

TRUSTyFOOD

Strategic Technological Convergence with Blockchain in Agri-Food



Funded by
the European Union

www.trustyfood.eu



WHITE PAPER

“Strategic Technological Convergence with Blockchain in Agri-Food”

Views and opinions expressed do not necessarily reflect those of the European Union or Research Executive Agency; neither the European Union nor the granting authority can be held responsible for them

Table of contents

Introduction	3
Chapter 1 – Data Spaces	4
1.1. Data Spaces in EU landscape: Technological and business perspectives of a promising technology	4
1.2. Data Space on Agrifood Applications.....	6
1.3. Exploring the potential impact of the Blockchain Technology in a data sharing scenario implemented through a Data Space.....	8
1.4. Conclusions and future outlook.....	11
Acknowledgment.....	12
References	13
Chapter 2 – EU Digital Product Passport (DPP) for the Agri-Food Industry	14
Executive Summary.....	14
2.1. Introduction.....	15
2.1.1. What is the DPP	15
2.1.2. How does it work in practice	15
2.2. Interaction with blockchain.....	16
2.3. DPP for the Agrifood sector	17
2.3.1. Opportunities	17
2.3.2. Current limits	17
2.4. DPP with and without Blockchain	18
2.5. Conclusions.....	19
Acknowledgments	19
Chapter 3 – AI and Blockchain Synergies: Outline, Applications in Agri-Food, and Future Use Cases	20
3.1. Brief Outline of Current AI and Blockchain Synergies.....	20
3.2. AI and Blockchain Applications in the Agri-Food Sector.....	21
3.3. Key agri-food use cases powered by blockchain standards and AI.....	22
Chapter 4 – Digital Identity	24
4.1. Self-Sovereign Identity	25
4.2. Open standards supporting SSI.....	28
4.3. The EU Wallet and EU Projects.....	28
References	29

Introduction

White Paper 3 examines the strategic convergence of blockchain with emerging digital technologies or new trends as a means to address some of the most pressing challenges in Europe's agri-food sector.

The paper focuses on four key technological intersections, particularly: Data Spaces, Digital Product Passport (DPP), Artificial Intelligence (AI) and Self-Sovereign Identity (SSI).

Each topic is treated as a self-consistent Paper, emphasising the author(s) and eventual acknowledgments. However, these convergence themes are explored not as isolated innovations but as interdependent components of a digital transformation pathway toward a more transparent, efficient and sustainable food system across the European Union.

Chapter 1 – Data Spaces

Authors: **Elisa Rossi¹, Antonio Caruso¹, Mariarosaria Russo¹, Delia Milazzo¹, Marianna Faraldi²**

¹ Engineering Ingegneria Informatica S.p.A., Italy

²TECNOALIMENTI S.C.p.A., Chief research officer, Italy

1.1. Data Spaces in EU landscape: Technological and business perspectives of a promising technology

“Data is reshaping the way we produce, consume and live. It is the basis for creating many innovative products and services, driving productivity and resource efficiency gains across all sectors of the economy” [1]. That is the *incipit* of the COMMISSION STAFF WORKING DOCUMENT on Data Space, and it clearly summarizes the need of exploiting data. Data, properly analyzed, constitutes information, and more information are available, more conscious decisions can be taken. With the increased fragmentation of technologies, expertise, data, sharing data becomes a need, but also an opportunity.

In this sense, the Data Spaces has been conceptualized as *“A distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases”* [2]. In other words, Data Spaces amplify the opportunities lead by the pivotal technologies (i.e., Internet of Things, Digital Twins and Artificial Intelligence) in a controlled and reliable manner, in full compliance with current regulations on ethics and privacy, guaranteeing European values, democratizing access to data.

The Data Space technology is one of the pillars of the European strategy for data (2020) [3] sets out the path to the creation of a genuine single market for data in which both personal and non-personal data, including sensitive business data, will be able to flow seamlessly across borders and sectors in a safe and secure manner, in line with EU rules and values, for the benefit of European businesses – notably AI innovators – and citizens. This will enable the EU to become a leading role model for a society empowered by data to make better decisions – in business and the public sector. To realise this vision, common European data spaces are being established to facilitate trusted and secure data pooling and sharing in strategic economic sectors and domains of public interest. The sectoral and domain-specific common European data spaces will gradually be interconnected to form a pillar of the single market for data. This will allow for the development of more data-driven, evidence-based policies across the EU.

Four key European organizations (IDSA, Gaia-X, FIWARE, BDVA/DAIRO) have formed an alliance creating one voice and a common framework to make data spaces happen. Together, the DSBA represents 1,000+ leading industry players, associations, research organizations, innovators, and policymakers worldwide. With its combined cross-industry expertise, resources, and know-how, the DSBA drives awareness and technology adoption, shapes standards and enables integration of data spaces across industries. (https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/1_introduction)

- IDSA - International Data Spaces Association (<https://internationaldataspaces.org/>), which main aim is to establish a global standard for international data spaces (IDS) and interfaces, as well as fostering certifiable software solutions and business

models, that will drive the data economy of the future across industries. Among key initiatives held by IDSA, the collection of preliminary Data sharing platforms and Data Spaces pilots is available in the Data Space Radar. Together, they represent 1,000+ leading key industry players, associations, research organizations, innovators, and policy makers expert in data sharing platforms and data spaces concepts. Thankful to DSBA activities, a common framework, based on existing architectures and models, will be promoted, leveraging each other's efforts on infrastructure and implementations to make data spaces happen. This has been also part of the recently published DSBA - Technical Convergence Document.

- Gaia-X - European Association for Data and Cloud AISBL (<https://gaia-x.eu/>), representing one of the first examples of European Data Spaces across Europe as the first federated and secure data infrastructure, whereby data are shared, with users retaining control over their data access and usage. The Gaia-X Association enables the creation of data spaces through the work of the regional hubs. Each hub has the objective to focus on its regional strategic data spaces and develop concrete business cases creating consortia of member companies around them.
- FIWARE (<https://www.fiware.org/>), a non-profit organization that drives the definition and encourages the adoption of open standards (implemented using Open Source technologies) that ease the development of smart solutions (digital twins, data spaces) across domains.
- BDVA (Big Data Value Association)/ DAIRO (Data, AI and Robotics) (<https://bdva.eu/dairo/>), ambition is to closely collaborate with other communities to jointly engage at the intersection of the key disciplines of Data, AI and Robotics. It was established in 2020 from the previous BDVA to better engage the European Commission on topics such as the Europe fit for a Digital Age agenda, the Green Deal and the Data Strategy. Furthermore, the Association benefits from a privileged position in supporting the establishment of networks and forms of collaborations between Digital Innovation Hubs and i-Spaces in Europe and supporting the development of a European Data Space. The overarching objective of DAIRO is to *“boost European Artificial Intelligence (AI), Data and Robotics research, development and innovation and to foster value creation for business, citizens and the environment”*.

Further relevant initiatives on Data Spaces are:

- the DSSC – Data Space Support Centre, supported by the Digital Europe Programme, will facilitate the deployment of Common European Data Spaces, to enable data reuse within and across sectors, fully respecting EU values, and contributing to the European economy and society. Among its objectives, the DSSC will deliver iteratively the Data Spaces Blueprint, composed of common building blocks encompassing the business, legal, operational, technical and societal aspects of data spaces. The Blueprint continuously evolves with a user-centric approach, as the result of co-creation with the stakeholders.

1.2. Data Space on Agrifood Applications

The application of Data Spaces (DS) technologies in the agrifood domain is transforming this sector by enabling seamless data exchange, optimizing resource use, and enhancing sustainability.

This sector is evolving towards the digital transformation and several R&I projects are pioneering the development and implementation of Data Spaces to support efficiency, transparency, and environmental responsibility. Among them, the CLARUS, DIVINE, and AgriDataSpace projects stand out for their contributions to sustainable food manufacturing and supply chain optimization. Each of these initiatives implements DS with unique methodologies and objectives, offering valuable insights into the role of data-driven solutions in agrifood applications. While CLARUS focuses on AI-driven resource optimization in frozen food production and meat by-product logistics, DIVINE explores secure and interoperable data-sharing frameworks, and AgriDataSpace works towards creating a federated data ecosystem for the agricultural sector. By analyzing their distinct approaches, implemented scenarios, and technological innovations, this section highlights the impact of DS in agrifood and underlines the differences and peculiarities of each project.

The CLARUS project aims to connect the Sustainable Manufacturing Paradigm in the food industry with AI-based applications, by developing a platform with high communications and processing capabilities, promoting the use of standardized open protocols and data models that will allow resource consumption assessment and traceability for food industry processes. Communications within the platform will be enabled through the design and development of the CLARUS Data Space, a secure, trusted, standardized, and interoperable environment for data exchange that will facilitate seamless communication between all the stakeholders involved in the supply chain while ensuring data sovereignty, confidentiality, and compliance with European regulations.

CLARUS focuses on two real-world key pilots within the agrifood sector, both of which stand to benefit significantly from the implementation of the DS scenarios. The first pilot addresses the substantial energy and water consumption associated with frozen food manufacturing by integrating AI and data technologies to optimize production efficiency, reduce waste, and improve resource management. The DS will facilitate the data exchange feeding the collaborative platform for data-driven decision-making, enabling manufacturers to analyze real-time data, benchmark sustainability indicators, and implement predictive analytics to mitigate inefficiencies. The second pilot faces meat by-product industry, where sustainability challenges include energy-intensive operations and transportation inefficiencies. In this scenario, CLARUS seeks to enhance logistics coordination, minimize heat loss, and improve the overall sustainability of rendering processes and the DS will enable real-time tracking, process optimization, and data harmonization across stakeholders, ensuring enhanced transparency and sustainability throughout the supply chain.

The Data Space in CLARUS project plays a key role in transforming agrifood industry operations by offering interoperability and standardization, enabling different entities—manufacturers, suppliers, and regulators—to exchange and utilize data efficiently. It also allows real-time data processing, ensuring timely decision-making and process optimization, reducing waste, and enhancing sustainability. Through compliance with IDSA (International Data Spaces Association) principles, the DS ensures that businesses retain control over their data while fostering collaboration overcoming fears and reluctances related to sharing their data.

The agrifood industry is at a turning point where digital transformation can directly impact global sustainability efforts and in this perspective the DS is not merely a technical infrastructure but a strategic enabler for achieving the European Green Deal goals. By providing a robust framework for data exchange and AI-driven optimization, the DS ensures that agrifood businesses can achieve lower carbon footprints by optimizing energy and water use, reduced food and packaging waste through real-time monitoring and process refinement, improved resilience and efficiency across supply chains through enhanced logistics coordination, and compliance with sustainability regulations by offering a structured approach to measure and improve sustainability performance.

The DIVINE project aims to create an impact in the agricultural sector by developing an Agricultural Data Space Ecosystem (ADSE) that facilitates efficient data sharing and integration between private and public stakeholders. By adopting a standardised and interoperable framework, primarily based on IDSA, the project aims to increase trust, transparency and data sovereignty while ensuring the secure exchange of agricultural data.

Through real-world pilots, DIVINE introduces a modular and scalable platform that integrates heterogeneous data streams to enable traceability, compliance and monitoring. DIVINE is also showcasing novel solutions such as the Divine Dashboard for data and decision visualisation support, a data integration and management bundle powered by an Apache Kafka-based data pipeline, the Agricultural Information Model (AIM) specifications to ensure semantic data interoperability and insights provided by data analytics services to a precision agriculture. In coordination, these devices improve resource optimisation, farm performance and sustainability environment, providing stakeholders with valuable information to increase farm productivity and profitability. To assess market opinion on the ADSE concept, the DIVINE consortium conducted market surveys on business models, shared benefits and data monetisation plans. The goal of the work done was to collect the views of the whole consortium to inform the development of a comprehensive business plan. The primary objective of the survey was to gather key fundamentals which are essential for identifying potential broader commercialisation opportunities across the activities of DIVINE. The purpose of the survey is to elicit the necessary information that is critical to the development of a robust and comprehensive business strategy.

The survey results showed a strong preference among stakeholders for a freemium strategy, offering free access to typical data services and charging for higher value advisory and analytical solutions. Stakeholders noted the very high value to be gained from sharing data to improve farm asset management, benchmarking and decision support, and identified the potential for ADSE to facilitate better access to accurate and reliable agricultural information. However, respondents also identified key barriers to adoption, including lack of awareness, high costs, connectivity and infrastructure limitations, and interoperability issues. These issues highlight the need for affordable, scalable and easy-to-use solutions that can support the wider adoption of agricultural data ecosystems. Despite these challenges, the agricultural industry is showing increased willingness to embrace data spaces, supported by growing demand for sustainable agriculture, government initiatives and rapid technological advances. Projects such as DIVINE are important in filling market gap by creating collaboration, improving data protection and providing low-cost digital solutions tailored to the agricultural sector.

By fostering innovation and improving efficiency, ADSEs can make the agricultural sector more productive, drive economic development and help ensure the long-term sustainability of the sector. Going forward, strategic investments in infrastructure, stakeholder engagement and policymaking will be essential to unlock the full potential of data-driven agriculture and achieve large-scale adoption of digital ecosystems.

1.3. Exploring the potential impact of the Blockchain Technology in a data sharing scenario implemented through a Data Space

The data economy based on the digitization of information in all sectors of the European economy pushes research and innovation to develop new value-added services and data-driven digital infrastructures, towards the increase of business opportunities for companies operating in different markets by making a large amount of data available [4]. A data economy according to both economic and social indicators, represents an opportunity for economic growth in various sectors including health, food security, climate and resource efficiency.

In this context, the concept of Data monetization, from Gartner [5] is defined as *'the process of using data to obtain quantifiable economic benefit [...] (including) using data to make measurable business performance improvements and inform decisions [...], data sharing to gain beneficial terms or conditions from business partners, information bartering, selling data outright (via a data broker or independently), or offering information products and services (for example, including information as a value-added component of an existing offering).'*

The Data Space technology has been developed to support and facilitate the data economy, providing a structured framework for managing and sharing data. The Data Space enables seamless data exchange across different systems and organizations, thereby expanding opportunities for data monetization through innovative combinations and applications of data.

The *de facto* standard in Europe for Data Spaces is the IDS Data Space model, which defines the components [6] a Data Space should have to cover the functionalities [7] proper of the technology, and the roles [8] that may assume its stakeholders. Among the Data Space components, the IDS Clearing House [9] plays the role of logging service that records information relevant for clearing and billing data transactions as well as usage control within the Data Space. Based on the interactions between Data Providers and consumers recorded by the Clearing House, billable data usage is forwarded for settlement avoiding the risk of unrecognized transactions. In other words, the Clearing House is a generic, cross-domain service that receives information about transactions, participants and references to any existing legal contracts, stores this information in an non-reputable, verifiable form, and makes it available to the participants.

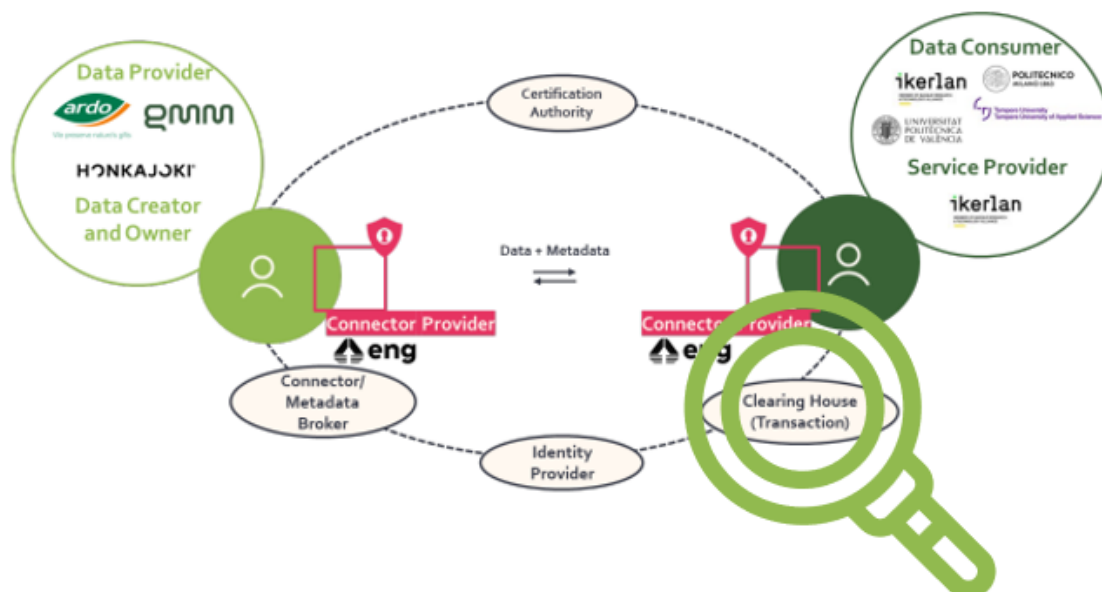


Figure 1: CLARUS Data Sharing Infographic

TRUSTyFOOD's readers would have likely made a bridge among the Data Space and the Clearing House component definition and the blockchain technology. Many concepts are recurrent within the two technologies, Table 1 resumes the similarities.

Table 1: Similarities among Blockchain [10] and Data Space technologies

	<i>Blockchain</i>	<i>Data Space</i>
<i>Transparent</i>	Every node of the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks it's valid, then it's added to the ledger. This promotes transparency and makes it corruption-proof.	At the basis of Data Spaces there is and there must be trust. Every actor is required to be assessed and certified before being granted access to a reliable data exchange ecosystem.
<i>Decentralized</i>	The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead a group of nodes maintain the network making it decentralized.	The architecture of the Data Spaces is decentralized with respect to data storage and does not impact on the actual data storage. It therefore promotes the decentralization of data storage, which means that the data physically remains with the respective data owner until they are transferred to a trusted party.
<i>Security</i>	As it eliminates the need for central authority, no one can just simply change any characteristics of the network for its benefit. Also using encryption ensures another layer of security for the system.	All the application components of the Data Spaces are based on and must comply with the most up-to-dated security measures (the technical components necessary to establish a Data Space are certified)
<i>Distributed</i>	The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.	From the DSSC definition of Data Space [2]: A distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases.
<i>Consensus</i>	Every blockchain thrives because of the consensus algorithms. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decisions.	The Data Owner specifies in a contract the restrictions on the use of its data before sending them to the recipient (Data Consumer), in line with the principle of Data Sovereignty. The Data Consumer before consuming data must accept these limitations.
<i>Faster settlement</i>	Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster, which saves a lot of time in the long run.	The Data Space is not managing payments.

Being based on the same pillars, and applicable to any domain, could it make any advantage to integrate the Blockchain and the Data Space technologies? How can these technologies be integrated?

The proposal could be to adopt the Blockchain technology instead of the IDS Clearing House to manage transactions and support data monetization. In this sense, once integrated, the Data Space facilitates data sharing, while Blockchain ensures the data sharing is secure, verifiable, and transparent. Furthermore, Blockchain's smart contracts can automate transactions, ensuring that payments are made only when data meets the criteria defined by the Data Owner. The payment management, as blockchain feature, is unexplored in the IDS framework, hence could constitute the main selling point of the combination of the technologies.

On the use cases aspect, Blockchain is often adopted for tracking purposes, in the Agrifood sector, it has been applied for instance to Olive Oil Traceability [12], with many commercial applications (e.g. in Italy Alce Nero¹, Coricelli² among the others). The Data Space technology as well is suitable for traceability purposes [13], but as per writer's knowledge there isn't any commercial application in the Agrifood domain so far. While the Blockchain in the domain has commercial application, and is recognized as a secure and trusted way to track products lifecycle, the Data Space has not yet been exploited at least on a large scale. This gap may be covered in the near future thanks to other concepts frequently associated with Data Spaces such as the Digital Product Passport (DPP)³: EU is introducing as part of the Circular Economy Action Plan, some indications related with the DPP, starting from the sectors that mostly impact climate change, but progressively also Agrifood will be covered.

Lastly, it should be noted that in the last IDS RAM4.0 [15] (i.e., the last architectural model released by IDSA) the Clearing House has not be included anymore, and its functionalities have been assigned to other components. An integration with the blockchain technology could be explored to shift the functionalities from the Clearing House, without compromising the functioning of the other Data Space components.

¹ https://www.alcenero.com/pages/blockchain-olio?srsId=AfmBOoq5CBiuw5ZkRgBa9ZRaO-getZWEP6i1JQgbhz_rVQeoAuybx-kM

² <https://blockchain.coricelli.com/>

³ Digital Product Passports (DPPs) are virtual passports of goods, designed to collect and share data about a product and its supply chain across the entire value chain. DPPs enable all stakeholders, including consumers, to gain a deeper understanding of the materials used in products and their associated environmental impacts. [14]

1.4. Conclusions and future outlook

The Blockchain technology can be integrated with the Data Space technology, in particular can replace the functions of an IDS Clearing House by enabling decentralized and secure data exchange. Although there could be many advantages and use cases, such technologies integration also presents certain challenges that must be addressed to fully realize its potential. These challenges include:

- **Scalability and Performance:** One of the primary concerns is Blockchain's scalability. The technology's ability to handle large volumes of transactions efficiently is crucial. Blockchain networks, especially those using consensus mechanisms like proof-of-work, can struggle with high transaction loads, potentially leading to slower processing times and higher costs. This performance issue is compounded by the need for consensus across multiple nodes, which adds complexity and can affect the overall efficiency compared to traditional clearing houses.
- **Privacy and Data Protection:** Blockchain's inherent transparency can conflict with the need for privacy in sensitive data exchanges. While the technology provides a transparent and immutable ledger, ensuring that confidential data remains protected requires advanced privacy-preserving techniques, such as zero-knowledge proofs. Balancing transparency with privacy is essential to maintaining data protection while leveraging Blockchain's benefits.
- **Regulatory Compliance and Governance:** The decentralized nature of Blockchain can complicate adherence to existing regulatory frameworks, which are typically designed for centralized systems. Adapting these regulations to fit a decentralized model is a complex task. Additionally, establishing clear governance and accountability structures within a decentralized system presents challenges. Defining roles, responsibilities, and decision-making processes becomes more complex when traditional hierarchical structures are replaced with decentralized ones.
- **Integration Complexity and Interoperability:** Transitioning from the IDS Clearing House to a Blockchain-based system involves significant integration efforts. Existing systems and workflows need to be adapted to accommodate the new technology. Ensuring that Blockchain systems can interact seamlessly with other systems and standards used in data exchanges is also critical. This may require substantial development and customization to achieve effective interoperability.
- **Cost of Implementation and Technical Expertise:** Implementing Blockchain technology can be costly, involving expenses related to technology development, deployment, and training. Additionally, Blockchain requires specialized knowledge, which can be a barrier if organizations lack personnel with the necessary expertise. This need for specialized skills impacts both the initial setup and ongoing maintenance of the Blockchain system. Same applies to Data Spaces.
- **User Adoption and Training,** i.e., the transition to a new system, may face resistance from users accustomed to the existing IDS Clearing House processes. Ensuring that users are adequately trained and comfortable with the new Blockchain system is essential for a smooth transition and effective ongoing operation.
- **Adoption reluctance:** One of the key challenges in integrating blockchain with data spaces is the prevailing scepticism surrounding data spaces adoption. Many enterprises remain hesitant to embrace data-sharing ecosystems due to concerns over governance, interoperability, and tangible business value. The concept of decentralized, controlled data

exchange is still in its early stage, and widespread adoption has yet to be achieved. Introducing blockchain into this equation adds an additional layer of complexity. While blockchain offers benefits such as enhanced data integrity, traceability, and security, it is often perceived as an over-engineered solution with unclear return on investment. The combination of these two technologies risks being seen as too ambitious. This challenge is not only technical, as previously described, but also cultural and strategic: convincing stakeholders of the practical applicability and business value of such a dual-technical approach is a hard task and the success will depend on demonstrating clear, low-friction use cases, addressing concerns around scalability and cost, and fostering trust in an ecosystem that many organizations are still wary of and this could be done through future European initiatives and through the communities and networks described in Section 1.

By addressing these challenges proactively, organizations can leverage Blockchain to create a more efficient, transparent, and secure environment for data sharing and collaboration, ultimately driving innovation and progress in the industry, particularly within the context of the Agrifood EU sector. The Agrifood Sector stands to benefit by enabling decentralized, transparent, and secure data sharing, while Blockchain can foster greater collaboration and efficiency within the sector.

Acknowledgment

The project would like to thank the external contributors to this paper. We express our gratitude in particular to Engineering Ingegneria Informatica, contributor in representation of the projects funded by the European Union CLARUS (Horizon Europe, grant agreement No. 101070076) and DIVINE (Horizon Europe, grant agreement No. 101060884), for the valuable support in the definition and development of this Chapter.

References

- [1] COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces, 2024, available online at:
file:///C:/Users/erosi/Downloads/Staff_Working_Document_Z5HILQr82Y8IzJyLoIHQIEzc_101623.pdf
- [2] A. Poikola, B. Verdonck, R. Joosten, T. Guggenberger and S. Salminen, "DSSC Glossary," September 2023. [Online]. Available:
<https://dssc.eu/space/Glossary/176553985/DSSC+Glossary+%7C+Version+2.0+%7C+September+2023>
- [3] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>, accessed in February 2025
- [4] Fessl, A. et al. (2024). Supply Chain Data Spaces–The Next Generation of Data Sharing. In: Haber, P., Lampoltshammer, T.J., Mayr, M. (eds) Data Science—Analytics and Applications. iDSC 2023. Springer, Cham. https://doi.org/10.1007/978-3-031-42171-6_11
- [5] <https://www.gartner.com/en/information-technology/glossary/data-monetization>
- [6] <https://docs.internationaldataspaces.org/ids-knowledgebase/ids-g/components>
- [7] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_2_functionallayer
- [8] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3-1-business-layer/3_1_1_roles_in_the_ids
- [9] https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_5_clearing_house
- [10] <https://101blockchains.com/introduction-to-blockchain-features/>
- [11] <https://dssc.eu/space/bv15e/766068145/Provenance+&+Traceability>
- [12] Rami Alkhudary, et al., "Enhancing the competitive advantage via Blockchain: an olive oil case study", IFAC-PapersOnLine, Volume 55, Issue 2, 2022, Pages 469-474, ISSN 2405-8963, <https://doi.org/10.1016/j.ifacol.2022.04.238>.
- [13] <https://dssc.eu/space/bv15e/766068145/Provenance+&+Traceability>
- [14] <https://www.circularise.com/blogs/digital-product-passports-dpp-what-how-and-why>
- [15] <https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4>

Chapter 2 – EU Digital Product Passport (DPP) for the Agri-Food Industry

Authors: **Marianna Faraldi**¹, **Denis Avrillionis**², **Theofilos Papasternos**²

¹ TECNOALIMENTI S.C.p.A., Chief research officer, Italy

² COMPELLIO, Luxembourg

Version	Date
0.1	20 Jan 2025
0.2	10 March 2025
0.3 (final)	22 December 2025

Executive Summary

The EU Digital Product Passport (DPP) is a regulatory initiative under the European Green Deal and the Circular Economy Action Plan⁴. It aims to provide detailed, standardized, and accessible information about products, helping industries track their environmental impact, enhance sustainability, and combat counterfeiting. The DPP is part of the Ecodesign for Sustainable Products Regulation⁵ (ESPR) and will become mandatory for specific industries, including agri-food, by the late 2020s.

The practical guidelines for implementation of DPP are defined in **CIRPASS** projects. **CIRPASS 1**⁶ laid out the groundwork, **CIRPASS 2**⁷ will roll out the first pilot projects in textiles, electrical and electronic equipment, tyres and construction value chains.

The Digital Product Passport contains data about a product's origin, composition, durability, environmental impact, and supply chain, accessible to manufacturers, suppliers, regulators, and consumers. For the agri-food industry, it would cover details such as production practices, carbon footprints, traceability for food safety, and compliance with sustainability standards.

⁴ https://environment.ec.europa.eu/strategy/circular-economy-action-plan_en

⁵ https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/ecodesign-sustainable-products-regulation_en

⁶ <https://cirpassproject.eu/project-results/>

⁷ <https://cirpass2.eu>

2.1. Introduction

2.1.1. What is the DPP

The **Digital Product Passport (DPP)** is a standardized digital document that provides comprehensive and accessible information about a product throughout its lifecycle.

The **core objectives** of the DPP include:

1. **Enhancing Product Transparency:** Making detailed information about a product's origin, composition, environmental impact, and supply chain traceable and publicly available.
2. **Facilitating Circularity:** Enabling easier recycling, reuse, and repair by providing precise details about materials and components.
3. **Enabling Regulatory Compliance:** Helping industries meet EU regulations for sustainability and environmental responsibility.
4. **Combatting Counterfeiting and Fraud:** Ensuring authenticity by offering secure digital records of a product's history and certifications.
5. **Supporting Consumers and Businesses:** Empowering consumers to make informed choices and enabling businesses to optimize supply chains for better sustainability and efficiency.

2.1.2. How does it work in practice

At its core the DPP is a web resource that can be accessed by scanning the product.

- Scanning can be anything from taking a picture to using NFC chips. The definition of DPP is wide enough to accommodate any means of accessing the DPP identifier. This component is called "data carrier"
- The DPP identifier must be enough to understand exactly which web resource to access. The easiest way to do this is by setting a full URL as an identifier. Alternative approaches use the concept of GS1 digital link (<https://www.gs1.org/standards/gs1-digital-link>), where the scanning device queries a server that, given a GTIN, returns the full URL of the connected web resource. This component is called "look-up-mechanism". There also exists a current proposal for a central EU "look-up-mechanism" at least for Customs use (https://taxation-customs.ec.europa.eu/eu-single-window-environment-customs_en).
- Finally the web resource is a page with the product description, in industries where single item serialization is possible the web page contains data of that specific object, in industries where only batch serialization is possible, the page contains only batch information.
- The minimum set of information depends on the industry and it will be identified by dedicated legislation reflecting the compliance needs of that specific product-group (<https://cirpassproject.eu/wp-content/uploads/2024/03/A2-EC-Michele-Galatola.pdf>). This means that it "can be used" to showcase the agri-food supply chain but there are no legislative requirements to do so for now.
- The global digital product passport market size was valued at USD 213.9 million in 2024 and is expected to expand at a CAGR of 34.9% from 2025 to 2030⁸. This growth is primarily driven by the increasing global demand for product transparency, sustainable manufacturing practices, and circular economy solutions. Blockchain-enabled DPPs can enable long-term value chain sustainability by providing the digital infrastructure necessary for consistent, verifiable material traceability, lifecycle tracking, and regulatory compliance. By automating data capture and integrating stakeholders (e.g. via an API-based interoperability layer), transaction costs and compliance burdens are reduced, incentivizing continuous use and expansion. The business opportunity is strong, with growing European momentum around Digital Product Passports. According to the European Commission, the circular economy could increase EU GDP by 0.5% by 2030 and create 700,000 new jobs.⁹
- DPPs for agri-food could also be connected to EU CAP's eco-schemes: Eco-schemes are payment schemes in agriculture aiming at the protection of environment and climate. They

⁸ <https://www.grandviewresearch.com/industry-analysis/digital-product-passport-market-report#:~:text=The%20global%20digital%20product%20passport,practices%2C%20and%20circular%20economy%20solutions>

⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0098>

are a key element of the Common agricultural policy (CAP) (Article 31 of Regulation (EU) 2021/2115 of the European Parliament and of the Council¹⁰). Agrifood DPPs could facilitate streamlined compliance of eco-schemes reporting within food tracking processes (for producers, producers associations, public agencies, auditors, policy makers); Deliver enhanced trust, verification, and transparency capabilities related to regulated eco schemes disclosures (for citizens and consumers); Facilitate trusted and interoperable data exchanges and integrations with 3rd party solutions providers.

2.2. Interaction with blockchain

There is no explicit mention of blockchain within the (current) DPP minimum requirements, in fact it is possible to build a DPP system on classic IT stack. Nonetheless, fail cases for DPP highlight when and why blockchain can be useful.

- A web resource can be edited at will, so whenever something non compliant is found, the owner could just change the content and hide the problem
- A QR code with a link and related website is very easy to create, frauds and counterfeiters can create them as well.

Blockchain offer an unmodifiable¹¹ storage which addresses both weaknesses:

- The hash of a web resource can be recorded on a blockchain, creating a chronological record of which version was official at any given time. However, simply storing a snapshot of the information does not prove what was actually sent to the client. To enhance security, clients (such as app or website users scanning a QR code) should verify the data they receive by consulting a trusted authority or scanning the blockchain to confirm that they have the latest official version.
- Data hashes can be signed, and when a registry of approved signing keys is available (e.g., the EUIPO AuthenticView project for registered brand owners <https://www.euipo.europa.eu/en/observatory/enforcement/authenticview>), clients can verify that a hash comes from a legitimate source. As with the previous case, clients should either rely on a public list of trusted keys or consult an authority to determine which keys are valid.

Common misunderstandings on the interaction between DPP and blockchain:

- Storing everything in blockchain, this approach in practice due to costs and technical bottlenecks generates technology and providers lock-in, only hashes should be signed and stored, this lighter approach allows for cheaper solutions which achieve the same functional results and are easier to switch to and from.
- “If it’s in the blockchain it is absolutely true” that’s not the case, signed data only ensures that: “the signing entity confirms that was the data at the time”. Do you trust the signing entity is completely outside of the scope of the blockchain, which only freezes a lie in time but cannot detect a lie.

Blockchain standards that work well with DPP:

- DID, distributed identifiers, it’s a way to create unique serial numbers and make sure that serial number is controlled by a specific set of keys. This is the type of technology offered by EBSI for all of its use cases (EUIPO, University certificates, digital identity..)
 - DPP identifiers must be unique and as highlighted above should also be linked to a signing key so that anyone can understand who is responsible for the connected data.
- Timestamping, it’s the activity of incorporating a hash into a block. Although there are various routines to do so, the general concept is always the same and it’s been

¹⁰ <https://eur-lex.europa.eu/eli/reg/2021/2115/oj>

¹¹ Unmodifiable: depending on the blockchain used, the cost of rewriting the past changes. Unmodifiable in this context means: the monetary cost is too high or the faith in the organization ensuring the chronological order of the blockchain is high enough.

implemented also within EBSI. <https://hub.ebsi.eu/tools/cli/upcoming-apis/create-timestamp>

- Creating a timestamp means obtaining the block and transaction identifier where a specific hash has been incorporated. The service needs to i) accept a hash to create a new timestamp or ii) accept a hash as a query parameter and return the block information where the hash is incorporated. Given the simple setup this can easily be implemented in any blockchain.

2.3. DPP for the Agrifood sector

2.3.1. Opportunities

The agri-food sector plays a critical role in the EU's sustainability and food security agenda, making it one of the most significant industries for DPP implementation. Unlike existing systems, which often focus on internal traceability within supply chains, the DPP extends this information into a universally accessible format, enabling stakeholders at every level: regulators, businesses, and consumers to interact with the same data.

Standardized and Interoperable Framework:

- The DPP creates a common EU-wide standard for product data, ensuring compatibility across sectors and borders. This is critical for aligning fragmented systems and allowing seamless data sharing between stakeholders.
- It builds on **existing traceability systems** but moves beyond proprietary tools by creating a centralized, open, and transparent infrastructure.

Consumer-Focused Transparency:

- While current systems are often aimed at business-to-business (B2B) operations, the DPP ensures that information such as origin, carbon footprint, and certifications is easily accessible to consumers through **QR codes** or **digital tags**.
- Consumers are empowered to make informed decisions based on sustainability, ethical practices, or specific health concerns.

Integration with Circular Economy Goals:

- The DPP enables tracking beyond the supply chain into a product's end-of-life stage, supporting recycling, reuse, and waste reduction initiatives. This makes it a unique tool for aligning the agri-food sector with broader circular economy policies.
- Eco-schemes provide support for farmers who observe agricultural practices beneficial for the environment and climate. It is a measure to reward and incentivise farmers for taking action towards a more sustainable farm and land management with the objective to maintain public goods. The participation of farmers is voluntary. Member States are however obliged to include one or more eco-schemes in their CAP Strategic Plans (CSPs). It offers more flexibility than the former greening payments of the CAP as Member States are free to set the scheme's content and budget. As a result, they can design the eco-schemes according to their environmental and climate needs on a national and regional level. Less administrative burden and annual payments instead of long-term commitments shall contribute to a simplification.

2.3.2. Current limits

Despite its strong potential, the Digital Product Passport for the agri-food sector is still at an early stage of maturity. Several limitations currently constrain its adoption and practical impact:

Lack of applied use cases: At present, there are no large-scale, real-world DPP implementations specifically tailored to agri-food products. Existing CIRPASS2 pilots focus on textiles, electronics, tyres, and construction, leaving agri-food largely unexplored beyond conceptual discussions. This absence of concrete examples makes it difficult for stakeholders to assess costs, benefits, and operational implications.

Missing sector-specific legal framework: While the EPR establishes the overall DPP framework, there is currently no dedicated delegated legislation defining mandatory data requirements for agri-food products. As a result, adoption remains voluntary and fragmented, with no clear compliance drivers or enforcement mechanisms for producers and processors.

Heterogeneity of agri-food supply chains: Agri-food supply chains are highly diverse, ranging from small-scale farms to global industrial players, and from bulk commodities to high-value, serialized products. This heterogeneity complicates standardization, particularly for batch-based products where item-level traceability is not feasible.

Data availability and data quality challenges: Many sustainability indicators relevant to agri-food (e.g. carbon footprint, biodiversity impact, farming practices) are complex to measure and often rely on estimates or self-declared data. Without harmonized methodologies and reliable data collection processes, DPP information risks being incomplete, inconsistent, or difficult to compare.

Cost and administrative burden for small actors: Small and medium-sized farms and food producers may face disproportionate costs in adopting DPP solutions, including data collection, IT infrastructure, and ongoing maintenance. Without adequate incentives, simplification measures, or integration with existing reporting obligations (e.g. CAP eco-schemes), uptake among smaller actors may remain limited.

Interoperability and governance uncertainties: Although the DPP promotes interoperability, questions remain around governance of identifiers, lookup mechanisms, trusted authorities, and signing keys, especially in cross-border contexts. The coexistence of private, sectoral, and potential EU-level lookup mechanisms may create fragmentation if not clearly coordinated.

2.4. DPP with and without Blockchain

This section compares the added value of Digital Product Passports implemented with and without blockchain in the agri-food sector, highlighting when blockchain provides tangible benefits beyond a traditional IT approach. It focuses on key areas - compliance, consumer engagement, and operational efficiency - to clarify in which scenarios blockchain meaningfully enhances trust, coordination, and process efficiency across the supply chain.

Area of interest for Agrifood	DPP without BCT	DPP with BCT
Compliance	Standardize the way data is displayed for multiple compliance checks	Add evidence of the chronological order of events for the data and their backups
	Ensure there are backups of the data	
	moderate	relevant
Consumer engagement	Share with consumers interactive resources about their products.	When there's a secondary market for serialized products, DPP with blockchain can also be used to record the "current owner" of the object.
	Can be relevant for high-end products even in agri-food (wines, olive oil, truffles..)	
		This can be done also without blockchain, but blockchain comes with a market of "investors", which historically has been the

		reason to choose blockchain.
	moderate	relevant
Operational efficiency	Standardizing agri-food data across the supply chain, reducing manual data exchanges, duplication, and reconciliation between actors.	Shared, tamper-evident source of truth that reduces disputes, verification steps, and intermediaries between supply-chain actors.
	Centralized and structured product information streamlines compliance reporting, audits, and internal process optimization.	Immutable timestamps and signed data enable faster audits, automated controls, and more reliable coordination across complex, multi-party agri-food supply chains.
	moderate	relevant

2.5. Conclusions

The Digital Product Passport represents a foundational building block for the EU’s transition towards a more transparent, sustainable, and circular agri-food system. By enabling standardized, accessible, and verifiable product information, the DPP has the potential to connect regulatory compliance, supply-chain efficiency, and consumer trust within a single digital framework.

For the agri-food sector, the DPP could significantly enhance traceability, support sustainability claims, and streamline reporting obligations—particularly when aligned with CAP eco-schemes and other environmental policies. Its consumer-facing nature also marks a shift from traditional, inward-looking traceability systems toward greater public transparency.

Blockchain technologies are not a mandatory component of the DPP, but they can add value in specific scenarios, particularly where immutability, chronological evidence, anti-counterfeiting, and trust across multiple stakeholders are required. A lightweight approach - focusing on hashing, tokenisation, signing, and timestamping rather than full on-chain data storage - offers a pragmatic balance between security, cost, and flexibility.

However, the realization of this potential depends on resolving current limitations: the absence of agri-food-specific legislation, the lack of pilot implementations, data quality challenges, and the need to ensure inclusiveness for smaller producers. In the short term, experimentation through voluntary pilots and alignment with existing digital and regulatory initiatives will be essential.

In the medium to long term, a clear legal framework, harmonized data standards, and well-defined governance mechanisms will determine whether the DPP becomes a transformative tool for the agri-food sector or remains a niche compliance instrument. If implemented thoughtfully, the DPP can act as a catalyst for trust, sustainability, and innovation across Europe’s food systems.

Acknowledgments

The authors would like to thank Thomas Rossi (Eonpass) for the contribution which helped refine the final version of this Chapter.

Chapter 3 – AI and Blockchain Synergies: Outline, Applications in Agri-Food, and Future Use Cases

Author: **Konstantina Pantelidou**¹

¹ Research Associate, Centre for Research & Technology Hellas (CERTH), Institute of Information Technologies (ITI), Greece

3.1. Brief Outline of Current AI and Blockchain Synergies

Artificial Intelligence (AI) and **Blockchain (BC)** are among the most transformative technologies over the past few decades, each offering distinct, but complementary capabilities. AI enables intelligent data processing, automation and predictive modeling, while blockchain provides decentralized, secure and tamper-evident data storage and transaction verification. When integrated, these technologies create powerful synergies, enhancing trust, transparency, and decision-making across complex systems.

Key Synergies between AI and Blockchain

1. Data Integrity for Trustworthy AI

The performance and reliability of AI systems depend heavily on the quality and integrity of input data. The immutable and transparent ledgers of blockchain technology offer a reliable basis for data provenance, significantly reducing the risk of bias, manipulation, or corruption in AI inference and training.¹²

2. Enhanced Security and Privacy

Blockchain's cryptographic architecture facilitates secure data sharing across decentralized networks. This is particularly important in privacy-sensitive AI applications, such as federated learning, where multiple stakeholders collaborate without exposing underlying data, thereby preserving confidentiality and compliance with data protection regulations.¹³

3. Decentralized Machine Learning

By enabling AI model training across distributed nodes, blockchain supports decentralized learning frameworks that do not require centralizing sensitive data. This approach improves system robustness, mitigates single points of failure, and promotes inclusive participation in AI development.¹⁴

4. Explainability and Traceability

Blockchain provides a permanent, tamper-proof record of AI activities, including model results, decision explanations, and important data exchanges. This transparency is important in industries such as healthcare, finance, and public services, where meeting regulations and maintaining trust with stakeholders are essential.¹⁵

5. Optimized Blockchain Operations Through AI

AI can enhance blockchain operations by optimizing consensus algorithms, predicting transaction loads and detecting anomalous behaviors such as fraud, spam, or performance

¹² Hussain, Adedoyin A., and Fadi Al-Turjman. "Artificial intelligence and blockchain: A review." *Transactions on emerging telecommunications technologies* 32.9 (2021): e4268.

¹³ Alzoubi, Mahd M. "Investigating the synergy of Blockchain and AI: enhancing security, efficiency, and transparency." *Journal of Cyber Security Technology* (2024): 1-29.

¹⁴ Tyagi, Priyanka, et al. "Synergizing artificial intelligence and blockchain." *Next-Generation Cybersecurity: AI, ML, and Blockchain*. Singapore: Springer Nature Singapore, 2024. 83-97.

¹⁵ Sgantzios, Konstantinos, and Ian Grigg. "Artificial intelligence implementations on the blockchain. Use cases and future applications." *Future Internet* 11.8 (2019): 170.

bottlenecks. These capabilities contribute to more efficient, secure and adaptive blockchain ecosystems.¹⁶

The convergence of AI and blockchain is redefining digital infrastructure across industries. Together, they lay the groundwork for more autonomous, transparent, and resilient systems, accelerating the transition toward a more decentralized and intelligent digital future.¹⁷

3.2. AI and Blockchain Applications in the Agri-Food Sector

The agri-food sector is facing multiple challenges, such as ensuring food security, addressing climate change, protecting biodiversity, managing fragile supply chains and meeting complex regulations. To resolve these issues, the combined use of AI and Blockchain is playing an important role in reshaping how digital technologies are applied in agri-food systems. These technologies are transforming how food is produced, tracked and valued across the entire supply chain. In the European Union, this digital shift supports key policy initiatives like the European Green Deal, Farm to Fork Strategy, and the Common Agricultural Policy (CAP), all of which aim to build more sustainable, innovative, and resilient food systems. When used together, AI and blockchain can help move the agri-food sector toward a future that is more transparent, efficient, and climate-friendly.¹⁸

3.2.1. Supply Chain Transparency and Traceability

Blockchain technology offers a decentralized and tamper-proof system for recording every step in the food supply chain, from farm to consumer. It captures critical information, such as product origin, certification status, transport conditions, and storage history in a permanent and transparent way. AI adds value by interpreting this data to uncover inefficiencies, predict potential disruptions, and streamline regulatory compliance. Together, these technologies strengthen traceability, improve the speed and precision of recalls, help prevent food fraud, and enhance consumer and stakeholder confidence in the integrity and sustainability of food products.¹⁹

3.2.2. Automated Transactions via Smart Contracts

Smart contracts on blockchain platforms enable the automatic execution of predefined agreements, such as processing payments, updating inventory, or releasing goods, once specific conditions are fulfilled (e.g., crop quality validation, sensor data thresholds, or confirmed deliveries). These contracts reduce the need for manual intervention and enforce trust between parties without intermediaries. AI enhances this process by validating inputs in real time, using tools like computer vision for quality checks or geospatial data for optimizing logistics. This seamless integration minimizes administrative overhead, reduces the risk of disputes, and streamlines operations, particularly valuable in large-scale, cross-border agri-food supply chains.²⁰

3.2.3. Compliance and Food Safety Monitoring

AI-driven sensors, satellite imagery, and autonomous drones are transforming the way farms track soil quality, water consumption, crop growth, and animal health. These continuous, real-time data streams are essential for complying with the EU's growing requirements around sustainability, safety, and traceability. Once collected, this verified information is securely recorded on a

¹⁶ Konrad-Adenauer-Stiftung, "Synergies of Blockchain and AI".

¹⁷ European Parliament, EPRS Study (2023), "Artificial Intelligence in the Agri-Food Sector".

¹⁸ Hurduzeu, Gheorghe, and Maria-Floriana Popescu. "Blockchain in Agriculture: Transforming the Food Supply Chain for Transparency and Efficiency in the European Union." *Agricultural Economics and Rural Development* 20.2 (2023): 145-153.

¹⁹ Ahamed, N. Nasurudeen, and R. Vignesh. "Smart agriculture and food industry with blockchain and artificial intelligence." *Journal of Computer Science* 18.1 (2022): 1-17.

²⁰ Samala, Harshita. "Blockchain technology in Agriculture: Applications, Impact and Future." *International Research Journal of Engineering and Technology* 9.11 (2022): 77-83.

blockchain, capturing key environmental and production details, such as pesticide application, temperature monitoring, and livestock welfare, establishing a compliance record accessible to regulators, certification bodies, and supply chain stakeholders.²¹

3.2.4. Precision Agriculture with Verifiable Data

Modern farming uses a lot of data, from weather forecasts and soil sensors to harvest maps and images from drones. AI helps make sense of this information by turning it into useful advice for farmers, so they can use fewer resources, reduce pollution, and grow more products. Blockchain supports this system by making sure the data is real, time-stamped and easy to check on later. This is especially important when farmers apply for climate-related subsidies, environmental certifications, or agricultural insurance, where verified data and traceability are essential for eligibility and compliance.²²

3.2.5. Disease Detection and Crop Quality Assurance

Machine learning models trained on high-resolution imagery and environmental data can detect early signs of crop disease, pest outbreaks, or product degradation before they become critical. This enables proactive interventions, reducing waste and preserving quality. When logged on a blockchain, these alerts are shared transparently and in real time with cooperatives, transporters, buyers and authorities, allowing coordinated responses and minimizing economic and reputational losses across the supply chain.²³

3.2.6. Decentralized Agricultural Data Marketplaces

Farmers, cooperatives, and agri-food platforms generate huge amounts of agronomic data, but lack systems for properly sharing, monetizing, or maintaining control over it. Blockchain enables the development of decentralized data marketplaces in which individuals or organizations can exchange datasets in a transparent, permissioned environment. AI benefits from these diverse datasets by training more accurate models. In return, data contributors gain fair compensation, retain data ownership, and access enhanced forecasting tools, crop models, and digital advisory services, supporting a more inclusive and data-driven agricultural economy.²⁴

3.3. Key agri-food use cases powered by blockchain standards and AI

As digital innovation increases, the integration of AI and blockchain technology in agri-food systems progresses from early acceptance to near-term implementation. The following use cases demonstrate where this convergence has the potential to have a significant impact across economic, environmental and operational aspects.

3.3.1. End-to-End Food Traceability

Each component of a food product, from initial raw materials to final packaging, can be securely logged on a blockchain, recording critical information such as origin, handling conditions, transportation records, and certification status. AI tools process and interpret this data to identify irregularities, generate real-time alerts, and provide a transparent view of the product's path from source to shelf. This combination enables faster, more accurate recalls, improves food safety

²¹ European Commission, "Digitalising the EU Agricultural Sector".

²² IJOEAR, "Transforming the Future of Farming with Blockchain and AI".

²³ Venturini, Rafael Elias. "Technological innovations in agriculture: the application of Blockchain and Artificial Intelligence for grain traceability and protection." *Brazilian Journal of Development* 11.3 (2025): e78100-e78100.

²⁴ Protocol, Ocean. "Ocean Protocol." 2023,

oversight, and builds trust among consumers and investors—especially in markets prioritizing transparency, ethical sourcing, and ESG compliance.²⁵

3.3.2. Dynamic Supply Chain Optimization

AI algorithms can continuously forecast supply and demand fluctuations by analyzing variables such as weather, market trends, and geopolitical factors. Smart contracts on blockchain automatically respond to these predictions, rerouting shipments, adjusting procurement, or reallocating inventory. This responsiveness reduces waste, improves shelf-life, and enhances the resilience of perishable supply chains in the face of disruptions like pandemics, climate events, or trade restrictions.²⁶

3.3.3. Automated Subsidy and Insurance Payouts

Another use case gaining recognition is the automation of subsidy and insurance payouts. Farmers often face long delays and paperwork when seeking financial support. AI can verify crop damage or yield data through satellite imagery, drone footage, and sensor readings. Blockchain then ensures these verified inputs are used to trigger smart contracts that release payments transparently and quickly. This system reduces fraud, speeds up relief for farmers, and ensures fair, rules-based distribution of public or private fund.²⁷

3.3.4. Sustainability and Carbon Tracking

AI systems can accurately measure key environmental factors on farms, such as greenhouse gas emissions, use of water and energy, and impacts on biodiversity. These sustainability metrics, once verified, can be recorded and tokenized by using blockchain, allowing farmers to take part in carbon credit markets or regenerative agriculture programs. This creates new income opportunities, helps companies access trusted data for ESG reporting, and supports the larger transition to climate-smart, sustainable farming practices.²⁸

3.3.5. Fraud Prevention and Product Authentication

Fraud prevention and product authentication are also areas where AI and blockchain work powerfully in parallel. Blockchain's immutable records secure food documentation and certification processes, while AI analyzes transactions and logistics data to flag suspicious behavior, such as inconsistencies in origin claims, supply anomalies, or unusual patterns in supplier behavior. This dual approach helps detect mislabeling, counterfeiting, and product dilution early, protecting consumers and maintaining the integrity of agri-food value chains.²⁹

These use cases signal a paradigm shift in how agri-food systems can operate—one that is automated, transparent, responsive, and sustainable. As digital infrastructure matures, AI and blockchain are not just enabling tools but strategic enablers of a next-generation food economy, aligned with global goals for climate action, food security, and rural development.³⁰

²⁵ Schebesta, Hanna, Nadia Bernaz, and Chiara Macchi. "The European union farm to fork strategy." *European food and feed law review* 15.5 (2020): 420-427.

²⁶ Daraghmi, Eman, et al. "Smart contracts for managing the agricultural supply chain: A practical case study." *Ieee Access* (2024).

²⁷ SmartAgriHubs EU Project Reports, 2022. <https://www.smartagrihubs.eu/>

²⁸ Boumaiza, Ameni, and Kenza Maher. "Leveraging blockchain technology to enhance transparency and efficiency in carbon trading markets." *International Journal of Electrical Power & Energy Systems* 162 (2024): 110225.

²⁹ Authority, European Food Safety, et al. "Food safety regulatory research needs 2030." *EFSA Journal* 17.7 (2019): e170622.

³⁰ Rodriguez, Maria Angeles, Llanos Cuenca, and Angel Ortiz. "FIWARE open source standard platform in smart farming-a review." *Working Conference on Virtual Enterprises*. Cham: Springer International Publishing, 2018.

Chapter 4 – Digital Identity

Author: **João Rodrigues**¹

¹ Scientific Researcher INOV, Instituto de Engenharia de Sistemas e Computadores Inovação, Portugal

In this Chapter we will be focusing on the well-known digital identity management models, and then contrast it with the self-sovereign identity model.

In the first model, centralized identity, one single organization issues credentials to their users, enabling them to access the organization's services [1] [2]. These are usually username and password credentials. These systems are simple to implement and manage, but the user's information is stored and controlled by the organization. Another problem it is burdensome to the users as they need to have separate credentials to have access to different services from different organizations.

The Federated identity model, on the other hand, enables a user to use credentials from one organization to authenticate and access to other organization's resources. [1] [2]. Examples of this are access to scientific papers through the alumni credentials from universities. The identity managing organization is called an Identity Provider (IDP), and the authentication to other organizations are done through the Single-Sign-On functionality (e.g., SAML, OIDC). This service reduces the need for multiple credentials, reducing the number of entities storing user's information. It is also beneficial to the users as they don't need to store and/or remember every username and passwords to every services they use. However, the user still doesn't have any control over their data as they are stored on a central organization.

The concept of Self-Sovereign Identity emerged from concerns stemming from users' lack of control over their data, minimal disclosure and interoperability [3]. Kim Cameron introduced the Laws of Identity, laying the foundational principles for protecting the aforementioned concerns. Moxie Marlinspike advocated for a "Sovereign Source Authority" model, where individuals could generate and asset their own identities without depending on a centralized authority. In this model, identity is self-issued and self-managed, and trust is earned socially or contextually rather than being inherited from a centralized authority [3], [4]. Another contribution came from Christopher Allen who defined the 10 core principles of what is now known as the principles for Self-Sovereign Identity [3], [5], [6]:

- **Existence:** Users must exist independently of any centralized system or digital identity provider. Users must have independent existence from the digital word;
- **Control:** Users must have control over their identities and personal data. The identity system should ha a well-understood and secure algorithms supported a continued validity of the identity and its' claims;
- **Access:** Users must have access to their own data and identities.
- **Transparency:** Systems and algorithms must be transparent and understandable. Algorithm should be free, open-source, well-known and as independent as possible of any particular architecture
- **Persistence:** Identities should last as long as the user desires. Though private keys need to be rotated and data might need to be changed, the identity remains. The right to be forgotten must be supported: a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time.
- **Portability:** Identities should be portable and not tied to any single platform. Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user.

- **Interoperability:** Identities must work across systems and platforms to enable wide usability.
- **Consent:** Data sharing should occur only with user consent.
- **Minimization:** Only the necessary amount of data should be shared. Disclosure of claims must be minimized. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlability is still a very hard task
- **Protection:** Users must have protection of their rights and data. When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.

Summing up, a Self-Sovereign Identity system is a decentralized identity model that eliminates dependencies with third-parties whenever the user interacts or accesses organizations services. Users credentials, like it's national ID, driver's license, professional credentials, are emitted by the authoritative parties (e.g., government, university, enterprise) and stored on the user's digital wallet. The user can use these credentials revealing only relevant data whenever it needs to proof some claims. The user can also emit his own credentials in a similar way one does when registering into any service website.

4.1. Self-Sovereign Identity

In the Self-Sovereign Identity model, we have three key actors: The Issuer of credentials, The Holder of the credential and the verifier. Supporting the service is an infrastructure called the trusted registry. This trusted registry can be implemented recurring to blockchain, but it is not mandatory.

Credentials Issuing

The issuer is responsible for confirming the identity of the holder, and for creating a set of signed credentials to the holder. The issuer can be the Government, Transport Licensing Authority, University or any other organization that are credited with the authority to issue credentials. The issuer will emit **Verifiable Credentials** (VCs) (claims, digitally signed by the issuer and cryptographically verifiable), and a **Decentralized Identifier (DID)** document with cryptographic materials. Like the user's public keys and other relevant information for verifying the VCs. The DID document is quickly referenced by a DID (a unique identifier of the document), similar in structure to a URL, which acts as a pointer to the DID document. The DID and the DID document are stored in a decentralized repository, such as a Distributed Ledger. Note that both the DID document and the Verifiable Credentials are digitally signed by the Issuer.

Credentials Management with Digital Wallet

The Holder requests the Verifiable Credentials emission to the Issuer and stores them in a digital wallet, as well as the respective DID and private keys. The Holder can proof ownership of the DID document by proving ownership of the private keys related to the public keys stored in the document. Moreover, the DID document and the Verifiable credentials are signed by the Issuer, enabling authenticity verification by any party, once they are revealed.

The user can also emit DID documents and credentials. He can sign the DID documents with new private keys, unrelated to other credentials, or related to some of the issued credentials, giving added layer of trust. It will depend on the use case.

User issued credentials are useful for separating his activities in different services, protecting his privacy.

Credentials Verification

The Verifier, usually a service provider, or an authority, request proofs of some credentials to the holder. It could be drivers' license category, age, or some certification for accessing services. For example, the police could ask for the driver's license from the holder. The holder sends the DID and the necessary part of the VCs (e.g., license permit, without revealing any further information), to the verifiers' machine (e.g., computer, mobile phone). What is particular about these credentials is that they can be stored and authenticated separately. In the case of drivers' license, the holder can send the verifiable credential, saying that the holder has license to drive B2 vehicles, without revealing any further information. The Verifier can verify this credential by accessing the trusted registry, retrieving the respective cryptographic material, and verifying the digital signature. This is useful in car renting services, where the holder does not need to give the full information present in a driver's license, for example, protecting it's privacy. This property of the VCs is called **selective disclosure**.

Depending on the cryptographic algorithms used for Verifiable Credentials, they can also support Zero Knowledge Proof protocols. These protocols enable the holder to prove claims about its credentials without revealing the actual information. One example is the proof of majority of age (for example, more than 18 years old, or senior age), which are helpful when selling certain goods (e.g., tobacco, alcohol) or even giving access to government services for senior age citizens.

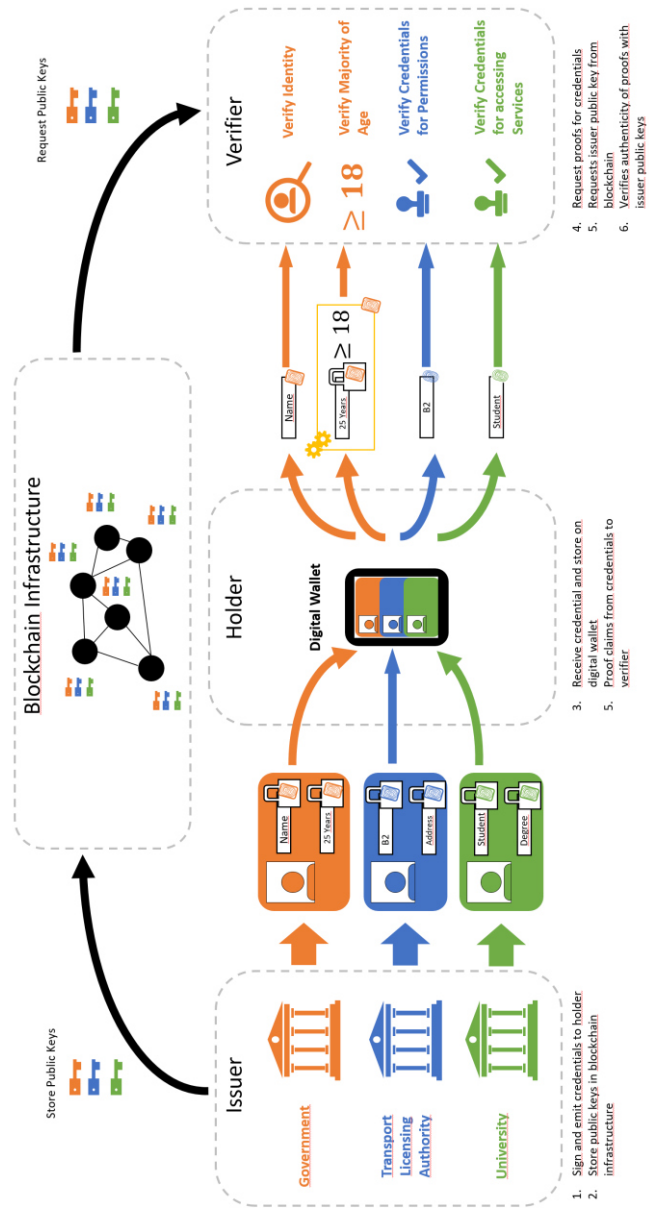


Figure 2 Self-Sovereign Identity credential issuing and verification processes. In this example, the key and DID storage is done recurring to a blockchain infrastructure

4.2. Open standards supporting SSI

The list of standards supporting a SSI is the following:

- W3C Decentralized Identifiers (DIDs) – defines a globally unique, persistent and cryptographically verifiable identifier [7];
- W3C Verifiable Credentials Data Model [8] – defines how verifiable credentials are expressed, issued and verified in a secure, privacy-preserving, and interoperable way;
- DIDComm Protocol [9]– enables secure and private point-to-point communication using DIDs.
-
- OpenID Connect for Verifiable Presentations (OIDC4VP) [10] – standard for using VCs with OIDC;
- OpenID Connect for Credential Issuance (OIDC4VCI) [11] – standard for issuing VCs for someone holding an OIDC credentials.

4.3. The EU Wallet and EU Projects

The European Commission is committed to deliver an EU Digital Identity Wallet, available for all EU citizen, that is safe, reliable and privacy enhancing. This comes as the response from the EC to the increasing tendency of public and private services turning digital [12]. The key functionalities of the EU Wallet are the following:

- Store digital documents, like education credentials, train tickets, drivers' license, citizen credentials, in a secure, privacy-preserving manner.
- Access to online services, in a private manner, without needing to manage countless passwords;
- Share digital documents, providing only the strictly necessary information (selective disclosure). Many digital documents will be accepted anywhere in Europe;
- Sign documents safely, providing a legally binding e-signature for businesses.

Moreover, on April 2024, the Regulation (EU) 2024/1183 was published and, according to it, every EU Member must provide to its' citizens EU Digital Identity Wallets [13]. As a consequence, there are EU large scale pilot projects include [14]:

- EU Digital Wallet Consortium (EWC) - Focused on Digital travel Credentials across Member States [15] , [14]. EWC published a deliverable for shared network infrastructure based on distributed ledger technology for anchoring W3C DIDs, endpoints and other features for organizational wallets [17].
- Digital Credentials for Europe(DC4EU) - Focused on the educational and social security sectors, explores the trans-European interoperable digital service infrastructure and cross-border trust frameworks. The DC4Eu will explore 3 candidates for trust infrastructures. The eIDAS federated identity system, the EBSI, and the third one is the OpenID federation. [18].
- POTENTIAL - Explores the potential of the EU Digital Wallet in six different sectors: governmental services, banking, telecommunications, mobile driving licenses, electronic signatures and healthcare.
- NOBID Consortium - Explores the use of EU Digital Wallet for authorization of payments for products and services. To the best of our knowledge, there is no explicit mention of blockchain or DLT.

References

- [1] N. Naik and P. Jenkins, "Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems," em *2020 IEEE International Symposium on Systems Engineering (ISSE)*, Vienna, 2020.
- [2] [Online]. Available: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>.
- [3] Satybaldy, A., Nowostawski, M., & Ellingsen, J., " Self-Sovereign Identity Systems: Evaluation framework. Computer Science Department," *NTNU, Gjøvik, Norway*..
- [4] Marlinspike, M., "Sovereign Source Authority," 2012. [Online]. Available: <http://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html>.
- [5] Allen, C., "The Path to Self-Sovereign Identity," 2016. [Online]. Available: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>.
- [6] N. Naik and P. Jenkins, "Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems," Aston University and Cardiff Metropolitan University.
- [7] [Online]. Available: <https://www.w3.org/TR/did-1.1/>.
- [8] [Online]. Available: <https://www.w3.org/TR/vc-data-model-2.0/>.
- [9] [Online]. Available: <https://identity.foundation/didcomm-messaging/spec/>.
- [10] [Online]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0-16.html.
- [11] [Online]. Available: https://openid.net/specs/openid-connect-4-verifiable-credential-issuance-1_0-05.html.
- [12] [Online]. Available: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet>.
- [13] [Online]. Available: <https://www.european-digital-identity-regulation.com/>.
- [14] [Online]. Available: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects>.
- [15] [Online]. Available: <https://eudiwalletconsortium.org/>.
- [16] [Online]. Available: https://eudiwalletconsortium.org/wp-content/uploads/2024/11/EWC-D4.10-Shared-network-infrastructure-available_v1.pdf.
- [17] [Online]. Available: https://dm158x9fyyzgp.cloudfront.net/wp-content/uploads/2024/10/DC4EU_D7.3_Interop-Lab-guide_v.1.0.pdf.
- [18] [Online]. Available: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects>.



TRUSTyFOOD, December 2025