraging blockchain technology to address the challenges of creating Digital Product Passports (DPPs)?

DPP collects information about a product during all stages of its life cycle and makes the data available as digital information. It is in brief a descriptive digital twin of a real asset attached to its digital representation. The DPP supports multiple actors to query or record the origin of a product, its authenticity, and sustainability compliance. This trustable data is crucial to enable end-users, governments, manufacturers, and other actors in a product life cycle to make environmentally focused decisions and help keep products longer in circulation, thus stimulating reparation, reuse and recycling and reducing the extraction of new resources. Providing trustable data that is tamper-proof is challenging, especially in a decentralized environment. To prevent this data from being tampered with, the IOTA Tangle can be used to ensure the auditability and immutability of the data in the DPP, which can be under control of multiple actors. The IOTA DLT offers services suitable for creating this auditability layer of the DPP, covering data integrity in an efficient and scalable manner.

Another challenge in creating DPPs is getting the right balance in terms of the information exchange and the data privacy of both personal and business data. During Phase 2A of the EU Blockchain PCP IOTA has produced together with Digimarc a Decentralized Blueprint for Digital Product Passports. Within that Blueprint IOTA implemented Decentralized Identifiers (DID) and Verifiable Credentials (VC), allowing digital signing transactions on the Ledger in compliance with those W3C standards. These components ensure that only relevant stakeholders to a product passport can write new information, based on their respective rights and thus ensure data sovereignty.

Further the combination of the components can ensure, by identifying the author of an event (via a DID), that the entity is 1) authorized, and 2) competent to report the specific event. This can help to certify that for example cotton used to produce a garment was indeed organic and increase the trust in the data stored in the DPP.

Apart from that, an important factor in the context of the circular economy and in the implementation of the DPP is human behaviour. To achieve more environmentally conscious behaviour, incentive systems can be helpful. Implementing these in connection with DPP is not always easy. Tokenization in combination with IOTA Smart Contracts can bring the missing adaptability and flexibility. For instance, parameters can be programmed to reward green behaviour with tokens.

Based on your experience, are there any relevant benefits from using a decentralized architecture for DPPs compared to a centralized one?

Introducing a decentralized system architecture for DPPs involving multiple parties with little need to trust each other is going to revolutionise the current fragmented and untransparent value chains. With decentralization the trust issues are being tackled. DLT's are means to create and base actions upon a digital, shared truth. By decentralizing the shared truth and the consensus over it, the system avoids having to trust rulers. There is no central entity owning all digital product passport information, but instead multiple actors are cooperating, acting as data controllers, having the DLT as a layer of trust. In fact, each stakeholder keeps their own sovereignty of their data they are generating, but this data can be trusted through commitments of their recording/register, which is being added to the DLT, enabling data verification without "calling home". Through decentralization the security and reliability of value chain data are enhanced, which is going to be crucial for the Circular Economy. In a decentralized network, the reliability of information is ensured by the network's consensus rules. This feature shall limit data misuse and manipulation. Having a decentralized rather than a centralized architecture where one system/actor manages all information about a product centrally further mitigates the single point of failure, a well-known security risk in centralized databases. As the whole system is distributed across many devices (nodes) there is neither a single point of failure nor a single point of attack. Finally, a decentralized architecture, specially one which involves DLT as IOTA, enables seamless participation of multiple actors without the need of complex onboarding processes or "a priori" knowledge.

What are the main technological and/or regulatory barriers for the application of blockchain technology for DPPs?

Many approaches and standards are already now available, but there is no universally acknowledged standard approach in relevant technical components like digital credentials. Agreeing on a set of standards, that guarantee minimal interoperability, is crucial for creating a portable and interoperable system and enabling efficient value chains. As an example, there are different DID approaches which can lead to different storage locations and management approaches. Through efforts in achieving a harmonized standardization the DPP system can scale. To further ensure interoperability among blockchain itself, efforts to expand the technology so that it can interoperate with other blockchains, and systems is worth emphasizing. At IOTA we are also aiming to build our technology in a way so that it promotes interoperability. For instance, within our Stardust protocol, recently it has been launched the ShimmerEVM test chain on the Shimmer Testnet (Testnet for Stardust). Within the Shimmer EVM Smart Contracts enable seamless and bridgeless native asset transfer between Shimmer L1 and EVM chains, which build the basis for extended EVM (Ethereum) compatibility. We are also planning to fully align our IOTA Identity framework with the European Digital Identity Framework (eIDAS) recommended standards (and European Blockchain Services Infrastructure (EBSI) standards).

Generally, from a regulatory perspective it can be said that for some technological approaches for e.g., Non-Fungible Tokens (NFTs) things are unclear. The unknown of future regulation can of course hinder the adoption of approaches in blockchain. But regulation can change anytime also in parts that are already defined. So most importantly is the support of government and regulators to promote blockchain adoption for sustainability, to ensure that organizations and individuals feel encouraged to build on blockchain. Here it's worth mentioning that to receive their support and direction they first need input from practitioners and research groups. That said, in summary a continuous and constructive dialogue between regulators, practitioners, and researchers is needed to shape the future of blockchain-based DPP systems so that they can add value to sustainability and society.

What are your views about the use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and/or other decentralized technologies for the implementation of DPPs? What are their respective advantages and disadvantages?

NFTs, DIDs and VCs all represent valuable technologies for the implementation of DPPs. To identify the advantages of each of the technologies it is important to differentiate their core functionalities.

The DIDs in combination with VCs can be used to identify and trust different entities (Organizations, Applications, Devices, etc.) when implementing DPPs. For instance, certificates that describe a product can be issued by the product owner in the form of electronically signed, trustworthy verifiable credentials and linked to the DPP. Verifiable credentials contain claims about subjects and enable the verification of selected claims

about a product. While DIDs in combination with VCs can help proving identities, and are suitable for any kind of identity issue, NFTs are proving what someone owns and encodes ownership of an asset in a digital format. Thus, NFTs can be used for ownership-based access management but not for all identity use cases.

For example, an NFT could be built as a digital twin of a product that includes the product's history digitally available as an NFT. With the help of Smart Contracts, the DPP could for example provide rewards for a green behaviour linked to a product, such as issuing a token when the product is recycled or distributing immutable carbon credits to actors that demonstrate green behaviour which can provide flexibility and opens up multiple further DPP specific use cases. However, using NFTs is not ideal when looking at data for individuals. Data privacy may be violated as NFTs are usually anchored on a public blockchain. Thereby specifically the right to be forgotten according to GDPR stands in contradiction to the aspect of immutability of blockchains. Furthermore, there is no regulation in place right now which may impose a potential barrier as it is unknown how regulation will frame the future use of NFTs for DPPs. In contrast, for DIDs some regulation is already moving forward such as eIDAS 2.0. Moreover depending of course what is the underlying DLT infrastructure this might influence scalability and costs. At IOTA right now we are aiming with the Stardust Tokenization Protocol Framework to support many actions in a scalable, green, and feeless way.

Still depending on what the aim is within the DPP system one is building here it varies what is most suitable of the aforementioned technologies.

What are the key lessons learned from following a blockchain-based approach for the DPPs?

The first question as with every technology that is planned to be used is of course, what exactly you want to achieve and how blockchain as a technology can be the right approach. One of the points to look at initially is whether a decentralized infrastructure is needed. In cases where decentralized infrastructure increases trust, the technology can be considered just as for our examples in DPP. There can be uncertainty as to whether the materials of a product have been properly identified and tracked where blockchain can be for example helpful. The integration of incentive systems can also bring many benefits by motivating more sustainable behaviour. One should be considerate with the choice of the type of blockchain and look at aspects such as scalability, sustainability, and data security beforehand. For instance, it doesn't bring many benefits to model an incentive system if the energy overhead of a certain blockchain consumes an excessive amount of energy and would offsets energy saving aimed through greener incentivized behaviour. As we have seen in the questions before, you also must think about what you want from the DPP system, because NFTs can't replace DID completely when it comes to the data of individuals. Here one has to be careful and keep in mind exactly what the respective vision is and where which frameworks fit better with respecting for example data privacy.

Based on your experience, what are the best practices for implementing a DPP?

One best practice is for sure finding the right stakeholders you can actually build a trusted DPP system with. Although blockchain offers many possibilities the Digital Product Passport, it entails more than just the blockchain. Finding the right stakeholder to work together on development and testing is key. This counts for example employees and partners in. Looking at the partners specifically they can bring key knowledge from a specific domain, be it textile, plastics etc. Importantly choosing a domain where I already have valuable stakeholders with whom I can achieve my target is an advantage. Next is defining clear criteria and a project plan. Defining clear objectives for developing a DPP, and a plan of what you would need to do to actually reach them and how to measure their successful achievement, will provide you guidance throughout the implementation of the DPP. Important criteria to look at are for example interoperability, scalability, sustainability, data security and privacy and commercialization just to mention a few. Important to keep in mind is the compliance with regulation and where possible coming together with regulators to shape the future of DPP with legal frameworks (such as the future Regulation on Ecodesign for Sustainable Products (ESPR) of the EU) that do bring us forward. If we aim for adoption that is future proof, we have to be compliant. However, if we notice that regulation is unclear in some points or hinders a valuable development for society, we need to come together with regulators and other actors and see how to change or shape regulation for the better.

What is IOTA being building in relation to DPPs in the context of the European Blockchain Pre-Commercial Procurement? Please provide a high-level overview of your project proposition.

In the last Phase 2A of the EU Blockchain PCP as mentioned already in Question 2 IOTA has produced together with Digimarc a Decentralized Blueprint for Digital Product Passports. Within that Blueprint IOTA implemented Decentralized Identifiers and Verifiable Credentials, allowing digital signing transactions on the Ledger in compliance with those W3C standards. The components developed ensure that only relevant stakeholders to a product passport can add new information, based on their respective rights, and thus ensure data sovereignty.

Further the combination of the components can ensure, by identifying the author of an event (via a DID), that an entity is 1) authorized, and 2) competent to perform the specific event. This can help to certify that the material used to produce a product was indeed what it claimed to be and increase the trust in the data.

Apart from that in the previous Phase 2A in partnership with UPC, the Technical University of Catalonia, we have developed a Digital Product Passport for Consumer Electronics, supporting the porting of their solution to the IOTA Tangle. The developed solution included a workbench tool, an end-user software that enables information about consumer electronics (i.e., serial numbers, refurbishment status, components status, usage hours, etc.) to be captured. The Workbench communicates with a device hub, which interconnects with the IOTA Tangle to immutably store relevant proofs and to allow their verification by third parties, thus guaranteeing DPP integrity.

A DPP prototype for electronic products, and more specifically for ICT products shall be developed and tested in Phase 2B beyond our results achieved in Phase 2A. The updated prototype for Phase 2B incorporates a set of smart contracts to regulate management of verifiability information, including verification for audit purposes.

In general, beyond the preliminary testing of the DPP prototype systems in Phase 2A, we aim at the involvement of real economic operator actors of the circular economy in Phase 2B as “testers” of the DPP prototype system and looking at the interaction of the DPP within the current EBSI network.

We might look for other industries to approach during Phase 2B as we make progress in creating new liaisons such as with CIRPASS.

What is next for IOTA under the European Blockchain Pre-Commercial Procurement?

To give an overview of the whole process of the pre-commercial procurement, it is worth noting that it consists of three phases. After being selected, along with six other projects out of 35 applicants, for Phase 1 of the EU Blockchain PCP where we created a design to implement the project, and successfully completing prototyping and lab testing in phase 2A of the EU Blockchain PCP, the IOTA Foundation, along with two other projects, was selected for the final phase 2B for product finalization and the field testing. Phase 2B has different testing cycles which need preparation and actual testing. Right now, we are at the very beginning of this Phase where we have defined our Work plan and are doing the actual preparation for testing. Once the preparation is completed, we go into testing, we then head to the next testing preparation and actual testing phase. Phase 2B will last one year. The difference to Phase 2A is the difference in the testing environment. In Phase 2B the testing environment aims to get close to reality. Points that would be of importance are for e.g., the involvement of real-world stakeholders and the actual integration with the current EBSI software. To accelerate the development and uptake of IOTA on the EBSI solution, the IOTA Foundation, as indicated already before, joined forces with partners to speed up the work on the development of different use cases and to enable testing with real users.

DYNE

Interview with Andrea D’Intino, DYNE

Could you please briefly introduce your use case?

The Interfacer platform is an open-source solution enabling teams working open source hardware to collaborate. The main target of Interfacer is Fab Cities: an innovative urban model that re-localises production to the city and its bioregional context, by empowering communities with the technology to build their own sustainable, innovative and regenerative urban futures.

The main features of Interfacer:

- The whole lifecycle of products is traced in a DPP, all the raw materials, the services and designs used in the products are traced too. The lifecycle is described using the ValueFlows ontology.
- Upon sign-up, each user generates a DID (example) containing a set of public keys and an EVM blockchain address. Every user interaction on the platform is cryptographycally signed, applying the end-to-end cryptography principle.
- The platform uses GraphQL and data can be queried to produce OpenData.

Dyne.org has been working on the DPP platform since 2019, the development started in the H2020 project Reflow (success story) and the Interfacer project. We have presented the platform at the WCEF 2023 and at at Maker faire 2023.

How is your use case leveraging blockchain technology to address the challenges of creating DPPs?

Blockchain is used to notarized the hash of a version of the DPP on chain: the DPP itself is a rather large JSON object which can be retrieved at anytime and matched with a hash stored inside a transaction on chain.

At the same time, W3C-DIDs can also be stored on chain, in order to provide certainty for the data provenance.

We also implemented a prototype of economic system named CreativeFlows that allows user to gain tokens based on their activity and collaboration on the platforms.

Based on your experience, are there any relevant benefits from using a decentralized architecture for DPPs compared to a centralized one?

A decentralized ledger is crucial for DPP's traceability, resilience and certainty of origin. A centralized storage system without distributed notarization is subject to change by the administrator of the storage system, thus jeopardizing the trust that is central to the aims of a DPP.

What are the main technological and/or regulatory barriers for the application of blockchain technology for DPPs?

The main challenge currently is the lack of standardization: while the EC has clearly expressed its goal to increasingly require DPPs in several industries, the standardations efforts (such as Cirpass) are still in their infancy. The current DPP landscape is highly fragmented and characterized by use-case specific, non-interoperable solution. A strong regulatory effort, coupled with a strong industrial reaction, is cornerstone in for the interoperability - and thus the mass adoption - of a technology like the DPP.

On the technological side, the components are mostly there: cryptography, distributed storage and blockchain, coupled with SSI/Identity technologies such as W3C-DID and W3C-VC to manage the data policies involved in writing a DPP.

What are you views about the use of NFTs, Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and/or other decentralized technologies for the implementation of DPPs? What are their respective advantages and disadvantages?

NFTs can find application to define digital twins of physical object, this can place a pivotal role in traceability of resources, allowing consumers to make better informed choice of the provenance of the products they are purchasing.

The W3C-DID and W3C-VC standards, couple with end-to-end cryptography are used respectively to enable complete traceability in the DPP data entries and to enact CRUD policies, enabling each actor to only perform the operations they have been enabled to make.

The main downside of these technology, especially if combined, is the lack of standardization and interoperability: while the standard for DIDs and VCs are mature enough to offer a resilient data generation on *single platform*, several blocks are missing to offer data and policy interoperability.