
# European Blockchain Sandbox
# Best practices report (2023)
# 1st Cohort, Part A

Bird & Bird & OXYGY

European
Blockchain
Sandbox

## Internal identification

Contract number: CNECT/2021/OP/0019
VIGIE number: CNECT-PN-2021-000018-EBP

**EUROPEAN COMMISSION**

Directorate-General for Communications Networks, Content and Technology
Directorate E — Future Networks
Unit E.3 — Next-Generation Internet

*Contact: CNECT-E3@ec.europa.eu*

*European Commission*
*B-1049 Brussels*

# European Blockchain Sandbox - Best practices report. 1st Cohort, Part A

Directorate-General for Communications Networks, Content and Technology
2024 EN

***EUROPE DIRECT is a service to help you find answers to your questions about the European Union***

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

## LEGAL NOTICE



| PDF | ISBN 978-92-68-11619-7 | doi: 10.2759/841857 | KK-09-24-009-EN-N |
|---|---|---|---|

Manuscript completed in December 2023.

First edition



Luxembourg: Publications Office of the European Union, 2024

# TABLE OF CONTENTS

# Best Practices Report

# (1st cohort, Part A - 2023)

## 1. Introduction

### 1.1 Objectives and policies

The *European Blockchain Sandbox* is a regulatory sandbox which aims to establish a pan-European framework for regulatory dialogue. The Sandbox brings together national and EU regulators and authorities with providers of innovative blockchain/DLT applications in both the private and public sector to identify possible issues and solutions from a legal & regulatory perspective in a safe and confidential environment. The regulatory dialogues will allow innovators to better understand relevant laws and regulations. The exchanges will allow regulators and authorities to enhance their knowledge of cutting-edge technologies involving blockchain and distributed ledger technologies, and to exchange views and experiences with other regulators and authorities.

The European Blockchain Sandbox does not imply legal endorsement or regulatory approval of the use cases, nor does it allow for derogations of applicable laws. Results are made available to the wider community through best practice reports.

The sandbox is funded under the Digital Europe Programme and delivers on the Commission Communication "SME" of 10 March 2020[1] and "A European Strategy for Data" of 19 February 2020.[2] Funded by the Digital Europe Programme and delivering on the SME strategy, the sandbox runs from 2023 to 2026 and will annually support 20 projects including public sector use cases on the European Blockchain Services Infrastructure. Projects are chosen through calls for expression of interest. After the dialogues for each cohort, the most innovative regulator participating in the sandbox will be awarded a non-monitory prize.

The European Blockchain Sandbox is facilitated by a consortium under the leadership of the law firm Bird & Bird and its consulting arm OXYGY supported by blockchain experts of Warren Brandeis, local regulatory experts in all EEA Member States and web-designers of Spindox, which has been procured through an open call for tenders in 2022. The selection process for each cohort is overseen by a panel of independent academic experts. An overview of the consortium is included in **Annex 1**.

[1] An SME Strategy for a sustainable and digital Europe COM (2020) 103 (10 March 2020).
[2] A European strategy for data COM(2020) 66 (19 Feb. 2020).

The sandbox is a contribution to responding to the call for action in the Council Conclusions from November 16, 2020,[3] where it stipulates as follows:

> *Regarding regulatory sandboxes: CALLS on the Commission to organise, in cooperation with Member States, an exchange of information and good practices regarding regulatory sandboxes between Member States and itself in order to:*
>
> *a) establish an overview of the state of play regarding the use of regulatory sandboxes in the EU;*
>
> *b) identify experiences regarding the legal basis, implementation and evaluation of regulatory sandboxes;*
>
> *c) analyse how learning from regulatory sandboxes at national level can contribute to evidence-based policy making at EU-level.*

The pan-European blockchain regulatory sandbox and other EU initiatives such as the European Forum for Innovation Facilitators ("**EFIF"**)[4] for Digital Finance and the sandboxes that will be established on the basis of the AI Act[5] are complementary and reinforce each other. The European blockchain regulatory sandbox provides a framework for a cross-border regulatory dialogue with a focus on innovative blockchain applications across industry sectors covering a broad range of regulatory and potential legal issues, while the AI Regulatory Sandboxes to be established across the EU under the AI Act will be specialized on AI to foster innovation and provide a controlled regulatory environment for the development, validation and testing of innovative AI systems, including where relevant in real-world conditions, under the guidance and supervision by competent authorities under the AI Act. EFIF provides innovative financial firms with a single access point to national financial supervisors, including national regulatory sandboxes in several Member States to actually test innovative financial products, financial services or business models.[6] Blockchain use cases that have been onboarded through the European blockchain regulatory sandbox can be connected with relevant financial supervisors through EFIF in pertinent use cases. Given the increasing convergence of innovative technologies in use cases often involving several industry sectors, there is a close collaboration between the European Blockchain Sandbox and these other initiatives on EU and national level to make sure that experiences and insights are shared and synergies are leveraged.

Moreover, the pan-European blockchain regulatory sandbox is an integral part of the European Commission's blockchain strategy.[7]

---

3 Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, 13026/20 BETREG 27 (16 November 2020).

4 European Forum for Innovation Facilitators | EU Digital Finance Platform (europa.eu).

5 Commission welcomes political agreement on Artificial Intelligence Act, 9 December 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473.

6 European Forum for Innovation Facilitators | EU Digital Finance Platform (europa.eu) with a reference to the Joint ESA report on regulatory sandboxes and innovation hubs; see page 5: "Regulatory sandboxes: these provide a scheme to enable firms to test, pursuant to a specific testing plan agreed and monitored by a dedicated function of the competent authority, innovative financial products, financial services or business models. Sandboxes may also imply the use of legally provided discretions by the relevant supervisor (with use depending on the relevant applicable EU and national law) but sandboxes do not entail the disapplication of regulatory requirements that must be applied as a result of EU law."

7 Blockchain Strategy | Shaping Europe's digital future (europa.eu).

### 1.2 Content of this report

This first best practices report summarizes the experiences and status of the European Blockchain Sandbox in the first year (2023). At the time of publication of this report, the first regulatory dialogue meetings have been concluded and others have been or are being scheduled.

The emphasis of this report is therefore on the organization of the sandbox and the different tasks required for its set-up with a focus on lessons learned regarding the organization and the application & selection process as well as the matching with relevant regulators and supervising authorities for the first cohort of 20 use cases. The initial experiences with the cross-border regulatory dialogues are more briefly discussed. The lessons learned and best practices that have been identified during the dialogues for the first cohort will be discussed in more detail in the next report which will be published after completion of the dialogues for the first cohort.

Section 4 of this report briefly discusses DLT/Blockchain terminology and the relevant laws and regulations. Section 5 of this best practices report explains the setup of the European Blockchain Sandbox. Section 6 summarizes the application process and the selection for the 1st cohort. In Section 7, the experiences in relation to the outreach to regulators/authorities and the matching for the 1st cohort are discussed. In Section 8 the first experiences regarding the dialogue phase for the 1st cohort of participating use cases will be discussed. Section 9 looks ahead in anticipation of the application process for the 2nd cohort which will start in the first months of 2024.

Best practices and lessons learned will be identified at the end of each section.

## 2. Terminology, relevant laws and regulations

### 2.1 Terminology

Despite its name, the European Blockchain Sandbox is not only open for blockchain use cases but for all Distributed Ledger Technology (“DLT”) use cases. The terminology in relation to DLT infrastructures and use cases is not always applied in a consistent manner. In this report we

will use the terminology and definitions in the DLT specific legal instruments such as the DLT Pilot Regulation[8] and the MiCA Regulation[9] as a starting point.

'Distributed Ledger Technology' or 'DLT' means a technology that enables the operation and use of distributed ledgers.[10] 'Distributed Ledger' means an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism.[11] 'Distributed ledger address' means an alphanumeric code that identifies an address on a network using distributed ledger technology (DLT) or similar technology where crypto-assets can be sent or received.[12] The DLT or blockchain application can be deployed either stand-alone or in combination with other innovative technologies (e.g. ICT services, cloud services, big data, AI, IoT, quantum computing, etc.). Blockchain is one type of a distributed ledger which organizes data into blocks, which are chained together in an append only mode.

## 2.2 Blockchains and DLT infrastructures

Blockchains and other DLT infrastructures can be private or public and permissioned or permissionless. The terms public/private refer to who has read-write access to the chain; a public blockchain can be accessed by anyone and in a private blockchain access is limited. The second distinction, permissioned/permissionless, refers to the nodes in the network that validate updates to the ledger. In a permissionless blockchain anyone can be a node in the network and validate updates while in a permissioned blockchain this is restricted to a specific group. Private-permissioned blockchains are mainly found in consortia of companies that all know each other and where transactions are mostly limited to the group of companies participating in the consortium such as a trading system within a specific industry.

The consensus mechanism are the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated.[13] Blockchain and distributed ledger technology use cases operate on the basis of smart contracts meaning a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.[14]

Blockchain technology is therefore not a one size fits all. The characteristics of the blockchain infrastructure and technical standards, the data flows and the use cases are important to understand the regulatory issues.

---

8 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (**DLT-pilot Regime**).

9 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (**MiCA**).

10 Article 2(1) DLT-pilot Regime and Article 3(1) MiCA.

11 Article 2(2) DLT-pilot Regime and Article 3(2) MiCA.

12 Article 3(18) of Regulation 2023/1113 on information accompanying transfers of funds and certain crypto-assets.

13 Article 2(3) DLT-pilot Regime and Article 3(3) MiCA.

14 Article 2(39) of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (**Data Act**).

## 2.3 Relevant laws and regulations

A broad range of EU and national laws and regulations can be relevant to individual blockchain infrastructures and use cases. Many of these laws and regulations are in the process of development or under review or have been adopted very recently while competent authorities on a national level still need to be designated. Moreover, existing laws and regulations have to be applied in a decentralised context which incurs new regulatory questions as well.

At the start of the project the following (proposed) areas of regulation and (proposed) DLT specific regulations/provisions were identified that could become relevant for the regulatory dialogues depending on the outcome of the selection process. The table below is not exhaustive and will need to be updated regularly.

| Generic relevant regulatory areas | Sector specific relevant regulatory areas | DLT specific regulations |
|---|---|---|
| • AI<br>• Commercial registers<br>• Cyber security<br>• Consumer protection<br>• Competition law<br>• Customs<br>• Data protection and data regulation<br>• Digital Identity<br>• Batteries / Digital Product Passports<br>• Environmental, Social & Governance (ESG) | • Automotive<br>• Crypto assets<br>• Energy & Utilities<br>• Education<br>• Financial markets<br>• Government<br>• Health<br>• Media<br>• Retail<br>• Trade & logistics | • MiCA Regulation[15]<br>• DLT pilot Regulation[16]<br>• Regulation on information accompanying transfers of funds and certain crypto-assets[17]<br>• Certain provisions in the Data Act[18]<br>• Provision in the proposed European Digital Identity Regulation[19] |

Relevant regulatory areas and DLT specific regulations (not exhaustive)

[15] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

[16] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (**DLT-pilot Regime**).

[17] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypt0-assets and amending Directive (EU) 2015/849.

[18] E.g. Article 2(39) and 36 relating to smart contracts in Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (**Data Act**).

[19] The last compromise text was published by the European Parliament on 2 March May 2023 and can be accessed here: https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html. On 8 November 2023, the European Parliament reached a provisional agreement with the Council on the new Regulation introducing European Digital Identity Wallets. The agreement reached by the co-legislators is now subject to formal approval by the European Parliament and the Council. Once formally adopted, the European Digital Identity framework will enter into force on the 20th day following its publication in the Official Journal. Based on the last amendments approved, recitals 34-35, Article 3 paragraphs (53-53a) and articles 45h and 45i (as amended) will be relevant for electronic ledgers.

Many of the regulatory instruments in the areas referred to in the above table have evolved in the past two years or are currently reviewed or in the process of development. Examples are the provisional agreement that was reached in December 2023 on the AI Act[20], the EC proposals for the reform of the EU Customs Union which were presented in May 2023[21], the Data Governance Act which is applicable since September 2023[22], the Digital Services Act that applies to so-called VLOPs[23] and VLOSEs[24] since the end of August 2023 and that will apply to all platforms from 17 February 2024[25], the Data Act of 13 December 2023[26], the provisional agreement by the co-legislators about the review of the eIDAS Regulation on 8 November 2023[27], the new European Battery Regulation which entered into force on 17 August 2023[28], the provisional agreement by the co-legislators about the Ecodesign for Sustainable Products Regulation on 5 December 2023[29] and the recently adopted corporate sustainability reporting directives.[30] Moreover, DLT specific EU regulatory instruments have been recently adopted: the DLT Pilot Regulation which became applicable on 23 March 2023 and the MiCA Regulation of 31 May 2023 that will become fully applicable on 30 December 2024.

All these changes in existing and proposed new EU legislation and regulations stress the relevance of the cross border dialogues as part of the European Blockchain Sandbox and the fact that this project is set up as a longer term project.

# 3. Set up of the regulatory sandbox

## 3.1 General observations

In order to set up the sandbox, engage with innovators, regulators/authorities and the wider community and to support the cross border regulatory dialogues the following project organisation was applied.

---

20 Commission welcomes political agreement on Artificial Intelligence Act, 9 December 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473.

21 EU Customs Reform: A data-driven vision for a simpler, smarter and safer Customs Union, 17 May 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2643.

22 Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data.

23 Very large online platforms.

24 Very large online search engines.

25 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services.

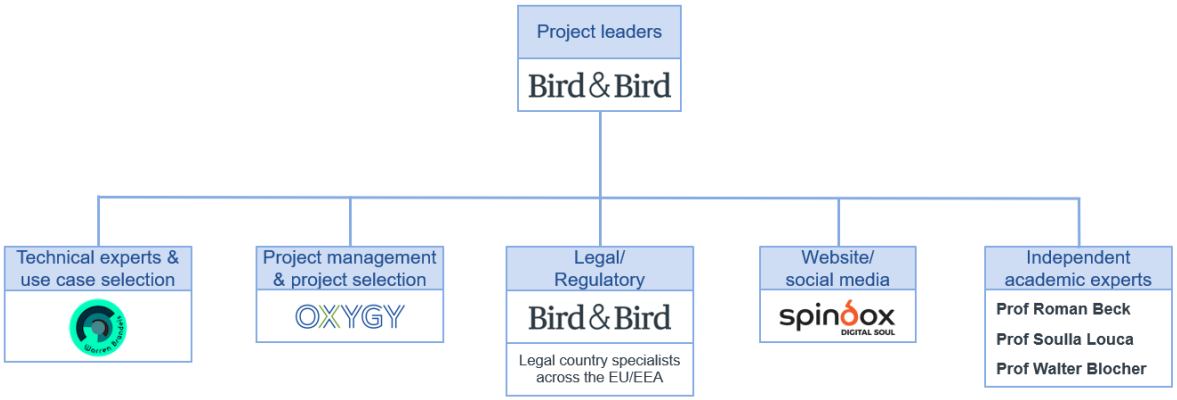
26 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (Data Act).

27 Commission welcomes final agreement on EU Digital Identity Wallet, 8 November 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651.

28 Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries.

29 Commission welcomes provisional agreement for more sustainable, repairable and circular products, 5 December 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6257.

30 The rules introduced by the Non-Financial Reporting Directive (Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups) remain in force until companies have to apply the new rules of the new Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 […] as regards corporate sustainability reporting.




The consortium is led by the international law firm **Bird & Bird** and its consulting arm **OXYGY**. The Bird & Bird offices and Bird & Bird cooperation firms cover all EU/EEA Member States. Technical expertise is provided by the technical blockchain experts from **Warren Brandeis** and the project website was designed by **Spindox**.

Specific attention is given to the fact that the selection of use cases for the different cohorts and the most innovative regulator award should take place in a non-discriminatory and transparent manner. Therefore, the selection of the use cases was led by independent blockchain specialists from Warren Brandeis. Bird & Bird has seconded legal expertise to the selection team but has not participated in the selection and does not have access to the applications. The selection process is supervised by a panel of independent academic blockchain experts consisting of **Professor Roman Beck** (Copenhagen University, Denmark), **Professor Soulla Louca** (University of Nicosia, Cyprus) and **Professor Dr. Dr. Walter Blocher** (University of Kassel, Germany). **Annex 1** provides a detailed overview of the project organisation.

## 3.2 Project website and external communication

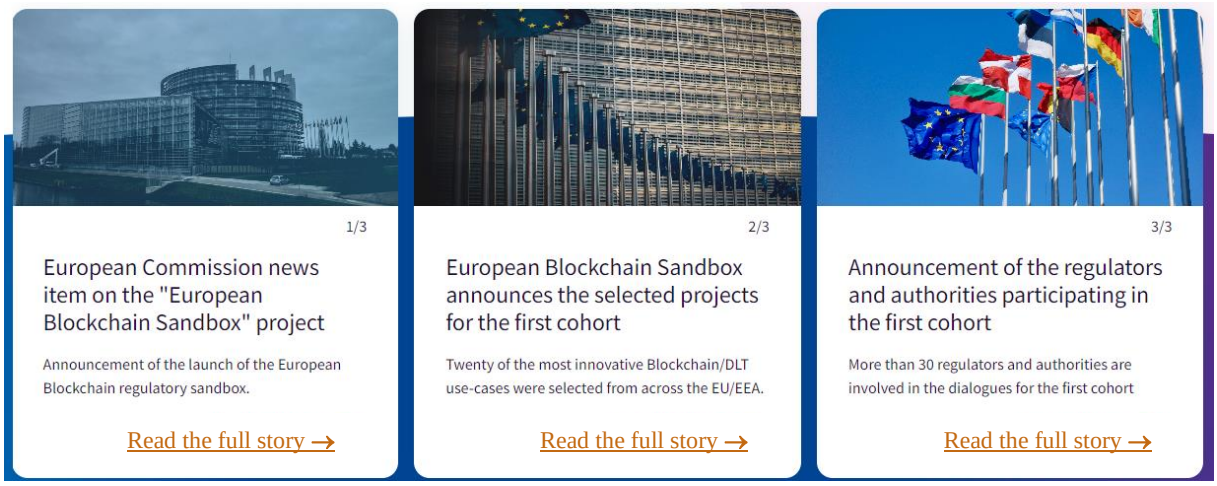
A project-specific public-facing website using the Europa domain was launched on 14 February 2023 at the launch of the application term for the first cohort (www.blockchain-sandbox.eu). The main functions of the public-facing website are to provide:

- Information on the European Blockchain Sandbox and the application and selection process for the different cohorts
- A brief description of the project organisation
- News items in relation to the project
- "Contact us" functionality (responses by e-mail: info@blockchain-sandbox.eu)
- FAQs, both generic and specific for the application process
- An interface to enable use case owners to submit their applications through EUSurvey during the application rounds.
- Best practices and lessons learned during the sandbox operations will be distilled and summarized in best practices reports that will be published on the website.


The website provides information and hyperlinks to the supporting documents including the Application Terms, the Protocol for Sandbox Participation, the Selection criteria for the use cases, the Application Form (accessible when the application process for a cohort is open), the Criteria for the annual Most Innovative Regulator award process and the Privacy Statements for the Sandbox application and selection and for the Onboarding and Operations. The main principles underlying the setting up, the population and the operation of the sandbox are laid down in the Protocol for Sandbox Participation.

News items were released and published on the website for each milestone that was reached:

| # | News item | Date |
|---|---|---|
| 1. | Announcing the launch of the European Blockchain Sandbox | 14 February 2023 |
| 2. | Announcing the start of the first application round | 14 February 2023 |
| 3. | Announcing the start of the selection phase | 17 April 2023 |
| 4. | Announcing the first cohort of 20 use cases | 3 July 2023 |
| 5. | Open invitation for regulators and authorities to participate in the European Blockchain Sandbox | 27 July 2023 |
| 6. | Announcement of the names of the participating use cases for the first cohort | 6 September 2023 |
| 7. | Announcement of the participating regulators and authorities for the first cohort | 7 December 2023 |



In order to keep the wider community informed about the developments, updates about relevant developments are shared via weekly newsletters in combination with social media posts.

### 3.3 Secure site

A secure site is deployed to provide access to documents and to share information in a secure and confidential manner. The secure site is used for reviewing the applications as part of the selection process and for the operation of the European Blockchain Sandbox in the dialogue phase.

Exchange of confidential information during the Sandbox dialogues takes place through the secure site. Participants are not able to download and disseminate information on the Access platform externally. Such information must remain on the platform.

### 3.4 Data protection compliance

Measures have been implemented to ensure that the sandbox is set up in full compliance with the applicable data protection rules laid down in particular in Regulation (EU) 2018/1725 (“EUI DPR”), Regulation (EU) 2016/679 (“GDPR”) and Directive 2002/58/EC (“ePrivacy Directive”). Further details are provided in **Annex 2**.

### 3.5 Conclusions, Best Practices and Lessons Learned – Setup of the European Blockchain Sandbox

The setup of the European Blockchain Sandbox, including the project organisation, the functionalities of the project website which is hosted on the EBSI site in the eu-domain and the operation of the secure site worked well. No technical and operational issues were experienced.

The term “sandbox” is used for different testing environments that often involve technical or operational testing and/or derogation from existing legislation or regulatory approval. The characteristics of the European Blockchain Sandbox are different compared to these other sandboxes. The European Blockchain Sandbox provides a framework for a confidential and cross-border regulatory dialogue between regulators/authorities and innovators. Use cases that are participating in the European Blockchain Sandbox are selected on the basis of transparent and non-discriminatory application terms and selection criteria. Moreover, the European Blockchain Sandbox does not provide a framework for derogation of certain laws or regulations and the participating use cases are not “approved” by the participating regulators/authorities. Also, the dialogues that take place as part of the European Blockchain

Sandbox consist of not more than two online regulatory dialogue meetings and do not include technical or operational testing.

Throughout the project these specific characteristics of the European Blockchain Sandbox continue to have to be explained in order to avoid confusion with other (regulatory) sandboxes. The European Blockchain Sandbox is in fact complementary to other sandboxes as it provides innovators and regulators/authorities the possibility to enter into a confidential and informal dialogue which can be followed up by an application to a sandbox that provides a legal/regulatory and/or operational testing environment. The potential synergies between the European Blockchain Sandbox and national regulatory sandboxes are explored in more detail as part of the matching process and the dialogues.

The relationship between the European Blockchain Sandbox and the European Blockchain Services Infrastructure (EBSI) incurred some questions as well. The European Blockchain Sandbox is open to private and public sector companies from all industry sectors and of all sizes (including start-ups and scale-ups) for blockchain projects beyond a proof-of-concept stage and already close to the market. Annually up to 20 private and public sector use cases can participate in the Sandbox. There are separate lots for i) microenterprises, ii) small enterprises, iii) medium-sized or larger enterprises and iv) public entities. The qualification of the enterprises depends on staff headcount and turnover or balance sheet based on EU Commission recommendation 2003/361. Five use cases from each category that meet the eligibility test will participate in the Sandbox if sufficient candidates are in the final shortlist. EBSI use cases that are proposed by the European Blockchain Partnership (EBP) are automatically qualified to participate in the sandbox if they submit an application before the end of the application term and fall within the category of public entities (Article 4.2 Application Terms).

# 4. Application process and selection for the 1st cohort

## 4.1 General observations

The website and the application process for the 1st cohort were launched on 14 February 2023, starting with a coordinated media campaign by the European Commission and the European Blockchain Sandbox consortium on 14 February 2023. The application term for the 1st cohort ran for two months ending on 14 April 2023 at 23:59 hrs CET.

Throughout the process, the project team has built a library of Frequently Asked Questions about the application and selection process. During the application term for the 1st cohort, more than 40 Q&As with respect to the application process were published on the website to ensure accessibility to the public in an equal and transparent manner.

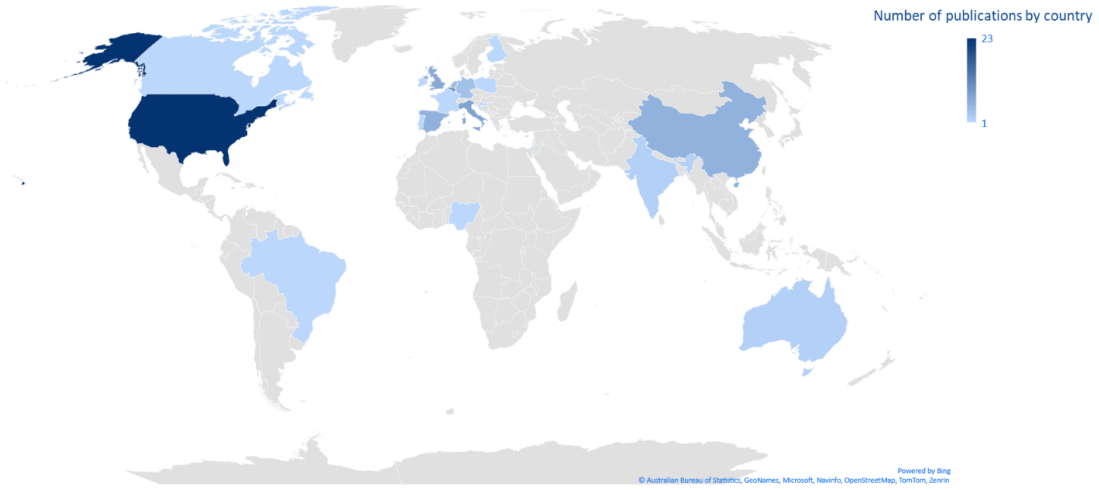
## 4.2 Outreach to use case owners

The aim of the outreach campaign was to create awareness among innovators throughout the EU/EEA explaining the objectives of the European Blockchain Sandbox and the application and selection process. The following benefits for use case owners were identified:

- Specialist legal and regulatory advice.
- Constructive regulatory dialogue and cooperation with national and EU regulators.
- Having input heard for the development of fit-for-purpose regulations.
- Opportunity to extend their network and reputation through participation in this pan-European project.
- No fee will be charged for the application and participation in the Sandbox.
- The opportunity to share and highlight needs for regulatory and legal certainty to regulators in a safe environment.

To attract relevant use cases and authorities/regulators and to ensure a balance of representation across sectors, countries, company types and blockchain applications, a multichannel approach was taken for calls for expression of interest including presentations at conferences/events, media interviews/publications, regular posts on social media, the project newsletter and a range of webinars. The activities were significantly supported by a press release and a news item of the European Commission and supporting activities by the consortium partners and the Bird & Bird network in all EU/EEA regions. All these activities funnelled traffic, generated by the multichannel campaign, to the public-facing website to increase awareness using a detailed understanding of the characteristics of the European Blockchain Sandbox, the selection process and the benefits for use case owners.

Presenting at conferences and webinars for blockchain use case owners, influencers, investors, and associations/communities, the project team had the opportunity to collect valuable feedback and gauge public reception. The blockchain ecosystem welcomes the project as a step to build critical bridges between regulators/authorities and use-case owners on a cross-sectoral basis and in a cross-border dialogue. The collaboration of respected blockchain stakeholders, including the European Blockchain Partnership (EBP), International Association of Trusted Blockchain Applications (INATBA), and the EU Blockchain Observatory and Forum, was invaluable in ensuring effective promotion and outreach of the initiative. The regulatory sandbox attracted considerable media attention, having been covered by 120+ publications from around the world (in Europe, the Americas,, India, China, and the Middle East).




*Representative spread of publications about the European Blockchain Sandbox in the weeks immediately following the launch of the applications process.*

### 4.3 The application process for the 1st cohort

The application term for the 1st cohort ran for two months ending on 14 April 2023 at 23:59 hrs CET. The Application Terms governing the applications, the Selection Criteria including the eligibility criteria and the award criteria and the Sandbox Protocol, governing the operation of the sandbox for the selected applicants were made available on the project website at the start of the application term. As mentioned above throughout the application process, the project team has built a library of Frequently Asked Questions about the application and selection process. During the application term for the 1st cohort, more than 40 Q&As with respect to the application process were published on the website to ensure accessibility to the public in an equal and transparent manner.

By the deadline on the 15th of April 00:00, almost 90 applications were submitted, which confirmed the keen interest by the blockchain innovators in the project as a step to build critical bridges between regulators/authorities and use-case owners across a range of industry sectors and in a cross-border dialogue. Applications were received from throughout the EU/EEA. There was one complaint received through the info@blockchain-sandbox.eu e-mail address which referred to a technical issue which prevented them from uploading all relevant annexes to their application. As no such issues were reported for any of the other applications, and the consortium has also not received such signals through other channels, it appears that this issue was not caused by the website or EUSurvey. A relatively small group of use cases did not pass the eligibility test mostly because mandatory annexes were missing.

### 4.4 Selection of use cases for the 1st cohort

Given the number of applications, a selection had to be made in accordance with the selection criteria as agreed with the European Commission and published on the project website.

Eligibility criteria included that the applicant must be established in the EEA and have been a legal person for at least six (6) months either as: i) a legal entity registered in the professional or commercial register according to the rules of the EEA Member State where it is established, or ii) a public body established in one of the EEA Member States. Moreover, the use case must be operated in the EEA but the fact that the use case could also operate outside the EEA is not a ground for exclusion. EEA-based companies can operate in a consortium with non-EEA companies provided that the beneficiary project in the Sandbox is under the lead of an EEA-based company. These eligibility criteria should also ensure that the use cases will have a sufficiently mature organization to participate in the sector.

Other eligibility criteria related to submitting a financial statement, an extract from a commercial register and a signed (in-person or electronically by a legal representative) and dated Declaration on Honour. In the FAQs that are published on the project website, a more detailed explanation is provided. These criteria have a more formal nature and act as requirements safeguarding that the applicants are serious about their application, are of good standing and can prove their statements about their establishment.

Lastly, eligible use cases should have a validated proof of concept. A validated proof-of-concept means that the DLT use case has been validated in a relevant environment. This should be determined in the context of EU-funded projects and specifically projects funded under the Horizon 2020 and Horizon Europe framework programs (the so-called TRL-levels). Normally speaking, the validated proof of concept test will be met if a solution is already implemented at clients of the applicant but evidence needed to be provided to be evaluated as part of the selection process.

Award criteria included three main parameters. The first parameter was the maturity of the use case. This was tested against TRL levels 5 to 9 to assess that the use case is ready to be commercialised or is already being commercialised in the EEA, meaning that use cases that are closer to commercialisation will get a higher score. The system of TRL levels was used to align with Horizon Europe funding and to ensure consistency for applicants to European Union projects. The second parameter was legal and regulatory relevance. The assessment of this criterion was done with an eye on the types of DLT used and the related novelty of the legal and regulatory challenges that are raised by the applicant. The final parameter was the relevance with EU's wider policy priorities, such as the Green Deal and Data Strategy. 40% of the total score was based on the maturity of the use case, another 40% was based on the legal and regulatory relevance and 20% was distributed based on the relevance with EU's wider policy priorities. Based on the award criteria, the applicants were awarded points based on their scores on the award criteria and a long list was created. An exception is the EBSI use case which qualified automatically. For the 1st cohort, one EBSI use case was proposed by the EBP to participate in the Sandbox and this use case automatically qualified to participate in the Sandbox in the public lot.

A further important element in the selection process was the lots. Shortlisted use cases were divided into lots – i) microenterprises, ii) small enterprises, iii) medium-sized or larger enterprises (based on the SME definition[31]) and iv) public entities. In principle, each lot was

[31] COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

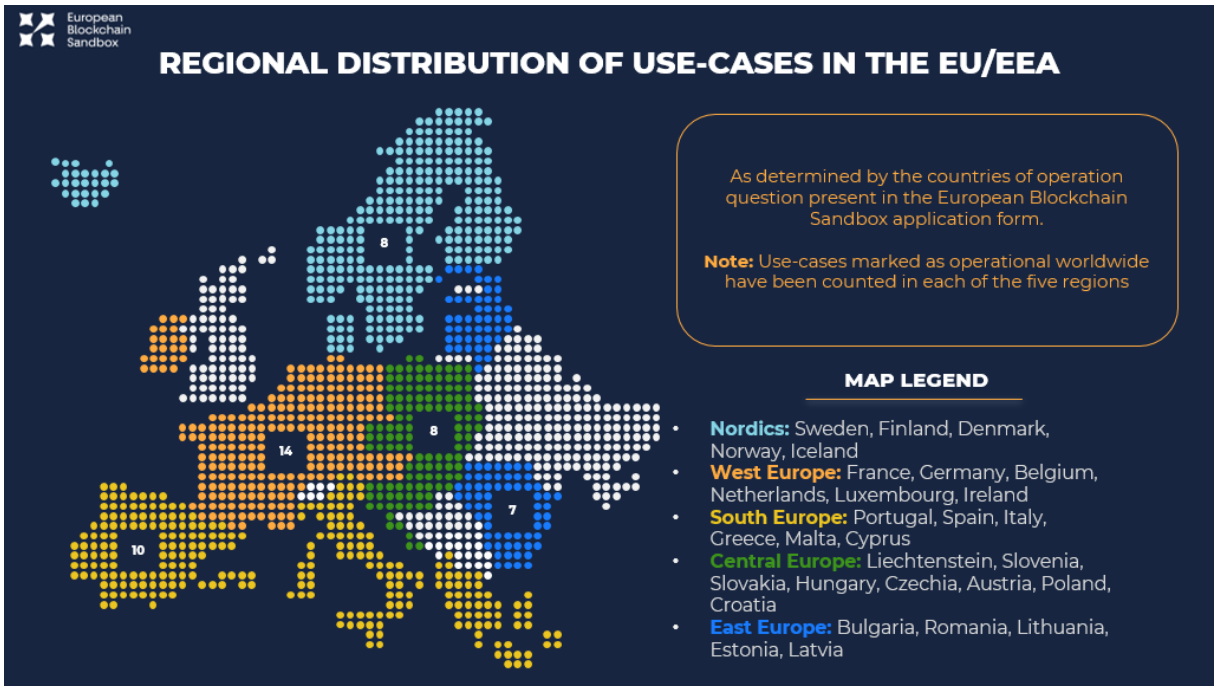
filled with five use cases. This meant that from the shortlisted use cases, the five best scoring ones in their respective lots were selected. If a lot could not be filled with five use cases (the public entities lot was not completely filled), the left-over spot(s) is (are) distributed amongst the next highest scoring use case.

Where use cases scored enough points to be eligible, tie breakers could be applied to determine which use case was going to be selected. The geographical uniqueness tie breaker comes into play if one of the EEA regions is underrepresented or not represented at all in the final shortlist of candidates. In that case the selection team, at its discretion, may select a use case from such a region that meets the eligibility criteria. The second tie breaker, the existence of regulator support, is applied as a tie breaker if use cases (within a lot) that are short-listed have similar scores that qualify for selection. A similar score is a score with 1 point or less difference, out of a total of 100 points.

The tie breaker "geographical uniqueness" was applied once for the 1st cohort to ensure that there was at least one selected use case established in every EU/EEA region. However, it should be noted that all EU/EEA regions are well presented in the 1st cohort in view of the fact that many DLT use cases are operational throughout the EU/EEA. The regulator support tie breaker was not applied for the 1st cohort.

The last step in the selection process was to meet the final eligibility criteria. In this phase, the shortlisted use cases were requested to submit additional documents and/or statements. Firstly, shortlisted use cases should go through the regular client acceptance procedure for law firms under European and national legislation. Second, shortlisted use cases were asked to agree with the engagement terms to the Sandbox, should provide evidence of good standing and should not have been involved in any insolvency or related procedures.

The outcome of the selection process for the 1st cohort was approved by the European Commission before the summer of 2023 and shows a balanced spread of use cases across the 5 EU/EEA regions as summarized in the graph below.



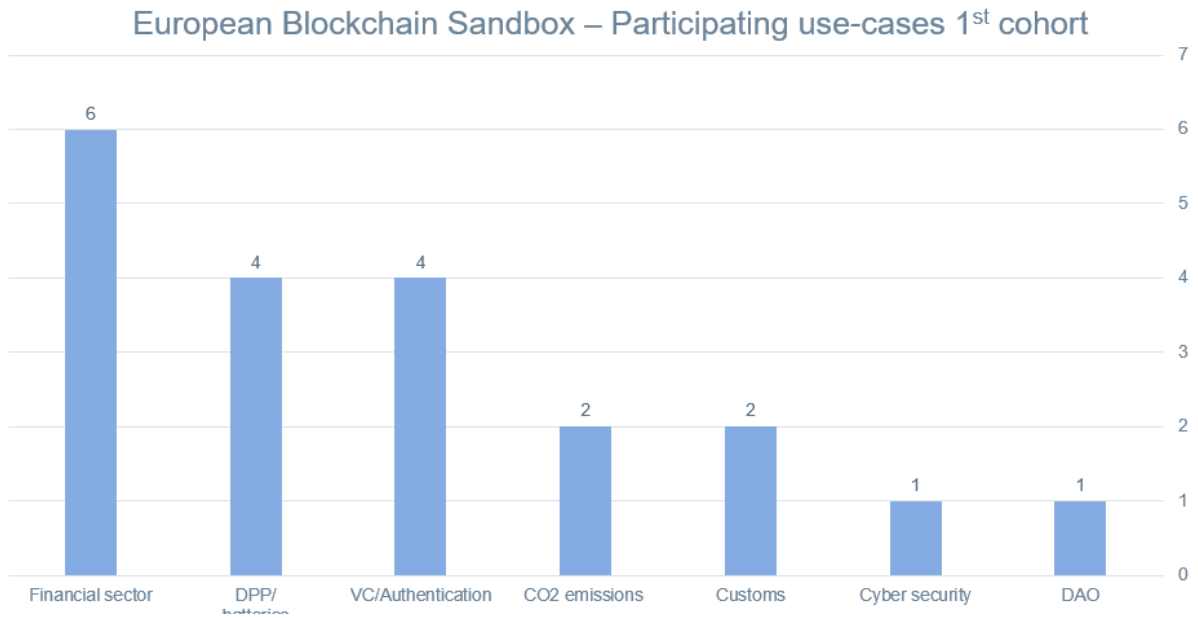
*Note that a selected use case can be operational in multiple regions, hence the numbering shown here may count a given use case multiple times. The selected use-cases are operational in all five EU/EEA regions, as per the objective of cross-geographic representation.*

Following the final eligibility check in accordance with the Application Terms the names of the selected projects for the first cohort were announced on the project website on 6 September 2023.

| | | | |
|---|---|---|---|
| ACCUDIRE | COINFIRM | EBSI Verifiable Credentials Use Case | INO MTÜ |
| Almaviva | Commissariat à l'énergie atomique | Equilibrium | Lokovice / unBlock (Murcia City Counsel, LleidaNetworks Serveis Telematics, Bankerex Financial, ES SOLO Holdings) |
| Anotherblock | Compellio (Uni Systems) | Eviden (Atos) | Stichting 2Tokens (Rabobank, ABN AMRO Bank, Catena Investment, Enercoin, Catena Power) |
| Blockchain Italia | deltaDAO | Fraunhofer (Open Logistics Foundation, ALS Holding) | Traent |
| Chunk Works | DNV | Globallogic (Nuggets) | Twinu |

Short descriptions for each of the use cases and the relevant regulatory topics in generic terms are included in the **Annex 3** to this best practices report. Eligible applications for the 1st cohort that have not been selected have the possibility to update their applications and participate in the application process for the 2nd cohort in early 2024.

The selected use cases for the 1st cohort are linked to a range of industry sectors and applications including the financial sector, digital product passports and battery supply chains, verifiable credentials/authentication, CO2 emissions, customs, cyber security and Decentralised Autonomous Organisations as shown in the table below.




## 4.5 Conclusions, Best Practices and Lessons Learned - Application and selection process 1st cohort

The application process showed a great interest from innovators in all EU/EEA regions and across industry sectors to participate in the European Blockchain Sandbox.

The application and selection process for the 1st cohort worked well and no significant technological, procedural or legal/regulatory issues were experienced. Consistent feedback regarding the application and selection process was that the applicants and regulators/authorities appreciated that all information about the application and selection process was made public on the website and that the selection process was done on the basis of transparent and non-discriminatory selection criteria by independent blockchain specialists and overseen by the panel of independent academic experts.

The Application terms, Application Form and Sandbox Protocol worked well. In view of the FAQs, some clarifications in the Application Terms and the Application Form are considered for the 2nd cohort.

Some of the lessons learned during the 1st round of the application and selection process may lead to certain adjustments of the application process including:

- The documents that need to be submitted together with the application, such as financial statements, may be simplified to reduce the chance of non-eligible applications. This means that not all documents will have to be submitted as part of the application and copies can be requested as part of the final eligibility test. Other documents, such as the extract of the commercial register / proof of incorporation, the Declaration on Honour and the documents that support the use case still need to be submitted as part of the application.
- The regulator support tie breaker could be further facilitated in the 2nd cohort by providing a template regulator support letter. It also needs to be clarified that

regulator support does not mean that the regulator has analysed or approved the use case but merely that the regulator or authority is prepared to join the cross-border dialogue for the use case as part of the project.

- Certain innovative use cases earned lower scores against the award criteria because technical novelty is not part of the award criteria. As technical novelty may be somewhat less relevant for a *regulatory* sandbox, it is considered to add "technical novelty" as another tie breaker.

Adjustments of the application process will be reflected in the documentation on the project website before the start of the 2nd round of applications.

# 5. Outreach to regulators and the matching process

## 5.1 Outreach to regulators

The outreach to regulators and authorities necessarily needed to be more generic at the beginning as the selected use cases for the 1st cohort were not yet known and the relevant regulatory areas for the first cohort still needed to be established. Around 500 regulators/authorities across the EU/EEA have been invited for regulator-only webinars. The first regulator-only webinar took place on 30 March 2023 and was attended by 57 regulator contacts. As there appeared to be a keen interest among regulators that were unable to attend to learn more about the project, a second regulator-only webinar was held on 26 April 2023 which was attended by 64 regulator contacts. The presentations and the recording of the regulator-only webinars were sent to all registrants (in total 190 regulator contacts). During the webinars, the setup of the European Blockchain Sandbox and the regulatory dialogues were presented.

The following benefits for regulators/authorities were identified.

- Discuss regulatory issues in a cross-border setting.
- Exchange experiences and ideas with innovators and other regulators.
- Increase access to knowledge concerning cutting-edge technologies.
- Support applications of use-cases for the Sandbox that are considered particularly relevant.
- Be credited as participants of the Sandbox.
- Contribute to the development of best practices and lessons learned included in the best practices report.
- Have the chance to be awarded as the "most innovative regulator" after the dialogues for each cohort.

## 5.2 Invitations of regulators and authorities to participate in the European Blockchain Sandbox

Based on the selection of use cases the most relevant regulatory areas for the dialogues for the first cohort and a tentative list of regulatory topics for these dialogues for each participating use case have been identified based on initial meetings with every use case owner.

| Regulatory focus areas area 1st cohort | Relevant (proposed) EU legislation per regulatory area[32] |
|---|---|
| **AML/KYC** | AML Directive[33] / Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets[34] |
| **Batteries & Waste batteries regulation / Digital Product Passports** | Battery Regulation[35] / proposed ESPR[36] |
| **$CO_2$ emissions** | European Union Emissions Trading Scheme[37] / MRR[38] / AVR[39] |
| **Commercial Registers / DAOs** | Company Law Directive[40] and other European company law instruments[41] including the Shareholders Rights |

[32] This list is not exhaustive and national legislation is not included.

[33] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. The European Commission has published a proposal to renew this Directive: Anti-money laundering and countering the financing of terrorism legislative package, 20 July 2021, which can be accessed via the following hyperlink: https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.

[34] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypt0-assets and amending Directive (EU) 2015/849.

[35] Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries.

[36] Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products (COM/2022/142 final) and the provisional agreement by the co-legislators about the Ecodesign for Sustainable Products Regulation on 5 December 2023 (https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6257).

[37] Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a system for greenhouse gas emission allowance trading, lastly amended by Directive (EU) 2023/959 of the European Parliament and of the Council of 10 May 2023.

[38] Commission Implementing Regulation (EU) 2018/2066 on the monitoring and reporting of greenhouse gas emissions pursuant to Directive 2003/87/EC of the European Parliament and of the Council, lastly amended by Commission Implementing Regulation (EU) 2023/2122 of 17 October 2023.

[39] Commission Implementing Regulation (EU) 2018/2067 on the verification of data and on the accreditation of verifiers pursuant to Directive 2003/87/EC of the European Parliament and of the Council, lastly amended by Commission Implementing Regulation (EU) 2020/2084 of 14 December 2020.

[40] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law.

[41] Company law | Fact Sheets on the European Union | European Parliament (europa.eu)

| | |
|---|---|
| | Directive[42], the Register Interconnection Regulation[43] and the Digital Company Law Directive[44] / AML Directive[45] |
| **Customs regulation** | Union Customs Code[46] / Implementing Regulation of the UCC[47] |
| **Cyber security** | NIS2 Directive[48] / CER Directive[49] / DORA[50] / Proposal for a Cyber Resilience Act[51] |
| **Data protection** | GDPR[52] / IDPR[53] |
| **Data governance** | Data Governance Act[54] |
| **DLT- and crypto asset specific regulations** | MiCA Regulation[55] / DLT-pilot Regulation[56] / Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets[57] |

42 Directive 2007/36/EC of the European Parliament and of the Council of 11 July 2007 on the exercise of certain rights of shareholders in listed companies.

43 Commission Implementing Regulation (EU) 2021/1042 of 18 June 2021 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers.

44 Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law.

45 See footnote 3433 above.

46 Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code. The European Commission has published a proposal to renew this regulation: EU Customs Reform: A data-driven vision for a simpler, smarter and safer Customs Union, 17 May 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2643.

47 Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of the Union Customs Code.

48 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

49 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities.

50 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

51 Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (COM/2022/454 final).

52 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

53 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

54 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance.

55 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

56 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology.

57 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypt0-assets and amending Directive (EU) 2015/849.

| | |
|---|---|
| **eIDAS / Digital identity regulation** | eIDAS[58] |
| **Financial markets regulation** | MiFID II[59] / MiFIR[60] / CSDR[61] / ECSPR[62] / EMD II[63] / PSD II[64] / Prospectus Regulation[65] / TFR[66] |

As a starting point, the competent regulators/authorities from the countries of establishment/main operations of the use case owners were approached. In addition, EU regulators and the relevant regulators and authorities who had expressed an interest in the sandbox dialogues were approached. In some cases additional invites were sent to regulators and authorities that were recommended by participating regulators and authorities. Finally, several other regulators and authorities were approached taking into account the geographical spread and relevance of the use cases.

Introductory meetings were offered to all regulators/authorities that were invited/interested. During these meetings an explanation was given about the (objectives of) the project and what it means for regulators/authorities to participate in the dialogues as well as the required time commitment.

### 5.3 Participating regulators and authorities

Regulators and authorities expressed considerable interest in participating in the European Blockchain Sandbox. By the end of 2023 more than 40 national and EU regulators/authorities with competences across the aforementioned regulatory focus areas for the 1st cohort and from all EU/EEA regions had accepted the invitation to join the 1st cohort sandbox dialogues for one

---

58 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. This Regulation is set to be amended by a new eIDAS regulation: Commission welcomes final agreement on EU Digital Identity Wallet, 8 November 2023, which can be accessed via the following hyperlink: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651.

59 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

60 Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/201, lastly amended by Regulation (EU) 2022/858 (DLT Pilot Regulation)

61 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (Central Securities Depository Regulation), lastly amended by Regulation (EU) 2022/858 (DLT Pilot Regulation)

62 Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937

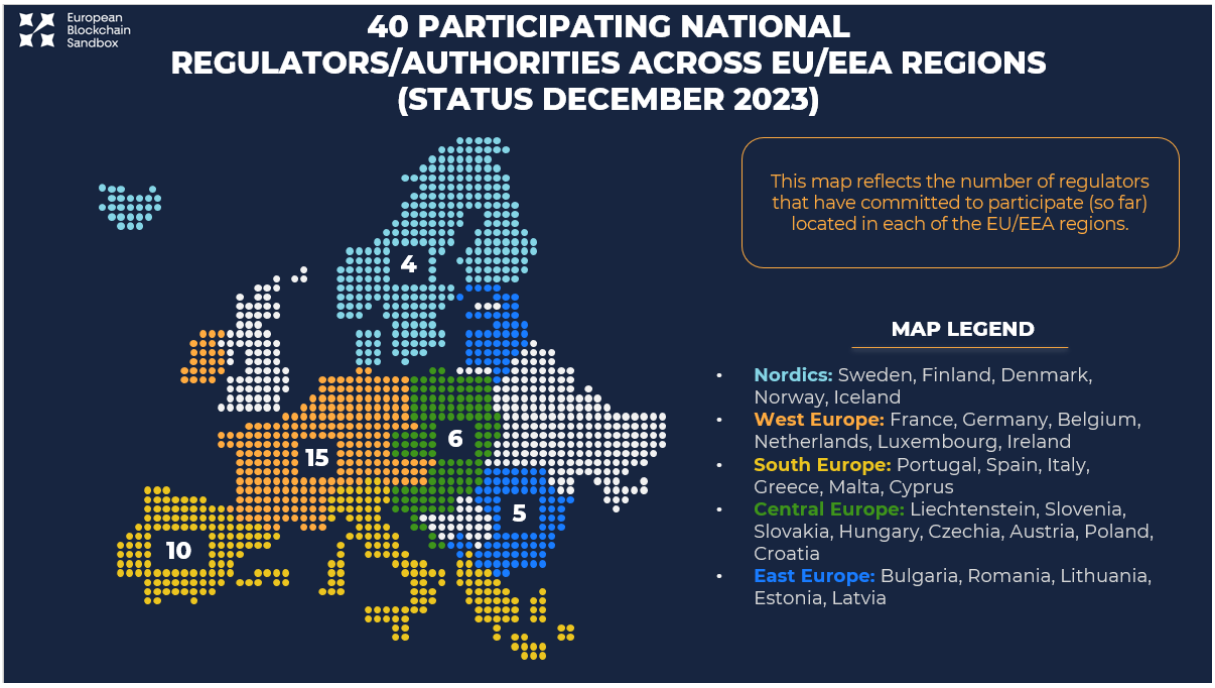
63 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

64 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

65 Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market.

66 Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets.

or more use cases.[67] A graph showing the spread of participating national regulators/authorities across the various EU/EEA regions is included below.




Several regulators/authorities participate in the dialogues for more than 1 use case. Therefore, on average more than 3 national and EU authorities participate in the dialogues for each of the use cases of the 1st cohort exceeding the aim of having an average of at least 1.5 regulator/authority per use case.

During the introductory meetings with the regulators/authorities, a range of questions have come up. These questions and answers are set out below and are or will be made available on the project website.

| Issues and questions raised during the introductory meetings | Answers / comments |
|---|---|
| **Regulators/authorities were not yet familiar with the European Blockchain Sandbox** | Objectives of the project and what it means for regulators/authorities to participate were explained during the introductory calls. |
| **Questions about potential overlap with national regulatory sandboxes or reservations to participate in a regulatory** | The European Blockchain Sandbox provides a framework for a regulatory dialogue about possible regulatory issues and solutions. The European Blockchain Sandbox does not |

[67] The list of participating regulators/authorities that already have agreed to be mentioned as participants in the dialogues can be found here: Announcement of the regulators and authorities participating in the first cohort - EBSI SANDBOXCollab - (europa.eu).

| | |
|---|---|
| **sandbox with a focus on testing/regulatory approval** | provide for a derogation of existing laws and regulations, nor does the sandbox provide any form of approval by the participating regulators/authorities of a certain use case. Synergies with national regulatory sandboxes are explored. |
| **Concerns regarding time commitment required to participate in the sandbox dialogues** | The sandbox dialogues include two online meetings of each 1.5 hours. The regulatory dialogues are preceded by an optional one-hour session for the participating regulators/authorities with the blockchain experts in the consortium. |
| **Questions about the role of the regulators and authorities in the regulatory dialogues** | The roles of the regulators and authorities can range from active preparation/participation to a semi-observer/learner role. Active participation normally adds value if there are regulatory topics or questions that are considered specifically relevant and should be added to the agenda. Active participation also provides the possibility to test views and ideas with the other regulators/participants in the dialogue meetings. Participating as an observer/learner would have the advantage that the participation is less time-consuming, and it might help to become familiar in an efficient way with typical questions/topics in relation to new technologies (DLT/Blockchain) and/or in relation to new areas of regulation. |
| **Concerns regarding (too) little knowledge about blockchain/DLT technologies** | In fact, this is a good reason to join the sandbox as one of the aims of the European Blockchain Sandbox is to enable regulators and authorities to enhance their knowledge about blockchain/DLT technologies which is also the reason why the separate sessions with the blockchain experts for the participating regulators and authorities are offered. |
| **Questions if the regulator/authority has the right competences for the regulatory dialogue in relation to a specific use case** | Clarification of the tentative regulatory topics for each use case. Sometimes introductory meetings led to subsequent invitations to other competent regulators |
| **New laws and regulations have not been adopted or implemented.** | Under these circumstances, it can be more difficult to find the relevant regulators/authorities. However, a dialogue can still be helpful to discuss not only the application of existing laws and regulations |

| | |
|---|---|
| | but also the question if certain regulatory topics will/can be solved in new laws and regulation. |
| **Regulators/authorities have not yet been appointed** | If it is clear which competent regulator or authority will be appointed, a regulatory dialogue can be useful and efficient. |
| **Reluctance to favour a specific use case** | This question was solved by clarifying the non-discriminatory, transparent application and selection process and the role of the panel of independent academic experts |

### 5.4 Conclusions, Best Practices and Lessons Learned - outreach to regulators and the matching process.

The outcome of the matching process with more than 40 participating regulators and authorities and on average more than 3 participating regulators/authorities per use case dialogue is encouraging and exceeding the aim and expectation of at least 1.5 regulator per use case dialogue. Moreover, almost all regulatory focus areas for the 1st cohort are covered.[68] Regulators and authorities are not specifically interested in use cases established in their home country but in particular in the regulatory topics for the dialogues for each of the use cases.

The matching process took several months which was needed to set up the introductory meetings and to answer follow-up questions while the regulators and authorities needed time for internal alignment and approval and sometimes for alignment with other competent authorities for the same regulatory area.

In most regulatory areas, there is a balance between the number of use cases and the participating regulators/authorities such as in the financial sector where the use case owners as well as the regulators/authorities expressed a clear interest in participating in the European Blockchain Sandbox and the regulatory dialogues. In other regulatory areas, there was more of a discrepancy, in particular for digital product passports/battery regulation which is a focus area for 4 use cases in the 1st cohort. The reason appears to be that the EU legislation in the area of digital product passports is not yet harmonized and there is no specific DLT legislation in place.

[68] Only the regulatory focus area “consumer protection” is not covered in the regulatory dialogues for the 1st cohort but will likely become relevant again in the 2nd cohort.

# 6. The dialogue phase

## 6.1 Structuring of the dialogue phase – first experiences

At the time of publication of this Best Practices Report, the first regulatory dialogue meetings have been held and others have been scheduled. The meetings are organised in accordance with the project's Protocol for Sandbox Participation.[69] The nature of the dialogues depends on the regulatory focus area, whether there is harmonized EU legislation in place and the maturity of such harmonized legislation. In areas where regulators and authorities have to deal with DLT use cases on the basis of existing laws and regulations (such as in the financial sector), the dialogues have a clear focus on the relevant regulatory topics that need to be addressed in the application of such laws and regulations in different Member States. In those areas where EU harmonized legislation is not yet in place, such as in the area of digital product passports, the emphasis of the dialogues will be more on the lack of applicable laws and regulations and how this could be addressed.

The dialogues follow the following protocol:

- One-hour technical blockchain session
  - *per dialogue; regulators/authorities-only;*
  - *run by consortium blockchain experts - about blockchain infrastructures and applications in general; and*
  - *with a focus on relevant industry sector or area for the dialogue*.
- The one-hour technical blockchain session can also be used to prepare the 1st dialogue meeting.
- Onboarding webinar of 15 minutes (recording available on the site).
- First use-case dialogue meeting (1.5 hours, online).
- Second use-case dialogue meeting (1.5 hours, online).
- Provide feedback by submitting a feedback form via EUSurvey.

In the feedback form, the participants (both the use case owners and the regulators/authorities) are asked if participation in the European Blockchain Sandbox dialogues has met their expectations from a content and a time commitment perspective and how they would rate the dialogue meetings. In addition, the participants are requested to share any recommendation for additional regulatory topics for future dialogues and if they have any suggestions for improvement of the dialogues in the next cohort.

To ensure an efficient use of time, relevant information and materials are made available on the secure platform in advance of the dialogue meetings. The agendas for the dialogues for the different use cases are determined on a case-by-case basis to ensure an efficient and effective dialogue and shared before the start of the dialogue meetings together with other relevant information. This includes, e.g., general information about the use case and a slide deck containing specific information about the use case. Depending on the use case, the regulatory area(s), the competences and expertise of the participating regulators/authorities,

[69] This Protocol can be accessed through the following hyperlink: https://ec.europa.eu/digital-building-blocks/sites/download/attachments/634979024/Sandbox%20Protocol%20for%20Participation%20-%20FINAL%202023-02-13.pdf?version=1&modificationDate=1676320692356&api=v2.

the roles of the regulators/authorities can range from active preparation/participation to a semi-observer role. Regulatory experts from Bird & Bird take the lead in preparing the agenda for the dialogue meetings, but the use cases and the participating regulators/authorities can take an active role in these preparations and are invited to share their expectations regarding the dialogues and to contribute regulatory topics for discussion.

Best practices & lessons learned that could be communicated externally are shared in draft at the end of each dialogue meeting for review/comments by the participants. Best practices and lessons learned are only published with the consent of the participants.

### 6.2 Conclusions, Best Practices and Lessons Learned dialogue phase.

Based on the first experiences, the format for the dialogues consisting of an optional session with the blockchain experts for the participating regulators/authorities which can also be used for the preparation of the dialogues and followed by two online 1.5 hour meetings appears to work well, given that the European Blockchain Sandbox dialogues do not involve actual testing and regulatory approval. There are, however, differences in approach:

- For use cases which incur not too many regulatory topics which are relevant for all Member States, a larger group of regulators/authorities from different jurisdictions appears to work well.
- For use cases which incur a range of different regulatory topics under various legal instruments, a more in-depth dialogue with specific regulators/authorities appears to work better as a first step.
- For use cases with a focus on laws and regulations which are being developed, a broader group of participating regulators and authorities from different jurisdictions and on EU level appears to work best.

A full report with the best practices and lessons learned that have come out of the dialogues will be published after the dialogues for the 1st cohort are complete. This follow-up report will also include a more detailed assessment of the effectiveness and efficiency of the format for the regulatory dialogues.

## 7. Next steps, looking ahead

In the first half of 2024, the regulatory dialogues for the 1st cohort will be continued and completed. Best practices and lessons learned which have been and will be identified during the dialogues will be covered in more detail in a separate report after completion of the dialogue meetings.

In parallel, the applications for the 2nd cohort will start with again an application term of 2 months, likely followed by a selection phase.

The regulatory dialogues for the 2nd cohort are expected to start in the second half of 2024. The regulatory focus areas for the 2nd cohort will likely not be the same as for the 1st cohort.

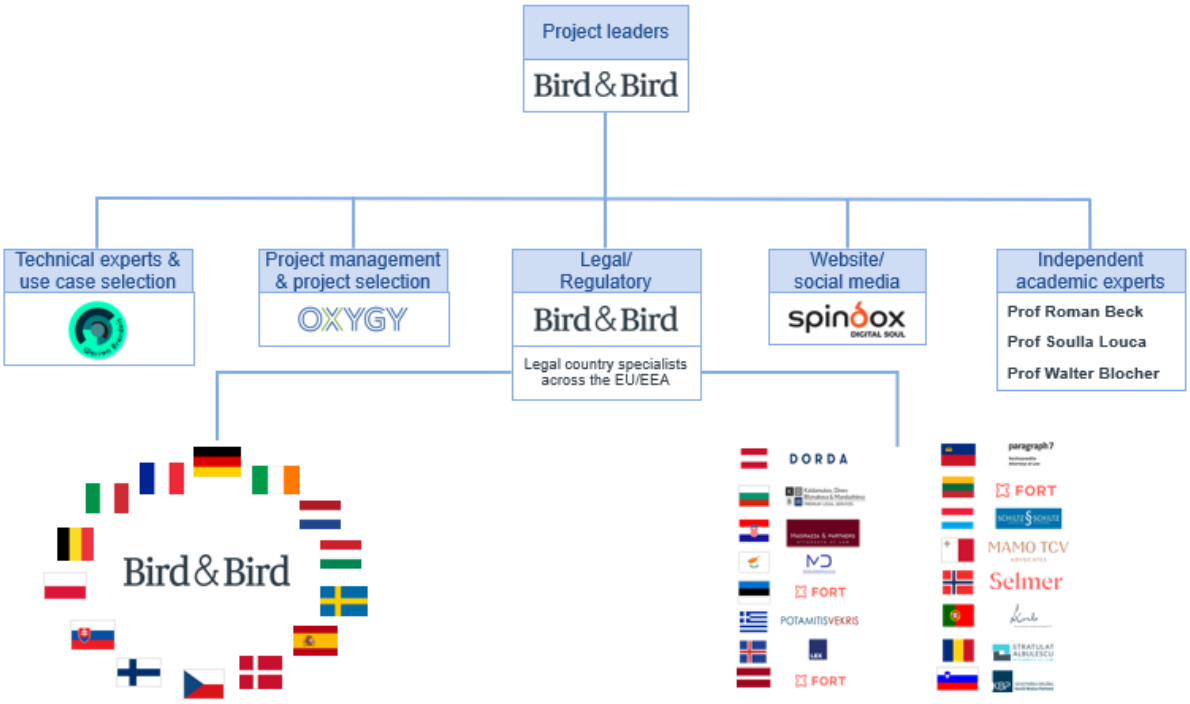
The recently adopted amendments and ongoing reviews of existing EU legislation and proposed new EU legislation referred to in paragraph 4.3 stress the relevance of the cross-border regulatory dialogues. For the 2nd cohort, additional and new regulatory areas such as the AI Act, the Data Act, eIDAS2 and the implementation of ESG regulation could become relevant.

# Annexes

## Annex 1. Project organisation

European Blockchain Sandbox – an initiative of the European Commission

*The project will be run by the following consortium of experts:*



## Annex 2. Data protection compliance

As briefly mentioned in paragraph 3.4, measures have been implemented to ensure that the sandbox is set up in full compliance with the applicable data protection rules laid down in particular in Regulation (EU) 2018/1725 ("**EUI DPR**"), Regulation (EU) 2016/679 ("**GDPR**") and Directive 2002/58/EC ("**ePrivacy Directive**").

The principles of data protection by design and data minimisation are the guiding principles for the setup of the public website, the application and selection process and for the sandbox operation. In all cases, appropriate technical and organisational measures are taken to ensure an appropriate level of security based on an assessment of the risk of the data processing.

The application and selection process is set up in such a way that no personal data is collected unless this cannot be avoided. This means more concretely that only legal entities can apply for participation in the regulatory sandbox. Applicants accept the application terms before they can submit their application for participation in the European Blockchain Sandbox and agree to only share personal data in the application form when this cannot be avoided. They also must ensure that applicable data protection rules are complied with if they share personal data and provide a copy of the privacy notice for applicants and participants in the European Blockchain Sandbox to their employees or any other data subjects of whom they share personal data. The application form itself will be hosted on EUSurvey. After submission the application forms will only be available for the blockchain specialists in the consortium and the panel of independent academic experts in accordance with the Application Terms as needed for the selection process.

The same principles guide the sandbox operations. Sandbox participants will need to accept the Sandbox Protocol for participation and are informed about the Privacy notice before they can get access to the sandbox. They also must ensure that applicable data protection rules are complied with if they share personal data and provide a copy of the privacy notice for the Sandbox operation to their employees or any other data subjects of whom they share personal data. Access to information on the platform will be restricted and on a need-to-know basis. At the end of the sandbox operation, the participants will be blocked from accessing the platform and the data will be archived.

The Privacy notices for the Sandbox Application and selection and the Sandbox Onboarding and Operations set out what rights data subjects have and how they can execute these rights. Appropriate technological and organisational measures are taken to ensure that these rights can be complied with where appropriate.

Any processing of personal data on the website or the Access platform for the purposes of the sandbox will be done by Bird & Bird and its subcontractors as data processors on behalf and under the instructions of the European Commission as data controller. Bird & Bird and its subcontractors are bound to contractual terms that meet the requirements of Art. 28 GDPR/Art. 29 EU IDPR. The Commission is not responsible for any processing of personal data by the sandbox participants outside of the regulatory sandbox. Under the Application Terms and the Sandbox Protocol, the relevant participants will be solely responsible and liable for any such processing.

## Annex 3. Use case descriptions 1st cohort

1. ACCUDIRE
2. ALMAVIVA
3. ANOTHERBLOCK
4. BLOCKCHAIN ITALIA
5. CHUNK WORKS
6. COINFIRM / LUKKA
7. COMMISSARIAT À L'ÉNERGIE ATOMIQUE
8. COMPELLIO (UNI SYSTEMS)
9. deltaDAO
10. DNV
11. EBSI VERIFIABLE CREDENTIALS USE CASE
12. EQUILIBRIUM
13. EVIDEN
14. FRAUNHOFER (OPEN LOGISTICS FOUNDATION, ALS HOLDING)
15. GLOBALLOGIC (NUGGETS)
16. INO MTÜ
17. LOKOVICE / UNBLOCK (MURCIA CITY COUNSEL, LLEIDANETWORKS SERVEIS TELEMATICS, BANKEREX FINANCIAL, ES SOLO HOLDINGS)
18. STICHTING 2TOKENS (RABOBANK, ABN AMRO BANK, CATENA INVESTMENT, ENERCOIN, CATENA POWER)
19. TRAENT
20. TWINU

**ACCUDIRE**


ACCUDIRE's use case was conducted in July 2021 and presented two months later in Trieste during the conference "Italy Smart Export". The "Pilot 1.0" was a shipment from Italy to Turkey with a complete digitisation of the logistics documentation and interoperability between public and private subjects involved. It was the first fully digital shipment exploiting blockchain technology in Italy and Europe, and it involved the following players: Benetton Group (exporting company), Port of Trieste (customs and place of departure for the Ro-Ro shipment), ADM (the Italian Customs Agency which gave a quality check about the correctness of the process), a global freight forwarder and a Turkish Import Company. The shipment has been made using the ACCUDIRE platform and creating an e-CMR (Electronic Consignment Note for road transportation). The identities of the subjects involved have been verified through two-factor authentication and their signatures have been geolocated and saved on blockchain, interoperating with AIDA (ADM's software) and sending the pre-arrival notification of goods to the PCS (Port Community Systems) to facilitate the truck entry procedure. Specifically, the e-CMR document needs 3 signatures (sender, carrier and receiver) and ACCUDIRE saves on the blockchain these signatures (including geolocation, identity and all other relevant information) in order to guarantee immutability, traceability and security of the shipping-related information in accordance with the requirements of the authorities. Blockchain used is a permissioned Hyper Ledger Fabric supplied by TrustedChain with nodes all in Italy at AgID (Agency for Digital Italy) qualified entities (Trust Service Providers, according to the eIDAS-regulation) and has been chosen to make the processes fully verifiable and robust even in case of inspections and audits.

The results of the pilot were satisfactory, and the participants were particularly enthusiastic and willing to work in synergy towards the same direction: a smoother, more transparent, and efficient supply chain on global markets. The feedback was so positive that the pilot has been inserted as a use case of the DTLF and mentioned in Subgroup 1 (Paperless Transport) of the e-FTI (Electronic Freight Transport Information) discussions, which is regularising and formalising digital processes related to the transport of goods across Europe. Finally, with great satisfaction, it has been selected as one of the 20 use cases that will participate in the first cohort of the European Blockchain Sandbox.

The challenges are there and are mostly related to culture and regulation: today, companies and logistics operators are used to work in a traditional way with poor digitisation. The operational and economic environment is opaque, lacking in transparency, with a high risk of falsification of logistics and customs documents and a high exposure to administrative sanctions. The players along the supply chain are many, struggle to communicate with each other and generate a slow and complex flow. For them, embracing digital transformation is not immediate or simple thus the difficulties are more in preparing the market to accept new technologies than technological in the strict sense. Similarly, national and international regulations and laws mention digitisation, security, traceability and other features that are protected by blockchain technology; however, they hardly ever speak explicitly about blockchain, and this makes the regulatory situation opaque and unprofitable for those proposing innovative solutions that exploit DLT.

Despite the difficulties, the impact of the use case has been relevant for Italy and Europe. The pilot represented the first shipment with fully digitised documents and processes with blockchain, simplifying all the procedures and especially the dialogue between public and private players

involved. Thanks to the pilot, it was possible to learn and demonstrate that the identified solution was fully functional, and now exporting companies, logistics operators, and authorities (Customs Agencies and Port Authorities) know that can operate completely digitally through a paperless and eco-friendly approach preserving "Made in" and protecting products against counterfeiting. Thanks to logistics digitization, companies can reduce costs, maximise margins, decrease waste and work in synergy with the many other actors involved along the chain. In addition, this paves the way for opportunities to also connect trade and trade finance, simplifying the flow of financial information and thus the payment of the goods and the dialogue between banks and firms.

In a nutshell, there is still a long way ahead, but the value of digitising logistics processes exploiting blockchain technology is now clear to operators, who are increasingly keen to approach interoperable and innovative solutions.

## ALMAVIVA

### Giotto OnChain Notarization SaaS

### PROJECT SNAPSHOT

Giotto OnChain Notarization SaaS represents a cutting-edge evolution in blockchain notarization applications. This service certifies the authenticity and integrity of digital assets by assigning a timestamp and an identifiable owner to each transaction. Its significance lies in easing the accounting burdens associated with cryptocurrency management and technological integration for businesses and Public Bodies, offering compatibility with various blockchains thanks to the API model and a flat-fee paid upfront instead of purchasing crypto-currencies to pay for transaction costs. As a Software as a Service (SaaS) platform, it employs blockchain, other decentralized technologies, and cloud services to enable notarization on public blockchains like Ethereum and Bitcoin. Additionally, it adheres to the European Blockchain Services Infrastructure (EBSI) standards and produces Chainpoint-compliant interoperable receipts, ensuring verifications can be done independently of the originating Service.

### CHALLENGES & OPPORTUNITIES

The service, that we implemented internally to certify AlmavivA's press releases[70], overcomes traditional challenges of blockchain applications such as data privacy and cryptocurrency management, providing key benefits to the industry.

***Operational***: by simplifying the integration of blockchain services with IT systems, offering scalability through global, national, or EU infrastructures thanks to the API model to maximise interoperability and integration with existing and future systems.

***Commercial***: by providing cutting-edge features and qualified tools, it ensures regulatory compliance and enhanced data security.

***Social and Public (Digital Identity & Timestamping)***: by enhancing the transparency of public documents and processes, it increases trust and social impact, particularly for citizens and public administrations, ensuring proof of ownership and authenticity, linked to identity, of any type of file to prove its originality and existence at a certain date and time.

***Economic***: by eliminating cryptocurrency risks from customer balance sheets and ensuring true disintermediated verification, it fosters economic reliability.

[70] https://www.almaviva.it/en_GB/Press-Release/show-pressrelease/d040a37c-8a81-4a05-a4bd-9f4f436677d1/AlmavivA-launches-a-document-certification-service-using-Blockchain-Technology.

***Technical & Privacy***: by optimising multiple operations performing a notarisation round, from which receipts are generated, it prevents the appearance in the receipts of other customers data hashes, ensuring data privacy.

Adoption: by simplifying access to qualified blockchain services published in relevant marketplaces such as the Italian National Cybersecurity Agency (ACN)[71] for Institutional and Public Administration adopters and AWS[72] one for private business adopters.

**INSIGHTS & LEARNINGS**

The technical features of Giotto OnChain Notarization SaaS make it a service suitable in contributing to the European Strategy for Data's interoperability pillar, avoiding vendor lock-in and enabling trustless verification. This aspect is crucial for cooperation between public bodies and private entities. The service is also instrumental in R&D projects related to carbon footprint certification, supporting enterprises in achieving their ESG goals under the European Green Deal. Furthermore, its role in certifying information authenticity is a key tool in combating fake news and misinformation, thereby supporting media pluralism, and preserving European democracy.

71 https://catalogocloud.acn.gov.it/service/1562.
72 https://aws.amazon.com/marketplace/pp/prodview-dl6qrdhuzxngc.

## ANOTHERBLOCK


Introducing Anotherblock, a revolutionary platform powering emotional and financial bonds between creators and consumers.

The platform provides a space for music creators to sell their fractionalised and tokenized music rights directly to investors. Utilizing cutting-edge blockchain technology, Anotherblock has implemented music ownership tokens based on the ERC-721 standard (the NFT standard) on Ethereum and Base.

Each token is endowed with a unique custom ID, securely storing a certain percentage of music rights ownership for a particular song on the blockchain. These tokens not only feature distinctive artworks but also embody real-world legal contracts, outlining the terms of streaming royalties and guaranteeing the investor's legitimate ownership rights. This innovative way of selling NFTs linked to an underlying asset in the form of music rights introduces a groundbreaking model for both the traditional music industry as well as the financial sector. Fractionalizing future income from streaming royalties lets investors earn yield from assets uncorrelated with financial macro environments and gives creators the possibility to finance their artistic creation without debt to record labels or music publishers.

Through Anotherblock, creators gain the unprecedented opportunity to sell their music rights directly to consumers, ensuring a fair and transparent transaction. By eliminating intermediaries, creators secure a fair price for their music rights while retaining control over their artistic endeavors. For consumers, Anotherblock offers a possibility to invest directly into individual tracks and be part of the potential future financial upside along with the creators. Anotherblock's platform pioneers a seamless and inclusive music investment experience, providing a win-win solution for both creators and consumers.

Anotherblock is innovating on all fronts, and is engaging all of its stakeholders - the music industry, fans, consumers and more - in an effort to create a fair market for music rights. Amid this innovation, it's crucial for Anotherblock to recognize and manage risks. Anotherblock sees a great opportunity in being a part of the European Blockchain Sandbox to get the chance to address practical challenges arising in relation to classify music right NFTs under Financial Services Regulation and MiCAR and to increase legal certainty for blockchain and tokenization solutions with underlying real-world assets for the purpose of foster a safe environment for consumers and businesses.

## BLOCKCHAIN ITALIA

### Project Snapshot

Our use case pertains to notarization and tokenization services associated with the administration of diverse digital documents. It is specifically dedicated to overseeing the entire document lifecycle, encompassing data storage, preservation systems, and the processes of validation and signature. The incorporation of blockchain technology into these processes, coupled with other technological solutions such as digital identity access or decentralized storage, represents a significant innovation aimed at enhancing procedural efficiency.

### Challenges & Opportunities

Presently, the primary challenges revolve around acknowledging blockchain technology as an adequate instrument to supplement signature tools and expand the spectrum of certification processes to include new participants. Moreover, there is a documented disparity at the European level concerning digital identity, marked by the simultaneous presence of various recognition methods. In this context, on the one hand, there is a need for dialogue to integrate the EUDI Wallet and verify the requirements necessary to initiate the process, and on the other hand, to determine how the blockchain can integrate the functions of notarization and signing of documents and, above all, what the technical and legal requirements are to initiate a complete and effective integration.

Given the above, it is essential to engage in discussions with regulators, and integrating solutions endorsed by the European Union holds the potential to streamline the exchange and signing of documents among European citizens.

A collaborative effort with regulatory bodies could prove pivotal in establishing guidelines for the judicious utilization of these technologies.

In conclusion, the main objective is to find the right tools, in terms of integrating blockchain technologies, to identify an effective model to manage, store, and sign documents in a streamlined and fast way, which is recognized by the European legislator and Member Countries' legislators, solving conflicts in terms of certification, data storage, and privacy.

### Insights & Learnings

The inclusion in the European Blockchain Sandbox represents a significant opportunity to address critical aspects surrounding several gaps, particularly concerning the integration of the EUDI Wallet and the broader application of the eIDAS regulation.

Notably, divergent perspectives have emerged regarding the application of blockchain technologies and processes compliant with the General Data Protection Regulation (GDPR). These aspects are expected to play a pivotal role in the forthcoming dialogues with regulatory bodies.

Conversely, positive feedback has been received from clients and investors regarding our participation in the Sandbox project.

Concerning the path currently taken in our use cases, we can affirm the willingness of our clients to identify tools that use blockchain solutions to improve document processes: the pilot project initiated with BNP Paribas in Italy, for example, has obtained positive feedback both from a legal point of view, configuring for the flows involved the required level of Advanced Electronic Signature, and from an operational point of view, improving problems related to uploading or forwarding documents and significantly reducing the time it takes to sign paperwork, as well as reducing abandonment rates.

## CHUNK WORKS

### Chunk Works: next-gen data security

Chunk Works helps organizations make their cybersecurity future-proof. Its software ensures they are prepared not only for today's challenges but also for the uncertainties of a quantum computing breakthrough.

### QuSec: quantum-resistant end-to-end security software for critical data

QuSec is a robust, software-based solution that protects critical data. It is designed to pair multiple encryption options into a single, simple-to-implement software product, defending against present ransomware and future quantum computing attacks. QuSec gives enhanced control over cryptography, ensuring the ongoing safety of data assets.

### Key features of QuSec

QuSec offers universal compatibility as a highly adaptable data security layer made to integrate with existing on-premise, cloud, applications, and IoT infrastructure. It provides security for data at rest by acting as a vault, protecting critical data from ransomware. Through quantum resilience, it also protects all data passing through your infrastructure against so-called Harvest Now, Decrypt Later attacks, which could be intercepted now and decrypted later when quantum computers emerge.

### Benefits for organizations

QuSec's seamless integration with existing infrastructure allows for rapid deployment. This minimizes downtime and ensures business continuity. Its future-proof architecture keeps organizations' cybersecurity ahead of emerging threats with crypto-agility. QuSec's adaptable, modular design safeguards robustness without disruptive system updates. The flexible approach to libraries and algorithms ensures any standardized and certified cryptography can be imported, simplifying documentation for audits.

### Current developments

The first customers are currently implementing and testing QuSec. Chunk Works is also working with selected implementation partners and resellers to scale up deployment with more and larger customers to provide them with a future-ready, quantum-resistant data infrastructure.

## COINFIRM / LUKKA

Lukka®

# Coinfirm Analytics and Coinfirm Investigator Use Case

## Project Snapshot

Coinfirm Analytics and Investigator solutions involve the gathering and analysis of blockchain data from multiple sources, including on-chain, off-chain, and shared intelligence data sources. Through advanced algorithms, we process this data to provide forensic-level knowledge of asset flows related to crime and money laundering. Our primary goal is to support crypto market participants in meeting regulatory requirements and combat financial crime in the blockchain ecosystem. This use case is significant in the context of blockchain innovation as it enhances trust and transparency in the industry, ensuring compliance with anti-money laundering (AML) and counter financing of terrorism (CFT) regulations.

## Challenges & Opportunities:

One of the main challenges we face is the ever-evolving nature of financial crime and the need to constantly adapt our algorithms and analytics to detect new patterns and methods used by criminals. Additionally, regulatory compliance in various jurisdictions presents complexities, as regulations and requirements may differ from one country to another. The technical challenge lies in processing and analyzing vast amounts of data across multiple blockchains efficiently and in real-time.

These challenges present opportunities for us. By providing advanced risk-based analytics and real-time monitoring of address clusters and transactions, we help crypto market participants stay ahead of regulatory requirements and effectively combat financial crime. The adoption of our AML platform and solutions by various VASP's (Virtual Asset Service Providers) such as banks, financial intermediaries, custodians, exchanges, payment providers, FIUs, and DeFi protocols further presents opportunities for industry-wide collaboration and a standardized approach to AML compliance.

## Insights & Learnings:

We have gathered critical insights about the nature of financial crime in the blockchain space. By monitoring over 40,000 active blockchain entities, covering more than 80 blockchains and over 1.5M+ digital assets , we have observed various patterns and behaviors associated with money laundering and illicit activities. These insights enable us to continuously enhance our algorithms and stay one step ahead of criminals.

Feedback from stakeholders, including European banks, crypto exchanges, trading platforms, wallet providers, custody service providers, payment providers, and FIUs, has been instrumental in refining our solutions and ensuring they meet the industry's needs. Moreover, through close collaboration with regulators and governments, we have been able to educate and raise awareness about the importance of crypto AML and provide risk management and blockchain analytics services.

Lukka's solutions such as Coinfirm Analytics and Coinfirm Investigator demonstrate tangible results in identifying suspicious transactions, tracing the source of funds, and conducting investigations to support law enforcement agencies. These solutions strengthened our position as a trusted partner in combating financial crime in the blockchain ecosystem.

Overall, our solutions not only facilitates regulatory compliance but also contributes to the evolution of a safer and more transparent blockchain industry.

## About Lukka

Founded in 2014, Lukka serves the most risk-mature businesses in the world with institutional data and software solutions. As a global company, headquartered in the United States, Lukka bridges the gap between the complexities of blockchain data in a global crypto ecosystem with traditional business and reporting needs.

Coinfirm Analytics and Investigator solutions support businesses globally with on-chain analytical to solve risk and compliance needs for the constantly evolving and hyper-innovative blockchain and digital asset ecosystem.

All of Lukka's products are created with institutional standards, such as AICPA Service and Organization Controls (SOC), which focus on data quality, financial calculation accuracy & completeness, and managing technology operational risk. Lukka has obtained AICPA SOC 1 Type II and SOC 2 Type II Audits, an ISO/IEC-27001 certification, NIST Cybersecurity Assessment, and continues to lead the industry with best in class technology risk governance.



Lukka | coinfirm

Learn more at lukka.tech

## COMMISSARIAT À L'ÉNERGIE ATOMIQUE

Project snapshot:

In the context of the environmental challenges of today's world, reliable climatic information is crucial to guide geo-political decisions, to promote eco-responsible industry and to engage the public into the logic of climate action. The Green Blockchain aims at developing an electronic tool for collecting, processing and visualising the concentration of greenhouse gases, with the collaboration of indpendent, specialised laboratories that control low-cost sensors deployed in urban areas and process the collected data under the lead of expert environmental scientists. In order to guarantee the integrity and exactitude of the climatic information produced by such a decentralised network of independent laboratories, we propose a blockchain-based tool that guarantees that the collected data remains unchanged and enables its auditability, this is, the mutual surveillance of each laboratory's processing of the data in order to prevent unintentional errors and/or malfeasant tampering. Our tool offers a trusted notarisation service that anchors the collection and processing of the data to the blockchain, by taking cryptographic fingerprints of data snapshots. We provide a dashboard that is publicly accessible online for visualising the resulting climatic information, and for enabling third-parties to also audit the collection and processing of the data. In doing so, our tool is itself green: we target low-energy consuming blockchain technology and we ensure our notarisation service incurs in a very small energy overrun. The Green Blockchain combines Tech4Green and GreenTech for providing reliable climatic data and for bringing confidence and transparency in climatic matters to the public.

Our tool has been tested and demonstrated in collaboration with CEA's Laboratory for Environmental and Climate Sciences ("Laboratoire des Sciences du Climat et de l'Environnement", LSCE) which is the Paris node of the European Integrated Carbon Observation System (ICOS). We aim that our tool be adopted in the near future by laboratories in other 2 pilot cities of the ICOS Cities project (Zurich and Munich), and by any other institutional or private European environmental players (whether or not in the ICOS ecosystem) in the long-term.

Challenges & opportunities:

The main challenge of our project is to ensure the integrity and auditability of the climatic data produced by a decentralised network of independent laboratories, while still incurring in a very low energy overrun. To meet this challenge, we target non-consuming blockchain technologies (Ethereum 2.0 with Proof-of-Stake, BESU IBFT 2.0 with Proof-of-Authority, ...) and we

implement the notarisation service via a lightweight smart contract that optimises the number of calls and the amount of information stored in theblockchain (typically, two smart contract calls that together store two 32-byte words in the blockchain for each sensor and day). According to our preliminary tests with a realistic blockchain (SEPOLIA testnet) our notarisation service incurs in a consumption of approximately 45W per sensor, from which 40W correspond to the sensor's embedded hardware, and 5W correspond to the validation of the smart contract calls in the blockchain for the notarisation of the data flow coming from the sensor. We maximise the computing resources already in place (massive data storage and data processing at the laboratories) by letting our notarisation service be transparent to the normal operation of the laboratories.

While the challenges above are mostly technical, some regulatory issues exist concerning the input data (sensor measures) provided by each independent laboratory (including the public or private intermediaries that may be hosting a sensor) and the potential use of the output data (processed climatic information) by public or private entities. The measurements and observations collected by the laboratories within the ICOS Cities project are expected to be published under a CC BY 4.0 licence, but this data could be used together with other publicly accessible information to reveal sensitive data (e.g. identity or location) of an intermediary party hosting a sensor. The blockchain itself only stores hashes (cryptographic digests) of the data, but the online dashboard for data visualisation stores full samples of data, which can also be accessible to final users of the dashboard (whether staff at the laboratories, or the public). The dashboard manages the identity of these final users for access and authentication purposes, which may concern protection of personal data and/or other cybersecurity aspects.

We intend our project to constitute a breakthrough in environmental matters. On the one hand reliable climatic information may be used by a huge range of potential applications, whether public or private. On the other hand, the trust and transparency that our tool brings to the public can go a long way in engaging citizens in the logic of climate action. Our tool and the associated blockchain-based notarisation service are general enough as to meet any scenario for data collection and processing, other than that of the climatic information. Thus, our solution could become a model for similar initiatives on issues with high societal impact and global outreach.

Insights & Learnings:

The main difficulty in the development of our demonstrator has been to cope with an inter-disciplinary team with very diverse competences in climate sciences, embedded systems, blockchain systems, and software development. In addition to that, some of the team members have contributed to the project only temporarily, and some components have been developed by third-parties with expertise in UX-UI design. As is the case in this kind of projects, the challenge has always been that at every point in time, all the knowledge in the different areas necessary for the project's advancement had remained under at least one skull.

Since this kind inter-disciplinary is very typical in innovative blockchain projects, we believe the experience gathered within Green Blockchain to be very valuable for future blockchain projects.

## COMPELLIO (UNI SYSTEMS)

Our use case paves the way for standardising and adopting Digital Product Passports (DPP) for cultural goods and intellectual property (IP) assets.

In collaboration with Uni Systems, and by using Compellio's multi-sector DPP solution, we leverage blockchain technologies to:

- facilitate immutable digital preservation of cultural heritage,
- strengthen protection against illicit trafficking of cultural goods,
- enable tokenisation services for managing IP rights,
- safeguard derived value of IP assets and non-tradeable cultural goods.

DPPs are an important element of the EU digital strategy, aimed at providing access to verifiable information by citizens, businesses, public bodies, and consumers within the Single Market and globally.

Our objective is to extend the scope of DPPs by developing the next-generation infrastructure components that will provide the technical backbone for building interoperable compliance & assurance solutions for cultural goods and IP assets (our DPP Early Adopters programme is accessible via this link).

In this journey, active collaboration with regulators and policymakers is critical. Europe leads the way in setting up advanced regulatory frameworks and guiding principles for all breakthrough innovations. Although there are still challenges that hinder the wider adoption of blockchain tech by public and private organisations, we believe there is momentum in addressing domains such as cultural goods/heritage and IP management, also because of the following facts/opportunities:

a) Substantial focus on blockchain tech, related business models, and legislative effort is channelled to the finance sector, especially through the MiCA Regulation. Such efforts set the scene for a larger set of use cases beyond finance, where the value in exchanging assets encompasses several dimensions from economic to social as well as environmental aspects.
b) The legal characterisation of movable assets (tangible or intangible) as well as the types of security interest in them, vary greatly across European jurisdictions. An EU common framework for secured transactions based on standardised definitions of assets could unlock new commercial web3 interoperability within the Single Market.
c) Implementing new solutions in traditional industries and markets opens an immense potential for further digitalisation where integrations of blockchain with existing electronic platforms and services largely remain untapped.

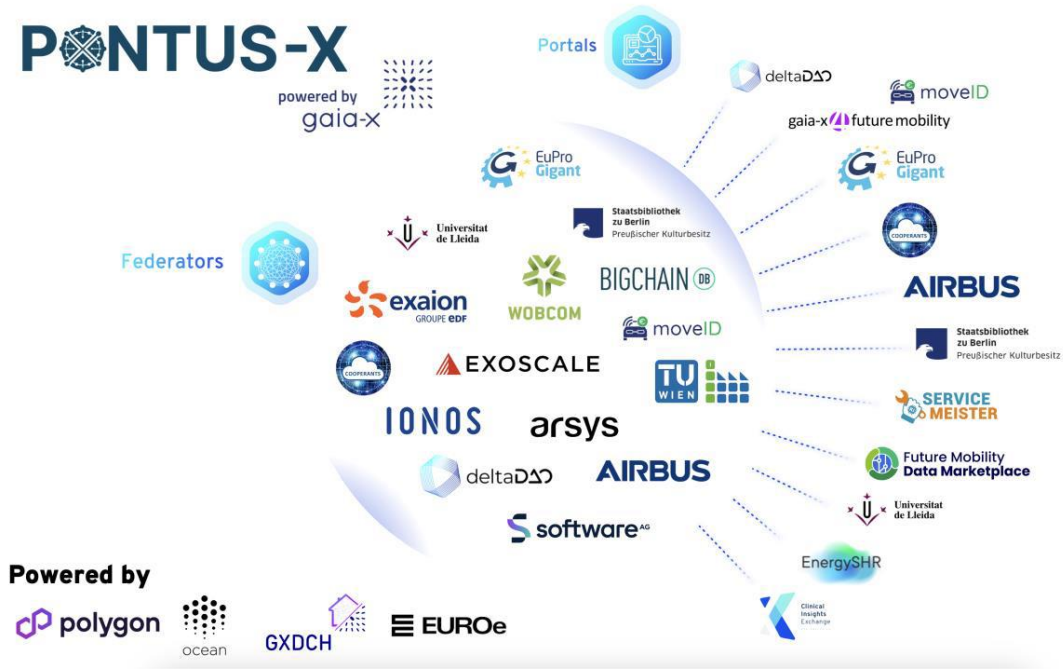
Looking ahead, our collaborative work in the context of the Sandbox helped us identify new opportunities for blockchain-based solutions within the evolving EU regulatory frameworks and flagship digital transformation projects, particularly those related to enterprise systems integrations and asset transfers across federated data spaces. The benefits from this

endeavour do not only entail operational efficiencies in terms of higher auditability and accountability standards, but more importantly they catalyse added value for the real economy.

Specifically for Real World Assets (RWAs) with IP-derived value, the expected growth impact is staggering. The goal of creating robust technical capabilities that can facilitate secure and interoperable management of assets feels more urgent than ever before. Not only for protecting consumers, investors, and brands but also for creating the “new digital rails & bridges” that modern economies can use to connect globally and grow sustainably.

**deltaDAO**

**Pontus-X - European Smart Contract-Based Data and Digital Service Ecosystem powered by Gaia-X**




deltaDAO AG (delta-dao.com), in collaboration with a network of European data ecosystem federators, proudly introduces Pontus-X (pontus-x.eu), the largest public smart contract-based data and digital services ecosystem in Europe powered by Gaia-X (gaia-x.eu).

The primary goal of the initiative, supported by Gaia-X, is to implement the European data strategy, EU digital strategy, and EU policy priorities by promoting a competitive, secure, and transparent digital single market that is connecting both the real economy and the financial markets. Pontus-X provides a domain-agnostic solution in sectors including aerospace, transportation, automotive, healthcare, open science, digital services, IT, cloud services, AI and data-driven businesses, industry 4.0, and manufacturing. It reduces lock-in effects regarding centralized data platforms and cloud service providers.

The primary benefits of the Pontus-X ecosystem, as a blueprint for next-generation data spaces, include an efficient transaction layer allowing consumers to orchestrate data, software, and cloud services from all kinds of providers on-demand from an open market, following the Gaia-X Trust Framework to ensure interoperability and compliance with regulation and quality criteria. Participants can buy and monetize any digital service, including AI, data streams, secure cloud computing and perform instant settlement using European-regulated electronic money in compliance with the Markets in Crypto Assets Regulation (MiCAR) and potential other financial market statutes such as the DLT Pilot Regime. It reduces operational costs and

the costs of compliance through IP- and privacy-preserving technologies and automized contracting, reducing search, payment, and contracting costs for all participants.

To address the main challenges of interoperability, scalable trust, vendor neutrality, and economic sustainability, this digital ecosystem operating across Europe uses Smart Contracts, Distributed Ledger Technology (DLT), eIDAS Trust Service Providers, digital signatures, and is powered by Gaia-X and Ocean Protocol, as free open-source data economy software frameworks. The identity and trust layer are based on European Trust Anchors, the Gaia-X Trust Framework, Self-Sovereign Identity (SSI) and W3C Verifiable Credentials to allow open identity ecosystems, a major opportunity to reduce fragmentation and market friction in Europe with the upcoming European Digital Identity for legal and natural persons.

This use case, already validated through real-world deployments and collaborations with industry leaders, aims to create a European and global decentralized, secure, and transparent digital services infrastructure across domains.

The use of blockchain technology, smart contracts, utility tokens compliant with MiCAR and other financial market regulations, electronic money tokens, and metadata NFTs, in compliance with EU regulations such as the DLT Pilot Regime, is critical to fostering data-driven innovation and collaboration across domains.

deltaDAO is proud to be a Gaia-X member, the Gaia-X AISBL endorsed representative for the European Blockchain Regulatory Sandbox and committed to comply with the Gaia-X rules and conformity framework and rules to promote Europe’s sovereignty and competitiveness.

Pontus-X Ecosystem powered by Gaia-X: https://www.pontus-x.eu/

**DNV**

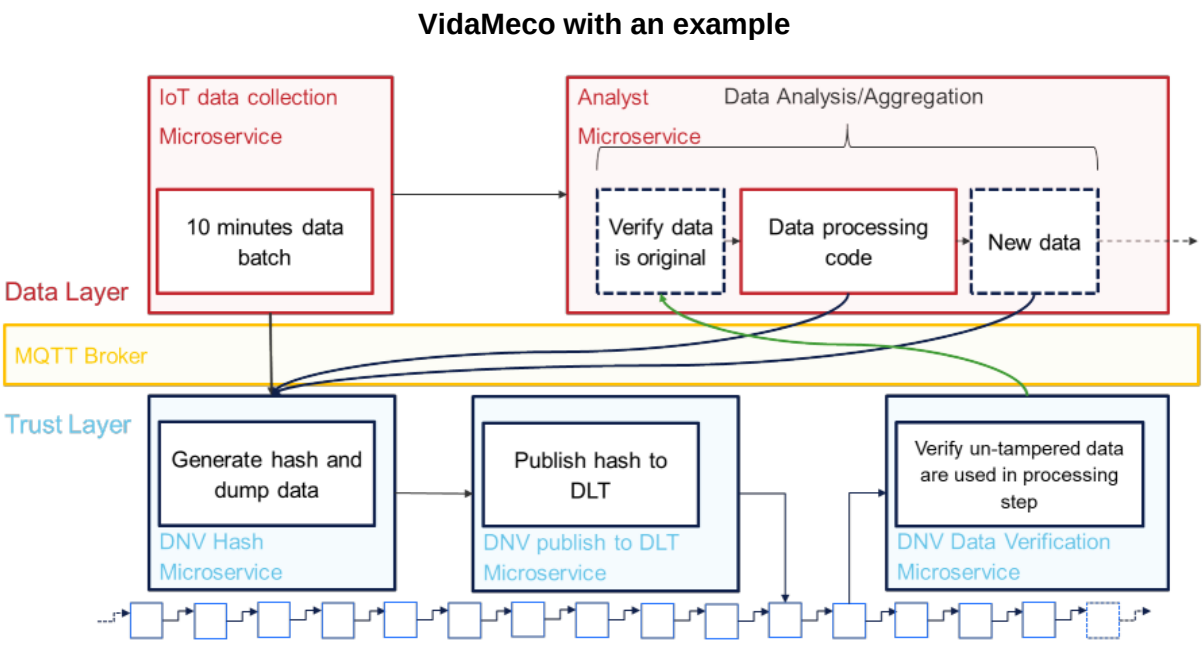



**Figure 1: Vidameco Architecture**

## 1. Introduction

Regulatory bodies are placing increasing emphasis and enforcement on ESG metrics reporting with large fines imposed for failure to comply. The key challenge to report ESG related topics effectively is that standards and regulations are continuing to evolve and there is no universally adopted standardization. Organizations are seeking support in what to measure, how to store data and a way to track data in an efficient and reliable manner. Further, there is a need for transparency in ESG reporting that continues to present a challenge for business and also regulators tasked with determining metrics that are real. There is a need and a role for tools, solutions and services that can allow regulators and the public to ensure they can trust that ESG reporting is accurate and transparent, which DNV seeks to address through the use case it has submitted for discussion in the European Blockchain Sandbox.

VidaMeco offers a solution to provide immutable and automated reporting of a number of data points through the use of blockchain in a way which allow the Maritime industry a trusted solution to meet its ESG reporting obligations, especially in relation to the Emissions Trading System (ETS) compliance cycle.

In order to better explain the DNV use case in practice, as well as the regulatory topics DNV would like to discuss, we will in the following describe a scenario using the VidaMeco Architecture linked to the EU Monitoring, Reporting and Verification (MRV) regulation and the ETS and Carbon Intensity Indicator (CII) compliance cycle.

In relation to this, it may be relevant to read more about DNV's role, as well as the services and products offered in relation to EU MRV and ETS. You can find a high-level description here. However, in short, the implementation of the EU ETS in 2024 in the Maritime industry will expose Document of Compliance holders (often the ship managers) to significant risk as emission costs will need to be factored into contracts between stakeholders to ensure fair distribution. Therefore, collecting, managing and sharing accurate and reliable data in the Maritime chain will become crucial for compliance reporting.

## 2. EU ETS – problems and solutions

In order for a vessel to be able to report in accordance with EU ETS, annual aggregated data reports will no longer be sufficient to manage and control ETS allowance and CII performance. Instead, there is a need for a trusted and verified voyage statement based on daily real time-reporting of data. This report needs to be verified by an accredited verifier, like DNV, before being submitted to the EU Commission.

Today, emission calculations are estimated based on different data sets sent from different stakeholders, such as:

- data from vessels in the form of daily reports ("noon reports"), including the amount of fuel burnt and other operational data;
- documentation from fuel suppliers, such as invoices on fuel sale, in order to back up the reported fuel burnt with an additional data source (also known as "bunkering");
- data from laboratories, such as studies on samples of fuel from a batch;
- etc.

Thus, in order to report, the entity responsible for reporting must collect data from different stakeholders as listed above, prior to handing over the report to an accredited verifier, like DNV, for verification and final submittance of the report to the EU Commission.

VidaMeco architecture and the corresponding use case represents a solution to solve parts of the challenge in supporting the whole maritime value chain.

To better explain, sensors will be used to collect source data on the vessels. DNV will inspect and certify the sensors that are used to collect the source data but cannot in any way influence or create the data that is collected by the sensors. Further, there is no need for source data to be stored with DNV in order to use this solution.

The ship will then begin the voyage. The data is collected in ten-minute batches, converted and published as a hash on the blockchain. DNV will store the transaction ID on the blockchain in a look up table to find the transaction for any hash.

When a data consumer wants to verify the integrity of a particular batch of data, they input the data that they would like to verify, a hash of that data is created, and the corresponding transaction ID is looked up. If by using the transaction ID, the corresponding blockchain entry is found, the source data has been protected against tampering. This in turn increases the integrity of the data and provides better assurance for regulators to ensure reporting is accurate.

In addition to data collected in batches, documentation such as invoices issued by a fuel supplier can also make use of the solution. Invoices can also be put through the hashing process on the blockchain and make use of the same benefits as described above.

### 3. Regulatory topics to be discussed

Based on the above descriptions of the VidaMeco architecture and use case, DNV is looking to discuss the following regulatory topics:

- Do the regulators have any objection to the digital verification of the emissions data rather than reliance on documentation?;
- Given the impartiality requirements of the MRV legislation, would the creation of a blockchain ecosystem be considered advisory software and do the regulators see any potential conflict with the third-party verifier role? If there are any perceived conflicts what steps are sufficient to abate this issue? Further, given that providers of third-party services are often best placed to assist regulators in ensuring data used for reporting is accurate, if there is not an actual conflict of interest will future legislation exempt blockchain solutions that are not providing a judgment or decision from the impartiality debate? Has this been looked at?;
- Given that the solution may tie a blockchain identity to specific individuals, do the regulators have any objection on the use of blockchain in this way from a GDPR perspective? If there are any perceived conflicts what steps are sufficient to abate this issue?

## EBSI VERIFIABLE CREDENTIALS USE CASE


**EBSI-VECTOR - EBSI enabled VErifiable Credentials & Trusted Organisations Registries**

The Digital Europe project «EBSI-VECTOR» that started on June 1st, 2023, with a term of two years, has launched its official Kick-Off Meeting on July 5th 2023. This project is the result of the unique historical moment that we are living, where digital transformation represents a step forward from the merely adoption of any enabling technologies towards a process guided by a strategy of revisiting and redesigning existing ways of living, working, doing business and managing public good.

Hence, digital transformation is pushing governmental entities towards an open, transparent, citizen-centred, decentralised, multi provider and co-operative model that can be supported by cutting-edge blockchain and distributed ledger technologies (so-called DLTs). Blockchain is a type of distributed ledger, that organizes data into blocks, and they are chained together in an append – only mode, meaning data can only be added in time-ordered sequential order. Furthermore, distributed ledgers use independent computers (so-called nodes) to record, share and synchronize transactions in their respective (decentralized) electronic ledgers.

The blockchain technology currently sits within the innovators and the early adopter user groups (e.g., citizens, students, etc.). EBSI stands for European Blockchain Services Infrastructure, is the first EU-wide blockchain infrastructure, and several national initiatives are moving towards the overcoming of "Proof of Concept" stage, to accelerate the creation of cross-border services and put blockchain at the service of public administrations for the purpose of verifying information, increase efficiency and making the services trustworthy.

*Blockchain becoming fully operational.*

In this frame EBSI-VECTOR aims to support in an organized and coordinated way a series of activities aimed at reducing the gap between a "pre-production" implementation and a real-life production adoption in specific application sectors. In particular, the project overarching vision is to "Improve the capabilities of social security, educational credentials and ESSIF use cases, extending the paradigm of self-sovereignty, and decentralized verifiable credentials and decentralized trusted registries for each use case related with real end user services for European citizens via the support of the European Blockchain Service Infrastructure (EBSI) and implement this in different countries and cross-border interactions". EBSI-VECTOR will also inspire and support the EUDI development with the elaboration of current and new EBSI-capabilities and engaging more stakeholders and actors in the decentralized identity ecosystem.

*Demonstration in three relevant use cases*

The potential behind EBSI VECTOR will be demonstrated through the following use cases that will be developed and deployed in a cross-border context.

• Education: use case learning outcomes achievements, use case transcript of records and use case student ID.

• Social Security: use case European Health Insurance Card (EHIC) and use case Portable Document PDA1.

• Business registries: use case identity of legal persons deployed with selected partners.

*Consortium:*

*More than 50 partners from 20 countries ….*

The EBSI VECTOR consortium, therefore, consists of a well-balanced but extraordinary large group of partners that make the implementation of verifiable credentials in the education and social security domain possible and extend the current capabilities for further uptake. The collaboration between the public sector organisations from the European Blockchain Partnership (which explored the verifiable credentials and decentralised registries in the past three years) with the business domain experts and policy advisors of education and social security (actively engaged in different use case groups and related projects) supplemented with academic and technical experts (most of them already provide EBSI compliant solutions and with lots of development and design experience) is the best guarantee to achieve the objectives of this project. This consortium widely represents Europe including partners from Austria, Belgium, Cyprus, Denmark, France, Germany, Greece, Hungary, Italy, Lithuania, Luxembourg, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and The Netherlands.

## EQUILIBRIUM


### Equilibrium Group: Tokenized securities – Share-tokens of private unlisted companies

Equilibrium Group is a leading Web3 development powerhouse in the EU with 75 employees in over 20 countries worldwide. We build decentralized solutions for our clients, who are world-renowned players in the Web3 space. In the context of the EU Blockchain regulatory sandbox program, Equilibrium aims to tokenize shares of private unlisted companies and enable them to operate on DLT/Blockchain based systems.

### Project snapshot

In our endeavor to modernize the way private companies manage their shares, we are exploring the tokenization of shares – a revolutionary approach that allows us to represent ownership in a digital format on a blockchain. The primary goal is to enhance liquidity, accessibility, and efficiency in the trading of unlisted company shares.

With deep technical capabilities Equilibrium can leverage its experience in Web3 development and build the necessary systems for technical tokenization of shares. In our view the technical implementation and creation of such share-tokens seems relatively straightforward and can be done utilizing various DLT- or blockchain networks. As the Ethereum network is currently utilized widely and its token-standards are most compatible with current DeFi- and wallet infrastructure, we are planning to use an Ethereum token standard in the first phase of this project.

### Challenges and opportunities

In their current state, unlisted company shares suffer from liquidity issues and administrative burdens. Limited market activity makes them challenging to trade, exacerbated by the absence of forums for exchange. Manual updates to shareholder registers and paperwork for private share transfers contribute to administrative challenges, creating barriers for investors and hindering the efficient functioning of unlisted company shares in the financial ecosystem.

However, the opportunities presented by tokenization are substantial. We foresee increased liquidity, making it easier for investors to buy and sell shares. Accessibility will allow smaller investors to participate in markets traditionally reserved for larger players. Moreover, the transparency and security inherent in blockchain technology should foster trust and confidence among investors.

Currently the main challenges lie in the regulatory framework/landscape regarding the tokenization of real world assets and shares of unlisted companies specifically. Currently common European legal rules regarding both crypto assets and traditional markets make it unclear, as to how a tokenized share of an unlisted company will be treated and ultimately how it can be utilized, who can utilize it and in which situations?

### Insights and learnings

Through our participation in the sandbox project we have gathered valuable insights into the regulatory topics and questions that need to be solved before this kind of tokenization is possible. It seems that the answers consist of a combination between common European regulations such as MiFID2 and national corporate and financial markets regulations. Hence, being able to engage regulators and policymakers through the sandbox project has been a great opportunity for Equilibrium.

**EVIDEN**

The Eviden Battery Passport EcoSystem is based on the platform initiative of the (European) automotive industry. It offers digital passports for all car batteries in use for electric vehicles, which allows the car and battery manufacturers to distribute battery production information (where required) and collect battery performance and usage information across the full battery lifetime, from production to any usage scenario including recycling in circular economy setups.

**The Eviden Battery Passport (patent pending) includes the following key technologies.**

**The Eviden Battery Pass Creator Solution**
Leads the Product Manufacturer through a guided Battery Passport Creation Process,
Certifies and visualizes the Battery Passport Data Composition (Blueprint),
Allows the Setup of a Development and Supply chains (in dedicated Views)
AI highlighted failure and breaches in in the Data Composition Path
Capability of delegated Data Acquisition to the supply Chain and automated Data Integration
Only the Battery Manufacturer decides what will be visible in a released Product Pass
AI Solution certifies the Product Passport for EU Authorities

**The Battery Pass Control Center Solution**
Monitors and analyzes all in Field Lifecycle Battery Passport Return Data
Generates Graphics and Statistics by the in-Field Battery Performance
AI tracks the implications between Battery performance in the field and blueprint changes.
AI Highlights Critical Events and Outliers in the Field, and escalates them in the CC View
AI Detects several kinds of Product Copies, frauds, and manipulations in the field.

**The Battery Pass Distribution Solution**
Is a self-sovereign, Blockchain based Fully Distributed Platform Technology
Allows a simple, direct access to the relevant Battery Passport information.
No manual onboarding needed – it works as a data-driven self-sovereign process instead
A private Blockchain Technology handles high volume of accesses stable and secure.
Fingerprints to grant data integrity for a once released Battery passport blueprint.
Battery Lifecycle Data Handling (in Field Feedback Handling) within the Blockchain
Battery Passport Import and Export Technologies for other international networks.

**Main Features of Eviden Battery Passport Platform**

The complete battery life cycle beginning with the product creation, over product usage in the market, to product recycling, product disposal, in all steps and with all applied rules is transferred from the real world to the industrial metaverse. The chosen blockchain technology grants that the Eviden Battery Passport is always accessible, highly durable, secure, and eco-friendly. Blockchain an AI are the backbones of every communication and data storage in the Eviden Battery Passport network. Batteries are represented as unique instances on the platform in order to assure reliability of the battery information over its full lifetime.

The platform is open to all participants in the manufacturing and affiliated industries, in particular in the automotive industry including its supply chains and ecosystems, but also to use cases which embed digital passports into industrial products. The distributed platform is fully cloud based, though participating entities can manage their relevant data as they see fit under full sovereignty. The platform can be joined without vetting or approval from third parties.

## FRAUNHOFER (OPEN LOGISTICS FOUNDATION, ALS HOLDING)

### Open Customs Blockchain

Open Customs Blockchain introduces **European-made**, **open source blockchain software** into **logistics** and **customs processing** to **simplify data exchange** and **increase transparency** in cross-border supply chains. The project is initiated and supported by the Open Logistics Foundation and its Working Group Open Customs Blockchain. It consists of major logistics companies Rhenus, DHL and DACHSER, as well as customs and IT service providers ALS, AEB, IP Customs Solutions and leading logistics research institution Fraunhofer Institute for Material Flow and Logistics

The goals of Open Customs Blockchain include the creation of more transparency in supply chains, improved efficiency in data sharing, speeding up border processes, decreasing transit times, reducing the need for physical inspections at the border, and finally, making international trade more sustainable by replacing current paper-based documentation with a more efficient, trustworthy technology: **Blockchain**.

Customs clearance is subject to fraud, evasion of duty and undervaluation. Additionally, the use of paper-based procedures causes discontinuities and delays in cross-border process flows. The project therefore follows an end-to-end integration of customs and logistics processes in external trade, that is tamper-proof, trustworthy, cross-border and open source.

Existing solutions worldwide require multiple parties to follow a complicated coordination process until agreement on a large and complex data set is reached. This complexity is reflected in the technological implementation as well. However, studies show that the collected data by authorities and entered by economic operators exceeds what would be necessary for customs clearance process handling. Instead, the opportunity lies in focusing on essential customs data that authorities consider to be the main source of fraud and duty evasion and is used recurrently in most customs processes. This data set contains basic information on the seller, the buyer, the invoice, origin, and classification of the goods traded. Another focus is on an EAD-based dataset as it is used in the European customs union. For these reasons, the proposed approach of the Open Customs Blockchain includes the following: customs information – based on the original invoice data (Goods Passport ID Project) and the export accompanying document (EAD) as exemplified by the project BORDER – is stored in a tamper-proof way and distributed along the supply chain. Together, the two sub-projects form the framework of the Open Customs Blockchain. As the customs-related information is required repeatedly in various steps of an export or import process by several parties, blockchain increases transparency and trust by making data origins consistently traceable.

Nevertheless, despite the potential, blockchain-solutions in the customs domain have not seen full deployment yet. Based on the insights of other blockchain customs projects that were mainly driven by private and closed company initiatives, major implementation challenges include the lack of expertise, high costs, low acceptance by other stakeholders, disagreement

on governance processes, scalability, and finally share of costs and profits among each participant. A trustful collaboration between authorities and businesses is a crucial factor. Innovators, software providers, economic operators and customs authorities should pay more attention to speaking a common language in the future, for example by observing and adhering to standardized data models. The premise for administrations under which upcoming digital transformation can succeed is, in particular, more trust in economic operators as a basic assumption on the part of customs. The use of new technologies can simplify and accelerate the legitimate, cross-border trade of these "trusted traders" without creating new risks in terms of illegitimate trade, faulty declarations, or offences in general.

These learnings emphasize the necessity of an open and collaborative approach on aspects such as decision processes, software development, governance structures and standardization, which all can be pursued under an open-source project such as the Open Customs Blockchain.

## GLOBALLOGIC (NUGGETS)

GlobalLogic implements trusted European cross-border payments using Nuggets. Combining Verified Self-Sovereign Decentralized Identity (SSDID), Verifiable Credentials, Selective Disclosure, Zero Knowledge Proofs, Auditable Nuggets and Blockchain we're able to facilitate secure, efficient, and compliant remittances between individuals, businesses or Governments in different European countries. All whilst meeting the requirements for AML, CTF, KYC regulation and eIDAS2.

Cross-border payments are a common occurrence, whether it's a small business owner in France paying a supplier in Germany or Governments conducting international transactions. However, traditional methods of cross-border payments often involve sharing PII data that could be compromised, there's fraud and false positives risks, plus complex processes, high fees, and security concerns. The emergence of Self-Sovereign Decentralized Identity (SSDID), Verifiable Credentials and blockchain technology is poised to transform this landscape.

Here are some of the key challenges we address and the benefits we provide to both businesses and individuals.

### Identity Verification

Both the directors of the business and the business itself have their own SSDIDs, which are encrypted to their own private keys, secured and tamper-proof digital identities tied to the blockchain, whilst ensuring no PII is on-chain. These identities contain essential information for identity validation, such as public keys and relevant credentials.

### Ownership and Control with SSDIDs

One of the primary advantages of SSDIDs is that they grant full ownership and control over digital identities to individuals and organizations. This means that both the business owner and supplier can manage their identity credentials, enhancing security, privacy, and flexibility compared to centralized identity systems.

### Biometric Verification

By combining biometrics with SSDIDs, the business owner and supplier ensure that only the genuine individuals involved can access and initiate and receive payment, even when moving from device to device. This additional layer of security guards against identity theft, fraud, and unauthorized access.

### Secure Communication with DIDComm

In addition to the payment functionality, the business owner and supplier can also communicate through decentralized messaging utilizing DIDComm. DIDComm is a secure and private messaging protocol based on Decentralized Identifiers (DIDs). It encrypts messages end-to-end, ensuring that only the intended recipients can decrypt them, with no man-in-the-middle attacks.

### Privacy and Prevention of Tracking with peerDIDs

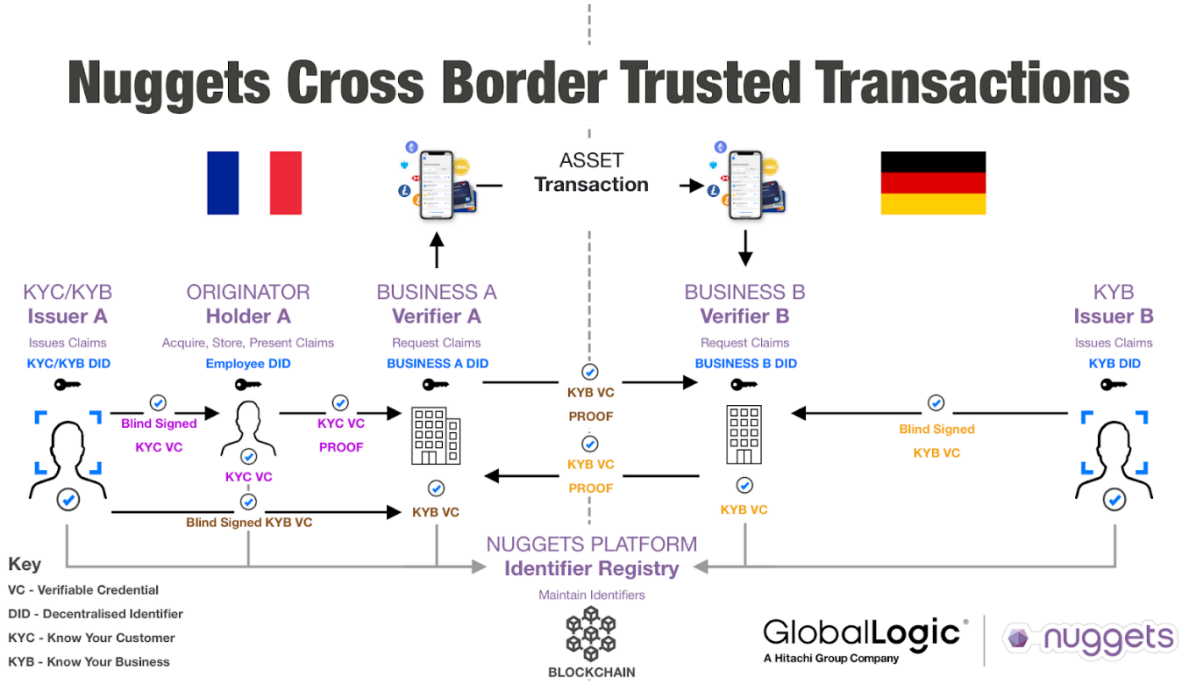
For enhanced privacy and to prevent tracking or correlation of their identities, users use peerDIDs with holder binding and blind signatures. PeerDIDs are DIDs generated for a specific pairwise relationship between two entities, facilitating private and secure communication.

### Integration of W3C Verifiable Credentials (VCs)

Furthermore, the use of W3C Verifiable Credentials (VCs) in the SSDID and payments system ensures seamless cross-border transactions with benefits such as enhanced security, improved privacy, increased trust, interoperability, simplified compliance and cost efficiency.

### Auditable Nuggets

Trusted compliance is encrypted to the required participants' private keys with access to time-restricted nuggets of information - Auditable Nuggets - for regulatory and auditing purposes, without the need to keep PII data within their own systems.



**INO MTÜ**


**Introducing the Internet Native Organization (INO) Initiative:**

In today's rapidly evolving digital landscape, the way organizations operate is undergoing a significant transformation. Traditional models, with their set hierarchies and processes, often struggle to adapt to the dynamic needs of the digital age. Recognizing this gap, the Internet Native Organization (INO) initiative was born.

**What is INO?**

The INO model represents a fresh approach to organizational structures, designed specifically for the digital realm. It takes inspiration from Decentralized Autonomous Organizations (DAOs) but elevates the concept to be more inclusive, adaptable, and legally sound. At its core, INO emphasizes:

- **Unified Collaboration:** Bringing together individuals from across the globe, fostering a sense of unity and shared purpose.
- **Distributed Governance:** Ensuring that decision-making is a collective effort, drawing on the insights and expertise of the entire community.

**Innovation and Impact:**

The INO initiative has already achieved significant milestones. Notably, it became Estonia's first legally registered DAO in August 2022, setting a precedent for others to follow. This achievement was further amplified in March 2023 with the successful hosting of DAO Day Estonia, a landmark event that brought together key players from the DAO, legal, and public sector ecosystem. Furthermore, their dedication to the cause, underscored by their recent

induction into the European Blockchain Regulatory Sandbox, has led the team to actively engage with regulators and authorities across various jurisdictions.

Beyond the technical achievements, the societal impact of INOs cannot be understated. By promoting equitable participation and decision-making, INOs have the potential to create a more inclusive digital society, where everyone's voice is heard and valued.

**Legal Challenges & The Way Forward:**

The legal landscape for both DAOs and INOs is still very much a work in progress. Different jurisdictions have different views, and there's a lot of ambiguity. However, the INO team is not just waiting for the rules to be written. They're actively engaging with commercial registers and regulators across various jurisdictions, advocating for a legal framework and streamlined process that's both supportive and practical. Their goal is clear—to ensure that INOs can operate seamlessly across borders, without constantly running into legal roadblocks.

The INO initiative is not just another organisational model; it's a vision for the future. A future where digital organisations are more inclusive, adaptable, and aligned with the needs of the digital age.

## LOKOVICE / UNBLOCK (MURCIA CITY COUNSEL, LLEIDANETWORKS SERVEIS TELEMATICS, BANKEREX FINANCIAL, ES SOLO HOLDINGS)

**unBlock: Transforming cities to make life easier for European citizens**

unBlock is the *Superapp* that connects cities, businesses, and people. With a simple and effective vision, it enables any citizen to access services, information, and personalized experiences anytime and anywhere from a single app. Users can pay, shop, or book any product or service.

Powered by Telefónica's blockchain technology and Lleida.net's Digital Certificates and Biometric Identity system, unBlock brings to life the revolutionary European Digital Identity (EUDI WALLET).

The purpose of this **European Digital Identity** is clear: to be used in all facets of citizens' and tourists' lives. From accessing public transportation to attending events, museums, sports facilities, or libraries, all with the highest level of security guaranteed by blockchain technology and its unique validation of each action.

Thus, **unBlock presents a challenge to European cities: to transform them into real Smart Cities and Smart Tourism Destinations.** This requires active collaboration to improve the management of strategies focused on tourism, innovation, and sustainability. By implementing the platform in all spaces, both public and private, the city begins to understand the behavior, use of services, flows, and interests of its residents and visitors.

unBlock goes beyond being a simple application; it is a **blockchain-based Superapp that acts as the comprehensive gateway to the city**, offering an easy and engaging experience while maintaining the highest security standards. From making payments at establishments to obtaining certifications or making reservations, it simplifies life in the city. José Luis Núñez, responsible for the Blockchain business at Telefónica Tech, explains: "One of the pillars of new blockchain-based services is the ability to give users back some of the value they generate."

Many innovation projects related to citizenship are forgotten due to complexity, required resources, and bureaucracy. unBlock is born to reverse this situation, **making cities collaborate on a single Smart City platform that turns cities into smart tourism destinations for the first time.**

In summary, unBlock is leading the transformation of European cities towards excellence in urban management and citizen comfort. And all of this comes with significant cost and time savings, thanks to the immediate deployment of the platform in every corner of the city and our unique business model.

The solution is already available in several cities and destinations in Spain, such as Murcia, Seville, Malaga, A Coruña, the Community of Madrid, and the Catalan Tourism Agency. As

Javier Párraga, Director of Digital Transformation at the City of Murcia, details, "unBlock provides us with the opportunity to implement a global solution for all spaces and businesses in a simple way. An effective way to have a new Smart Murcia."

(Watch the project video)

**STICHTING 2TOKENS (RABOBANK, ABN AMRO BANK, CATENA INVESTMENT, ENERCOIN, CATENA POWER)**

**Tokenized securities with payments through stablecoins – a cooperation of 2Tokens, ABN AMRO, Assetblocks and Rabobank**

Tokenization of real world assets is seen as one of the most promising and innovative applications using blockchain technology. In our tokenized securities with payments through stablecoins use case, we aim to legally explore the innovative use case of a tokenized financial security and a stablecoin integration. With our cooperation (2Tokens, Assetblocks, ABN AMRO and Rabobank), we want to bridge the gap between the physical world and the digital economy by tokenizing real assets and the euro's used for the payments.

The use case provides the possibility for both professional as well as non-professional investors to invest in the tracking stock of SPVs that represent renewable energy sources like wind, solar and battery parks. The proof of ownership is tokenized and represented by a Non-Fungible Token (NFT) where the smart contract on the blockchain is the true primairy register. The issuance is a security under MiFIDII. Owners of the tracking stock, based on their (number of) NFT(s) are potentially entitled to pro rata dividend payments.

Owners of the tokenized securities are not necessarily in the country of origin of the issuer of tracking stock. Payments can thus be cross-border, but within the EU/SEPA region. Up until recently, payments were only made using fiat currency, but going forward, payments, both for purchase/sale of the tokenized securities and distribution of dividends, should be performed using a stablecoin.

Our use case aims to explore the use of Euro or bank deposit stablecoins as well as tokenized assets. Both non-hosted wallet held by the owners as well as hosted wallets provided by banks will support these stablecoin transactions, ensuring new ways of accessibility and convenience for investors. Although on first hand this might look straight forward, implicitly this can raise interesting questions on the background, e.g. as for any transaction of stablecoins or tokens on a public permissionless network, local cryptocurrencies are needed. To gradually built up our use case we divided it into various scenarios we will explore:

Payment scenario one will focus on buying, selling and buy-back of the tokenized securities using a stablecoin. The token owners will use accounts and hosted wallets at banks to hold their tokens as well as stablecoins for buying, selling an receiving dividend pay-out, with the possibility to on- and of ramp EUR stablecoins via the bank. The type of stablecoin will be existing regulated stablecoins, EUROC (Circle) and/or EURe (Monerium) and/or Euro stablecoin issued by Rabobank and ABN AMRO (deposit backed token). Any transaction of these types of stablecoins or tokens will require the local blockchain network cryptocurrency

as well, implicating that, in case of hosted wallets, these cryptocurrencies, besides the tokens and stablecoins, will need to be on the books of the wallet hosting parties as well.

The second scenario build on the first one but will be extended with various elements. For all actions described in the first scenario (buy, sell, dividend payment, on- and of ramping), the possibility to do so in cryptocurrency instead of stablecoin is added as well. Furthermore, besides using hosted wallets at the banks, the usage of unhosted wallets is in place as well. In this scenario, there are a few more elements enclosed.

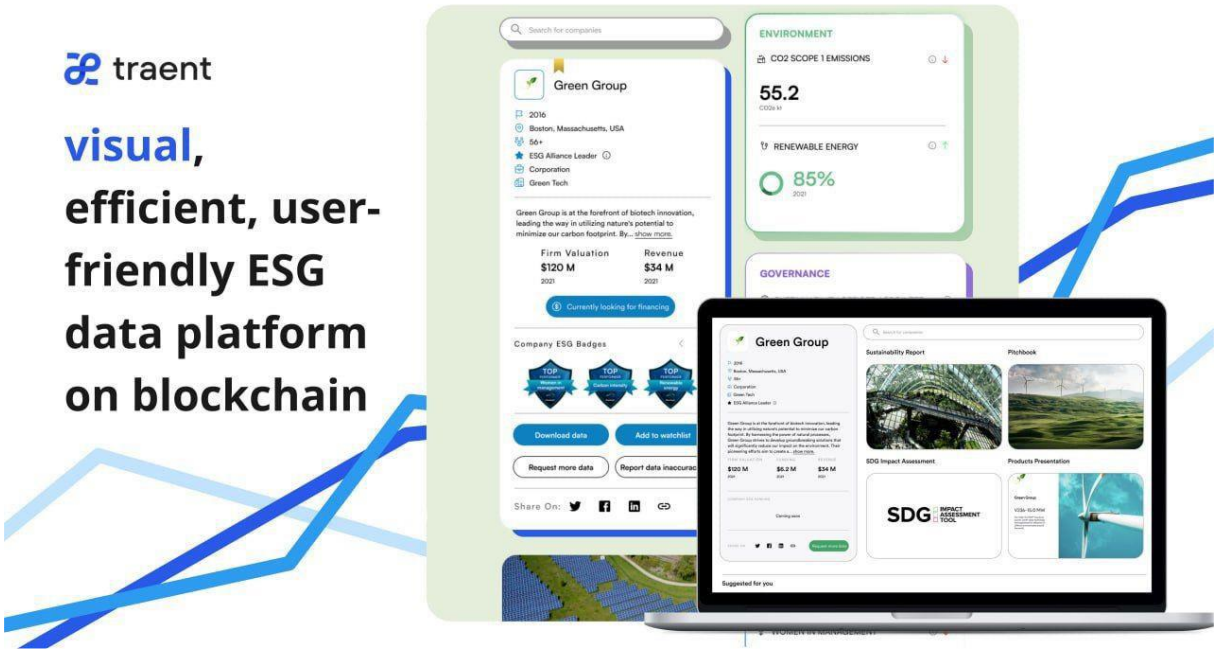
Furthermore, in the second scenario, the possibility to set up peer-to-peer escrow smart contracts for real time settlement of payment through stablecoins in the transfer of ownership of the tokenized security without the use of a third party is explored. Also owners of the tokens, besides having economic rights, will be able to be part of the governance (voting rights) in the SPV. The type of stablecoins for this scenario is all types. Including dollar versions like USDT/USDC and non-fiat related stablecoins.

We are also interested to explore other options to tokenize assets as a security token, such as bonds or equity. This presents a third scenario for us, to explore if the answers to the questions asked in the first two scenarios are still valid.

## TRAENT

traent

**How to leverage hybrid blockchain technology for trustable and accurate ESG reporting**




Traent develops hybrid blockchains, a novel technical solution that combines public and private to bring real-time and data-intensive applications on blockchain while preserving the confidentiality and auditability of data. Traent's primary mission is to promote ethical, sustainable, and transparent behaviour in companies and organizations. For this purpose, the Italian start-up aims to provide a secure, transparent, and efficient work environment for better manufacturing processes and tracking of environmental, social, and governance (ESG) data.

In pursuit of these objectives, Traent has encountered two significant challenges.

1. The first revolves around usability, a crucial barrier to widespread blockchain adoption. Currently, the user experience of a Web3 application often falls short when compared to that of a Web 2.0 platform. Working on blockchain should be as straightforward as using everyday productivity tools like Excel or Slack, but the industry seems far from this goal.
2. The second challenge pertains to data management within decentralised networks. Public blockchains ensure data immutability but lack confidentiality, while private networks provide confidentiality and higher performance but lack data immutability. Hybrid blockchains involve using private blockchains, whose data is "notarized" onto a public blockchain, making this commitment (not the data) immutable.

Traent has chosen the hybrid blockchain approach, refining it to balance the need for transparency and privacy. This allows for maintaining private data with restricted access, while simultaneously enabling selective data disclosure in a form that ensures its auditability.

Thanks to its visual and user-friendly ecosystem, Traent enables companies from various industries and continents to track, collect, and review their ESG data with ease. Tracking environmental, social, and governance metrics on a blockchain platform provides a transparent and secure way to manage sustainability data. By leveraging blockchain technology, data is securely recorded and tracked, providing reliable and tamper-proof ESG performance. Furthermore, establishing a dedicated private blockchain for a company's ESG data will allow a secure, granular data disclosure, progressively enhancing company transparency over the years. Another benefit would be having ESG data updated constantly, allowing third-party auditors to perform due diligence remotely and in real-time.

Moreover, Traent's ecosystem extends beyond ESG reporting. It is a versatile tool for creating product passports and streamlining supply chain processes. This holistic approach empowers companies to provide customers with comprehensive information, including their ESG data, via product passports. This not only enhances transparency but also enables customers to make informed decisions at the point of purchase, contributing to responsible consumer choices.

In conclusion, hybrid blockchain solutions address critical challenges related to ESG data management while unlocking opportunities for data privacy, transparency, and responsible consumerism in alignment with evolving regulatory landscapes and industry needs, offering a transformative solution for the secure, transparent, and sustainable management of data in today's interconnected world.

**TWINU**


**How blockchain plays a fundamental role on the Circular Economy.**

Since the industrial revolution, every single aspect of the linear economy has been optimized. A one click purchase can get most products at your door with single day shipping. I can track my Christmas purchases by the minute, but if you ask brands how many of their products are recycled, repaired or still on use, the most common answer is: we don't know.

Regulations as the **D**igital **P**roduct **P**assport (DPP), Extended Producer Responsibility, and the Right to Repair are pushing for a Circular Economy. But implementing **R-strategies** (collection, reuse, repair, recycle, etc) in a transparent and secure way requires dedicated digital infrastructure. Twinu is using blockchain to build this infrastructure.

Twinu offers a SaaS Circular Solution to issue DPPs and manage **R-strategies** around them. These DPPs are tokenized in the blockchain, making each one unique, traceable, and persistent – all required properties for enabling **circular processes**. Products have a direct link to these DDPs containing all related information – from features to its ownership history. Consumers can 'chat' with their products through our AI interface and ask for recycling or trade-in opportunities. Events such as collection, refurbishment, or repairs, are registered directly into the **token** using a mobile phone and a single tap of an authentication badge. This means all events are easily **auditable**, all information is **immutable** and important data as repair instructions or material composition of the products is stored in a way that it will **outlive** the physical product it represents. We have learned these features are elemental for circular business models and is **hard** to foresee achieving these properties **without** the use of a **distributed ledger technologies** like the **blockchain.**

## GETTING IN TOUCH WITH THE EU

**In person**

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

**On the phone or by email**

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

## FINDING INFORMATION ABOUT THE EU

**Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

**EU publications**

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

**EU law and related documents**

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

**Open data from the EU**

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

KK-09-24-009-EN-N

Publications Office
of the European Union

doi:10.2759/841857
ISBN 978-92-68-11619-7