European Blockchain Sandbox
Best practices report
1st Cohort, Part B

Bird & Bird / OXYGY

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 B

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 978-92-68-17451-7	doi: 10.2759/76203	KK-06-24-099-EN-N

Manuscript completed in June 2024.

First edition

Luxembourg: Publications Office of the European Union, 2024

TABLE OF CONTENTS

1. Introduction

a. Objectives and policies

The *European Blockchain Sandbox* is a regulatory sandbox which aims to establish a pan-European framework for regulatory dialogue. This initiative of the European Commission 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 cross-border 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 initiative annually supports 20 projects and has started in 2023. The sandbox is open to use cases based on any blockchain infrastructure. Blockchain/DLT use cases are selected on the basis of published eligibility and award criteria and matched with relevant regulators and supervising 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.

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;*

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).
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).

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]

b. Participants to the 1st cohort dialogues

After the launch of the 1st round of applications on 14 February 2023, the European Blockchain Sandbox has gone through a successful first application round, which after a rigorous selection process resulted in an impressive 1st cohort of 20 innovative blockchain/DLT use cases which were announced in September 2023. The 1st cohort of selected use cases (including one EBSI use case) represents between them all EU/EEA regions and a range of industry sectors. The financial/crypto asset applications are well represented in the 1st cohort but not dominating, and a broad variety of other use cases is represented in the 1st cohort as well, covering areas such as verifiable credentials/authentication, CO2 emissions, digital product passports, cultural asset passports, customs, cyber security, data sharing and DAOs. The 1st cohort selected use cases are included in **Annex I** to this report.

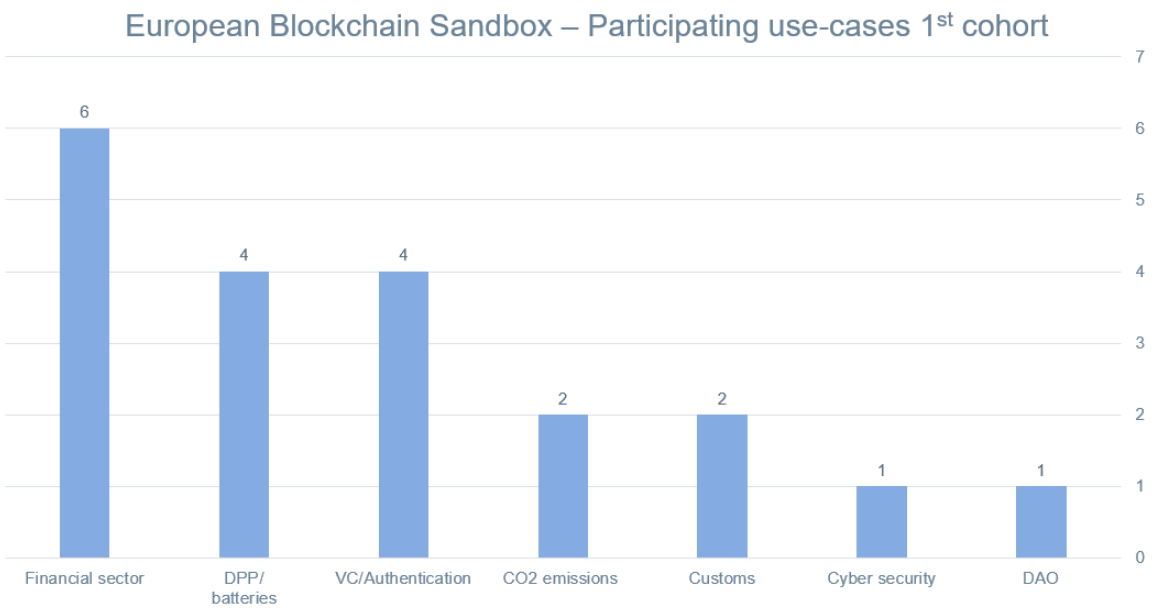
---

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

5 Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/?utm_source=brevo&utm_campaign=AUTOMATED%20-%20Alert%20-%20Newsletter&utm_medium=email&utm_id=320

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).



Equally encouraging is that the European Blockchain Sandbox attracted significant interest among national and EU regulators/authorities. The use cases in the 1st cohort have been successfully matched with well over 50 national and EU regulators/authorities from across the EU/EEA and covering a broad range of regulatory areas. An overview of the participating regulators/authorities is published on the project website (link).

c. Outcome of the matching for the 1st cohort

At the end of the matching process every 1st cohort use case was matched with relevant regulators/authorities. At this moment, the dialogues for 19 use cases are complete and the dialogues for each of these use cases resulted in best practices/lessons learned. The dialogue for 1 use case is still ongoing and will be completed before the summer of 2024.

On average, more than 4 regulators/authorities have participated in the 1st cohort cross-border dialogues for each individual use case (exceeding the objective of on average 1.5 regulators per use case). Financial market authorities competent for financial sector regulation, MiCAR and AML were well represented in the dialogues for the 1st cohort, which is important in view of the number of financial sector use cases in the 1st cohort and the broad range of relevant regulatory areas within the competences of the financial sector authorities.

An overview of the participating regulators/authorities is published on the project website (link).

The dialogues for almost all 1st cohort use cases were cross-border with a range from 1 to 8 regulators /authorities per use case. A combination of national and EU regulators participated in the dialogue meetings for 9 of the 1st cohort use cases. Several regulators /authorities participated in more than 1 use case with a range from 1 to 4 use cases. The regulatory dialogues for 5 use cases focussed on more than 1 regulatory area such as the combination of the GDPR and Cyber Security, AML and the GDPR and DPPs/Battery Passports and the GDPR.

d. Format of the 1st cohort regulatory dialogues

The dialogues for the 1st cohort were organized in accordance with the project's Protocol for Sandbox Participation.[8] The regulatory focus areas and regulatory topics for the dialogues were determined based on the selected use cases and in consultation with the selected use case owners while taking into account an appropriate balance of relevant regulatory areas for the 1st round of dialogues. All participants were given access to a recorded 15-minute onboarding webinar.

In preparation of the dialogue meetings, one-hour blockchain expert sessions were held per dialogue for the participating regulators/authorities. These sessions were provided by the consortium blockchain experts from Warren Brandeis and covered blockchain infrastructure and applications in general with a focus on the relevant industry sector or category of applications for the dialogues.

The actual dialogues consisted of two online dialogue meetings of each 1.5 hours. Regulatory experts from Bird & Bird have taken the lead in preparing the agenda for the dialogue meetings with the regulatory topics, taking on board suggestions and information from the use case owners and the participating regulators/authorities.

To ensure an efficient use of time, information about the use case and the agenda for the dialogue meetings with relevant legal/regulatory context and further relevant information as appropriate were made available on the secure platform in advance of the dialogue meetings. Depending on the use case and the regulatory area(s) as well as the competences and expertise of the participating regulators/authorities, the roles of the regulators/authorities ranged from very active preparation/participation to a semi-observer role.

Summaries of the discussion during the dialogue meetings were shared in draft with the participants to the individual dialogues after each meeting. For most of the use cases, the first dialogue meeting started with a presentation by the use case owner followed by a Q&A. The first dialogue meeting also served as a stepping stone for the second dialogue meeting: based on the dialogue in the first meeting the agenda could be adjusted, additional participants could be invited and further information could be shared. For some dialogues an additional meeting or demo was held.

Following the dialogue meetings, a draft best practices document was prepared by Bird & Bird with draft lessons learned, best practices and recommendations for review by the participants to the dialogue. The draft documents were adjusted on the basis of the comments submitted by the participants and semi-final versions were shared for final comments. The final best practices documents are the core of the best practices, lessons learned and recommendations that are presented in this best practices report.

The dialogues for the 1st cohort have resulted in important lessons learned, best practices and recommendations which are relevant for the wider community. The results are presented in this report (*1st cohort, Part B*). The setting up of the European Blockchain Sandbox, the application & selection process and the matching with relevant regulators and supervising authorities for the first cohort of 20 uses cases is published as the best practices report, *1st cohort, Part A* (link).

Participants were requested to provide feedback by submitting a feedback form via EUSurvey. In the feedback form, the participants (both the use case owners and the

[8] This Protocol (version 1.0) can be accessed through the following hyperlink: https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Key+documents.

regulators/authorities) were 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 were 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.

Feedback from the 1st cohort selected use cases and the participating regulators/authorities is very positive. The use cases appreciate the legal/regulatory guidance and the possibility to have an open dialogue with regulators/authorities. The regulators/authorities appreciate to learn more about DLT use cases and to have a cross-border dialogue with other national and EU regulators/authorities.

Almost all regulators/authorities are interested to participate again in the next round of dialogues (depending on use cases and regulatory areas/topics) and many regulators/authorities have shared helpful feedback and recommendations for possible improvements for the next rounds of dialogues.

e. Focus of the 1st cohort regulatory dialogues

The focus of the regulatory dialogues depended on the use case and the regulatory area.

- Several dialogues focused on **regulatory compliance** by DLT/Blockchain use cases. Examples are the dialogues with a focus on the GDPR, Cyber Security, AML, MiCAR and financial sector regulation. During these dialogues valuable guidance was provided by the participating regulators/authorities to the use cases which resulted in best practices and lessons learned which are presented in this best practices report. These best practices and lessons learned are presented on a generic level and are not specifically linked to individual use cases or dialogues.
- Other dialogues focused on how the use DLT/Blockchain applications can **support efficient and effective compliance and oversight**. Examples of the use of Blockchain/DLT applications as an extra tool, making compliance and oversight more efficient, were discussed in connection with customs legislation, for Battery Passports/DPPs and Cultural Asset Passports and in the EU ETS / MRV regulatory area. The use of Blockchain/DLT as part of mandatory monitoring, reporting and oversight will likely become a relevant area for the dialogues in the next cohorts.
- Finally the use of new areas of regulation and existing or new regulatory tools and qualifications with a focus on **regulation as a facilitator** were discussed in some of the dialogues, such as (i) the use of legal wrappers for DAOs, (ii) the use of the EUDI Wallet and new categories of qualified trust services in scope of the eIDAS 2 Regulation and (iii) the possibility to qualify as a recognized Data Altruism Organisation in the sense of the Data Governance Act.

f. Content of this report

This best practices report summarizes the lessons learned and best practices that have been identified during the dialogues for the first cohort.

Section 2 of this report discusses Blockchain/DLT Terminology and the relevant laws and regulations for Blockchain/DLT applications in general and more in particular for the 1st cohort. The best practices and lessons learned for the 13 focus areas for the 1st cohort dialogues are presented in Sections 3 to 15. The conclusions and next steps are discussed in Section 16.

2. Terminology, relevant laws and regulations

a. Terms, abbreviations, and legislation

A list of terms, abbreviations and (abbreviations of) legislation is included at the end of this best practices report (link).

b. Blockchain and DLT infrastructures

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 and the MiCAR as a starting point.

DLT or blockchain applications 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.

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 consists of the rules and procedures by which an agreement is reached, among DLT network nodes, that a transaction is validated.[9] 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.[10]

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.

c. Relevant laws and regulations for Blockchain/DLT applications

A broad range of EU and national laws and regulations can be relevant to individual blockchain/DLT 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

[9] Article 2(3) DLT-pilot Regime and Article 3(3) MiCA.
[10] Article 2(39) of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 (**Data Act**).

dialogues depending on the outcome of the selection process. The table below is not exhaustive and is updated regularly.

Generic relevant regulatory areas	Sector specific relevant regulatory areas	DLT specific regulations
• AI Act • AML/KYC • Battery Regulation • Cyber security • Consumer protection • Customs • Data Act • Digital Services Act • Data Governance Act • DAOs - Commercial registers • eIDAS 2 • EU ETS / MRV • GDPR • ESPR • Environmental, Social & Governance (ESG) regulation	• Automotive • Crypto assets • Cultural assets • Energy & Utilities • Education • Financial sector • Government • Health • Media • Retail • Trade & logistics	• MiCA Regulation • DLT pilot Regulation • Regulation on information accompanying transfers of funds and certain crypto-assets • Provisions in the Data Act • Provisions in eIDAS 2

Table 1: Relevant regulatory areas and DLT specific regulations (not exhaustive). A more elaborate list of relevant EU legislation is included at the end of this best practices report (link).

d. Legal and regulatory focus areas for the 1st cohort

The legal and regulatory focus areas for the 1st round of dialogues have been determined on the basis of an analysis of each of the selected 1st cohort use cases and in consultation with the use case owners. These regulatory areas are set out in the table below. The results of the 1st cohort dialogues are discussed in the next chapters of this report.

Regulatory focus areas area 1st cohort	Relevant (proposed) EU legislation per regulatory area[11]
1. GDPR - Regulatory compliance	The GDPR
2. Cyber security – Regulatory compliance	The NIS2 Directive[12]
3. DAOs - Commercial Registers	EU Company Law[13] including the Company Law Directive, the Shareholders Rights Directive, the Register Interconnection Regulation and the Digital Company Law Directive, EEIG Regulation. SCE Regulation, SE Regulation, Proposed Directive for ECBAs
4. Customs – Blockchain/DLT solutions under the existing customs regulatory framework	Union Customs Code / Implementing Regulation of the UCC
5. Blockchain/DLT solutions for Battery Passports and DPPs	Battery Regulation / (proposed) ESPR
6. Blockchain/DLT solutions to help preventing trafficking in cultural goods	Cultural heritage policies and regulation[14] / UNESCO Convention 1970
7. Blockchain/DLT solutions for EU ETS / MRV reporting	EU ETS / MRR / AVR / Directive (EU) 2023/959 / MRV Maritime Regulation / Commission Delegated Regulation (EU) 2023/2917
8. Blockchain/DLT solutions – Data collection & sharing under the Data Governance Act	Data Governance Act (DGA)

11 This list is not exhaustive and national legislation is not included. The full references to the legislation are included at the end of this best practices report (link).

12 The RCE Directive and DORA were not part of the 1st round of dialogues. In particular DORA will likely become relevant in the 2nd round of dialogues.

13 https://www.europarl.europa.eu/factsheets/en/sheet/35/company-law.

14 EU Action Plan against Trafficking in Cultural Goods (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13352-Trafficking-in-cultural-goods-EU-action-plan_en); Commission Recommendation (EU) 2021/1970 of 10 November 2021 on a common European data space for cultural heritage (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021H1970); Ex–ante impact assessment Report on a European collaborative cloud for cultural heritage (https://op.europa.eu/en/publication-detail/-/publication/90f1ee85-ca88-11ec-b6f4-01aa75ed71a1/language-en); Directive 2014/60/EU of the European Parliament and of the Council of of 15 May 2014 on the return of cultural objects unlawfully removed from the territory of a Member State and amending Regulation (EU) No 1024/2012 (Recast) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0060; Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0880); Implementing Regulation (EU) 2021/1079 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1079).

Regulatory focus areas area 1st cohort	Relevant (proposed) EU legislation per regulatory area[11]
9. Relevance of the eIDAS regulation for Blockchain/DLT solutions	eIDAS 2
10. Blockchain/DLT solutions for AML compliance	AMLD IV / AMLD V / TFR / DORA / AMLD V / AMLR
11. MiCAR & Financial sector regulation – Scope and delineation	MiFID II / MiFIR / CSDR / ECSPR / EMD II / PSD II / Prospectus Regulation / TFR / MiCAR / DLT-pilot Regime / TFR
12. Tokenization of shares and dividend payments	MiFID II / MiFIR / CSDR / ECSPR / EMD II / PSD II / Prospectus Regulation / TFR / PRIIPs Regulation / DLT Pilot Regime
13. Application of Financial Sector regulation to Smart Contracts	Financial sector regulation.[15]

e. Legal and regulatory focus areas for the next cohorts

The regulatory areas for the first cohort will continue to be relevant for the next cohorts. The next rounds of dialogues will allow for deeper dives into specific topics and to take account of new developments on the basis of secondary legislation, administrative decisions and case law.

Moreover, many of the regulatory instruments in the areas referred to in the above tables have evolved in the past two years or are currently reviewed or in the process of development. Therefore, other (new) regulatory areas will become relevant for the next cohorts such as the Data Act, the Digital Services Act, DORA, the AI Act, ESG regulation (including CSRD compliance), standardization and the regulation of smart contracts.

Areas for further clarification and dialogue for the next cohorts that have been identified during the 1st round of dialogues are set out in the respective sections for each of the regulatory areas (Sections 3 to 15).

The ongoing developments in existing and proposed EU legislation and regulations and the required deeper dives into topics that were identified during the 1st round of dialogues underline the relevance of the fact that the European Blockchain Sandbox is set up as a longer term project.

[15] Specific regulatory provisions in other areas of regulation such as Article 36 Data Act and Article 22 of the GDPR will likely become relevant for the next round of dialogues.

3. Data Protection (GDPR) – Regulatory compliance

a. Introduction

A blockchain is a distributed but shared and synchronised digital database that is maintained by a consensus algorithm and stored on multiple nodes (computers that store a local version of the database). Blockchains can be imagined as a peer-to-peer network, with the nodes serving as the different peers. Some nodes only store a copy of the ledger whereas other nodes can also help process and validate transaction blocks as part of the consensus process so that they can be added to the permanent ledger of the blockchain. Data is collected, stored and processed in a decentralised manner in the form of blocks. Because these blocks are continuously added, but in principle never removed, a blockchain can be qualified as an append-only data structure.

The data that is recorded on the blockchain can relate to transactions (cryptographic digital signatures and timing of entries), digital content (documents, photos, videos, etc.) or applications (smart contracts). When this data directly or indirectly relates to an identified or identifiable natural person, it qualifies as personal data and data protection laws come into play.

In the EU, this means the Regulation (EU) 2016/6792016/679 or General Data Protection Regulation ("GDPR") applies. The GDPR provides for a harmonized set of rules for the processing of personal data by controllers and processors in the EU.[16]

As set out in Section 2 of this report, different blockchain technologies have different characteristics. Compliance with the GDPR, depends to a large extent on the specific technical choices, and the governance set up of the use case. It is recommended to design the blockchain from the outset in a manner that takes the requirements of the GDPR into account, in accordance with the principles of data protection by design and default (Art. 25 GDPR).

The lessons learned and best practices that were discussed during the GDPR focused dialogues are presented in the next paragraphs.

b. Key question: Does the data recorded on the ledger qualify as personal data?

In order to determine if information recorded on the ledger (or otherwise processed) qualifies as personal data, the use case owner should assess whether the data contains information that relates to an identifiable natural person. Data that does not relate to a natural person, but to a legal person, will normally not qualify as personal data, but it may still qualify as such when the data will be used in order to treat a certain individual in a certain way (the purpose of the processing) or the processing is likely to have an impact on a certain individual (result of the processing). The same goes for data that relates to an object, e.g. a product.

To determine whether the data relates to an identifiable natural person account should be taken of all the means reasonably likely to be used (such as singling out) either by the controller or by a third party to identify the natural person directly or indirectly. Encrypting or hashing personal data is unlikely to make the data anonymous data (which no longer qualify as personal data). In most cases, such data is only pseudonymized data which still qualifies as personal data and therefore the GDPR requirements must be met.

---

[16] The EUI DPR (Regulation (EU) 2018/1725) provides for similar rules that are specifically aimed at the EU institutions, agencies and bodies that process personal data as controller or processor. The 1st round of dialogues focussed on the GDPR.

The mere fact that personal data on the ledger are unintelligible does not mean that such data no longer qualify as personal data. As long as there still is a link between the data recorded on the ledger and personal data off-chain, it should be assumed that the data on the ledger will also qualify as personal data. The non-intelligibility of some components of the data, or of the data as such does not remove this identification potential. For this reason, the data on the ledger should be treated as personal data (pseudonymized data) even if the only party that can use the link is the recipient of the service.

A case-by-case assessment is needed to determine whether envisaged or implemented de-identification measures are sufficient to qualify data as anonymous data and therefore as non-personal data to which the GDPR requirements do not apply.

Examples - Qualification of data on the ledger:

- Public keys associated with natural persons and single person legal entities can be assumed to be personal data.
- A hash that refers to transaction data that are stored off-line and contain personal data can still be assumed to be personal data.
- If the public keys from legal persons (other than single person legal entities) are repeatedly used by the same natural person working for the same legal entity, the public keys could still qualify as personal data if such a natural person would be identifiable (taking into account all means reasonably likely to be used by the controller or a third party. In that case, appropriate security measures pursuant to Art. 32 GDPR should be taken to avoid exposure of the natural persons handling the public keys.
- If verifiable credentials associated with natural persons are processed outside of the ledger, but some data relating to these verifiable credentials are recorded on the ledger (such as status information), such data could qualify as personal data and then would need to be handled in a manner compliant with the GDPR and/or other applicable data protection laws.
- Data on the ledger, linked to a product, will normally not be considered as personal data, unless the data relate to an identifiable natural person (e.g. the user or the repairer of the product).

The below ECJ case law and EDPB guidelines will be helpful to make this assessment, but important elements are still “work in progress”.

Relevant case law CJEU:

- C-582/1 (*Breyer*): In this landmark case, the CJEU found that a dynamic IP address registered by a provider of online media services when a data subject visited the website should be considered as personal data, in relation to that provider, when the latter has the lawful means to identify the natural person with additional data in the possession of a third party such as in this case the internet service provider.
- C-479/22 P (*OC*): The CJEU found that the question whether information contained in a press release emanating from a Union institution or body is covered by the concept of ‘personal data’ is to be assessed exclusively in the light of the conditions laid down by the EUI DPR.[17] ‘Indirect identification’ of a person necessarily means that additional information must be combined with the data at issue for the purposes

[17] See previous footnote.

of identifying the person concerned. The EUI DPR does not lay down any conditions as regards the persons capable of identifying the person to whom an item of information is linked, since recital 16 of that regulation refers not only to the controller but also to 'another person'.

- C-413/23 P (*SRB*) (currently pending in appeal): in this case, the CJEU has to decide on the appeal of the EDPS against the judgment of the General Court.[18] The case takes place in the context of the adoption of a resolution scheme, involving the Single Resolution Board (SRB), in its capacity of Banking Union resolution authority, and a Spanish bank called Banco Popular. During the process of resolution, the SRB had invited the shareholders to submit comments in order to assess whether they should be given compensation. To examine these comments, the SRB classified them and attributed them an alphanumeric code. Some comments were sent to an independent valuer to help complete the assessment. Following these events, some shareholders filed a complaint before the EDPS on the ground that they had not been informed of their personal data being transferred to a third party. The EDPS agreed with the complainants that their personal data had been processed by the valuer while they had not been informed of any transfer of their data by the SRB and that therefore there had been a violation of the EUI DPR. The General Court, however, held that the transfer of comments which were attributed an alphanumeric code was not per se a transfer of personal data. The EDPS should have assessed from the view of the data recipient whether it had any lawful means available which could in practice enable the latter to access the additional information necessary to re-identify the authors of the comments.

EDPB guidelines:

- Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007.
- Art. 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014.
- EDPB, Blockchain guidelines (work in progress).
- EDPB, Guidelines on anonymization / pseudonymization (work in progress).

In the event of doubt, it is recommended to have an open discussion with the competent data protection authority before launching the service or to assume that data on the ledger could qualify as personal data and should be treated as such.

If the data on the ledger qualifies as personal data, this does not mean that the use case could not be compliant. It means that appropriate measures have to be taken by the controller to ensure and demonstrate compliance with the GDPR such as inter alia 1) determine the data protection roles of the different stakeholders (i.e. (joint) controller, data processor, or neither) and 2) for the controller(s), determine the legal basis for the processing of the personal data concerned (e.g. legal obligation, contractual necessity, consent or legitimate interest), 3) comply with data subject rights such as the right to erasure and 4) implement appropriate technical and organizational (security) measures as required by art. 32 GDPR (e.g. access control mechanisms). Which measures have to be taken, depends on the purpose of the processing, the setup of the DLT use case and the risk for the rights and freedoms of data subjects that is associated with the data processing on the ledger.

The less risk for data subjects is associated with the data processing, the less (extensive) technical and organisational measures controllers and processors are necessary to take to

[18] Judgement of the General Court in the Case T-557/20

ensure compliance with the GDPR. Implementing appropriate encryption and/or other privacy enhancing technologies, including storing only very limited or unintelligible personal data on the blockchain, will lead to a lower risk of (re)identifiability of data subjects and therefore will generally make it easier to comply with the GDPR.

Best practices - Qualification of data on the ledger:

- Encrypting or hashing personal data is unlikely to make the data anonymous. In most cases, such data is only pseudonymized data which still qualifies as personal data.
- A case-by-case assessment is needed to determine if de-identification measures are sufficient to qualify data as anonymous data and therefore as non-personal data to which the GDPR requirements do not apply.
- ECJ case law and EDPB guidelines will be helpful to make this assessment, but important elements are still "work in progress".
- Data related to products are not personal data unless the data relates to an identifiable natural person (user/repairers or the use/handling by an identifiable natural person). If a data protection assessment has been made and it is shown that the data about products is only product-related without a link with an individual owner/user/repairer or that there is no risk of identification, then it can be assumed there is no personal data on the ledger.
- In the event of doubt, it is recommended to have an open discussion with the competent data protection authority before launching the service or to assume that data on the ledger could qualify as personal data and should be treated as such.

c. Data protection roles

In a blockchain use case, different parties may separately process personal data in their systems. Such parties may be controllers if they determine purposes (why) and means (how) of the processing.[19] They may be processors if they only process personal data on behalf of other parties operating as controllers.[20]

The GDPR assumes that the processor processes data on behalf of a controller governed by a contract or other legal act under Union or Member State law, and that there is a controller that can be identified for every element of the data processing route.[21] In accordance with the principle of accountability, it is necessary to assess the roles of all the parties using or involved in blockchain technologies. In this assessment, various elements need to be taken into account, such as, for instance, the nature of the service provided, the blockchain governance mechanism, the precise legal, technical and organisational characteristics of the blockchain, the relationships between the different actors involved, as well as the relevance of the processing of personal data within the scope of the service provided.

The governance mechanism of the blockchain defines the decision-making model. In a permissioned blockchain, node operators would operate as data processors if they process data on behalf of other parties. These other parties would then act as (joint[22]) controllers or as a data processor for another controller (e.g. the company that is the customer of the

[19] Art. 4(7); Art. 24 GDPR.
[20] Art. 4(8); Art. 28 GDPR.
[21] Art. 4(7) GDPR; https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.
[22] Art. 4(7) GDPR; Art. 26 GDPR.

service provider), depending on the circumstances of the case. The GDPR stipulates that the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject (Art. 28(1) GDPR). Also, the processing of personal data by the node operators needs to be governed by a data processing agreement or other legal act under EU or national law meeting the requirements of Article 28(3) GDPR.

- In a permissioned blockchain the implementation of these requirements can be relatively straight forward. In a permissionless blockchain however the assessment of the data protection roles and the implementation of compliance measures is more complex. The possibilities to make use of permissionless blockchain options will be discussed in more detail in the next rounds of dialogues.

If the DLT provider does not process any personal data but only develops and sells software but the customer decides how the software is used without any involvement by the DLT provider and the DLT provider cannot see which data is used (including which data is stored) and also does not have the keys to decrypt the data, and does not have a say in who is processing the data, then the DLT provider would likely be neither a controller nor a processor under GDPR, but only a mere technology provider.

This could be different if the DLT provider (and not the customer) would determine the settings and thereby determine essential means or if it would receive diagnostic/telemetry data for its own purposes. In that case, the DLT provider could qualify as a controller or a joint controller.

If the DLT provider would be able to view personal data (e.g. see or store user accounts or diagnostic/telemetry data) for support purposes on behalf of the customer, the DLT provider could qualify as a data processor for this data processing.

Lessons learned - data protection roles:

- In a **permissioned** blockchain, **node operators** would normally qualify as data processors on behalf of the application service providers (ASPs) as controllers if (and as long as) they (only) process personal data on behalf of these ASPs:
  - The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects (Art. 28(1) GDPR).
  - The processing of personal data by the node operators needs to be governed by a data processing agreement or other legal act under EU or national law meeting the requirements of Article 28(3) GDPR.

  In the case that the ASPs would themselves act as data processors processing personal data on behalf of their customers as controllers, the node operators would be subprocessors.

- In a permissionless blockchain the assessment of the data protection roles is more complex. The role of node operators in a permissionless blockchain could become part of the upcoming dialogues for the next cohorts.

d. Legal basis

Processing of personal data requires a legal basis (Article 6(1) GDPR). Depending on the characteristics of the use case, the legal basis "performance of a contract" ("contractual necessity")[23], if applicable, seems an efficient legal basis for cross-border use cases, because the interpretation of this legal basis will generally not be dependent on national laws and interpretations (assuming that the contract contains a governing law provision). The legal basis "legal obligation"[24] could also work in a cross border setting, but this basis depends on the applicable EU and/or Member State national legislation.

An alternative legal basis could be to ask for the data subject's "consent" to the processing of their personal data[25], but consent needs to meet strict requirements which can be complex to comply with in practice. For example, the consent must be freely given in order to be valid.[26] Also, the requirement that the data subject should be able to withdraw a given consent at any time and then the processing should be stopped, requires careful consideration in a blockchain context. Other legal bases could also be relevant, depending on the characteristics of the use case, and will often require an analysis on a country-by-country basis.[27]

Lessons learned and best practices – Legal basis

- "Performance of a contract" ("contractual necessity"), if applicable, can be an efficient legal basis for cross-border use cases, because the interpretation of this legal basis will generally not be dependent on national laws and interpretations (assuming that the contract contains a governing law provision).
- Other legal bases could also be relevant, depending on the characteristics of the use case:
  - "Legal obligation", if applicable, will depend on EU legislation or on the applicable EU or Member State national legislation.
    - *Example: Battery passports / Digital Product Passports in relation to mandatory information.*
  - "Legitimate interest" would not be appropriate for the processing activities carried out by controllers that are public authorities in the performance of their tasks.
    - *Possible example: Non-mandatory information in Digital Product Passports serving legitimate interests if the conditions are met.*
  - "Consent" from the data subject needs to meet strict requirements which can be problematic to comply with in practice:
    - *the consent must be freely given in order to be valid.*
    - *the data subject should be able to withdraw a given consent at any time and then the processing should be stopped which requires careful consideration in a blockchain context.*
- Please note that in order to rely on one of the above legal bases, the relevant conditions need to be met as set out in Art. 6 GDPR and further elaborated in case law and guidance.

[23] Art. 6(1)(b) GDPR.
[24] Art. 6(1)(c) GDPR.
[25] Art. 4(11) GDPR; Art. 6(1)(a) GDPR.
[26] This can for instance not easily be assumed in an existing or future employment.
[27] Art. 6(1)(e) & (f) GDPR; the legal basis "legitimate interest" (6(1)(f)) would not be appropriate for the processing activities carried out by Issuers that are public authorities in the performance of their tasks.

e. Data subject rights – right to erasure

Data subject rights require specific attention in a blockchain setting:

- Transparency (Articles 12-14 GDPR): Data subjects must be provided with clear, transparent, and easily understandable information about how their personal data is processed.
- Access (Article 15 GDPR): Data subjects have the right to obtain confirmation of whether their personal data is being processed and, if so, to access that information.
- Rectification (Article 16 GDPR): Data subjects have the right to rectify inaccurate personal data and to complete incomplete data.
- Erasure (Right to be forgotten) (Article 17 GDPR): Under certain circumstances data subjects have a right to have their personal data erased.
- Restriction (Article 18 GDPR): Data subjects have the right to obtain a restriction on the processing of personal data relating to them in a number of circumstances.
- Data portability (Article 20 GDPR): Data subjects have the right to receive the personal data which they have provided to a controller in a structured, commonly used and machine-readable format, and to have that data communicated to another controller without hindrance from the controller to whom the personal data have been provided.
- Objection (Article 21 GDPR): Under certain circumstances, data subjects have the right to object to the processing of personal data if based on Article 6(1)(e) GDPR ("*public interest*") or Article 6(1)(f) GDPR ("*legitimate interests*"). Where personal data are processed for direct marketing purposes, the data subjects shall have the right to object at any time to processing of personal data concerning them for such marketing,
- Automated decision-making (Article 22 GDPR): Data subjects have the right not to be subject to a decision based solely on automated processing by the controller, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Transparency and the exercise of the right of access, objection, restriction and data portability appear to be not very problematic in a blockchain setting but due to the immutable nature of blockchain the enforcement of the right to erasure and the right to rectification could be more difficult to implement depending on the technical settings.

In principle the right to be forgotten / right to erasure could be implemented by breaking the link between the hash that is recorded on the ledger and the off-line storage, assuming a perfect cryptography/anonymization so that the hash cannot be reverse engineered to the personal data in the off-chain storage in any way. It should be noted that such an on-chain/off-chain architecture requires the use of another system in order to store the data itself. This means that there will also be a personal data processing in another component of the infrastructure which requires a separate risk assessment of this other system.

Lessons learned and best practices – Right to erasure

- In principle the right to be forgotten / right to erasure could be implemented by breaking the link between the hash that is recorded on the ledger and the off-line storage, assuming a perfect cryptography/anonymisation so that the hash cannot be reverse engineered to the personal data in the off-chain storage in any way.
- It should be noted that such an on-chain/off-chain architecture requires the use of another system in order to store the data itself. This means that there will also be a personal data processing in another component of the infrastructure which requires a separate risk assessment of this other system.

f. Security measures

Pursuant to Art. 32 GDPR, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Examples mentioned in Article 32 GDPR include (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Therefore, providers of DLT/blockchain technology that qualify as controllers/processors under the GDPR should also consider the security requirements under the GDPR and, in so far as relevant, comply with the guidance issued by the European Data Protection Board ("EDPB") and the guidance issued by the local data protection authorities. This includes, for example, the Guidelines on Data Protection by Design and by Default (see the website of the EDPB) and relevant guidance that is available on the national level such as the guidance developed by the German Data Protection Conference (DSK) on the implementation of concrete technical and organisational measures (see here and here).

It should be ensured that a new data processing activity or a change in an existing data processing activity does not accidentally lead to the processing of more personal data than needed ("the principle of data minimisation"). In addition, it should be ensured that the data processing does not result in (additional) security risks for the rights and freedoms of the concerned data subjects (data leakage, data scraping of personal data or accidental ongoing viewing rights).

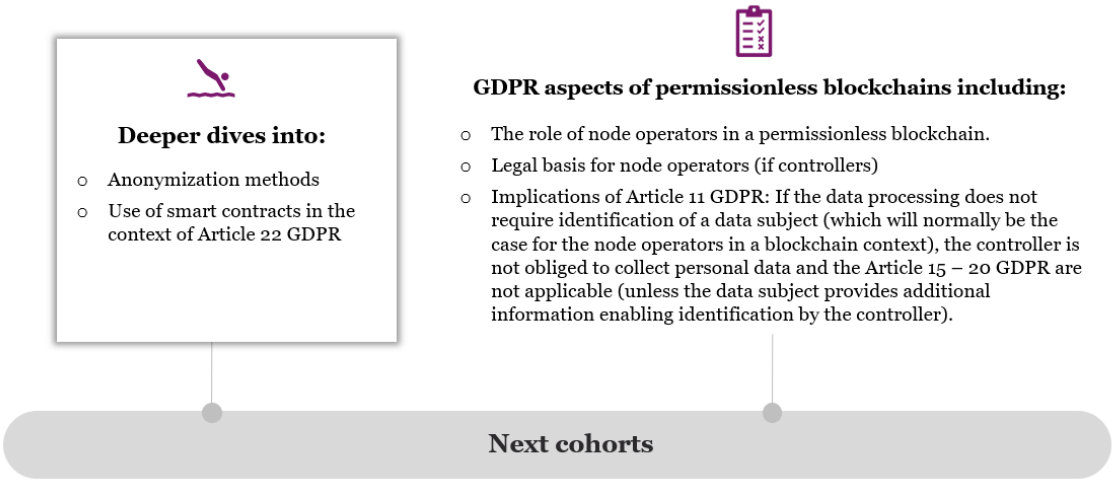
Best practices & lessons learned – security measures:

- The less risk for data subject rights and freedoms is associated with the data processing, the less (extensive) technical and organisational measures controllers and processors are required to take to ensure compliance with the GDPR.
- Appropriate encryption and/or other privacy enhancing technologies, including storing only very limited or unintelligible personal data on the blockchain, help to minimize the risk in case of data breach and are a way to protect and secure data during transfer or storage.

g. Areas for further clarification & dialogue topics for the next cohorts

The GDPR related dialogues were not exhaustive and further topics and developments in case law and the EDPB guidelines will be discussed in the next cohorts if they become available.

For instance, anonymization methods and the use of smart contracts in the context of Article 22 GDPR could be relevant topics for the next cohorts as well as a more detailed discussion in relation to the GDPR aspects of permissionless blockchains.



4. Cyber Security (NIS2) – Regulatory compliance

a. Introduction

Cyber security legislation is another important regulatory area for most of the blockchain/DLT use cases. The relevant regulation was recently amended/adopted: the NIS2 Directive,[28] the CER Directive,[29] and DORA.[30]

By 17 October 2024, Member States will need to adopt and publish the measures necessary to comply with the NIS2 as well as the CER Directive. They will apply those measures from 18 October 2024 and the DORA will apply from 17 January 2025.

During the 1st round of dialogues, the focus was in particular on the scope of NIS2 and the relevance for blockchain/DLT use cases in preparation of the relevant national law provisions becoming applicable.

NIS2 is the key piece of cybersecurity legislation that will impose more detailed and stringent obligations on entities within its scope, replacing the NIS Directive from 18 October 2024.

Importantly, unlike the GDPR, the NIS2 focus is not on personal data but on the network and information systems used by the entities within the scope of the NIS2 Directive for the provision of their services. Therefore, the NIS2 regulatory requirements apply in addition to the GDPR security requirements if applicable.[31]

The NIS2 Directive follows a minimum harmonisation approach: while all Member States must implement new national laws to reflect the NIS2 Directive, the directive does not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity. As a result, providers of DLT/blockchain technology should closely monitor the national implementation of the new NIS2 Directive in the jurisdictions in which they are regulated, so that appropriate account of the correct set of rules can be considered when implementing new requirements.[32]

b. Key question: To what extent is cybersecurity legislation relevant for DLT/Blockchain providers?

For providers of DLT/blockchain technology, in particular the provisions of the NIS2 legislation and the transposition in national legislation will often be relevant. As mentioned above, unlike the GDPR, the focus of NIS2 is not on personal data but on the network and information systems used by the entities within the scope of the NIS2 Directive for the provision of their services.

There are three main reasons why the NIS legislation is relevant for Blockchain/DLT applications:

---

28 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (**"NIS2 Directive"**).

29 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (**"CER Directive"**).

30 *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("**DORA**"). The DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities and addresses both, the digital as well as physical dimension. It constitutes the lex specialis regarding the NIS2 Directive and addresses in a comprehensive manner the physical resilience of financial entities with the consequence that certain provisions set out in the CER Directive do not apply to those entities.*

31 See Section 4.

32 See the Bird & Bird NIS2 Directive Implementation Tracker, available under: https://www.twobirds.com/en/trending-topics/cybersecurity/nisd-tracker.

- Blockchain/DLT providers can be **directly** within scope of the NIS2 Directive.
- Blockchain/DLT providers can be **indirectly** in scope of the NIS2 Directive.
- Blockchain/DLT solutions will in the future be part of the **security measures** that can be used in cybersecurity; standards for blockchain/DLT solutions will be adopted.

Direct relevance

A provider of a DLT/blockchain technology will often be directly within the scope of the NIS2 Directive and will need to comply with its obligations in conjunction with the relevant local implementation.

A provider of a DLT/blockchain technology (for example, a provider of DLT-powered data storage) will often qualify as a managed service provider (**"MSP"**) under the NIS2 Directive. Other categories could be relevant as well, such as managed security services providers (**"MSSP"**), cloud computing providers or content delivery network providers.

- MSPs and MSSPs that do not meet or exceed the ceilings for medium-sized enterprises (as further specified in the Recommendation 2003/361/EC), will normally be exempted from the NIS2 requirements (but check national specific rules).
- If a development towards exceeding the thresholds is expected, it is recommended to consider the cybersecurity requirements at an early stage, before the thresholds are reached, in order to prepare for compliance in the most efficient way.

If a provider of a DLT/blockchain technology that qualifies as an MSP (or as MSSP) provides its services within the EU/EEA and meets or exceeds the ceilings for medium-sized enterprises (as further specified in the Recommendation 2003/361/EC),[33] it must, comply with the NIS2 requirements from 18 October 2024. The application of the NIS2 Directive to MSP/MSSP, irrespective of their size, is more likely to be an exception. However, if the thresholds are not exceeded, but a development towards exceeding the thresholds is expected, it is recommended to consider the NIS2 cybersecurity requirements at an early stage, before the thresholds are reached, in order to prepare for compliance in the most efficient way.

In addition, trust services in the sense of the eIDAS 2 regulation fall within the scope of NIS2 as essential or important entities, regardless of their size. As a result of the extended definition of "trust services" in the eIDAS 2 regulation, Blockchain/DLT use cases will often be in scope of the definition of trust service providers (**"TSPs"**) which is another reason why the NIS2 legislation is directly relevant for blockchain/DLT services.[34] Therefore, if the blockchain/DLT provider is also a TSP in the sense of the eIDAS 2 regulation, the use case can likely not rely on the thresholds in NIS2 applicable for MSPs/MSSPs.[35]

---

[33] The category of medium-sized enterprises is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million. A small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. See Article 2 of the Annex to Recommendation 2003/361/EC, available under https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361&from=EN.

[34] See Section 11 of this report.

[35] Member States can identify entities of a type referred to in Annex I or II as essential or important entities regardless of their size, where (i) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities; (ii) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health; (iii) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact; or (iv) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State (see

For most use cases, the country where the provider has its main establishment will determine the relevant jurisdiction and the competent authority irrespective of where customers are based.[36]

Indirect relevance

Blockchain/DLT providers can also be indirectly subject to the NIS2 rules if the provider is part of the supply chain and provides its services to customers which are regulated under the NIS2 Directive. Such customers will then need to impose certain obligations on their DLT/blockchain technology providers.

As a result of the broadening of the scope of the cybersecurity regulation in the NIS2 Directive compared to NIS 1, additional categories of customers qualify as essential or important entities as defined in the NIS2 Directive. Reference is made to the table below. Based on the national implementation the extended scope could also include e.g., public administration entities at local level and educational institutions, in particular where they carry out critical research activities.

Annex I – Sectors of high criticality	Annex II – Other critical sectors
• Energy • Transport • Banking • Financial market infrastructure • Health • Drinking water • Wastewater • Digital infrastructure • Internet Exchange Point providers • DNS service providers, excluding operators of root name servers • TLD name registries • Cloud computing service providers • Data centre service providers • Content delivery network providers • Trust service providers • Providers of public electronic communications networks • Providers of publicly available electronic communications services • ICT service management (B2B) • Managed service providers (MSP) • Managed security service providers • Public administration • Public administration entities of central governments as defined by a Member State in accordance with national law • Public administration entities at regional level as defined by a Member State in accordance with national law	• Postal and courier services • Waste management • Manufacture, production and distribution of chemicals • Production, processing and distribution of food • Manufacture of medical devices, certain electronic products as well as machinery and transport • Digital providers • Providers of online marketplaces • Providers of online search engines • Providers of social networking services platforms • Research organisations

Art. 3(1), point (e), Art. 3(2) in conjunction with Article 2(2), points (b) to (e) NIS2 Directive). In addition, entities identified as critical entities under the CER Directive shall be also considered as essential entities, regardless of their size.

[36] The main establishment is where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union (Art. 26(1)(b) and Art. 26(2) NIS2 Directive).

• Space	

If customers qualify as essential or important entities in the sense of the NIS2 Directive, the competent cyber security authority is the country of the customer. Depending on the nature of the customer's services/operations, this can be the country in which the customer is established, has its main establishment or provides its services.[37]

Blockchain/DLT solutions in support of cyber security

Blockchain/DLT will in the future likely be part of the security measures that can be used in cybersecurity. Standards take time and will in the case of compliance with NIS2 be closely connected with the standards that will be adopted pursuant to the eIDAS 2 regulation;[38] therefore, there is currently not yet a standard for blockchain.

c. Relevant regulatory provisions for (suppliers of) entities in scope of NIS2

In the context of cybersecurity risk-management requirements, an essential or important entity in the sense of NIS2 legislation will need to take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the network and information systems which it uses for the provision of its services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Such measures must include inter alia incident handling, business continuity and supply security. Compared to the NIS1 Directive the regulatory obligations for essential and important entities will become more stringent. This includes in particular the following:

(i) Registration requirements (Article 3(4) in conjunction with Article 3(3) NIS2 Directive; Article 27(2), (1) NIS2 Directive): The entities in scope of the NIS2 Directive will need to submit certain minimum information (including i.a., the name of the entity, address, up-to-date contact details, etc.) to the competent authorities in connection with the Member State's list of essential and important entities as well as entities providing domain name registration services. In addition, certain types of entities covered by this legislative act (including inter alia cloud computing service providers, content delivery network providers and managed service providers as set out in Article 27(1) NIS2 Directive) will be required to submit certain information to the competent authorities in connection with the ENISA's registry of entities referred to in Article 27 by 17 January 2025.

(ii) Jurisdiction (Article 26 NIS2 Directive): NIS2 Directive determines which Member State or Member States have jurisdiction.

(iii) Strengthened cybersecurity risk-management requirements (Article 21 NIS2 Directive): The entities will need to have certain measures in place (e.g., measures regarding incident handling, business continuity, supply chain security, human resources security, access control policies and asset management) to manage the risks to the security of the network and information systems.

(iv) More detailed reporting obligations (Article 23 NIS2 Directive): The NIS2 Directive follows a graduated approach with respect to notification of significant

[37] Art. 26(1) NIS Directive.
[38] Section 11 of this report.

incidents to the CSIRT or, where applicable, the competent authority. The entities will also need to notify the recipients of their services in certain cases.

(v) Cybersecurity certification (Article 24 NIS2 Directive): For the purposes of demonstrating compliance with cybersecurity risk-management measures, Member States may require essential or important entities to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes. In addition, the Commission is empowered to adopt delegated acts, to supplement the NIS2 Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme.

(vi) Explicit governance requirements (Article 20 NIS2 Directive): The management bodies of essential and important entities will be required to approve and oversee the implementation of the cybersecurity risk-management measures. In addition, the members of these management bodies will be required to follow training and shall encourage entities to offer similar training to their employees on a regular basis.

(vii) Accountability of top management, supervision and enforcement (Article 20(1) first subpara. NIS2 Directive, Article 31 et seqq. NIS2 Directive): The new legislative act also introduces accountability and liability of top management for the non-compliance with cybersecurity obligations, more stringent supervisory measures for national authorities as well as stricter enforcement requirements and aims to harmonise sanctions regimes across Member States.

d. Areas for further implementation

Further harmonization regarding technical and methodological requirements for e.g. MSPs, MSSPs and TSPs will be laid down in an implementing act which will be adopted by the European Commission by 17 October 2024 (Art. 21(5) NIS2). See the following European Commission's website addresses:

- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Rules-specifying-the-obligations-laid-down-in-Articles-21-5-and-23-11-of-the-NIS-2-Directive_en;
- https://digital-strategy.ec.europa.eu/en/policies/nis2-directive and
- https://commission.europa.eu/index_en

In addition, the implementing acts and standards on the basis of the eIDAS 2 regulation will often be relevant for blockchain/DLT providers that qualify as TSPs.[39]

Regarding compliance with the cybersecurity risk-management requirements under the NIS2 Directive, compliance with ISO 27001 is a good starting point. The NIS2 Directive refers in its recitals to the ISO/IEC 27000 series as an example of standards in line with which entities within the scope of the NIS2 Directive should address cybersecurity risk-management measures.

Finally, further requirements related to blockchain/DLT solutions, such as may be issued by the European Union Agency for Cybersecurity ("**ENISA**"), may become relevant in the future. In this regard, the publications of the ENISA should be closely followed (see https://www.enisa.europa.eu/publications#c3=2014&c3=2024&c3=false&c5=publicationDa

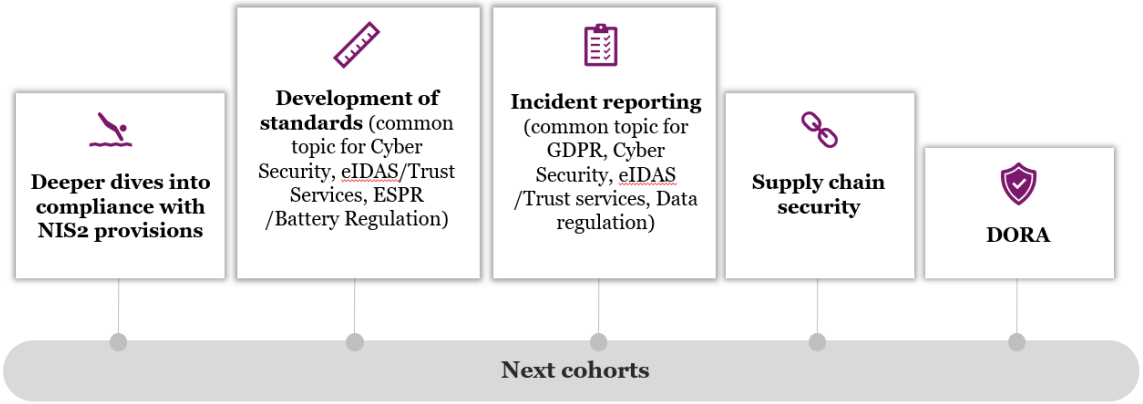
[39] Section 11 of this report.

te&reversed=on&b_start=0. See for example the ENISA guidance provided regarding DLT and cybersecurity in the context of the financial sector (see https://www.enisa.europa.eu/publications/blockchain-security).

e. Areas for further clarification & dialogue topics for the next cohorts

In view of the fact that the next generation of EU cyber security legislation is relatively new and further implementation acts and standardisation are expected, cyber security will likely continue to be an important regulatory area for the upcoming cohorts.

Additionally, if a provider of a DLT/blockchain technology provides its services to customers that are financial entities, the Digital Operational Resilience Act ("**DORA**") will need to be considered. This legislation will apply from 17 January 2025 in all EU/EEA Member States without the need for implementing national legislation. DORA will also likely be an important regulatory area for the upcoming cohorts.



5. DAOs – Commercial registers

a. Introduction

DAOs (Decentralized Autonomous Organizations) present a challenge to both national and Union legislation with respect to the incorporation, registration, existence and the application of and compliance with regulation of legal entities. DAOs as such are not recognized as a separate category of legal entities.

At this point in time, DAOs are often registered in commercial registers through legal 'wrappers': registering a DAO through existing legal entities, mostly foundations or associations. This practice does exist in few European countries, such as Switzerland, Liechtenstein and Estonia. Registering DAOs as independent legal entities is not yet foreseen in any national law within Europe currently.

b. DAO definitions in EU and national legislation?

A Decentralized Autonomous Organisation ("**DAO**") is not a defined term and is currently not used in EU legislation. There are different types of "DAOs": **with or without a legal wrapper** and **for-profit/non-profit**.

The European Central Bank is using the following definition: "A DAO is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralised (i.e. independent from central control)."[40]

Other Examples of published DAO-descriptions include:

- World Economic Forum: Decentralized autonomous organizations (DAOs) are organizational structures that use blockchains, digital assets and related technologies to allocate resources, coordinate activities and make decisions.
- INO (Internet Native Organisation):[41] "A digital-native organizational structure that operates on distributed ledger technology such as blockchain, governed by a set of self-executing rules and decisions made through the collective input of its members which could be public or non-public."
- Dutch Blockchain Coalition: It is an organizational structure characterized by the absence of hierarchical management. A DAO consists of a group of people who share a common mission and can vote democratically on ways to achieve that mission. An important part is that members of the group can submit proposals themselves, which can then be voted on. This form of governance is facilitated with blockchain technology. DAOs use smart contracts, which are programs that ensure that actions are carried out automatically when certain criteria are met. This makes it possible to make decisions and perform tasks in a transparent, fast and decentralized way.[42]

The common denominators appear to be the use of distributed ledger technology such as blockchain and "decentralized governance" meaning that decision-making is distributed among multiple parties.

In Malta: CAP 592 Innovative Technology Arrangements and Services Act ("**ITAS Act**") addressing Innovative Technology Arrangements ("**ITAs**") including DLTs. Article 5(1) of

---

40 European Central Bank, 'Occasional Paper Series, The future of DAOs in finance, No 331' p. 8 (https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf)

41 https://internetnative.org/defining-decentralized-autonomous-organizations-daos/.

42 https://dutchblockchaincoalition.org/nieuws/decentralized-autonomous-organizations.

this Act states that the application for a registration as an ITA should be submitted by a legal or natural person who can be addressed/held responsible:

- Article 5(1) - "Any person who desires to obtain recognition for any innovative technology arrangement or any innovative technology service as stated in the Schedules may apply to the Authority (the Malta Digital Innovation Authority) by making use of the relevant prescribed forms issued by the Authority for the purpose or in the absence of a prescribed form, by an application in writing providing the information required by the Authority for such purpose with reference to the subject matter of the application."
- Article 9(7) of the ITAS ACT refers to "innovative technology service providers' such as, systems auditors whose role is to audit the innovative technology arrangement or service and is not the 'person who desires to obtain recognition for any ITA or any ITS".

Common denominators in DAO descriptions:

- The common denominators appear to be the use of distributed ledger technology such as blockchain and "decentralized governance" meaning that decision-making is distributed among multiple parties.

c. Regulatory compliance by DAOs

DAOs operating on a distributed ledger system, without legal entity status and lacking a central authority figure, may be incompatible with certain existing legal frameworks which are designed to govern legal or natural persons. Thus, such DAOs (depending on their activities) may face compliance issues and pose a complex challenge for regulators due to their inherent conflict with traditional legal frameworks. At the same time individual DAO-members who operate without legal entity status may face complex regulatory and civil liability issues if something goes wrong.

Some examples of regulatory instruments assuming legal entity status include:

- Financial sector regulation and MiCAR assume legal entity status with limited exceptions for e.g. investments firms and crypto asset services.[43]
- The Data Governance Act requires legal entity status for registration or notification of a Data Intermediation Service Provider or a Data Altruism Organisation.[44]

Financial sector regulation and MiCAR also require a registered office in a Member State while other EU legal/regulatory instruments such as the NIS2 Directive[45], and notification/registration/authorization requirements in (other) sector specific legislation require at least a physical address (contact/agent/establishment) in the EU/EEA.[46]

Therefore, legal entity status of a DAO and a physical address will often be in the interest of all involved (including competent authorities) for reasons of regulatory compliance, civil liability issues and the possibility to "own" assets such as solar parks, IP rights etc.

---

43 Art. 4(1)(1) MiFID 2; Art. 4(1), 5(1), 16(1) and 59(3) MiCAR.
44 Art. 18(b) DGA; Art. 12(a) DGA.
45 Directive (EU) 2022/2555 (Article 27).
46 Examples include: Article 12(4) point (c) Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code; Article 8(1) Regulation (EU) No 1169/2011 of 25 October 2011 on the provision of food information to consumers; Article 9(1) Regulation (EU) No 1227/2011 of 25 October 2011 on wholesale energy market integrity and transparency.

Lessons learned

1. There are different types of "DAOs": **with or without a legal wrapper** and **for-profit/non-profit**.

2. Legal entity status and a physical address of a DAO will often be in the interest of all involved (including competent authorities) for reasons of regulatory compliance, civil liability issues and the possibility to "own" assets such as solar parks, IP rights etc.

d. Legal entity status – Qualification

Although there is no complete codified European company law as such, harmonisation of the national rules on company law has created some minimum standards. More specific corporate law Union legislation includes rules regarding the formation, capital and disclosure requirements, and operations (such as mergers and divisions) of companies, such as the Commission Implementing Regulation (2021/2042) on the system of interconnection of business registers, Directive 2017/1132 relating to certain aspects of company law, and Shareholders rights Directive 2007/36/EC. In addition, the freedom of establishment is one of the core freedoms of Union law.[47]

Under EC regulations, certain European legal entities exist throughout the EU and coexist with national ones, such as the European Company (SE) and the European Cooperative Society (SCE). Although based upon EU regulations, such European legal entities are governed by national company law. Apart from these legal entities with a basis in EU legislation, there are also legal entities that can only be incorporated by member states and that are not governed by national law, such as the European Research Infrastructure Consortia (ERICs) and the ERIC and the European Digital Infrastructure Consortia (EDICs).[48]

Registering a legal entity is primarily a matter of national laws and is mandatory from a company law perspective. In addition, several regulations require that a company is registered with regulatory and supervisory authorities for licensing, registration or notification purposes, incident reporting, first point of contact for cybersecurity regulation etc.

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

[48] By way of an example reference is made to the Commission Implementing Decision (EU) 2024/1432 of 21 May 2024 setting up the European Digital Infrastructure Consortium for European Blockchain Partnership and European Blockchain Service Infrastructure (EUROPEUM-EDIC) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401432).

Legal entity status – Qualification:

- Article 49 TFEU: If a legal entity is recognised in one Member State (either on the basis of the incorporation theory or on the actual seat theory), such legal entity should also be recognised as a legal entity in other Member States:
  - incorporation theory: the laws that apply to a legal entity are those of the jurisdiction in which the legal entity has been incorporated; and
  - actual seat theory: according to this theory, the law of the country where the company has its 'real' seat (i.e. its management and control centre) is the law applicable to company relationships (https://europa.eu/epso/doc/en_lawyling.pdf).
- The categories of legal entities are determined by national law or based on EU legislation such as for instance an EEIG (Regulation (EEC) No. 2137/85), an SCE (Regulation (EC) No. 1435/2003) or an SE (Regulation (EC) No. 2157/2001).
- Legal entities are governed by the national law of the Member State where they are established or by the national law of the Member state where they are incorporated:
  - If a legal wrapper is used: based on the national law governing the relevant legal entity
  - In other cases: depending on applicable national legislation
- Therefore, whether a DAO (either with or without a legal wrapper) is recognised as a legal entity is a matter of national law, but once it is recognised as a legal entity in one of the Member States, all other Member States are required to recognise the DAO as such. Whether a DAO is a legal entity requires a case-by-case analysis.

During the dialogues several characteristics of an effective DAO have been identified and can serve as a checklist to “test” to what extent such characteristics can be facilitated by legal entities legislation (this list is not meant to be exhaustive):

- Members with voting rights;
- A well-defined purpose which is aligned with the interest of the members;
- Distributed/multi stakeholder and transparent governance and interests (financial or non-financial);
- Required organs for decision making and representation, including appointments and change of members;
- Decentralised/electronic, decision-making, bookkeeping and administration;
- Limitation of liability of founders/individual members;
- Acceptance of the use of smart contracts for decision-making;
- Clear rules regarding representation vis-à-vis other market parties/authorities. And the power of intervention: who has the power to intervene when things are going wrong, while maintaining the decentralized aspect of the DAO;
- Rules for winding up a DAO.

Given the increasing relevance of DAOs, not only in the EU but internationally, it is important to find a balance between centralized elements such as a physical address and a board/agent for external communication and decentralized governance. Further consultations would be welcome regarding:

- Registration requirements in the commercial register(s), including minimum registration requirements;

- UBO qualification and registration; and
- DAO regulation initiatives in different countries, including various US States.

Further understanding and research is required to determine whether it is possible – at least to a relevant extent - to facilitate the above-mentioned characteristics by "associations" with legal entity status, although 100% decentralization of governance, decision-making and communication appears not realistic.

In addition, it could be investigated in further detail if the European Cooperative Society ("SCE")[49] and the proposal for European cross-border associations ("ECBAs")[50] are or could become appropriate EU legal vehicles for respectively DAOs for profit and non-profit DAOs (see overviews in **Annex IV**).

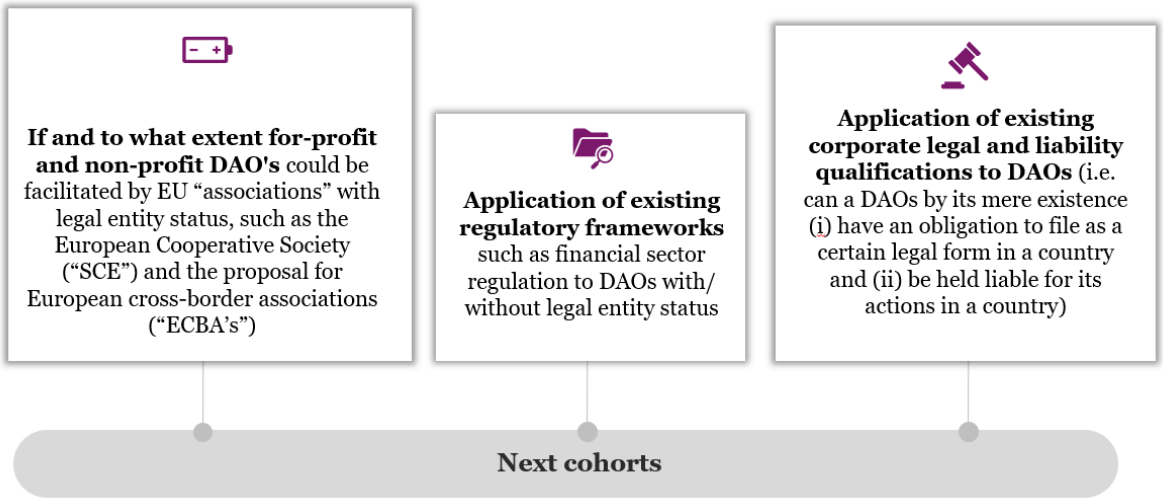
Areas for further analyses:

Given the increasing relevance of DAOs, not only in the EU but internationally, it is important to find a balance between centralized elements such as a physical address and a board/agent for external communication and decentralized governance. Further consultations would be welcome regarding:

- Registration requirements in the commercial register(s), including minimum registration requirements;
- UBO qualification and registration;
- DAO regulation initiatives in different countries, including various US States;
- Could the European Cooperative Society ("SCE")[51] and the proposal for European cross-border associations ("ECBAs")[52] become appropriate EU legal vehicles for respectively DAOs for profit and non-profit DAOs?

e. Areas for further clarification & dialogue topics for the next cohorts

Although the European Blockchain Sandbox is not the right forum for the additional consultations and research identified above, certain elements will likely become relevant topics for the dialogues in the upcoming cohorts.



[49] Regulation (EC) No. 1435/2003.
[50] Proposal of 5 September 2023 for a Directive on European cross-border associations (COM(2023) 516 final.
[51] Regulation (EC) No. 1435/2003.
[52] Proposal of 5 September 2023 for a Directive on European cross-border associations (COM(2023) 516 final.

6. Customs & DLT solutions

a. Introduction

The Union Customs Code (UCC) provides a comprehensive legal and harmonized framework for customs rules and procedures in the EU customs territory, nonetheless leaving room for individual Member States to implement the UCC-provisions into national legislation.

Concerns have been raised that the EU Customs Union is burdened by fragmented digitalisation, suboptimal coordination between national authorities and overall complexity, resulting in high administrative compliance costs for traders and opportunities for criminals to commit fraud. As a response to these concerns, on 17 May 2023 the European Commission put forward proposals for what it says is the most ambitious and comprehensive reform of the EU Customs Union.

One of the key elements of this reform is the establishment of an EU Customs Authority, which would oversee a new EU Customs Data Hub enabling businesses that want to bring non-EU goods into the EU to log all the information on their products and supply chains into a single online environment.

The idea behind the EU Customs Data Hub is bringing together data provided by businesses and providing customs authorities a bird's-eye view of the supply chains and the movement of goods. The use of blockchain is also being explored, as this could enable customs authorities to securely store and share critical information such as customs declarations, product information and shipment status, as well as simplify customs processes by providing a secure, transparent and efficient way to manage data.

Operational example from outside the EU:

- In Egypt a document based commercial blockchain solution was introduced by the Egyptian government in cooperation with CargoX a few years ago.[53] The solution is mandatory. It has reduced clearance times on average from 29 days down to 9 days.
- The example shows that blockchain can be used and if it is used it could result in significant efficiency in the customs clearance process.
- The mandatory solution in Egypt requires significant transaction fees to be paid by traders. In considering possible blockchain solutions, whether or not a financial contribution is appropriate would likely be part of the considerations.

b. Blockchain/DLT solutions under the existing EU Customs regulatory framework

Existing and proposed EU legislation in the customs area is technology neutral and does not preclude the use of blockchain applications for e.g. import and export declarations. However, it can be challenging to meet the current regulatory customs requirements through blockchain solutions as a result of e.g. formal requirements regarding data submission in the national customs legislations.

- According to Article 6(1) UCC all exchanges of information, such as declarations, applications or decisions, between customs authorities and between economic

[53] https://cargox.io/content-hub/blockchain-blockbuster-egyptian-government-cargox.

operators and customs authorities, and the storage of such information, as required under the customs legislation, shall be made using electronic data-processing techniques. Based on Article 6(2) UCC common data requirements shall be drawn up for the purpose of the exchange and storage of information referred to in paragraph 1. Pursuant to Article 8(1) (a) UCC the Commission shall specify, by means of implementing acts where necessary, the format and code of the common data requirements referred to in Article 6(2) UCC. Format and codes are specified in various Annexes (notably Annex B) to the Delegated Act to the UCC (Regulation (EU) 2015/2446).

Nevertheless, blockchain solutions could already be used in the customs area as an extra tool (an additional layer of trust) for instance for the verification of import or export declarations or in a broader sense for the interaction between private players and public authorities and in the data sharing between different public authorities in combination with the usual formal documentation, in particular in those areas and between entities where there could be trust issues.

Lessons learned

- Existing and proposed EU legislation in the customs area is technology neutral and does not preclude the use of blockchain applications for declarations such as for import or export.
- Although it can be challenging to meet the current mandatory regulatory customs requirements through blockchain solutions as a result of e.g. formal requirements regarding data submission in the national customs legislations, blockchain solutions can already be used in the customs area as an extra tool in particular in those areas where there could be trust issues and/or for efficiency reasons.

c. Examples of Blockchain/DLT solutions as an extra tool

Several interesting examples/best practices of Blockchain/DLT solutions as an **extra tool** were tested/discussed during the 1st cohort dialogues in particular in the areas of i) e-CMR & e-Export and ii) e-Import. These solutions will be described in more detail below.

Example 1: e-CMR and e-Export

Blockchain/DLT applications can already be used and are for instance applied in Italy to ease both communication between private entities and controls by public authorities. Solutions discussed during the dialogues related to three main situations in which blockchain technology is used:

- in the e-CMR module, the stakeholders involved are private parties and the document can be notarized on blockchain, including advanced electronic signatures.
- in the e-Export (Export Declaration) module, the stakeholders involved are private parties and authorities (Customs Agency) whereby the acceptance of the PoA (Power of Attorney) is notarized on blockchain before sending the Customs File to the Customs Authority
- the blockchain-based e-CMR can also be used for intermodal transport, for example to communicate with the port's PCS to send Advance Notice of Arrival of the goods, enabling automatic entry into the port area. In this case there is a hybrid approach, where the e-CMR is enriched with specific customs data (such as HS codes and MRN).

Moreover, in this case checks by Public Authorities on documents can already be performed via blockchain. Therefore, although today the blockchain is mostly used in interactions

performed by private players on the digital documents, the hashcode is already transferred to the authorities and can be used for verification by officials.

Example 2: e-CMR and e-Export

Another example that was discussed were efficiency gains that can be realized because e-CMR blockchain solutions commonly contain most of the data required for an export declaration even though the formal lodging of an export declaration on the basis of the existing customs legislation is still a separate formal requirement.

Today the e-CMR is already used by the market to manage shipments by road (mainly into the European territory). However, in for instance Italy the e-CMR has been used for allowing the entrance into the port area. The blockchain solution managed (in parallel) an electronic export declaration, retrieved the MRN and the HS codes, and thanks to all this info it was possible creating the Pre Arrival Notice with customs validity and sending it to the PCS (Port Community System). For the port, the mandatory pieces of info were the e-CMR and relevant customs information to enter the port area and the Export Declaration to exit the port area. Today, the e-CMR cannot replace the Customs file, but what it can do is simplify the creation of the customs file by sharing a large amount of shipment information (all secured and unaltered) easily and automatically without the need for printed paper. Among the benefits, this approach makes the upstream process robust and avoids manual errors.

It is important to consider that the technology might be used to merge information that is identical in the two types of documents (the e-CMR and the customs documentation.

Example 3: eFTI4EU

The 'Electronic Freight Transport Information for Europe' (eFTI4EU) is inspired by the EU Regulation 2020/1056 and financed under the 'Connecting Europe Facility' (CEF) programme of the European Commission. The aim is to create a standardised and interoperable approach at European level for the operation of eFTI gates, as well as to design and implement a harmonised architecture for the exchange of logistics and transport data. The project is not only prospective but brings concrete and upcoming actions. Reference is made to the following examples which are published on the RAM website: https://www.ramspa.it/node/1355/printable/print:

- By December 2024, an intermodal shipment (truck+train+ship) will be handled using blockchain-based e-CMR of the use case. The secure and traceable information contained in it will be automatically exchanged for the creation of the other waybills. Blockchain will also be useful for facilitating inspections by the competent authorities during the cargo's journey.
- By June 2025, the first shipment from Italy to another European country will be made using blockchain-based e-CMR. It will represent the first communication between the Italian e-FTI Gate and the foreign country e-FTI Gate.

eFTI4EU is an interesting opportunity for blockchain use cases and could become even more attractive from a customs regulatory perspective once customs legislation is also considered in this project (next to e-CMR).

Example 4: Import declarations

As mentioned above blockchain solutions could also be used in the customs area as an extra tool (an additional layer of trust) for instance for the verification of import declarations to reduce duty avoidance, identify prohibited/restricted goods or in a broader sense for the interaction between private players and public authorities and in the data sharing between

different public authorities in combination with the usual formal documentation, in particular in those areas and between entities where there could be trust issues.

Implementation of blockchain solutions as an extra tool, would likely be even more effective and efficient in the event of mutual recognition between the EU and third countries of such a solution and accreditation of parties that could provide the data via the DLT/blockchain applications for verification purposes.

A first step could be to start testing the application of blockchain for the verification of import declarations in a pilot environment to determine e.g.:

- Which data/documents should be provided through the blockchain. A basic set of data including country of origin, Harmonized System (HS)-code, value and quantity provided by the seller could already make an important difference.
- Would it add value to make the original documents or secure references accessible via blockchain such as to a bill of lading or an invoice?
- How to identify a true seller (seller accreditation).
- What would be the efficiency gains that could be achieved including possible reductions of clearance times. For instance, in Egypt[54] reduction in clearance times were reported as a result of the use of blockchain from 29 days down to 9 days.[55]
- The avoidance of false positives.
- Is there any impact on the technical processes of the customs authorities or can this be avoided? And could the efficiency gains still be realized without any change in the technical systems?
- What is the impact on the operational processes of the customs authorities? How will the information be presented to the customs authorities and who is making the operational decisions on the basis of the information. What would this mean in terms of efficiency?

In general, it is not 'the more data, the better', but 'the more trusted data, the better.' If there would be a system where there is a strong incentive for the seller to provide accurate data, meaning that accurate information would come in early in the supply chain process and would feed the risk management process, this could be interesting.

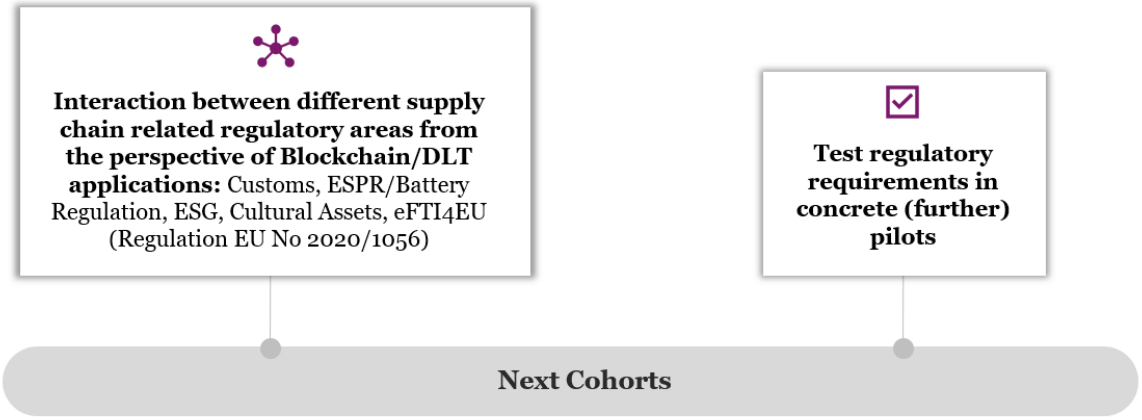
The starting point is that the responsibility for the accuracy of the declarations does not change. In sorting out possible liability questions as a result of incorrect data on the blockchain (and to prevent incorrect data on the blockchain as much as possible) it could be important that as part of the blockchain solution only the provider of the data is able to amend the data. The Blockchain allows to track the edits and history of changes.

54 https://cargox.io/content-hub/blockchain-blockbuster-egyptian-government-cargox.

55 In Egypt adopting this solution requires a mandatory financial contribution by traders. In considering possible blockchain solutions, whether or not a financial contribution is appropriate would likely be part of the considerations.

d. Areas for further clarification & dialogue topics for the next cohorts

Building on the dialogues in connection with the above examples one of the next cohorts could be used to test the regulatory requirements in concrete (further) pilots. In addition, the possibilities to increase regulatory effectiveness and efficiencies in the interaction between different supply chain related regulatory areas will likely become relevant for the next cohorts.



7. Battery Passports and DPPs

a. Introduction Battery Regulation and ESPR

On 17 August 2023, the new European Battery Regulation (EU 2023/1542)[56] entered into force. The regulation is part of the European Green Deal, which aims for the EU to become climate neutral by 2050. It establishes strict requirements regarding sustainability, performance, safety, labelling and information, collection and recycling of batteries. The regulation thereby governs the entire life cycle of batteries placed on the market in the EU, with the aim of strengthening a climate-friendly circular economy. Design and manufacturing of batteries should be geared towards optimising their performance, durability and safety and reducing their carbon footprint. In addition, the regulation aims to ensure that environmental and human rights due diligence requirements are complied with in the battery value chains.

The Battery Regulation introduces a mandatory digital battery passport. From 18 February 2027 each light means of transport (LMT) battery, each industrial battery with a capacity greater than 2 kWh and each electric vehicle battery placed on the market or put into service shall have an electronic record ('battery passport').[57]

On 27 May 2024, the Council of the EU approved the Ecodesign for Sustainable Products Regulation (ESPR)[58] which was the subject of an interinstitutional agreement on 5 December 2023 and had already been approved by the European Parliament on 23 April 2024. The ESPR is a framework regulation. Secondary legislation will determine the product groups and also the relevant levels (product, batch, category) for which the DPP requirement will become relevant including the applicable rules and requirements to be followed by DPP service providers. The EC will aim to conduct dialogues, consultations and studies with different stakeholders to identify best solutions in this regard. In determining the groups of products for which the DPP requirement will become relevant, the policy objectives of the DPP to simplify digital access to relevant product-specific information in the area of sustainability, circularity and legal compliance will be taken into account. In particular, durability and recyclability aspects will be carefully considered. The track and tracing functionality may also be included in the secondary legislation when appropriate. The product groups will be determined in the ESPR working plan that is expected withing 9 months after the entry into force of the ESPR and therefore during the first half of 2025. . The industry, as well as national administrations, will have 18 months, after the adoption of the relevant delegated acts, to adapt to the new the eco-design requirements. However, in some duly justified cases, the Commission can set an earlier date of application.

---

56 The Regulation can be accessed in full through the following hyperlink: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542.

57 Article 77(1) Battery Regulation.

58 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 final approval to the ESPR by the European Council (https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/green-transition-council-gives-its-final-approval-to-the-ecodesign-regulation/). The final Council text (Regulation of the European Parliament and of the Council of 16 May 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (PE-CONS 106/23)) is available through: https://data.consilium.europa.eu/doc/document/PE-106-2023-INIT/en/pdf.

The ESPR is a framework regulation.

- Secondary legislation will determine the product groups for which the DPP requirement will become relevant (and on which level – product, batch, category) including the applicable rules and requirements to be followed by DPP service providers taking into account the policy objectives of the DPP (sustainability, circularity and legal compliance).
- Track and tracing functionality may be included when appropriate.
- The product groups will be determined in the ESPR working plan that is expected withing 9 months after the entry into force of the ESPR and therefore in the first half of 2025.

b. Regulatory requirements regarding Battery Passports and DPPs

"Battery Passports" and "Digital Product Passports" ("DPPs") are defined terms in the Battery Regulation and the ESPR.[59]

Article 77(2) and Annex XIII to the Battery Regulation.	Article 2(28) ESPR	Article 2(32) ESPR
The 'battery passport' shall contain information relating to the battery model and information specific to the individual battery, including resulting from the use of the battery.	'digital **product passport'** means a set of data specific to a product that includes the information specified in the applicable delegated act adopted pursuant to Article 4 and that is accessible via electronic means through a data carrier in accordance with Chapter III.	**'a Digital Product Passport (DPP) service provider'** means a natural or legal person that is an independent third-party authorised by the economic operator which places the product on the market or puts it into service and that processes the digital product passport data for that product for the purpose of making such data available to economic operators and other relevant actors with a right to access those data under this Regulation or other Union law.

Specific requirements regarding Battery Passports and DPPs are laid down in chapter IX/Annex III of the Battery Regulation and Chapter III of the ESPR.

Battery Passports

The battery passport shall contain information relating to the battery model and information specific to the individual battery, including resulting from the use of the battery.[60] A battery passport shall cease to exist after the battery has been recycled.[61]

[59] References to the ESPR are based on the "final Council text" that was published in May 2024 (https://www.parlament.gv.at/dokument/XXVII/EU/184943/imfname_11374156.pdf). The (numbering in the) final version to be published in the Official Journal might deviate although no substantial changes are to be expected.

[60] Article 77(2) and Annex XIII to the Battery Regulation.

[61] Article 77(8) Battery Regulation.

The information in the battery passport shall be accessible to different categories of stakeholders distinguishing between a) information accessible to the general public, b) information accessible only to notified bodies, market surveillance authorities and the EC and c) information accessible only to any natural or legal person with a legitimate interest in accessing and processing that information as specified in the Battery Regulation and in the implementing acts which shall be adopted by the EC by 18 August 2026 specifying whichpersons are to be considered persons with a legitimate interest.[62]

The battery passport shall be accessible through a QR code referred which links to a unique identifier. The QR code and the unique identifier shall comply with the ISO/IEC standards 15459-1:2014, 15459-2:2015, 15459-3:2014, 15459-4:2014, 15459-5:2014 and 15459-6:2014 or their equivalent which can be amended or supplemented by the EC by delegated acts in light of technical and scientific progress.[63]

All information included in the battery passport shall be based on open standards and be in an interoperable format, transferable through an open interoperable data exchange network without vendor lock-in, machine-readable, structured and searchable, in accordance with essential requirements regarding the technical design and operation of the battery passport.[64] These essential requirements relate to:

a) interoperability with other digital product passports required by EU law,
b) free of charge differentiated access rights,
c) storage of data in the battery passport,
d) prohibition of reselling, re-using or processing mandatory data in the product passport by operators that are authorised to act on behalf of the responsible economic operator that is placing the battery on the market,
e) continued availability of the battery passport after the responsible economic operator ceases to exist of ceases its activity in the EU,
f) limitation of the rights to access, introduce, modify or update information in the battery passport,
g) ensuring data authentication, reliability and integrity and
h) ensuring a high level of security and privacy and avoidance of fraud.

Digital Product Passports

The ESPR provides general requirements for digital product passports covering similar topics as the Battery Regulation which can be activated and tailored towards specific product categories in delegated acts,[65] e.g.:

- The DPP must be connected to a data carrier to a unique product identifier and the data carrier shall be physically present on the product, its packaging or on documentation accompanying the product. These requirements will be specified in the applicable delegated acts.[66]
- Consumers, economic operators and other relevant actors shall have free access to the product passport based on their respective access rights which will be specified in the applicable delegated acts.[67]
- Essential requirements relating to the technical design and operation of the DPP covering similar categories of essential requirements as the Battery Regulation such as interoperability, free of charge access rights, storage of data, restrictions

62 Article 77(2), Annex XIII and Article 77(9) Battery Regulation.
63 Article 77(3) Battery Regulation.
64 Article 77(5) in conjunction with Article 78 Battery Regulation.
65 Articles 9 and 10 ESPR.
66 Article 8 and 9 ESPR in conjunction with Article 4 ESPR.
67 Articles 8, 9(1) and 10 ESPR.

regarding reselling/re-use of data, continued availability of the DPP, limitation of the rights to access, introduce, modify or update information in the battery passport, ensuring data authentication, reliability and integrity and a high level of security/privacy/avoidance of fraud.[68]

c. Blockchain/DLT solutions for Battery Passports and DPPs under the Battery Regulation and the ESPR

Several interesting Blockchain/DLT solutions for Battery Passports/DPPs were tested/discussed during the 1st cohort dialogues from a regulatory perspective including the potential of blockchain/DLT-solutions that support effective and efficient compliance with the Battery Regulation and the ESPR.

The Battery Regulation and the ESPR are based on the principle of technology neutrality. Further clarification and guidance to reflect this principle will be given through the standards and secondary legislation regarding compliance with the Battery Regulation and ESPR requirements in relation to DLT applications.

The degree of information required on DPPs (static or dynamic) will depend on the product group and will be further defined in secondary legislation. An important point that will further be considered is the usefulness of dynamic information required on DPPs for the purpose of circularity. According to the Battery Regulation, certain categories of dynamic information will have to be part of the battery passports (Articles 14(1) and 45(2) and Annex VII).

Blockchain solutions can be helpful to comply with due diligence obligations as laid down in Chapter VII of the Battery Regulation. The ESPR does not include due diligence provisions.

Regulatory requirements in the Battery Regulation and the ESPR leave room for additional content/functionality as long as minimum requirements are met. The Battery regulation and ESPR do not include restrictions regarding the recording of additional/non-mandatory information, the use of such information and access rights.

Compliance with other regulatory instruments like the GDPR, the AI Act, the Data Act, the Data Governance Act and NIS2 is relevant for the recording of data in Battery passports/DPPs and the use of and access rights to such data (mandatory and additional). These other regulatory instruments can also be particularly relevant if other technologies such as AI and IoT data analyses are used to monitor/verify the correctness of the data that is recorded on the blockchain.

[68] Article 10 ESPR.

Blockchain/DLT solutions for Battery Passports and DPPs

- Several interesting Blockchain/DLT solutions for Battery Passports/DPPs were presented/discussed during the 1st cohort dialogues including the potential of blockchain/DLT-solutions that support effective and efficient compliance.
- Existing and proposed EU legislation for Battery Passports and Digital Product Passports is **technology neutral** and does not preclude the use of Blockchain/DLT applications.
- Blockchain/DLT solutions will need to facilitate **different access regimes for different stakeholders**: interested parties, authorities/notified bodies and the general public.
- The Battery Regulation and the ESPR provide **"minimum requirements"** and do not include restrictions regarding the recording of additional/non-mandatory information, the use of such information and access rights. Exceeding the minimum requirements (such as for instance the QR code as a minimum requirement in the Battery Regulation) should not be a problem from a Battery passport/DPP regulatory perspective and subject to compliance with other regulations.
- **Compliance with other regulatory instruments** like the AI Act, the Data Act, the Data Governance Act, eIDAS 2, the GDPR and NIS2 is relevant for recording of data in Battery passports/DPPs and the use of and access rights to such data (mandatory and additional). This could be particularly relevant if other technologies such as AI and IoT data analyses are used to monitor/verify the correctness of the data that is recorded on the blockchain.

d. Elements of relevance for secondary legislation

Several elements of relevance were mentioned during the dialogues for the secondary legislation, including e.g.:

a) Product identification levels: The question if product passports should be established on an individual product level or if a passport per batch or stock-keeping unit (SKU) might suffice can be addressed in secondary legislation. For circularity use cases (R strategies – reuse, repair, resell, etc) unique identifiers on a product level can be an elemental enabler and therefore a preferable option for manufacturers and brands (such as furniture, fashion, and electronics).

b) Unique identifiers: Regarding how unique identifiers should be designed, the EC standardization mandate (see below) to the CEN (European Committee for Standardization), the CENELEC (European Committee for Electrotechnical Standardization) and and the European Telecommunications Standards Institute will provide direction. The aim is to be technology neutral while also considering what's in the market.

c) Data carriers: different types of data carriers may be allowed (QR, NFC, RFID, etc.) depending on the product category. Durability and recyclability aspects should be carefully considered.

- The Battery Regulation suggests the QR code as a "minimum requirement". Going beyond this requirement should not be a problem from a regulatory perspective and subject to compliance with other regulations. Preferably the regulation should be flexible in order to support industry innovations.

d) Interoperability & Standards: Standards regarding e.g. technical, semantic and format aspects are welcome to enhance early implementation/adoption of DPPs

and interoperability. Interoperability requirements are needed to ensure that data can be seamlessly accessed through all the value chain.

e) Data access: data search functions should be designed in a way where all parties should get access to data in an interoperable and easy manner, without always asking for “economic operator” (EO) permission. It is important to have a search function to access data through a blockchain or via a web portal, however IP-protected data may not be available to all access seekers

- EC will define which type of data should be made available and be interoperable via delegated acts. See also Art. 12a ESPR regarding the EC web portal for data search functions.

f) Responsible actor(s) for regulatory purposes: The Battery Regulation refers to the “economic operator” as the responsible actor to make sure there is a point of contact for regulatory purposes. In principle similar observations apply for the ESPR where the "economic operator" (EO) could be seen as responsible actor for data storage on the DPP, but responsibility can be given to the DPP service provider via contractual means. Art. 8(2)(g) ESPR provides room for flexibility and designation of other/additional actors.

g) Flexible legislation: Secondary legislation aims to define minimum requirements and can adapt/be flexible to industry needs and suggestions. Therefore, it’s important to contribute to the legislative process and to inform policy makers of all available alternatives.

h) Energy consumption: It is important to keep track of environmental footprint & energy consumption aspects when using blockchain/DLT solutions in specific use cases.

i) Regulatory compliance: The possibility of blockchain/DLT solutions to enhance effective/efficient compliance, monitoring and supervision of specific regulatory requirements for both companies and regulators/authorites can be explored in more detail as part of the development of secondary legislation and in the next cohort dialogues for the European Blockchain Sandbox.

Important information about the status of secondary legislation and ongoing/upcoming consultations, as well as information on how interested parties can provide their views is made available on:

- DG Environment news page – available here.
- EC website “Have your say - Public Consultations and Feedback” – available here.
- CIRPASS – latest news page – available here.

Information on how interested parties can be kept updated about events and expert sessions is made available on:

- DG Environment news page – available here.
- ESPR page – available here.
- CIRPASS – latest news page – available here.

e. Standards are of key importance

Standards play a crucial role for developing Battery Passport / DPP solutions and defining e.g. the technical, semantic and formatting aspects of mandatory DPP data. These standards are expected to impact also non-mandatory data and their applications. It is important that they do not unnecessarily limit EU innovation and economic development and support the principle of technology neutrality also between different Blockchain/DLT technologies.

On the one hand it is important that standards become available in time and provide enough certainty to enhance investments and market adoption and on the other hand too much detail that could hamper new developments and solutions has to be avoided. The Battery Regulation and the ESPR provide flexibility by referring not only to ISO/IEC standards 15459 but also to equivalent standards (art. 77(3) Battery Regulation) or by referring to ISO/IEC standards 15459 as an example not excluding other standards (Art. 9(1)(c) ESPR). In addition, the EC is empowered to adopt delegated acts in view of technical and scientific progress (Art. 77(2 & 3) Battery Regulation).

Implementation of standards: the development of standards has already been mandated by the EC and input can be provided to bodies working on such standards (CEN/CENELEC, ETSI and national standardization bodies). Standards have to be developed by the end of 2025.

- According to the draft EC mandate eight new areas of harmonised standards to be drafted to support the implementation of the proposed DPP-system have been identified. In particular: a) Unique identifiers b) Data carriers and links between physical product and digital representation c) Access rights management, information security, and business confidentiality d) Interoperability (technical, semantic, organisation) e) Data processing, data exchange protocols, and data formats f) Data storage, archiving, and data persistence g) Data authentication, reliability, integrity h) APIs for the DPP lifecycle management and searchability.

Following the approval of the draft EC mandate by the Committee on Standards (Comitology Committee, composed of Member States Experts) on 1 April 2024, the draft is now expected to be published on this website as a final text. The draft is a Commission Implementing Decision requesting CEN, CENELEC and ETSI to draft new European standards in support of EU policy on ecodesign requirements for sustainable products and on batteries and waste batteries, including on DPPs, by 31 December 2025

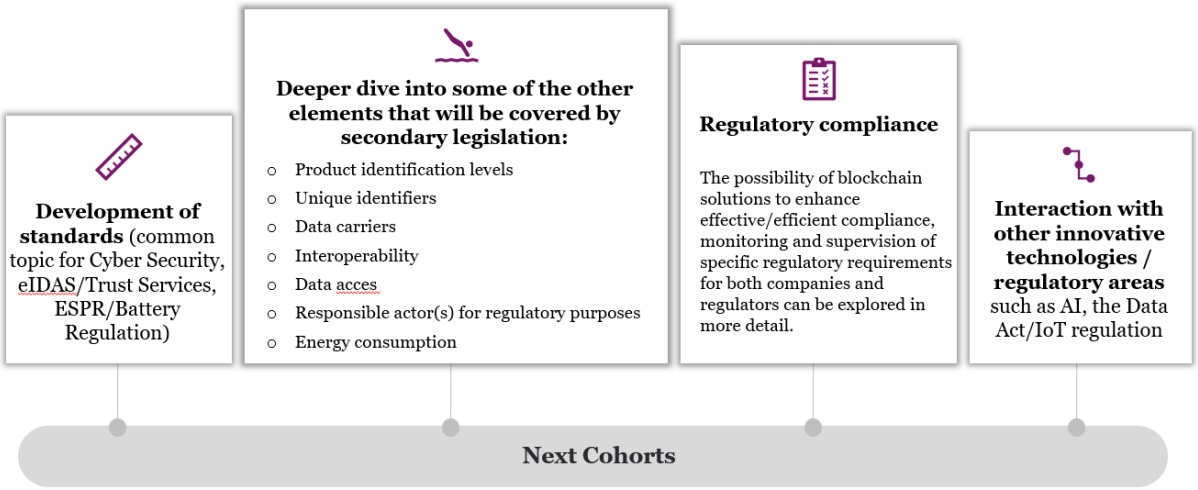
Guidance on how and when interested actors can intervene to collaborate in the standards development process can be found on the following website: Standardisation and SMEs - European Commission (europa.eu).

Implementation of standards:

- Standards have been mandated already by the EC and input can be provided to bodies working on such standards (CEN/CENELEC, ETSIand national standardization bodies), which should be ready by the end of 2025.
  - Draft EC Decision requesting CEN, CENELEC and ETSI to draft new European standards in support of the EU policy on ecodesign requirements for sustainable products and on batteries and waste batteries, including on DPPs, by 31 December 2025.
  - Eight new areas of harmonised standards to be drafted to support the implementation of the proposed DPP-system. In particular: a) Unique identifiers b) Data carriers and links between physical product and digital representation c) Access rights management, information security, and business confidentiality d) Interoperability (technical, semantic, organisation) e) Data processing, data exchange protocols, and data formats f) Data storage, archiving, and data persistence g) Data authentication, reliability, integrity h) APIs for the DPP lifecycle management and searchability.

f. Areas for further clarification & dialogue topics for the next cohorts

The Battery Regulation and the ESPR are to a large extent new regulatory instruments. The 1st cohort dialogues showed the potential of blockchain/DLT solutions for Battery Passports and DPPs and formed the basis for deeper dives and additional regulatory topics which can be discussed in the dialogues for the next cohorts.



8. Blockchain/DLT solutions for the prevention of trafficking of cultural assets

a. Introduction – Existing international and EU legal framework

According to the UNESCO Conventions, including the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970) (**"UNESCO Convention 1970"**) it is a collective duty of the State Parties to act against the illicit trafficking of cultural property and to protect cultural heritage.[69]

In accordance with the UNESCO Convention 1970, the State Parties are bound to set up within their territories one or more national services for the protection of the cultural heritage, e.g. establishing and keeping up to date, on the basis of a national inventory of protected property, a list of important public and private cultural property whose export would constitute an appreciable impoverishment of the national cultural heritage.[70] In addition the State Parties have undertaken to introduce an appropriate certificate in which the exporting State would specify that the export of the cultural property in question is authorized. The certificate should accompany all items of cultural property exported in accordance with the regulations and export of cultural property without a said certificate is prohibited.[71] In addition, the State Parties shall take all appropriate measures to prohibit and prevent the illicit import, export and transfer of ownership of cultural property in their territories[72] and have undertaken to e.g. ensure that their competent services co-operate in facilitating the earliest possible restitution of illicitly exported cultural property to its rightful owner.[73]

The UNESCO Conventions mention inventories of assets, but do not specify the support/technologies underpinning them. In accordance with the UNESCO Conventions, State Parties have adopted national legislation and have established national registries. However, the measures that are taken on a national level are currently not harmonized.

EU Customs legislation refers to the development of a centralized electronic system that allows national authorities to record certificates of products with a reference to the object ID standard recommended by UNESCO.[74] It is assumed that the reference to a centralized electronic system does not preclude the use of blockchain/DLT.

- Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0880
- Implementing Regulation (EU) 2021/1079 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1079)

Softlaw and EU legislation is established on an EU level addressing trafficking in Cultural Goods including:

---

69 The World Heritage Convention (1972) link; The Convention for the Safeguarding of the Intangible Cultural Heritage (2003) link; The Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970) (link); The Convention on the Protection and Promotion of the Diversity of Cultural Expressions (2005) link; The Convention for the Protection of Cultural Property in the Event of Armed Conflict (1954) and its two Protocols (link).

70 Article 5 UNESCO Convention (1970).

71 Article 6 UNESCO Convention (1970).

72 Article 12 UNESCO Convention (1970).

73 Article 13(b) UNESC Convention (1970).

74 (EU) 2019/880, preamble 15.

- EU Action Plan against Trafficking in Cultural Goods (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13352-Trafficking-in-cultural-goods-EU-action-plan_en)
- Commission Recommendation (EU) 2021/1970 of 10 November 2021 on a common European data space for cultural heritage (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021H1970)
- Ex–ante impact assessment Report on a European collaborative cloud for cultural heritage, completed in March 2022 (https://op.europa.eu/en/publication-detail/-/publication/90f1ee85-ca88-11ec-b6f4-01aa75ed71a1/language-en)
- Directive 2014/60/EU of the European Parliament and of the Council of of 15 May 2014 on the return of cultural objects unlawfully removed from the territory of a Member State and amending Regulation (EU) No 1024/2012 (Recast) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0060

Blockchain and other advanced technologies are mentioned in the aforementioned Commission Recommendation (EU) 2021/1970 among the technologies which can be explored for automatically identifying cultural goods that are illicitly trafficked and to ensure a more efficient process of digitisation, digital preservation and higher quality access, use and reuse. In particular:

- (8) [..] Artificial intelligence, **blockchain** and other advanced technologies can also be explored for **automatically identifying cultural goods that are illicitly trafficked**. The uptake of such advanced technologies has a significant impact on European recovery and growth following the COVID-19 pandemic, and Member States should support it by taking appropriate measures.
- 5. The national strategy should contain measures to support the cultural heritage institutions in taking up advanced technologies, such as 3D, artificial intelligence, extended reality, cloud computing, data technologies **and blockchain**, to ensure a more efficient process of digitisation and digital preservation and a higher quality content for a wider access, use and reuse.

Blockchain technology is also mentioned in the ex–ante impact assessment Report on a European collaborative cloud for cultural heritage (link) as a possible technology to log the access and use of data and for the protection of data sources.[75]

DG HOME has commissioned a Study on measures to increase traceability of cultural goods in the fight against cultural goods trafficking at EU Member State level and at EU level.[76] The current use of DLT/Blockchain solutions is explored as part of this study.[77]

[75] Ex-ante impact assessment report, pages 10, 38, 85 and 91.
[76] Stakeholders at international and national level are currently being consulted, and in particular International organisations/EU Commission, National authorities, Representatives of the art market and other stakeholders (i.e. Academia, research, NGOs).
[77] Stakeholders at international and national level are currently being consulted, and in particular International organisations/EU Commission, National authorities, Representatives of the art market and other stakeholders (i.e. Academia, Research, NGOs).

UNESCO Conventions and EU regulatory framework:

- According to the UNESCO Conventions, including the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970) ("UNESCO Convention 1970") it is a collective duty of the State Parties to act against the illicit trafficking of cultural property and to protect cultural heritage.
- The UNESCO Conventions mention inventories of assets, but do not specify the support/technologies underpinning them. In accordance with the UNESCO Conventions State Parties have adopted national legislation and have established national registries. However, the measures that are taken on a national level are currently not harmonized.
- DLT/Blockchain solutions are explored as part of the Study on measures to increase traceability of cultural goods in the fight against cultural goods trafficking that commissioned by DG HOME.

b. How could a DLT cultural passport and EU legislation support effectiveness and efficiency of regulation and oversight in this area?

One of the use cases with a focus on cultural asset passports formed the basis for a dialogue to discuss compliance with the international obligations laid down in the UNESCO Conventions against the prevention of trafficking of cultural assets and the potential of blockchain/DLT-solutions to support effective and efficient regulation and oversight in this area.

The introduction of a digital cultural asset passport using blockchain was discussed as a potentially important tool to prevent trafficking in cultural goods also from a global perspective.

Inspiration could be drawn from the regulation of digital product passports in the ESPR.[78] Key characteristics underlying the regulation of digital product passports that could be supported by blockchain/DLT solutions to enhance traceability of cultural goods and effectiveness and efficiency of regulation against trafficking of cultural goods include the recording of static and dynamic data, standardisation, interoperability and accessibility for different groups of stakeholders such as authorities (including the competent national authorities, musea and archeological sites and the general public).

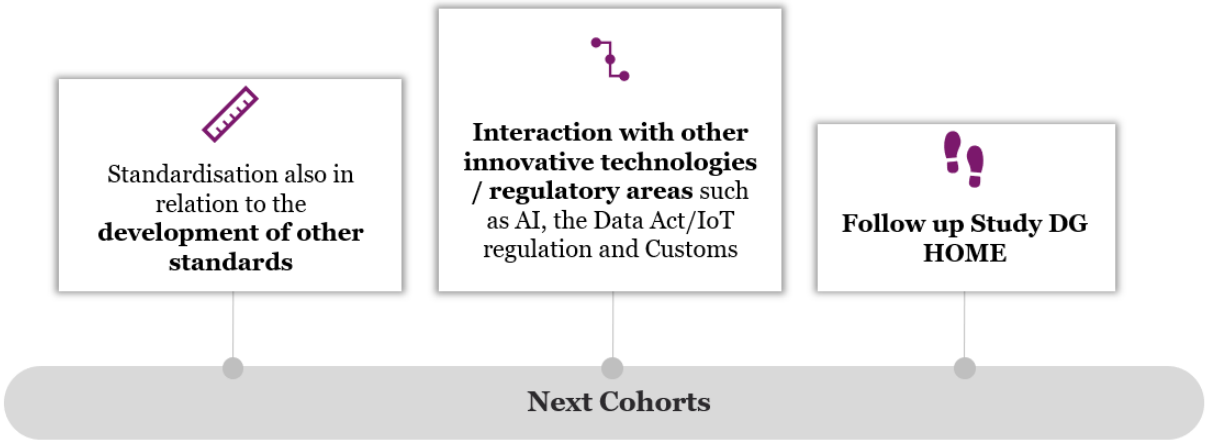
[78] Proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products (COM/2022/142 final) and final approval to the ESPR by the European Council (https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/green-transition-council-gives-its-final-approval-to-the-ecodesign-regulation/). The final Council text (Regulation of the European Parliament and of the Council of 16 May 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (PE-CONS 106/23)) is available through: https://data.consilium.europa.eu/doc/document/PE-106-2023-INIT/en/pdf.

Blockchain/DLT solutions for Cultural Asset Passports

- The introduction of a digital cultural asset passport using blockchain technology was discussed as a possible important tool in a harmonized approach against trafficking in cultural goods also from a global perspective.
- Inspiration could be drawn from the regulation of Digital Product Passports in the ESPR and blockchain/DLT solutions to enhance traceability of cultural goods and effectiveness and efficiency of regulation against trafficking of cultural goods.

c. Areas for further clarification & dialogue topics for the next cohorts

The Study by DG HOME could lead to relevant follow up areas. In addition, the potential of digital cultural asset passports making use of blockchain technology could be further explored in the next cohorts with similar additional focus areas as in relation to DPPs and Battery Passports: development of standards and interaction with other innovative technologies/regulatory areas such as AI, the Data Act/IoT and Customs.



9. Blockchain/DLT solutions for EU ETS / MRV reporting

a. Introduction – Existing EU legal framework

The European Union Emissions Trading Scheme (EU ETS) was introduced in the EU by 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. This ETS caps the emissions of specified pollutants over an area and allows companies to trade emissions rights within that area. The area in this case is the European Union plus Iceland, Norway, Liechtenstein and in certain cases also Switzerland and the United Kingdom. The scope of the EU ETS Directive was most recently extended to maritime transport by Directive (EU) 2023/959 of 10 May 2023.

In addition to this limitation in trading of greenhouse gas emission, the entities involved must also monitor and report their emissions of greenhouse gases. The annual procedure for monitoring, reporting and verifying (MRV), together with all the associated processes, is known as the ETS compliance cycle. Every year, operators must submit an emissions report. The data for a given year must be verified by an accredited verifier by 31 March of the following year. Once verified, operators must surrender the equivalent number of allowances by 30 April of that year. The rules related to the compliance cycle are set out in two regulations:

- Monitoring and Reporting Regulation (MRR) (Commission Implementing Regulation (EU) 2018/2066); and
- Accreditation and Verification Regulation (AVR) (Commission Implementing Regulation (EU) 2018/2067).

Specific regulations apply to the maritime sector: the MRV Maritime Regulation (EU) 2015/757 on the monitoring, reporting and verification of carbon dioxide emissions from maritime transport, and amending Directive 2009/16/EC. This Regulation was most recently amended by:

- Regulation 2023/957 of 10 May 2023 amending Regulation (EU) 2015/757 in order to provide for the inclusion of maritime transport activities in the EU Emissions Trading System and for the monitoring, reporting and verification of emissions of additional greenhouse gases and emissions from additional ship types (hyperlink), and
- Commission Delegated Regulation (EU) 2023/2776 of 12 October 2023 amending Regulation (EU) 2015/757 of the European Parliament and of the Council as regards the rules for monitoring greenhouse gas emissions and other relevant information from maritime transport (hyperlink).

Furthermore, there is the Commission Delegated Regulation (EU) 2023/2917 of 20 October 2023 on the verification activities, accreditation of verifiers and approval of monitoring plans by administering authorities pursuant to Regulation (EU) 2015/757 of the European Parliament and of the Council on the monitoring, reporting and verification of greenhouse gas emissions from maritime transport, and repealing Commission Delegated Regulation (EU) 2016/2072. Finally, ISO 14065:2020 contains general principles and requirements for bodies validating and verifying environmental information referred to in Article 42(2) of EC Delegated Regulation (EU) 2023/2917 (Procedures for verification activities).

b. Blockchain/DLT solutions for EU ETS / MRV reporting

The use of blockchain/DLT for the purposes of EU ETS/MRV reporting purposes was another interesting application that was discussed during the 1st round of dialogues.

Existing EU legislation in the area of the monitoring, reporting and verification of CO2 emissions from maritime transport is technology neutral and does not preclude the use of blockchain applications for *statutory* reporting purposes.

A study on the potential of blockchain technology in facilitating EU climate policy implementation was conducted on behalf of the European Commission's Directorate General for Climate Action setting out how certain key climate EU policy challenges could potentially be addressed by blockchain solutions and the pros and cons of the introduction of blockchain to EU climate policies including the EU ETS and the MRV regulatory areas.[79]

Apart from the annual statutory reporting obligation, blockchain could potentially be used as an *extra* tool for verifiers and competent authorities against fraud and to detect mistakes at an early stage (an additional layer of trust). Integrity of reported data is of key importance and more frequent reporting and transparency for verifiers/regulators through a blockchain solution could help to ensure correct reporting.

A combination of blockchain with IoT applications with a focus on data quality could make the solution even more interesting.

The verification of the data on the basis of the EU ETS/MRV regulations is the task of the verifier. If the blockchain solution works for the verifier the tool could also be a welcome addition for the regulators.

A first step could be to test the extra tool in a pilot environment to determine e.g.:

- Impact of the extra tool on data integrity/data quality;
- Appropriate frequency, content and presentation of additional data provided by the extra tool;
- Possible impact on the technical and operational processes for the competent authorities and how could this be avoided?

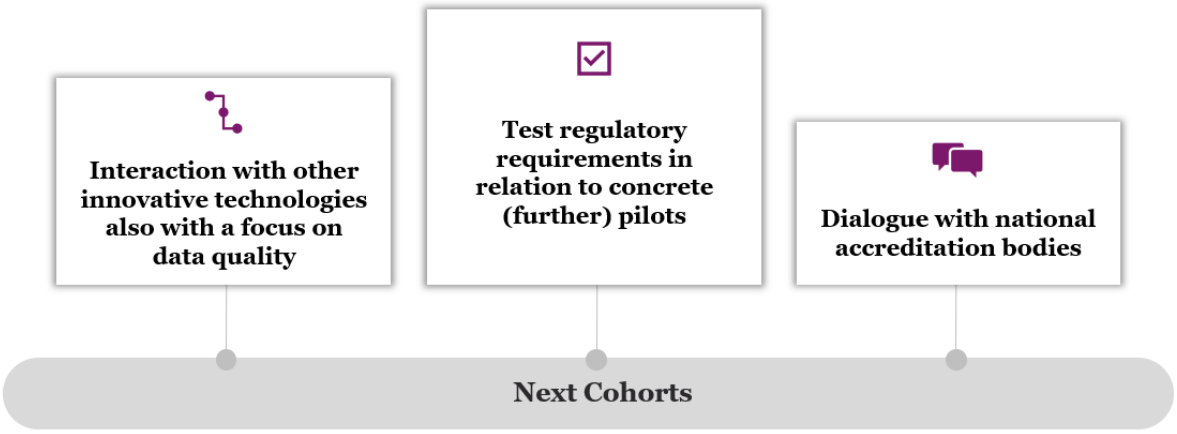
[79] Study on the potential of blockchain technology and other digital tools in facilitating EU climate policy implementation, published in December 2023 (Study on the potential of blockchain technology and other digital tools in facilitating EU climate policy implementation - Publications Office of the EU (europa.eu))

Blockchain/DLT solutions for EU ETS/MRV reporting:

- Existing EU legislation in the area of the monitoring, reporting and verification of CO2 emissions from maritime transport is technology-neutral and does not preclude the use of blockchain applications for statutory reporting purposes.
- A study on the potential of blockchain technology in facilitating EU climate policy implementation was conducted on behalf of the European Commission's Directorate General for Climate Action setting out how certain key climate EU policy challenges could potentially be addressed by blockchain solutions and the pros and cons of the introduction of blockchain to EU climate policies including the EU ETS and the MRV regulatory areas. [80]
- Apart from the annual statutory reporting obligation, blockchain could potentially be used as an extra **tool** for verifiers and competent authorities against fraud and to detect mistakes at an early stage (an additional layer of trust). Integrity of reported data is of key importance and more frequent reporting and transparency for verifiers/regulators through a blockchain solution could help to ensure correct reporting.
- A combination of blockchain with e.g. IoT applications with a focus on data quality could make such solutions even more interesting.

c. Areas for further clarification & dialogue topics for the next cohorts

Building on the results of the 1st round of dialogues various regulatory areas/topics were identified for the next cohorts including the interaction with other innovative technologies also with a focus on data quality and the testing of regulatory requirements in relation to concrete (further) pilots). In addition, a dialogue with national accreditation bodies could be relevant.



[80] Study on the potential of blockchain technology and other digital tools in facilitating EU climate policy implementation, published in December 2023 (Study on the potential of blockchain technology and other digital tools in facilitating EU climate policy implementation - Publications Office of the EU (europa.eu)).

10. Blockchain/DLT solutions – Data collection & sharing under the Data Governance Act

a. Introduction – Data Governance Act

The Data Governance Act (DGA) enhances the re-use of public-sector data (Chapter II), creates a regulatory framework for Data Intermediation Services (Chapter III) and encourages data altruism for the common good through Data Altruism Organisations (Chapter IV). The DGA applies from 24 September 2023.

The Data Governance Act (**"DGA"**) is in particular relevant for Blockchain/DLT use cases that qualify as Data Altruism Organisation (voluntary regime) or as Data Intermediation Services (mandatory regulatory obligations) in the sense of the DGA.

- It should be noted that in the context of the DGA the abbreviation "DAO" is not used to refer to a Decentralised Autonomous Organisation[81], but to a Data Altruism Organisation.

The DGA applies to both personal and non-personal data. EU and national law on the protection of personal data and enforcement by data protection authorities take priority over the DGA in relation to the protection of personal data. The DGA does not create a legal basis for the processing of personal data nor does it affect any of the rights and obligations set out in the GDPR/EUI DPR, the ePrivacy Directive (2002/58/EC) or the data protection law enforcement directive ((EU) 2016/680).

The DGA does not explicitly refer to the use of blockchain/DLT technology but blockchain/DLT applications are certainly not excluded from the scope of the DGA.

Re-use of certain categories of protected data held by public sector bodies

The DGA facilitates data-sharing of certain categories of public-sector data such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data. Chapter II applies to data held by public sector bodies[82], but excluding educational establishments.[83] Chapter II of the DGA includes a prohibition of exclusive arrangements, conditions for re-use of the defined categories of protected data, charging of fees, assistance by competent bodies to the public sector bodies with respect to granting or refusing access for re-use of such data, availability of a single information point in the Member States and a procedure for requests for re-use.

Regulation of Data Intermediation Services

The DGA introduces a mandatory regulatory framework for Data Intermediation Services in Chapter III. The regulatory obligations and compliance requirements for Data Intermediation Services do not apply to recognized Data Altruism Organisations (see below) or other not-for-profit entities insofar as their activities consist of seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism unless those organisations and entities aim to establish commercial relationships between an undetermined number of data subjects and data holders on the one hand and data users on the other.

---

81 See Section 5 of this report.
82 See definitions of 'public sector body' and ''bodies governed by public law' in Article 2(17) and 2(18) DGA.
83 Article 3 (1 & 2) DGA.

Regulatory obligations for Data Intermediation Services include a mandatory notification obligation to the competent authority for intermediation services in the Member State in which it has its main establishment[84] and the obligation to comply with the conditions for providing Data Intermediation Services laid down in the DGA[85] regarding e.g. the use of the data, tying with other services, a prohibition of restrictive format provisions, the obligation to apply fair/transparent/non-discriminatory access procedures and conditions, interoperability obligations, information obligations in the event of unauthorized transfer, transparency obligations regarding intended data uses by data users and the obligation to maintain a log record of the data intermediation activity.

Data Altruism Organisations

Data altruism organisations are organisations that collect and share data for objectives of general interest as provided for in national law without seeking or receiving a reward that goes beyond compensation related to the incurred costs. Such data altruism organisations may apply to be listed in a national register of recognized data altruism organisations on a voluntary basis in which case the provisions of Chapter IV of the DGA are applicable.

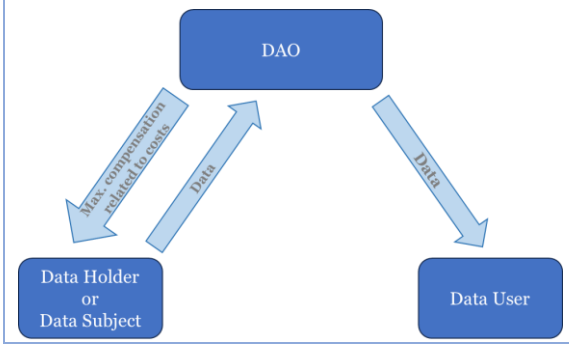
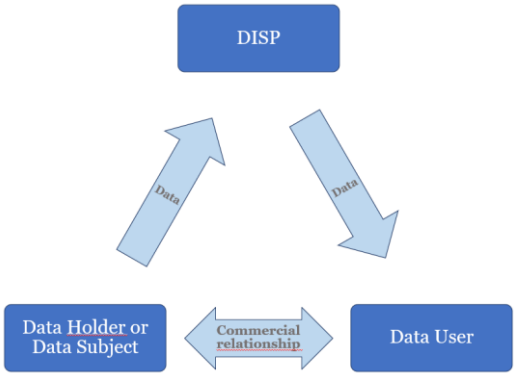
Data altruism organisation may submit an application for registration in the public national register of recognized data altruism organisations to the competent authority for the registration of data altruism organisations in the Member State in which it has its main establishment.[86]

Regulatory requirements include transparency requirements including accurate record keeping and the obligation to submit an annual activity report to the competent authority[87] and specific requirements to safeguard rights and interests of data subjects and data holders with regard to their data.[88]

b. Blockchain/DLT solutions that qualify as Data Intermediation Services and Data Altruism Organisations – Best practices and lessons learned

The Data Governance Act is in particular relevant for use cases that qualify as Data Altruism Organisation (voluntary regime) or as Data Intermediation Services (mandatory regulatory obligations).

84 Article 11 DGA.
85 Article 12 DGA.
86 Article 19 DGA.
87 Article 20 DGA.
88 Article 21 DGA.

Data Altruism Organisation	Data Intermediation Service
Is involved in the voluntary sharing of data on the basis of the consent of data subjects/data holders on a non-profit basis	Aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects/data holders and data users.
For objectives of general interest as provided for in national law which needs to be part of the statutory aim	Establishing commercial relationships; no limitation to objectives of general interest
Voluntary registration; requirements applicable in the event of registration	Mandatory notification and mandatory requirements
Legal entity required (Art. 18(b) DGA)	Legal entity required (Art. 12(a) DGA)
Data Altruism activities functionally separated (Art. 18(d) DGA)	Data Intermediation Service provided through a separate legal person (Art. 12(a) DGA)
Inclusion in public registers for Data Altruism Organizations held by the national competent authority and the European Commission; use of label DAO recognized in the Union (upon being listed in national public registry) and use common logo	Inclusion in public register for DISP held by the European Commission based on the information provided by the national competent authority ; use of label DISP recognized in the Union (if recognized upon request) and use of common logo
Requirements in Articles 18 – 22 DGA	Requirements in Articles 11 & 12 DGA
Simplified overview of data and compensation of costs flows for a Data Altruism Organization ("DAO"): 	Simplified overview of data and compensation flows for a Data Intermediary Service Provider ("DISP"): 

The qualification "Data Altruism Organisation" or "Data Intermediation Service" are mutually exclusive (Art. 15 DGA). Registered Data Altruism Organisations and Data Intermediation Services could also be data holders but the roles should be kept separated (functionally separated for Data Altruism Organisations and provisionally through a separate legal entity for Data Intermediation Services).

Use cases operating DLT/blockchain technology to offer services in scope of the DGA, should identify which stakeholder offers the Data Altruism or the Data Intermediation Services and the interplay with smart contracts.

The role of smart contracts and how these are used for the collection, notarisation and sharing of data as well as which stakeholder has developed and deploys these smart contracts could be relevant to identify the relevant party/parties under the DGA.

The regulation of smart contracts in the Data Act could become relevant for the compliance with the requirements of the DGA for Data Altruism Organisations and Data Intermediation Services.

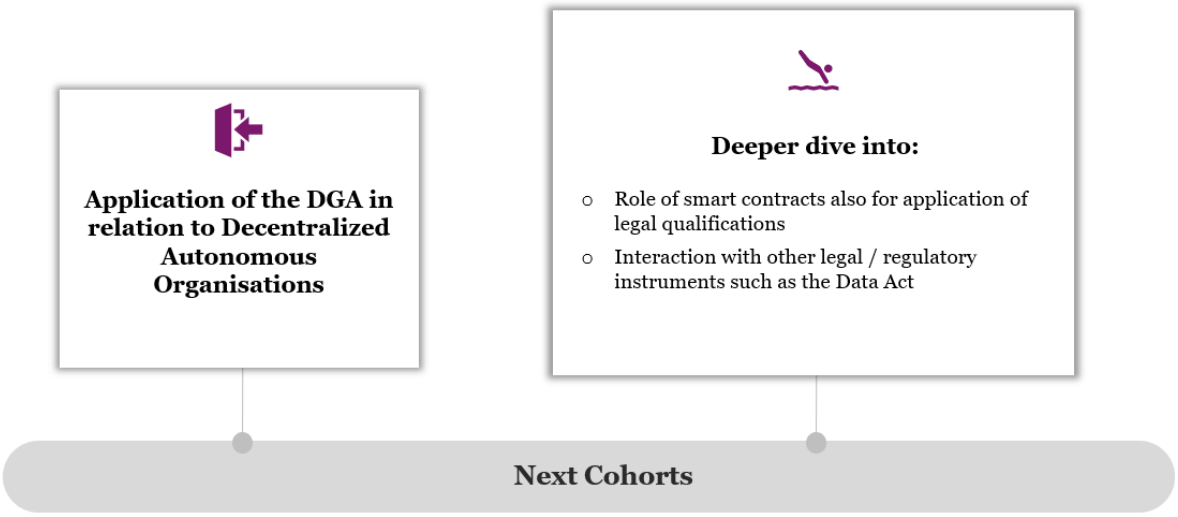
In view of the fact that the DGA is relatively new and uses novel legal concepts such as Data Altruism and Data Intermediation Services, the most efficient way forward will normally be that the use case owner (on the basis of a first legal analysis regarding the qualification of the service) discusses the qualification of the service with the competent authority/authorities to determine which regulatory obligations apply and if notification/registration is mandatory/feasible.

Best practices and lessons learned:

- The Data Governance Act is relevant in particular for use cases that qualify as Data Altruism Organisation or as Data Intermediation Services in the sense of the DGA.
- In view of the fact that the DGA is relatively new and uses novel legal concepts, the most efficient way forward will normally be that the use case owner discusses the qualification of the service with the competent authority/authorities to determine which regulatory obligations apply and if notification/registration is mandatory/feasible.

c. Areas for further clarification & dialogue topics for the next cohorts

An interesting regulatory area for the next cohorts would be the application of the DGA in relation to Decentralized Autonomous Organisations. In addition, a deeper dive into the role of smart contracts, also for the application of the legal DGA qualifications and the interaction with other legal/regulatory instruments such as the Data Act would be relevant.



11. eIDAS 2 - Regulatory compliance by Blockchain/DLT solutions

a. Introduction

Regulation (EU) 2024/1183 of 11 April 2024 (**"eIDAS 2"**) amending Regulation (EU) No 910/2014 (**"eIDAS 1"**) has entered into force on 20 May 2024. eIDAS 2 covers the EUDI wallet, electronic identification schemes and trust services (both qualified and non-qualified). This is an important step towards harmonising digital identity and trust services across the EU.

A notable change in eIDAS 2 is the introduction of the so-called **"European Digital Identity Wallet"** or **"EUDI Wallet"**. The European Commission plans to adopt implementing acts for the EUDI Wallet's measures by 21 November 2024.

This new means of electronic identification allows users (natural persons and legal entities) to identify and authenticate themselves electronically, across borders, to access a wide range of public and private services. Additionally, users will be able to use it to sign documents with qualified electronic signatures and as part of strong customer authentication (SCA) systems. The EUDI Wallet will also serve as the foundation for a common system to issue and validate attributes (qualified and unqualified) such as educational qualifications (including university degrees, other academic degrees and professional qualifications), driving licenses and permits.

In addition, the list of **"trust services"** is significantly extended by eIDAS 2.

Article 3(16) eIDAS 1 as amended by eIDAS 2:

"trust service" means an electronic service normally provided for remuneration which consists of any of the following:

(a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

(b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

(c) the creation of electronic signatures or electronic seals;

(d) the validation of electronic signatures or electronic seals;

(e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;

(f) the management of remote electronic signature creation devices or remote electronic seal creation devices;

(g) the issuance of electronic attestations of attributes;

(h) the validation of electronic attestation of attributes;

(i) the creation of electronic timestamps;

(j) the validation of electronic timestamps;

(k) the provision of electronic registered delivery services;

(l) the validation of data transmitted through electronic registered delivery services and related evidence;

(m) the electronic archiving of electronic data and electronic documents;

(n) the recording of electronic data in an electronic ledger".

New categories of trust services introduced by eIDAS 2 which can be particularly relevant for Blockchain/DLT applications include “electronic attestation of attributes”, “electronic archiving services” and “electronic ledgers”:

- ‘electronic attestation of attributes’ means an attestation in electronic form that allows attributes to be authenticated.[89]
- ‘electronic archiving’ means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.[90]
- ‘electronic ledger’ means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records.[91]

eIDAS 2 distinguishes between the requirements for non-qualified trust services and for qualified trust services which are both in scope of eIDAS 1. The regulatory requirements for both non-qualified and qualified trust services have become more stringent under the amended eIDAS 1 (see next paragraph).

Qualified trust service providers have to be notified to the supervisory body together with a conformity assessment report.[92] In addition, qualified trust service providers must undergo an audit by a conformity assessment body at least every 24 months, at their own expense.[93] The conformity assessment report and the audit have to confirm that the providers and the qualified trust services they offer meet the requirements outlined in eIDAS 2.[94]

eIDAS 2 refers to a range of implementing acts which need to be adopted by the European Commission, e.g. in relation to the EUDI Wallet, non-qualified trust services and qualified trust services.

b. Relevance of eIDAS 2 for Blockchain/DLT solutions

Blockchain/DLT solutions will normally qualify as trust services and/or will use trust services which are governed by eIDAS 2.

eIDAS 2 is relevant for the provision of trust services not only in relation to qualified trust services but also in relation to non-qualified trust services. All trust services shall be made accessible for persons with disabilities and special needs as set out in Article 15 eIDAS 2 and should comply with the security requirements set out in Articles 19 and 19a of eIDAS 2. According to Article 19a(2) of eIDAS 2 the EC shall by 21 May 2025 establish a list of reference standards and where necessary establish specifications and procedures in relation to the provision of non-qualified trust services.

An important difference between qualified and non-qualified trust services is the liability regime and the burden of proof which is much stricter for qualified trust service providers (Article 13 eIDAS 2). Another important difference is that the conformity assessment does not apply in relation to non-qualified trust services.

The way in which the use of DLT will be assessed in applications for the grant of the “qualified status” for trust services will be regulated by means of implementing acts of the European Commission. How the use of DLT will be taken into account for either *trust services using ledger* and for *trust services providing ledger* still needs to be determined.

---

89 Article 3(44) eIDAS Regulation as amended by eIDAS 2.
90 Article 3(48) eIDAS Regulation as amended by eIDAS 2.
91 Article 3(52) eIDAS Regulation as amended by eIDAS 2.
92 Article 21 eIDAS Regulation as amended by eIDAS 2.
93 Article 20 eIDAS Regulation as amended by eIDAS 2.
94 Article 20 and 21 eIDAS Regulation as amended by eIDAS 2. Following eIDAS 2 references to the cybersecurity risk management measures laid down in Article 21 of the NIS2 Directive have been added to Articles 20 and 21 of the eIDAS Regulation.

Relevance of eIDAS 2 for Blockchain/DLT solutions

- Pursuant to eIDAS 2 the list of "trust services" regulated by eIDAS 1 is extended. New categories of trust services which can be particularly relevant for Blockchain/DLT applications include "electronic attestation of attributes", "electronic archiving services" and "electronic ledgers".
- Blockchain/DLT solutions will normally qualify as trust services and/or will use trust services which are governed by eIDAS 2.
- eIDAS 2 is relevant for the provision of trust services not only in relation to qualified trust services but also in relation to non-qualified trust services.
- An important difference between qualified and non-qualified trust services is the liability regime and the burden of proof which is much stricter for qualified trust service providers (Article 13 eIDAS 2). Another important difference is that the conformity assessment does not apply in relation to non-qualified trust services.

c. Implementing acts will provide more clarity and guidance.

For qualified electronic ledgers the EC shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements specified in Article 45l of eIDAS 2 for qualified electronic ledgers: *"(a) they are created and managed by one or more qualified trust service providers; (b) they establish the origin of data records in the ledger; (c) they ensure the unique sequential chronological ordering of data records in the ledger; (d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time."*

"A trust service making use of electronic ledger" can in theory also be qualified if the ledger that is used is not qualified as long as the requirements of eIDAS 2 (including the further specification thereof in implementing acts) are met but the ledger could be relevant to take into account as part of the conformity assessment of the "trust service using ledger". Clarity on how this will work out in practice will be welcome.

Application of eIDAS 2 in relation to electronic ledgers

- For qualified electronic ledgers the EC shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements specified in Article 45l of eIDAS 2 for qualified electronic ledgers: *"(a) they are created and managed by one or more qualified trust service providers; (b) they establish the origin of data records in the ledger; (c) they ensure the unique sequential chronological ordering of data records in the ledger; (d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time."*
- How the use of DLT will be taken into account in applications for the grant of the "qualified status" for trust services will be regulated by means of implementing acts of the European Commission. A distinction will have to be made between:
  - Trust services **using** electronic ledger and
  - Trust services **providing** electronic ledger.
- "A trust service using ledger" can in theory also be qualified if the ledger that is used is not "qualified" as long as the requirements of eIDAS 2 are met but the ledger could be relevant to take into account as part of the conformity assessment of the "trust service using ledger". Clarity on how this will work out in practice in the implementing acts will be welcome.

Standards are of key importance. It is important that the standards facilitate continuity and further developments of existing applications and that they do not unnecessarily limit EU innovation and economic development (and support the principle of technology neutrality and also neutrality of different DLT/Blockchain solutions). In this regard it is important that standards become available in time and provide enough certainty to enhance investments and market adoption and on the other hand too much detail that could hamper new developments and solutions has to be avoided.

Standards will have to be adopted also in relation to electronic ledgers. An introduction to a comprehensive overview about eIDAS 1 standards and additional information, to be updated for eIDAS 2 while the logic is expected to remain the same can be found here: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/esig_pdf.pdf?__blob=publicationFile&v=6

Worldwide Technical Standards on Electronic ledger exist and are further developed in: ISO TC 307 (Blockchain and distributed ledger technologies). They will foreseeably be adopted into the European Framework by CEN JTC 19 so that only the delta has to be standardized in Europe.

- ISO TS 23353 - Auditing Guidelines
- ISO 23257 Reference Architecture
- ISO 23635 Governance Guidelines
  https://www.iso.org/committee/6266604/x/catalogue/p/1/u/1/w/0/d/0

eIDAS 2 refers to implementing acts in relation to the EUDI Wallet, non-qualified trust services and qualified trust services which will provide more clarity and guidance:

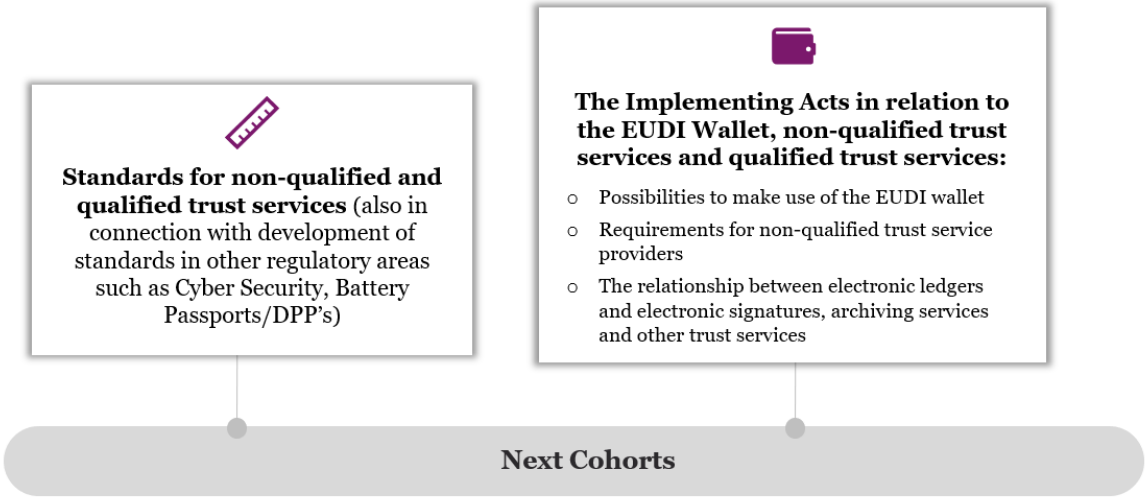
- Possibilities to make use of the EUDI wallet (also as a relying party in connection with the implementing act referred to in Article 5b(11) eIDAS 2)
- Requirements for non-qualified trust service providers, including standards (see also implementing act on the basis of Article 19a(2) eIDAS 2)
- The relationship between electronic ledgers and electronic signatures, archiving services and other trust services (to what extent will the conformity assessment for electronic signatures or archiving services also comprise a conformity assessment of the underlying electronic ledger that is used)
- Standards for non-qualified and qualified trust services.

The possibilities to provide input on the implementing acts that will be based on eIDAS 2 and on the standards that will be determined would be welcome as well as guidance on how and when interested actors can contribute their views and can intervene to collaborate in the standards development process.

Clarification and guidance (and the avoidance of possible inconsistencies) regarding the relation with standards for blockchain and distributed ledger technologies in other areas, such as DPPs would be welcome.

d. Areas for further clarification & dialogue topics for the next cohorts

eIDAS 2 was adopted in April 2024 and the implementing acts that will also establish the list of reference standards are not yet adopted. Standards for non-qualified and qualified trust services will be an important area for the next cohorts also in connection with the development of standards in other regulatory areas. In addition, the provisions of the implementing acts will be an important area for the next cohort dialogues.



12. Blockchain/DLT solutions for AML compliance

a. Introduction

Entities qualifying as virtual asset service providers under financial sector regulation or (in the future) CASPs under MiCAR[95] will have to comply with AML requirements. These are set out in the AMLD IV (Directive (EU) 2015/849 as amended, including the amendments made by the AMLD V).[96] EU member states are allowed to extend the AML & KYC rules to other categories of undertakings. The European Commission would have to be notified of such extension.

Under Articles 25 and 26 AMLDV, Member states may permit obliged entities to outsource the application of certain customer due diligence measures (CDDs) to third parties. Despite the fact that obliged entities can outsource certain CDDs, they do remain liable for regulatory compliance for all CDDs-related obligations. The same applies to outsourcing under Article 6(10) of the Digital Operational Resilience for the financial sector regulation Act ("DORA") and other outsourcing activities falling under the scope of the EBA Guidelines on outsourcing arrangements.[97]

The obligations laid down in the AMLD IV include risk assessment, identification and verification of the identity of clients and their beneficial owners, due diligence measures upon entry and throughout the business relation, obligation to file suspicious transaction reports to Financial Intelligence Units (FIUs), internal audit and reporting, and implementation of asset freezing measures.

The AMLD V sets out a series of measures aimed at combating terrorist financing more effectively and guaranteeing more transparency in financial transactions. This directive aims to make legal entities and legal structures more transparent by extending access to beneficial owner registers, harmonizing the enhanced due diligence measures to be implemented for business relationships or transactions that involve high-risk third countries, specify the measures to be implemented in the event of a creation of a remote business relationship, and provide for certain virtual asset service providers to be regulated under the anti-money laundering and countering the financing of terrorism (AML/CFT) rules.

Additionally, the Transfer of Funds Regulation[98] will apply also to CASPs. CAPSs will be obliged to collect and make accessible certain information about the sender and beneficiary of the transfers of crypto assets they operate, regardless of the amount of crypto assets being transacted. This ensures the traceability of crypto-asset transfers in order to be able to better identify possible suspicious transactions and, as necessary, block them. To this end, the EBA has issued amended guidelines on CDD requirements for risks associated with crypto asset service providers.[99]

Lately, a new AMLD VI was proposed by the European Commission in July 2021 and has been adopted by the European Parliament on 24 April 2024 and is currently awaiting the Council's 1st reading.[100] In order to effectively detect criminals attempting to misuse the financial systems for illegal purposes and to further strengthen the integrity of the internal market, further improvement of the current framework was considered necessary by the

---

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

96 Directive (EU) 2018/843.

97 https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.

98 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 and amending Directive (EU) 2015/849.

99 Available via: https://www.eba.europa.eu/sites/default/files/2024-01/a3e89f4f-fbf3-4bd6-9e07-35f3243555b3/Final%20Amending%20%20Guidelines%20on%20MLTF%20Risk%20Factors.pdf.

100 *The status and consolidated* text so far are accessible via: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0250(COD)&l=en.

European Commission. The AMLD VI will, for example, lead to changes in the field of ultimate beneficial owners and the powers of FIUs in relation to pending transactions.

Alongside the adoption of the AMLD VI on 24 April, the European Parliament also adopted the 'EU Single Rulebook Regulation', the so-called "**AMLR**".[101] This new legislative measure mainly covers the gap due to the lack of directly applicable rules under the current AML directives. This new harmonized approach should enable a strong and coherent approach at Union level to prevent money laundering and predicate offences. In the AMLR currently includes a list of obliged entities applicable in all EU Member, exemptions for certain activities and companies, facilitating compliance for cross-border obligations and additional requirements for internal policies, procedures and controls.

b. Best practices and lessons learned

AML is another important regulatory area for blockchain/DLT applications from different perspectives:

- Entities qualifying as virtual asset service providers under financial sector regulation or (in the future) CASPs under MiCAR will have to comply with AML requirements.
- Blockchain/DLT providers provide tools to support obliged entities to ensure AML compliance in their business relationships with crypto exposure.

The transposition of AML requirements into national legislation in the Member States is currently not harmonized across the EU/EEA. The step from AMLD to AMLR may already be an important step towards harmonization of AML processes. The eIDAS 2 regulation could also play a role in a more harmonized approach for AML purposes for instance in the area of identification (e.g., introducing the EU Digital Identity Wallet).

In the meantime more clarity about the national requirements in the various EU/EEA Member States would be welcome. For the time being in order to harmonise processes and operations a solution can be to implement AML measures on the basis of the strictest requirements also for those countries with a less strict regime.

The risk-based approach of AML-legislation makes it difficult to come up with an exhaustive list of risks that should be taken into account for AML due diligence, which is a burden for solutions offered by for instance blockchain analytics use cases to provide sufficient risk information for obliged entities. More guidance in this field would be welcome for the market.

Accordingly, there is a need for more guidance and/or sharing know-how (sandboxes, consultations) for obliged entities under AMLD in relation to risks associated with business relationships with clients with crypto exposure. An example is the initiative to develop a Polish standard on cooperation between financial institutions and virtual asset service providers prepared by market participants working together within a working group coordinated by the FinTech Poland foundation.

In addition, different kinds of crypto-assets (e.g. EMT or ART) could have different risk profiles with varying impact on the AML-assessments.

At the same time initiatives to allow regulators to obtain a better in-depth understanding of innovative solutions such as blockchain analytics would be welcomed. Supplementing the Sandbox dialogues with a more detailed focus on the actual testing could be helpful. In addition, a dialogue with market participants and exchange of knowledge and experiences

[101] The status and consolidated text so far are accessible via: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0239(COD)&l=en.

in this specific area could help to accelerate effectiveness and efficiency of compliance with regulation and supervision and to facilitate application of innovative solutions.

AML – Better understanding of possible crypto specific risks

- There is a need for more guidance and/or sharing of know-how (sandboxes, consultations) for obliged entities under AMLD in relation to risks associated with business relationships with clients with crypto exposure.
- Initiatives to allow regulators to obtain a better in-depth understanding of innovative solutions such as blockchain analytics could be helpful. Supplementing the Sandbox dialogues with a more detailed focus on testing of such applications could be helpful to support effective and efficient compliance and supervision in the AML area.

Different criteria impacting the assessment of whether a procured service qualifies as outsourcing (e.g., the criticality of services that are provided by third party), as well as coexistence of various outsourcing regimes (i.e, AML outsourcing[102], sector-specific outsourcing regimes applicable to financial institutions[103], EBA and ESMA guidelines on outsourcing[104]) may lead to uncertainty for service providers and financial institutions if services they provide / receive qualify as regulated outsourcing. This is another area were more guidance would be welcome.

If a financial entity purchases a license for standardised software that does not entail data exchange between the entity and the software provider, such an arrangement should not be considered outsourcing. However, as mentioned above, it is important to note that the application of DORA will introduce an ICT third-party risk management framework that extends beyond outsourcing ICT agreements, encompassing any contractual arrangements with an ICT third-party service provider.

AML – The role of outsourcing providers and ICT third-party service providers

- Different criteria impacting the assessment of whether a procured service is outsourcing, as well as coexistence of various outsourcing regimes (i.e, AML outsourcing, sector-specific outsourcing regimes applicable to financial institutions, EBA and ESMA guidelines on outsourcing) may lead to uncertainty for service providers and financial institutions if services they provide / receive constitute regulated outsourcing. This is another area where more guidance would be welcome.
- If a financial entity purchases a license for a standardised software that does not entail data exchange between the entity and the software provider, such an arrangement should not be considered outsourcing.

[102] Section 4 of Directive (EU) 2015/849.
[103] E.g., Article 19(6) of Directive (EU) 2015/2366 (PSD2) or Article 73 of Regulation (EU) 2023/1114 (MiCAR).
[104] Accessible via: https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.

c. Areas for further clarification & dialogue topics for the next cohorts

AML will continue to be an important regulatory area for many blockchain/DLT applications and tools to support effective and efficient compliance and supervision are important. In the dialogues for the next cohorts, new related regulatory areas such as the AMLR, (supplier related obligations under) DORA and eIDAS 2 can be discussed in more detail.

13. Financial sector regulation & MiCAR – Scope and delineation

a. Introduction

The issuing of or the rendering of services for third parties relating to a specific token might be subject to European regulatory regimes depending on the qualification as a financial instrument under national transposition(s) of MiFID II (Markets in Financial Instruments Directive)[105] or a crypto-asset subject to MiCAR (Markets in Crypto Assets Regulation).[106]

MiCAR does not apply to crypto-assets that qualify as financial instruments as defined in Article 4(1), point (15), of MiFID II.[107]

The concept of "financial instrument" is not defined in one single definition in MiFID II, but described in a list of instruments including "transferable securities" included in Annex I. MiFID II includes the following definition of 'financial instrument':[108]

- '**financial instrument'** means those instruments specified in Section C of Annex I;
- Section C of Annex I refers to "Transferable securities" and a range of other financial instruments.
- Transferable securities are in turn defined in Article 4(44) MiFID II:

  'transferable securities' *means those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:*
  (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
  (b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
  (c) *any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures;*

MiFID II is a directive that needs to be transposed in the national legislation of the Member States. These national laws are not fully harmonized.[109] As a result, there are still different national interpretations whether a token may qualify as security in each member state.

MiCAR is a regulation and is directly applicable in the Member States. The various rules set out in MiCAR are to enter into force at different points in time:

- Rules regarding asset-referenced tokens (ARTs) and e-money tokens (EMTs) set out in Title III and Title IV will apply from 30 June 2024.
- Rules regarding the authorisation and ongoing supervision of crypto asset service providers (CASPs) in Title V will apply from 30 December 2024.
- All the other provisions of MiCAR (in particular Title II and Title VI) will also apply from 30 December 2024. In addition, some individual articles already apply as of 29 June 2023.

---

[105] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast).
[106] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
[107] Article 2 point (4) MiCAR
[108] Article 4(15) MiFID II.
[109] Reference to ESMA consultation doc. Of 29.01.2024.

The definition of "crypto-assets" is laid down in Article 3(1) point (5) MiCAR:

- *'*crypto-asset' means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar *technology;*

MiCAR does not cover all types of crypto-assets.[110] Non-Fungible-Tokens (NFTs) are outside the scope of MiCA under certain conditions set out in the regulation.[111]

The MiCAR definition of crypto-assets is also distinct from the definition of 'DLT financial instrument' in the DLT Pilot Regime which refers to a specific subcategory of 'financial instruments":[112]

- *'*DLT financial instrument' means a financial instrument that is issued, recorded, transferred and stored using distributed ledger technology;

Whether a security token, currency token/cryptocurrency (e.g. a stablecoin) or a utility token or security token is subject to a certain regime (MiFID, MiCAR or neither) depends on the specific features of the respective token and must be determined on a case-by-case basis. An important first assessment to be made is if the token qualifies as a "financial instrument", such as a "transferable security" under the relevant national legislation by which MiFID II is transposed in national law.[113] If a specific token/coin qualifies as both, the MiCAR regime will not apply, but instead the MiFID II regime is applicable.[114]

ESMA consultation paper of 29 January 2024

- The delineation between financial instruments covered by MiFID II and crypto-assets covered by MiCAR is addressed in the ESMA consultation paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments.[115]

b. Best practices and lessons learned

The topics that were discussed during the 1st round of dialogues were linked to the relevant use cases and are therefore not exhaustive. The topics can be explored in more detail and additional topics can be added in the next dialogue rounds.

MiCAR - Scope

The term non-fungible tokens (NFT) is often used in relation to crypto assets and MiCAR. However, in the context of MiCAR the use of this term is confusing as in principle only fungible tokens are within scope of MiCAR. The confusion is caused by the fact that based on the technology used, e.g., tokens using the ERC 721-protocol, usually presume the non-

110 More specifically, the MiCA Regulation does not apply either to crypto-assets that qualify as deposits, funds (except if they qualify as e-money tokens), securitisation positions, non-life or life insurance products and pension products (Article 2(4) MiCAR).
111 Recitals 10 and 11 MiCAR.
112 Regulation (EU) 2022/858 of the European parliament and of the council of 30 May 2022 ("DLTR")
113 Article 4(1)(15) MiFID (definition of financial instrument) in conjunction with Annex I, Section C, to MiFID II (reference to "transferable securities") and Article 4(1)(44) MiFID (definition of "transferable securities").
114 Article 2(4)(a) MiCAR.
115 https://www.esma.europa.eu/sites/default/files/2024-01/ESMA75-453128700-52_MiCA_Consultation_Paper_-_Guidelines_on_the_qualification_of_crypto-assets_as_financial_instruments.pdf.

fungibility of that token due to the technical characteristics. However, the legal assessment if a token is non-fungible is not determined on the basis of this technical characteristic alone.

- Whether a token is “fungible” needs to be determined on the basis of the assessment of legal fungibility and not only on the basis of the technical characteristics.

Transferability is a key element in the definition of “crypto-asset” in the sense of Article 3(1) point (5) MiCAR:

- If a token is never in the hands of someone else than the issuer, it is minted upon request by the issuer and simultaneously minted and burnt this could be an indication that the token is not transferable.

The term and regulation of tokenized deposits is subject to discussions. The delineation between tokenized deposits and e-money tokens is relevant and needs to be discussed. It could generally be argued that so-called tokenized deposits are not de facto e-money tokens since MiCAR does not apply to deposits (Art 2(4)(b) MiCAR), but further guidance would be welcome. The regulation of deposits, however, has a different scope than MiCAR.

MiCAR vs Financial sector regulation (delineation)

It is important to determine whether instruments qualify as financial instruments under MiFID or as crypto assets subject to MiCAR. The consultation by ESMA will be helpful but the understanding of the term "financial instrument" will still depend on the interpretation in the individual member states.

In view of the implications, it is not only important to assess if an instrument qualifies as a financial instrument or a crypto asset subject to MiCAR but also which party qualifies as issuer and which party qualifies as Service Provider/CASP.

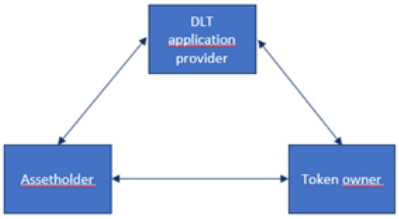
	Financial Markets Regulation	MiCAR
Issuer	Prospectus regulation	White paper obligation
Service provider / Crypto-asset Service Provider (CASP)	License requirement	License requirement

The main indicator for the issuer is the person who is responsible for fulfilling the (payment) obligations linked to the instrument. This assessment will depend on the set up and the contractual relations. In the graph below, the DLT application provider would most likely be qualified as the issuer and offeror in scenario 1, while in scenario 2, depending on the exact services offered, the DLT application provider could be qualified as service provider and depending on the service as offeror.

Scenario 1:
DLT application provider enters into agreement with Assetholder to receive in its own name all revenues.

DLT application provider issues tokens to token owner and promises to token owner to pay revenue received from the Assetholder's assets.

Scenario 2:
DLT application provider 'brokers'/'facilitates' direct agreement between Assetholder and token owner under which Assetholder promises to token owner to pay revenues.



Crypto asset services vs Payment services – Initial findings during the 1st cohort dialogues

Different aspects may be considered as part of the assessment of the exchange of tokens and if this could qualify as a payment service:

- Not being involved in the payment between the customer and the service provider, not receiving any funds and if the service provider can accept the payment or not, could be indications not to qualify the use case as a payment service.
- The role of the smart contract to complete the transaction between the service provider and the customer could also be relevant. Smart contracts created by and which benefit the owner/operator, could result in the owner/operator to be involved in service provisioning. In that case, smart contracts may act as an (automated) exchange, which may qualify as a payment service.

Exchanging corresponding amounts (as required in the definition of money remittance) requires that funds are paid on both sides. A payment service necessitates that both directions of the transfer are in funds and if not, it is no payment service. If there is a transfer of a crypto-asset (other an EMT or ART) on one side, it is likely that there is no payment service. If there is a transfer of EMT, it is likely there is.

Providing transfer services for crypto on behalf of clients can be considered as a crypto-asset service, regardless of whether it can be qualified as an exchange, and should therefore be licensed under MiCAR.

Delineation between a payment service and a crypto-asset service also depends on qualification of certain stablecoins as e-money tokens or not, as these tokens are classified as funds. Further clarifications regarding qualification and categorization of stablecoins could provide more clarity here.

	Token to pay a service is a Crypto-Asset other than an E-Money Token	**Token to pay a service is an E-Money Token and therefore considered as Funds**
Token to access a service is a Crypto-Asset	Crypto-asset <-> Crypto-asset ➔ *Exchange of CA for CA*	Crypto-asset <-> Funds ➔ *Exchange of CA for Funds* ➔ *Payment Service*
Token to access a service is not a Crypto-Asset	Service <-> Crypto-asset ➔ *Transfer services for CA on behalf of clients*	Service <-> Funds ➔ *Payment Service*

In relation to the qualification of tokens under MiCAR and the delineation between crypto-asset services and payment services, additional guidance on an EU level, for instance through a consultation by ESMA/EBA would be welcome.

Compendium of topics where clarification from EBA/ESMA would be welcome

Several topics were identified during the 1st cohort dialogues where clarification from EBA/ESMA would be welcome.

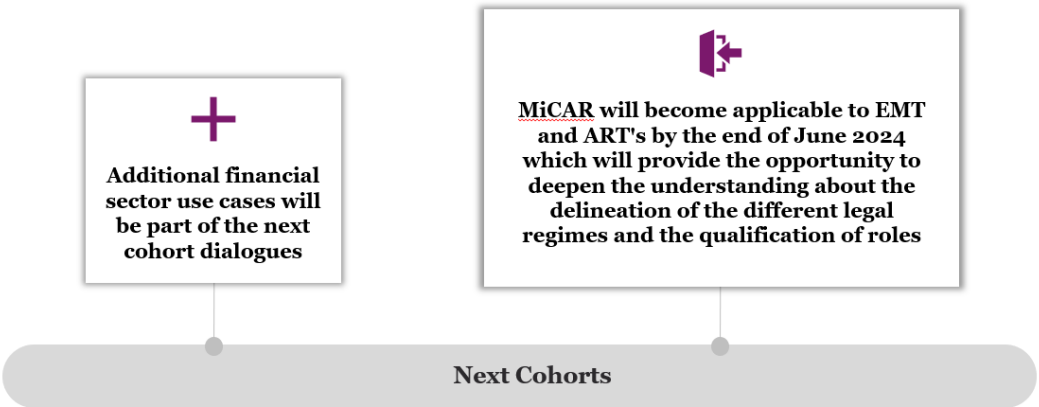
- Interplay between MiCAR and PSD/EMD:
  - can the transfer of crypto assets qualify as a payment service?
  - if a service is both a payment service and a crypto asset service clarity on the question if one of the two would be sufficient would be welcome.
- Clarity about the list of existing stablecoins that are issued outside the EU and does not reference the official currency of a Member State[116] is needed as it is not really possible to use a non-approved stablecoins that is not on the transitional list.
- In case the offeror is not based in the EU or in case of non-approved stablecoins guidance regarding the party who is responsible for publishing a whitepaper (if such stablecoin is not traded by any platform based in the EU) would be welcome.
- Also from the perspective of supervisors, guidance is welcome in relation to the enforcement procedures of MiCAR in relation to third country offerors or persons admitting to trading of crypto assets other than ART/EMT.

In view of the fact that the EU legislation is relatively new (MiCAR) and that the delineation between the new legislation and prior existing financial regulation (for example MiFID II and PSD2) requires a case-by-case assessment and will determine which kind of license(s) will be required, most efficient way forward will normally be that the use case owner:

- Provides the relevant competent authority with a first legal analysis on the qualification of the service;
- Then discusses the qualification of the service with the competent authority to determine which regulatory obligations apply and if/which license application needs to be submitted.

c. Areas for further clarification & dialogue topics for the next cohorts

Additional financial sector use cases will be part of the next cohort dialogues and MiCAR will become applicable to EMT and ARTs by the end of June 2024 which will provide the opportunity to deepen the understanding about the delineation of the different legal regimes and the qualification of roles.



[116] See article 48(2) MiCAR: "*An e-money token that references an official currency of a Member State shall be deemed to be offered to the public in the Union.*"

14. Tokenization of shares and dividend payments under MiFID / Financial sector regulation

a. Introduction

In this chapter it is assumed that tokenized shares qualify as financial instruments under the relevant applicable national law transpositions of MiFID II. If the token does not qualify as a "financial instrument" under MiFID II, the token could qualify as a crypto asset subject to MiCAR or other national law not based on European Directives (or could be unregulated). The delineation between qualifications under MiFID and MiCAR was an important topic in the 1st round of dialogues and is discussed in the previous chapter.

In relation of the issuance of financial instruments to the public the Prospectus Regulation[117] needs to be complied with as well as the PRIIPs Regulation.[118]

Relevant EU regulations to consider when offering activities with financial instruments includes e.g. MiFID, MiFIR[119], CSDR[120], DLT Pilot Regime[121] and ECSPR[122]. The DLT Pilot regime regulation was adopted on 23 March 2023 providing a sandbox environment for trading and settlement in a.o. tokenized shares.

b. Best practices and lessons learned

To realize the potential of harmonized EU legislation and an efficient/effective application of Financial Sector Regulation, potential civil/corporate law issues regarding ownership and transfer formalities with respect to e.g. the tokenization of shares, will have to be looked into in further detail in particular in a cross border setting.

Irrespective of MiFID harmonizing national legislations, there are still different interpretations whether a token may qualify as security in each member state. Different approaches to transferability of shares or interests under national corporate or partnership law can be a reason for the national differences in interpretation if a token that tokenizes such shares or interests qualifies as a security.

- For example, the question arises if a share or interest normally not easily transferable reaches transferability qualifying it as a security because of its tokenization.
- MiFID, as a Directive, needs to be transposed into national law by the Member-States and the term "security" in Article 4(1) para 15 MiFID in conjunction with Section C of Annex I appears to leave the room as set out in the previous point for national interpretation.[123]

---

[117] 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.

[118] Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs).

[119] 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 648/2012.

[120] 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.

[121] 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, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

[122] 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.

[123] These national differences will in itself not change as a result of the fact that Article 18 of the DLT Pilot Regime Regulation adds to the definition of financial instrument that financial instruments can also be issued by means of distributed ledger technology.

The regulatory requirements for issuing financial instruments such as transferable securities (e.g. shares in stock corporations) should be considered separately from the regulatory requirements for offering financial services with financial instruments to the public. The latter includes services such as placement of financial instruments and/or the operation of a multilateral trading facility or a central securities depositary. The regulatory perimeter for any offer of activities with financial instruments in a DLT/blockchain context should be considered on a case-by-case basis. Relevant EU regulation to consider when offering activities with financial instruments includes MiFID, MiFIR, CSDR, DLT Pilot Regime and ECSPR.

Member States could therefore facilitate the EU DLT Pilot Regime by corporate law amendments in national law

Example:

- The EU DLT Pilot Regime Regulation is facilitated in Finland by corporate law amendments on a national level enabling the registration of shares in a limited liability company in a DLT based settlement system instead of a traditional book-entry securities system. This amendment goes beyond the change of the definition of "financial instrument" following the amendment of MiFID II in accordance with Article 18 of the EU DLT Pilot Regime Regulation.

Subject to additional requirements applicable in Member States following the national transposition of MiFID II, there is no regulatory requirement at EU level that dividend payments should be paid in cash or scriptural money; this could also be in e-money token (EMT) or asset-referenced token (ART).

- There could be certain consequences from an AML perspective because different kinds of crypto-assets (e.g., EMT or ART) could have different risk profiles with varying impact on the AML-assessments.
- There could be an impact on capital requirements based on the status/risks associated with different types of crypto-assets (EMT or ART) and their underlying DLT.
- The qualification of fiat currency is not yet harmonized and there may be consequences from other perspectives (e.g. civil law, taxation).

c. Areas for further clarification & dialogue topics for the next cohorts

There are still different interpretations whether a token may qualify as a security in individual Member States and national civil/corporate law is not harmonized. The next cohorts could provide the possibility for a deeper dive into national differences both in legislation and interpretation. In addition, the experiences with the DLT Pilot Regime will likely be a topic for the next rounds of dialogues.

15. Application of Financial Sector regulation to Smart Contracts

a. Introduction

Smart contracts are a key element for the development and the provision of DLT/Blockchain solutions. Financial sector regulation does not include provisions that specifically focused on smart contracts.

The Data Act includes sector agnostic provisions regarding smart contracts that are also relevant for smart contracts used by (suppliers to) DLT/Blockchain applications in the financial sector. The Data Act will apply from 12 September 2025.[124]

Smart contracts are defined in Article 2(39) of the Data Act:[125]

- ***'smart contract'*** *means 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;*

The provisions of the Data Act will be relevant for a.o.:[126]

- participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

Vendors of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of the execution of (part of an) agreement to make data available shall ensure that those smart contracts comply with certain essential requirements.[127]

The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available should perform a conformity assessment with a view to fulfilling the essential requirements.[128]

In addition, Article 22 GDPR regarding automated individual decision-making could be relevant which provides the right for data subjects not to be subject to a decision based solely on automated processing which produces legal effects unless certain conditions are met.[129]

b. Initial findings for financial sector use cases

The application of smart contracts in financial sector and other use cases was briefly discussed in some of the 1st cohort dialogues from a financial regulatory perspective.

---

[124] However, the obligation resulting from Article 3(1) on B2B data access by design shall apply to connected products and the services related to them placed on the market after 12 September 2026. Chapter IV will apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are: of indefinite duration; or due to expire at least 10 years from 11 January 2024.

[125] Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). The Data Act entered into force on 11 January 2024.

[126] Article 1(3) point (g) Data Act.

[127] Article 36(1) Data Act.

[128] Article 36(2) Data Act. In order to facilitate the conformity assessment, the Data Act provides for a presumption of conformity if certain harmonized standards are met which will be adopted (Article 36(4 & onwards) Data Act.

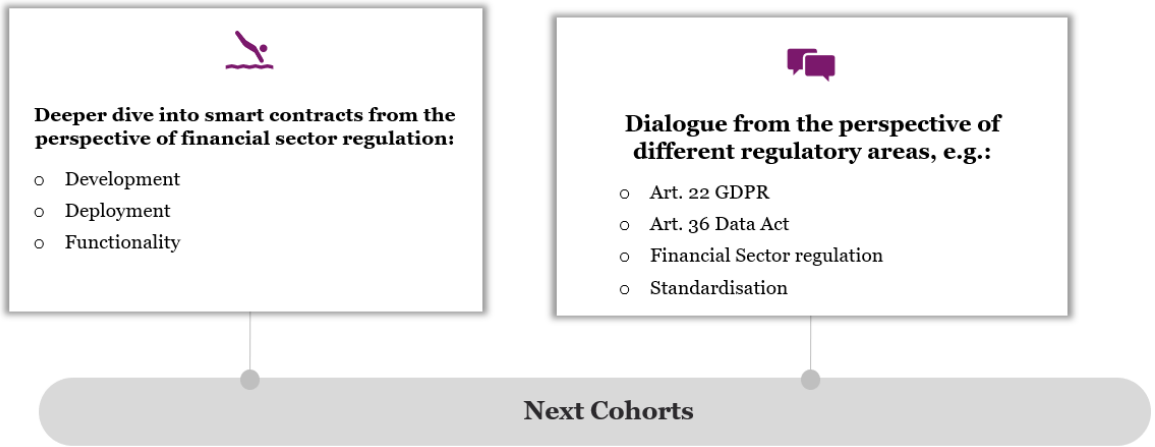
[129] See Article 22 for further details.

The wide range of potential functionalities of smart contracts in finance requires a case-by-case analysis.

- If the smart contract allows for certain activities to take place and those activities are regulated, then the smart contract should be evaluated in the same way as other similar activities. This follows the principle of 'same activity, same risk, same rules'.
- However, if the 'activity' is the same needs to be assessed. This is of particular importance as operationally some specificities related to the DLT/blockchain environment, such as decentralized players, might have to be taken into consideration. Also, each smart contract needs to be interpreted in connection with the applicable legal arrangements. In addition, new 'rules' such as the new crypto-asset related regulation (such as MiCAR) may lead to new legal qualifications, compared to "traditional" similar activities.
- In general, a smart contract issuing or operating a token as such will not change the applicable regulatory requirements, but the regulatory assessment could change if other functionalities are available over time. The person identified as "in control" of the smart contract would be responsible for the regulatory requirements which requires a more detailed case-by-case analysis in a DLT/blockchain context.
- The role of the smart contract to complete the transaction between the service provider and the customer could also be relevant. Smart contracts created by and which benefit the owner/operator of the smart contract, could result in the owner/operator to be involved in service provisioning. In that case, smart contracts may act as an (automated) exchange, which may qualify as a payment service.

c. Areas for further clarification & dialogue topics for the next cohorts

The expectation is that the development, deployment and supply of smart contracts for financial sector and other use cases will be in important area for the next cohorts. Depending on the use cases Article 36 Data Act, Article 22 GDPR and sector specific characteristics and regulation could be relevant.



16. Conclusions and next steps

The 1st round of regulatory dialogues resulted in a broad range of best practices, lessons learned and recommendations which are presented in the *Best practices report, 1st cohort, Part B*.

The European Blockchain Sandbox project team would like to thank the participants to the 1st round of dialogues for sharing their expertise and experiences and for contributing to the best practices, the lessons learned and the recommendations that were identified during the dialogue meetings.

Feedback from the 1st cohort of selected use cases and participating regulators/authorities is very positive. The use cases appreciate the legal/regulatory guidance and the possibility to have an open dialogue with regulators/authorities. The regulators/authorities appreciate to learn more about DLT use cases and to have a cross-border dialogue with other national and EU regulators/authorities. Almost all regulators/authorities are interested to participate again in the next round of dialogues (depending on use cases and regulatory areas/topics) and many regulators/authorities have shared helpful feedback and recommendations for possible improvements for the next rounds of dialogues.

Although this is only the 1st round of dialogues it appears safe to say that the European Blockchain Sandbox is delivering a clear and positive impact for the whole Blockchain ecosystem. With “impact” we refer to the pivotal role that the Sandbox is playing to reinforce the perceived maturity and potential of blockchain technology. This important outcome has been achieved thanks to the following results:

- increased legal certainty through enhancing a better understanding of relevant laws and regulations by innovators and greater confidence of compliance;
- enhancing confidence among stakeholders and regulators/authorities by showing the potential of Blockchain/DLT solutions to support effective and efficient compliance and supervision across different industry sectors;
- the possibility to improve the regulatory framework as a result of the identification of regulatory issues and solutions and of areas for clarification, leading to more effective regulations;
- cross border collaboration facilitated by the project among European and national regulators/authorities and innovators, promoting a more unified regulatory approach of Blockchain/DLT solutions which will enhance more harmonized regulatory practices and will help to create a more cohesive regulatory framework;
- facilitate the sharing of knowledge and experience between regulators/authorities and with innovators on the basis of concrete use cases resulting in a better understanding of compliance requirements among Blockchain/DLT innovators and regulators/authorities;
- acceleration of innovation by providing a safe environment for refining blockchain applications to support compliance by design;

It is obviously a journey that will continue for the next cohorts. The regulatory areas for the first cohort will continue to be relevant and the next rounds of dialogues will allow for deeper dives into the various topics and to take account of new developments on the basis of secondary legislation, administrative decisions and case law. In addition, other (new) regulatory areas will become relevant for the next cohorts such as the Data Act, the Digital Services Act, DORA, the AI Act, ESG regulation (including CSRD compliance), standardization and the regulation of smart contracts.

The expectation is that the impact of the sandbox with the lessons learned from the 1st cohort will be even more appreciated and will serve as a best practice for similar future initiatives.

Finally, the EBS project team would like to thank the project team at DG CONNECT for the seamless cooperation and the excellent input and guidance that is provided at all stages of the project.

17. List of abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
AML	Anti money laundering
ASP	Application service provider
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CO_2	Carbon dioxide
DAO	Depending on the context: Data Altruism Organisation (in the sense of the Data Governance Act) or Decentralized Autonomous Organization
DISP	Data Intermediation Service Provider
DLT	Distributed Ledger Technology
DP	Data Protection
DPP	Digital product passport
EBP	European Blockchain Partnership
EBS	European Blockchain Sandbox
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EDIC	European Digital Infrastructure Consortium
EDPB	European Data Protection Board
eFTI4EU	Electronic Freight Transport Information for Europe
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI	European Union Digital Identity
EU ETS	European Union Emissions Trading System
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
IT	Information Technology
KYC	Know Your Customer
Member States	EU/EEA Member States
MRV	Monitoring, reporting and verifying (based on the MRR & AVR)
MS	Member State(s)
MSP	Managed service provider
MSSP	Managed security services provider
NFT	Non-Fungible Token
QTSP	Qualified Trust Service Provider
SCA	Strong Customer Authentication
SPV	Special Purpose Vehicle
TSP	Trust service provider
VAT	Value Added Tax

18. Definitions

a. Terms used in the Report

Term	Explanation
Distributed ledger	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.[130]
Distributed ledger address	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.[131]
Member State	A Member State of the EU/EEA
Regulators/Authorities	The regulator(s) and authorit(y)(ies) that participate together with the selected use case owners in the European Blockchain Sandbox.
Smart contracts	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.[132]

b. Common short forms of EU legislation

Short form	Full reference
AI Act	Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final. The latest draft of the Regulation was published by the European Council on 21 May 2024.[133]
AMLD IV	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 most recently amended by Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures.
AMLD V	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU
AMLD VI	Directive (EU) 2024/… of the European Parliament and of the Council on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of

130 Article 2(2) DLT-pilot Regime and Article 3(2) MiCA.
131 Article 3(18) of Regulation 2023/1113 on information accompanying transfers of funds and certain crypto-assets.
132 Article 2(39) of the Data Act.
133 https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/?utm_source=brevo&utm_campaign=AUTOMATED%20-%20Alert%20-%20Newsletter&utm_medium=email&utm_id=320.

Short form	Full reference
	money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849
AMLR	Regulation (EU) 2024/… of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
AVR	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.
Battery Regulation	Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries.
Commission Delegated Regulation (EU) 2023/2917	Commission Delegated Regulation (EU) 2023/2917 of 20 October 2023 on the verification activities, accreditation of verifiers and approval of monitoring plans by administering authorities.
Company Law Directive	Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law.
CSDR	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).
CSRD	Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting.
Data Act	Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data.
Data Governance Act	Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance.
Digital Company Law Directive	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.
Directive (EU) 2023/959	Directive (EU) 2023/959 of the European Parliament and of the Council of 10 May 2023 amending Directive 2003/87/EC establishing a system for greenhouse gas emission allowance trading.
DLT-Pilot Regime	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.
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

Short form	Full reference
DSA (or Digital Services Act)	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services.
ECSPR	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.
EEIG Regulation	Council Regulation (EEC) No 2137/85 of 25 July 1985 on the European Economic Interest Grouping (EEIG).
eIDAS 1	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.
eIDAS 2	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
EMD II	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.
ESPR	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).
EU ETS	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.
EUI DPR	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.
GDPR	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 and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1
Implementing Regulation of the UCC	Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of the Union Customs Code.
MiCAR	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.
MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.
MiFIR	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and

Short form	Full reference
	amending Regulation (EU) No 648/201, lastly amended by Regulation (EU) 2022/858 (DLT Pilot Regulation).
MRR	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.
MRV Maritime Regulation	Regulation (EU) 2015/757 on the monitoring, reporting and verification of carbon dioxide emissions from maritime transport, as amended.
NIS2 (Directive)	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.
PRIIPs Regulation	Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs).
Proposed Directive for ECBAs	Proposal of 5 September 2023 for a Directive of the European Parliament and of the Council on European cross-border associations (COM(2023) 516 final).
Prospectus Regulation	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.
PSD II	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.
RCE Directive	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
Register Interconnection Regulation	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.
TFR	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 and amending Directive (EU) 2015/849.
SCE Regulation	Council Regulation (EC) No 1435/2003 of 22 July 2003 on the Statute for a European Cooperative Society (SCE).
SE Regulation	Council Regulation (EC) No 2157/2001 of 8 October 2001 on the Statute for a European company (SE)

Short form	Full reference
Shareholders Rights Directive	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.
TFR	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.
UNESCO Convention 1970	UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970).
UCC	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.

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-06-24-099-EN-N

Publications Office
of the European Union

doi: 10.2759/76203
ISBN 978-92-68-17451-7