MICAR ROUNDTABLE EXPERT SERIES

LONDON

The MiCAR Roundtable Expert Series had been initiated by thinkBLOCKtank in cooperation with Validvent as contribution to increasing legal certainty within the realm of the EU crypto markets. As a new regulatory framework, the application of MiCAR still raises numerous questions. The MiCAR Roundtable Series aims at facilitating expert discussions, resulting in public reports and specific calls to action. The roundtables will be held across Europe throughout the year 2024.

On March 25th, the first MiCAR Roundtable of this series commenced in London at the Austrian Trade Commission. Organised by thinkBLOCKtank, Validvent, ADVANTAGE AUSTRIA UK, the Austrian Professional Association for Financial Service Providers, and the Vienna Business Agency, in partnership with APCO, INATBA, and EUBOF, a diverse group of experts had been invited to discuss a selected number of issues when applying for MiCAR.

The London roundtable discussion included reports from MiCAR experts Elise Soucie on Sustainability Requirements, Dr. Max Bernt on the intricacies of EMTs and E-Money, and Joey Garcia on the challenges related to reverse solicitation in the context of application store fronts.

This report aims to consolidate the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants or the respective rapporteur.

1. Sustainability requirements

The discussion on sustainability requirements was led by Elise Soucie, Director of Global Policy & Regulatory Affairs at Global Digital Finance. The conversation focused on how jurisdictions implementing MiCA could integrate renewable reporting aligned with existing sustainability frameworks like the Corporate Sustainability Reporting Directive (CSRD), the Sustainable Finance Disclosure Regulation (SFDR), and the European Sustainability Reporting Standards E1 (ESRS E1). These frameworks emphasise the importance of including positive metrics in renewable reporting to offer a more comprehensive view of the ecosystem's impact on climate change—both positive and negative.

The initial proposed solution encouraged jurisdictions to adopt additional reporting mechanisms equivalent to those in ESRS E1 and CSRD, providing broader context and enabling the inclusion of both qualitative and quantitative data on sustainability risks and opportunities. This alignment with broader EU sustainability requirements was seen as crucial for fostering a holistic understanding of the ecosystem's impact.

Several critical issues were raised concerning the integration of sustainability metrics into regulatory frameworks. Concerns were voiced about potential fragmentation within MiCA legislation, particularly regarding the alignment of sustainability indicators with other existing EU frameworks. Participants noted that inconsistent implementation across member states could misrepresent the digital asset industry if only negative metrics are reported without the ability to showcase positive indicators.

Questions arose about who should report the metrics, debating whether it should be a combined effort between the issuer and the CASPs, or if CASPs should report independently. It was suggested that for accuracy, CASPs might report solely on the metrics they directly influence, but a cooperative approach including issuers and both Layer 1s and Layer 2s could offer a more holistic view of the ecosystem.

The impracticality of CASPs reporting on the sustainability metrics of entire public chains was also acknowledged, with consensus that this could lead to inaccurate and potentially redundant reporting. The discussion then shifted to the balance between mandatory and voluntary reporting, especially considering whether the inclusion of positive metrics should be mandatory. Since the Corporate Sustainability Reporting Directive (CSRD) usually applies to larger businesses, the group pondered if mandating these requirements for smaller entities would be disproportionate. However, the voluntary inclusion of such metrics was suggested as a potential solution.

Political challenges were also highlighted, particularly the difficulty in achieving national alignment with EU-wide frameworks like CSRD and ESRS E1, given their political nature. This led to a proposal that the integration of positive metrics might be more suitably addressed in an update to MiCA legislation.

Concerns about regulatory arbitrage were discussed, with suggestions that the European Securities and Markets Authority (ESMA) could provide

additional guidance or issue a Q&A to help standardize the inclusion of positive metrics and prevent inconsistencies across jurisdictions.

Finally, the roundtable identified a tension between flexibility in reporting and the risks of greenwashing. A proposed solution was to standardize quantitative reporting of positive metrics and allow more flexibility in qualitative reporting. It was noted that even the absence of negative metrics (indicating carbon neutrality) could be considered a positive outcome. To conclude, the participants agreed that a collaborative effort between the public and private sectors would be crucial to determine what data is already being collected and how it can be integrated effectively into the reporting framework, ensuring that the measures are practical and appropriate across the industry.

There was a consensus at the roundtable that aligning MiCA proportionately with ESRS E1 and CSRD would be beneficial, including provisions for reporting positive metrics. The participants unanimously agreed that the most immediate and effective step forward involves a collaborative discussion between the public and private sectors to determine which criteria and data are currently reported and how they can be incorporated into the MiCA framework. Such integration would enhance the accuracy, proportionality, and practicality of MiCA sustainability reporting across the industry.

Moreover, there was a general agreement that despite some challenges regarding data availability for CASPs, it would be most effective for CASPs to report metrics as a single entity. Additionally, a collaborative approach could be considered, developing a unified set of metrics for issuers and CASPs, as well as for Layer 1 and Layer 2 networks, to foster a more comprehensive view of the ecosystem.

Regarding the oversight of positive metrics inclusion, the group suggested that these metrics could be incorporated into a subsequent regulatory update or, alternatively, ESMA could issue further guidance or a Q&A to standardise the inclusion of these metrics across member states, thereby reducing the risk of regulatory arbitrage. The consensus supported standardising positive metrics for quantitative reporting, potentially making them mandatory, while allowing more flexibility for qualitative metrics to be voluntarily reported.

The topic discussion culminated in a strong recommendation for the public and private sectors to work together closely to define what data is currently being reported and how it can be effectively integrated into the MiCA framework. This collaborative approach would ensure that sustainability reporting under MiCA is practical and truly reflective of the industry's capabilities, facilitating a balanced and thorough regulatory framework.

Primary call to action for Sustainability requirements:

The primary call to action for regulators in the context of sustainability requirements within MiCA is to incorporate positive sustainability metrics into reporting frameworks. This involves:

- Developing and implementing additional reporting mechanisms that align with existing sustainability frameworks such as the CSRD and the Sustainable Finance Disclosure Regulation (SFDR).
- Regulators are urged to establish clear guidelines and standards that allow for the inclusion of both positive and negative environmental impacts, ensuring that the digital asset industry's contributions to sustainability are accurately represented.

2. EMTs and E-Money: Regulatory Treatment

The second topic of the Roundtable, led by Dr. Max Bern, Managing Director, Europe of Taxbit, provided a comprehensive exploration of the regulatory treatment of Electronic Money Tokens (EMTs) under MiCA, along with related directives such as the Electronic Money Directive 2 (EMD II), Payment Service Directive 2 (PSD II), and the forthcoming Payment Services Directive 3 (PSD3). The session emphasised the complex regulatory landscape, highlighting significant challenges and discussions regarding the current classification and regulatory approaches towards EMTs.

The discussion commenced with a critique of MiCA's Article 48(2), which controversially equates E-money tokens with electronic money, a simplification that could overlook the fundamental differences between traditional electronic money and EMTs. To frame this discussion, electronic money was defined as electronically stored monetary value issued on receipt of funds for payment transactions and accepted by entities other than the issuer, as per EMD II. In contrast, EMTs, as defined by MiCA, are digital representations of value referencing a single official currency, including a diverse range of digital assets from fully backed stablecoins to algorithmic tokens.

Key distinctions between EMTs and traditional electronic money emerged from the discussion, particularly noting that EMTs are regulated under MiCA which does not blanket apply the regulations of the E-Money Directive. EMTs may be issued by a broader range of entities, unlike traditional electronic money which is restricted to issuance by Electronic Money Institutes or credit institutions. Additionally, EMTs enable permissionless transfers, a stark contrast to the permissioned nature of traditional electronic money transfers, and are used both as payment methods and mediums of exchange, while traditional electronic money primarily serves payment purposes.

Discussions on the regulatory treatment of EMTs highlighted significant complexities under the upcoming Payment Services Directive 3 (PSD3). There was a proposal for defining EMTs under PSD3 as those (i) duly issued by an entity meeting Article 48(1) of MiCA and (ii) in compliance with Title IV of MiCA requirements. This definition would clarify that only entities performing

public offerings or seeking trading admissions—as EMIs or credit institutions—should issue EMTs.

Throughout the roundtable, participants expressed scepticism about regulators' openness to discussing such a sensitive topic. They questioned the feasibility of the proposed classifications under PSD3, particularly with the broad categorization of EMTs under MiCA and its implications for various crypto-assets. Concerns were raised about the adaptability of regulatory frameworks to diverse EMT mechanisms and the challenges of aligning them with PSD3 requirements.

The discussions culminated in several key recommendations aimed at refining the regulatory framework to effectively address the unique attributes of EMTs. These included enhancing regulatory flexibility to accommodate diverse EMT structures and developing specific criteria for EMT classification under PSD3 based on compliance with MiCA. Additionally, there was a strong push for international collaboration to standardise regulations across jurisdictions and periodic reviews of the regulatory frameworks to ensure they remain relevant and effective amid rapid technological advancements. These initiatives are designed to promote stability, transparency, and protection in the digital financial market while fostering an environment conducive to innovation.

All involved parties agreed that a close public-private collaboration would be crucial to ensure that regulators can better address the complexities associated with EMTs, ensuring that the regulatory environment supports innovation while safeguarding the financial system and protecting consumers. Also, a closer look should be taken at the AML-requirements that would result from the qualification of EMTs as electronic money.

Primary call to action for EMTs and E-Money: Regulatory Treatment:
For EMTs, the primary call to action for regulators focuses on the clarification and adaptation of regulatory frameworks to better accommodate the unique characteristics of EMTs under PSD3. This involves: • Defining specific regulatory criteria for EMTs under PSD3 that ensure all EMTs are issued by entities compliant with MiCA's stipulations, particularly focusing on those EMTs that adhere to stringent operational and collateralization standards as outlined in MiCA. • Encouraging the implementation of a dynamic regulatory sandbox where EMTs can be innovatively tested under regulatory oversight, allowing for real-time adaptation and risk management.

3. Solicitation

The third topic of the Roundtable, led by Joey Garcia, explored the evolving challenges of solicitation of business, focusing particularly on licensing triggers and the enduring 'characteristic performance' tests amidst modern digital landscapes. During the discussion, it was highlighted the rigorous updates to guidelines by platforms like Apple, Google, and other social media that host crypto-related services, necessitating stringent jurisdictional assessments based on the principle of reverse solicitation.

The tests for the Solicitation of Business, licensing triggers and legacy 'characteristic performance' tests have been in place for some time. Modern application store fronts like Apple have updated their guidelines which crypto related service providers are obliged to comply with. Exemptions or permissions for crypto related service providers to continue to be able to run and update their applications are subject to compliance with these guidelines. Various participants in the industry are required to go through jurisdictional assessments on the principle of reverse solicitation. For example, Apple has updated their processes to ensure compliance with the FinProm rules in the UK for the UK facing App Store.

ESMA's Reverse Solicitation Guideline under Art 61(3) of MICA has significant implications for global crypto related service providers which intend to continue to offer services, and in particular new services through any form of application. How will international service providers that service users in the EU be able to continue to offer services through European App Stores on the basis of the extended definition around the concept of solicitation. There is no ability to geo-fence (a general 'strong indicator' against the principle of solicitation), and it will be unclear as to whether the interaction with an app store can be construed as on the initiative of the user, whether the app store will itself be constructed as the intermediary or 'arranger' of the introduction/transaction, or whether the wording, description, images etc accompanying the application will be the basis of an interpretation of this being a 'solicitation'.

How will financial institutions which may ultimately also offer crypto related exposure be treated and will they be treated under existing (MiFID) rules or under these new standards? To address the challenges discussed, the following solutions were proposed: First, initiate consolidated and constructive interactions with major application storefronts, aiming for a clear interpretation that allows international crypto-related service providers to align with updated guidelines. Second, provide consolidated feedback on the ESMA consultation, focusing specifically on application interactions. Third, achieve a definitive determination on whether a properly described application should be considered as constituting solicitation under the guidelines. Lastly, clarify whether a financial institution, although not necessarily authorized under MiCA but licensed within the EU, is exempt from or subject to these guidelines.

The existing frameworks for determining the solicitation of financial services across borders have long been guided by criteria set by the European Commission, the Financial Conduct Authority (FCA), and the Bank of England, specifically concerning the banking sector. For

instance, the Commission's interpretative communication indicates that to locate where an activity is carried out, one must identify the "characteristic performance" of the service—the crucial supply for which payment is due. This is echoed in the EBA October 2019 report, which notes the challenges of pinpointing this characteristic performance in the era of digital and long-distance services. It suggests considering factors such as the physical location where the service's key performance occurs, whether the service is targeted at the host member state, the territorial scope within which the service is provided, and who initiated the service relationship. The complexity and lack of uniform EU regulations on whether online activities constitute cross-border services require that each case be assessed individually.

Moreover, under MiFID II, if a retail or professional client within the EU independently initiates a service from a third-country firm, the firm isn't required to seek authorization to operate. However, ESMA's January 2021 statement clarifies that solicitation or advertising by a third-country firm within the EEA does not qualify as client-initiated, affecting how services are legally classified and regulated. This underscores the nuanced nature of 'reverse solicitation' and the importance of accurately assessing solicitation activities to comply with regulatory expectations.

Under MiCA the position has been determined as follows: “Where a client established or situated in the Union initiates at its own exclusive initiative the provision of a crypto-asset service or activity by a third-country firm, the requirement for authorisation under Article 59 shall not apply to the provision of that crypto-asset service or activity by the third-country firm to that client, including a relationship specifically relating to the provision of that crypto-asset service or activity.”

Unlike traditional solicitation, where service providers actively seek clients, reverse solicitation occurs when the initiative to acquire a service stems solely from the client’s behalf. Such authorisation exemption is further clarified in Recital 75 of MiCA, where it states that MiCA “should not affect the possibility for persons established in the Union to receive crypto-asset services by a third-country firm on their own initiative”. In brief terms, the reverse solicitation regime established by MiCA comes down to whether the service can be seen as provided within the European Union, as well as depend on the extent to which EU based clients are directly solicited by the Crypto-Asset Service Provider (CASP).

The phrase 'own exclusive initiative' is subject to ambiguous and uncertain interpretation since MiCA refrains from offering a definitive description or elucidation of its intended meaning. The only reference to date is identified in the ESMA consultation paper published in accordance with Article 61(3) on the draft guidelines on reverse solicitation under MiCA, stating the following: “The client’s own exclusive initiative should be construed narrowly. The assessment should be a factual one”. The term, therefore, may be interpreted in a way that the client must, exclusively and without any external influence, solely signify that they intend to receive a specific service from a third-country firm. This term aims to eliminate the mere possibility of CASPs in any way

attempting to persuade or influence to receive the crypto-asset service. Though, the terms “own exclusive initiative” and the remaining part of Article 61 MiCA signify additional uncertainties revolving around the scope and content of the ‘marketing prohibition’ under Article 61 MiCA.

Apple’s “App Store Review Guidelines” (the “Guidelines”) available on the Apple App Store were recently updated and explain, inter alia, that they are designed to help developers/programmers understand the guidelines required to proceed through Apple’s App review process quickly. In relation to exchanges of cryptocurrencies, sub-clause 1.3.5(iii) of the Guidelines provides that: “Apps may facilitate transactions or transmissions of cryptocurrency on an approved exchange, provided they are offered only in countries or regions where the app has appropriate licensing and permissions to provide a cryptocurrency exchange. Section 5 of the Guidelines states that apps must adhere to all legal requirements in any location where they are made available. It emphasises the developers' responsibility to ensure their apps comply with all applicable local laws, not just the guidelines provided.

In practice, Apple will request the licensing status as a CASP in any store front that it is offered. They will typically halt and restrict any updates in the application from running until this has been provided. They may however accept individual legal assessments in respect of each jurisdiction through which the Application is active. This is of course subject to on-going reviews, updates and challenges. The most concrete example of this has been the Financial Promotion Rules in the UK. Post the introduction of the FinProm rules Apple will typically request evidence of FCA authorisation or evidence of the approval of the Application and the App Store wording as a Financial Promotion. They may also request direct confirmation from the FCA.

In the case of the EU, ESMA has been clear that even the geo-blocking of a website may be persuasive but not determinative in the assessment of whether business is being solicited from the EU. It is likely that Apple, and subsequently other application providers like Google will begin to form positions around this in the near future. The question is whether the act of downloading and using an application should be deemed to, within itself, constitute a financial promotion, regardless of the language, image or description accompanying the application. On this matter, participants of the roundtable unanimously agreed that this should not be the case.

During the roundtable, participants also discussed the complexities surrounding the provision of 'new services' by Third Country CASPs. These providers are generally restricted from marketing new types of crypto assets or services to existing clients. A variety of interpretive questions need to be carefully assessed to clarify these rules. The participants highlighted several key factors:

Firstly, if a client has already initiated engagement with a crypto-related service provider, there is generally an understanding that the provider might offer additional services over time. The introduction of new services under these circumstances is often and should not be considered solicitation, especially if the client has agreed to receive updates or new offerings as part of their initial contract.

Conversely, if a service provider actively markets new services directly to clients—through methods like targeted ads within the app, push notifications highlighting the new service, or direct emails—this could be seen as solicitation. This is because such direct promotion might be perceived as an invitation or inducement to engage in a new investment activity.

Furthermore, general updates within an app about new features or services, which do not directly target the client to undertake new investment activities, are typically not and should not be regarded as solicitation. The core of this distinction depends on how the updates are presented and whether they appear as general information or as an explicit encouragement to engage in specific investment activities.

Lastly, the introduction of entirely new services or assets that significantly differ from the initial engagement could necessitate a cautious approach. The participants highlighted that according to ESMA guidelines, if a third-country firm offers types of crypto-assets or services not originally requested by the client, this could be construed as solicitation unless it fits within what is considered the same type of service originally requested by the client.

Primary calls to action for Solicitation:

The primary calls to action for regulators regarding the solicitation of business under MiCA involve concrete steps to address ambiguities and inconsistencies in how digital services are regulated across the EU. These actions aim to:

- Form a working group to engage with major application storefronts, such as Apple's App Store and Google Play, to clarify and standardise the interpretation of solicitation in digital contexts. This group would focus on drafting a position paper that clearly defines when the language in these storefronts may constitute financial promotion or solicitation, aiming to establish exemption standards across all major platforms.
- Develop and Implement a Financial Services Test by designing a framework to distinctly differentiate between the solicitation tests under MiFID II and those under MiCA. This involves the industry proactively engaging in dialogue with regulatory bodies and submitting formal responses to the ESMA consultation to harmonise the varied tests for solicitation across different financial services frameworks within the EU.

For an overview of the event please visit: https://www.youtube.com/watch?v=v-onh05G10w

MICAR ROUNDTABLE EXPERT SERIES

BERLIN

The MiCAR Roundtable Expert Series is an initiative of Validvent, thinkBLOCKtank and siedler legal with the aim to increase legal certainty within the realm of the EU crypto markets. As a new regulatory framework, the application of MiCAR still raises numerous questions and as such the MiCAR Roundtable Series aims at facilitating expert discussions, resulting in public reports and specific calls to action. The roundtables will be held across Europe throughout the year 2024.

Following the March roundtable in London, on April 23rd, the second MiCAR Roundtable of the series was held in Berlin in cooperation with Berlin Partner, the EUBOF and INATBA.

The Berlin roundtable included a keynote from Joachim Schwerin, Principal Economist at the European Commission.

This roundtable counted with expert contributions of Joanna Rindell on NFTs; Luiza Castro and Alireza Siadat on grandfathering issues; Dr. Max Bernt on Crypto-asset classification; Daniel Resas around frontend providers for DeFi; Tiana Whitehouse on Reverse Solicitation; and Jörn Erbguth on transaction history for privacy coins.

This report aims to consolidate the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants or the respective rapporteur

siedler legal · thinkBLOCKtank · Validvent · BERLIN BERLIN PARTNER for Business and Technology · EUBlockchain Observatory and Forum · INATBA International Association for Trusted Blockchain Applications

1. NFTs: Regulatory Perspectives and Challenges

The discussion around NFT was led by Joanna Rindell, General Counsel at World of Women. The discussions centred on the need for precise definitions and clearer assessment criteria to prevent the misclassification of NFTs either as typical crypto assets under MiCAR or as financial instruments under MiFID.

The participants debated the application of MiCAR's broad language to NFTs, stressing the importance of a substance over form approach in their classification. This approach necessitates a detailed evaluation of each NFT's components—artwork, technical standards, and utility offered by the project to ascertain their collective and individual value contributions. It was noted that the uniqueness of the artwork and the specific utility provided, such as governance rights in a DAO, contribute significantly to the NFT's value, distinguishing it from standard financial instruments.

A major challenge highlighted was the ambiguity in current regulatory frameworks, which could lead to inconsistent interpretations across EU member states and potentially curb innovation. The lack of explicit assessment criteria risks erroneous classification of NFTs, potentially subjecting them to inappropriate regulatory burdens meant for more traditional financial instruments.

The roundtable reached a consensus on the necessity for clear, tailored criteria for NFT assessment, focusing on

- Artistic Uniqueness: Evaluations should consider the originality of the artwork, trait variations, the artist's reputation, and the artwork's cultural significance.
- Nature of Utility: Utilities should be assessed based on the type of benefits they provide — distinguishing financial from non-financial benefits. Utilities offering access to exclusive content or community benefits, like voting rights in a DAO, should indicate a non-financial utility, thus not classifying the NFT as a financial instrument.
- Market Dynamics and Trading Volume: Analysis should include a review of trading volumes over significant periods to discern the NFT's market stability and interest, preventing misclassification due to transient market activities.
- Issuance and Seriality: The definition of a 'large series' of NFTs needs clarity. While MiCAR suggests that issuing NFTs in large series implies fungibility, this should be one of several factors considered in the assessment.

Implementing these recommendations would enable a more accurate evaluation of NFTs, recognizing their unique characteristics and the complex interplay of their artistic and utility-based values. This approach aims to ensure that NFTs are regulated in a manner that acknowledges their distinct nature from traditional financial assets, thereby fostering a regulatory environment conducive to innovation while ensuring appropriate consumer protections. By establishing a

comprehensive framework for NFT assessment, regulators can better navigate the evolving landscape of digital assets, supporting innovation while safeguarding against potential market abuses and consumer risks.

Primary call to action for NFTs:
The primary call to action from the Berlin roundtable is to collaborate with the aim that regulators adopt and implement clear, detailed criteria for NFT classification that align with MiCAR's objectives. This involves: • Developing guidelines that accurately reflect the unique artistic and utilitarian aspects of NFTs. • Ensuring these guidelines are flexible enough to accommodate the diverse nature of NFTs and prevent their misclassification as traditional financial instruments. • Proposing these guidelines to the regulators involved.

2. Crypto-Assets Classification under MiCAR and MiFID II

The discussion around crypto-assets classification under MiCAR and MiFID II was led by Max Bernt, Managing Director, Europe at Taxbit. The discussions brought to light the absence of a universal definition of "financial instruments" in the EU, a situation that contrasts starkly with jurisdictions like the U.S. that employ the Howey test for clarity. This disparity has been exacerbated with the advent of MiCAR, prompting urgent questions about how crypto-assets should be categorised under both MiFID and MiCAR regimes.

A key area of concern is the handling of crypto-assets resembling derivatives but settling in unconventional forms, such as stablecoins. These assets pose unique challenges due to their ambiguous classification under existing frameworks. In response, ESMA has proposed guidelines suggesting that crypto-assets which represent contractual rights to underlying assets be classified as derivatives. This definition extends to assets whose values are tied to reference assets and involve financial settlements or deliveries of the underlying asset.

The roundtable recognized the need for a more nuanced regulatory approach to accommodate the complex nature of crypto-assets. Stakeholder responses advocate for regulatory flexibility, stressing the importance of substance over form in classification to avoid stifling innovation or enabling regulatory arbitrage.

To address these challenges, the roundtable emphasised several strategic recommendations:

Harmonisation across the EU is crucial, and while the introduction of a Howey-like test in the EU was debated, it was agreed that a more immediate and practical approach would involve establishing specific criteria based on the substantive qualities of tokens. These criteria should focus beyond the

mere "negotiability" of a token to include the intentions and functionalities outlined in its White Paper and the promises made by issuers.

Regulatory priorities should aim for clarity and certainty while fostering innovation. Regulators are encouraged to provide clear, accessible guidelines for National Competent Authorities (NCAs), which balance specificity with flexibility. This approach would ensure that the intrinsic qualities of tokens, especially those promising future returns or capital gains, are the primary factors in their classification.

An impact assessment is necessary to address the potential inconsistencies in how tokens are treated across different jurisdictions. The roundtable called for ESMA to ensure that a passport granted by one NCA is respected across all EU and EEA jurisdictions, and for the provision of operational definitions of negotiability and transferability with practical examples to aid NCAs.

These recommendations aimed to refine the regulatory landscape for crypto-assets, ensuring clarity and consistency while fostering an environment conducive to technological innovation and market stability.

Primary calls to action for Crypto-Assets Classification under MiCAR and MiFID II:

The primary call to action is to collaborate with the aim of regulators refining and clarifying the classification guidelines for crypto-assets within the MiCAR framework. This involves:

- Developing specific, substance-based criteria for crypto-asset classification that reflect the unique characteristics and functionalities of these assets.
- Supporting regulators to establish regulatory guidelines that are clear and tailored, allowing for flexibility in their application to accommodate the evolving nature of digital assets.
- Facilitating continuous dialogue and collaboration among NCAs and the crypto industry to harmonise regulatory practices and ensure that innovations in the digital asset space are supported rather than stifled.

3. Reverse Solicitation

The third topic of the Berlin Roundtable was presented by Tiana Whitehouse, Co-Founder & Managing Director of SWOT Team Consulting GmbH, focusing on the challenges posed by ESMA's Reverse Solicitation Guideline 1 under MiCAR Art. 61(3). According to the roundtable participants the current guidelines, considered overly restrictive, potentially misinterpret social and professional activities as solicitations, potentially stifling educational and collaborative efforts rather than merely regulating commercial endeavours.

The discussions delved into how ESMA's broad interpretation includes various activities—from road shows to

educational courses—as potential solicitation methods, thereby exposing participants, particularly third-country firms, to undue regulatory risks. The guideline could lead to unintended consequences, such as limiting educational and professional development activities that are crucial for informed industry engagement and innovation.

To mitigate these impacts, the roundtable proposed several solutions:

- Clarification of Purpose: It was suggested that ESMA should delineate more clearly between commercial solicitation and non-commercial activities like education and professional development. Providing explicit guidelines on what constitutes solicitation would help differentiate brand promotion activities from educational or collaborative interactions.
- Class Exemption: Introducing exemptions for non-commercial gatherings was discussed. This could involve specific categories for events like workshops, conferences, and academic meetings, which do not primarily serve commercial purposes but rather aim to foster industry knowledge and network building.
- Risk-Based Enforcement: Adoption of a risk-based approach to enforcement by National Competent Authorities (NCAs) would prioritise resources towards activities with higher risks of consumer harm rather than broad surveillance of all professional engagements.

Further discussions highlighted the potential negative implications of the current guidelines on international cooperation and discourse, crucial for advancing regulatory and technological understandings. The possibility of a labelling framework was also discussed, where events meeting specific non-commercial criteria could be recognized as exempt from solicitation categorization, aiding in clear compliance and fostering continued global dialogue.

Primary calls to action for Reverse Solicitation:

The primary call to action focuses on collaborating on refining ESMA's guidelines to prevent the overreach of reverse solicitation regulations into non-commercial, educational, or professional development activities. Industry stakeholders are urged to:

- Propose revised and clarified definitions within the guidelines to ensure a precise understanding of what constitutes solicitation, exempting inherently non-commercial activities explicitly.
- Propose a labeling system for events, providing a framework that clearly identifies and exempts non-commercial, educational, or policy-driven activities from being classified as solicitations.

- Encourage active dialogue between industry and regulators to develop practical, clear guidelines that support healthy industry evolution without compromising regulatory objectives or stifling necessary professional interactions.

4. Grandfathering: Crypto-asset offerings prior to 2025

The discussion on grandfathering, initiated by Luiza Castro from FiO Legal, delved into the critical transitional measures within the MiCAR framework. This discussion provided a detailed look at the grandfathering provisions essential for aligning existing operations with the new regulatory framework set to fully take effect after December 30, 2024.

The discussion started mentioning that MiCAR introduced a grandfathering regime affecting crypto-assets not classified as asset-referenced or e-money tokens, with the regulation becoming fully applicable in stages as outlined in Articles 149(2), (3), and (4). This transitional period allows entities time to align their operations with MiCAR's provisions, bridging the gap between the enforcement of MiCAR and their compliance.

The discussions highlighted that until December 30, 2024, crypto-assets already admitted to trading are exempt from MiCAR's new marketing communication rules. This provides a strategic window for entities to either conclude their marketing activities or ensure compliance with the impending regulations, suggesting a six-month transitional window into 2025 for additional adjustments.

The participants of the roundtable agreed on the following marketing communication challenges that will occur during the transitional period:

- Entities admitted to trading and publishing marketing communications before the deadline can temporarily avoid the new MiCAR standards. However, they must transition to compliance within a reasonable period, possibly six months into 2025.
- The responsibility for ensuring compliance in marketing strategies, especially in dynamic digital and social media campaigns, remains a significant challenge. These campaigns require meticulous planning to ensure that all content adheres to MiCAR standards post-deadline.
- The discussion also touched on the strategic opportunities and compliance risks associated with pre-deadline marketing, emphasising the importance of clear, strategic planning and the potential for regulatory scrutiny if reshared or reposted content fails to comply with new standards.

Based on those challenges, the participants highlighted some possible strategic and operational recommendations necessary to navigate the grandfathering provisions effectively.

For example, it was mentioned that entities should review and adjust their marketing strategies with the MiCAR timeline in mind, ensuring that communications set to extend beyond the 2024 deadline are compliant with new regulations.

Moreover, it was agreed upon by the participants that ongoing dialogue between regulators and industry stakeholders is crucial to clarify any ambiguities in transitional measures and ensure that the implementation of these rules does not disrupt the operational capabilities of crypto-related businesses.

Primary call to action for grandfathering rules under MiCAR:
The primary call to action from the Berlin roundtable on grandfathering rules under MiCAR encourages entities to proactively plan and adapt their strategies to align with the upcoming MiCAR regulations. This includes: • Developing detailed plans for transitioning marketing strategies to comply with MiCAR standards by the end of 2024. • Engaging in continuous dialogue with regulators to address and clarify transitional provisions, ensuring a smooth adaptation process for all stakeholders involved in crypto-assets trading.

5. Grandfathering: Art. 143 subsec. 3 MiCAR

Following the previous discussion on grandfathering, Alireza Siadat, Partner at Annerton, delved into the transitional regime outlined in Art. 143 para. 3 of MiCAR, which has raised significant concerns due to its ambiguous provisions.

This discussion focused on the challenges and ambiguities surrounding the transitional regime of Art. 143 para. 3 of MiCAR. This article allows crypto-asset service providers that were operational in compliance with applicable laws before December 30, 2024, to continue their operations until July 1, 2026, or until a decision on their authorization is made, whichever is sooner. However, Member States have the discretion to opt out of this regime or shorten its duration if their existing regulations are less strict than those proposed by MiCAR.

During the roundtable, concerns were raised about the clarity of the legislation, particularly the specific references to dates and the ambiguity around what qualifies as "services in accordance with applicable law." The discussions highlighted the need for greater transparency on how Member States will notify the Commission and ESMA about their implementation decisions, as well as the challenges CASPs face in navigating different national transitional regimes.

A significant part of the debate centred on the interpretation of "services in accordance with applicable law." There was a consensus that this should

include not only regulated CASPs but also those operating in areas not explicitly covered by current regulations, such as services related to utility tokens or portfolio management. This broader interpretation is crucial for those CASPs that are currently unregulated but still operate within the law.

The roundtable also stressed the importance of clear and harmonised guidelines from the NCAs and ESMA. These guidelines are essential for ensuring that CASPs can effectively plan their compliance strategies and for maintaining the integrity of the internal market. The discussion advocated for a proactive approach from NCAs, like Austria's FMA, which are already addressing MiCAR's implications, to lead by example and assist other Member States.

To conclude, the primary calls to action from the discussion emphasised the urgent need for regulatory clarity and a harmonised approach to the transitional regime. It was suggested that regulators quickly provide detailed guidelines on the application and scope of Art. 143 para. 3 to aid CASPs in their compliance efforts. Furthermore, there was a strong push for consistency across the EU to ensure that the transitional provisions support a unified regulatory approach and foster a stable environment for innovation in the crypto asset space.

Primary calls to action for Grandfathering: Art. 143 subsec. 3 MiCAR:

The primary call to action from the Berlin roundtable on the transitional regime under MiCAR is for regulators and industry stakeholders to collaborate closely to navigate the complexities introduced by Art. 143 para. 3. Interested industry players are encouraged to:

- Collaborate in order to jointly propose clear, detailed guidelines explaining the application and scope of Art. 143 para. 3. Those will help CASPs plan and adjust their operations in compliance with the new regulations.
- Explain to NCAs the importance of a unified approach to the transitional regime. To eliminate discrepancies could hinder the functioning of the internal market and avoid disadvantages to CASPs based on their jurisdiction.
- Create proactive support and guidance to CASPs, particularly those that are not fully regulated under current laws but are compliant with the broader legal framework. This support is crucial for helping these businesses transition smoothly into the regulatory framework established by MiCAR.

6. Transaction History for Privacy Coins.

The discussion, led by Jörn Erbguth from Geneva Macro Labs and the University of Geneva, focused on the complex requirements of MiCAR's Article 76 subsec. 3, which mandates the disclosure of "transaction history" for privacy coins. The current guidelines demand that trading platforms prevent the trading of crypto-assets with

anonymization functions unless the crypto-assets and their transaction histories can be identified by service providers.

The primary concern revolves around the interpretation of "their" in the regulation—whether it refers to the transaction history of the holder or to the crypto-asset itself, which could have changed hands multiple times. The roundtable debated the practicality and implications of each interpretation, emphasising the importance of clarity to prevent undue burdens on holders who may not have access to the full transaction history of their assets.

The conversation highlighted the GDPR implications, particularly the right to be forgotten, and how it conflicts with the permanent nature of blockchain records. Participants discussed how the integration of privacy by design in privacy coins could address these concerns by minimising the exposure of pseudonymous personal data.

The proposed solution focused on limiting the disclosure requirement to the transactions directly involving the holder, thereby aligning with the GDPR's principles and reducing the potential for unnecessary exposure of personal data. The discussion also touched on the technical solutions like differential privacy and decentralised IDs, which could help reconcile privacy concerns with regulatory requirements.
To enhance the practical application of Article 76 subsec. 3, the roundtable suggested that exchanges should only be required to identify the direct customer, the immediately preceding transaction, and the counterparties involved in that transaction. This approach would protect privacy while complying with AML directives, emphasising that only transactions above a certain threshold should be disclosed to exclude micropayments.

In conclusion, the discussion underscored the need for a balanced approach that respects both the privacy rights enshrined in the EU Charter of Fundamental Rights and the regulatory mandates aimed at preventing money laundering and other illicit activities. The roundtable urged that the use of privacy-enhancing technologies that respect privacy by design should not be blocked by extensive and disproportionate interpretation of the disclosure requirements for trading privacy coins.

Primary calls to action for Transaction History for Privacy Coins

The primary call to action from the Berlin roundtable on the transaction history of privacy coins emphasises the importance of this technology, which adheres to the data protection by design principle. Any regulatory approach must be feasible and proportionate. Disclosure requirements must not extend beyond the last transactions of the transacting party.

- The industry should emphasise the importance of this technology to meet the increasing demands for data protection and privacy. All transactions being

openly available on a public ledger must not become a de facto legal requirement of financial regulation.
- Encourage the adoption of technologies that enhance privacy while meeting regulatory requirements, such as differential privacy techniques and decentralised identity solutions.
- Advocate for policies and regulatory guidance that respect privacy rights while addressing regulatory concerns, ensuring that privacy coins can operate within legal frameworks without compromising fundamental rights.

7. Frontend providers for DeFi operators

The discussion led by Daniel Resas from Placehodlr centred on the intricate role of non-custodial frontends in decentralised finance (DeFi) under the Markets in Crypto-Assets Regulation (MiCAR). This conversation explored whether these frontend providers qualify as "operators" under MiCAR, shedding light on the nuanced regulatory landscape these entities navigate.

Non-custodial frontends enable users to interact with decentralised protocols without the service provider holding custody of the user's assets, setting them apart from custodial platforms. This distinction is crucial, as it introduces unique regulatory challenges, particularly concerning the potential misclassification of these frontends as operators, which would subject them to stringent regulatory standards not aligned with their operational realities.

The roundtable highlighted the ambiguity in legal treatment and its significant implications for the operation of platforms like Uniswap. These platforms exemplify the ongoing tension between decentralised applications and existing regulatory frameworks, emphasising the need for clarity in how regulations apply to non-custodial services to avoid stifling innovation.

Given that in most member states non-compliance with MiCAR by providing crypto-asset services without a required licence results in criminal charges, the conversation highlighted the principle of foreseeability in criminal law (nullum crimen sine lege certa) prohibiting an interpretation that goes beyond the wording of the specific crypto-asset services described.

Participants discussed the importance of distinguishing non-custodial providers from custodial services to preserve the integrity and innovative potential of DeFi platforms. They stressed the need for regulatory bodies to provide clear guidelines that accurately reflect the operational model of non-custodial frontends to prevent undue regulatory pressures.

The discussion concluded with several key takeaways:

- Regulatory Clarity: It is crucial for regulators to outline and communicate clear guidelines that recognize the unique operational models of non-custodial frontends, ensuring that these entities are not inappropriately burdened with regulations meant for traditional financial operators.
- Legal Risk Management: Non-custodial frontends must strategically manage legal risks by engaging proactively with regulators. This engagement will help foster a deeper understanding of decentralised technologies and mitigate risks associated with regulatory misclassification.
- Industry Advocacy: Stakeholders are encouraged to advocate for a regulatory approach that acknowledges the distinct characteristics of DeFi and non-custodial platforms. This advocacy should aim to shape regulations that support innovation while ensuring consumer protections and market integrity.

Primary calls to action for Frontend providers for DeFi operators

The primary call to action from this discussion is for stakeholders in the DeFi ecosystem to actively engage with regulatory bodies to ensure that the unique aspects of non-custodial frontends are understood and appropriately regulated. This includes:

- Efforts should be made to educate regulatory authorities about the fundamental operational differences between non-custodial frontends and traditional financial operators.
- Advocating for clear legal definitions and guidelines that reflect the non-custodial nature of these platforms, ensuring that regulations are both applicable and conducive to the growth of decentralised finance.
- Encouraging collaboration within the industry to present a unified voice in regulatory discussions, enhancing the effectiveness of advocacy efforts.

For an overview of the event please visit: https://www.youtube.com/watch?v=xJYgKmvlszw

Thank you to all the participants of the Berlin Roundtable: Alexander Harutunian (now with AML Incubator, formerly N26), Alireza Siadat (Annerton), Benedikt Faupel (Bitkom), Christopher Payne (Independent consultant), Daniel Resas (Placehodlr), Giti Said (Arweave), Gustav Hemmelmayr (Kilt protocol), Ilija Rilakovic (WALK Attorneys), Inbar Preis (DLNews), Jakob Zwiers (Berlin Partner), Jannick Piepenburg (tBt), Joachim Schwerin (European Commission), Joanna Rindell (World of Women), Johannes Anderl (Validvent), Jörn Erbguth (Head of Technology Insights at Geneva Macro Labs), Karan Aswani (Gnosis), Laura Kajtazi (Validvent), Luiza Castro Rey (FiO Legal, Partner | Head of Business and Web3, Lisbon), Mariana de la Roche (Validvent/INATBA/tBt), Max Bernt (Taxbit), Michal

Truszczynski (Bitpanda), Nina-Luisa Siedler (siedler legal/tBt), Patrick Hansen (Circle), Tiana Whitehouse, J.D. (Swot Consulting), and Willem Roell (De Roos Advocaat).

MICAR EXPERT ROUNDTABLE

VIENNA

20 May 2024

The MiCAR Roundtable Expert Series is an initiative of thinkBLOCKtank, Validvent and Siedler Legal with the aim to increase legal certainty within the realm of the EU crypto markets. As a new regulatory framework, the application of MiCAR still raises numerous questions and as such the MiCAR Roundtable Series aims at facilitating expert discussions, resulting in public reports and specific calls to action. The roundtables will be held across Europe throughout the year 2024.

Following the March roundtable in London and the April roundtable in Berlin, on May 20th, the third MiCAR Roundtable of the series was held in Vienna in cooperation with the European Commission and sponsored by Crystal Intelligence, AML Incubator and Bitpanda.
The Vienna roundtable commenced with a keynote from Joachim Schwerin, Principal Economist at the European Commission and included the expert contributions of Alexander Harutunia (AML Incubator) on token concentration and decentralisation; Hedi Navaza (Crystal Intelligence) on listing on non-EU exchanges in light of reverse solicitation; Oliver Völkel (SVLAW), on white paper exceptions; Philipp Bohrn (Bitpanda) on Austrian grandfathering issues; and Romena Urbonaite (Bitpanda) on market abuse monitoring.

This report aims to consolidate the insights from these discussions. Please note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants or the respective rapporteur.

Validvent siedler legal thinkBLOCKtank European Commission AML INCUBATOR bitpanda Crystal

1. **Decentralisation in the Context of MiCA**

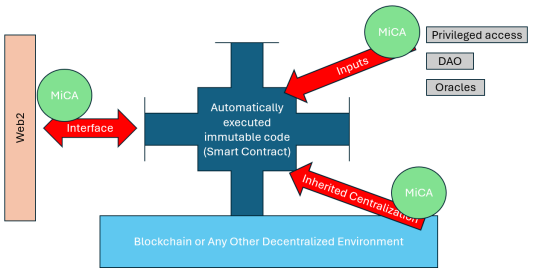
The roundtable discussion on decentralisation was led by Alexander Harutunia (AML Incubator) and it began by emphasising that Recital 22 of MiCA broadly characterises services provided in a fully decentralised manner as exempt from regulation. Yet, the absence of a formal definition for "decentralisation" presents a risk of varied interpretations, which could impact the operational dynamics across the crypto industry

The essence of decentralisation in crypto arises from eliminating central parties and achieving consensus on transaction records—a concept that remains partially unresolved despite significant advancements. While no ecosystem has reached complete decentralisation, certain segments operate autonomously, such as non-upgradeable smart contracts on robust blockchains.

Centralization Vectors in Decentralization

The discussion introduced the concept of centralization vectors to evaluate the level of control within decentralised systems, focusing on three primary areas:

1. **Smart Contract Access:** The control mechanisms, such as service accounts or kill switches, must be decentralised or under stringent regulatory oversight to prevent misuse.
2. **Web2 Interfaces:** Connections to conventional web applications introduce centralization. For example, the need for a website. Centralization is inherent in such applications, thus licensed agents are required at this junction.
3. **Platform Dependence:** The underlying platform's security and governance also influence the decentralisation of applications built upon it. Decentralised applications have no option to undo the damage caused by the protocol-level breach of rules. Licensed agents should maintain a register of platforms that can be considered safe for decentralised applications.



Discussion and Recommendations

Participants acknowledged the challenges of defining decentralisation due to the technological limitations of achieving a fully decentralised consensus. The discussion highlighted the need for clear regulatory guidance to distinguish between fully and partially decentralised services under MiCA. This distinction is crucial as only fully decentralised entities are exempt from regulation.

Examples from the industry, including the debate around the Tornado Cash mixer, illustrated potential oversights in recognizing centralization within ostensibly decentralised frameworks. These discussions pointed to the subtle nature of decentralisation, where indirect

controls could still exert significant influence over the operations.

The debate touched on the differentiation between disintermediation and decentralisation, noting that removing intermediaries does not inherently achieve decentralisation if indirect control mechanisms remain.

During the discussions it was proposed the idea of 'islands' that can be classified as fully decentralised when all three vectors of centralization are properly covered by licensing and standard-setting agents. Some round table participants found the claim about the lack of full decentralisation provocative and proposed examples of tangible sources of classification, such as identifiable commercial contracts or the Howey test.

The roundtable concluded by reminding that the criteria discussed to define decentralisation should aim to protect users by implementing safeguards against potential manipulation or control by central entities and recognize that effective systems do not always require centralization. This approach promotes a balanced framework where decentralised systems can operate within regulated environments to ensure both user safety and system integrity.

Primary call to action of Decentralization:

The roundtable concluded with a call for more rigorous research into decentralisation, suggesting a detailed examination of each centralization vector to develop comprehensive regulatory guidelines. Participants proposed the following actions:

- **Clarify Decentralisation Definitions:** Develop precise criteria that outline what constitutes full versus partial decentralisation, focusing on control and influence within the ecosystem rather than mere operational autonomy. Some of the criteria proposed where:

    a. Return on Investment or Fees: Assessing whether there are returns on investment or fees extracted from the system can indicate centralised control. Systems where returns or fees are funnelled in a manner that benefits a specific group disproportionately could suggest centralization.
    b. Token Concentration: The level of token concentration within a network can highlight potential control points. A higher concentration of tokens in the hands of few entities might lead to centralised decision-making power.
    c. Presence of a Service Provider: Identifying whether a distinct service provider exists who could manipulate or significantly influence the system's operation. The absence of such a provider can imply a more decentralised nature.
    d. Contractual Promises: Examining the presence of contracts that imply promises or obligations to deliver services. A decentralised system typically lacks a central authority responsible for fulfilling contractual promises, thereby reducing the potential for centralised control.#

- **Standardise Regulatory Approaches:** Implement a unified framework that addresses the nuances of decentralised technologies, ensuring that innovations are not stifled by overly broad or misapplied regulations.

- **Engage with Technological Developments:** Regulators should stay informed about technological advances to adapt regulatory frameworks in real-time, ensuring that they accurately reflect the current state of technology and its governance structures.

2. Reverse Solicitation Under MiCA

The topic of reverse solicitation led by Hedi Navaza (Crystal Intelligence) is a central point within the MiCA framework. The roundtable participants highlighted its significance in regulating interactions between the EU clients and third-country crypto-asset service providers. Under MiCA, reverse solicitation is strictly limited to situations where a service is initiated at the exclusive initiative of a client, a stipulation meant to be narrowly construed to prevent potential regulatory avoidance.

Reverse solicitation primarily affects third-country firms as per Article 61 of MiCA, explicitly prohibiting these firms from soliciting EU-based clients unless the service was requested without any prior solicitation. ESMA is mandated to issue guidelines to specify the scenarios that constitute solicitation and to outline supervisory practices to detect and prevent the abuse of this exemption. These guidelines are intended to ensure uniform application across the EU, preventing third-country firms from circumventing MiCA requirements through indirect solicitation methods such as online advertising, influencer partnerships, or visible sponsorship deals.

Discussion at the roundtable also covered the complexities involved with the listings of tokens by EU-based issuers on third-country exchanges. There is an ongoing concern about the extent of liability that EU issuers bear when their tokens are listed without their active involvement, emphasising the need for clarity on how these listings are treated under MiCA. This aspect of the regulation aims to safeguard EU clients from inadvertently engaging with non-compliant foreign entities, thus ensuring that only those services initiated by the clients themselves fall outside the direct scope of MiCA.

Further, the regulation stipulates that services provided by third-country firms to EU clients without any solicitation are not considered as being offered within the Union. However, if a third-country firm engages in any form of solicitation directed at EU clients, it must be authorised within the EU as a crypto-asset service provider. This includes activities conducted by entities closely linked to the third-country firm or any promotional efforts that target EU clientele.

Key Discussion Points

During the roundtable, a significant focus was placed on the complexities involved with the listings of tokens by EU-based issuers on third-country exchanges. This discussion highlighted concerns about the regulatory implications of such listings under MiCA. Specifically, the participants noted that in countries like Germany and the Netherlands, local supervisory bodies have previously considered that actively listing tokens on a third-country exchange subjects the issuer to the regulatory framework of the exchange's location. According to this interpretation, issuers would need to secure the same licences as the exchange itself.

However, questions remain about the liabilities of EU issuers when their tokens are listed without their active involvement. This scenario raises a crucial question: If the tokens of an EU issuer are listed on a third-country exchange without the issuer's explicit consent, is the issuer still liable under MiCA regulations? Roundtable participants debated this point, with some arguing that without direct involvement by the issuer in the listing process, holding them liable might extend the regulatory scope of MiCA unfairly.

To address these concerns, the discussion also touched on the necessity for clear guidelines from ESMA that define the responsibilities of EU issuers in the context of third-country listings. These guidelines would help ensure that EU issuers are not unduly penalised for listings that they do not control, while still maintaining the protective intent of MiCA for EU investors.

Primary call to action of Reverse Solicitation:

The primary calls to action from the roundtable emphasised the need for specific and detailed guidelines from ESMA to prevent the misuse of the reverse solicitation exemption and ensure fair competition:

- **Define Non-Solicitation Criteria:** Establish clear criteria that outline what does not constitute solicitation. This includes no active marketing, absence of sponsorship deals directly targeting the EU market, and not providing specific payment infrastructures or services tailored for EU customers.
- **Enhanced Supervisory Framework:** Develop a robust supervisory framework that includes monitoring and enforcement mechanisms to detect and deter any attempts by third-country firms to circumvent MiCA through indirect solicitation methods.
- **Clarification and Guidance:** Provide detailed guidance on the application of reverse solicitation rules, particularly in scenarios involving token listings by EU issuers on third-country exchanges, to clarify their obligations and liabilities under MiCA.

3. MiCA and the Requirement for Crypto-Asset Whitepapers

The discussion on the need for whitepapers under MiCA led by Oliver Völkel (SVLAW), focused on the distinction between offerors of crypto-assets and CASPs. MiCA outlines specific obligations for each, with offerors primarily addressed under Title II, which mandates the publication of a whitepaper when crypto-assets are offered to the public or admitted to trading. Notably, Title II specifies exemptions where a whitepaper is not required, such as offers directed at fewer than 150 persons per Member State or offers that do not exceed 1 million EUR over 12 months.

On the other hand, Title V, Chapter 2 of MiCA places obligations on CASPs, particularly under Art 66 (3), which requires CASPs to provide their clients with hyperlinks to any whitepapers associated with the crypto-assets they service. This stipulation aims to ensure that clients are fully informed of the risks involved in crypto-asset transactions. The roundtable discussion raised critical questions about the intersection of these requirements, particularly what CASPs should do if no whitepaper exists due to the exemptions specified in Art 4.

An initial interpretation suggested that if a whitepaper is not mandated under Art 4, then CASPs are not required to provide a hyperlink under Art 66 (3). However, this was challenged by some of the participants with the argument that the legislative intent of Art 66 (3) is to warn clients about risks, implying that CASPs need to find a way to fulfil this obligation, possibly by relying on voluntarily published whitepapers, even if third-party.

The conversation also touched upon the potential discrepancies in MiCA's language versions, with the English text appearing clear but other versions allowing room for different interpretations. This linguistic variation could lead to inconsistencies in regulatory compliance across Member States.

The roundtable concluded that while CASPs might use third-party whitepapers to meet their obligations, this approach raises practical and regulatory challenges, especially when no whitepaper is available. The necessity for explicit regulatory guidance to clarify these obligations was unanimously agreed upon, highlighting the need for a balance between compliance and protecting investor interests.

Key Discussion Points

There were some critical questions and topics raised during the roundtable discussion regarding the absence of whitepapers due to exceptions specified in Art 4 of MiCA centred on several key issues:

- Obligation of CASPs: The main question centred on the obligations of CASPs when there is no whitepaper due to exemptions. The roundtable emphasised that despite the absence of a whitepaper, CASPs are still required to inform their clients about the risks associated with the crypto-assets. It was suggested that CASPs might consider using alternative informational resources or

third-party whitepapers to fulfil this requirement.

- Scope of CASP Responsibilities: Discussion explored the extent of responsibility CASPs have in ensuring the availability of whitepapers. The consensus was that while CASPs are not responsible for creating whitepapers, they must ensure that sufficient information is available to clients, aligning with MiCA's intent to protect investors.
- Legal Interpretation and Compliance: There was a debate on how to interpret the legal texts, especially concerning whether CASPs are still required to provide links to whitepapers that technically do not need to exist according to certain exemptions. The roundtable called for regulatory clarity, noting that the current language could lead to varied interpretations and potential compliance issues across Member States.
- Risk Warning Requirements: Given that Article 66(3) is designed to ensure clients are aware of the risks associated with crypto-assets, the roundtable discussed what alternative measures CASPs could take to fulfil this requirement when no official whitepaper is available. It was agreed that CASPs should develop comprehensive risk disclosure policies that do not solely rely on the existence of a whitepaper, ensuring that all clients receive adequate risk information.
- Practical Implementation Challenges: The practicalities of how CASPs can ensure compliance when dealing with exempted crypto-assets were also a topic of concern. The roundtable acknowledged the challenges CASPs face and suggested that flexibility in regulatory approaches could help address these issues effectively.
- Use of Third-Party Whitepapers: The feasibility of using third-party whitepapers to fulfil regulatory obligations was discussed. While third-party white papers could be a viable option, the roundtable highlighted the need for these documents to meet certain standards of reliability and relevance to be considered valid under MiCA regulations.

These critical points reflect the complexity of implementing MiCA regulations in scenarios where the traditional requirement of a whitepaper does not apply, highlighting the need for clear guidance and practical solutions for CASPs.

Primary call to action Requirement for Crypto-Asset Whitepapers:

The primary calls to action are intended to enhance understanding and compliance with MiCA regulations, ensuring that both crypto-asset offerors and service providers operate within a clear, fair regulatory framework that safeguards investor interests.

- **Establish Clear Guidelines for CASP Compliance:** Regulators should provide explicit guidelines that detail how CASPs can comply with Art 66 (3) in situations where no whitepaper exists due to exemptions. This should include

criteria for acceptable alternatives to whitepapers, such as third-party documents or comprehensive risk disclosure statements developed by CASPs themselves.

- **Define Parameters for Third-Party Whitepapers:** ESMA and other regulatory bodies need to specify the conditions under which third-party white papers can be used to fulfil regulatory requirements. These standards should ensure that third-party documents are up-to-date, factually accurate, and provide a transparent analysis of risks similar to what would be expected in a directly issued whitepaper. Additionally, these documents should include verifiable sources and clear documentation of methodologies used in their preparation, ensuring that they meet the informational and regulatory standards set forth by MiCA.

- **Issue Directives on Risk Disclosure:** Given the critical role of informing clients about risks, regulators should issue directives that outline how CASPs can develop their own risk disclosures in the absence of a whitepaper. These directives should guide CASPs on the essential information to be included and the format to ensure comprehensiveness and clarity.

- **Support Mechanisms for CASPs:** Authorities should develop and implement support mechanisms that assist CASPs in accessing reliable third-party documents or in creating their own informational resources that comply with MiCA's requirements. This could include a regulatory-endorsed repository of approved third-party white papers or a toolkit for creating compliant risk disclosures.

- **Clarification of Exemption Implications:** Regulators should clarify the implications of whitepaper exemptions under MiCA, specifically addressing the responsibilities of CASPs when no whitepaper is required for a crypto-asset. This should aim to eliminate ambiguity and ensure that all CASPs understand their duties under the law. Examples of such clarifications could include specific guidelines on how CASPs should provide risk disclosures in the absence of a whitepaper, such as through standardised risk warning statements or alternative documentation that outlines the crypto-asset's characteristics and potential risks. Additionally, it should be clear under which conditions such as small-scale offerings, offerings to qualified investors, or utility token distributions, the exemptions apply and how CASPs should proceed in each case.

- **Facilitate Regulatory Alignment Across EU Member States:** Regulators should work to standardise the interpretation and application of MiCA provisions regarding whitepapers across all EU languages and jurisdictions to prevent disparities in compliance and enforcement.

4. Grandfathering in Austria

The topic of grandfathering in Austria was led by Philipp Bohrn, (Bitpanda), and it provided a detailed overview of the recently published national Austrian laws transposing MiCA regulation. The discussion primarily focused on the complexities and ambiguities surrounding the application of grandfathering provisions for CASPs under the new MiCA framework.

According to the roundtable the scope of the grandfathering rules for CASPs in Austria is relatively unclear. The draft of the national law implementing MiCAR (MiCAR VVG) was only recently published, raising questions about the applicability of these provisions.

Austria has implemented a broad scope of services under FM-GwG based on the FATF proposal, including transfer, swap, and other financial services, which extends beyond the scope of AMLD5. However, new services under MiCAR, such as advice and portfolio management, have not been regulated previously, leading to uncertainty about whether grandfathering rules apply if these services were not registered under AMLD5. Additionally, there is ambiguity in how services under AMLD5 translate into MiCAR services. The current national law in Austria lacks detailed provisions on this matter, and it remains unclear how long the implementation phase (Art 143 (3)) of MiCA will be, though it seems to be heading towards a 12-month period according to the MiCAR VVG draft. Furthermore, the process for evaluating whether a crypto-asset is already listed on a trading platform is uncertain, especially since no trading platforms are yet licensed under MiCAR.

Another concern is the handling of EMTs and ARTs if the national law is not in place, as the NCA has not been defined, and the timeline for public consultation is short. This lack of clarity extends to whether third-party offerings of assets would obligate issuers or the entire market to provide documentation under the grandfathering provisions.

Key Discussion Points

The discussion began by examining whether CASPs could continue their activities under the grandfathering provisions if they were not registered under AMLD5 but are now providing services regulated under MiCAR. In summary for the roundtable participants currently it seems unclear:

- if the grandfathering rules apply also if a CASP has not been registered under national Austrian laws transposing AMLD5;
- how the services under AMLD5 translate into the crypto asset services defined by MiCAR;
- what the scope of other provisions of grandfathering are - e.g. how to evaluate if a crypto-asset is already listed on a trading platform if there is no trading platform yet licensed under MiCAR.

Regarding the first point, the roundtable participants agreed that registered VASPs should be broadly covered by the grandfathering rules to ensure regulatory continuity.

When it comes to AMLD5, the participants explored the translation of services under AMLD5 to MiCAR and whether new services like advice, previously unregulated, would be

included. Participants emphasised the need for a broad interpretation to prevent disruption of services.

Regarding the third point, the roundtable also debated how to evaluate if a crypto-asset is already listed on a trading platform when no platforms are yet licensed under MiCAR. In this point, it was concluded that trading platforms should be deemed compliant with grandfathering provisions if they meet the requirements outlined in Art 143 (2) of MiCAR.

There was a consensus on the urgency for Austria to adopt national laws before MiCA became applicable in July 2024 to avoid regulatory gaps, particularly concerning stablecoins and EMTs/ARTs. The roundtable stressed the importance of a clear and timely legislative process.

Primary call to action Requirement for Grandfathering in Austria:

The primary calls to actions on the grandfathering in Austria were

- **Provide Detailed Guidelines on Grandfathering Scope:** Regulators should issue comprehensive guidelines that clarify the specific services and entities covered under the grandfathering provisions. This should include a detailed mapping of how services previously regulated under AMLD5 translate into MiCAR services, ensuring that no currently compliant CASPs are inadvertently excluded.

- **Establish a Simplified Transitional Procedure:** Implement a clear process for transitioning to MiCAR compliance, especially for services that were not previously regulated. This should involve clear criteria for determining eligibility for grandfathering and simplified application procedures to reduce administrative burdens on CASPs.

- **Define Criteria for Crypto-Asset Listings:** Develop specific criteria for assessing whether a crypto-asset is already listed on a trading platform, considering the current lack of licensed platforms under MiCAR. These criteria should include verification of trading activity, recognition by established industry sources, and adherence to preliminary regulatory standards to ensure the asset's legitimacy and market acceptance.

- **Implement Provisional Measures for Stablecoins and ARTs:** Establish interim regulatory measures for EMTs and ARTs to ensure continuous oversight and compliance until the full adoption of national laws. This could include temporary registration requirements or provisional guidelines to manage the regulatory gap effectively.

In general the participants agree that it will be relevant to strengthen collaboration between industry stakeholders and the FMA to ensure that all regulatory requirements are clearly communicated and understood. Regular updates, workshops, and consultation sessions should be conducted to address any emerging issues and provide ongoing support to CASPs during the transition period.

5. **Market abuse monitoring requirements and inside information disclosure under MiCAR versus MiFID II**

The discussion on market abuse monitoring requirements and inside information disclosure was led by Romena Urbonaite (Bitpanda). The focus was on the challenges posed by MiCAR's requirements, which draw inspiration from Regulation 596/2014 (MAR).

Market abuse requirements under MiCAR will apply to a broad range of participants, including validators and other entities typically outside MiCAR's scope. The discussion aimed to address the uncertainties and practical implications of these requirements, especially concerning their application to DeFi.

MiCAR's market abuse provisions are extensive, requiring all persons involved in unlawful activity, including those professionally arranging transactions, to detect and prevent market abuse. However, MiCAR does not define what constitutes "persons professionally arranging or executing transactions in crypto-assets," meanwhile MAR provides a definition. This lack of clarity raises concerns about the scope of the regulation, particularly for entities like validators and those involved in DeFi. Additionally, the definition of "admission to trading" remains ambiguous, leading to questions about whether it includes trading platforms outside the EU.

Key Discussion Points

The roundtable participants discussed several critical issues, including the scope of market abuse requirements, the definition of relevant market participants, and the implications for inside information disclosure.

The main concern was the broad application of market abuse requirements to a wide range of participants. The roundtable emphasised the need for clear guidelines from regulators to define the scope of these requirements, particularly for entities like validators and those involved in DeFi. It was noted that MiCAR's market abuse requirements are inspired by MAR and will apply to all persons engaging in unlawful activity, extending to validators and potentially DeFi platforms.

The discussion around the definition of market participants highlighted the ambiguity surrounding the definition of "persons professionally arranging or executing transactions in crypto-assets." Recital 2 of ESMA draft RTS provides defines such persons and expands the scope by including all types of crypto-asset service providers which are not included in case of investment firms. However, participants agreed that regulators should provide a clear and comprehensive definition and stick to the MiCA scope to ensure consistent application of the rules.

Moreover, the scope of the term "admission to trading" was debated, with participants questioning whether it applies only to EU trading platforms or includes those in other jurisdictions. The roundtable concluded that regulators should clarify this term for the market to prevent different interpretations across the market.

Furthermore, the requirements for disclosing inside information were discussed, particularly the new means of disclosure, such as social media, and the

broader range of individuals covered by these requirements. Participants stressed the need for clear guidelines on how to handle inside information in the context of modern communication methods. Unlike MAR, MiCAR does not require companies to maintain insider lists, leading to potential challenges in ensuring compliance. Without insider lists, it becomes more difficult to track and monitor who has access to sensitive information, increasing the risk of insider trading. Additionally, the absence of these lists complicates the ability of regulators to investigate and enforce actions against market abuse, as there is no clear record of individuals who had access to inside information.

Lastly, regarding monitoring and enforcement, the roundtable addressed the challenges of monitoring market abuse in the context of DLT and the potential need for specialised tools and departments within exchanges to handle these requirements. The participants emphasised the importance of systemic enforcement by regulators to ensure compliance. The discussion also covered the necessity of providing suspicious transaction reports (STORS) and the legal basis for reporting such transactions.

Primary Call to Action for Market Abuse Monitoring Requirements and Inside Information Disclosure

The primary calls to action from the roundtable focused on providing concrete steps for regulators to address the identified issues:

- **Clarify the Scope of Market Abuse Requirements:** Regulators should explicitly define "persons professionally arranging transactions' within MiCA, aligning it with the scope of MiCA. This definition should ensure clarity on which parties are included, preventing unnecessary extension of scope to entities or individuals providing certain crypto asserts services (like exchange of crypto assets and portfolio manager) and validators and miners.

- **Clarify the Scope of "Admission to Trading":** Regulatory authorities need to specify whether "admission to trading" includes markets outside the EU. Clear criteria should be established, potentially considering the regulatory status of the trading platforms and the jurisdiction in which they operate, to ensure uniform understanding and application of MiCA's provisions.

- **Establish Monitoring and Reporting Protocols for STORS:** Create comprehensive protocols for the submission of Suspicious Transaction and Order Reports (STORS). These protocols should include specific instructions on identifying and reporting suspicious activities, with a focus on mitigating risks associated with Maximum Extractable Value in blockchain transactions.

Thank you to all the participants of the Vienna Roundtable:

Alexander Harutunian (AML Incubator), Andelika Schiller (Bitfly), Artem Semko (Crystal Intelligence), Biyan Mienert (LUKSO), Christian Steiner (Bitpanda), Emanuel Sanchez de la Cerda (Bitbuy), Esen Esener (Lido), Fabian Schinerl (University of Vienna), Georg Brameshuber (Validvent), Hedi Navazan (Crystal Intelligence), Joachim Schwerin (European Commission), Klaus Pateter (CMS), Lavan Thasarathakumar (GDF), Laura Kajtazi (Validvent), Mariana de la Roche (Validvent/tBt), Matthias Bauer (Chainalysis), Matthias Lehmann (University of Vienna), Max Bernt (Taxbit), Michał Truszczyński (Bitpanda), Nicolette Brown (Crystal Intelligence), Nina-Luisa Siedler (siedler legal/tBt), Oliver Völkel (SVLAW), Philipp Bohrn (Bitpanda), Ralph Rirsch (Kraken), Raphael Toman (Brandl Talos), Romena Urbonaite (Bitpanda), Tibu Sanz (Crystal Intelligence), and Tigran Rostomyan (AML Incubator).

For an overview of the event series, please visit:
https://validvent.com/expert-series/
https://www.siedler.legal/micar

Validvent siedler legal thinkBLOCKtank European Commission AML INCUBATOR bitpanda Crystal

MICAR ROUNDTABLE EXPERT SERIES

Brussels

The MiCAR Roundtable Expert Series is an initiative of Validvent, thinkBLOCKtank and siedler legal with the aim to increase legal certainty within the realm of the EU crypto markets. As a new regulatory framework, the application of MiCAR still raises numerous questions and as such the MiCAR Roundtable Series aims at facilitating expert discussions, resulting in public reports and specific calls to action. The roundtables will be held across Europe throughout the year 2024.

Following the roundtables in London, Berlin and Vienna the fourth roundtable was held in Brussels in collaboration with APCO and Crystal Intelligence and with the support of the Web3 Foundation

The Brussels roundtable included a keynote from Peter Kerstens, Advisor on Technological Innovation and Cybersecurity at the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union and Joachim Schwerin, Principal Economist at the European Commission.

This roundtable counted with expert contributions of Beata Sivak on white papers; Romena Urbonaite on supervision under MiCAR and Roeland Van der Stappen on reverse solicitation.

This report aims to consolidate the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants or the respective rapporteur.

siedler legal · thinkBLOCKtank · Validvent · apco · Crystal · European Commission · web3 foundation

1. Disclosures & Whitepapers

The topic of disclosures and whitepapers under MiCA, presented by Beata Sivak, Government Relations & Policy Head, EMEA at Kraken, focused on the various challenges the industry faces regarding the scope, timelines, and liabilities attached to these requirements. MiCA outlines specific disclosure requirements related to crypto-assets, including environmental impacts (Article 66(5)) and more comprehensive whitepaper requirements (Article 6). The key issues highlighted were:

1. Scope: While the scope is clear for stablecoins, questions arise regarding decentralised assets and assets with no issuer. There is a concern that multiple disclosures or whitepapers produced by different market players for a single asset could confuse customers.
2. Timelines: Assets listed before December 30, 2024, benefit from a three-year grandfathering period, but newly listed assets require an immediate whitepaper. This discrepancy could create a bottleneck. Additionally, environmental disclosures are required earlier than whitepapers, raising concerns about feasibility and data reliability.
3. Liability: The liability primarily lies with the preparer or writer of the whitepaper, raising doubts about the practicality of reusing whitepapers with written consent. MiCA allows third parties to prepare whitepapers but does not address the economics of such arrangements, questioning the viability of a healthy vendor market.

The initial proposed solution was that the authorities could issue detailed guidance on the scope and make the process transparent to prevent duplication of whitepapers notified to NCAs and communicated to ESMA. Moreover, it was suggested that the environmental disclosures should be delayed until December 2027, aligning with the whitepaper mandate for all assets.

Key Discussion Points:

During the roundtable discussion, it was emphasised that MiCA is crucial for bringing digital asset companies into a regulated environment, which is beneficial for standardising digital asset management within the real economy. Participants noted that while MiCA may not be the first to require disclosures, it demands a higher level of detail and complexity. Challenges in complying with new disclosure requirements were outlined, particularly given the complexity and volume of digital assets managed.

The need for detailed information in white papers for specific digital assets was emphasised, highlighting the requirement for platforms to disclose the environmental impact of each asset on their websites. This adds complexity to compliance efforts. Comprehensive whitepaper disclosures are mandatory by 2027, posing a significant preparatory burden despite the time allowance. Participants expressed the need for more

detailed guidance on the implementation timeline, especially concerning the preparation and submission of white papers and environmental disclosures. The responsibility for the contents of the white paper lies with the entity writing it, and this responsibility cannot be transferred to those who merely read or use the white paper. The liabilities associated with the white papers are strictly tied to their authors.

There was a common agreement on the need for additional regulatory guidance to address ambiguities in the scope and responsibilities associated with MiCA. Engaging more actively with academic and research institutions to develop a standardised methodology for assessing the environmental impact of cryptocurrencies was suggested. Participants also discussed pooling resources from various blockchain foundations to fund research into the environmental impact of digital assets, leading to a sustainable, industry-wide standard.

The Cambridge Energy Consumption Index for Blockchain was mentioned, which provides data on major cryptocurrencies but lacks coverage for the broader spectrum of digital assets. Advocacy for a new, comprehensive index providing detailed environmental impact data for a wider array of cryptocurrencies, potentially spearheaded by European institutions, was discussed. The requirement for environmental impact disclosures is crucial but challenging due to the diverse nature and operational specifics of different cryptocurrencies. Concerns about inconsistencies between different national regulatory frameworks within the EU could lead to confusion and compliance difficulties for companies operating across borders.

Any crypto asset distributed within the EU needs to have a white paper, except for those without a formal issuer like Bitcoin. White papers must clearly state who is issuing the asset and what the asset is, with the issuer liable for the accuracy of the information provided. Discussions highlighted the need to integrate crypto regulations with broader environmental sustainability goals. The ongoing discussions aim to translate regulatory requirements into practical actions that companies can realistically implement.

Primary call to action for Disclosures & Whitepapers:

The primary call to action from the Brussels roundtable involved:

- **Establish Clear and Detailed Definitions:** Regulators should setting standards for the depth and breadth of information required, ensuring that whitepapers provide comprehensive, relevant data without overwhelming customers with duplicative or conflicting information, specially for decentralised assets.
- **Develop a Liability Framework for Whitepapers:** Authorities should establish clear guidelines on the liability associated with whitepapers, distinguishing

between the responsibilities of the preparers and those who use the whitepapers. This framework should include mechanisms for accountability and recourse in cases of misinformation or omission, ensuring that the preparers are held responsible for the content.

- **Standardise Third-Party Whitepaper Preparation:** Regulators should create standards for third-party preparation of whitepapers, ensuring these documents meet the required accuracy, reliability, and comprehensiveness. This could include setting up a certification process for third-party vendors and creating a repository of approved providers to help CASPs easily access reliable whitepaper preparation services.
- **Implement a Streamlined Notification System:** Establish a system for the notification and dissemination of whitepapers to NCAs and ESMA, reducing duplication and ensuring that all relevant parties have access to the same information. This system should include a centralised database accessible to all stakeholders, providing a single source of truth for whitepaper information.

2. Supervision under MiCA: Significant Issuers and CASPs

The topic of supervision under MiCA, presented by Romena Urbonaite from Bitpanda, focused on the complexities and challenges of ensuring harmonised supervision across EU member states. MiCA introduces a dual supervision regime for issuers of significant ARTs and EMTs, involving both national and EU-level oversight. This regime aims to address systemic risks but also presents several practical and regulatory challenges, such as possible re-assessments. .

The primary issue regarding supervision is the lack of harmonisation in supervision practices across EU member states. Factors contributing to this include varying capabilities of national competent authorities, differences in organisational structures, and diverse supervisory powers, different level of administrative penalties. The dual supervision regime for significant ARTs and EMTs aims to mitigate systemic risks, but the criteria for significance and the lack of reporting requirements for CASPs and issuers introduce further complexities, such as requests for ad-hoc reporting, different national requirements)

Key Discussion Points:

The roundtable discussion highlighted several key points regarding the implementation and effectiveness of MiCA's supervision framework. Participants emphasised the importance of supervisory convergence, with ESMA playing a crucial role in coordinating efforts among national authorities. There was a focus on the challenges and importance of supervisory convergence across the EU to maintain a harmonised regulatory environment. The discussion centred on how ESMA and national authorities might handle the supervision of significant CASPs. The potential shift towards more centralised EU-level supervision was debated, considering its effectiveness compared to national-level oversight.

The variability in supervision practices was noted, as EU competent authorities have diverse opinions, leading to different supervisory approaches. This variance affects the consistency of market regulations across the EU, allowing market participants to exploit the most favourable jurisdictions.

Moreover, MiCA's dual supervision model for significant ARTs and EMTs adds a layer of complexity. The roundtable discussed that the criteria for determining significance, such as having more than 15 million active users for CASPs, are not well-calibrated because they do not adequately reflect the systemic importance of the entities and could lead to inconsistent regulatory oversight. Participants noted that currently, there are no extra obligations for significant CASPs. However, they emphasised that if dual supervision is implemented for these entities, the regulation must be refined to ensure it only includes CASPs that are systemically important.

The lack of standardisation in applying supervisory measures and penalties across member states was also discussed. Participants pointed out that this can lead to inconsistent enforcement and varying degrees of compliance. There is a need for standardised supervisory measures and penalties across member states. The current lack of harmonisation can result in fragmented enforcement and varying degrees of compliance. The fragmented approach to assessing the reputation of qualifying shareholders and management, which varies significantly across member states, was also highlighted.

MiCA does not mandate regular reporting from issuers and CASPs, instead allowing national authorities to request information on an ad hoc basis. This could be burdensome for CASPs, who may be unprepared for unexpected information requests. The participants discussed the practical difficulties of implementing MiCA, particularly the varied interpretations and applications by different member states. This includes how significant market players are regulated and supervised. There was speculation about future revisions to MiCA, addressing changes that might be necessary as the digital asset market evolves and the regulatory landscape matures.

Concerns about the “passporting” system, which allows firms regulated in one member state to operate across the EU without needing further authorization, were discussed. The discussion covered the risks of regulatory arbitrage, where firms might choose to base operations in member states with more lenient regulatory environments. A proposal was made to harmonise sanctions and penalties across the EU to avoid discrepancies that could lead to uneven enforcement and compliance challenges. Issue of “reverse solicitation”, where services are marketed to clients in jurisdictions without the provider seeking local authorization, were addressed. This includes how different national regulations and practical enforcement of the requirements might affect the uniform application of MiCA.

The potential for regulatory arbitrage was discussed extensively, with concerns about how differing national interpretations of what constitutes a security versus a crypto asset could

impact the uniformity and effectiveness of MiCA. The conversation underscored a broad consensus on the need for more robust, coherent, and harmonised regulatory frameworks to manage the complexities of crypto markets effectively. Participants expressed a desire for clearer guidelines from ESMA to aid in consistent application and enforcement of MiCA across member states. There is an ongoing debate about the balance between national sovereignty in regulatory matters and the benefits of centralised EU-level supervision, highlighting the delicate interplay between local autonomy and EU-wide regulatory goals.

The primary call to action for supervision under MiCA emphasised the need to establish standardised supervisory practices and harmonise administrative penalties across all EU member states to ensure a level playing field. This includes developing specific criteria for assessing the reputation of qualifying shareholders and management bodies and implementing these standards through regulatory technical standards rather than guidelines. Practical cooperation among national competent authorities should be strengthened, with ESMA or EBA taking a leading role in ensuring supervisory convergence. This could include facilitating regular training and workshops to align supervisory practices and improve communication channels between national authorities. Introducing mandatory regular reporting requirements for issuers and CASPs to provide national competent authorities with consistent and timely information was recommended. This will help prevent the ad hoc nature of current information requests and ensure better preparedness among market participants.

The need to reevaluate and refine the criteria for determining significant CASPs to ensure that only systemically important entities are subject to dual supervision was also highlighted. This includes considering additional factors beyond the number of active users, such as market impact and transactional volume. The discussion suggested considering implementing a centralised supervision model for major global players and significant market participants to ensure consistent regulatory oversight and address potential systemic risks. This model should include clear guidelines on the roles and responsibilities of national and EU-level authorities. These actions aim to create a more coherent and effective supervisory framework under MiCA, fostering a stable and transparent crypto asset market within the EU.

The participants considered that the regulator should provide comprehensive guidance on the practical implementation of MiCA's supervisory provisions. This should cover the classification of crypto assets, the responsibilities of significant entities, and the specific requirements for compliance, helping to ensure a uniform application of the regulations. Moreover, the NCAs and regulatory authorities should develop mechanisms to prevent regulatory arbitrage, ensuring that entities cannot exploit discrepancies between national regulations. According to some of the participants this could include stricter passporting rules and closer monitoring of cross-border activities.

One of the discussions at the roundtable also addressed the issue of passporting a MiCA licence from one jurisdiction to another. In particular, the concern was

about how a certain asset might be classified differently in various jurisdictions—such as being considered a utility under MiCA in one country but a security under MiFID in another. The discussion emphasised the need for clarity in ensuring that once a MiCA licence is passported, the asset should maintain its classification across all jurisdictions to avoid regulatory confusion. It was noted that the regulator should ensure that once a MiCA licence is passported, the classification of assets remains consistent across jurisdictions. This could involve providing clear guidelines on how assets should be treated when moving from one regulatory framework to another, particularly in cases where assets might be considered utilities in one country and securities in another.

Primary Call to Action for Supervision under MiCA:

The primary calls to action from the Brussels roundtable on the topic of supervision under MiCA emphasise practical and concrete steps that regulators can take to ensure a harmonised and effective supervisory framework. The industry urges regulators to:

- **Harmonise Supervisory Practices:** Regulators should work towards fully harmonised supervision practices across all EU member states. This includes standardising administrative penalties, supervisory powers, and the interpretation of key regulatory provisions to prevent regulatory arbitrage and ensure a level playing field.
- **Establish Centralised Supervision for Systemically Important Entities**: Consider centralising supervision for systemically important CASPs and significant issuers of ARTs and EMTs at the EU level, possibly under the oversight of ESMA, EBA, or EIOPA. This would ensure more consistent and rigorous supervision of major market players.
- **Improve Criteria for Significance:** Refine and better calibrate the criteria for determining significant CASPs. This could involve incorporating additional factors such as market impact, transaction volumes, and interconnectedness with other financial systems, beyond just the number of active users.
- **Standardise Reporting Requirements:** Implement clear and consistent reporting requirements for CASPs and issuers across all member states. This should include regular, standardised reports rather than ad hoc information requests, to reduce the burden on entities and ensure timely and accurate data for regulatory oversight.

3. Reverse Solicitation Requirements

The discussion on reverse solicitation requirements under MiCA was led by Roeland Van der Stappen, Deputy Director and Head of Policy and Advocacy at the Swiss Finance Council. The primary focus was on the necessity of ensuring that EU consumers engage with CASPs authorised in the EU. This necessity arises from the concern that

certain third-country CASPs may operate with limited or no regulation.

MiCA's stringent reverse solicitation requirements aim to prohibit third-country CASPs from soliciting clients in the EU. ESMA's task was to modernise the concept of marketing, considering technological advancements and the current methods of crypto asset promotion, such as social media and sponsorship deals. Consequently, ESMA's draft guidelines interpret solicitation broadly, potentially prohibiting brand-building marketing even when it is not directly linked to specific crypto assets or services. This interpretation could prevent well-regulated third-country financial institutions from responding to EU client requests for crypto asset products or services if they engage in brand marketing in the EU.

A significant concern discussed was the presumption that a website in an official EU language indicates solicitation of EU clients. This assumption poses challenges for third-country financial service providers with strong EU ties, such as those in Switzerland with shared language roots, as local activities could be misconstrued as marketing to EU customers.

During the roundtable, participants highlighted the benefits of strict reverse solicitation requirements for EU-authorised pure crypto firms, ensuring a level playing field against offshore firms. However, they debated whether adapting these requirements to allow continued brand marketing by third-country financial firms with multiple business lines would create an unfair advantage. The consensus was that establishing a clear nexus between marketing and a specific crypto asset service or product would help maintain a level playing field.

It was considered that this approach aligns with MiCA's objective of protecting EU consumers, recognizing that existing financial institutions capable of performing certain CASP activities are already subject to equivalent regulations. Moreover, it was noted by the participants that the NCAs and regulatory authorities should reevaluate the presumption that having a website in an EU official language indicates solicitation. It was highlighted that there should be clearer criteria to prevent local activities from being misinterpreted as marketing efforts targeting EU clients.

Primary calls to action for Reverse Solicitation Requirements:

The primary calls to action from the Brussels roundtable on reverse solicitation requirements under MiCA emphasise practical and concrete steps for regulators:

- **Establish a Clear Nexus for Marketing:** Regulators should establish a clear connection between brand marketing and specific crypto asset services or products. This ensures that brand marketing by firms with multiple business lines and brands not predominantly associated with crypto assets or services is not unfairly restricted.

- **Allow for Continued Brand Marketing:** Adapt the proposed reverse solicitation requirements to allow for brand marketing by third-country financial firms with diversified business lines, ensuring these firms can continue their brand-building efforts without being wrongly categorised as soliciting EU clients.

Thank you to all participants of the Brussels roundtable: Aaron Tait (Lighter), Alessandro Marco Patti, Beata Sivak (Kraken), Christian Stoll (CCRI), Delphine Forma (Solidus Labs), Dimitrios Psarrakis (GBBC), Francesco Paolo Patti, Georg Brameshuber (Validvent), Hedi (Crystal), Ilija Rilakovic (WALK Attorneys, Belgrade), Joachim Schwerin (EU Commission), Louise C. D. Hubert (Crystal) Maggie Parsons (Lighter), Marcin Zarakowski (BSV), Maria Riivari (Aave), Mariana de la Roche (Validvent and tBt), Miguel Angel Calero (Isertix), Nathalie Boyke (Web3 Foundation), Nina Siedler (siedler legal and tBt), Olena Zabrodska (1inch), Pelle Braendgaard (NotaBene), Peter Kerstens (EU Commission), Roeland van der Steppen (Swiss Council), Romena Urbonaite (Bitpanda), Tim Boeckmann (Vidos), Tommaso Astazi (APCO), Vladimir Sotirov, and Zalan Noszek (Crystal).

MICAR ROUNDTABLE EXPERT SERIES

Berlin 2.0

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the MiCAR Roundtable Expert Series aims to increase legal certainty within the realm of a new regulatory framework, the EU Markets in crypto-assets regulation MiCAR. The Roundtable Series facilitates expert discussions, resulting in public reports.

The fifth roundtable of this series was again hosted by Berlin Partner in August 2024. Franziska Giffey, Senator for Economic Affairs, Energy and Public Enterprises, stated:

"*Berlin is the city of startups and innovation. New ideas are developed and tried out here. The areas of Web3, crypto and fintech also play a crucial role on Berlin's path to becoming the innovation capital of Europe. With the House of Finance and Tech, Berlin now provides a central contact point for the fintech industry. Find more info on berlin.de/startups. We warmly welcome the experts and innovators to Berlin!*"

We thank Joachim Schwerin, Principal Economist at the European Commission, for his keynote, and Crystal Intelligence and Validvent for their ongoing support as well as the Blockchain Bundesverband (Bundesblock) and Web3 Foundation for their collaboration.

The roundtable focused on the contributions of Anja von Rosenstiel on AMM as public offer; Axel von Goldbeck on past communication as current offer and Nina-Luisa Siedler on the reverse solicitation exemption for offerors.

This report aims to consolidate the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants nor the respective rapporteur.

1. Automated Market Makers (AMMs) as a Public Offer?

Anja von Rosenstiel presented the challenges and complexities surrounding the regulation of AMM software and liquidity pools under MiCAR. AMMs are an innovative way and a crucial component of DeFi, enabling the exchange of digital assets through liquidity pools. This raises questions about whether providing liquidity and/or opening up a liquidity pool could be considered a public offer under MiCAR or fall under the regulatory remit of CASPs and therefore require authorization under MiCAR. The roundtable focused on the regulatory implications of AMMs and the potential risks associated with their operations.

The roundtable began by defining the structure and function of AMMs. Liquidity providers (LPs) contribute pairs of crypto assets to a liquidity pool open to market participants. The pool holds the contributed crypto assets in a custodial function for the liquidity provider but itself does not hold title to the liquidity provided. The providers receive liquidity provider (LP) tokens representing their share of the pool like a receipt. The purpose of LP tokens is to provide a mechanism for the distribution of accumulated trading fees on a pro-rata basis. LPs must cash these tokens in (burn them) in exchange for the return of the liquidity which they provided once they exit the pool.

AMMs enable users to trade digital assets they hold for any other asset held by the pool. Smart contracts running AMM software algorithmically determine the asset value based on the ratio of assets within the pool. One of the primary concerns was whether providing liquidity and communicating the availability of such liquidity pools to the public would constitute a public offer subject to MiCAR's regulatory framework.

The debate centred on whether LPs could be classified as "offerors" under MiCAR. "Offeror" means any person, undertaking or issuer, who offers crypto-assets to the public. "Offering to the public" requires a communication to persons, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets.

Drawing parallels with the Prospectus Regulation which contains basically the same definition of public offer, participants discussed whether the act of providing liquidity to and advertising or

informing the public about this liquidity pool could be construed as a public offer in this sense.

According to Recital 28 of MiCAR (mirroring Recital 14 of the Prospectus Regulation), the mere admission to trading or the publication of bid and offer prices should not, in and of itself, be regarded as such an offer. Thus, like admitting to trading, providing liquidity to a pool only anticipates the future investment opportunity and communicating the existence of a liquidity pool, including publishing mathematical formula for price determination, is not specific enough to constitute an offer pursuant to Recital 28.

Further, according to the definition the activity must aim at concluding a purchase agreement. The concept of a public offer generally requires sufficient information to enable an investment decision by the purchaser and therefore merely passively providing an investment opportunity is not enough. The invitation to make an offer to exchange crypto assets qualify as an offer to the public must be accompanied by the intent to conclude a transaction to sell their respective proprietary crypto assets. The consensus was that simply providing liquidity to a pool does not fulfil this requirement. Contributing to the pair of crypto assets (maker) does not constitute an invitation to anyone to exchange a specific crypto asset. It lacks the intent by the LP to conclude a specific token transaction and sell and transfer title in the LP's specific proprietary assets to any specific user of the pool. The LP rather wants to earn a proportion of the pool fees as passive income. In other words, providing liquidity to a pool is exposing all those assets in the pool to sale at the pool's current exchange rate determined by the respective smart contract. LPs are not necessarily actively involved in offering assets to the public. They do not contract with any buyer directly, neither do they receive any purchase price. This exposure does not in itself constitute a public offer under MiCAR.

Based on materials of German implementation legislation for the Prospectus Regulation, an offeror is the person responsible for the offer, meaning having full control over the public offer. The roundtable agreed that a liquidity provider cannot be said to have control over the offer of pooled crypto assets, if it means to be able to make a "disposition" of them. However, depending on the circumstances of the case at hand whoever creates a liquidity pool and provides the initial crypto assets for the token pair, sets

its initial price which later automatically adjusts depending on the pool's composition. If this is combined with public announcements or advertising, this initial control might justify the qualification as "offeror" under MiCAR. However, it might still remain out of scope of MiCAR if the respective smart contract has been fully decentralised.

Furthermore, participants explored whether LPs could be considered regulated crypto asset service providers ("CASPs") under MiCAR. Generally, to qualify as CASP, the service must be provided on a professional basis and within a contractual relationship with a client. Here a key distinction was made between AMMs and traditional market-making activities. While AMMs serve a similar liquidity function as traditional market makers, they may operate in a decentralised, algorithm-driven environment where pool participants do not interact directly with liquidity providers via order books but exchange crypto assets via liquidity pools run by smart contracts. Participants stressed that there is no client relationship created between LPs and users in such case. LPs do not actively set prices, execute transactions against their own proprietary capital or profit from the bid-ask spread of trades like traditional MMs. That said, dealing on one's own account is equivalent to the exchange between crypto assets according to MiCAR. By the letter of the law MiCAR does not contain any explicit provision to exempt proprietary trading from its overall scope and therefore does also not contain the reverse exemption for market-making (as in MiFID II). Draft technical standards however require trading platform providers to give information on AMMs they use as trading systems.

Moreover, the roundtable discussed the criteria for differentiating between "fully decentralised" and "partially decentralised" AMM trading systems using liquidity pools and mathematical pricing and valuation models for the automatic execution of individual transactions. This discussion revolved around several factors. Fully decentralised AMMs operate without any central authority controlling key functions, such as mathematical asset pricing and valuation and the execution of individual transactions, or governance of the smart contract operating the liquidity pool or the AMM protocol, while partially decentralised platforms may still rely on a central entity to operate a user interface to access and communicate with the AMM or for decisions like contract upgrades or

governance interventions. Additionally, in fully decentralised AMMs, liquidity providers retain ownership of their assets through a self-custody wallet mechanism. Governance structures also play a role, as fully decentralised AMM protocols typically involve community-based voting mechanisms, whereas partially decentralised ones may have more centralised decision-making or execution. These distinctions are critical for regulators in defining the level of oversight or authorisation required under MiCAR for liquidity pools of different types of AMM protocols.

Despite these conclusions, participants emphasised the need for further regulatory clarity regarding potential risks associated with AMM activities. There should be pre-trade transparency for AMMs, regarding risks providing information for users, including about the risk of impermanent loss (when the value of assets in the liquidity pool is less than outside on the market) or price slippage / impact (lower price after execution of the trade). Whereas the risk of pump-and-dump schemes would be covered by the market abuse provisions of MiCAR, the risk of money laundering was identified as a potential key area for regulatory oversight. This might lead to the requirement to assess the use of AMMs in light of the AML and counter-terrorist financing regulations, particularly when AMM activities are tied to the issuance of virtual assets through opening up a liquidity pool.

In conclusion, participants largely agreed that AMMs currently fall outside the specific regulatory scope of MiCAR as public offerings. The same applies to crypto-asset services if provided in a fully decentralised manner. However, there is an obvious need to clarify the conditions under which participating in an AMM might actually be regulated under MiCAR. It was recommended to further assess whether certain risks inherent in AMM activities require regulatory intervention.

Primary Call to Action for AMMs as a Public Offer:

The primary calls to action based on the discussion on AMMs as a public offer are:

- **Clarify the Definition of Public Offers in DeFi Context:** Regulators should establish clear criteria whether initiating an AMM could be classified as public offers under MiCAR. This would also involve defining if the mere deployment of an AMM on a public blockchain or only the advertisement of a liquidity pool crosses the line to constitute a public offer.

- **Set Parameters for Dealing with Market Manipulation in DeFi:** CASPs should create standards to detect and prevent price manipulation schemes using AMMs. This includes monitoring transaction patterns that indicate potential abuse.

- **Develop Mechanisms for Disclosing Risks to Liquidity Providers:** CASPs providing access to AMMs for their customers should disclose specific risks, such as impermanent loss, price slippage market volatility and liquidity risks during stress events, to liquidity providers and users of liquidity pools in a standardised manner. This could involve setting technical standards for pre-trade transparency and specific risk disclosures for trading systems in the context of decentralised exchanges.

- **Differentiate Between Fully Decentralised and Partially Decentralised Market Makers**: Regulators should define criteria for what constitutes a "fully decentralised" AMM, which operates without central authority over key functions like liquidity pool, mathematical pricing, or governance of its underlying protocol, and would thus be exempt from certain regulatory obligations. In contrast, "partially decentralised" activity, which may rely on central entities to provide user interfaces for AMMs, as predetermined only counterparty to trades, or for decisions such as contract upgrades or governance of underlying protocols.

2. Past Communication as Public Offer

The topic of past communication as a public offer, presented by Axel von Goldbeck, explored the challenges concerning legacy public offers under MiCAR and the obligations they may trigger. As many issuers and supporting vehicles may have publicly offered tokens in the past and still have tokens available for sale, the question arises: Do these entities need to review past content on their websites, social media, or other communication channels accessible from within the EU to ensure they do not publicly offer crypto-assets in 2025 which fall under MiCAR. The discussion focused on understanding the regulatory implications of such communications and how offerors can mitigate potential risks.

Participants were reminded that under MiCAR, a public offer requires communication in any form—oral, written, electronic, or otherwise—and that past communication, if still accessible, could be considered current communication unless actively removed. Many issuers might not realise that content still publicly available could trigger MiCAR compliance obligations, even if the initial offer occurred before MiCAR was proposed.

Article 143 of MiCAR states that white paper obligations and other requirements will apply to any public offering of non-ART and non-EMT tokens that are not terminated before December 30, 2024. This means that any legacy public offer extending beyond this date, whether by intent or lack of an explicit termination period, may fall under MiCAR's regulatory scope.

One of the primary issues discussed was the ambiguity around whether public offers made years ago—before MiCAR was enacted—would need to comply with the new obligations. Participants debated whether this retroactive application could violate the principle of legal certainty, as offerors could not have anticipated these requirements at the time of the offering. Despite these concerns, it was acknowledged that this protection would require legislative intervention at the EU level.

To address this challenge, the roundtable discussed practical solutions that offerors could take in the absence of legislative changes. One suggestion was for offerors to proactively publish statements clarifying that any past communication regarding their token offerings, whether on websites, social media, or other platforms, no longer holds binding effect

as of December 31st, 2024. This self-regulation approach would provide clarity and reduce the risk of being retroactively held accountable for past communications while still selling the respective crypto-asset in 2025. The roundtable also proposed the creation of a standardised template for such declarations, which could be shared through industry platforms and community channels.

Moreover, participants recommended that a request be made to ESMA to include guidance on past communications in its forthcoming FAQ on MiCAR. This guidance would help clarify the extent to which legacy offers must comply with MiCAR's white paper and disclosure requirements.

Primary calls to Past Communication as Public Offer:

The primary calls to action for regulators and authorities, based on the discussion of past communication as a public offer, are:

- **Clarify the Retroactive Application of MiCAR to Past Offers:** Regulators should provide clear guidance on whether and how MiCAR applies to public offerings made before its enactment, particularly regarding the legal certainty of issuers who could not have anticipated these obligations at the time of their offering.
- **Request ESMA to Issue Specific Guidance on Legacy Offers:** A formal request will be made to ESMA to address the treatment of past offers in its FAQ, particularly focusing on whether offerors need to review and remove historical content from accessible channels to avoid non-compliance with MiCAR.
- **Encourage Proactive Declarations by Offerors:** Authorities might consider encouraging offerors to publish statements regarding past communications, clarifying that such communications no longer hold binding effect after December 30, 2024. A standardised template for such declarations should be developed and made available to the industry.

The roundtable suggested to further discuss the following template:	
English	**Deutsch**
Please note: This text is for informational purposes only and does not constitute legal advice. It was drafted in accordance with German law and only takes into account the relevant national regulations. Neither the author nor any other individuals or companies assume liability for the completeness, accuracy, or timeliness of the information provided. It is strongly recommended to seek independent legal advice in all matters related to this information.	***Bitte beachten: Dieser Text dient ausschließlich zu Informationszwecken und stellt keine Rechtsberatung dar. Er wurde unter Anwendung des deutschen Rechts verfasst und berücksichtigt ausschließlich die entsprechenden nationalen Bestimmungen. Weder der Verfasser noch andere Personen oder Unternehmen übernehmen eine Haftung für die Vollständigkeit, Richtigkeit oder Aktualität der bereitgestellten Informationen. Es wird ausdrücklich empfohlen, sich in sämtlichen mit diesen Informationen zusammenhängenden Angelegenheiten eigenständig rechtlichen Rat einzuholen.***
Important Notification with Regard to the xyz Token Offering XYZ Ltd. (the "Company") has been offering xyz-Tokens (the "Token Offering") since [Date of initial public offering]. It considers the Token Offering exempt from any white paper disclosure obligations applicable from December 30, 2024, under Art. 4 MiCAR.	Wichtige Mitteilung bezüglich des xyz-Token-Angebots XYZ Ltd. (das „Unternehmen") bietet seit dem [Datum des ersten öffentlichen Angebots] xyz-Token (das „Token-Angebot") an. Es betrachtet das Token-Angebot als von jeglichen Offenlegungspflichten eines Whitepapers nach Art. 4 MiCAR ab dem 30. Dezember 2024 befreit. Bezüglich des Token-Angebots wird jegliche

With regard to the Token Offering, any communication in any form (written or oral, on social media platforms, by email, [in the White Paper if applicable] or through any other channel) by the Company and/or its executives, staff, advisors and/or other service provided instructed to advise on and/or assist in the Token Offering regarding the Company's intention to apply for a listing of xyz-Tokens is being revoked by the date of this notification. [Place, Date] XYZ-Company	Kommunikation in jeder Form (schriftlich oder mündlich, auf Social-Media-Plattformen, per E-Mail, [im Whitepaper, falls zutreffend] oder über andere Kanäle) durch das Unternehmen und/oder seine Führungskräfte, Mitarbeiter, Berater und/oder andere beauftragte Dienstleister, die mit der Beratung und/oder Unterstützung beim Token-Angebot beauftragt sind, hinsichtlich der Absicht des Unternehmens, einen Antrag auf Listung der xyz-Token zu stellen, mit Datum dieser Mitteilung widerrufen. [Ort, Datum] XYZ-Unternehmen

3. Reverse Solicitation for Crypto-Asset Offerors

The topic of reverse solicitation for crypto-asset offerors, presented by Dr. Nina-Luisa Siedler, addressed a critical issue regarding the absence of an explicit reverse solicitation exemption for crypto-asset issuers and offerors under MiCAR. While MiCAR contains reverse solicitation rules for CASPs, it lacks such provisions for crypto-asset offerors, leading to concerns about whether this gap could create regulatory discrepancies. The discussion explored whether MiCAR's silence on reverse solicitation for offerors was intentional or is simply based on the historically evolved financial regulation, and what implications this has for the industry.

The problem starts with the fact that reverse solicitation is a concept well understood under the Prospectus Regulation and MiFID II. Under the Prospectus Regulation, a public offer requires the offeror to actively reach out to the public and induce investors to make an investment decision. If an investor

takes the initiative without any inducement or encouragement from the offeror, the offer is not considered "public," and therefore, the usual regulatory requirements do not apply.

MiCAR contains similar reverse solicitation rules for service providers under Article 61, where third-country CASPs do not need authorization if a client initiates the provision of services independently. However, this exemption does not explicitly extend to crypto-asset offerors, raising questions about how MiCAR should be interpreted in this regard.

The roundtable began by analysing the historical and legal background of MiCAR's provisions on reverse solicitation. Participants noted that MiCAR's structure appears to have been borrowed from both the Prospectus Regulation and MiFID II. The Prospectus Regulation, which serves as the foundation for MiCAR's rules on crypto-asset offerings, does not include explicit reverse solicitation provisions. Conversely, MiFID II, which inspired MiCAR's rules for crypto-asset service providers, does contain such a rule for service provision. Therefore, it is likely that the absence of a reverse solicitation rule for crypto-asset offerors is due to the historical roots of the legislation, rather than an intentional differentiation by MiCAR.

A key issue discussed was whether the absence of explicit reverse solicitation provisions for offerors under MiCAR implies a stricter regulatory regime for public offerings of crypto-assets compared to traditional securities. The consensus was that while MiCAR does not explicitly mention reverse solicitation for public offerings, the established legal interpretation of the Prospectus Regulation should apply. This means that, in practice, if an investor independently initiates a crypto-asset purchase without any inducement from the offeror, this should not be considered a public offer subject to MiCAR's regulatory obligations.

The discussion also covered the potential risks associated with allowing reverse solicitation for crypto-asset offerors. While extending the reverse solicitation rule to offerors might provide clarity and flexibility, participants expressed concerns that this could open a loophole for issuers to claim reverse solicitation when, in fact, they had actively promoted the offering through indirect means such as social media campaigns or influencer partnerships. Striking a balance between regulatory oversight and flexibility for

offerors is essential to avoid potential abuses.

Primary calls for Reverse Solicitation for Crypto-Asset Offerors
The primary calls to action for Reverse Solicitation for Crypto-Asset Offerors are: • **Extend Reverse Solicitation to Crypto-Asset Offerors:** Regulators should clarify that the established legal principle under the Prospectus Regulation—that reverse solicitation is not considered a public offer—applies to crypto-asset offerors under MiCAR. This would provide consistency between the treatment of traditional securities and crypto-assets, ensuring that issuers are not subject to unnecessary regulatory burdens when investors independently initiate a purchase. • **Define Clear Parameters for Reverse Solicitation:** Authorities should establish clear guidelines outlining the conditions under which reverse solicitation applies to crypto-asset offers. This should include clear distinctions between investor-initiated transactions and situations where offerors indirectly induce investments through marketing or other promotional activities. • **Prevent Misuse of Reverse Solicitation Claims:** To avoid abuse of reverse solicitation provisions, regulators should monitor for situations where offerors may claim reverse solicitation while engaging in indirect marketing. Clear enforcement mechanisms should be put in place to ensure that reverse solicitation is not used as a means to circumvent MiCAR's public offering requirements and to protect the legitimate market for crypto-asset offerings.

We thank all participants of the Berlin roundtable for contributing to the discussion:

Anja von Rosenstiel (FINLAW), Anna-Maria Irgang (Validvent), Axel von Goldbeck (Möhrle Happ Luther), Celina Mousa (research assistant with siedler legal), Dr. Ulrich Gallersdörfer (Carbon Credit Rating Institute), Emma Chenning, Gustav Hemmelmayer (Botlabs), Izabela Kuprasz (Web3 Foundation), Jakob Zwiers (Berlin Partner), Jannik Piepenburg (tBt), Joachim Schwerin (European Commission), Johannes Ruppel (CZR / carbonify), Joanna Rindell (World of Women), Laura Kajtazi (Validvent), Mariana de la Roche (INATBA), Martin Sommerfeldt, Maximilian Göth (DLT Finance), Michal Truszczynski (Bitpanda), Nina-Luisa Siedler (siedler legal), Tim Adrelan (Osborn Clarke), Tim Zölitz (Crypto Risk Metrics), and Verena Ritter-Döring (Taylor Wessing).

MICAR ROUNDTABLE EXPERT SERIES

Zug

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the MiCAR Roundtable Expert Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). The series facilitates high-level expert discussions, leading to the creation of public reports that compile insights on MiCAR's implementation across Europe.

The sixth roundtable in this series was hosted at CV Labs in Zug, Switzerland, on October 2nd, 2024. We extend our sincere gratitude to Joachim Schwerin, Principal Economist at the European Commission, for delivering the keynote address. We also thank our partners Crystal Intelligence, Token Recovery, and CV Labs for their invaluable support in making this event a success.

The Zug roundtable brought together regulators, industry leaders, and legal experts to explore key challenges associated with MiCAR. The discussions focused on contributions from Peter Lohmann, who addressed reverse solicitation in a group context; Tina Rebecca Balzli, who explored cross-border crypto-asset custody for EU-based clients; and Reto Luthiger, who discussed managing the combination of reverse solicitation and offering regulations for crypto-asset issuers.

This report consolidates the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants nor the respective rapporteurs.

in cooperation with:

with the support of:

1. **Navigating the Reverse Solicitation Labyrinth in a Group Context: Is Reverse Solicitation Possible for Third-Country Firms with a MiCAR-Licensed Subsidiary in the EU?**

Peter Lohmann, Head Legal Internationalisation at Sygnum Bank AG, explored the complexities surrounding the availability of reverse solicitation by third-country firms with a MiCAR-licensed subsidiary in the EU.

Under MiCAR, crypto-asset service providers (CASPs) are generally required to be established within the EU. Third-country crypto-asset service providers may only serve EU customers under the reverse solicitation exemption. Therefore, when both the third-country firm and its EU subsidiary operate under the same brand, there is a heightened risk that marketing activities by the EU subsidiary could be interpreted as indirect solicitation by the parent company, thus jeopardising compliance with MiCAR's strict requirements.

Participants agreed that while MiCAR's goal of regulating crypto-asset services within the EU should not be undermined, ESMA's interpretation of "means of solicitation" and "person soliciting" might be overly broad. This could make it difficult for firms with EU subsidiaries to maintain compliance, especially in cases where the subsidiary's marketing is seen as soliciting on behalf of the parent company' additional services. They also noted that imposing geo-blocking to prevent EU residents from accessing third-country services may be easily circumvented using VPNs and would also unduly limit EU citizens' freedom of choice.

The idea of creating a separate brand identity for the EU subsidiary was also discussed but was deemed counterproductive. It could reduce the value of globally recognized brands and make the EU market less attractive to businesses. The participants agreed that solutions should allow third-country firms to maintain their brand identity while ensuring compliance with MiCAR.

To address these challenges, several practical solutions were proposed. Firstly, third-country firms should clearly separate their service offerings from those of their EU subsidiary. This could be achieved by creating distinct sections of the website for EU customers and using location-based IP mapping to direct users to the appropriate service (without blocking them from intentionally also visit

the third-country section). Secondly, firms should ensure that their customer-facing employees are well-trained to understand the differences between the parent company's services and those offered by the EU subsidiary, avoiding any inadvertent promotion of the third-country firm's services. Finally, it is crucial to properly document how customers initiated contact to the third-country parent, as standard disclaimers may not suffice. Firms must maintain detailed records to prove that EU customers approached them independently.

The roundtable participants agreed that while MiCAR's provisions on reverse solicitation should be upheld, a nuanced approach is needed to prevent unnecessary restrictions on EU citizens' rights to choose a third-country service provider. Such servicing groups should implement clear service separations, train their staff, and maintain robust documentation.

Primary Calls to Action on Reverse Solicitation for Third-Country Firms with MiCAR-Licensed EU Subsidiaries

The primary calls to action based on the discussions are:

- **Seek clarification of the Scope of Reverse Solicitation for Group Structures:** Reach out to supervisory authorities to clarify the precise scope of reverse solicitation to third-country firms with EU subsidiaries under MiCAR by preparing a detailed overview of the intended marketing activities by EU subsidiaries.
- **Allow for Brand Consistency While Ensuring Compliance:** The roundtable participants were of the opinion that third-country firms should be permitted to maintain their global brand identity when operating in the EU, provided that they implement distinct separations in service offerings. This could include specific rules on website structures (e.g., IP-based redirection) and clearly defined service sections to ensure transparency and compliance without forcing firms to operate under separate brands. However, geoblocking of EU customers from using third-country firm's services would infringe the EU customers' freedom of choice and should be avoided.

- **Set Clear Documentation Standards for Reverse Solicitation:** Service providers should establish specific documentation requirements to prove that solely EU-based customers initiated the contact independently and seek clearance from the national competent supervisory authority. This could involve mandatory data collection processes or logging mechanisms to ensure firms can provide evidence of customer-initiated interactions during regulatory reviews.
- **Limit Geo-Blocking Requirements:** Instead of mandating geo-blocking, regulators should focus on compliance solutions that respect EU citizens' rights to access services outside the EU. This could involve designing systems that ensure transparency about which services are offered by the EU subsidiary versus those offered by the third-country firm, rather than outright restricting access.

2. Handling the Combination of Reverse Solicitation in Crypto-Asset Services with Offering Regulations for Crypto-Asset Issuers

Dr. Reto Luthiger presented a significant issue during the MiCAR Roundtable, focusing on the challenges faced by third-country crypto projects that both provide crypto-asset services and issue crypto-assets. These projects must navigate two distinct regulatory regimes under MiCAR: the stringent reverse solicitation rules for third-country crypto-asset service providers as third-country firms cannot obtain a CASP licence according to MiCAR. To the contrary, third-country token issuers may compliantly issue crypto-assets from a third-country by observing the respective obligations, especially the white paper obligation. This dual compliance creates a unique challenge for such projects, which need to ensure they meet both sets of requirements without undermining the reverse solicitation exemption.

Under MiCAR, reverse solicitation allows third-country firms to provide crypto-asset services to EU customers only if solely the customer initiates the contact. This regime imposes strict limitations, such as prohibitions on promotional activities, and access restrictions to ensure that firms are not actively soliciting EU-based customers. At the same time, these projects are allowed to issue and market crypto-assets in compliance with

MiCAR's whitepaper requirements. The central question posed in the discussion was if third-country crypto projects can compliantly market their crypto-asset in the EU without threatening the availability of the reverse solicitation exemption for their service offering.

The solution lies in recognizing that while the rules for providing crypto-asset services are very restrictive, it still must be possible to comply with both sets of regulations concurrently. The issuance of crypto-assets must be clearly distinguished from the service provision. Therefore, one recommendation was to maintain separate websites: one for crypto-asset services clearly not targeting the EU, and another freely marketed and accessible to EU/EEA residents for the issued crypto-assets and whitepapers. Social media activity should also be limited to promoting self-issued crypto-assets, avoiding any reference to crypto-asset services to prevent conflicts with the reverse solicitation rules. Sponsorships should similarly focus on the product (the self-issued crypto-assets), while avoiding any links between those assets and the additional crypto-asset services.

Throughout the discussion, participants emphasised that the mere issuance of a crypto-asset by the project itself should not per se invalidate the reverse solicitation exemption for providing crypto-asset services. This aligns with the principle that reverse solicitation aims to prevent targeted service provision, not independent product issuance. Additionally, comparisons were made with MiFID II and the Prospectus Regulation, which regulate public offerings and service provision separately: Unlike these traditional financial markets, where these functions are split into different regulatory regimes, MiCAR covers both the issuance of crypto-assets and the provision of services within the same regulation. This complexity necessitates careful handling of crypto-asset and service interdependencies. A key distinction was made between crypto-assets that are closely tied to the service (e.g., tokens required for exchange access) and those that are independent (e.g., utility tokens unrelated to the service), which preserves the reverse solicitation exemption.

In conclusion, the roundtable agreed that maintaining a clear separation between crypto-asset issuance and service provision is crucial to comply with both regulatory regimes under MiCAR. The issuance of brand-related tokens, provided they are not intertwined with

the provision of services, was considered permissible without threatening the leveraging of the reverse solicitation exemption.

.

Primary Calls to Action on Reverse Solicitation for Product Offerors Providing Crypto-Asset Services
The primary calls to action based on the discussions are: • **Ensure Regulatory Separation:** Maintain a clear separation between the issuance of crypto-assets and the provision of crypto-asset services. This can be done through distinct marketing strategies, separate websites, and clear disclaimers. • **Avoid Overlap in Promotion**: Any promotion for self-issued crypto-assets should avoid overlapping with the promotion of crypto-asset services to prevent undermining the reverse solicitation exemption. • **Assess Token-Service Connection**: Before issuing a crypto-asset, carefully assess the relationship between the token and the service. If the asset is closely tied to the service, it could prevent the service provider from accepting EU customers under the reverse solicitation rule. • **Use Separate Channels for Services**: Utilise distinct channels, including (even geo-blocked) websites, for crypto-asset services, while promoting crypto-asset issuance through general channels to ensure compliance with both regulatory regimes.

3. Third-Country Custody Infrastructure for use by MiCAR-Licensed EU Entities

Tina Rebecca Balzli, Partner, Attorney-at-Law and Head of Fintech & Blockchain at CMS Switzerland, presented the important practical question of whether third-country crypto-asset

custody infrastructure and operations can be used on a cross-border basis for EU based clients.

Under MiCAR, crypto-asset service providers (CASPs) are generally required to be established in an EU member state in which they conduct at least part of their crypto-asset service business. Accordingly, a pure cross-border provision of crypto-asset services (including custody services) from Switzerland directly to EU-based clients is generally not possible under MiCAR, except under the general reverse solicitation exemption. Unlike in the area of offering crypto-assets, this applies regardless of the type of client being addressed (i.e. retail vs. qualified investors).

Against this background, the main question discussed during the roundtable was whether third-country service providers (such as in particular banks) can somehow nevertheless leverage their crypto-asset custody infrastructure and operations for their EU branches and take advantage of synergies.

Under certain general conditions, EU CASPs may outsource services or activities to third parties in third-countries, such as Switzerland. However, MiCAR requires, among other things, that EU CASPs must ensure that the third parties involved cooperate with the supervisory authorities responsible for supervising the EU CASP and that such supervisory authorities have access to the information required for their supervisory activities at the third parties' premises at all times (cf. Art. 73 (1) lit. d MiCAR).

The participants in the roundtable agreed that third-countries should seek to enter into bilateral treaties with EU member states to allow for such access to information by the supervisory authorities responsible for supervising the EU CASP, including at the third parties' premises. This will eliminate one of the most important hurdles for EU CASPs to use specifically intra-group third-country services providers.

In addition to the general outsourcing conditions, further specific rules apply to the custody [and administration] of crypto-assets for clients. These stipulate that if EU CASPs, which provide custody [and administration] of crypto-assets on behalf of clients, use other CASPs, they may only use CASPs that are themselves MiCAR-authorised, i.e. CASPs authorised within the EU (cf. Art. 75 (9) MiCAR).

On its face, this seems to exclude the use of custody infrastructure abroad by an EU CASP. Nevertheless, the roundtable participants rightly raised the question of how custody is defined under MiCAR.

Pursuant to the definition provided in MiCAR, 'providing custody [and administration] of crypto-assets on behalf of clients' means the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys (cf. Art. 3 (1) no. 17 MiCAR).

The participants therefore agreed that the term 'providing custody' in the sense of MiCAR should be construed to only cover circumstances where a service provider disposes of individual access to the crypto-assets by way of the private cryptographic keys. This rightly excludes pure custody infrastructure providers without individual access to the crypto-assets from the scope of application of the specific outsourcing rules applicable to custody services.

Under this interpretation, third-country service providers (such as in particular banks) can still leverage their crypto-asset custody infrastructure and operations for their EU branches and take advantage of synergies as long as they do not have individual access to the crypto assets.

The roundtable participants further agreed that this interpretation also makes sense from a risk-based approach in that the main goal of the MiCAR provisions on crypto custody is to minimise the risk of loss of the client in the event of the custody provider's insolvency. This is due to the fact that unless there is individual access to the crypto-assets, they will not fall into the bankruptcy estate of the provider in most jurisdictions.

There was further a general agreement amongst the participants that in interpreting the rules of MiCAR, regulators should generally prevent unnecessary restrictions on third-country firms, be it in connection with reverse solicitation (see supra Section 1) or as service providers in conjunction with EU CASPs (here Section 2). This will prevent the EU from unnecessarily being secluded from technological developments and innovative competition from which EU based clients should be able to benefit also from an economic perspective. It further avoids that the EU branche can deliver its service at higher costs and thereby EU clients might choose the third-country service instead.

Primary Calls to Action on Third-Country Custody Infrastructure for Use by MiCAR-Licensed EU Entities

- **Seek to enter into bilateral treaties with EU Member States:** Third-countries should, in their own interest, seek to enter into bilateral treaties with EU Member States in order to allow the supervisory authorities responsible for the oversight of the EU CASP to access information necessary for their oversight of outsourcing arrangements, including at the premises of third parties.

- **Precise interpretation of the term 'providing custody [and administration] of crypto assets on behalf of clients'**: This term should only cover cases where the service provider effectively disposes of individual access to the crypto-assets by way of the private cryptographic keys. This will exclude pure custody infrastructure providers without individual access to the crypto-assets from the scope of application of the specific outsourcing rules applicable to custody services and allow them as service providers in this field.

- **Take a risk-based approach when interpreting MiCAR provisions:** The proposed interpretation of the term also makes sense from a risk-based approach in that the main goal of the MiCAR provisions on crypto custody is to minimise the risk of loss of the client in the event of the custody provider's insolvency. However, unless there is individual access to the crypto-assets, they will not fall into the bankruptcy estate of the respective provider in most jurisdictions.

- **Respect EU citizens' rights to access services outside the EU:** Any interpretation of the rules of MiCAR should generally prevent unnecessary restrictions on third-country firms, be it e.g. in connection with reverse solicitation or as service providers in conjunction with EU CASPs. This will prevent the EU from unnecessarily being secluded from technological developments and innovative competition from which EU based clients should be able to benefit also from an economic perspective.

We thank all participants of the Zug roundtable for contributing to the discussion:

Anne-Lorinne Mognetti (MME), Benedikt Kukacka (Crystal Intelligence), Dr. Jean-Claude Spillmann (PwC), Eduardo Peris (Impact Plus), Gregory Aillaud (Swiss Fintech Law AG), Irina Gorbach (Crystal), Iwona Strzepka (Onchain Foundation), Joachim Schwerin (European Commission), Katharina Lasota-Heller (LEXcellence / CVA), Lena Klaassen (Carbon Ratings), Marcin Zarakowski (Token Recovery), Mariana de la Roche Wills (de la Roche W. Consulting), Marina Khaustova (Crystal), Marta Chavarria Romero (Spain Gov.), Nicola Massella (Storm), Dr. Nina-Luisa Siedler (siedler legal), Peter Lohmann (Sygnum Bank), Petko Vladov (AskRegulations), Reto Luthiger (MLL), Stephan Meyer (Obligate), Tina Balzli (CMS Zurich).

MICAR ROUNDTABLE EXPERT SERIES

Vaduz

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the MiCAR Roundtable Expert Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). The series facilitates high-level expert discussions, leading to the creation of public reports that compile insights on MiCAR's implementation across Europe.

The seventh round table in this series was hosted at the University of Liechtenstein on October 4th, 2024. We extend our sincere gratitude to Dr. Clara Guerra, Director of the Office for Financial Market Innovation and Digitisation (SFID) in Liechtenstein, for delivering the keynote address, and to Prof. Dr. Konstantina Papathanasiou for her warm welcome and introductory remarks. We also thank our partners Bitpanda, Nägele Rechtsanwälte, Stabsstelle Finanzplatzinnovation & Digitalisierung, Token Summit Liechtenstein and the University Liechtenstein for their invaluable support, along with thinkBLOCKtank, INATBA, and CCA for their collaboration.

This report consolidates the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants nor the respective rapporteurs.

in cooperation with:

with the support of:

1. Handling Own Fund Requirements under MiCAR

Dr. Christian Steiner, Director of Regulatory Compliance, Bitpanda presentation focused on the new "own fund requirements" introduced under the MiCAR for CASPs. These requirements bring the crypto industry closer to traditional financial setups, aligning it with prudential standards observed in banking and investment firms. However, the application of these requirements poses several challenges, particularly due to their rigidity and the one-size-fits-all approach. Five key issues were discussed:

1. Threshold of Own Funds: MiCAR's initial own fund requirements, ranging from €50,000 to €150,000 depending on the services provided, seem reasonable for smaller CASPs. However, for larger CASPs, the ongoing own fund requirements based on fixed overheads (FOR) can become disproportionately high, sometimes reaching millions of euros. Unlike traditional financial institutions, such as banks or MiFID II investment firms, CASPs lack the flexibility of using risk-sensitive factors or internal models to reduce the burden of own fund requirements. This results in a one-dimensional system based on overhead costs, which can be particularly detrimental for CASPs investing heavily in development and technology.

The solution lies in recalibrating the own fund requirements to better reflect the scope and nature of the activities undertaken by CASPs. Borrowing elements from MiFID II or banking regulations, such as incorporating risk-weighted assets (RWA) or K-factors into the calculation, could create a more balanced and proportional approach. This adjustment would ensure that own fund requirements are tailored to the actual risks faced by CASPs, rather than being driven solely by overhead costs. Additionally, regulators should allow for greater flexibility in how CASPs meet these requirements, taking into account different business models and investment strategies.

2. Inclusion of Unregulated Services in Fixed Overheads: MiCAR requires CASPs to include all business expenses, even for non-regulated services, in the calculation of fixed overheads. This means that expenses related to unregulated business activities, such as IT consultancy or other ancillary services, are factored into the own fund requirements. This broad inclusion creates an inflated calculation of own funds, which could force CASPs to split their operations into separate entities

to reduce the regulatory burden—an inefficient and costly approach, particularly for smaller firms.

A precedent for addressing similar issues exists in MiFID regulations, which explicitly outline criteria for excluding certain non-core expenses from own funds calculations for investment firms. MiFID's approach demonstrates a way to balance comprehensive oversight with operational flexibility, offering a relevant framework for MiCAR to consider.

To address this issue, MiCAR should allow for the exclusion of non-regulated services from the fixed overhead calculation. This would enable CASPs to focus on their core crypto-asset services without being penalized for operating additional business lines. Regulators could also introduce thresholds or criteria for determining when these activities can be excluded from the fixed overheads calculation, providing much-needed flexibility. This would prevent the need for CASPs to split their operations, thereby reducing costs and complexity, while still ensuring regulatory compliance.

3. <u>CET1 Instruments Only – Restrictions on AT1 and Tier 2 Instruments:</u> MiCAR restricts CASPs to using only Common Equity Tier 1 (CET1) instruments to meet their capital requirements. This is in contrast to other financial sectors, such as banking and investment firms, where Additional Tier 1 (AT1) and Tier 2 instruments are also allowed. This restriction limits the flexibility of larger CASPs in managing their capital structure and may lead to overburdening requirements as they grow, particularly because no other risk-sensitive instruments are permitted.

To address this limitation, MiCAR should be expanded to allow CASPs to use AT1 and Tier 2 instruments, in line with the Capital Requirements Regulation (CRR) applied to banks and other financial institutions. These instruments are already well-regulated, and their inclusion would provide greater flexibility for CASPs, particularly larger ones, in meeting their capital obligations. While smaller CASPs may opt not to use these instruments, they should have the option available to them, creating a more level playing field across different types of financial entities. This adjustment would reduce the financial strain on CASPs and enhance their ability to manage capital more efficiently.

4. <u>Monitoring Own Funds and Regulatory Clarity:</u> MiCAR imposes a requirement for CASPs to continuously monitor their own

funds, but there is little legal clarity on how this should be implemented. For smaller CASPs, this presents a significant challenge, as they may not have the internal resources or personnel (such as risk managers or compliance officers) to carry out ongoing monitoring. Furthermore, the lack of standardized guidelines for how to monitor own funds could lead to inconsistent implementation across different CASPs and varying interpretations by national regulators (NCAs).

To address this challenge, regulators should provide clear and standardised guidelines on how CASPs should monitor their own funds. These guidelines should be uniform across the EU to ensure consistent application and reduce the compliance burden on smaller CASPs. Additionally, MiCAR should introduce clear reporting requirements, outlining the specific information CASPs must provide to NCAs. This would create transparency and predictability for both CASPs and regulators, helping to reduce the risk of ad-hoc reporting requests and last-minute compliance issues.

5. Deductions – Classification of Crypto-Assets as Intangible Assets: A critical issue discussed was the potential classification of crypto-assets as intangible assets under MiCAR, which would require them to be deducted from a CASP's own funds under the CRR. This presents a unique challenge for the crypto industry, as crypto-assets, while from a civil law perspective, intangible in nature, have a clear market value and liquidity. If treated as intangible assets, the deduction of crypto-assets from a CASP's own funds could lead to significant undercapitalization, especially given the volatile nature of these assets.

The solution lies in clarifying that crypto-assets should not be classified as intangible assets under the CRR. Unlike goodwill, software, or other intangible assets, crypto-assets have a tangible market value and can be liquidated in times of financial stress. Therefore, they should not be subject to the same deductions as other intangible assets. Additionally, if crypto-assets were treated as intangible assets, they could be subject to "double deduction" under the Basel Committee's strict capital treatment for crypto-assets, which would be both unnecessary and harmful to the industry. Regulators and auditors, whether under IFRS or national accounting standards, should align on this interpretation to avoid unintended consequences for the crypto industry.

Conclusion:

The roundtable discussion highlighted the importance of creating a more flexible and proportionate framework for own fund requirements under MiCAR. By allowing for the inclusion of AT1 and Tier 2 instruments, excluding non-regulated services from fixed overhead calculations, and clarifying the treatment of crypto-assets, MiCAR can better align with the unique characteristics of CASPs. These adjustments will ensure that the regulation remains supportive of innovation in the crypto space while maintaining the necessary prudential safeguards.

Primary Calls to Action for Own Fund Requirements

The primary calls to action based on the discussions are:

- **Revise the Calculation of Own Funds:** Regulators should consider incorporating risk-sensitive factors (e.g., K-factors) and provide more flexibility for CASPs, particularly when calculating fixed overhead requirements. This will ensure the rules are proportionate to the size and scope of each CASP's business.
- **Allow Deductions for Non-Regulated Services:** MiCAR should be amended to allow CASPs to exclude non-regulated services when calculating fixed overheads, or at least provide clear criteria for when such deductions can be made.
- **Permit Use of AT1 and Tier 2 Instruments:** Expand the scope of allowable capital instruments under MiCAR to include AT1 and Tier 2 instruments, which are already in use by banks and other financial institutions under CRR.
- **Clarify Monitoring Requirements:** Establish clear, consistent guidelines for the monitoring of own funds and ensure that all NCAs apply these standards uniformly across the EU.
- **Exclude Crypto-Assets from Intangible Asset Deductions:** Explicitly clarify that crypto-assets should not be classified as intangible assets under CRR Article 36, given their market liquidity and unique characteristics. Regulators and auditors

should interpret this classification consistently, recognizing that the tangible market value and liquidity of crypto-assets distinguish them from traditional intangible assets and warrant a separate treatment.

2. Handling "Gas Fee Stations" and the Implications of Art. 75 MiCAR

Nina Gartmann from Celsion Finance AG led a crucial discussion on the implications of Article 75 MiCAR concerning the segregation of client and own funds for CASPs. The focus was on the practical and legal challenges surrounding "gas stations" used by CASPs to pay for network transaction fees (gas fees) and whether these practices comply with the strict segregation requirements outlined in MiCAR. The roundtable explored multiple facets of this issue, including the technical and legal complexities, as well as potential solutions.

1. Interpretation of Art. 75 MiCAR on Fund Segregation: Art. 75 para (7) MiCAR requires crypto-asset service providers offering custody and administration services to segregate client crypto-assets from their own on both a legal and operational level. This is akin to traditional banking rules, ensuring that in the event of bankruptcy, client funds remain safe and separate from the provider's own assets. While this is straightforward at the operational level, the same article also mandates that client and provider assets be segregated on the distributed ledger.

In practice, many CASPs use omnibus wallets for multiple clients and maintain "gas stations" to pay for network fees. These "gas stations" raise concerns because the gas fees are paid from the provider's wallet, potentially co-mingling client and provider assets in the process. This co-mingling, if interpreted strictly, could violate the segregation requirements of MiCAR, particularly when gas station funds are attributable to the provider, even though they are pre-financed through fees charged to the clients.

The solution lies in ensuring that client and provider assets are clearly distinguishable at all times, either through advanced technical measures, such as creating distinct wallets, or through proper documentation and

record-keeping practices that provide clarity on asset ownership.

2. Legal Argumentation Around Ownership of Gas Fees: A key point of the discussion focused on whether the assets used in gas stations could legally be considered client assets rather than those of the CASP. Several legal arguments were made to suggest that gas fees could be classified as client funds, particularly if clients pre-finance these fees through service charges or if the terms of service explicitly state that gas fees are part of the transaction cost borne by the client.

The proposed solution involves ensuring that legal documentation, such as general terms and conditions (GTC) or service agreements, clearly defines gas fees as client assets. This would provide a legal basis for treating gas fees as client funds, thus avoiding the need to classify them as CASP assets under MiCAR.

3. Technical Solutions for Asset Segregation: On a technical level, the roundtable participants discussed whether enhanced segregation techniques could be applied to prevent the co-mingling of client and provider funds in gas stations. Implementing a higher degree of segregation at the distributed ledger level might solve the problem, but it also introduces operational risks, as managing multiple wallets can be more complicated and may increase the likelihood of errors.

The proposed solution here is for CASPs to explore more advanced technical solutions, such as using multiple wallets to segregate client and provider assets. However, for smaller CASPs, this may not be feasible. Therefore, a balance between technical solutions and strong documentation practices could be the optimal path forward.

4. Third-Party Solutions for Gas Fee Management: Another option discussed was the use of third-party providers to manage gas stations. By outsourcing this function, CASPs could avoid holding gas fee assets themselves, thus circumventing the need to segregate these funds on the ledger. However, the use of third-party providers introduces additional costs, which could ultimately be passed on to clients.

Third-party solutions offer CASPs the ability to maintain compliance without significant internal changes to their systems. While this approach may increase operational costs, it provides a clear pathway to compliance, particularly

for larger CASPs that handle higher transaction volumes.

5. Provision of Transfer Services: The roundtable also considered whether gas fees could be reclassified as a transfer service under Article 82 MiCAR. By charging clients a fee for the transfer of assets, CASPs could argue that the gas fees are part of a distinct service, thus removing the need for strict segregation on the ledger.

This solution would require careful structuring of service agreements and might necessitate regulatory approval, but it provides a viable pathway for handling gas fees without breaching MiCAR's requirements for fund segregation.

6. Other Risk Mitigating Measures: Lastly, the discussion emphasised the importance of clear documentation and record-keeping as a risk mitigation strategy. Even if gas fees are handled through a gas station, as long as there is proper documentation of the ownership distribution via a core banking system or similar records, the risks of co-mingling can be minimised.

CASPs should maintain meticulous records of all gas fee transactions, ensuring that they can demonstrate at any time which assets belong to clients and which are their own. This level of transparency can help mitigate risks and ensure compliance with MiCAR, even when full segregation on the distributed ledger is not technically feasible.

The roundtable participants agreed that while the strict requirements of Art. 75 MiCAR pose significant challenges for CASPs using gas stations, there are several viable solutions. These include legal agreements that define gas fees as client funds, technical improvements in wallet segregation, outsourcing to third-party providers, and reclassifying gas fees as part of a transfer service. Clearer regulatory guidance would also be beneficial, particularly concerning the segregation of assets on the ledger and the legal structure of gas fee payments.

Primary Calls to Action on Gas Fee Stations and Fund Segregation
The primary calls to action based on the discussions are:

- **Clarify Regulatory Expectations on Asset Segregation:** Regulators should issue specific guidance on the technical and legal expectations for segregating client and provider assets on the distributed ledger.
- **Permit Flexibility in Gas Fee Handling:** Regulatory frameworks should allow for flexible solutions in handling gas fees, including the possibility of outsourcing or classifying gas fees as part of transfer services.
- **Provide Legal Templates for Compliance:** Regulators or industry bodies should develop templates for legal agreements that clarify the ownership of gas fees and ensure alignment with MiCAR's segregation requirements.
- **Encourage Best Practices for Risk Mitigation:** CASPs should adopt best practices in documentation and record-keeping to ensure transparency and compliance, particularly when full ledger segregation is not possible.

3. Intervention of NCA vs Passporting Art. 105 vs 65 MiCAR

The third topic, presented by Alireza Siadat, delved into the relationship between National Competent Authorities (NCAs) and the cross-border provision of crypto-asset services under MiCAR. The central question revolved around whether an NCA in a host Member State has the authority to intervene in the services of a CASP that operates across borders, and how the provisions of Art. 65 (Passporting) and Art. 105 (Product Intervention) apply in such scenarios.

Art. 65 MiCAR: Passporting and Cross-Border Services MiCAR establishes a harmonized framework across the EU, allowing Crypto-Asset Service Providers (CASPs) to provide their services across Member States under a single authorization from their home NCA. According to Art. 65, once a CASP receives authorization from its home Member State, it may notify the authority of its intent to offer services in other Member States. Upon notification, the CASP can provide services in the host Member States without needing additional permissions.

This system of passporting is designed to encourage cross-border business growth and provide equal opportunities for market entry, supporting the innovation and expansion of crypto-asset services across the EU. Furthermore, it ensures that crypto-assets can scale up their businesses without unnecessary regulatory hurdles from host Member States, fostering competition and efficiency in the EU crypto markets.

Art. 105 MiCAR: Product Intervention While Art. 65 MiCAR promotes cross-border activities, Art. 105 sets out specific conditions under which NCAs can intervene in the marketing, distribution, or sale of particular crypto-assets or activities that pose a significant risk to market integrity, investor protection, or financial stability. Such interventions are allowed only as a last resort and must be based on clear, objective criteria laid out by the Commission.

The key point of Art. 105 is that it restricts NCAs from broadly intervening in the services of CASPs, unless there is a specific product-related issue that justifies intervention. Therefore, any action taken by an NCA must be directed at a product or type of activity and cannot be a general intervention against the CASP.

Challenges with Implementation and Regulatory Discrepancies The roundtable discussion highlighted that, in practice, some NCAs do not fully respect the cross-border nature of MiCAR, particularly when it comes to product intervention. The rapporteur noted instances where host Member State NCAs were reluctant to allow certain CASPs to operate within their jurisdiction, despite the CASP having valid permission from their home NCA. In some cases, these authorities either delayed cooperation agreements between domestic and foreign CASPs or subjected them to intensive audits, creating a de facto barrier to entry.

This reluctance and resistance to cross-border activities create a regulatory environment that undermines the very purpose of MiCAR—fostering a unified, competitive market for crypto-assets in the EU. Some NCAs perceive cooperation agreements between domestic and foreign CASPs as attempts to bypass local regulations, leading to discrimination against both domestic and foreign entities.

Proposed Solutions and Best Practices The roundtable agreed that NCAs must adhere strictly to the framework set out by MiCAR. Art. 65 should be fully respected, allowing CASPs to provide services across Member States without undue

interference. Product interventions under Art. 105 must be limited strictly to situations where a specific crypto-asset or activity presents a significant risk. NCAs must not intervene in general service provision unless the intervention is directly related to the risks identified under MiCAR's product intervention rules.

To further support this, the roundtable proposed establishing a "whistleblowing" communication channel to the European Supervisory Authorities (ESAs) or the European Commission, where CASPs facing discrimination from NCAs can report these issues without fear of further discrimination. This would help create a more transparent and fair regulatory environment, ensuring that cross-border services can thrive under MiCAR's intended framework.

The roundtable underscored the importance of ensuring that NCAs across the EU implement MiCAR uniformly, respecting the rights of CASPs to offer their services cross-border under Art. 65, while limiting intervention to product-specific issues under Art. 105.

Primary Calls to Action on NCA Intervention and Passporting under MiCAR

The primary calls to action based on the discussions are:

- NCAs must respect the cross-border framework established under Art. 65 MiCAR, allowing CASPs to provide services in host Member States without unnecessary barriers or delays.
- Product interventions under Art. 105 must be directed solely at crypto-assets or specific activities that pose a significant risk, not at CASPs in general.
- The European Commission and ESAs should establish a whistleblowing channel for CASPs facing discrimination from NCAs, providing a safe mechanism for reporting regulatory overreach.
- Ensure cooperation between NCAs is in line with MiCAR's goal of fostering cross-border growth and innovation, with no undue interference from host Member States.

4. Outsourcing to Non-EU/EEA Based Service Providers

Dr. Thomas Nägele's presentation focused on the challenges posed by Article 73 of MiCAR, which mandates that Crypto-Asset Service Providers (CASPs) remain fully responsible for meeting all regulatory obligations, even when outsourcing certain services. CASPs must ensure that outsourced services comply with the same regulatory standards as those performed in-house. This requirement effectively restricts outsourcing to entities that hold the same MiCAR license, thereby limiting outsourcing to service providers within the EU or EEA. Traditional outsourcing destinations, such as the U.S. or Switzerland, are off-limits for key services under MiCAR.

It was highlighted the practical difficulties this creates, particularly for Liechtenstein-based companies that have historically outsourced services to Switzerland. MiCAR does not include a "Safe Harbor" provision, unlike the General Data Protection Regulation (GDPR), which allows data transfers to third countries deemed adequate by the European Commission. Consequently, organisations relying on non-EU/EEA service providers will need to seek alternatives within the MiCAR framework once the regulation comes into force.

The Austrian Financial Market Authority (FMA) has provided some guidance on what constitutes outsourcing, particularly regarding custody and management of crypto assets. The FMA specifies that if a service provider controls private keys, manages seed or recovery phrases, or holds one of the signatures in a multisignature wallet, this would be considered outsourcing under MiCAR and require a license. The FMA further indicated that even managing offline wallets could trigger the need for a MiCAR license, depending on the level of control exerted by the service provider. The overarching principle is that the more control a service provider exerts over crypto assets, the more likely they are to require MiCAR licensure.

During the discussion, participants explored potential workarounds, including relocating Swiss employees to Liechtenstein or setting up technical infrastructure in Switzerland while keeping the keys with a Liechtenstein-based CASP. However, these options may not be viable for companies unwilling to take on key management responsibilities. Ultimately, the most feasible solution seems to be discontinuing outsourcing to third countries and shifting to EU or EEA partners that comply with MiCAR regulations, unless the services in question do not meet MiCAR's definition of outsourcing as interpreted by the FMA.

Primary Calls to Action for Outsourcing to Non-EU/EEA Based Service Providers
The primary calls to action based on the discussions are: • **Clarify the Definition of Outsourcing:** Regulators should provide more specific guidelines on what constitutes outsourcing under MiCAR, particularly with respect to key management and control over crypto-assets. • **Establish a "Safe Harbor" Equivalent:** Similar to the GDPR, MiCAR should introduce provisions that allow outsourcing to third-country service providers that meet comparable regulatory standards. • **Explore Alternative Approaches for Third-Country Outsourcing:** Develop practical solutions, such as relocating employees or setting up hybrid models, that allow continued collaboration with non-EU/EEA providers while remaining compliant with MiCAR. • **Provide Detailed Examples and Interpretations:** Regulators, such as the FMA, should continue to offer examples and case studies that clarify how different outsourcing arrangements are treated under MiCAR.

We thank all participants of the Zug roundtable for contributing to the discussion:

Alireza Siadat (thinkBLOCKtank), Alice Zhang (Q Development), Asim Soysal (21X), Christian Steiner (Bitpanda), Clara Guerra (Stabsstelle Finanzplatzinnovation & Digitalisierung), Gezime Shaquiri (Stabsstelle Finanzplatzinnovation & Digitalisierung), Greg Chew (QPQ), Heinz Konzett (Stabsstelle Finanzplatzinnovation & Digitalisierung), Johannes Wirtz (Bird&Bird), Jörn Erbguth, Mariana de la Roche (de la Roche Consulting), Marta Chavarria Romero (Spain Gov.), Martin Angerer (Uni. Liechtenstein), Miguel Vaz, Nina Gartmann (Celsion), Nina Siedler (Siedler Legal), Prof. Dr. Konstantina Papathanasiou, LL.M. (Uni. Liechtenstein), Ricardo Simoes (INATBA), Sidney Lukman (Stabsstelle Finanzplatzinnovation & Digitalisierung), Siegfrie Herzog, Sven Hildebrandt (Crypto Risk Metrics), Thomas Nägele (Nägele), and Victoria Vickery(Nägele).

MICAR ROUNDTABLE EXPERT SERIES

Madrid

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the MiCAR Roundtable Expert Series continues to build legal clarity within the EU's evolving regulatory framework for crypto-assets under MiCAR.

The eighth roundtable in this series was hosted at the historic Palacio de Cibeles in Madrid on October 10th, 2024. We are deeply grateful to our partners and supporters who made this event possible: the European Commission, Crystal Intelligence, Merge Madrid, and Taxbit.

The Madrid session brought together key players from the regulatory and crypto sectors to explore essential topics related to MiCAR. The discussions were led by contributions from Tommaso Astazi, who examined the integration of the Transfer of Funds Regulation (TFR) with MiCAR; Max Bernt, who addressed privacy and data protection challenges across MiCAR and other regulatory frameworks; and Albi Rodriguez Jaramillo, who discussed the compliance requirements and systemic risks associated with E-Money Tokens (EMTs).

This report consolidates the insights gathered during the Madrid discussions. It is essential to note that the perspectives and conclusions presented here represent the collective understanding of these topics and do not reflect the individual positions of any participants or rapporteurs.

1. **Expanding the Regulatory Landscape: TFR and Its Integration with MiCAR**

Tommaso Astazi, Head of Regulatory Affairs at Blockchain For Europe, began the presentation by emphasising that the EU regulatory framework for crypto-assets not only includes MiCAR but also incorporates other critical legislation, notably the Transfer of Funds Regulation (TFR) as part of the AML package. The TFR aligns with FATF Recommendation 16, expanding the "Travel Rule" to the crypto sector, requiring CASPs to exchange information about the originator and beneficiary of each crypto transaction they facilitate. Under this rule, whenever a CASP is involved in a transaction, it must collect and transmit the originator and beneficiary information. This process is straightforward for transfers between two CASPs, as both have established customer relationships (including KYC verification).

However, the landscape becomes more complex when transactions involve self-hosted wallets (SHWs). Transfers between a CASP and an SHW raise complications in the collection and verification of information related to the originator and beneficiary since SHW providers typically do not verify user identities through KYC processes. Negotiations to finalize the TFR in June 2022 led to a compromise, allowing CASPs to forego mandatory identity verification for SHWs under certain thresholds. For transfers under €1000, a simple information collection is required, while transfers above €1000 to a user's own SHW mandate CASP verification of wallet ownership. Above this threshold to a third-party SHW, CASPs can apply a risk-based approach to determine the appropriate due diligence measures.

Nevertheless, the European Banking Authority's (EBA) recently released Travel Rule guidelines appear to deviate from this political agreement by suggesting CASPs may need to gather "additional data from other sources to verify" third-party SHW information. This shift could force many CASPs to halt transfers above €1000 to third-party SHWs, disrupting user access to compliant transactions and potentially pushing activity toward unregulated markets, contradicting the TFR's intent.

Discussion Highlights

1. Regulatory Clarity: Participants emphasised that developing Level 2 measures under MiCAR and TFR should ensure regulatory clarity

without reintroducing the discarded verification requirement. The political compromise acknowledged that a mandatory verification for SHWs could not only be impractical but would create data security risks by fostering databases vulnerable to cyber threats. Stricter rules would deter CASPs from offering transfers to third-party SHWs, moving transactions toward unregulated markets – counterproductive to the legislative goal of increased oversight.

2. KYC-Compliant SHWs and Technological Innovations: New wallet solutions incorporating privacy-enhancing technologies (such as decentralized identities, ZKPs, and decentralized KYC tokens) could offer a balanced solution, allowing CASPs and law enforcement to identify wallet owners when necessary. This approach aligns with the TFR's political language, aiming to support technology capable of verifying SHW ownership on an as-needed basis.
3. Current Industry Solutions: There are existing and emerging technological tools that enable secure information exchange and third-party verification, such as Notabene's solution, which facilitates identity verification requests for third-party wallets via secure messaging. Solutions like these support CASPs in fulfilling verification requirements without compromising user privacy.
4. Misconceptions of Web3 Risk: Applying the Travel Rule – originally designed for the traditional financial (TradFi) sector using SWIFT – directly to Web3 without adaptation overlooks the technological differences between these spaces. Participants argued that regulatory scrutiny over crypto-transfers should not exceed that applied to cash transactions, which remain far less traceable. Blockchain analytics already provide a robust method for tracking illicit activities, offering more transparency than equivalent mechanisms in the TradFi space.
5. Risk-Based Approach and Flexible AML Solutions: The roundtable reaffirmed the importance of a risk-based approach, allowing CASPs to assess individual transactions based on risk, using transaction monitoring and blockchain analytics for a

proportionate response. This approach respects users' privacy while ensuring regulatory goals are met.

unique characteristics of the Web3 ecosystem and the regulatory goals of MiCAR and TFR, ensuring a balanced approach to AML compliance in crypto

This session underscored the need for regulations that accommodate both the

Primary Calls to Action for Expanding the Regulatory Landscape: TFR and Its Integration with MiCAR

The primary calls to action based on the discussions are:

- **Reinforce the Risk-Based Approach:** Regulators should uphold a risk-based framework, enabling CASPs to tailor services based on their risk tolerance and the specifics of each transaction, rather than imposing blanket requirements.
- **Support Technological Solutions:** Regulatory frameworks should allow for and promote technological innovations that enhance compliance while protecting user privacy. Tools like identity-on-demand solutions can help maintain compliance without excessive user data collection.
- **Clarify SHW Verification Thresholds and Standards:** Regulators need to offer clear guidance on thresholds for enhanced due diligence and establish ID standards that work with evolving digital identity solutions, ensuring consistent and practical application across the EU.
- **Avoid Stricter Rules than in TradFi:** Treating crypto-transfers as inherently riskier than cash transactions lacks a factual basis. Regulations for blockchain-based assets should be proportionate to the transparency and traceability that blockchain provides.

2. E-Money Tokens and Systemic Risk: Ensuring Compliance and Financial Resilience under MiCAR

Albi Rodriguez Jaramillo, Law Consultant at Garrigues, presented an in-depth analysis of E-Money Tokens (EMTs) under MiCAR, discussing their systemic importance and the regulatory requirements necessary to mitigate potential risks. He began by highlighting how tokenized money, which operates on Distributed Ledger Technology (DLT), has transformed aspects of the financial system, offering increased efficiency, transparency, and cost reduction across wholesale and retail markets.

Stablecoins have become a significant component in the tokenized money market, acting as a bridge for crypto investors to enter and exit the market efficiently. However, as Rodriguez noted, not all stablecoins are built alike, varying widely in their regulatory and operational standards. He pointed out that with substantial market capitalizations—Tether at $119 billion and USDC at $35.8 billion—these stablecoins play a key role in transactions, with daily volumes rivalling even major cryptocurrencies like BTC and ETH.

Under MiCAR, EMTs are defined as digital representations of value intended to maintain parity with a single official currency, effectively serving as electronic surrogates for traditional money. These tokens must be issued by authorised institutions within the EU, ensuring holders can redeem them at any time at par value with the reference currency. MiCAR also introduces the designation of Significant EMTs, which bear heightened regulatory scrutiny, particularly if they reach certain thresholds in transaction volume, market capitalization, or interconnectedness with the financial system.

Rodriguez referenced the EBA's recent supervisory priorities for ART/EMT issuers, which emphasise financial resilience and effective risk management. He highlighted how MiCAR's own funds and reserve requirements are essential to EMT issuers' financial stability and that EMTs classified as "Significant" require stringent capital and liquidity buffers, regular stress testing, and detailed reporting to both NCAs and the EBA.

Challenges in Reporting and Supervision Coordination

Rodriguez Jaramillo underscored the complexities in EMT reporting, especially

with different supervisory bodies at both the EU and national levels. As EMTs interact heavily with CASPs (Crypto-Asset Service Providers), issues arise from differing standards and real-time supervision requirements. The dual supervision model for Significant EMTs—overseen by both NCAs and the EBA—adds further complexity to aligning processes and ensuring prompt, harmonised reporting.

To address these issues, Rodriguez advocated for stronger technological solutions, such as Supervisory Technology (SupTech) tools like BIS Pyxtrial, to streamline data integration across NCAs, enhancing the efficiency and reliability of EMT supervision. He emphasised the need for uniform data reporting standards and specialised regulatory personnel to handle these emerging technologies and complex reporting requirements.

The discussion around the proposed Solutions by the roundtable included

1. Reliable Reporting Mechanisms: EMT issuers should implement verifiable reporting protocols that integrate data from authorised providers.
2. SupTech Adoption for Real-Time Supervision: Tools like BIS Pyxtrial could standardise reporting, giving regulators a centralised view of EMT health and compliance.
3. Enhanced Capacity Building: Establish standardised training programs across the EU to equip regulatory staff with the necessary technical and legal expertise, with funding supported by EU Digital Transformation grants.
4. Improved CASP Collaboration: CASPs should be proactive in sharing relevant information with regulators, especially for systemic EMTs.

Roundtable Discussion Highlights

Participants acknowledged the inherent complexity of regulatory coordination for systemic EMTs, noting the valuable role SupTech could play in managing cross-jurisdictional reporting. The discussion emphasised the need for regulatory clarity to avoid redundant or excessive reporting, while also allowing for regulatory flexibility during the initial implementation phase. Capacity building within regulatory bodies was widely agreed upon as crucial for effective oversight of EMTs, as was fostering a productive dialogue with CASPs to ensure

the collection of relevant, not excessive, data.

The roundtable concluded that clear, harmonised compliance standards and a focus on leveraging technology, particularly SupTech, are essential to effectively manage systemic risks associated with EMTs. Events such as this roundtable, facilitated by De La Roche W. Consulting and Siedler Legal, play a vital role in fostering a shared understanding of regulatory challenges and solutions across the EU.

Primary Calls to Action on E-Money Tokens and Systemic Risk

The primary calls to action based on the discussions are:

- **Enhance Reporting Consistency through SupTech Tools:** Regulators should actively adopt SupTech solutions like BIS Pyxtrial for real-time, consistent, and centralised supervision of EMTs. This would ensure that reporting is both harmonised and capable of addressing the complexities unique to systemic EMTs.
- **Standardise Regulatory Training Across the EU:** Establish an EU-wide training program to build regulatory capacity on EMT supervision, equipping staff with the necessary expertise in emerging financial technologies. This program should be funded through EU Digital Transformation grants.
- **Clarify Compliance Standards for EMT Reporting:** Regulatory authorities should provide clear guidelines on reporting obligations for EMT issuers, particularly for those classified as Significant EMTs. This includes defining the data requirements and thresholds to prevent redundant reporting and to streamline compliance.
- **Promote CASP Collaboration in Data Sharing:** Encourage Crypto-Asset Service Providers (CASPs) to collaborate closely with regulators, ensuring timely and relevant information sharing for effective supervision. This partnership would also support adherence to MiCAR's risk and liquidity standards.

3. Addressing Privacy and Data Protection Challenges within MiCAR, AML, DAC8, and CARF Frameworks

Max Bernt, Managing Director, Europe at Taxbit, provided an in-depth examination of the privacy and data protection challenges faced by Crypto-Asset Service Providers (CASPs) under the increasingly complex reporting obligations imposed by regulatory frameworks like MiCA, AMLD6/AMLR, TFR, DAC8, and CARF. He identified key concerns arising from these obligations, including data handling risks, inadequate tools for investigation, and cross-border data-sharing complexities, all of which put CASPs at heightened risk of privacy breaches and regulatory non-compliance.

One significant issue is the process of combining on-chain public data with off-chain private data for compliance purposes. This integration introduces notable privacy risks, including potential data leaks, breaches of tax secrecy, and exposure of sensitive personal information. Although tools like Crystal, Chainalysis, and TRM Labs are commonly used to manage data, improper handling can violate user privacy rights.

Another challenge relates to the use of inadequate tools for conducting sensitive investigations. Regulatory bodies have sometimes relied on insecure, non-specialized tools (such as retail-grade web applications) for tax or AML investigations. These tools often lack robust encryption, access control, and advanced security measures, making CASPs vulnerable to unauthorised access and data exposure.

A third concern centres on cross-border data-sharing, particularly under frameworks like DAC8 and CARF, which facilitate extensive exchanges of crypto-related user data across borders. Bernt noted that insufficient guidelines are provided for secure handling of such information, especially when data is repurposed for non-tax uses, such as AML or counter-terrorism efforts, increasing risks to data privacy.

Finally, the expanding scope of reporting obligations under DAC8 and AMLD6 raises concerns about potential violations of individual privacy and data protection rights. Combining on- and off-chain datasets without adequate privacy safeguards may expose sensitive data, creating legal uncertainty and raising the

risk of infringing fundamental privacy rights.

To address these challenges, Bernt recommended several key solutions. Firstly, he advocated for stricter regulatory oversight on reporting tools, suggesting that authorities require the use of government-certified platforms for handling sensitive off-chain data during tax and AML investigations. Closed cloud solutions, he argued, offer higher privacy standards through robust encryption, security auditing, and controlled access.

Secondly, Bernt emphasised the need for a clear separation between on- and off-chain data in regulatory frameworks. He proposed developing protocols to manage these data types independently, incorporating specific safeguards to protect off-chain data when combined with on-chain analytics.

He further recommended that DAC8 and MiCA introduce comprehensive privacy guidelines for cross-border data exchanges. These should encompass encryption, secure communication channels, and restricted access to sensitive data, thereby protecting user information, even when it is repurposed for other compliance areas.

Lastly, Bernt highlighted the importance of balancing transparency with privacy, suggesting that CASPs and regulators limit data collection to only essential information. Anonymization techniques, he noted, could be applied to larger datasets, thus allowing effective regulatory oversight while safeguarding individual privacy rights.

Primary Calls to Action on Privacy and Data Protection for CASPs
The primary calls to action based on the discussions are: • **Mandate Secure Reporting Tools:** Regulatory authorities should enforce the use of certified, high-security platforms for all sensitive off-chain data handling, with required encryption and access control standards.

- **Develop Data Handling Protocols:** Establish and enforce specific guidelines for managing and securing on- and off-chain data separately, with clear protective measures for any integrations.
- **Clarify Cross-border Data Privacy Standards:** Implement robust guidelines for cross-border reporting under DAC8 and CARF, ensuring secure handling protocols, restricted access, and encryption measures.
- **Adopt Privacy-Enhanced Transparency:** Regulate data collection and sharing to focus strictly on necessary information, using anonymization techniques where feasible to minimise data exposure while maintaining oversight.

We thank all participants of the Madrid roundtable for contributing to the discussion:

Adri Wischmann (IoT Netherlands), Alain Otaegui (European Banking Authority), Akli Le-Coq (Ministry of Finance), Albi Rodriguez (Garrigues), Almudena de la Mata (Blockchain Intelligence), Ana Carolina Oliveira (Venga), Carlos Escobedo (EtherNodes), and Gonzalo Navarro (ONTIER), Joaquin Sastre (Boerse Stuttgart Digital), Luiza Castro Rey (FiO Legal), Magnus Jones (EY Sweden), Marina Villalonga (Asensi Abogados), Max Bernt (Taxbit/INATBA), Mike Sadarangani (Zodia Custody), Nina Siedler (siedler legal and thinkBLOCKtank, organiser), Pedro Casanova (BBVA), Pedro Mendez de Vigo (Kraken), Reagan Cook (Taxbit), Tiburcio Sanz (Crystal), and Tommaso Astasi (BC4EU).

MICAR Expert Roundtable Series
in collaboration with the European Commission

Dublin Session

25th November 2024

Initiated by Mariana de la Roche W. and Dr. Nina-Luisa Siedler, the MiCAR Roundtable Expert Series continues to build legal clarity within the EU's evolving regulatory framework for crypto-assets under MiCAR.

The tenth roundtable in this series was hosted at the Trinity Business School on November 25th, 2024. We are deeply grateful to our partners and supporters who made this event possible: the European Commission, Crystal Intelligence, Zumo, Blockchain Ireland, Trinity Business School, as well as thinkBLOCKtank.

The Dublin session brought together key players from the regulatory and crypto sectors to explore essential topics related to MiCAR. This session focused specifically on specific monitoring and reporting issues for CASPs. The discussions were led by contributions from Daniel Taylor (Zumo) who examined application and enforcement of CASP sustainability disclosure requirements as well as challenges and opportunities in the MiCA sustainability reporting template, and Tiburcio Sanz (Crystal Intelligence) who addressed interpretations inconsistencies between EU's Transfer of Funds Regulation and the Financial Action Task Force (FATF) recommendations.

This report consolidates the insights gathered during the Dublin discussions. It is essential to note that the perspectives and conclusions presented here represent the collective understanding of these topics and do not reflect the individual positions of any participants or rapporteurs.

1. **Application and enforcement of CASP sustainability disclosure requirements**

Daniel Taylor, Research & Policy Lead at Zumo, led an in-depth discussion on the challenges and operational implications of MiCA's incoming sustainability disclosure requirements for CASPs. These disclosures, mandated under Article 66(5) of MiCA, are designed to provide standardized sustainability metrics for crypto-assets serviced by CASPs, and represent a critical 'Day 1' compliance obligation. However, the industry lacks clarity on how NCAs will assess CASP preparedness for meeting these requirements and the enforcement mechanisms that will follow.

Participants examined ESMA's guidance, which does not foresee any delayed application of these sustainability disclosure requirements. Despite this, questions remain about how NCAs will integrate assessments of CASP sustainability readiness into authorization processes. It was noted that these challenges are compounded by transitional discrepancies: while sustainability disclosures are expected from Day 1, other MiCA obligations, such as white paper requirements for non-EMT/ART assets, benefit from a grace period extending to 2027. This creates an uneven compliance landscape, posing significant operational challenges for CASPs.

Discussion also addressed the divergent readiness levels among NCAs, many of which are still setting up processes for assessing CASP applications under MiCA. Concerns were raised about regulatory arbitrage, as CASPs may seek jurisdictions perceived to have less stringent or clearer requirements. Some participants flagged the significant operational burden on CASPs of meeting sustainability disclosure requirements without comprehensive guidance or aligned enforcement practices across member states.

The group further explored the role of ESMA in ensuring alignment and reducing inconsistencies. Participants emphasized the need for ESMA to issue more detailed guidance on sustainability disclosures, not only to CASPs but also to NCAs. Examples of potential guidance included clarifications on acceptable compliance solutions, integration of sustainability assessments into consultation and application templates, and alignment efforts to minimize enforcement disparities between jurisdictions.

It was also noted that regulators and CASPs would benefit from industry collaboration to identify best practices for sustainability assessments. These discussions could inform regulatory approaches and foster a more uniform understanding of how sustainability

disclosures should be implemented and enforced.

Participants emphasized the operational challenges posed by MiCA's sustainability disclosure requirements, particularly the misalignment between immediate obligations for CASP sustainability disclosures and the transitional grace periods granted for other MiCA mandates, such as white paper compliance for non-EMT/ART assets. This discrepancy places a significant operational burden on CASPs, requiring them to implement processes without the benefit of a phased introduction.

A key concern was the varying readiness levels of NCAs across member states. Participants highlighted the risk of regulatory arbitrage, where CASPs might seek jurisdictions perceived to have less stringent or better-defined requirements. These disparities could lead to uneven enforcement, undermining the harmonization objectives of MiCA.

The role of ESMA emerged as pivotal, with participants stressing the need for centralized, detailed guidance to ensure uniform application of sustainability requirements. This guidance should clarify acceptable compliance solutions and provide actionable steps for both CASPs and NCAs. ESMA's proactive engagement with member states is essential to fostering alignment and mitigating inconsistencies.

Finally, the discussion underscored the importance of collaboration between regulators, CASPs, and industry stakeholders. Participants agreed that sharing best practices and maintaining an open dialogue would not only enhance compliance strategies but also reduce friction in the implementation process, ensuring a more cohesive regulatory environment across the EU.

Primary Calls to Action for Application and enforcement of CASP sustainability disclosure requirements
The primary calls to action based on the discussions are: • **Facilitate Industry Engagement:** NCAs should engage with industry stakeholders to gather best practices on assessing CASP sustainability requirements. • **Provide Detailed Guidance:** ESMA must prioritize issuing comprehensive guidance to NCAs and CASPs, ensuring clear operational pathways for compliance with sustainability disclosure obligations. • **Clarify Regulatory Priorities:** If sustainability requirements are to be treated as a pressing issue, this must be explicitly communicated by ESMA and NCAs to avoid uncertainty and inconsistent enforcement.

2. Interpretations inconsistencies between EU's and FATF Transfer of Funds Regulation

Tiburcio Sanz, representing Crystal Intelligence, delivered a comprehensive analysis on the inconsistencies between the EU's Transfer of Funds Regulation (TFR) and the Financial Action Task Force (FATF) recommendations, with a particular focus on Recommendation 15 / 16 and the FATF Guidance on Virtual Assets and VASPs. His discussion delved into the complexities of implementing the Travel Rule, customer due diligence (CDD), and enhanced due diligence (EDD) for high-risk jurisdictions, highlighting the operational challenges that VASPs face when reconciling varying global and EU standards.

The FATF Travel Rule mandates that VASPs collect and exchange originator and beneficiary information for transfers exceeding $1,000, aiming to combat money laundering and terrorist financing. However, this standard becomes intricate when applied alongside the EU's TFR, which extends the due diligence

requirements to smaller transactions and introduces different thresholds and expectations. The divergence between these frameworks often results in operational inefficiencies and jurisdictional inconsistencies, leaving VASPs to grapple with the practicalities of compliance while managing privacy concerns and interoperability issues.

The roundtable identified key operational challenges stemming from these regulatory overlaps, including counterparty due diligence and transaction monitoring obligations. For instance, while VASPs are required to monitor funds and ensure compliance, non-cooperation or delayed responses from counterparties often create significant roadblocks. This lack of timely interaction undermines the efficiency of the ecosystem and may lead to "jurisdiction shopping," where VASPs choose regulatory environments with less rigorous oversight.

An interesting discussion emerged around the potential for a "trust seal" or certification for compliant and cooperative VASPs, aiming to build transparency and incentivize good behavior within the sector. By publicly recognizing role models in compliance and cooperation, the sector could foster better interoperability and trust, reducing friction in meeting regulatory requirements.

Participants emphasized that creating clear and standardized protocols for collaboration is essential for the effective implementation of both the TFR and FATF standards. This requires establishing minimum expectations for cooperation, defining timelines for counterparty responses, and building systems to address gaps in compliance.

In the broader context of MiCA, the session acknowledged the risk of divergent practices among member states, fueled by varying levels of enforcement and differing risk appetites. The group proposed enhanced collaboration and data sharing between VASPs and regulators to harmonize expectations and streamline compliance efforts across jurisdictions.

The participants underscored the urgent need for harmonized regulations and robust collaboration mechanisms to address the inconsistencies between the TFR and FATF frameworks, ensuring a unified approach to AML and CTF compliance in the crypto sector.

Primary Calls to Action fo rInterpretations inconsistencies between EU's and FATF Transfer of Funds Regulation
The primary calls to action based on the discussions are: • **Create a Sector-Wide Trust Seal:** Develop a certification system that recognizes VASPs for compliance excellence, transparency, and cooperation with counterparts, fostering trust and interoperability. • **Establish Minimum Cooperation Standards:** VASPs should collaborate to define clear expectations for counterparty due diligence, response timelines, and data-sharing protocols, ensuring consistent practices across jurisdictions. • Annual Data Reporting: Build a repository of compliance data for licensed VASPs and produce yearly reports for regulators to enhance transparency and identify trends, gaps, and best practices within the sector. • **Regulator-Driven Alignment Efforts:** Regulators should facilitate alignment between the TFR and FATF standards by issuing detailed guidance on compliance overlaps and interoperability challenges.

3. Challenges and opportunities in the MiCA sustainability reporting template

Daniel Taylor, Research & Policy Lead at Zumo, facilitated a deep dive into the complexities of the MiCA sustainability reporting template, focusing on existing ambiguities and opportunities for refining the framework in future iterations of the regulation. The session explored both the operational challenges of complying with ESMA's draft RTS and potential directions for improving sustainability reporting standards in the evolving cryptoasset landscape.

Participants began by addressing the ambiguities within the current reporting template. Notable issues include the interpretation of "best efforts" and acceptable methodological limits, which lack a unified pan-industry standard. While adherence to rigorous methodologies is essential, the absence of standardization leaves room for inconsistent practices. The discussion also highlighted technical uncertainties, such

as the treatment of multichain tokens, modular or layer 2 architectures, and distinctions between tokens and native base layer assets. These gaps underscore the need for ESMA to provide more precise guidance, especially given the growing prevalence of wrapped and bridged assets that complicate classification.

A central theme was the importance of clarifying the definition and assessment of "material changes" requiring updated disclosures. Participants suggested basing these assessments on quantifiable metrics, such as percentage deviations from initial baseline observations, to ensure consistent and objective reporting triggers.

Looking ahead, the roundtable considered how sustainability reporting could evolve under "MiCA 2.0." One proposition was the introduction of entity-based disclosures alongside asset-based ones. This would allow CASPs to showcase tailored sustainability efforts and mitigation activities, providing a more holistic view of their environmental impact. Participants also discussed the convergence of crypto-specific regulations with broader financial sustainability frameworks like SFDR and CSRD, predicting a blending of governance and risk considerations from traditional finance with the metrics-heavy approach of MiCA.

The discussion concluded with a call for proportionality in future sustainability regulations, emphasizing the need for alignment with broader EU competitiveness goals. Participants stressed the importance of collaborative consultation between regulators and industry stakeholders to ensure that evolving regulations are both practical and effective.

Primary Calls to Action for Challenges and opportunities in the MiCA sustainability reporting template
Primary calls to action • **Issue Supplementary Guidance:** ESMA should provide detailed, non-legislative guidance to address ambiguities in the reporting template, particularly around technical classifications and methodological standards. • **Foster Industry-Regulator Collaboration:** Regulators should engage industry stakeholders in shaping future iterations of sustainability reporting, ensuring alignment with practical realities and harmonization across methodologies. • **Enable Proportional Regulation:** Future sustainability requirements should balance regulatory rigor with the competitiveness of the EU's crypto and financial markets, drawing on broader EU sustainability frameworks to create cohesive, effective standards.

MiCAR Experts Roundtable Attendees

Participant	Organizations
Adam Funnel	Zumo
Amelie Arras	Zumo
Cameron Carr	Central Bank of Ireland (CBI)
Cara Hennessy	Provenance
Cathal Houlihan	Valentia Partners
Christopher Martin	KPMG Law
Daniel Taylor	Zumo
Sinead Meany	Hogan Lovells
Gerardine Stack	Kraken
Ian McLaughlin	FS Reg Solutions
Irina Gorbach	Crystal
Juilian Godsil	Irish Times
Lisa Gibbons	Blockleaders
Mai Santamaria	Treasury
Marina Louarn	Department of Finance
Michael O'Sullivan	Department of Finance - ireland
Nina-Luisa Siedler	siedler Legal
Robin Renwick	Trilateral Research
Ronan Gahan	StoneX
Shane Kelleher	William Fry
Tiburcio Saenz	Crystal

DARTE SERIES

Oslo

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks.

The Oslo MiCAR Expert Roundtable was hosted at Crucible Hub on January 31st, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on MiCAR's implementation in the EEA, its interaction with existing financial regulations, and the broader impact on operational resilience and compliance strategies.

We extend our sincere gratitude to the European Commission, Nordic Blockchain Association, Zumo and thinkBLOCKtank for their invaluable support in making this roundtable possible. Special thanks to Kirsteen Harrison, Magnus Jones, and Romena Urbonaite for their contributions to the discussions.

This report consolidates the insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participants nor the respective rapporteurs.

1. Interplay Between MiCA and PSD2

The first topic of the Oslo roundtable, presented by Romena Urbonaite, Chief Compliance Officer from Axiology, focused on the regulatory overlap between MiCA and the Payment Services Directive 2 (PSD2), particularly regarding the double authorization requirements for certain CASPs engaging with e-money tokens (EMTs). The discussion explored regulatory inconsistencies, supervisory challenges, and potential solutions to streamline compliance for market participants.

Under MiCA, EMTs are considered a form of e-money, meaning their issuance and the provision of services with them trigger obligations under both MiCA and E-money Directive (EMD), and additionally PSD2 where related with payment transactions. This dual regulation results in scenarios where a single activity could require authorization under both MiCA and PSD2, creating legal uncertainty and operational challenges for market participants.

The session focused on understanding which activities fall under MiCA, PSD2, or both, the implications of double licensing requirements, and the potential short- and long-term regulatory solutions to avoid unnecessary burdens on CASPs while maintaining market integrity.

One of the main concerns discussed was the ambiguity in classifying specific transactions, leading to inconsistencies in supervisory approaches across jurisdictions. Some NCAs require separate licenses (MiCA and PSD2) but allow for dual authorization for one single entity. Other Member States do not permit an entity to hold both licenses simultaneously, forcing firms to restructure operations or create separate entities, increasing compliance complexity and costs.

A key point of discussion was how different transaction types should be classified under MiCA and PSD2. Several real-world examples were examined, revealing uncertainty around when EMT transactions qualify as payments or crypto-asset transfers, and when PSD2 licensing should be required:

- Moving funds between two accounts held by the same person – It remains unclear whether this should be treated as an internal transaction or require a payment services license.

- Transfers of EMTs between wallets (custodial and non-custodial) – Under MiCA, non-custodial wallets remain outside the regulatory perimeter, but there is confusion over whether transferring EMTs between custodial and non-custodial wallets triggers PSD2 rules.
- Payments between two individuals – Participants discussed whether a peer-to-peer EMT transaction should be classified as a MiCA transfer or a PSD2-regulated payment service.
- Payments for services using EMTs – If EMTs are used for payment transactions in exchange for services, there is debate over whether the transaction should be governed by MiCA, PSD2, or both.

The roundtable also explored the capital requirements issue, questioning whether CASPs with dual MiCA and PSD2 licenses must meet two separate capital requirements. In practice, regulators typically require the higher capital threshold of the two, but the lack of harmonized application across jurisdictions makes implementation difficult for firms operating in multiple EU markets.

Moreover, industry participants noted that the MiCA framework for EMTs was not designed to require dual authorization under PSD2, and the need for separate licensing appears to be an unintended regulatory consequence rather than a deliberate policy choice.

To address these challenges, the roundtable proposed a two-phase approach:

1. **Short-Term Solution: No-Action Letter from the EBA**

   In December 2024, the European Commission requested the EBA and ESMA to issue a no-action letter, ensuring that NCAs do not require dual authorization during the transitional period while PSD2 is under review. Participants agreed that this should be implemented as soon as possible to prevent unnecessary market disruptions.

2. **Mid-Term Solution: Revision of PSD3 to Clarify EMT Regulatory Treatment**

   The mid-term solution will be addressed as part of the PSD3 revision, with discussions already

underway in the European Parliament and the Council to exclude EMT transactions from PSD2's payment transaction definition where a CASP already holds MiCA authorization. This would eliminate the need for dual licensing, ensuring consistency across Member States.

While the short-term solution of a no-action letter would provide immediate relief, the long-term solution of revising PSD3 is critical to ensuring a harmonized and practical regulatory framework.

Additionally, participants agreed that the industry should lead the creation of a standardized "taxonomy" to clearly define which activities fall under MiCA, PSD2, or both, and outline the corresponding compliance requirements. The taxonomy could include for example:

- Moving funds between accounts – Establishing whether intra-account EMT transfers require regulatory oversight.
- Transfers of EMTs between wallets – Clarifying which transactions fall under MiCA's transfer service and which require PSD2 licensing.
- Peer-to-peer EMT transactions – Determining whether person-to-person transfers are considered MiCA-regulated transactions or PSD2 payment services.
- Payments for goods and services using EMTs – Defining at what point an EMT transaction is classified as a payment under PSD2 versus a MiCA transaction.

This taxonomy could serve as a guidance framework for CASPs, regulators, and policymakers, ensuring a harmonized application of MiCA and PSD2 across EU jurisdictions.

Primary Calls to Action on the Interplay Between MiCA and PSD2
The key recommendations from the discussion are: • Develop a Standardized Regulatory Taxonomy – The industry should lead the creation of a taxonomy clearly outlining which activities fall under MiCA, PSD2, or both, providing practical compliance guidelines for CASPs. • Ensure Supervisory Harmonization Across Member States – The industry should call out on NCAs not aligning their supervisory practices to ensure that CASPs are not subjected to conflicting interpretations of MiCA and PSD2. • Clarify Capital Requirements for Dual Licensing – The industry expects a clear and uniform approach for determining capital requirements when firms hold both MiCA and PSD2 licenses, for the time being assuming that the higher of the two potential thresholds will apply.

2. MiCA implementation in Norway and the European Economic Area.

The second topic of the Oslo roundtable, presented by Magnus Jones, Board Member from the Nordic Blockchain Association, focused on the status of MiCA implementation in Norway and the broader EEA region, highlighting regulatory delays, challenges for market participants, and uncertainties around cross-border operations.

Norway did not submit its MiCA proposal to the EEA committee until December 17, 2024, meaning that Liechtenstein and Iceland—which also fall under the EEA framework—are still waiting for Norway's process to move forward before MiCA can be fully adopted across the EEA region.

Because of these EEA-specific challenges, Norway has yet to establish a timeline for the MiCA implementation, including details on the grandfathering period and application procedures for CASPs. The key question is how Norwegian, Liechtenstein, and Icelandic market participants should navigate operations within the EU market while waiting for

MiCA to be formally integrated into EEA law and implemented at the national level.

Since Norway has not finalized its MiCA implementation timeline, CASPs and VASPs in the country face significant uncertainty about their ability to continue operating within the EU market. Many Norwegian-registered CASPs have offices, employees, or operational ties to EU countries, raising concerns about whether they must pause or adjust their activities while awaiting formal MiCA approval.

A major challenge discussed was reverse solicitation, which allows firms to provide services to EU-based clients only if the client initiates the business relationship without active solicitation from the firm. While reverse solicitation remains a grey area in MiCA, it could be a temporary strategy for Norwegian CASPs looking to maintain EU clients. However, firms must be cautious—without a MiCA license, operating digitally or physically in the EU could violate regulatory requirements, leading to potential enforcement actions and increased scrutiny for a later MiCA application.

Another concern raised was whether Norwegian CASPs that are already registered as VASPs in an EU member state could use MiCA's grandfathering regime as a basis for continuing business with EU clients until MiCA licenses are available. While best efforts and compliance with national registration requirements may offer some temporary protection, firms must carefully avoid violating outsourcing requirements and reverse solicitation rules when routing EU customers to the EEA parent until MiCA is fully operational in Norway and the EEA.

Additionally, the variation in grandfathering periods across EU Member States adds another layer of complexity. Some jurisdictions have implemented longer transition periods, allowing CASPs more time to comply, while others require immediate adaptation to MiCA rules. The roundtable suggested that EEA market participants could benefit from sharing regulatory best practices from different countries to create greater clarity on compliance expectations.

Given the uncertainty surrounding MiCA adoption in the EEA, the roundtable highlighted several strategies for Norwegian and EEA-based CASPs to navigate the transition period effectively. Engaging in regulatory dialogue was emphasized as a key step, with participants agreeing that Norwegian CASPs should actively seek clarifications

from local regulators on MiCA's timeline and any potential temporary measures available for firms already registered under existing frameworks. Collaboration with Liechtenstein and Iceland could further support the development of a unified EEA approach to MiCA implementation, ensuring consistency across jurisdictions.

Another approach discussed was leveraging reverse solicitation with caution. While reverse solicitation could serve as a temporary workaround for servicing EU clients, firms must be careful with their outreach and marketing efforts to avoid unintentional regulatory breaches. Establishing clear internal guidelines for customer engagement would help mitigate compliance risks during this uncertain period.

Structuring business operations for compliance was also identified as a priority. CASPs with employees or branches in EU Member States should assess whether their operations require restructuring to align with MiCA once the transition period ends. In some cases, firms may need to delay expansion plans into the EU until a clear licensing path is available, reducing the risk of non-compliance.

Finally, the roundtable emphasized the importance of monitoring and adopting best practices from other jurisdictions. Given the variability in MiCA grandfathering periods across the EU, EEA-based firms should closely follow how companies in other jurisdictions manage the transition. Sharing regulatory best practices among industry players could help create a more predictable and coordinated compliance strategy, allowing firms to proactively prepare for MiCA's eventual implementation in the EEA.

Primary Calls to Action on MiCA in Norway/EEA

The primary calls to action based on the discussions are:

- Develop Industry Guidelines for Reverse Solicitation – Given the lack of clear enforcement precedent, industry participants should create best practices for reverse solicitation compliance under MiCA.

- Encourage Information Sharing on Grandfathering Strategies – EEA firms should exchange insights and strategies on managing grandfathering discrepancies across jurisdictions.

3. Sustainability Disclosures under MiCAR

The final topic of the Oslo roundtable, presented by Kirsteen Harrison, Sustainability Director at Zumo, focused on the challenges that CASPs face in addressing MiCAR's sustainability disclosure requirements.

The discussion highlighted regulatory uncertainty, grandfathering disparities, and the absence of clear implementation guidelines, all of which contribute to an uneven playing field across EU jurisdictions. A key concern is that CASPs in jurisdictions with shorter grandfathering periods must comply with MiCAR's sustainability requirements sooner than their counterparts in other Member States, creating a first-mover disadvantage. Early adopters must navigate compliance without the benefit of regulatory clarifications, enforcement precedents, or additional guidance, while later entrants can observe and adapt based on evolving interpretations.

The session explored industry-driven solutions to support CASPs in demonstrating compliance efficiently and consistently across EU markets. It was noted that MiCA requires CASPs to disclose sustainability-related information under Article 66, but the lack of detailed operational guidance is not consistent with other sustainability disclosure requirements, such as CSRD or ISSB. Furthermore, Member States have taken different approaches to implementation, creating inconsistencies that place some market participants at a disadvantage.

In jurisdictions with shorter grandfathering periods, CASPs must determine disclosure methodologies and data sources without additional regulatory clarity. This issue is further compounded by the late-stage introduction of MiCAR's sustainability requirements, which were primarily a response to concerns over proof-of-work (PoW) energy consumption. Unlike dedicated sustainability disclosure

requirements such as CSRD or ISSB, MiCA's sustainability rules were added onto a financial services framework, making them structurally distinct from other EU-wide disclosure requirements. ESMA has already indicated that it does not plan to issue further guidance, leaving CASPs without a clear regulatory reference point.

Additionally, there is a misalignment between CASP and crypto-asset issuer reporting obligations—while CASPs must immediately comply with sustainability disclosure requirements, issuers of the assets they service may not yet be required to publish their own sustainability data via the White Paper. This gap further complicates CASP compliance efforts, as they may lack access to critical sustainability data, and yet be legally required to disclose it, putting the burden on the CASP.

While the discussion largely focused on addressing implementation challenges, a minority of participants expressed disagreement with the sustainability disclosure requirements themselves, arguing that they place unnecessary burdens on CASPs and introduce disproportionate obligations compared to other financial service providers. Moreover, some participants from Norway voiced frustration that they had not been part of the original EU legislative discussions on MiCA, yet now find themselves subject to these requirements as part of the broader regulatory framework. This sentiment reflects broader concerns about the imposition of EU financial regulations on non-EU jurisdictions within the EEA, raising questions about the extent to which local regulatory autonomy can be maintained.

To address the challenges around the sustainability discussion, the roundtable participants proposed developing an industry-driven compliance preparedness initiative, modeled on existing proposals for a Wiki-style MiCA resource.

A centrally provided compliance toolkit could serve as a repository for sustainability disclosures, compiling existing industry practices, regulatory interpretations, and implementation examples. While such a toolkit could provide structured guidance, practical templates, and best practices based on observed approaches, its role would primarily be to facilitate knowledge-sharing rather than to issue prescriptive guidance. Governance and oversight of such a resource would need careful consideration to avoid potential liability risks, particularly if it were

perceived as regulatory guidance without official endorsement. Ensuring transparency in its development and avoiding conflicts of interest among contributors would be essential to maintaining its credibility and usefulness to CASPs.

Finally, ongoing engagement with ESMA and the European Commission would ensure that industry concerns are considered in future refinements of the regulatory framework. As part of these efforts, Zumo conducted a 'snapshot' survey of MiCAR sustainability preparedness among CASPs and has shared the results, along with a compilation of key industry points requiring regulatory clarification, with the relevant authorities. By taking a proactive approach to compliance preparedness, the industry can create a more transparent, standardized, and effective sustainability disclosure process under MiCAR.

Primary Calls to Action on Sustainability Disclosures Under MiCAR

The primary recommendations emerging from this discussion are:

- Facilitate an industry-wide compliance toolkit compiling best practices, regulatory interpretations, and implementation examples, ensuring it remains a non-binding resource while addressing governance and liability considerations.
- Establish a collaborative knowledge-sharing initiative, allowing CASPs to exchange best practices and regulatory updates in real-time.
- Encourage standardization efforts to mitigate the risk of regulatory fragmentation and ensure MiCA's sustainability disclosures are applied consistently across Member States.

We thank all participants of the Oslo roundtable for contributing to the discussion:

Adam Funnell (Zumo), Amelie Arras (Zumo), Åsa Skålén (Realjuridik), Astrid Hagen (Skatteetaten - Tax Authority), Erik Vesterlund (Goobit), Hanne Reese Holm (Reese Legal), Helen Landenberg (Safello), Johan Kr. Falk-Pedersen (FIRI), Johan Toll (Chromaway), Kaja Vagle (Crypto Clarity), Kirsteen Harrison (Zumo), Magnus Jones (Nordic Blockchain Association), Mariana de la Roche W (BlackVogel), Marius J. Moreno-Sandnes (Investments), Morten Myrstad (Kaupr), Morten Søberg (Sparebank1), Nikolai Gobel (DNB), Nina-Luisa Siedler (Siedler Legal), Odd Kleiva (DNB), Oskar Åslund (AKJ), Peder Østbye (Norges Bank - Central Bank), Romena Urbonaite (Axiology), Torbjørn Bull Jenssen (K33), Torkel Rogstad (Barebitcoin), Torstein Thinn (AKJ), MJM (Investments), Ken Erik Oelmheim.

DARTE SERIES

Lisbon

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the Digital Asset Round Table Expert (DARTE) Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks and additional regions.

The Lisbon MiCAR Expert Roundtable was hosted at Biblioteca Palácio Galveias on February 28th, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on reporting obligations, passporting processes for countries lacking their designated NCA, and third country (non-EU) token issuers under MiCAR.

We extend our sincere gratitude to the European Commission, Crypto Risk Metrics, and FIO Legal for their invaluable support in making this roundtable possible. Special thanks to Tim Zölitz, Luiza Rey, and Anthony Day for their contributions to the discussions.

This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.

1. Reporting Obligations According to Art. 66 (5) MiCAR

The first topic of the Lisbon roundtable, presented by Tim Zölitz, CEO of Crypto Risk Metrics, focused on the Reporting Obligations according to Article 66 (5) MiCAR: From December 30, 2024, CASPs and issuers of crypto-asset white papers are required to disclose information on energy consumption and greenhouse gas (GHG) emissions related to the crypto-assets they service.

These disclosure obligations present several practical implementation challenges, particularly concerning how this information is presented. According to guidance provided by ESMA, CASPs must prominently display on their websites information on the principal adverse environmental impacts associated with the crypto-assets they service. Additionally, MiCAR mandates that this information must be "fair, clear, and not misleading."

1. Placement of Disclosures:

One significant ambiguity discussed is the interpretation of the term "prominent place." The absence of a precise definition creates uncertainty, especially for CASPs whose primary interaction with customers occurs through mobile applications rather than websites.

Participants of the roundtable proposed and discussed some solutions to address these practical challenges. It has been noted that a uniform solution for all CASPs is neither apparent from the guidelines nor feasible due to the different setup of CASPs.

The roundtable agreed that the term "prominent place" should be interpreted flexibly, as long as the disclosures remain easily accessible and clearly visible to customers. Suitable approaches include:

- A clearly labeled link within the website's main navigation or footer.
- Placement on crypto-asset-specific webpages.
- Extending this principle to apps and similar communication means, ensuring compliance aligns with customer interactions.

While MiCAR requires the placement "on the website"only, the participants agreed that where the primary point of contact with the customer is an app and not a website, the disclosure requirements should be applied for the app as well. The legislator's main intention was to provide information to the CASP's customers and the reference to the website only may not be taken as limitation.

2. **Downloadable format:**

Further complicating the matter, the regulation explicitly requires CASPs to provide sustainability data in a downloadable format on their websites. However, the requirement to disclose "material changes" references only the presentation on websites, without clarifying if these updates must also be provided as downloadable files. Having discussed the issue, the roundtable recommended adopting downloadable files for both original disclosures and subsequent updates, simplifying compliance while maintaining transparency.

3. **Use of multiple DTIs:**

Another critical issue arises from ESMA's requirement to identify crypto-assets using Digital Token Identifiers (DTIs). The current structure necessitates individual DTIs for the same crypto-asset issued across multiple blockchains, resulting in numerous separate disclosures for economically identical assets. For example, SushiSwap has more than ten distinct DTIs across various blockchain networks, all requiring separate disclosures which complicates the reporting process and negatively impacts transparency for consumers.

The experts discussed the issue and agreed that in order to avoid confusion by issuing multiple, diverging reports for a token issued on a number of blockchains such tokens should be grouped . Creating a group of tokens in such cases and providing for a single report including the data for all tokens issued across various chains support the legislative intention for transparency, specifically for the key indicator "energy consumption".

In this regard, participants supported adopting the "Functionally Fungible Group" (FFG) approach developed by the Digital Token Identifier Foundation (DTIF) to streamline disclosures. This method aggregates multiple DTIs representing economically equivalent crypto-assets into a single identifier, significantly simplifying reporting obligations.

This solution not only reduces operational complexities for CASPs but also enhances consumer transparency by providing a unified, comprehensible disclosure for each economic crypto-asset group.

Expert opinion on the reporting obligations according to Art. 66 (5) MiCAR
The experts agreed on the following current best practices: • **"Prominent Placement" Requirements:** Best practice regarding the term "prominent place" is to choose an easily accessible and clearly visible place on both the CASP's websites and its mobile application, if the latter is a main tool to interact with customers. • **Downloadable file in case of "material changes"**: The industry recommends to CASPs to provide downloadable files for initial sustainability disclosures and subsequent material updates, enhancing transparency and simplifying compliance processes. • **Adopt Token Grouping (FFG) Methodology:** Regulators and industry participants should endorse the use of Functionally Fungible Groups (FFGs) or similar methodologies as a standard for aggregating economically identical crypto-assets which are issued on multiple chains, significantly reducing reporting complexity, enhancing transparency, and improving consumer understanding.

2. Passporting Process According to Art. 65 MiCAR.

The second topic of the Lisbon roundtable, presented by Luiza Rey, founder of FIO Legal, focused on the Passporting Process according to Article 65 MiCAR.

Under Article 65 of MiCAR, CASPs authorized in one EU Member State can operate across multiple Member States by notifying their home national competent authority ("NCA"), which then informs the host NCAs. However, procedural challenges arise in situations where Member States have not yet designated their NCA responsible for MiCAR authorizations.

The expert group discussed specifically Portugal, where the responsibilities are expected to be assigned to either CMVM or Banco de Portugal. Banco de Portugal (BdP) has publicly indicated it currently

cannot process MiCAR authorization requests due to Portugal's delay in appointing a designated NCA. This absence creates uncertainty regarding which authority should receive notifications when a foreign CASP intends to passport into Portugal, potentially obstructing the passporting process and complicating cross-border service provision under MiCAR.

In response to such regulatory gaps, participants discussed proactive strategies for CASPs:

1. CASPs operating or intending to operate in jurisdictions without a clearly designated NCA should proactively include all potentially relevant authorities in their notification (request), demonstrating due diligence and a clear intent to comply. For instance, in Portugal, CASPs should notify both the authority currently responsible for AML supervision (Banco de Portugal) and the expected NCA under MiCAR (potentially CMVM, though not yet confirmed).

2. CASPs should align their compliance documentation with MiCAR standards rather than outdated national regulations, ensuring readiness when an NCA is formally designated.

3. Notifications should also be submitted to overarching EU bodies such as ESMA and EBA to strengthen regulatory oversight and ensure broader compliance coverage.

4. Maintaining comprehensive records of all notifications sent is recommended as best practice, minimizing risks of potential legal disputes related to compliance.

The roundtable highlighted the broader issue of "notification gaps" or a "broken chain" of communication that arises when home NCAs lack clear points of contact within host jurisdictions.

In addition to Portugal, other jurisdictions including Poland, Norway, and Romania were mentioned as experiencing similar uncertainties.

Expert opinion on Passporting According to Art. 65 MiCAR
The experts agreed on the following current best practices: • **Adopt a Proactive Notification Approach**: CASPs should proactively (request to) notify all potentially relevant national authorities and EU regulatory bodies in jurisdictions lacking clearly designated NCAs to ensure operational continuity and compliance transparency. • **Encourage Regulatory Clarifications by ESMA and EBA:** Industry participants should request and advocate for additional guidance and clarity from ESMA and EBA regarding passporting notification processes, particularly in scenarios where NCA designation remains incomplete or unclear. • **Highlight the Need for Designated NCAs in All Member States:** CASPs and the wider crypto community should raise their voices to call member states to prioritize the final designation of their respective NCAs without any further delay to ensure a seamless passporting notification process.

3. Learnings from non-EU based L1s and White Papers

The third and final topic of the Lisbon roundtable, presented by Anthony Day from Midnight, focused on the learnings derived from third country (non-EU) Layer-1 blockchain projects looking into issuing a crypto-asset white paper, specifically in the context of token launches and airdrops under MiCAR.

One of the main issues highlighted by the participants is the choice of EU jurisdiction for notifying a MiCAR white papers. A MiCAR white paper needs to be notified to the competent authority in the home member state of the issuer. Art. 3 (33) (c) MiCAR states, that the home meber state for non-EU players is "either the Member State where the crypto-assets are intended to be offered to the public for the first time or, at the choice of the offeror or person seeking admission to trading, the Member State where the first application for admission to trading of those crypto-assets is made" Therefore, non-EU issuers may decide which EU jurisdiction they opt in.

The experts discussed a number of questions around the selection of a Member State for projects that intend to access the EU market. They identified the following key considerations:

- Member States such as Germany, the Netherlands, and France were noted as experienced and knowledgeable counterparts due to their historical engagement with crypto-related regulations. These countries may be chosen for reputational reasons but are feared for overcomplicated and lengthy processes.
- Certain jurisdictions may adopt a less stringent or more streamlined approach, potentially reducing the administrative burden for blockchain projects.
- In general, Western European Member States were perceived to offer greater reputational advantages compared to Eastern European counterparts.
- The presence of project staff or advisors in a Member States may facilitate smoother interactions with the local NCA.
- It does not seem advisable to chose on of the jurisdictions which did not yet assign their national competent authority.

To further simplify and streamline the submission process, the roundtable proposed establishing a unified, EU-wide digital submission portal. Such a portal would enable projects to submit whitepapers and select their preferred NCA, with subsequent automatic distribution of documentation to all other NCAs, if the whole EU is targeted. This would enhance transparency, improve efficiency, and promote consistency across regulatory engagements.

Expert opinion on L1s and Airdrop Whitepapers:
The experts recommended: • **Develop Cross-Jurisdictional Reviews:** The industry should develop and maintain (i) an EU-wide overview and comparison of the pros and conts for choosing an EU jurisdiction as home member state by third country (non-EU) issuers, and (ii) guidelines detailing the evidence required for submissions to the relevant NCA, including handling "material changes" during the mandated 20-day review period following the initial notification to such NCA. • **Establish a Centralized Submission Platform:** The round table proposes to create a unified EU-wide digital submission platform that allows projects to submit white papers to the relevant NCA, with automatic notification to and coordinated feedback from other relevant NCAs.

We thank all participants of the Lisbon roundtable for contributing to the discussion:

Adam Sadler (Intergiro), Ana Marques (Antas da Cunha), Anthony Day (Midnight), António Rolo (Banco Central de Portugal), Ashik Remetula (ML adv), Carlos França (Definancy), Catarina Veloso (Notabene), Daniel Silva (Polícia Judiciária), Duncan Smith (Uphold), Ege Enginol (Lawyer), Hugo Volz Oliveira (New Economy), Joana Perreira (IMS), Joana Rola de Veludo (Algorand foundation), João Matos Cruz (ANIPE), Joao Vieira dos Santos (CMVM), Jose Reis (Bloq4U), Leid Zejnilovic (Centro blockchain and Reg Tech Lab), Luiza Castro Rey (FiO Legal), Marcio Matos (MM Law), Mariana de la Roche W. (BlackVogel), Martinho Lucas Pires (Fintech House), Miguel Matos (PS), Nina-Luisa Siedler (siedler legal), Nuno Lima Luz (Blockchain Association), Paolo Cardoso Amaral (Católica), Ricardo David (Polícia Judiciária), Ricardo Filipe (Luso Digital Assets), Tim Zölitz (Crypto Risk Metrics), Yulia Murat (Global Ledger), Zalan Noszek (Taxbit).

DARTE SERIES

Brussels 2.0

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks.

The Brussels 2.0 DARTE edition was hosted by the European Commission on March 14th, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on the harmonisation of the Digital Operational Resilience Act (DORA) and European Banking Authority (EBA) Outsourcing Guidelines, the proportionality principle in regulation, and the integration of Decentralised Finance (DeFi) within existing regulatory frameworks.

We extend our sincere gratitude to the European Commission, Project Catalyst and DLT Finance for their invaluable support in making this roundtable possible. Special thanks to Joachim Schwerin, Rabia Karaarslan Turkut, Miguel Vaz, and Anne-Grace Kleczewski for their contributions to the discussions.

This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.

1. **Harmonisation of DORA and EBA Outsourcing Guidelines**

The first topic of the Brussels roundtable, presented by Rabia Karaarslan Turkut, Information Security Officer at DLT Finance AG, focused on the regulatory overlap between the DORA, MiCAR, and EBA's Outsourcing Guidelines.

Participants discussed the compliance challenges faced by CASPs due to fragmented and overlapping obligations under these frameworks. Particularly, concerns were raised regarding subcontracting and complex provider chains, emphasizing the difficulty in ensuring compliance beyond direct contractual relationships. Additionally, the complexity of maintaining multiple outsourcing registers, as required separately by DORA, MiCAR, and the EBA guidelines, was highlighted as a key operational burden.

Regulatory Alignment Challenges:

The roundtable explored specific compliance obligations, including:

- MiCAR Article 73: Requires CASPs to maintain written outsourcing agreements and comprehensive governance structures, with detailed documentation outlined by the regulatory technical standard (RTS) in form of a commission delegated regulation (CDR) on record-keeping.
- DORA Articles 28-30: Set rigorous standards for ICT third-party risk management, mandating via the relevant Commission Implementing Regulation on the Register of information a structured register of third-party ICT providers.
- EBA Outsourcing Guidelines (2019): Introduce tiered governance, monitoring, and due diligence obligations, explicitly differentiating between critical and non-critical outsourcing functions.

Participants highlighted ongoing uncertainty regarding the continued applicability of the 2019 EBA guidelines to MiCA-licensed CASPs. Article 73 MiCA contains an explicit provision on outsourcing for CASP and EBA announced the replacement of the 2019 guidelines by their upcoming new Guidelines on Sound Management of Third-Party Risks, which EBA had not already published by the time of this DARTE session.

Best Practices and Solutions:

Participants positively acknowledged the approach taken by the German financial supervisory authority, BaFin. It consolidated multiple reporting obligations into a single "Notification of Outsourcing," significantly reducing redundancy and compliance burdens for CASPs.

The roundtable also highlighted the European Commission's recent removal of overly extensive ICT subcontracting chain monitoring requirements initially proposed by the European Supervisory Authorities (ESA). This adjustment was

welcomed by participants as a pragmatic step toward reducing compliance complexity.

Expert Opinion on Harmonising Outsourcing Requirements under MiCA, DORA, and EBA Guidelines

The experts agreed on the following current best practices and recommendations:

- Promote Regulatory Harmonisation Across Applicable Regulatory Frameworks: Industry members should work with their NCAs on consistent interpretation and application of MiCA, DORA, and (adapted) EBA Outsourcing Guidelines.
- Adopt Unified Reporting Mechanisms: Industry representatives should encourage their local NCAs to develop and adopt streamlined reporting systems, mirroring Germany's "Notification of Outsourcing". This will enable CASPs to efficiently satisfy multiple regulatory obligations through a single integrated reporting mechanism, significantly reducing compliance burdens and ultimately reducing the complexity arising from fragmented national practices.

Expert Opinion on Harmonisation of DORA and EBA Outsourcing Guidelines

The key recommendations from the discussion are:

- **Push for Regulatory Consistency Across Member States:** Industry representatives should request their NCAs to align on interpretation and enforcement of MiCAR, DORA, and EBA Outsourcing Guidelines uniformly across all Member States, eliminating fragmentation and enhancing regulatory predictability for CASPs.
- **Implement Unified Reporting Systems:** Industry representatives should request to apply integrated reporting solutions comparable to German BaFin's "Notification of Outsourcing," allowing CASPs to fulfill multiple regulatory requirements simultaneously, thereby significantly reducing administrative burdens and compliance complexity.
- **Waiving outdated EBA Guidelines:** Industry associations should call for an explicit waiver of the application of the current 2019 EBA Guidelines and for promptly finalizing the new EBA Guidelines on Sound Management of Third-Party Risks, explicitly outlining their applicability to MiCA-licensed CASPs.

2. Proportionality Principle

The second topic of the Brussels roundtable, presented by Miguel Vaz, focused on applying the proportionality principle within the context of DORA and its interaction with MiCAR, particularly concerning CASPs.

Participants discussed how DORA imposes comprehensive operational resilience requirements on CASPs, irrespective of their size, significantly increasing compliance costs. CASPs are mandated to maintain robust risk assessments, implement comprehensive business continuity measures, and ensure operational safeguards for their critical or important functions. These requirements intensify the reliance on third-party ICT providers, who must also comply with stringent operational resilience, security, and incident reporting standards. The number of ICT providers offering such service is limited. The resulting compliance burdens directly increase costs for CASPs and ICT providers, impacting MiCAR's Tier 1 capital requirements. These pressures particularly affect smaller institutions, potentially leading to market concentration, reduced competition, and diminished innovation capacity.

A critical issue addressed was the complexity and rising costs associated with intra group outsourcing under DORA. Corporate groups must individually ensure compliance for both outsourcers and recipients within their structure, even when the outsourcing is internal. Financial groups may establish dedicated ICT subsidiaries or shared-service entities which fall outside of DORA to streamline compliance, but participants agreed that these solutions could introduce additional overheads without fully mitigating costs. Streamlining intra group contracts and oversight procedures were considered beneficial, yet regulatory obligations remain demanding, especially for critical ICT functions.

Additionally, the participants addressed the importance of establishing harmonized auditing frameworks to mitigate compliance duplication. Cloud providers and ICT suppliers serving multiple institutions face redundant auditing obligations, emphasizing the need for standardized and pooled auditing approaches. Participants highlighted ongoing developments toward ISO-level auditing guidelines but stressed the urgency for more immediate practical solutions. Pooled audit models, such as those promoted by the EU Cloud User Coalition, were recognized as viable approaches to reducing regulatory burdens and compliance inefficiencies across the industry.

The experts recommended applying the proportionality principle to alleviate compliance obligations, particularly for smaller institutions. Recognizing the adequacy of existing intragroup risk management structures could significantly simplify regulatory requirements for corporate groups. Participants agreed that standardized auditing practices and collaborative audit models should be

actively encouraged by regulators and industry participants alike to streamline compliance procedures.

Expert Opinion on the Proportionality Principle

The key recommendations from the discussion are:

- **Extend Proportionality Principles to Reduce Regulatory Burdens**: Industry representatives should request their NCAs to apply proportionality and industry associations should work with regulators to include proportionality in regulatory guidelines to reduce compliance costs for smaller institutions. This will prevent a monopolisation of the market and maintain a competitive, innovative market environment.
- **Recognize Intragroup Risk Management Structures:** Company groups should discuss with their NCAs to what extent intragroup compliance frameworks could be acknowledged and industry associations should work on a proposal on acknowledging intragroup compliance structures, simplifying requirements and reducing redundant oversight obligations within corporate groups.
- **Adopt Unified and Collaborative Auditing Frameworks:** Encourage and facilitate the industry-wide adoption of standardized, pooled auditing models to minimize compliance duplication and reduce administrative burdens across the sector.

3. DeFi Integration by CASPs

The third topic of the Brussels roundtable, presented by Anne-Grace Kleczewski, explored the integration of DeFi by CASPs under DORA and its interplay with MiCAR.

Participants highlighted how the initial drafting of DORA did not fully account for developments in the Web3 market, specifically the growing integration of DeFi protocols by centralized actors, such as CASPs, and potentially also by traditional financial institutions. A key challenge discussed was the regulatory classification of DeFi, particularly given that it cannot easily be categorized as an ICT asset or as an ICT third-party provider due to its inherently decentralized nature and lack of direct control by regulated entities. The

roundtable emphasized the need for regulatory clarity to ensure DeFi integrations are achievable without inadvertently circumventing DORA's objectives or undermining user protection.

Participants also emphasized the importance of clearly defining DeFi. A consensus emerged around distinguishing infrastructure decentralization (such as blockchain layers L1, L2, and L3) from decentralized applications built atop these infrastructures. Assessing decentralization requires specific, measurable criteria, such as the number and distribution of nodes, node clustering, centralized sequencers, or points of centralization like Infura. For decentralized applications, the existence and control of access rights, number of token holders, and their governance activity were highlighted as critical indicators.

The group considered whether regulated entities, particularly CASPs, could integrate DeFi while remaining compliant with DORA. It was broadly agreed that DeFi protocols typically do not constitute ICT assets or ICT third-party service providers under DORA due to their decentralized and community-driven governance structures. However, ambiguity persists, particularly since DORA lacks an explicit exclusion for DeFi (comparable to MiCAR's Recital 22), creating uncertainty regarding the legal permissibility of offering DeFi services in the EU.

The discussions further addressed the implications of DORA's operational resilience requirements, notably the need to mitigate service downtime and ensure reliable backup measures. Participants suggested differentiating between service downtime (manageable under regulatory oversight) and underlying infrastructure downtime (often unavoidable, similar to general internet disruptions). A practical solution discussed was for regulated entities to engage validator clusters operated by trustworthy consortiums, subject to enforceable Service Level Agreements (SLAs).

A significant point of concern was how compliance with traditional regulatory frameworks like DORA could inadvertently centralize DeFi, fundamentally altering its core decentralized nature. Participants discussed the risk that, to achieve regulatory compliance, DeFi protocols may adopt centralized features, deviating from their original ethos. They underscored the importance of developing clearly defined decentralization metrics and assessing infrastructure quality transparently, such as through structured disclosures like those promoted by initiatives such as DeFiScan.

Participants concluded that a clear regulatory taxonomy categorizing different types of DeFi integrations is essential to clarify regulatory expectations and facilitate constructive engagement between regulators and industry participants.

Expert opinion on DeFi Integration by CASPs

The key recommendations from the discussion are:

- **Establish Clear Regulatory Definitions and Taxonomy for DeFi:** Industry experts should establish precise definitions, decentralization metrics, and a clear taxonomy distinguishing between infrastructure and application-level integrations for discussion and alignment with the regulators. This would clarify compliance obligations and support innovation.
- **Differentiate Regulatory Expectations Based on Integration Type:** Develop regulatory guidance that explicitly differentiates between core regulated services, ancillary or unregulated services, and CASPs acting solely as order transmitters. This differentiation would reduce uncertainty and encourage appropriate DeFi integrations.
- **Facilitate Transparent and Collaborative Assessment of Decentralization:** Promote industry-wide adoption of structured disclosure frameworks, enabling regulators to assess DeFi protocols transparently, thus balancing regulatory oversight with DeFi's decentralized characteristics without forcing undue centralization.
- **Create Legal Certainty Regarding DeFi's Applicability under DORA:** Industry associations should work on a proposal that explicitly clarifies the extent to which DeFi is included or excluded from DORA's scope, for discussion and alignment with the regulators in order to reduce market uncertainty and ensuring DeFi protocols remain viable innovation drivers within the European financial ecosystem.

We thank all participants of the Brussels 2.0 DARTE event for contributing to the discussion:

Alessandro Darold (Kraken), Alireza Siadat (Deloitte), Ana James (XReg), Anne-Grace Kleczewski (MME), Astrid Freier (VÖB), Avtandil Papuashvili (Fung Payment, Flexicheck), Belen Suarez Lopez (Go To Innovation), Clark Povey (Zumo), Elizaveta Palaznik, Giuseppe

Maria Blasi (International Investment Bank), Hugo Volz Oliveira (New Economy Institute), James Newell (GSR), Joachim Schwerin (European Commission), Juan Ignacio Ibañez (DLT Science), Lavan Thasarathakumar (Hogan Lovells), Magnus Jones (Nordic Blockchain Association), Mariana de la Roche (BlackVogel), Mat Yarger (Demia), Miguel Vaz (Hauck Aufhäuser Digital Custody), Nina-Luisa Siedler (siedler legal), Peter Großkopf (Allunity), Peter Kerstens (European Commission), Rabia Karaarslan Turkut (DLT Finance), Sebastian Higgs (Cordial Systems), Shota Natenadze (Ripple), Thibault de Lachèze-Murel (DFNS), Thorstein Thinn, Tommaso Astazi (B4E), Walter Borst (DLT Finance).

DARTE SERIES

Buenos Aires- Special Edition

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the Digital Asset Round Table Expert (DARTE) Series aims to enhance legal clarity within evolving regulatory frameworks worldwide. Expanding beyond its European focus, the DARTE Series hosted a Special Edition at MERGE Buenos Aires on March 25th, 2025, at Palacio Libertad during Merge Buenos Aires, bringing together regulators, policymakers, and industry experts from Latin America and Europe.

We extend our sincere gratitude to the European Commission, Project Catalyst, Merge and Binance and all participating regulators and experts for their invaluable contributions. Special thanks to Roberto E. Silva, Juan Carlos Reyes, Álvaro Castro Lora, Victor Rondon de Paula Moura, Nidia Soto, Gabriel Campa, and Mariana de la Roche for leading the discussions; to Fabio Budris Klaz for the support with the organization and to Gonzalo Cantero Puig for being our rapporteur.

The Buenos Aires DARTE Special Edition facilitated high-level discussions on regulatory frameworks for crypto-assets across Latin America. Participants from Argentina, Brazil, Colombia, El Salvador, Panama, and Peru shared their jurisdictions' regulatory approaches, highlighting key priorities and challenges. Mariana de la Roche provided a comparative overview of the European crypto regulation MiCAR.

Different from other DARTE sessions, in this Special Edition, we did not request selected experts to present specific regulatory problems or open questions regarding the implementation of a particular regulatory framework. Instead, representatives from various jurisdictions were invited to share detailed overviews of their current regulatory landscapes. Additionally, key industry leaders—Andrés, General Manager for Argentina and Southern Cone at Binance, and Jeffrey Siler from Input Output of the Cardano ecosystem—provided opening and closing remarks. After these presentations, participants engaged in an open dialogue to explore pathways toward regional regulatory harmonization, identify the primary challenges and blockers, and discuss strategies to foster greater cooperation across Latin America.

The jurisdiction-specific insights presented in this report reflect the individual perspectives of each representative regarding their country's regulatory framework. These overviews are simplified summaries based on approximately ten-minute presentations and, therefore, do not capture the complete regulatory landscape of each country. Each speaker did an exceptional job explaining, within their limited time, the main regulatory considerations, providing valuable context and an overview of their respective jurisdictions.

The conclusions drawn from the open dialogue represent the collective understanding of the group discussions and do not necessarily reflect the individual positions of any participant or the rapporteur.

Opening Keynote

Andrés, General Manager for Argentina and Southern Cone at Binance opened the session emphasizing the importance of regulatory clarity for integrating crypto with traditional finance. Highlighting Binance's regulatory compliance efforts across multiple jurisdictions, he stressed that clear regulations foster safe, transparent crypto adoption and institutional investment.

Country-specific Regulatory Insights

- **Argentina -** Roberto E. Silva (President, CNV) shared Argentina's recent efforts to regulate Virtual Asset Service Providers (VASPs), establishing a registry with approximately 140 registered entities. New regulations require local presence, capital adequacy, and AML compliance. Future initiatives include defining non-security crypto-assets and a tokenization framework.
- **Brazil -** Victor Rondon de Paula Moura (Advisor, CVM) outlined Brazil's regulatory progress, splitting responsibilities between the Central Bank and CVM for digital assets. Brazil emphasizes dialogue with the industry, employing regulatory sandboxes to facilitate innovation while clarifying rules around tokenized securities.
- **Colombia -** Nidia Soto (Blockchain Specialist, Fiscalía Nacional) detailed Colombia's current AML-focused regulatory framework, highlighting mandatory KYC and

transaction reporting. She mentioned ongoing Congressional proposals and initiatives by law enforcement agencies to better understand crypto-related crimes and enforce appropriate legal frameworks.

- **El Salvador -** Juan Carlos Reyes (President, CNAD) highlighted El Salvador's unique regulatory environment driven by Bitcoin's adoption as national currency. El Salvador prioritizes deep technological understanding among regulators and actively collaborates with other Latin American countries, aiming to establish the region as a global hub for real-world asset tokenization.
- **Panama -** Gabriel Campa (Head of Digital Assets, Towerbank) explained Panama's special regulatory position due to the absence of a national central bank. Towerbank transparently collaborates with regulators, advocating for simplified yet effective regulatory measures. He emphasized the importance of transparency in client interactions to maintain regulatory trust.
- **Peru** - Álvaro Castro Lora (Damma Legal Advisors) described Peru's evolving regulatory landscape, noting recent AML-focused regulations and proactive bank-led sandbox initiatives. While traditional banks previously viewed crypto cautiously, recent developments signal growing institutional openness toward the sector.

At the end Mariana de la Roche (Founder, BlackVogel) presented an overview of the European Union's Markets in Crypto-Assets Regulation (MiCAR), outlining key aspects such as definitions, passporting processes, sustainability disclosures, and proportionality principles, providing a comparative perspective relevant to Latin American regulatory approaches.

Open Dialogue & Harmonization Challenges

Participants engaged in an open debate, addressing key regulatory harmonization challenges across Latin America. Discussions delved deeply into defining securities versus utility tokens, regulatory oversight of offshore offerings, and practical strategies for enhancing regional cooperation.

1. Variations in national priorities complicate regional harmonization:

Participants emphasized that local contexts, economic instability, political polarization, and currency devaluation significantly influence each country's regulatory focus. In jurisdictions dealing with severe inflation and unstable economic conditions, regulatory authorities often prioritize immediate economic stabilization and consumer protection over harmonizing crypto-asset regulations across borders. These differing priorities make aligning regulatory approaches challenging, despite apparent commonalities.

2. Challenges in existing and previous regional alliances:

Participants acknowledged past efforts toward regulatory integration, such as attempts by Peru, Chile, and Colombia to merge their capital markets. These attempts have struggled primarily due to diverging mandates, inconsistent regulatory goals, and differing national interests among participating countries. It was also highlighted that the absence of clear regulatory authorities or frameworks in certain countries further exacerbates the difficulties in fostering effective alliances.

3. Effective harmonization requires mutual recognition and collaborative regulatory frameworks:

A common point of concern was the absence of clarity regarding the competent regulatory authority in several jurisdictions. It was noted that some countries still lack clearly defined regulatory bodies specifically tasked with overseeing digital asset activities. Participants agreed that initiatives such as regulatory sandboxes and cooperative frameworks could serve as effective tools for facilitating mutual recognition and cross-jurisdictional collaboration. Nevertheless, creating sustainable frameworks requires overcoming existing structural, political, and administrative barriers.

4. Stablecoins as a significant opportunity for the region:

Participants identified stablecoins as particularly valuable instruments for Latin America, emphasizing their potential to provide countries with highly devalued currencies greater competitiveness in international markets. Participants urged regulators to consider specific frameworks that support stablecoin adoption, highlighting their role in enhancing financial inclusion and economic stability in volatile economic contexts.

5. Insights from Additional Discussions:

During the dialogue, participants explored the definitions of securities and utility tokens across jurisdictions, noting general similarities to the U.S. Howey Test or adaptations of the investment contract concept. Differences emerged regarding how jurisdictions handle offshore token offerings. While some regulators asserted their authority based on target populations, others noted limitations in overseeing offshore activities unless directly targeting local investors. It was also emphasized that regulatory frameworks and legal consequences vary significantly; for instance, in certain jurisdictions, offering securities without appropriate disclosure could constitute a criminal offense.

El Salvador's regulatory model—particularly their comprehensive approach to Bitcoin adoption and digital asset regulation—was presented as an example of proactive adaptation, rooted in extensive regulator education and technological understanding. However, participants acknowledged that El Salvador's circumstances, including its dollarized economy and particular political environment, might not be replicable in other Latin American contexts.

Closing Remarks:

Jeffrey Siler from Input Output emphasized the critical importance of education for authorities and regulators. He noted that achieving proportional and effective regulatory frameworks depends on regulators' comprehensive understanding of blockchain technology and its potential. Siler underscored the essential role of education initiatives, such as DARTE, which facilitate informed dialogue between industry experts and regulators, ultimately supporting balanced regulation and fostering mass adoption of crypto-assets. He highlighted that jurisdictions lagging in technological understanding—particularly the U.S.—risk developing regulations influenced by political biases rather than technical realities, hindering innovation and broader adoption.

Final Observations:

Superficially, Latin American countries share substantial commonalities—not only in language and culture but also in regulatory approaches toward digital assets. Across presentations, consistent themes emerged around AML/KYC requirements, VASP (CASP) registration, and securities definitions. Nonetheless, this perceived alignment is an assumption drawn from brief conversations during the roundtable. A comprehensive review of each jurisdiction's regulatory regime would be necessary to substantiate these preliminary observations and further support harmonization efforts.

We extend our sincere gratitude to all participants for their invaluable contributions to the discussion: Alfonso Ayuso (Minos Global), Agustina Pérez Comenale (Binance), Alvaro Castro Lora (Damma Legal Advisors), Cora Cecchini (KillB), Daniel Mangabeira (Circle), Elio Grillo (Binance), Fabio Budris (Gov. Buenos Aires), Felipe Taborda (Taurus), Filip Berg-Nielsen (Volven), Gabriel Campa (Towerbank), Gonzalo Cantero Puig (Asensi), Jacob Cohen (TRM Labs), JJ (IO), Juan Camilo (Asensi), Juan Carlos Reyes (Comisión Nacional Activos Digitales, El Salvador), Juan Ignacio Orlando (Binance), Larissa Moreira (Itaú), Leonardo Tamayo Tamayo (KillB), Luis Ayala (BitGo), Marcelo Eduardo Souza (Prosegur Crypto), María Fernanda Juppet (CryptoMKT), Mariana de la Roche (BlackVogel), Mauro Guivenale (Santander Argentina), Milagros Santamaría (Crecimiento / Aleph Argentina), Nicolás Pechersky (Tools for Humanity), Nidia Soto (Fiscalía Nacional de Colombia), Pablo Casadio (Bit2Me), Pablo Corredoyra (finREG360), Presidente de Sociedad Argentina de Inteligencia Artificial, Roberto E. Silva (Comisión Nacional de Valores de Argentina), Santiago J. Mora (Cámara Argentina Fintech), Teófilo Beato (Crecimiento), and Victor Rondon de Paula Moura (CVM - Comissão de Valores Mobiliários).

DARTE SERIES

Paris

Initiated by Dr. Nina-Luisa Siedler and Mariana de la Roche W., the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks and region-specific issues.

The Paris DARTE edition was hosted at the French Ministry of Finance on April 9th, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on the EU's regulatory competitiveness in light of recent U.S. developments, the UK's evolving post-MiCAR framework, and the large-scale implementation of the Travel Rule.

We extend our sincere gratitude to the European Commission, Project Catalyst, BPI France, VerifyVASP, and Zumo for their invaluable support in making this roundtable possible.

This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.

1. **The EU's Regulatory Competitiveness in the Wake of US Acceleration**

The first topic of the Paris roundtable, introduced by Nathan Catania, Partner at XReg Consulting, centered on Europe's positioning in the global regulatory race for digital assets, particularly in light of recent developments in the United States. While MiCAR remains the most comprehensive crypto regulatory framework globally, its complex implementation and increasing compliance burdens are raising concerns over the EU's ability to maintain its first-mover advantage.

Shifting Global Dynamics

Participants discussed how U.S. policy momentum — such as the approval of crypto ETFs and renewed legislative efforts around stablecoins, CASPs, and token classification — is reshaping the global regulatory landscape. Some argued that the perception of the U.S. as a more innovation-friendly jurisdiction is growing, leading firms to reconsider market-entry strategies and licensing plans. Meanwhile, the UK is advancing its own regulatory approach, which may present an alternative to MiCAR, though its final shape and competitiveness remain to be fully assessed.

There was a strong sense that Europe's initial leadership could quickly diminish if MiCAR is not adapted to remain competitive. Participants questioned whether the EU should begin early discussions on a "MiCAR 2.0" to address emerging regulatory gaps and provide a more agile, innovation-supportive environment.

Key Pain Points Identified

- MiCAR's implementation timeline was described as overly ambitious, making compliance practically impossible for many actors within the deadline.
- Jurisdictional fragmentation persists: VASPs in France, for example, are struggling with stricter local requirements compared to other EU countries, prompting businesses to consider relocation outside the EU (e.g., UAE, Hong Kong, US).
- There is no clear delineation of DeFi within MiCAR, and overlap between e-money, MiFID, and MiCAR licensing requirements remains unresolved.
- ESMA's and EBA's Level 2 guidelines were described as disproportionate, overly influenced by legacy financial norms, and lacking clarity, particularly regarding stablecoin treatment under Article 50 MiCAR.
- Participants highlighted the unintended consequence of driving active traders away from the EU following the delisting of Tether by trading platforms.

Recommendations and Forward-Looking Perspectives

Participants proposed several strategic options to preserve and strengthen Europe's position:5. Create a lighter MiCAR regime or modular approach for startups and low-risk actors.

1. Focus regulatory energy on enabling tokenization and supporting blockchain's integration into traditional financial markets.
2. Encourage regulators to prioritize AML compliance as a first step, while easing the full suite of obligations in a phased manner.
3. Push for greater alignment and transparency in Level 2 guidance from ESMA and EBA.
4. Reassess restrictions around stablecoins and interest payments to avoid pushing innovation out of the EU.
5. Highlight the importance of painting a compelling long-term vision: Where do we want the capital markets to be in five years, and what role should blockchain play?

The overall sentiment was clear: unless the EU modernizes and harmonizes its capital markets, it risks becoming a regulatory "flyover zone," with capital flowing between the U.S. to the Middle East and Asia — bypassing Europe altogether. Participants emphasized the need to think boldly, act strategically, and build regulatory frameworks that reflect where the market is heading, not just where it is now.

Call to actions regarding EU Regulatory Competitiveness

The key call to actions from the discussion are:

- **Reignite Strategic Dialogue on MiCAR 2.0 and Long-Term Vision:** Launch structured conversations on the future of MiCAR and Europe's broader digital finance framework, including the role of tokenization, DeFi, and blockchain integration into traditional capital markets.
- **Ensure Proportional and Predictable Implementation Across Member States:** Encourage consistent application of MiCAR across the EU, with tailored implementation timelines and requirements that avoid jurisdictional arbitrage and promote startup-friendly conditions.
- **Engage with ESAs to Align Level 2 Measures with Market Realities:** Advocate for practical, innovation-supportive technical standards by strengthening public-private collaboration with ESMA and EBA and addressing regulatory overreach that risks eroding EU competitiveness.

2. Navigating UK Compliance in the Post-MiCA Landscape

The second topic of the Paris roundtable, introduced by Devina Paul, Deputy CEO & CFO at Zumo, focused on the emerging UK regulatory framework for crypto-assets and how it compares with MiCAR. While the UK is positioning itself as a middle ground between the EU and the US, participants raised significant concerns about the operational burdens and ambiguities in the current UK proposals.

UK's Approach: Aiming for Balance, Risking Overreach

Participants discussed how the UK's proposed framework introduces specific admissions, disclosure, and market abuse rules intended to balance consumer protection and innovation. However, the practical impact of these rules may result in a higher compliance burden than MiCAR itself.

Participants noted that the proposed UK framework introduces obligations for crypto-asset trading platforms (CATPs) to publicly disclose their asset admission due diligence processes and to maintain clearly defined rejection protocols. While designed to promote transparency, these measures risk exposing proprietary assessments and adding administrative overhead without a clear compliance benefit.

Another key concern is the absence of provisions for mutual recognition of MiCAR-compliant white papers. Without the ability to reuse disclosures already approved under MiCAR, businesses operating across both jurisdictions face duplicative requirements and unnecessary compliance burdens.

The UK's proposed market abuse regime was also seen as overly demanding. It places significant responsibility on the industry to develop and operate cross-platform systems for identifying and reporting suspicious activity, with little infrastructure or guidance provided by regulators to support implementation.

Further compounding these issues is the fragmented nature of the UK's approach. Rather than issuing a centralized regulatory framework, requirements are spread across various documents and regimes — including financial promotions, asset disclosures, consumer duty rules, and stablecoin regulations — creating confusion and operational inefficiencies for market participants.

Participants acknowledged previous concerns about the lack of proportionality in the UK's proposed rules — particularly the one-size-fits-all model, which could place undue burdens on smaller or low-risk entities. However, it was noted during the discussion that on April 8th, the FCA publicly committed in its 2025/26 work programme to investing £7.8 million "in developing and implementing a proportionate and safe regulatory regime for crypto activities in the UK, promoting a competitive and innovative sector." This statement was seen as a positive signal, and participants expressed hope that proportionality would be more clearly reflected in the forthcoming regulatory drafts.

Finally, there remains no clear indication of the transition periods or run-in timelines that will be offered to businesses to adapt to the new framework, leaving firms uncertain about how and when to begin implementation planning.

Compliance and Market Implications

Participants expressed concerns that these burdens may hinder UK competitiveness by making the country less attractive for both domestic startups and international firms considering UK expansion. The regulatory uncertainty and complexity may particularly affect small businesses already struggling under MiCAR's cost and timing pressures.

The discussion highlighted:

1. The industry's role in building reporting mechanisms, as the regulator shifts responsibilities for transparency and suspicious activity monitoring onto market participants.
2. Concerns over how a lack of structured guidance could stall innovation and capital inflows. Participants noted lessons learned from the MiCA experience, emphasizing that early and clear guidance had been instrumental in helping stakeholders prepare for implementation. It was suggested that adopting a similarly structured approach in the UK could provide a competitive edge.
3. The need for simplicity in investor communications — providing only what users genuinely need to make informed decisions, avoiding information overload.

Recommendations and Strategic Opportunities

To ensure the UK maintains a competitive yet responsible regulatory framework, participants emphasized the need to develop a single, crypto-specific regulatory handbook. This consolidated source would integrate key obligations across various areas, simplifying compliance and offering clarity for firms operating in the UK market.

There was strong support for recognizing MiCAR white papers as sufficient to meet UK disclosure requirements. Such mutual recognition would significantly reduce duplicative compliance processes for firms already regulated under EU rules, promoting cross-border efficiency and lowering barriers to entry.

Participants also advocated for streamlining due diligence procedures and introducing proportional rules tailored to the type of market actor, the size and function of the asset, and the associated risks. This approach would create a more balanced and innovation-friendly environment, encouraging diverse participation in the UK's digital asset market.

There was broad consensus around the table that the FCA has historically excelled at drafting clear and effective regulation. Participants emphasized that maintaining this strength will be critical as the FCA moves forward with its crypto-specific framework, particularly to avoid overly complex or ambiguous disclosure obligations.

Call to Actions Regarding UK Regulatory Framework

The key call to actions from the discussion are:

- **Develop a Consolidated Crypto Rulebook:** Encourage UK regulators to streamline rules into a unified handbook, minimizing overlaps and providing clarity across disclosure, promotion, market abuse, and stablecoin obligations.
- **Introduce Proportionality and Recognition Mechanisms:** Call for activity-based thresholds, tiered requirements based on investor types and asset risk, and equivalency recognition for MiCAR disclosures to reduce duplicative burdens for international firms.
- **Strengthen Industry-Regulator Collaboration:** Support public-private dialogue to co-design infrastructure for suspicious activity reporting and investor transparency tools, ensuring practicality and interoperability across jurisdictions.

3. Travel Rule Implementation at Scale

The third session of the Paris roundtable, led by Elsa Madrolle from VerifyVASP, focused on the complex operational, technical, and legal challenges surrounding the implementation of the EU Travel Rule Regulation (TFR). Despite being technically in force from December 2024 — with a tolerance period extending until July 2025 — participants expressed concern over fragmented understanding, limited and sometimes contradictory guidance, and low alignment across jurisdictions.

Regulatory and Operational Friction

Participants highlighted widespread confusion across Member States regarding the interplay between TFR and MiCAR licensing obligations. Many CASPs are adopting inconsistent or superficial due diligence practices in order to maintain unrestricted transfers, often at the cost of violating both GDPR and TFR mandates. Examples included sending personal data to unverifiable recipients or proceeding with transfers despite inadequate or missing counterparty verification.

The conversation also explored how many technical implementation tools for the Travel Rule are falling short of regulatory requirements. Persistent issues flagged on several occasions by the FATF include verification failures, delayed data transmission, poor interoperability across VASP systems, and an overreliance on outdated technologies such as email.

These deficiencies not only raise compliance risks but also prompt traditional banks to cut fiat rails from VASPs perceived as high-risk.

Public-Private Collaboration and the Paradox of Identity

Some attendees emphasized that the current framing of identity — as names and addresses — is often ineffective for AML purposes. Instead, a more functional approach to identity verification was suggested, such as using blockchain-based attestations (e.g., "over 18," "not sanctioned") to determine transaction eligibility.

The paradox of transparency was also debated: while blockchain offers immutable traceability, cutting off illicit actors too early could hinder valuable forensic tracking. At the same time, letting high-risk VASPs participate unchecked compromises the integrity of the system and risks regulatory backlash. Participants stressed the importance of aligning on when and how counterparties should be restricted — and by whom.

Discrepancies Between Level 1 and Level 2

One of the concerns raised was the inconsistency between Level 1 legislation and Level 2 technical standards under the Lamfalussy process. While Level 1 acts serve as the legal foundation, some of the Level 2 provisions of recent crypto-asset regulations appear to be more restrictive and create interpretation challenges for both NCAs and CASPs. The discussion reaffirmed that Level 1 should prevail in any legal conflict and called for better clarity and alignment between the two levels.

Strategic and Tactical Paths Forward

The group ultimately agreed that both short-term tactical solutions and long-term strategic proposals for alternatives or enhancements are necessary. In the near term, a best practices guide on Travel Rule implementation should be developed to harmonize approaches and improve compliance. In the long term, if unresolved Travel Rule challenges remain, the industry can proactively propose an alternative regulatory model for AML compliance in crypto — one that leverages the transparency and programmability of blockchain technology.

Call to Actions regarding Travel Rule Implementation
The key call to actions from the discussion are: • **Publish a Travel Rule Best Practices Guide:** Develop a practical, jurisdiction-neutral guide outlining minimum technical and compliance standards, including counterparty VASP due diligence, VASP verification, data handling, and addressing interoperability issues to support both regulators and industry stakeholders. • **Clarify Level 1 vs Level 2 Hierarchies:** Advocate for clear legal interpretation guidance from the European Commission on the application of Level 1 versus Level 2 texts, to prevent misapplication and ensure proportional enforcement by NCAs. • **Explore a Strategic Alternative to the Travel Rule:** Begin a community-driven initiative to conceptualize and propose a long-term alternative or set of enhancements to the current Travel Rule, consolidating existing initiatives and emphasizing privacy-preserving identity, transaction traceability, and public-private oversight.

We thank all participants of the Paris DARTE event for contributing to the discussion:

Akli Le Coq (Ministry of Interior), Alex Wu (Stellar), Amelie Malmaison (AWIC), Cara Hennessy (Provenance Compliance), Catarina Veloso (Notabene), Celine Henry (Meria), Darren Robeiro (Zumo), Devina Paul (Zumo), Elsa Madrolle (VerifyVASP), Emilie Lahoud (BPI France), Frederik Gregaard (Cardano), Henriette Craindart (BPI France), Joanna Rindell (Trili), Juan Jiménez Zaballos (Santander / Alastria), Lorna Hutchman (BlackVogel), Mariana de la Roche (BlackVogel), Nathan Catania (XReg), Nina-Luisa Siedler (siedler legal), Peter Kerstens (European Commission), Razali Samsudin (Sustainable ADA), ShihYun Chia (VerifyVASP), Simon McFeely (Finvisor), Tracy Wood (Zumo).

DARTE SERIES

Milan

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks and region-specific issues.

The Milan DARTE edition was hosted at Università Bocconi on May 13th, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on critical legal and compliance challenges under MiCAR. The session focused on three core topics: legal uncertainty in the application of Title II (Prof. Francesco Paolo Patti, Università Bocconi), the role and liability of third parties in whitepaper drafting (Juan Ignacio Ibañez, MiCA Crypto Alliance), and the practicalities of the prevention and detection of insider dealing (Delphine Forma, Head of Policy, Europe, at Solidus Labs).

We extend our sincere gratitude to the European Commission, Project Catalyst, Università Bocconi, and MiCA Crypto Alliance for their invaluable support in making this roundtable possible and to Nena Dokuzov (Government of Slovenia) for her insightful Keynote.

This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.

1. Legal Uncertainty in the Application of Title II MiCAR

The first topic of the Milan roundtable, introduced by Prof. Francesco Paolo Patti from Università Bocconi, explored the interpretative and operational challenges stemming from the application of Title II of MiCAR. While Title II introduces a harmonized EU-wide framework for the drafting, notification, and publication of white papers, intended as an alternative to the traditional prospectus regime, participants emphasized that considerable legal uncertainty persists, particularly for borderline cases and novel token types.

The discussion began by addressing the ambiguity around when a crypto-asset qualifies for a white paper obligation under MiCAR. Key definitional gaps persist around terms like "offering to the public" and "admission to trading on a trading platform," especially in relation to utility tokens and memecoins. Participants noted that many tokens lack any tangible utility or associated rights, yet still carry significant market risk. Whether such assets fall under Title II's requirements is not always clear, and in the absence of a safe harbor or exemption, platforms may be exposed to legal liabilities.

Further uncertainty surrounds MiCAR's exemption regime for utility tokens, which lacks detailed interpretative guidance. This has led to diverging approaches by CASPs and regulators alike, potentially undermining harmonization and investor protection goals. Participants agreed that the current lack of regulatory clarity is placing CASPs in a difficult position, forcing them to make high-stakes decisions on white paper publication, often with limited legal certainty.

Key Practical Issues Identified

A number of additional concerns were raised:

- Platforms may face liability even when they are not the issuer: Under Article 15 MiCAR, trading platforms and their senior management could be held responsible for investor losses arising from misleading or incomplete white papers, even when they were not involved in the project directly. The duty to ensure accuracy remains regardless of authorship.
- "Rogue" white papers are emerging: Participants flagged that in some cases, white papers are being uploaded by individuals with no formal link to the crypto project, potentially breaching intellectual property rights, spreading misinformation, and complicating regulator oversight.
- MiCAR lacks clarity on who qualifies as a "third-party drafter": While Article 6 permits persons other than the issuer to submit a white paper, it does not specify who these persons can be. This regulatory vacuum creates uncertainty, especially as third-party drafting might otherwise offer a solution to operational bottlenecks in white paper preparation.

- Liability extends beyond delisting: Contrary to prior expectations, white papers are not treated as temporary marketing tools. Legal liability remains even after the token is delisted or the white paper is removed from public registries. Incomplete or unclear documentation could trigger legal action long after the asset has left the platform.

Recommendations and Forward-Looking Perspectives

Participants broadly agreed that the implementation of Title II must be accompanied by:

1. Clearer ESMA-level guidance on definitions such as "offer to the public," "utility token," and "third-party drafter" to harmonize enforcement across Member States. (If this topic is interesting for you check the Berlin 2.0 Round Table insights)
2. Stronger institutional recognition that white papers must be treated not just as compliance documents, but as long-term accountability instruments.
3. A cautious approach to treating memecoins and borderline tokens as "out of scope," given their potential to cause investor harm. Regulators and CASPs should assume these assets fall within the Title II perimeter unless an explicit exemption is provided.
4. Proactive compliance by trading platforms, treating white paper notification as a standard requirement before listing any token, regardless of its utility claims.

Participants concluded that if Title II's ambiguities are not resolved, it may expose both platforms and investors to unnecessary risk. In the interim, conservative interpretations and proactive disclosures are likely to be the safest route.

Call to actions regarding legal clarity under Title II MiCAR

The key call to actions from the discussion are:

- **Clarify key definitions and interpretative scope under Title II:** Urge ESMA to issue explicit guidance on core concepts such as "offer to the public," "utility token," and the role of "third-party drafters" to reduce fragmentation and ensure consistent application across the EU.
- **Reinforce platform accountability frameworks:** Encourage CASPs to adopt internal review mechanisms for all white papers, whether authored by issuers or third parties, and treat notification as a compliance prerequisite before listing any token to mitigate legal and reputational risks.
- **Establish long-term liability protocols:** Promote the development of legal safeguards and disclaimers clarifying liability boundaries, particularly in relation to delisted tokens, to ensure white papers are treated as enduring legal instruments rather than temporary promotional content.

2. Third Party Whitepaper Drafting: Liability Matters and Collective Action

The second session of the Milan roundtable, led by Juan Ignacio Ibañez from the MiCA Crypto Alliance, explored the legal and operational risks facing trading platforms under MiCAR when drafting whitepapers for crypto-assets not issued by themselves.

The discussion focused on the implications of Article 15 MiCAR, which establishes significant liability for misleading information in whitepapers, even for platforms not directly involved in the crypto asset project.

Legal and Strategic Dilemmas for Trading Platforms

Participants acknowledged that some crypto-assets lack cooperative or even identifiable issuers, offerors, or persons seeking admission to trading. While MiCAR requires a whitepaper to list such tokens, platforms face a dilemma: forgo the trading volume and revenue by refusing to list, or accept the liability risk by drafting the whitepaper themselves.

This creates a challenging environment for CASPs. Article 15 holds them and their management bodies individually liable for any misleading or incomplete information in the whitepaper, even if they are not the asset's originators. The risk is heightened in jurisdictions like Germany or France where such liability claims are more likely

to succeed, compared to countries like Italy.

The roundtable also raised again concerns about the emergence of "rogue" whitepapers submitted voluntarily by third parties without involvement of the actual crypto project. These documents, sometimes misleading, duplicative, or based on spam-like marketing further complicate compliance and threaten regulatory credibility. The MiCAR framework permits third-party drafting but offers no clarity on who these "other persons" are under Article 6, nor whether they are liable under Article 15.

Collective Action and Pooling Liability

One proposed solution involved CASPs pooling their efforts—and liabilities, through a jointly funded and governed legal vehicle. This cooperative approach could allow for standardized, high-quality whitepaper drafting backed by expert input. Participants discussed structuring this as a multi-tiered LLC without named directors to minimize liability exposure.

Still, this concept raised several questions:

- Would such a structure pass antitrust scrutiny?
- How would governance, capital contributions, and liability sharing be managed?
- Would large CASPs support smaller competitors, or would free-riding be inevitable?

Others pointed to Article 4(7) MiCAR, which requires written consent to reuse a whitepaper, as a mechanism to address IP concerns and free-rider problems.

Industry Realities and Regulatory Expectations

Several participants emphasized that this is primarily an industry problem, unlikely to be resolved in time through regulatory intervention. While supervisory authorities may offer limited guidance, the speed at which industry must act will outpace any EU-led solution. There was also discussion around creating whitepaper benchmarking tools to help standardize disclosures and reduce liability risk through industry validation.

Participants further noted that even post-delisting, residual liability from whitepapers remains actionable, underscoring the importance of long-term compliance thinking. AI-generated whitepapers do not remove liability from human actors, and plaintiffs are expected to target the most legally and financially accessible defendants, not necessarily those who first submitted a document.

Finally, some attendees argued that risk for well-known assets like Bitcoin may be minimal, while others disagreed, maintaining that regulatory scrutiny could still apply. The conversation ended on a cautionary note: third-party whitepapers might seem to reduce legal risk, but unless they are integrated with the issuer's input, they may create more liability than they solve.

Call to actions regarding third party whitepaper drafting

The key call to actions from the discussion are:

- **Establish a voluntary liability pool for whitepaper drafting:** Encourage trading platforms to consider a collective legal structure to jointly draft and submit whitepapers for crypto-assets without cooperative issuers. This would pool compliance costs and distribute legal exposure more equitably across market participants.
- **Develop industry-led benchmarking standards:** Support the creation of shared whitepaper benchmarking or scoring tools to assess completeness, fairness, and clarity. Such tools can act as "public goods" for the crypto sector, enhancing consistency, investor trust, and legal defensibility across the EU.
- **Clarify regulatory scope and liability allocation:** Propose a clarified interpretation to ESMA and NCAs regarding the role and liability of "other persons" drafting whitepapers under Article 6. Specifically, advocate that when such persons act in good faith, with transparent disclosure and without deceptive intent, their liability under Article 15 should be proportionate and clearly bounded. Encourage regulators to incorporate this interpretation into official guidance to reduce uncertainty and promote responsible third-party whitepaper drafting.

3. Prevention and Detection of Insider Dealing: Extent and Practicalities

The third topic of the Milan roundtable, introduced by Delphine Forma, Head of Policy at Solidus Labs, focused on the significant compliance challenges presented by Title VI of MiCAR, which establishes rules to prevent and detect market abuse, including insider dealing. The discussion explored how these obligations apply to Persons Professionally Arranging or Executing Transactions (PPAETs) and what constitutes sufficient controls in an ecosystem that diverges substantially from traditional finance.

Participants examined the broader scope of MiCAR Title VI, which applies to all PPAETs and is enforceable from December 30, 2024, without a grandfathering period. Unlike traditional finance, crypto trading operates 24/7 across centralized and decentralized venues, on and off chain with significant market fragmentation, millions of assets with divergent underlying characteristics, same assets trade at different prices across hundreds of centralized and permissionless venues, and specific manipulation typologies such

as cross-chains, cross venues and cross-products typologies as well as the preponderance of pump & dumps, venue-specific price deviations, and sentiment-driven schemes and on-chain vulnerabilities due to malicious smart contract code, oracle exploits, across asset life cycle ,. Furthermore, vast transaction data is public, transparent and located on-chain. However, most trading is still off-chain, in centralized entities with trading data being private, not transparent from on-chain perspective.

The group highlighted that traditional finance methodologies may not translate effectively. In traditional markets, employee communication is monitored, trading is largely centralized, and instruments are typically traded on few venues. In contrast, the crypto sector is decentralized, data-rich yet fragmented, and anonymity or pseudo-anonymity is often the norm. This creates both challenges and opportunities in detecting and deterring insider dealing.

Participants noted that neither MiCAR, nor the corresponding ESMA RTS, currently offer clear guidance on how to meet obligations around insider dealing prevention and detection. Key issues include:

- Lack of clarity on the definition of a PPAETs under MiCAR.
- Possible challenges of comprehensive employee surveillance due to privacy laws in certain jurisdictions.
- Challenges in mapping employee wallets and detecting off-chain trading, particularly on centralized venues.
- Detection of trading activity of connected persons

There was robust discussion on what a reasonable compliance framework could look like. While some advocated for NDAs, training programs, and policies as baseline safeguards, others proposed more robust approaches, including:

1. Personal account dealing policies requiring wallet address declarations.
2. Trade surveillance systems monitoring both on and offchain behavior and integrating on and off chain data (news sources, chatbot, social media, troll box, kyc information, etc…).
3. Transactions disclosure obligations for employees with access to inside information.
4. Insider lists and structured internal controls such as pre-clearance and use of Chinese walls.
5. Voluntary monthly trade reports from other venues.

The discussion made clear that the industry lacks consensus on the appropriate extent of employee monitoring and systemic surveillance, and current legislation does not offer adequate clarity. Participants emphasized that more structured dialogue is needed, particularly with NCAs and ESMA, to align on expectations and develop best practices.

Call to Actions regarding insider dealing detection under MiCAR

The key call to actions from the discussion are:

- **Clarify the personal scope of PPAETs:** Propose that ESMA and the European Commission define the personal scope of PPAETs under MiCAR Title VI to ensure consistent application across jurisdictions and reduce uncertainty for compliance teams.
- **Develop best practices for employees having access to inside information surveillance in crypto markets:** Encourage the creation of an industry-led working group to define realistic, legally compliant best practices for preventing insider dealing by employees having access to inside information and connected persons, including wallet declarations, insider lists, and internal monitoring tools.
- **Promote a risk-based surveillance framework:** Advocate for a hybrid surveillance approach that balances regulatory requirements with technological capabilities and privacy considerations, integrating on-chain analytics with off-chain intelligence (e.g., social media, internal communications, venue data).

We thank all participants of the Milan DARTE event for contributing to the discussion:

Aaron Evencio Sánchez (MiCA Crypto Alliance), Alessio Capriati (Hercle), Ana Carolina Oliveira (Venga), Andrea Berruto (Karuna Ethical Blockchain Advisory), Andrea Pantaleo (DLA Piper), Anne-Lorinne Mognetti (MME), Delphine Forma (Solidus Labs), Donna Redel (Fordham University), Filip Berg-Nielsen (Volven), Filippo Annunziata (Università Bocconi), Francesca Condò (Università Bocconi), Francesco Paolo Patti (Università Bocconi), Giacomo Weiss (Polimi), Gianfranco Gauzolino, Gianluca Santavicca (Banca Sella), Giuseppe M. Blasi (Confidential Bank), Juan Ignacio Ibañez (MiCA Crypto Alliance), Maria Broulia (JCW), Mariana de la Roche (BlackVogel), Mariolina Colomba (Treezor), Nena Dokuzov (Ministry of Economics), Nina-Luisa Siedler (siedler legal), Olta Andoni (Enclave Markets), Paolo Gangi (Studio legale Gangi), and Yuliya Prokopyshyn (Coinbase).

DARTE SERIES

Berlin 3.0

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other emerging regulatory frameworks and region-specific issues relevant to the crypto-asset ecosystem.

The Berlin 3.0 DARTE edition was held on June 13th, 2025, at HTW Berlin, in collaboration with the European Commission, Project Catalyst, and HTW Berlin. It took place alongside the 10th Blockchain@HTW Conference.

The session featured in-depth discussions on three critical themes: the criminalization risks of smart contract development (Judith de Boer, Hertoghs Advocaten), legal pathways for recognizing DAOs as compliant Web3 communities (Joachim Schwerin, European Commission), and the regulatory tension between GDPR and decentralized blockchain infrastructures (Gustav Hemmelmayr, Parity Technologies). We extend our sincere thanks to all speakers and participants for their contributions, and to HTW Berlin for hosting the event.

This report synthesizes the core insights and recommendations from the discussions. It is important to note that the views expressed herein reflect the collective outcomes of the roundtable and not the formal positions of individual participants or their respective organizations.

1. Coding as a Criminal Act?

The first topic of the Berlin 3.0 roundtable, introduced by Judith de Boer of Hertoghs Advocaten, explored the legal implications of developing and deploying autonomous smart contract systems, particularly in light of recent prosecutions such as the Tornado Cash case. The discussion centered on the boundaries of criminal liability for developers whose decentralized tools can be used for both lawful and unlawful purposes.

Participants emphasized that smart contracts, while merely code, can facilitate the transfer of billions in value autonomously. This presents a legal dilemma: at what point does writing immutable and unstoppable code constitute a criminal act? In the Tornado Cash case, a Dutch court concluded that the developers of the protocol, by intentionally designing and deploying an anonymizing privacy enhancing tool without KYC/KYT mechanisms, bore responsibility for the laundering of over 500,000 ETH from criminal origins.

The court argued that the developers' continued involvement in maintaining and promoting the protocol, combined with knowledge of criminal use, amounted to conditional intent ("voorwaardelijk opzet") under Dutch law. The immutability of the smart contracts was deemed a deliberate design choice, not a shield from liability. This finding has sparked concern among developers and legal professionals, who fear that similar interpretations could criminalize neutral or even beneficial tools depending on their use.

Participants discussed whether a tool could be inherently criminal if it is especially suitable for unlawful acts, even when it serves legitimate privacy functions and is not criminalised by law. They also debated the legal consequences of not embedding compliance measures into interfaces and questioned how legal certainty can be preserved in a world of open-source, decentralized innovation.

Challenges Identified

- Traditional concepts of "operator control" do not map well onto decentralized technologies, where governance is distributed and no single entity may have the ability, or legal authority, to halt or modify operations. This disconnect creates legal uncertainty when trying to assign responsibility using frameworks designed for centralized actors.

- Criminal liability frameworks struggle to accommodate code as an autonomous actor, particularly when smart contracts are deployed on immutable infrastructure. This raises foundational questions: Can accountability rest solely with the original developer, or must it consider governance mechanisms, ongoing involvement, and community control?

- Developers face significant legal exposure even in the absence of malintent, particularly when protocols are designed without embedded compliance features even though compliance is not required by law. The absence of

such features, while often a deliberate choice to preserve neutrality or privacy, seem to be interpreted as willful negligence in jurisdictions applying conditional intent standards.

- The lack of ex-ante regulatory guidance exposes open-source contributors to disproportionate post-hoc enforcement risk. In practice, developers operate in a regulatory vacuum where norms are defined retroactively through prosecution, not policy, undermining both legal certainty and innovation incentives.

Moreover, liability may be unevenly enforced across jurisdictions, depending on prosecutorial discretion, the interpretation of intent, and the national stance on privacy tools. This uneven playing field creates fragmentation and forum-shopping risks for developers and platforms alike.

Finally, participants noted a growing ambiguity between tool-building and service-provision. The more a developer maintains a project's interface, markets the tool, or manages relayer infrastructure, the more likely courts are to see them as operators rather than neutral technologists, a distinction that remains blurry and underdefined.

Participants agreed that legal clarity must catch up with technological realities. Developers should not be criminalized for contributing to decentralized ecosystems unless they knowingly enable and directly facilitate criminal activity. Decentralised tools should not be treated differently than other tools that can have multiple uses.

Regulators and courts should distinguish between bad actors and genuine innovators. A technology-neutral, principles-based framework is needed to preserve the benefits of decentralization while addressing legitimate law enforcement concerns. The Tornado Cash precedent underscores the urgency of clear legal boundaries.

Call to actions regarding criminal liability in decentralized development

The key call to actions from the discussion are:

- **Publish clear ex-ante guidance on developer liability:** Urge national and EU authorities to define the limits of criminal responsibility for developers of open-source smart contracts, focusing on intent and the presence of compliance safeguards. A call to action in this regard is the Digital Freedom Declaration (https://digitalfreedom.page).
- **Draw technology-neutral legal standards:** Establish criteria that reflect the unique structures of decentralized systems, ensuring that liability is linked to specific actions and responsibilities, not merely the creation of code.
- **Protect the principle of legal certainty:** Advocate for jurisprudence and enforcement actions that respect lex certa, ensuring that developers are not punished for conduct that was lawful and widely accepted at the time of creation.
- **Recognize dual-use technology:** Promote balanced regulatory approaches that acknowledge both the legitimate and illicit use cases of privacy-enhancing tools like mixers, avoiding overreach that could chill innovation.

2. DAOs as Compliant Web3 Communities

The second topic of the Berlin 3.0 roundtable, introduced by Joachim Schwerin, Principal Economist at the European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW), focused on the legal ambiguity surrounding the status and structure of Decentralized Autonomous Organizations (DAOs) in Europe.

The discussion examined the limitations of current legal wrappers, the absence of a DAO-specific regulatory framework, and emerging solutions that combine collective identity, on-chain governance, and external representation.

Key Regulatory and Structural Challenges

Participants highlighted the growing presence of DAOs across sectors, from DeFi to the social economy, and emphasized their functional similarities to offline cooperatives. Yet, unlike cooperatives, DAOs lack clear legal recognition. This forces projects to rely on suboptimal legal forms or remain outside the formal economy altogether.

Common issues raised included:

1. **Jurisdictional uncertainty:** DAOs operate globally but lack a clear framework for which national rules apply. Formal registration in one country often does not provide cross-border recognition.
2. **Undefined liability:** With no identifiable management or fixed membership, it's unclear who bears legal responsibility. Some participants suggested "collective liability" mechanisms supported by digital governance logs.
3. **Representation gap:** Without physical legal persons to interface with states, DAOs face difficulties in managing taxes, social contributions, or contractual obligations.
4. **Lack of minimum standards**: DAOs vary widely in size and complexity, from chatrooms to proto-states, requiring flexible, horizontal requirements that adapt to their function.

Drawing from sandbox use cases, the BlackVogel & Blockstand DAO studies and 2024 GROW study, the group outlined several building blocks for compliant DAO structures:

- **Digital Collective Identity**: Establish a unique and verifiable identifier for the DAO, combining on-chain membership records with off-chain verification methods such as EBSI-based attestations. This preserves pseudonymity while enabling accountability.
- **On-chain Governance Disclosure:** DAOs should document essential governance parameters, such as voting mechanisms, token distribution models, decision-making structures, and upgrade procedures, in a standardized format. This could resemble MiCAR-style white paper disclosures, ensuring external parties and members can assess the DAO's operational and risk profile.
- **Selective Disclosure with ZKPs:** To balance transparency with privacy, participants explored how zero-knowledge proofs and similar cryptographic tools could enable selective disclosure. These mechanisms would allow DAOs to prove regulatory compliance (e.g., identity requirements, financial controls) without revealing sensitive or personally identifiable information.
- **Orphan Fund Representation:** Use "Sachwalter" structures, where independent entities administer DAO assets without being part of the DAO. These can handle legal duties (e.g. taxes, compensations) on behalf of the DAO without altering its decentralised nature.
- **Flexible Legal Wrappers:** Explore adaptation of existing cooperative statutes (e.g., EU SCEs), foundations, or develop an optional regime. Each option must account for liability, ultimate beneficial owner identification, and AML compliance.

Integration with International Policy Trends

The roundtable echoed findings from broader industry research comparing DAO regulatory frameworks across jurisdictions. While DAO-specific legal forms are beginning to emerge, such as the Wyoming DAO LLC and Marshall Islands structures, these remain fragmented and inconsistent. Participants agreed that uniform standards on AML/KYC, taxation, and legal representation are essential to avoid jurisdiction shopping and to foster the legitimacy of DAOs within existing regulatory systems. It was also noted that regulatory sandboxes and modular legal templates could play a valuable role in supporting DAOs during their early growth stages, offering a pathway to compliance while minimizing legal risk. In this regard, the three DAO use cases in the upcoming third cohort of the European Blockchain Regulatory Sandbox will deepen these reflections.

Participants emphasized that DAOs will persist and scale regardless of recognition, but lack of legal clarity increases risk and stifles legitimate activity. Any European framework must be flexible enough to support experimentation while offering robust protections for DAO participants and third parties.

Call to actions regarding legal frameworks for DAOs

The key call to actions from the discussion are:

- **Establish standardized DAO governance principles and classification models**: Develop a unified taxonomy for DAOs based on their purpose (e.g., Non-Profit, Investment-focused, Community-driven) and governance structure (e.g., member-managed, algorithm-managed). This should be accompanied by core governance standards, such as transparency rules, trustee duties, and baseline documentation requirements, to guide compliant DAO operations across jurisdictions and support legal recognition.
- **Launch an EU-wide cross-jurisdictional DAO sandbox**: Create a regulatory sandbox specifically designed for DAOs, enabling experimentation with novel governance models, on-chain identity, and decentralized financial operations in a supervised, legally coherent environment. This would allow regulators and DAOs to test flexible compliance pathways while gathering the insights needed for broader legal integration.
- **Translate sandbox findings into a future-proof, tech-neutral legal framework**: Use learnings from the DAO sandbox to inform the development of a "28th regime" or optional DAO legal wrapper at EU level. This framework should be

technology-agnostic—relying on broad legal concepts like "Trustworthy Technology"and designed to accommodate rapid innovation while providing legal certainty and enforceable protections for participants and third parties.

3. Personal Data and Blockchain

The third topic of the Berlin 3.0 roundtable, introduced by Gustav Hemmelmayr, Senior Legal Counsel at Parity Technologies, focused on the regulatory tension between GDPR and public, permissionless blockchain infrastructures. The discussion centered on the European Data Protection Board's Guidelines 02/2025 and their implications for decentralized technologies.

Participants noted that although GDPR is a technology-neutral regulation in theory, in practice it remains deeply rooted in centralized data-processing assumptions. Public permissionless blockchains, which do not rely on data collection or identifiable intermediaries, challenge these assumptions. The recent EDPB guidelines fail to account for how decentralized systems actually function and place undue burden on infrastructure-level data like addresses and hashes.

A recurring theme was the distinction between infrastructure data and personal data. While a blockchain address may be seen as personal data when collected and linked to an individual off-chain (e.g., by exchanges or custodians for their KYC processes), that same address used anonymously on-chain should not be treated as personal data. Participants stressed that current interpretations blur this distinction, threatening to classify infrastructure data as inherently personal, undermining the possibility of privacy-by-design implementations.

Three main argumentation lines shaped the roundtable:

1. **Intermediaries and Privacy Risk**: Blockchain transactions generally do not require or reveal personal information unless intermediaries (e.g., custodial wallets, exchanges) collect and link data for regulatory compliance. These off-chain actors, rather than the blockchain infrastructure itself, should be the focus of GDPR compliance and liability.

2. **Infrastructure as Neutral Layer:** Public permissionless blockchains function like public utilities (e.g., a calendar or addresses on a map). Just as a calendar date is infrastructure to measure time independently from individual's links to a certain date (like their birthday), a blockchain address is anonymous infrastructure data on that blockchain even if someone offchain collects certain addresses as part of their data collection around a person. Destroying the infrastructure or restricting its usage due to potential personal data linkage is disproportionate

and ignores the neutral, anonymous and privacy-preserving nature of these decentralized systems.

3. **Expansive Interpretations of Personal Data:** Authorities' tendency to classify nearly all data as personal, even inherently anonymous data like cryptographic hashes, was criticized as impractical and counterproductive. Participants argued that a policy framework rooted in absolute identifiability undermines both technological neutrality and innovation, particularly in contexts where blockchain enhances, rather than threatens, user privacy.

Participants emphasized the urgent need for a recalibration of regulatory interpretations to enable privacy innovation without undermining fundamental rights or system integrity.

Call to actions regarding GDPR and decentralized technologies.

The key call to actions from the discussion are:

- **Reframe the legal interpretation of infrastructure data**: Advocate for a narrow interpretation of GDPR that excludes anonymous, infrastructure-level data from the definition of personal data. Public blockchain addresses or hashes used in privacy-preserving systems should not be treated as inherently personal.
- **Center regulatory responsibility on intermediaries**: Emphasize that GDPR rights and duties should apply primarily to data-collecting intermediaries who establish off-chain links to individuals. Blockchain infrastructure itself should not be held liable for personal data processing it does not perform.
- **Restore and reinforce technological neutrality in privacy regulation**: Encourage regulators to revisit GDPR principles through a teleological lens, recognizing privacy-by-design solutions embedded in blockchain technologies as aligned with the aims of the regulation. Challenge overly broad interpretations that hinder innovation and increase systemic risk.

We thank all participants of the Berlin 3.0 DARTE event for contributing to the discussion:

Arslan Brömme, Ameen Soleimani, Andrew Forson (DeFi Technologies), Bota Jardemalie, Daniela Boback (Bundesblock), Florian Daniel (Westernacher), Frederic Hannesen (M0), Dr.

Friedrich Popp (Popp Law), Gustav Hemmelmayr (Parity Technologies), Jacob Senftinger (SafeWallet), Janine Roemer, Joachim Schwerin (European Commission), Dr. Jörn Erbguth, Judith de Boer (Herthogs advocaten), Mariana de la Roche Wills (BlackVogel), Markus Kluge (tokenforge), Matthias Bauer-Langgartner (Chainalysis), Nuno Lima da Luz (Associação Portuguesa de Blockchain e Criptomoedas), Nurtilek Taalaibekov (CertiK), and Silvan Jongerius (TechGDPR).

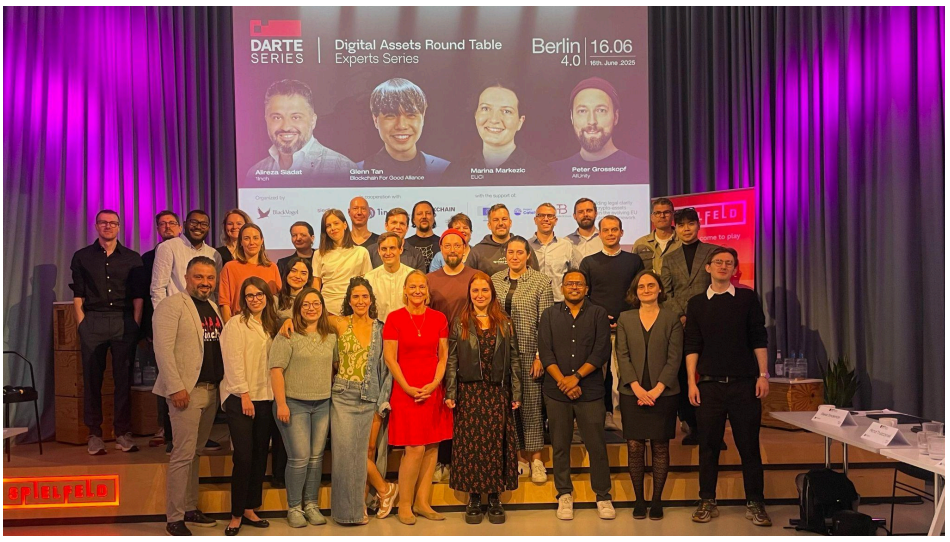
DARTE SERIES

Berlin 4.0

The Berlin 4.0 DARTE edition was held on June 16th, 2025, at Spielfeld Digital Hub, in collaboration with the European Commission, Project Catalyst, 1inch, Blockchain for Good Alliance, and Spielfeld. Taking place in parallel with Berlin Blockchain Week, this session brought together regulators, technical experts, compliance professionals, and legal scholars to explore MiCAR's practical implications for decentralized technologies and services.

The roundtable focused on three core topics around Descentralize Finance-DeFi: the regulatory distinction between technology providers and crypto-asset services (Peter Großkopf, AllUnity), the challenges of implementing DeFi-native security and compliance frameworks (Alireza Siadat, 1inch), and the uncertain treatment of DeFi interfaces under current EU supervisory practices (Marina Markezic, EUCI). The session also concluded with a keynote of Glenn Tan (GBA) about the impact of DeFi on the real economy. We extend our sincere gratitude to all speakers and participants for their insights, and to Spielfeld for hosting the event and to 1inch and the Blockchain For Good Alliance for their support.

This report consolidates the main insights and recommendations that emerged during the discussion. The views presented reflect the collective outcomes of the roundtable and do not represent official positions of any individual participant or organization.



1. **Tech Providers versus Crypto-Asset Services**

The first topic of the Berlin 4.0 roundtable presented by Peter Grosskopf, CTO/COO at AllUnity, previously co-founder at Unstoppable Finance who were building a self-hosted wallet in Germany, addressed the legal uncertainty surrounding the distinction between technical infrastructure providers (like self-hosted wallet companies) and regulated crypto-asset services under MiCAR. As DeFi frontends and wallets increasingly integrate complex functionality, such as DEX aggregation or transaction routing, regulators are scrutinizing the boundaries between neutral tooling and regulated intermediation.

Participants examined the evolving stance of BaFin, the German financial regulator, which considers certain interfaces as falling under the category of "Anlagevermittlung" (investment brokerage) when they simplify user interactions with blockchain-based financial instruments. BaFin's internal test evaluates whether a service engages in trading, facilitates access to financial instruments, or operates an intermediary layer between counterparties. Even without custody or fees, technical providers could be caught under MiCAR if they streamline DeFi usage to a degree deemed equivalent to financial intermediation.

This interpretation raised alarm among participants, who feared it could extend MiCAR obligations to self-hosted wallets and non-custodial applications. While some Member States adopt a tech-neutral approach (e.g., Liechtenstein), others may follow BaFin's expansive view, creating a patchwork of legal interpretations across the EU. The lack of harmonized criteria on what constitutes a "service" versus a "tool" could impose significant compliance burdens on developers and startups offering infrastructure software.

The discussion revealed that fee models are often decisive in regulatory classification, charging a transaction-based fee could tip an otherwise neutral tool into regulated territory. However, ambiguity remains: is a transaction summary a "simplification"? Does a wallet using WalletConnect to route trades still qualify as a neutral tool?

Participants agreed that greater technical understanding within supervisory bodies is urgently needed. A signed transaction submitted via a wallet cannot be altered by the interface provider. In such cases, applying traditional intermediary concepts may misrepresent the actual control, or lack thereof, held by the service.

Participants flagged several pressing legal ambiguities:

- The current lack of harmonized definitions under MiCAR leaves room for divergent national interpretations of what constitutes a crypto-asset service, versus a technology provider.
- Regulatory tests that focus on UX simplicity or interface design may result in overreach, capturing infrastructure tools that have no custodial control or financial discretion.

- Fee triggers are inconsistently applied across jurisdictions. In some Member States, charging a fee immediately classifies a tool as a regulated service; in others, intent and functionality weigh more heavily.
- The industry lacks clear guidance on whether and when decentralized frontends, or developer-maintained interfaces, might be exempt from licensing requirements.
- Developers seeking regulatory certainty often receive circular responses ("check with your local authority"), making it difficult to plan compliance pathways.
- Interface providers remain unclear on how to balance regulatory expectations with core DeFi values such as user sovereignty, non-custodial design, and immutability.

Participants emphasized that regulators must distinguish between core protocol developers, UI providers, and custodial intermediaries. Until then, the risk of overregulation may push innovation offshore or underground. A principled and tech-savvy interpretation of decentralization, rather than rigid checklists, is needed to align MiCAR enforcement with its stated goals of innovation and consumer protection.

Yet, the discussion was not solely focused on risks. Participants offered several pathways forward:

- Fee structures as a regulatory trigger were debated. Some participants, including legal practitioners and DeFi founders, argued that transaction-based fees remain the clearest line regulators could draw. However, others cautioned that absence of fees should not automatically imply exemption if the tool facilitates regulated activity in other ways.

- Frontend decentralization was discussed as a mitigation strategy, if no single entity operates the interface, liability becomes diffuse. Still, participants noted that full decentralization is difficult to achieve in practice, and legal ambiguity remains around code authorship, governance, and ongoing maintenance.

- Several attendees proposed a phased licensing model or regulatory sandbox for interface developers to engage with regulators early and test models without the full burden of authorization. This was seen as a way to provide legal certainty without sacrificing agility.

- Drawing from Swiss and Liechtenstein models, participants also suggested that functionality and control, not design or user experience, should be the basis for regulatory classification. A frontend that only signs and routes transactions, without custody or execution control, should not be equated with a financial intermediary.

- The notion of a "postal service" analogy was revisited: If a wallet

merely passes a sealed and signed transaction to a public blockchain, can it be considered an active service provider? Participants generally agreed that intent, discretion, and technical capacity must be clearly distinguished in legal terms.

While consensus was not reached on a single compliance strategy, the session revealed strong alignment around one point: MiCAR's future Level 2/3 guidance must account for the layered architecture of Web3. Interfaces are neither neutral nor custodial by default; context matters. If regulation is to be fair and future-proof, it must reflect the technical realities of how DeFi works—and how users interact with it.

Call to actions regarding regulatory clarity for DeFi interfaces

The key call to actions from the discussion are:

- **Clarify the scope of MiCAR for non-custodial interfaces:** Urge ESMA and NCAs to define under what conditions wallets, frontends, and integration layers qualify as regulated services, taking into account control, discretion, and fee structures.
- **Support function-based regulatory tests:** Promote legal interpretations that focus on technical functionality and access to user funds rather than on interface design or UX, to better reflect how DeFi tools operate in practice.
- **Establish EU-wide sandbox mechanisms for interface providers:** Encourage the development of experimental regulatory frameworks that allow DeFi interface developers to work with supervisors without immediate licensing requirements, fostering dialogue and iterative compliance pathways.

2. **DeFi Security and Risk Management**

The second topic of the Berlin 4.0 roundtable, presented by Alireza Siadat (1inch), addressed the growing urgency of developing effective risk management strategies in DeFi without compromising decentralization. As DeFi ecosystems scale, their openness and permissionless nature expose them to recurring threats such as smart contract exploits, wallet takeovers, and interactions with sanctioned entities.

Participants emphasized that while DeFi provides user autonomy and global access, it also challenges conventional AML frameworks due to its lack of intermediaries and transaction finality. The discussion centered on how infrastructure providers are responding

by building native risk mitigation tools, from real-time pool scanning APIs and malicious token detection to wallet screening and device fingerprinting.

A compelling example discussed was how a DeFi platform proactively identified and blocked a wallet associated with illicit activity using on-chain tools. These measures helped prevent further misuse and were reinforced through coordination with other DeFi peers. The case illustrates how collaboration with various partners, including law enforcement agencies, can play a crucial role in addressing financial crime. The U.S. government later acknowledged these efforts, commending the platform for its contribution to preventing illicit activity.The group broadly agreed that these proactive technical safeguards are more aligned with the ethos of DeFi than simply transplanting TradFi compliance models. Notably, participants endorsed collaboration between DeFi protocols, law enforcement, and regulators to enable timely responses to threats.

However, timing and regulatory clarity remain key concerns. Applying for licenses too early could stifle innovation, while waiting for MiCAR Level 2 and 3 standards might allow the industry to align compliance efforts with more appropriate frameworks. The discussion reinforced that self-regulation and cross-project cooperation can meaningfully reduce systemic risk, if paired with a supportive and technically informed regulatory approach.

Call to Actions regarding DeFi risk management

The key call to actions from the discussion are:

- Promote integration of on-chain and off-chain intelligence tools to detect suspicious activity and improve user protection.
- Support development of open, non-custodial risk mitigation infrastructure, such as wallet screening, token flagging, and security UX alerts, within DeFi protocols.
- Encourage structured collaboration between DeFi providers and regulators to define risk-based compliance frameworks that reflect the unique structure of decentralized finance.

3. **DeFi Interfaces**

The final topic of the Berlin 4.0 roundtable presented by Marina Markezic, Co-Founder of EUCI, examined the increasingly scrutinized role of user interfaces in DeFi. While smart contracts govern the back end of DeFi, it is often the front-end interfaces, websites, apps, and other gateways that link users to protocols. Participants discussed how regulators, such as the Danish FSA, are beginning to treat these interfaces as potential points of control, with implications for whether a project is truly "decentralized" or subject to regulatory obligations.

Drawing on policy examples from ACPR, IOSCO, and the European Parliament, the group acknowledged that interfaces may be the Achilles' heel of decentralization. When a DeFi protocol's access point is managed by a single legal entity, it risks being treated as a regulated service provider. Even in cases where the backend is autonomous, control over the user-facing layer may draw liability and obligations under MiCAR or national laws.

Participants explored current tools for minimizing front-end centralization, including decentralized hosting protocols such as IPFS and Swarm, and emerging solutions which enable users to run DApps locally with private shared consensus. These approaches aim to preserve censorship resistance, availability, and shared responsibility, especially critical in scenarios like Tornado Cash, where losing a DNS entry meant immediate loss of access for most users, despite the protocol remaining operational.

The conversation highlighted that decentralizing the interface layer is not just a technical challenge, it's a governance issue, too.

Without a shift toward multi-node or user-hosted solutions, DeFi risks remaining vulnerable to both regulatory enforcement and infrastructure failure. Still, the group recognized the importance of practical regulation: participants called for clarity on where regulatory responsibility begins and ends in multi-layered DeFi architectures, and emphasized the need for proportional frameworks that do not punish innovation.

Call to Actions regarding DeFi interfaces and decentralization

The key call to actions from the discussion are:

- **Recognize front-end decentralization as essential to protocol neutrality:** Regulators should assess decentralization across the full technology stack, including interfaces, rather than backend architecture alone.
- **Encourage adoption of decentralized hosting technologies:** Projects should integrate resilient, censorship-resistant access methods like IPFS, Swarm, and local execution layers to reduce central points of failure.
- **Define the regulatory boundary for interface provision:** Clarify when front-end operation by a legal entity constitutes a regulated activity under MiCAR, and provide safe harbor guidelines for fully decentralized or self-hosted front-ends.

We thank all participants of the Berlin 4.0 DARTE event for contributing to the discussion:

Adriana Rodriguez (N26), Alessandra Carolina Rossi Martins (Gnosis), Alireza Siadat (1inch), Anne Grace Kleczewski (MME), Colin Nimsz (Brighter AI), Esen Esener (Lido), Frederic Hannesen (M0), Glenn Tan (BGA), Holger Koether (ETO Group), Jacob Senftinger (Safe), Jannik Piepenburg (Deloitte), Joanna Rindell (Tezoz), Jon Gunnar (Monerium), Krill Pimenov, Mariana de la Roche (BlackVogel), Marina Markezic (EUCI), Mathias Nörenberg (N26), Michal Truszczynski (Bitpanda), Monika Hammer Muller (Gnosis), Moritz Stumpf (Token Forge), Nina-Luisa Siedler (siedler legal), Olena Zabrodska (1inch), Peter Großkopf (AllUnity), Rieke Smakman (Bitvavo), Sandeep Bajjuri (PositiveBlockchain), Tamari Asatiani (Raisin), Teresa Carballo (Pacifica Legal), Tim Adrelan (Osborn Clarke), and Toluth Opeyemi Apalowo (GFTN Europe).

DARTE SERIES

Vienna 2.0

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the MiCAR. Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks and region-specific issues.

The Vienna 2.0 DARTE edition was hosted at Central European University on September 10th, 2025, bringing together regulators, policymakers, and industry experts to engage in high-level discussions on critical legal and compliance challenges under MiCAR. The session focused on three core topics: the disclosure of inside information and the role of social media (Philipp Bohrn, Bitpanda), the classification challenges of decentralized assets (Georg Harer, Bybit), and the overlap between MiCAR and MAR using crypto derivatives as a case study (Giti Said, Arweave).

We extend our sincere gratitude to the European Commission, Project Catalyst, Bitpanda, Bybit, DLT Austria, and Central European University for their invaluable support in making this roundtable possible.

This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.

1. Disclosure of Inside Information & Challenges of Social Media

The first topic of the Vienna 2.0 roundtable, introduced by Philipp Bohrn (Bitpanda), focused on the challenges of complying with Article 88 MiCAR, which requires issuers of crypto-assets to publicly disclose inside information "without delay." Unlike traditional financial markets, where disclosure is centralized, timestamped, and structured through regulated outlets such as Bloomberg or Reuters, the crypto-asset ecosystem relies heavily on unstructured, decentralized platforms like X (Twitter), Telegram, and Discord. This poses significant challenges for regulatory enforcement, market surveillance, and investor clarity.

Participants emphasized the fundamental differences between traditional finance and the crypto industry. In traditional markets, disclosure is routed through trusted, centralized platforms with metadata and tagging that facilitate surveillance and public access. In contrast, crypto disclosures often lack standardization, are intermingled with speculation and marketing, and are difficult for both regulators and surveillance tools to detect or verify.

A key concern discussed was the inability of existing systems to scrape and identify material disclosures across the web in a reliable way. Social media posts rarely contain any form of Article 88-specific tagging, making it nearly impossible to automatically flag or cross-reference announcements with market activity. NCAs, even with enhanced tools, struggle to distinguish between material disclosures and general commentary. This regulatory blind spot not only undermines market integrity but also creates legal uncertainty for issuers.

Participants also highlighted the fragmented and global nature of crypto markets. MiCAR applies within the EU, but many crypto projects operate internationally. A disclosure posted on Discord or X by a U.S.-based issuer may not meet EU standards of "public availability," raising compliance questions. The group discussed the lack of guidance on whether such disclosures satisfy Article 88 requirements, particularly if they are inaccessible to large portions of the market.

In addition, a noteworthy point raised during the discussion was that if a market participant or issuer becomes aware that material inside information has been shared through unofficial channels, such as Telegram or social media, there is a responsibility to publish that same information through official disclosure routes without delay. This not only ensures broader market access but can also serve as evidence of timely compliance if regulatory questions arise later.

To address these issues, participants proposed a series of practical and forward-looking solutions. These included the development of centralized or hybrid disclosure platforms led by ESMA, potentially leveraging blockchain infrastructure to ensure transparency, immutability, and global accessibility. Other suggestions involved industry associations maintaining open-access repositories, standardized tagging

systems for social media disclosures, and AI-supported verification tools.

There was also strong support for combining social media with traditional disclosure routes, recognizing that social media can provide immediacy, while regulated channels ensure structure and credibility. Any proposed solution must remain open-access and low-cost to ensure that smaller issuers are not excluded, in line with MiCAR's principles of proportionality and inclusivity.

Ultimately, participants agreed that solving the disclosure dilemma requires both regulatory leadership and industry cooperation. ESMA and NCAs must clarify expectations and enforce harmonized disclosure standards, while the crypto industry must invest in tools, education, and voluntary compliance mechanisms.

Call to actions regarding insider information disclosure under MiCAR

The key call to actions from the discussion are:

- **Develop EU-wide disclosure standards:** To ensure consistency and legal clarity across Member States, industry actors should collaborate on defining a set of EU-wide disclosure standards. These could be used as a baseline reference, enabling scalable compliance solutions and promoting cross-border harmonization.
    - **Standardize tagging, classification, and timing of disclosures across channels:** The industry should align on a tagging framework (e.g., an "Article 88" tag) applicable across platforms including social media, and propose this standard to ESMA for endorsement. Additionally, strict disclosure timelines and tagging requirements should be adopted to reduce ambiguity, especially since the current mandate to disclose "as soon as possible" creates uncertainty and uneven compliance. Clear, uniform timing rules will help mitigate the risks of both over-reporting and under-reporting.
- **Develop a centralized or hybrid disclosure platform:** Industry stakeholders should collaborate to create a unified disclosure infrastructure that combines the reliability of traditional outlets with the accessibility of digital channels. This platform should ensure transparency, timestamping, and accessibility for both EU

and international market participants, with special attention to open-access and proportionality.

2. Classification Challenges of Decentralized Assets under MICAR

The second topic presented by Georg Harer (Bybit) addressed the persistent difficulty of classifying decentralized assets under the current EU regulatory framework, especially MiCAR. The discussion used Liquid Staking Tokens (LSTs) as a focal case study, with participants including CASPs, lawyers, and industry representatives voicing concern over the fragmented interpretations emerging across Member States.

Under MiCAR, crypto-assets are generally categorized as either utility tokens, Asset-Referenced Tokens (ARTs), or e-money tokens. However, innovative Web3 products like LSTs often do not fit neatly into any of these categories. LSTs are typically issued by autonomous smart contracts and allow users to participate in network staking while retaining liquidity, yet they do not offer price stability, a redemption mechanism, or a legal issuer, which disqualifies them from most existing classifications.

Participants explored several problematic overlaps:

- ARTs assume a centralized issuer who is liable for drafting and publishing a whitepaper. With LSTs, there is no identifiable issuer, and Ethereum (or another PoS token) is not directly "referenced" in a claimable way.
- MiFID II (Markets in Financial Instruments Directive) and AIFMD (Alternative Investment Fund Managers Directive) apply to instruments that include centralized portfolio managers or structured investment strategies, conditions that are incompatible with autonomous, immutable protocols.
- Some NCAs argue that merely enabling a return could push such assets into Alternative Investment Fund (AIF) territory, even if the underlying mechanisms are community-governed and open-source.

This uncertainty puts CASPs in a vulnerable position. Should regulators retroactively classify a token as an ART, financial instrument, or AIF, CASPs could face legal liability under MiCAR's strict provisions, particularly if no issuer exists to share that burden.

A standout point of comparison came from Italy, where participants mentioned that the regulator reportedly reviews and approves whitepapers substantively, rather than merely acknowledging receipt. This proactive approach provides an added layer of legal clarity and assurance for CASPs operating there, unlike in other jurisdictions, where whitepaper acknowledgment is procedural rather than

substantive. Such divergence in practice increases regulatory fragmentation across the EU and fuels forum shopping.

The group also discussed practical examples like ETH staking product, which offers liquidity for staked tokens via smart contracts and allows users to trade without traditional custodial intermediaries. These tokens exhibit properties of participation, representation, and tradability, but do not fit existing MiCAR definitions.

Key Challenges Identified

- Issuer ambiguity: Decentralized protocols often lack a legal entity or team that can serve as issuer under MiCAR definitions.
- No clear redemption rights: LSTs and similar assets don't offer contractual return claims or centralized redemptions, unlike ARTs or financial products.
- Varying regulator positions: NCAs interpret the same asset differently; some may classify a product as an ART or derivative, while others remain silent.
- Unaddressed legacy tokens: Tokens launched over a decade ago (e.g., Bitcoin forks) without whitepapers or issuers still circulate. How should they be treated today?
- Liability risk for CASPs: When listing innovative assets, CASPs may be left holding legal exposure without clarity from regulators or guidance from ESMA.
- Delays and opacity: Some regulators take months to respond to classification inquiries. Without predictable answers, CASPs face operational risk.

The discussion revealed a growing consensus that whitepapers remain useful, even when not legally required, by helping demonstrate transparency, outline risks, and offer protection to users. Some CASPs already publish whitepapers voluntarily and obtain liability insurance. Others rely on intermediaries to act as "whitepaper publishers," absorbing some of the legal responsibility.

Participants also proposed that a checklist-based framework, potentially validated through academic research, could support early classification and reduce regulatory ambiguity.

Call to Actions regarding classification of decentralized assets

The key call to actions from the discussion are:

- **Develop a structured token classification tool:** A working group comprising academic researchers and industry stakeholders should collaboratively build a taxonomy for decentralized assets, starting with cases like Liquid Staking Tokens. An initial academic draft could serve as a baseline for structured industry feedback, leading to a consolidated tool to support consistent classification across jurisdictions. Once aligned, this taxonomy could be submitted through ESMA's Q&A process to promote harmonization.
- **Define enhanced whitepaper disclosure standards for decentralized assets:** Where no issuer exists, CASPs should be responsible for publishing a MiCAR-compliant whitepaper. These disclosures should focus on technical and economic risks rather than issuer identity.

3. **Overlap in Market Abuse Provisions MiCAR&MAR, taking Crypto Derivatives as an Example.**

The third topic presented by Giti Said (Arweave, _Placehodlr) focused on the complex interaction between the Market Abuse Regulation (MAR) and MiCAR, particularly in the context of crypto derivatives. The discussion centered on the legal and compliance challenges arising when a single market behavior potentially triggers obligations under both regulatory regimes.

MiCAR and MAR pursue similar goals, namely, the prevention of market abuse, but apply to distinct categories of assets. While MAR governs traditional financial instruments, including derivatives admitted to trading on regulated venues, MiCAR applies to crypto-assets that fall outside the scope of MiFID II. However, many crypto market actions, such as trading a spot crypto-asset while simultaneously trading its derivative, can fall into both regulatory buckets, resulting in a "double application" of market abuse rules.

Participants explored a hypothetical but realistic example: a trader gains access to insider information about an upcoming upgrade to a blockchain network and purchases both the native token (covered under MiCAR) and a related futures contract (covered under MAR). In this case, a single act of insider trading could fall under both frameworks, exposing the actor to parallel investigations and potentially double sanctions.

This scenario poses several legal and compliance dilemmas:

- In the case of crypto-assets, it is often unclear who qualifies as the "issuer" or "operator" responsible for disclosure, especially when protocols are decentralized.
- MAR and MiCAR define and treat insider information differently, even when it concerns the same asset. The moment such information leaks via social media, questions arise about whether disclosure is still necessary, or whether the information is already deemed public.
- Participants expressed concern that the same behavior could lead to punishment under both MAR and MiCAR, challenging the legal principle of ne bis in idem (the prohibition of being penalized twice for the same offense).
- While MiCAR introduces lighter requirements in recognition that many crypto actors are SMEs (as noted in Recital 95), MAR maintains full obligations for financial instruments. This duality creates confusion for entities operating across both domains.

The group stressed that the growing complexity of financial instruments built on top of crypto-assets (such as perpetuals and tokenized derivatives) makes it increasingly difficult for service providers to understand their obligations. Moreover, regulatory guidance from ESMA to date has acknowledged these products, however, it does not distinctly address the overlap matter. Participants argued that the current fragmented approach to enforcement increases the risk of inconsistent interpretations by NCAs, legal uncertainty for market participants, and ultimately undermines investor protection.

There was broad agreement that a more holistic approach is necessary, one that respects the regulatory distinctions between MAR and MiCAR while preventing duplicative or conflicting enforcement.

Call to Actions regarding overlapping market abuse rules

The key call to actions from the discussion are:

- **Define a coherent enforcement approach for overlapping conduct**: Regulatory frameworks should treat actions that simultaneously trigger obligations under MiCAR and MAR as a single market abuse offense, ensuring that enforcement does not lead to duplicative sanctions for the same conduct. This requires aligned procedures between regimes and coordination among NCAs.

- **Develop proportionate compliance frameworks and educational tools for SMEs and market participants:** To mitigate the legal uncertainty from overlapping MiCAR and MAR obligations, regulators and industry bodies should jointly develop practical compliance toolkits, training programs, and tailored guidance reflecting the unique risks of crypto derivatives markets. Special attention should be given to SMEs with limited compliance capacity to ensure fair and consistent enforcement across the sector.

We thank all participants of the Vienna 2.0 DARTE event for contributing to the discussion: Aaron Glauberman (Legal Bison), Alex Scharrer (NEAR), Alexander Mike Stachniewicz (Volt / Science Vienna), Alexandra Lloyd (Youhodler), Alexandru Stanescu (thinkBLOCKtank), Alireza Siadat (Deloitte), Anne Grace Kleczewski (MME), Damian Skrobich (Bybit), Delphine Forma (Solidus Labs), Elfriede Sixt, Florian Wandruszka (Kucoin), Florian Wimmer (Blockpit), Gayane Mkrtchyan (Modul University), Georg Harer (Bybit), Giti Said (Arweave, _Placehodlr), Jacek Zmiel (Crystal), Kristina Szarvas (Central European University), Mariana de la Roche W. (BlackVogel), Matthias Bauer (Chainalysis), Michal Truszczynski (Bitpanda), Mihai Huiala (Lexters), Monika Hammermueller (Gnosis), Nina Siedler (siedler legal), Philipp Bohrn (Bitpanda), Saputra Beny (Central European University), Sebastian Becker (Bundesblock), and Tonia Damvakeraki (HAREVA)

DARTE SERIES

Munich

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the MiCAR. Over time, the series has expanded to cover not only MiCAR but also other related regulatory frameworks and region-specific issues.

The Munich DARTE edition was hosted at V-Bank on September 11th, 2025, in collaboration with the European Commission, Project Catalyst, FinPlanet, Bybit, and the TUM Blockchain Conference. The session convened regulators, legal practitioners, market infrastructure providers, and financial institutions to examine the legal friction points between traditional financial instruments (MiFID II) and tokenized securities in light of MiCAR and the DLT Pilot Regime.

Discussions focused on three key topics: secondary market restrictions for hybrid shareholdings (Christopher Görtz, Heuking), unresolved potential within the DLT Pilot Regime (Carola Rathke, YPOG), and the legal imbalance in executing rights attached to security tokens (Roland Gollenbeck, Bybit).

We extend our sincere gratitude to all speakers and supporters for making this roundtable possible. This report consolidates insights from these discussions. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or the respective rapporteurs.

1. **Secondary Markets in case of hybrid shareholdings**

The first topic of the Munich DARTE roundtable, introduced by Christopher Görtz (Heuking), addressed the liquidity and operational challenges associated with hybrid shareholdings, specifically, securities that can exist both as traditionally certificated shares (held giro-collectively and exchange-traded) and as electronic securities (e-securities) under the German Electronic Securities Act (*eWpG*). While current legislation allows conversion between the two forms, the technical infrastructure and market mechanisms to support such transitions remain underdeveloped.

Participants noted that while hybrid shares are legally feasible, the lack of a liquid secondary market for electronic securities significantly reduces their practical utility. Since these assets may trade on different platforms (centralized exchanges for traditional shares vs. DLT-based systems for tokenized ones), liquidity becomes fragmented, and price discrepancies across markets raise concerns. Conversion between formats is cumbersome and operationally opaque, further discouraging adoption.

Several models were discussed to address this market inefficiency. One approach involved a trustee-based structure, where shares from both formats are pooled and managed collectively.

Another proposal centered on a market-maker model, where a designated intermediary quotes bid/ask prices for electronic shares, ensuring continuous trading. However, both models raise concerns about settlement risks, pricing divergence, and regulatory implications, particularly around short-selling and capital requirements.

A more pragmatic solution, favored by some of the participants, envisions a bank acting as an intermediary. Under this model, if an investor wishes to sell a tokenized (electronic) share, the bank simultaneously sells a traditional share on the exchange, credits the investor, and receives the electronic share in return. The bank may leverage borrowed traditional shares from major shareholders to avoid short positions during settlement. This "share-loan conversion bridge" could provide the necessary liquidity without creating excessive regulatory overhead.

Importantly, this is not primarily a regulatory issue, but rather a market infrastructure and design challenge. The group discussed whether share loans in this context could be exempted from licensing requirements to facilitate broader implementation.

Participants also flagged the classification inconsistencies across jurisdictions: a token considered a MiFID financial instrument in one country might be viewed as an asset under MiCAR in another, compounding the complexity of cross-border trading for hybrid securities.

The conversation concluded that while the legal foundation exists for hybrid shareholdings, the absence of harmonized operational standards and market liquidity poses a barrier to adoption. A coordinated push involving market participants, financial intermediaries, and regulators is needed to test practical models and create interoperability between traditional and tokenized securities environments.

Call to actions regarding Secondary Markets in case of hybrid shareholdings
The key call to actions from the discussion are: • **Pilot bank-intermediated share conversion models**: Encourage financial institutions and large shareholders to experiment with loan-backed conversion mechanisms to improve liquidity for hybrid shareholdings while minimizing regulatory complexity. • **Clarify treatment of share loans in hybrid contexts**: EU policymakers should assess whether limited-purpose share loans used in hybrid settlements could be exempt from licensing requirements, to enable smoother market function without increasing systemic risk.

2. **Security-token rights are not equally executable EU-wide**

The second topic, introduced by Roland Gollenbeck (Bybit), focused on the lack of harmonized civil law treatment of security tokens across the EU, which results in unequal enforceability of tokenized rights.

While MiFID II and MiFIR provide a harmonized regulatory framework for the licensing, the provision of financial services and classifying financial instruments, the substantive rights embedded in security tokens, such as dividend entitlements, voting rights, and repayment claims, remain governed by national civil, corporate, and property laws, leading to legal fragmentation.

Participants emphasized that once a token qualifies as a financial instrument under MiFID II/MiFIR, it is subject to uniform regulatory oversight across the EU/EEA, including licensing, investor protection, and conduct rules. However, the execution and enforcement of the underlying rights depend entirely on national legal systems (except when operating under the DLT Pilot Regime), which vary widely in their treatment of ledger-based securities. This misalignment undermines the legal certainty and cross-border operability of security tokens.

For example, a security token issued in one jurisdiction may not offer equivalent shareholder protections or enforceable claims in another Member State, even if it meets the same regulatory classification. This creates friction for issuers, investors, and market operators aiming to scale their operations or offer pan-European products.

The discussion revealed that this issue is not unique to tokenized assets, but rather reflects a broader gap in EU civil securities

law. While financial market regulation has advanced toward harmonization, the civil law foundation underpinning ownership, transfer, and enforcement of rights remains fragmented and underdeveloped, especially in the context of DLT-based instruments.

Participants debated whether Decentralized Exchanges (DEXs) could provide a workaround by offering borderless trading infrastructure. However, most agreed that DEXs do not resolve the underlying legal enforceability issues, especially when disputes arise or when investor rights must be exercised in court.

Notably, this was the first topic across all DARTE roundtables where participants agreed that the only viable long-term solution appears to be the creation of a new law (preferably an EU Regulation).

Specifically, the group called for a pan-European "Electronic Securities Law", akin to Germany's eWpG, but harmonized at the EU level. Such a framework would define the legal effects of tokenized securities across all Member States, ensuring consistency in how rights are interpreted and enforced. While politically ambitious, this approach was seen as necessary to close the current gap between regulatory classification and enforceability.

In the short term, participants suggested that industry associations or legal consortia could develop model use cases to submit to regulators, illustrating the enforcement challenges and seeking interpretive guidance.

These use cases would highlight real-world scenarios where rights attached to security tokens fail to operate consistently across jurisdictions, helping build the case for eventual harmonization.

Call to Actions regarding Security-token rights are not equally executable EU-wide

The key call to actions from the discussion are:

- **Develop cross-border use cases to illustrate enforcement gaps**: Legal experts and market participants should collaboratively draft real-world case studies highlighting where tokenized rights fail to operate consistently under current national laws. These examples can be used to engage with regulators and accelerate legal convergence.
- **Promote the development of a harmonized EU Electronic Securities Law**: Industry stakeholders and policymakers should advocate for a common civil law framework that defines the legal status and enforceability of rights embedded in ledger-based securities across Member States.

3. DLT Pilot Regime: Potential Still Unlocked

The final topic introduced by Carola Rathke (YPOG), explored the current limitations and untapped potential of the DLT Pilot Regime, a cornerstone initiative intended to foster experimentation with blockchain-based financial market infrastructure. While the regime represents a major step forward in integrating distributed ledger technology into capital markets, participants agreed that its real-world utility remains severely constrained by both regulatory and technical limitations.

On the regulatory front, the most frequently cited challenge was the quantitative thresholds and restrictive scope imposed on eligible financial instruments and market participants. The pilot is currently limited to relatively small-scale issuances, excluding many complex or illiquid assets that would benefit most from blockchain's efficiency and transparency. Participants noted that these limits may unintentionally discourage institutional adoption and constrain innovation to theoretical proofs of concept rather than live market trials.

Technically, the group discussed the lack of interoperability between different DLTs and between DLT-based systems and traditional financial infrastructures. The fragmentation across service providers, networks, and tools leads to isolated "island solutions," impeding the creation of a single, unified European capital market. Without common technical standards, cross-platform settlement, or shared data exchange protocols, the promised benefits of DLT, such as real-time clearing, cost reduction, and transparency, remain largely unrealized.

Participants welcomed ESMA's recent review of the DLT Pilot Regime, which proposes adjustments to enhance flexibility and scalability. These include:

- Raising the quantitative caps on instrument issuance.
- Expanding the scope of tradable asset types to include more complex products.
- Making the regime permanent to give financial institutions and service providers long-term legal certainty.

There was broad consensus that regulatory ambition must now match technological capability. Financial institutions are beginning to recognize that blockchain infrastructure could provide a competitive edge, particularly for post-trade processes and cross-border issuance. However, concerns were raised about the readiness of DLT service providers, many of whom still face operational maturity issues.

The session also explored whether standards should be introduced now or left to emerge organically. Some compared the situation to the early days of SWIFT, where standardization ultimately enabled mass adoption. While some warned that premature standard-setting might stifle innovation, others argued that early-stage coordination around interoperability, wallet access, and API communication could accelerate the safe scaling of DLT systems.

Finally, the group touched on Layer 1 regulation, suggesting that clear guidance or baseline compliance expectations for

public blockchains might lower the entry barrier for institutional actors without compromising decentralization.

Call to Actions regarding DLT Pilot Regime: Potential Still Unlocked
The key call to actions from the discussion are: • **Support ESMA's proposed amendments to the DLT Pilot Regime**: Policymakers and market participants should collectively advocate for regulatory changes that increase instrument thresholds, broaden the scope of eligible assets, and transition the regime from temporary to permanent, ensuring long-term usability for both retail and institutional markets. • **Develop common European standards for DLT interoperability**: The industry should initiate collaborative efforts to define and promote open, modular technical and legal standards for data exchange, wallet interaction, and cross-chain communication. These standards should aim to reduce fragmentation and support a cohesive digital capital market across the EU.

We thank all participants of the Munich DARTE event for contributing to the discussion: Ayaan Shehryar, Andreas Kriegel, and Axel von Goldbeck (Möhrle Happ Luther), as well as Carola Rathke (YPOG), Christoph Kreiterling (Universität Trier), and Christopher Görz (Bundesverband elektronische Wertpapiere). The session also welcomed Dr. David An (Dracoon Ventures), Dr. Dirk Sturz (FinPlanet), Dr. Nina-Luisa Siedler (siedler legal), and Dr. Philipp Wagner (Deutsche WertpapierService Bank), alongside Hannes Claut (V-Bank), Holger Köther (ETO Group), Ilja Geier (Coinbase), and Jacek Trzmiel (Crystal Intelligence). Additional participants included Josh (Nova), Julia Lippoth (Bullish), Julian Saal (Edelman Smithfield), Kuan-Ning Tseng (Blockchain Founders Group), and Mariana de la Roche Wills (BlackVogel). Rounding out the group were Mathias Bauer-Langgartner (Chainalysis), Miguel Vaz (Hauck Aufhäuser Digital), Ralf Kaaz (Cashlink), Roland Gollenbeck (Bybit), Thomas Wodnitzki (21X), Tilo Palfner (Luminous Labs), Ulrich Gallersdörfer (CCRI GmbH), Walter Börst (DLT Finance), and Walter Hernandez (Exponential Science Foundation).

DARTE SERIES

Madrid 2.0

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU MiCAR. Over time, the series has expanded to address adjacent regulatory regimes, jurisdictional divergences, and emerging technological challenges shaping the crypto-asset ecosystem in Europe.

The Madrid 2.0 DARTE edition was held on October 7th, 2025, at the historic Palacio de Santoña, in collaboration with the European Commission, Project Catalyst, MERGE Madrid, Sumsub, and TRM Labs. The session brought together regulators, legal experts, compliance professionals, and industry innovators to engage in high-level dialogue around operationalizing MiCAR across borders, safeguarding crypto markets from abuse, and exploring novel asset structures such as liquid staking tokens.

Discussions centered on three key topics: cross-border implementation challenges of KYC/AML frameworks under MiCAR (Katherine Cloud, Sumsub), the evolving enforcement landscape around market abuse in crypto-assets (Luiza Castro Rey, TRM Labs), and a practical case study on tokenizing liquid staking mechanisms in a compliant way (Juan Ignacio Ibañez, MiCA Crypto Alliance). The roundtable opened with keynote remarks from Dr. Joachim Schwerin (European Commission) and Jacob Cohen (TRM Labs), who emphasized the growing importance of transatlantic cooperation, responsible innovation, and supervisory clarity as the sector matures.

We extend our sincere thanks to all speakers, contributors, and institutional partners for their generous support in making this roundtable possible. This report captures the insights shared during the session. The views presented reflect the collective understanding of the participants and do not necessarily represent the positions of individual attendees or rapporteurs.

1. **Cross-Border Implementation of MiCAR KYC/AML Standards**

The first topic, introduced by Katherine Cloud (Sumsub), examined the significant operational and legal challenges faced by CASPs in complying with MiCAR's KYC and AML standards across multiple EU jurisdictions. While MiCAR aims to harmonize crypto regulation within the European Union, real-world implementation is complicated by varying national laws, document types, identity verification procedures, and privacy rules.

Participants emphasized that CASPs with cross-border operations must navigate a patchwork of legal expectations that can delay onboarding, increase compliance costs, and heighten regulatory risk. Manual processes for identity verification and risk monitoring, still common in many jurisdictions, are prone to human error and create inconsistent user experiences. This inconsistency directly undermines MiCAR's goals of consumer protection, financial integrity, and regulatory oversight.

The discussion highlighted the potential of advanced technology, including AI-powered document checks, biometric matching, and dynamic risk-scoring models, to streamline compliance. However, without a recognized pan-European framework for digital onboarding and ongoing monitoring, CASPs face uncertainty over what counts as "adequate" under MiCAR.

A flexible but structured framework that could serve as a blueprint for both regulators and market participants was proposed. The model would emphasize transparency, auditability, and proportionality, defining minimum compliance expectations without imposing one-size-fits-all technical mandates. A key proposal was the creation of an expert working group that includes regulators, regtech firms, and EU institutions to map divergences and promote interoperability across Member States.

An illustrative example discussed involved RegTech providers reporting suspicious transactions directly to authorities on behalf of CASPs through secure APIs. This would help reduce operational burdens while ensuring traceability and regulatory alignment. Several participants also noted the need to ensure proportionality for smaller actors and startups, ensuring they can comply without incurring prohibitive costs.

Participants welcomed the notion that MiCAR compliance should be principle-based rather than driven by rigid templates. In particular, a risk-based and adaptive framework could better align with both the fast-moving innovation cycles in crypto and the varying maturity levels of compliance infrastructure across Europe.

Call to Actions regarding MiCAR KYC/AML Implementation

The key call to actions from the discussion are:

- **Establish a cross-border compliance coordination group:** Regulators, market actors, and regtech providers should jointly form an expert working group to develop common frameworks for identity verification, ongoing monitoring, and suspicious activity reporting, adapted to national differences but aligned with MiCAR's core principles.

- **Promote interoperable, principle-based technical guidelines:** Instead of rigid reporting templates, the industry should define adaptive technical and legal standards - such as secure APIs for RegTech integration—that ensure transparency, auditability, and proportionality in both onboarding and risk monitoring.

2. Prevention and Prohibition of Market Abuse Involving Crypto-Assets

The second topic, introduced by Luiza Castro Rey, addressed the urgent need for clearer operational standards and compliance tools under MiCAR Title VI, which came into full application on December 30, 2024, for all Persons Professionally Arranging or Executing Transactions (PPAETs). Participants focused on the structural challenges of preventing and detecting market abuse in the unique context of crypto markets - challenges that differ significantly from those in traditional finance.

Crypto markets are structurally complex: trading is continuous (24/7), assets are listed on hundreds of platforms, and prices vary widely across centralized and decentralized venues. Manipulative behavior takes on new forms, from pump-and-dump schemes to oracle exploits and cross-venue arbitrage strategies. While vast amounts of on-chain data are technically transparent, most actual trading still occurs off-chain, on opaque, centralized platforms, complicating surveillance. Additionally, pseudonymity and fragmented identities make it difficult to identify connected persons or employees engaged in insider dealing.

Participants expressed concern that MiCAR and its accompanying ESMA RTS fail to offer practical guidance on what "sufficient internal controls" should look like. Compliance teams are left to interpret broad obligations without clarity on how to approach:

- Employee wallet declarations.
- Surveillance across off-chain and cross-chain behavior.

- Balancing privacy laws with monitoring obligations.
- Distinguishing between material non-public information and publicly available on-chain data.

Another key discussion point was the definition of "inside information" in the crypto context. MiCAR borrows core principles from the Market Abuse Regulation (MAR) but implements them in a lighter form, particularly not requiring issuers from MAR-style insider lists. This is meant to ease the burden on SMEs and the still native crypto market. However, as soon as a crypto asset becomes underlying to a financial instrument (like derivative, ETN) the more comprehensive MAR market manipulation rules apply again. Participants also debated whether vulnerabilities in smart contracts, DAO governance proposals, or upcoming protocol upgrades qualify as inside information, especially when disclosed on-chain but not widely understood or flagged to the broader public.

Participants agreed that in the absence of consistent enforcement approaches across the EU, both compliance effectiveness and legal certainty are at risk. The roundtable called for structured dialogue with ESMA and national regulators to align on expectations and create crypto-specific adaptations of traditional market abuse controls.

Call to Actions regarding Market Abuse in Crypto Markets

The key call to actions from the discussion are:

- **Establish an industry-led insider dealing compliance taskforce:** Convene regulators, CASPs, and legal experts to develop realistic, proportionate best practices tailored to crypto markets - such as employee wallet frameworks, modified insider lists, and cross-chain surveillance protocols.

- **Clarify the definition of inside information for crypto-assets:** Align market understanding through regulatory Q&A and joint guidance, focusing on the treatment of on-chain disclosures, protocol vulnerabilities, and crypto-specific materiality thresholds, with scaled obligations for SMEs.

Launch of the Tokenization of Liquid Staking taxonomy.

Following the above expert discussions, the final presentation of the Madrid 2.0 DARTE session revisited a key topic that first emerged during the Vienna 2.0 roundtable: The classification challenges of decentralized assets, with Liquid Staking Tokens (LSTs) serving as a central case study. Building on those earlier discussions, the Liquid Staking Tokenization (LST) Project was presented as a concrete next step toward resolving regulatory ambiguity in this area.

LSTs represent a growing category of crypto-assets that allow users to retain liquidity while staking assets like ETH. However, they do not neatly fit into MiCAR's core classifications of utility tokens, ART or e-money tokens - due to the absence of identifiable issuers, claimable returns, or redemption mechanisms. Their decentralized nature and protocol-level governance further complicate their treatment under MiFID II or AIFMD.

To address this gap, the project proposes a dedicated taxonomy based on objective indicators such as decentralization, economic design, and technical risks. It also explores how the MiCAR whitepaper obligations could be adapted when no legal issuer exists, suggesting that the listing CASP could assume disclosure responsibilities focused on smart contract audits and risk transparency.

This project aims to support regulatory convergence, reduce liability risk for CASPs, and enable the safe and compliant offering of LSTs in the EU. It reflects the broader DARTE objective of facilitating industry-led solutions in cooperation with policymakers.

Please find the one-pager summarizing the LST Tokenization Project here.

We thank all participants of the Madrid 2.0 DARTE event for contributing to the discussion:

Adela Pizarro, Almudena de la Mata (Blockchain Intelligence), Andrea Disaro (DeFi Technologies), Andrew Stakiwicz (Hashgraph), Asa Dahlborn (BlackVogel), Ben Bowden (Binance), Claudia Sotelo (CMF), Dennis Rasch (Golem Foundation), Dmitrij Uskov (Bybit), Eric Piscini (Hashgraph), Fernando Zornig (Sumsub), Gabriel Campa (TowerBank), Hannah Zacharias (21Analytics), Jacob Cohen (TRM Labs), Jaime Pradenas (Banco Central Chile), Joachim Schwerin (European Commission), Juan Carlos Reyes (CNAD), Juan Eugenio Tordesillas (ECIJA), Juan Ignacio Ibanez (MiCA Crypto Alliance), Katherine Cloud (Sumsub), Lola Noguera (Binance), Lucia Suarez (Santander), Luiza Castro Rey (FiO Legal), Manu Fernandez (TRM Labs), Mariana de la Roche (BlackVogel), Mariona Pericas (finReg360), Marta Chavarria (SEG Social), Nicole Dyksant (TaxBit), Nil Daunis (Sumsub), Nina-Luisa Siedler (siedler legal), Pedro Mendez de Vigo (Crypto.com), Rocio Alvarez-Ossorio, Sonia Salvatierra (CNV Argentina), and Thomas Taranikuk (Sumsub).

DARTE SERIES

Washington

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of MiCAR and other adjacent policy domains. Over time, the series has expanded to include roundtables across Europe and internationally, addressing region-specific challenges and global coordination needs in the crypto-asset regulatory landscape.

The Washington D.C. DARTE edition was held on October 29th, 2025, at The Homer Building, in collaboration with the European Commission, Government Blockchain Association (GBA), Trilli Tech, Tezos and Linklaters. This marked the first DARTE session hosted in the United States, bringing together legal experts, protocol developers, policymakers, and compliance professionals to exchange perspectives on decentralized governance, cross-border regulatory recognition, and the emerging Liquid Staking Token (LST) taxonomy.

Discussions focused on three core topics: the global Liquid Staking Project emerging from prior Vienna 2.0 DARTE session, and currently under implementation by the MiCA Crypto Alliance, definitional challenges surrounding "fully decentralized" systems in EU law (led by Joanna Rindell and Alex Liu), and the question of mutual recognition of crypto regulations across jurisdictions (presented by Joshua Klayman). The session opened with remarks by Mariana de la Roche and Joshua K., who also delivered a welcome note on behalf of Gerard Dache (GBA). A closing keynote was presented by Mat Yarger (Demia) on the role of decentralized trust infrastructure in global governance.

In the opening remarks, participants acknowledged the accelerating integration of blockchain technologies into both public and private sector services, over 80% of Fortune 500 companies now engage with blockchain in some capacity. The DARTE initiative was recognized as a trusted forum for surfacing actionable policy insights, with outcomes reported to the European Commission and other authorities to inform regulatory development.

A highlight of the session was the keynote by Mat Yarger (Demia), who underscored that digital assets are no longer experimental, they are now part of global financial infrastructure. However, trust in the underlying data remains fragmented and uneven. Yarger advocated for a bottom-up trust model, where data integrity and interoperable standards form the foundation for cross-border digital finance. In parallel, top-down regulatory architectures must evolve to support efficient, transparent, and verifiable financial flows. He emphasized

the principle that systems which are faster, cheaper, more secure, and reduce intermediaries will be adopted by the market, but only if their data can be trusted.

Throughout the Washington edition, the emphasis was clear: legal clarity, regulatory interoperability, and data trust are critical to ensuring that the digital asset ecosystem scales safely and inclusively across borders.

We extend our sincere gratitude to all participants and supporting partners for making this roundtable possible. This report consolidates key insights from the session. It is important to note that the perspectives and conclusions presented herein represent the collective understanding of the topics discussed and do not reflect the individual positions of any participant or rapporteur.

1. **Defining "Fully Decentralized": Diverging Regulatory Perspectives in the EU and U.S.**

The first topic, jointly presented by Joanna Rindell (TriliTech) and Alex Liu (Tezos Commons), addressed the growing transatlantic divergence on how decentralization is defined, measured, and regulated under the EU's MiCAR and the U.S. proposed CLARITY Act.

At the heart of the discussion was Recital 22 of MiCAR, which provides that crypto-asset services "provided in a fully decentralised manner without any intermediary" fall outside the scope of the regulation. However, participants noted that the threshold for qualifying as "fully decentralized" is extremely high. Under MiCAR's substance-over-form approach, even minimal centralized involvement, such as maintaining a frontend or acting as a facilitator, may suffice to bring a protocol under regulatory scrutiny. This creates legal uncertainty for developers, particularly given the lack of operational guidance from ESMA and divergent interpretations among EU Member States. Innovators risk inadvertently falling under regulatory obligations, despite building toward decentralization as an evolving process.

By contrast, the proposed CLARITY Act proposes a more rules-based system, offering a pathway for decentralized protocols to be reclassified outside the

scope of U.S. securities laws. It introduces quantitative thresholds, such as no single entity or group holding more than 20% of governance power or token supply, along with requirements for open-source code, permissionless access, and community-led upgrade processes. While this provides clearer legal markers than the EU approach, participants emphasized that the CLARITY Act is still under consideration in the U.S. Senate and its implementation remains uncertain, especially given the current legislative delays due to the government shutdown.

Participants engaged in a lively comparison of regulatory philosophies: U.S. participants emphasized decentralization as a shield against liability, once a protocol is sufficiently decentralized, its developers should no longer be held accountable for how it's used. EU participants, however, highlighted consumer protection as the guiding principle, cautioning against definitions that might shield market players from responsibility too early or too easily. This divergence reflects not only legal systems but also the underlying values and risk perceptions shaping digital asset regulation.

A potential middle ground discussed was a multi-dimensional scoring framework to evaluate decentralization across vectors such as:

- Token ownership makeup
- Control of code generation & adoption
- Governance/upgradability
- Control of mining/token emission
- Control of token exchange markets
- Control of validation
- Consensus protocol
- Token category (LST, Coin, utility token, NFT, etc)
- community transparency and participation

These eight core dimensions were proposed, though participants acknowledged the complexity of defining each and aligning them across jurisdictions. A key proposal was to develop an objective framework with a rubric for definitive scoring, requiring both a minimum score in each individual dimension as well as a minimum aggregate score for a system to be considered decentralized.

However, some participants suggested that rather than centering regulation around the concept of decentralization, authorities should focus on regulating specific activities and associated risks, i.e., regulating what is done rather than how decentralized it is.

Several historical and technical complexities were also raised:

- Should a blockchain that once met decentralization standards remain exempt if later taken over?
- What about mutable tokenomics?
- How should AI and quantum computing risks be factored in?

The conversation underscored that any viable regulatory approach must balance precision with adaptability. While some feared that premature standardization would stifle innovation, others warned that, in the absence of guidance, definitions would be set by judges in

courtrooms, often with inconsistent or non-technical interpretations.

Ultimately, the session reinforced the urgency of regulatory dialogue and transatlantic coordination, not just to protect consumers and markets, but to provide innovators with clear parameters in which to build responsibly.

Call to Actions regarding Decentralization and Regulatory Clarity

The key call to actions from the discussion are:

- **Propose a transatlantic working group on decentralization standards**: Bring together EU and U.S. policymakers, regulators, and technical experts to explore convergent principles or mutual recognition for assessing decentralization in protocol governance and operation.
- **Develop a modular assessment framework for decentralization**: Encourage the creation of an open-source rubric that allows projects to self-assess across multiple decentralization vectors (e.g., governance, token distribution, frontend control), enabling more transparent regulatory engagement.
- **Clarify enforcement triggers under MiCAR Article 22**: ESMA and NCAs should publish operational criteria for determining what constitutes "intermediary" or "material control," reducing ambiguity for builders and ensuring consistent supervisory practices across Member States.

2. Cross-Border Regulatory Recognition

The second topic, presented by Joshua Klayman (Linklaters), addressed the persistent challenge of regulatory fragmentation across jurisdictions and proposed a pragmatic shift from full legal harmonization to cross-border recognition of crypto-asset regimes as a viable path forward. The session brought to light how diverging definitions, enforcement patterns, and political priorities are creating legal uncertainty that hampers innovation and market entry, not only globally, but even within single jurisdictions like the U.S.

Participants identified that the United States lacks a cohesive federal framework for digital asset markets. Instead, the U.S. legal environment is governed by a patchwork of judicial decisions (e.g., *SEC v. LBRY*, *Ripple*, *Terraform Labs*) and evolving regulatory postures. These rulings remain binding law unless Congress acts to overturn them, even as federal agencies (like the SEC under the current Trump administration) shift their enforcement priorities. Several noted that

while enforcement has paused in some cases, the absence of final judgments leaves legal uncertainty unresolved. In parallel, U.S. states frequently do not recognize each other's licenses, leading to duplicative regulatory burdens for service providers.

This fragmentation is mirrored at the international level. Definitions of "crypto-asset," "stablecoin," or "decentralized finance" differ significantly between the U.S., EU, UK, and jurisdictions such as Singapore or the UAE. Even globally coordinated efforts, such as IOSCO's DeFi Report, have diminished in practical utility as regulators pivot due to political shifts or agency reorganizations.

The group identified a new type of legal uncertainty: not stemming from enforcement, but from the disconnect between regulatory intentions, case law, and actual compliance obligations.

Recognition vs. Harmonization

Against this backdrop, the discussion turned to mutual recognition as a more flexible and achievable alternative to harmonization. Rather than waiting for all jurisdictions to agree on a single global framework, regulators could negotiate bilateral or multilateral recognition agreements based on shared principles.

Key principles that might underpin such recognition include:

- Governance transparency and accountability
- Open-source infrastructure and permissionless access
- Operational resilience and market integrity
- Decentralization safeguards and limits on control concentration
- Clearly articulated definitions and stable legal interpretations

This approach could allow countries to maintain regulatory sovereignty while enabling interoperability across systems and reducing compliance friction for global firms.

Participants stressed that recognition and harmonization are not mutually exclusive. In some areas, such as KYC/AML, financial promotions, or custody standards, harmonization might be appropriate. In others, such as decentralization thresholds or token classifications, recognition based on aligned principles may offer more flexibility.

A clear example was given in relation to UK financial promotion rules, which could be extended to recognize similarly regulated entities in the U.S. without requiring UK-specific licensing. Another example was the GENIUS Act, which could become a building block for mutual recognition between U.S. and EU stablecoin frameworks.

Additional Discussion Points

- State-level challenges in the U.S. (e.g., separate money transmitter licenses in all 50 states) were flagged as a major barrier for cross-border recognition.

- Some participants emphasized the political dimension, noting that

large U.S. firms sometimes resist federal licensing in order to avoid stricter consumer protection mandates.

- Atomic swaps, decentralized market-making, and unified ledgers were cited as market realities that regulators must catch up with, rather than regulate based on outdated infrastructure assumptions.

- The convergence of AI, blockchain, and quantum technologies was raised as a reason to avoid overly rigid harmonization, and instead pursue modular principles adaptable to technological change.

- Others cautioned against "regulatory arbitrage through recognition", where jurisdictions with lax standards are granted legitimacy by more stringent ones. Recognition frameworks must include guardrails and minimum standards to prevent abuse.

- A middle-ground proposal emerged suggesting activity-based harmonization (e.g., for custodial services or stablecoin issuance) combined with recognition of domestic differences in governance or decentralization models.

The session concluded with a shared understanding that while full harmonization of crypto-asset regulation remains a long-term aspiration, it is not a realistic near-term objective given geopolitical tensions, jurisdictional divergences, and differing regulatory philosophies. Instead, participants emphasized that regulatory recognition frameworks, rooted in common principles, offer a more adaptable path forward. Such frameworks can accommodate national sovereignty and technological evolution, while still fostering regulatory coherence, legal predictability, and global market access.

Importantly, the group also acknowledged that recognition and harmonization can coexist, with recognition applied to governance models and structural definitions, while harmonization may suit cross-border financial promotion rules, AML standards, and other operational obligations. Achieving this dual-track strategy will require industry initiative, political will, and ongoing transatlantic dialogue, but it is both necessary and feasible.

Call to Actions regarding Cross-Border Regulatory Recognition
The key call to actions from the discussion are: • **Promote mutual recognition over full harmonization**: Encourage bilateral and multilateral agreements recognizing crypto regulatory frameworks that meet shared baseline principles, such as governance transparency, market integrity, and operational resilience. • **Establish an industry-led interoperability coalition**: Bring together legal experts, regulators, and market participants to define and codify the common principles that could serve as benchmarks for cross-border recognition. • **Advance U.S. federal legislation aligned with global principles**: Support Congressional efforts (e.g. GENIUS Act, CLARITY Act) that would modernize the U.S. digital asset framework and enable clearer pathways for recognition by other jurisdictions.

We thank all participants of the Washington DARTE event for contributing to the discussion:

Participants in the Washington D.C. DARTE edition included Alex Liu (Tezos), Brittany Kaiser (AlphaTON), Carol Van Cleef (Luminous Group), Dan Spuller (Blockchain Association), Douglas Horn (EASE Protocol), Jane Heinrich (Federated Hermes), Janet Adams (Artificial Superintelligence Alliance), Joanna Rindell (Tezos), Josh Lawler (Zuber Lawler), Joshua Ashley Klayman (Linklaters), Joshua Kriger, Mariana de la Roche (BlackVogel), Mat Yarger (Demia), Paul Dowding (GBA Banking & Finance WG Leader), Ryan Singer (VEX), and W. Scott Stornetta (SureMark Digital).

Special thanks to our rapporteur Dexter Woods (Linklaters).

DARTE SERIES

Berlin 5.0

Initiated by Mariana de la Roche W. (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of MiCAR and expanded to include jurisdiction-specific discussions on data protection, identity, market integrity, and regulatory innovation.

The Berlin 5.0 DARTE edition took place on November 11th, 2025 in collaboration with the European Commission, Project Catalyst, and the Cardano Foundation. This roundtable brought together regulators, legal experts, and blockchain practitioners to explore the intersection of digital identity, privacy, and compliance across both public and permissioned blockchain environments.

The agenda centered on three key themes: the risks and trade-offs in implementing eID frameworks; the challenges of aligning decentralized identity systems with GDPR; and the role of digital ID in KYC/AML regulation. The session opened with welcome remarks from Frederik Gregaard (Cardano Foundation) and concluded with reflections from Dr. Joachim Schwerin (European Commission).

We extend our sincere thanks to all speakers, participants, and institutional partners for their valuable contributions. The views presented in this report reflect the collective understanding of the participants and do not necessarily represent the official positions of individual attendees or rapporteurs.

Opening remarks by Frederik Gregaard

The session opened with a keynote by Frederik Gregaard, CEO of the Cardano Foundation, who emphasized the foundational role of digital identity in enabling a secure and inclusive digital economy. He framed identity not merely as a compliance requirement but as a building block for scalable trust and human agency across decentralized systems. Drawing from Cardano's experience supporting identity frameworks in diverse jurisdictions, he underscored the need for regulatory clarity, interoperability between identity providers, and the role of public blockchains in anchoring verifiable credentials without compromising privacy. His remarks set the tone for a day of rich debate on how identity systems can serve both innovation and rights preservation in a fast-evolving regulatory landscape.

The opening reflections noted the persistent tension between user-centric design and data privacy, especially as agentic AI and blockchain-based interfaces become more seamless. Participants emphasized the importance of building trust through auditability, proportionate compliance measures, and greater transparency in digital ID architecture. The group also acknowledged that legal innovation must account for changing user behaviors, especially in contexts where users prioritize experience over control or anonymity.

1. Risks of eID

The first topic of the Berlin 5.0 DARTE roundtable presented by Florian Daniel (Westernacher) addressed the systemic and societal risks posed by centralized digital identity systems, particularly in light of recent amendments to the eIDAS regulation. The discussion opened with the warning that centralised architectures, especially when combined with programmable digital currencies like the Digital Euro, may endanger core European values such as privacy, freedom of expression, and self-determination.

Participants acknowledged the convenience and potential efficiency gains of a unified EUDI wallet containing credentials such as ID cards, driving licenses, and academic certificates. However, they stressed that without viable alternatives or opt-out mechanisms, such systems risk becoming coercive by design. Comparative examples were cited: India, where Aadhaar is required for access to government services; the UK, which has introduced eID-based entry controls; and Australia and Greece, where eID is tied to social media access. In each case, participants questioned how privacy rights and the presumption of innocence could be preserved, specifically, how to prevent identity systems from enabling disproportionate surveillance, restricting access to essential services, or creating centralized points of failure that could be exploited by malicious actors or misused by authorities. Proposed safeguards included the implementation of selective disclosure mechanisms (such as zero-knowledge proofs), the adoption of

fragmented identity models that prevent the consolidation of user data across contexts, and the creation of decentralized credential issuance networks that distribute trust rather than concentrating it in a single authority. Moreover, participants emphasized the need for revocable and unlinkable identifiers, the ability for users to manage consent at a granular level, and a strong commitment to purpose limitation and data minimization principles.

Legal frameworks, including eIDAS, were seen as flexible enough to accommodate these safeguards, but only if regulators and industry actors commit to implementing privacy-preserving architectures by design, not as afterthoughts.

The conversation further explored how eIDs, while often introduced under the pretext of AML, CTF, or child protection, may become tools of surveillance if embedded in centralized infrastructure. Concerns were raised over government visibility into individuals' digital footprints, especially when cash-based alternatives are phased out.

Participants identified several key technical and governance risks:

- Hacking vulnerability of centralized databases, with the German *elektronische Patientenakte* cited as a precedent for the risks associated with large, sensitive data repositories.
- Transaction traceability across all credential uses, which could enable behavioral profiling, blacklisting, or politically motivated control if misused.
- Accountability gaps in decentralized systems, particularly questions around liability in cases of failure, fraud, or dispute resolution, such as who can revoke access or respond to malicious use.
- Revocation and identity theft emerged as particularly difficult to address in decentralized architectures, where no single authority exists to intervene.

Despite these challenges, the group explored several promising alternatives aimed at preserving privacy and self-determination:

- Leveraging ZKPs to validate individual attributes, such as age, residency, or professional qualification, without revealing full identity or enabling transaction-level surveillance.
- Fragmented, context-specific eIDs where only minimal, relevant credentials are shared depending on the situation. For example, in international law enforcement settings, participants discussed how existing systems like Interpol can request identity-related data across jurisdictions, often with limited transparency or user protections. A privacy-preserving alternative would be to only verify that a person meets a specific criterion (e.g., not flagged in a criminal database or having a valid visa), without disclosing their full identity or unrelated credentials,

thus avoiding overreach while still enabling cooperation.

- Designing trust layers for decentralized structures, potentially aligned with the Qualified Trust Service Provider (QTSP) model under eIDAS, where verified nodes provide credentials and can issue or revoke them based on a clear governance framework.

- Using established standardization channels such as ISO and DIN, particularly via the NIA (Standards Committee for Information Technology and Applications), to propose and implement technical standards that safeguard core rights like data minimization, unlinkability, and user control.

Participants proposed building an industry-led identity stack anchored in existing regulatory frameworks but optimized for privacy and user control. Several emphasized the need for a risk-based taxonomy of identity use cases, distinguishing between identity, credentials, and characteristics, and enabling context-specific governance. Disposable eIDs, unlinkable credentials, and revocable permissions were all flagged as areas for further exploration.

Ultimately, the discussion highlighted the importance of distinguishing between control and service. As agentic AI and blockchain-based rails become more widespread, users may not even be aware of the backend infrastructure. Regulators must ensure that the convenience of digital identity does not override citizens' rights

Call to actions regarding eID and Digital Identity Risks

The key call to actions from the discussion are:

- **Propose a risk-matrix and taxonomy for eID systems:** Create a classification framework for identity types and usage contexts to inform proportional governance and technology design.

- **Develop ISO-standard proposals for privacy-preserving digital identity:** Industry stakeholders should coordinate through DIN/ISO to shape globally applicable, decentralized ID standards aligned with fundamental rights.

- **Encourage fragmented, revocable identity structures:** Promote architectures that allow multiple disposable IDs, context-specific credentials, and revocation mechanisms to reduce surveillance and misuse.

2. Digital IDs on public blockchain & GDPR

The second topic of the session, presented by Nicolas Jacquemart (Cardano Foundation) focused on reconciling digital identity systems on public blockchains with the European Union's data protection framework, particularly the GDPR. The discussion started by addressing the inherent tension between immutable, transparent infrastructures like public blockchains and legal requirements such as the right to erasure, data minimization, and purpose limitation.

Public blockchains are generally not recommended for storing personally identifiable information (PII) due to their append-only nature and universal accessibility. Any data recorded on-chain is potentially permanent and visible to anyone. This raises concerns under GDPR, which mandates that individuals retain rights over their personal data, including the right to rectification and deletion. Yet, the need for identity solutions that ensure accountability and trust in decentralized ecosystems has led to new models attempting to square this circle.

One such model is the Key Event Receipt Infrastructure (KERI), a standard that creates decentralized, self-certifying identifiers and cryptographic event logs (KELs). Instead of storing identity data on-chain, KERI logs key events and changes to identifiers. These logs are verifiable without exposing personal data. The argument presented was that, when properly implemented, the KELs and associated identifiers (AIDs) can be considered anonymous from the perspective of most nodes or observers, provided they lack the legal or technical means to link them to a natural person. In such cases, the GDPR would not apply to the processing of that data by those entities.

Participants debated whether such a system meets the relative or absolute threshold of identifiability under GDPR. Under the absolute approach (favored by some EU regulators), any possibility that someone could identify the data subject means the data is personal, regardless of who processes it. Under the relative approach, the key question becomes whether the specific processor (e.g. a node operator) has the means or legal authority to identify the subject. The relative view was generally preferred by participants, as it enables public blockchain participation without turning every node into a GDPR controller.

In addition, several participants referenced recent CJEU rulings (notably EDPS v SRB) which confirm that identifiability under data-protection law must be assessed in a contextual, actor-specific manner: even pseudonymised or hashed data may remain "personal" if the processor can re-identify, whereas for another actor lacking the means the same data may fall outside GDPR. The Court emphasised the controller's obligation at collection and the 'reasonably likely means' test of re-identification

Beyond identifiability, the session touched on the complexities of how GDPR compliance overlaps with other legal

requirements, especially those related to AML and the travel rule. Participants noted that while selective disclosure tools like ZKP and designated-access protocols could help limit unnecessary data exposure, AML frameworks often require full identity verification. This creates a tension: public blockchain architectures are built for transparency and decentralization, while AML enforcement increasingly demands traceability, risk flagging, and data retention.

The debate extended to the governance of these systems. Could a public, permissionless blockchain ever qualify as a "qualified electronic ledger" under eIDAS? While such ledgers would carry compliance obligations similar to qualified trust service providers, the certification process and practical feasibility of qualifying a decentralized infrastructure remains uncertain. Nonetheless, there was optimism that the legal framework allows for layering, building compliant identity services on top of public infrastructure without compromising core decentralization.

Participants also acknowledged practical risks. Even hashed identifiers or metadata patterns on-chain could, with enough auxiliary information, be used to profile users. Examples were raised of blockchain forensics firms mapping wallet behavior and linking accounts through off-chain data, undermining the assumption of pseudonymity. Moreover, use cases involving recovery from lost wallets, family-access credential sharding, and identity revocation were discussed as critical areas where technical innovation must align with user rights and legal safeguards.

Several proposed safeguards and governance mechanisms emerged:

- Create risk matrices and use-case taxonomies to define identity assurance levels, separating low-risk disclosures (e.g., age verification) from high-risk, sensitive attributes (e.g., health or criminal data).
- Encourage disposable and fragmented identity systems that give users control over what is revealed and to whom, minimizing centralized storage or reuse of full identities.
- Promote private-sector-driven standards for digital ID that complement official eIDAS frameworks, giving users interoperable but privacy-preserving tools.
- Recognize the importance of standardization bodies such as ISO and DIN in defining common criteria for selective disclosure, consent revocation, and data minimization.

The discussion closed with calls to harmonize AML and GDPR compliance approaches, noting that the current siloed development of these regimes leads to operational inefficiencies and excessive data exposure. Rather than forcing trade-offs between compliance and privacy, participants advocated for a rights-based design of digital identity systems where selective disclosure and auditability are not just technically feasible, but legally recognized

Call to Actions regarding Digital Identity & GDPR:

The key call to actions from the discussion are:

- **Advocate for a relative standard of identifiability under GDPR:** Building on identity protocols like KERI, encourage the European Data Protection Board and national authorities to adopt contextual, risk-based interpretations of identifiability. Where processors (e.g., blockchain nodes) lack reasonable means to re-identify individuals, such as when processing non-personal Key Event Logs (KELs), such data should be treated as anonymous, thus falling outside the scope of GDPR. This interpretation aligns with recent CJEU rulings (e.g., *EDPS v. SRB*) and reduces unnecessary compliance burdens on decentralized infrastructure operators.
- **Standardize selective disclosure and revocation mechanisms:** Work through ISO/DIN and industry consortia to create technical and legal standards for identity operations that balance verifiability with privacy.

3. Digital Identity in AML/KYC

The final topic, presented by Mariana de la Roche W. (BlackVogel), examined the evolving role of digital identity in AML, Know Your Customer (KYC), and Travel Rule enforcement. The session highlighted the paradox at the heart of compliance-driven identity systems: while they promise greater transparency and security, they risk creating excessive surveillance, undermining privacy, and placing disproportionate burdens on both users and industry actors.

Participants explored how digital identity frameworks could support a more efficient and rights-preserving approach to compliance, particularly if implemented using decentralized architectures and cryptographic tools. The idea of "identity on demand" emerged as a key concept: rather than transmitting personal data with every transaction, users could present a verifiable credential that proves a KYC check was performed by a trusted third-party. Only in the event of a flagged transaction would further identity verification be triggered. This selective disclosure model would allow compliance officers to fulfill regulatory obligations without accessing full user profiles or storing sensitive data unnecessarily.

Nevertheless, the crypto industry has proactively developed innovative compliance-enhancing tools since its early

days, not because of regulatory mandates, but because doing so was in the interest of users and market integrity. From selective disclosure to credential-based attestations, many solutions now exist that could help regulators meet their objectives without sacrificing privacy or inclusion.

Despite its promise, this approach currently faces legal and institutional barriers, especially within the EU. Under existing AML and GDPR frameworks, the reuse of KYC certificates and the non-sharing of personal data between entities may conflict with current interpretations of due diligence and supervisory access. Participants noted that in traditional finance, banks often rely on third-party KYC verifications without issue. Extending this logic to CASPs could yield significant privacy gains and reduce compliance costs, but would require regulatory clarification or reform.

There was a strong consensus that current AML rules are overengineered and inefficient. Participants cited empirical data and regulatory feedback indicating that the billions spent on AML compliance often yield minimal results. Many AML structures, it was argued, breed the very inefficiencies and inequalities they seek to prevent: smaller firms are priced out of compliance, while sophisticated actors circumvent controls with ease. In this context, digital identity frameworks risk becoming tools of exclusion or performative compliance, rather than meaningful safeguards.

To move forward, participants emphasized the importance of designing interoperable, risk-based systems that adapt verification requirements to transaction context and user risk profile. Credentials should be revocable, auditable, and compatible with GDPR. Authorities could confirm that obligations were fulfilled not through direct data access, but via cryptographic attestations or ZKP. This would reduce unnecessary data exposure while maintaining traceability.

The conversation also touched on the broader policy failure of siloed regulation: AML, data protection, and technological innovation have evolved in isolation, creating contradictory mandates. There was a call for greater coordination among regulators, as well as structured industry input, particularly through sandboxes and legislative feedback mechanisms.

Participants agreed that the aim is not to replace compliance with anonymity, but to realign it with proportionality, efficiency, and user agency. The industry must take the lead in proposing alternatives that respect rights without compromising on enforcement objectives.

Call to Actions regarding AML/KYC and Digital Identity
The key call to actions from the discussion are: • **Pilot privacy-preserving KYC models based on reusable credentials and selective disclosure**, allowing compliance obligations to be fulfilled through verifiable attestations rather than bulk data collection. • **Establish structured dialogue between regulators and industry innovators**,especially within EU innovation sandboxes, to test and co-design solutions that align AML enforcement with GDPR and fundamental rights.

We thank all participants of the Berlin 5.0 DARTE event for contributing to the discussion:

Aiden Ward (Radix Foundation), Åsa Dahlborn (BlackVogel), Benedikt Faupel (Bitpanda), Benjamin Buergi (Cardano Foundation), Colin Nimsz (Brighter AI), Florian Daniel (Westernacher), Florian Reul (Schufa), Janine Roemer, Jannik Piepenburg (Deloitte), Joachim Schwerin (EU Commission), Jonas Hammer (IDUnion), Jörn Erbguth (Geneva Macro Labs), layer0 (Powerhouse), Maria Claudia Rodriguez (BlackVogel), Mariana de la Roche (BlackVogel), Martijn Keuzenkamp, Mathias Nörenberg (N26), Nicolas Jacquemart (Cardano Foundation), Nina-Luisa Siedler (siedler legal), Oliver Nägele (Blockchain Helix), Radoslav Albrecht (Bitbond), Silvan Jongerius (TechGDPR), Tamari Asatiani (BVR), Yannick Scholz (BaFin).)

DARTE SERIES

Helsinki

Initiated by Mariana de la Roche W. (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), the DARTE Series is a high-level roundtable format designed to enhance legal clarity around digital assets, focusing on regulation, compliance, data protection, and market integrity.

The Helsinki DARTE edition took place on November 19th, 2025, in collaboration with the European Commission, Project Catalyst, Bybit EU, and Nordic Law. The roundtable gathered regulators, legal practitioners, and crypto infrastructure providers to explore the challenges and opportunities of cross-border compliance in the digital asset space.

The agenda focused on three strategic themes: 1) the legal and technical complexity of multi-jurisdictional stablecoin issuance, presented by Max Atallah (Nordic Law); 2) the tension between MiCAR and PSD2 in dual-licensing regimes, led by Simon Seiter (AllUnity) and 3) the emerging "reserves concentration crunch", analyzed by Magnus Jones (Nordic Blockchain Association).

We extend our sincere thanks to all speakers, participants, and institutional partners for their valuable contributions. The views presented in this report reflect the collective understanding of the participants and do not necessarily represent the official positions of individual attendees or rapporteurs.

Opening remarks by Mazurka Zeng

The Helsinki session opened with a keynote by Mazurka Zeng (Managing Director, Bybit EU), who called on the ecosystem to view stablecoins not merely as assets but as foundational infrastructure for Financial 3.0, a global shift toward programmable, borderless value transfer. Using the simple example of buying a coffee with crypto, Mazurka illustrated the persistent frictions of today's financial system: high fees, slow settlements, limited access, and an innovation gap in everyday payments.

She framed this moment as a convergence of timing, technology, and trust: programmable finance is now possible thanks to blockchain rails; stablecoins have matured into reliable value anchors; and regulatory clarity through frameworks like MiCAR is finally unlocking institutional participation. In this context, she argued, stablecoins can serve as trust, liquidity, and settlement layers, enabling transparent, real-time, and programmable transactions across borders.

Mazurka distinguished stablecoins from e-money and CBDCs, emphasizing their global, open-network potential compared to the domestic and sovereign limitations of legacy instruments. With Europe's vast export volume and the Nordics accounting for a significant share, she identified cross-border payments as the first killer application of stablecoins and urged the industry to align around this use case.

To fully unlock this potential, Mazurka highlighted three key challenges: integration with traditional financial infrastructure, liquidity and FX conversion corridors, and strengthening the real-world utility of stablecoins. She called for ecosystem coordination, incentives for users, and collaboration across sectors. Her remarks set a pragmatic and forward-looking tone for the roundtable's discussion: stablecoins are not just tools for crypto-native users, but gateways to a more inclusive, efficient, and programmable financial system, if built with interoperability, regulation, and utility in mind.

1. Multi-Jurisdictional Stablecoin Issuance

The first topic of the roundtable presented by Max Atallah (Nordic Law) examined the legal, operational, and supervisory challenges surrounding multi-jurisdictional issuance of stablecoins under MiCAR.

The discussion began by reaffirming a core point of legal clarity: MiCAR does not prohibit multi-jurisdictional issuance of EMTs or ARTs. On the contrary, Recital 54 and Articles 38 and 54–56 explicitly anticipate situations where tokens are issued inside and outside the Union, requiring that reserves corresponding to EU liabilities be held under EU law. This design confirms that MiCAR was drafted to manage cross-border issuance, not to exclude it.

Participants contrasted this legal reality with the current supervisory climate, noting that the ECB has opposed multi-jurisdictional issuance on prudential and monetary sovereignty grounds. This resistance is political rather than legal, yet

it has created a chilling effect across the market: some national authorities refrain from authorizing multi-jurisdictional structures, while others continue to process such applications. The result is an uneven supervisory landscape where similar applicants receive divergent treatment depending on the Member State.

Concrete examples discussed highlighted the fragmentation: stablecoin models where a token is issued simultaneously from an EU entity and a non-EU entity, such as U.S./France or Singapore/Finland issuance structures, illustrate the operational reality of global stablecoins. These models underscore that multi-entity issuance is already happening worldwide, and MiCAR's architecture is intended to regulate such arrangements rather than block them.

A central point raised was that, in practice, issuers operating globally must comply with two full legal regimes simultaneously: MiCAR on the EU side, and the applicable rules in their non-EU issuance location. This dual compliance burden inevitably favors larger, better-capitalized actors who can manage multiple reserve pools, legal teams, and supervisory interfaces, while smaller issuers face structural disadvantages. Some participants argued that this creates a competitive distortion within the EU market, contrary to MiCAR's intention of establishing a level playing field.

The roundtable then examined the operational consequences for consumer protection, especially in stress scenarios such as redemptions or bank-run-like events. Concerns were raised about the "mixing of baskets" problem, where reserves supporting EU-issued tokens and non-EU-issued tokens may become intertwined, complicating redemption rights and supervisory clarity. Suggestions such as burn-and-mint bridging mechanisms were discussed as possible ways to ensure jurisdictionally clean issuance flows, though not without operational trade-offs.

A strong theme in the discussion was the need for a coordinated market response, independent of immediate regulatory action. Participants noted that without unified industry signalling, policymakers and supervisors are left dealing with fragmented stakeholder input. It was suggested that an industry-driven interpretive note, clearly explaining why multi-jurisdictional issuance is allowed under MiCAR, could help correct misperceptions and restore confidence for both issuers and NCAs. Alongside this, the idea of creating a neutral EU Stablecoin Association was seen as a constructive way to consolidate expertise, develop shared operational standards (particularly around reserves and redemptions), and offer EU institutions a single, structured counterpart.

Finally, the session highlighted the broader strategic importance of industry advocacy. Participants referenced ongoing work in Brussels and other international forums, underscoring that MiCAR emerged partly in response to global stablecoin initiatives. Several voices encouraged more direct engagement with EU working groups, especially as the Commission is increasingly aware of the practical frictions that arise when

regulatory interpretation diverges across Member States.

Call to Actions regarding Multi-Jurisdictional Stablecoin Issuance
The key call to actions from the discussion are: • Develop a joint interpretive note clarifying why multi-jurisdictional issuance is fully permissible under MiCAR, drawing on Recital 54 and Articles 38, 54–56. • Launch an EU Stablecoin Association to coordinate issuers, harmonize reserve and redemption practices, and present unified input to policymakers and supervisors. • Promote shared operational standards, including reserve segregation and jurisdiction-specific redemption protocols, to strengthen consumer protection and reduce supervisory fragmentation.

2. Dual licensing requirement (MiCAR&PSD) by Simon Seiter

The second topic of the roundtable presented by Simon Seiter (AllUnity) focused on the emerging conflict between MiCAR's defined crypto-asset transfer services and PSD2 payment services, and the growing pressure for CASPs to obtain dual licenses.

While MiCAR Recital 90 and Articles 48(2) and 70(4) clearly authorize CASPs to provide "transfer services for crypto-assets" including the transfer of EMTs some national authorities and legal advisors are interpreting these activities as equivalent to PSD2-regulated payment services. As a result, CASPs are increasingly being pushed to apply for additional PSD licenses, even when their activities are already regulated under MiCAR and the EU TFR.

Participants highlighted that this dual licensing requirement arises from two core misinterpretations. First, wallets, especially non-custodial ones, are being incorrectly equated with PSD2 "payment accounts", even though PSD2 accounts involve bank-held instruments with specific settlement mechanisms, while wallets act more like digital vaults or bearer instruments. Second, on-chain transfers between crypto addresses are being mischaracterized as credit transfers or money remittances under PSD2, even though no traditional payment service provider (PSP) handles or forwards fiat-based "funds" in such transactions.

These interpretive overlaps have led to market distortion. CASPs operating under

MiCAR's scope face unnecessary legal uncertainty, higher compliance costs, and duplicative regulatory burdens. Several roundtable participants observed that MiCAR is a full regulation, whereas PSD2 is a directive, implying that MiCAR's provisions should, in theory, override conflicting interpretations. Nonetheless, in practice, several CASPs are preparing PSD2 license applications to preempt supervisory pushback.

The roundtable acknowledged that true PSD2 services, such as fiat payouts during redemption or merchant acquiring, do require a payment license and should be routed through regulated PSPs. However, the group strongly agreed that pure on-chain EMT transfers performed by CASPs are already governed by MiCAR and the TFR, and should not trigger PSD2 obligations.

A range of perspectives and examples were shared. Analogies were drawn to physical money transporters, which are not considered payment service providers under PSD2, even though they move value on behalf of clients. Similarly, EMT custody was likened to vault services rather than banking accounts. Concerns were also raised about minimum capital requirements for PSD2 (e.g., €700,000), which many CASPs are unable to meet, especially in jurisdictions applying high compliance thresholds.

The ambiguity around "the flow of funds", specifically when a transfer becomes a remittance, was repeatedly flagged as a source of divergence among national regulators. Several participants noted that the interpretation gap across the EU is big, with some NCAs adopting aggressive stances and others remaining neutral. This divergence undermines the harmonization intent of MiCAR and risks delaying market development across the bloc.

The discussion emphasized the need for immediate clarification to prevent the dual licensing issue from solidifying into practice. Participants proposed the development of a joint interpretive note clearly outlining when PSD2 applies, and when it does not. Such a document would define a clean perimeter for CASP transfer services under MiCAR, reaffirming that:

- CASPs do not operate PSD2 payment accounts;
- They do not receive or forward "funds" in the PSD2 sense;
- They solely provide transfer services as defined in MiCAR;
- Any fiat legs are executed by licensed PSPs or separate MiCAR entities under Article 70(4).

A lively exchange followed on possible institutional mechanisms to support this clarification. Ideas included launching a sandbox model to test these boundaries in practice, establishing a dedicated ombudsman-style body for crypto licensing disputes, and even mounting a strategic court case, with collective industry backing, to establish precedent.

However, participants noted that access to courts is limited, and few CASPs would challenge their own NCAs. This led to calls for creating a pan-European vehicle or platform through which stakeholders could jointly raise interpretive questions with the ECB, EBA, or Commission.

Participants expressed urgency, as several firms have already begun submitting PSD license applications out of caution, despite believing them unnecessary. The discussion closed with broad consensus that on-chain crypto transfers should not be treated as payment services under PSD2 and that decisive clarification is needed to avoid regulatory overreact

Call to Actions regarding Dual Licensing Requirements
The key call to actions from the discussion are: • Draft and circulate a joint interpretive note explaining why EMT transfers by CASPs fall under MiCAR, not PSD2, and specifying clear legal boundaries to avoid licensing duplication. • Push for proportionate convergence among national supervisors, including recognition that wallets are not PSD2 payment accounts, and that on-chain movements do not constitute money remittance. • Establish a structured forum or strategic coordination vehicle for raising interpretive challenges with EU-level institutions, enabling faster resolution of regulatory ambiguity across Member States.

3. The Reserves Concentration Crunch

The final topic presented by Magnus Jones (Nordic Blockchain Association). addressed the growing tension over how MiCAR and its forthcoming RTS should define and manage reserve requirements for stablecoin issuers, particularly around liquidity, custody, and concentration limits.

Participants examined the question at the heart of the policy debate: will tighter reserve rules reduce systemic risk, or will they simply concentrate that risk within a narrow group of large custodians and institutions? This issue has come into sharper focus following divergent views between the European Commission and the EBA on the draft Regulatory Technical Standards (RTS). While the Commission proposed more flexible rules for reserve assets in mid-2025, the EBA later pushed back, warning that overly permissive language could open the door to liquidity mismatches and regulatory arbitrage.

Several operational and structural risks were highlighted:

- Market bottlenecks and systemic concentration, as strict interpretations funnel reserves toward a small set of "eligible" custodians or high-quality liquid

financial instrument (HQLFI), increasing dependency on a few players.

- Funding and yield pressures, as narrow reserve categories drive up costs for issuers, either through lower yields or high custody premiums, undermining economic viability and raising barriers to entry.
- Regulatory ambiguity, with differing national interpretations of what qualifies as a HQLFI, or what custodial arrangements are permissible, leading to fragmentation and hesitation across Member States.
- Practical liquidity mismatches, where assets may appear liquid on paper but fail to monetize quickly under stress, especially if held through a single custodian or without pre-arranged liquidity lines.

Discussion also covered the legacy distinction between ARTs and EMTs, originally driven by political responses to past projects, which now appears outdated in practice. Participants questioned whether regulatory focus on reserve quality and concentration is addressing the right risks, or merely displacing them. There was broad concern that current approaches may entrench incumbents, reduce competition, and limit the market's ability to innovate responsibly.

The conversation further addressed the disconnect between the back-end mechanics of stablecoin systems, such as programmable settlement, multi-custody, and real-time attestation, and the still-static assumptions embedded in some of the RTS proposals. Participants called for more realistic, evidence-based calibration, including real-world stress scenarios and harmonized supervision of reserve management.

Ultimately, the group emphasized the need for a proportionate, risk-sensitive reserve framework that ensures redeemability and resilience without forcing the ecosystem into a fragile monoculture.

Call to Actions regarding Reserve Management
The key call to actions from the discussion are: • Calibrate reserve rules based on real liquidity risks, not just asset class labels: prioritize demonstrable stress resilience and convertibility over rigid categories. • Promote supervisory harmonization across Member States, especially on concentration thresholds and custody standards, to avoid fragmentation and reduce regulatory arbitrage. • Launch supervised pilots to gather operational evidence, allowing for phased calibration of RTS and the development of adaptable, transparent reserve frameworks that reflect the complexity of the ecosystem.

We thank all participants of the Helsinki DARTE event for contributing to the discussion:

Anna Agu (Lex Law Office), Åsa Dahlborn (BlackVogel), Aslak Smedshaug (Quantoshi), Cecilie Sturich, Gustav Buder (Bybit), Hanne Reese Holm (Reese Legal), Hans Henrik Hoffmeyer (Coinify), Jaakko Sorsa, Jani Ultamo (Coinmotion), Jon Hautamäki (Nordic Law), Jon Kåre Stene, Joonas Järvinen (Kvarn Investment Services), Kaja Vagle (Crypto Clarity), Magnus Jones (Nordic Blockchain Association), Markus Lehtonen (Blockchain Forum Finland), Martin Wichmann (Kvarn), Max Atallah (Nordic Law), Mazurka Zeng (Bybit), Dr. Nina-Luisa Siedler (siedler legal), Patrick Aarikka (Kvarn X), Raido Saar (Estonian Web3 Chamber / ComplyOnce), Robert Tollet (Northcrypto), Sascha Bross, Sigbjørn Rivelsrud (Quantoshi), Simon Seiter (AllUnity), Thorstein Thinn (Cointegrity), and Uve Poom (CryptoSwift).

DARTE SERIES

Rome

Initiated by Mariana de la Roche W. (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), the DARTE Series is a high-level roundtable format designed to enhance legal clarity around digital assets, focusing on regulation, compliance, data protection, and market integrity.

The Rome DARTE edition took place on December 5th, 2025, in collaboration with the European Commission, UNIDROIT, and Bybit. The roundtable gathered legal scholars, regulators, and industry leaders to explore the evolving intersection between private law doctrines and digital asset infrastructure, in light of the recently published UNIDROIT Principles on Digital Assets and Private Law.

The agenda focused on three strategic themes: (1) the key legal and operational challenges faced by the digital asset industry, presented by Georg Harer; (2) the practical implementation of the "control" concept in digital asset transfers, discussed by Tomáš Kozárek; and (3) the application of the UNIDROIT Principles on Digital Assets and Private Law to financial instruments, analyzed by Tecla Rodi. The session was opened with welcome remarks by Professor Ignacio Tirado (UNIDROIT Secretary-General) and concluded with a keynote address by Dr. Joachim Schwerin (European Commission).

We extend our sincere thanks to all speakers, participants, and institutional partners for their valuable contributions. The views presented in this report reflect the collective understanding of the participants and do not necessarily represent the official positions of individual attendees or rapporteurs.

Ignacio Tirado Keynote

The session opened with keynote remarks by Professor Ignacio Tirado, Secretary-General of UNIDROIT, who recalled that the work of UNIDROIT focuses on the harmonisation of private law and the modernisation of private law rules; it does not concern regulation or public law. Thus the UNIDROIT Principles on Digital Assets and Private Law need to be read as complementary to domestic regulatory frameworks. He emphasised that the UNIDROIT Principles on Digital Assets and Private Law address digital assets traded in the market and are meant to assist governments in complementing existing private law and financial regulations. Professor Tirado noted that the main purpose of the UNIDROIT Principles on Digital Assets and Private Law is to provide legal certainty in the use of digital assets. It is for this reason that the instrument provides a rule of control which is based in fact and not law, as well as rules on innocent acquisition to protect market transactions while being respectful of national definitions of bona fide acquisitions. Other rules protective of legal certainty include the shelter rule, and the provisions on custody and insolvency.

The keynote served as a call to anchor innovation in market infrastructure within the rule of law, ensuring protection, certainty, and interoperability across jurisdictions.

1. **Industry Challenges: Legal Certainty for CASPs and Private Law Fragmentation**

The first session of the Rome roundtable, presented by Georg Harer, Co-CEO of Bybit EU, explored the regulatory and civil law disconnects facing CASPs operating under MiCAR. While MiCAR establishes robust rules for custody, safekeeping, and operational conduct, it remains silent on core private law issues such as the legal nature of crypto-assets, their transferability, or enforceability.

These gaps create friction between compliance obligations and legal certainty, particularly when service providers operate across multiple Member States with divergent civil codes.

Participants emphasized that the absence of harmonized private law rules undermines MiCAR's intended legal clarity and cross-border effectiveness. While full unification of property law across Europe is politically unrealistic, there was strong support for a sector-specific harmonization instrument, akin to the EU Financial Collateral Directive, that could establish minimum standards for the recognition of ownership, transfer, and enforcement rights for crypto-assets.

The discussion drew on the experience of jurisdictions like Italy and Liechtenstein, which have begun to link digital asset frameworks with domestic securities and property law regimes. It also considered the role of soft law, with UNIDROIT's Principles on Digital Assets and Private Law cited as a functional template for building consensus and guiding legislative reform.

The roundtable featured three complementary approaches to addressing the legal uncertainty. First, the proposal for a dedicated EU directive was widely discussed. While many agreed on the need for a sector-specific instrument, some raised concerns that directives, unlike

regulations, leave room for national variation, potentially reintroducing fragmentation. A minority of participants suggested that a regulation might better serve the goals of consistency and legal certainty across Member States. Others, however, flagged the limitations under the Treaty on the Functioning of the European Union (TFEU), particularly Article 345, which reserves property law to national competence, and Article 114, which may not be sufficient on its own to justify harmonization. Some participants cited the CJEU's Essent judgment as a reminder that EU legislative efforts must remain within clearly defined legal bases.

Second, soft law solutions were highlighted as a valuable interim measure. The UNIDROIT Principles on Digital Assets and Private Law were seen as an appropriate tool to guide NCAs, legislators, and the private sector in interpreting and applying digital asset-related rules until formal EU legislation is adopted. Given the often lengthy and politically complex process of drafting hard law, soft law instruments offer flexibility and responsiveness in rapidly evolving technological contexts. Participants noted that a bottom-up approach, starting with shared definitions and best practices, may be more realistic than seeking full convergence at the outset.

Third, the concept of mutual recognition was introduced as a pragmatic alternative to harmonization. Rather than seeking to align national private law systems substantively, Member States could agree to recognize each other's legal characterizations of digital asset ownership, transfer, and enforcement rights. This approach would preserve national sovereignty while enabling cross-border legal operability, particularly for CASPs active across multiple jurisdictions. Participants noted that similar recognition mechanisms already exist in the treatment of e-money and financial instruments, offering a workable precedent for digital assets. Some further suggested that bilateral or multilateral agreements between Member States could help build legal bridges in the absence of binding EU law, and that such strategies could eventually be backed by a new treaty-based provision, akin to Article 118 TFEU on intellectual property rights, to support future legal harmonization of digital assets as intangible goods.

The group also debated key technical-legal questions: What constitutes ownership in a digital asset system? Where do rights start and end? If "control" is used as the functional equivalent of ownership, what happens to traditional legal notions like custody, enforcement, and title? Discussions highlighted that in many cases, civil law still relies on contractual agreement or user terms to define transfer rights, which is insufficient for robust legal certainty.

There was general consensus that "we can't build a regulatory regime on a legal fiction," and that allowing Member States to drift into incompatible interpretations would erode the effectiveness of MiCAR.

The roundtable concluded that legal certainty for digital assets, especially in the context of control, pledge, and custody, must be addressed not only through regulatory measures but also through private law instruments that ensure interoperability across borders. Whether

pursued through hard law, soft guidance, or mutual recognition, the shared objective remains clear: to align MiCAR's supervisory framework with enforceable legal rights that underpin trust and functionality in crypto markets.

Calls to Action regarding Legal Certainty for Crypto-Assets
The key calls to action from the discussion are: • Promote an EU Directive or Regulation on the Legal Certainty of Crypto-Assets, drawing from the Financial Collateral Directive model to align MiCAR with minimum private law standards. • Encourage Member States to recognize the proprietary character of digital assets and the validity of control-based transfer mechanisms, using the UNIDROIT Principles on Digital Assets and Private Law as reference. • Support the inclusion of crypto-asset legal effects in broader EU private international law instruments (e.g., Rome I, Rome II) to resolve cross-border legal fragmentation.

2. Implementing the "Control" Concept in Civil Law Systems

The second topic, presented by Tomáš Kozárek, Head of the International Law Unit in the Ministry of Industry and Trade of the Czech Republic, examined the challenges of incorporating the concept of control, as developed in the UNIDROIT Principles on Digital Assets and Private Law, into civil law jurisdictions. Control, as distinct from ownership, is the functional equivalent to possession of movables. It is a factual concept intended to reflect the technical capacity to manage a digital asset via private keys or similar mechanisms. However, this concept lacks a clear analogue in traditional civil codes, where property rights are closely tied to tangible possession or legal registration.

Participants debated whether control can be analogized to possession for the purposes of legal effect, or whether a sui generis legal category is needed. Some jurisdictions, such as the Czech Republic, are exploring interim solutions that interpret control functionally while avoiding structural changes to their civil law systems.

Others noted that analogies may be insufficient, particularly when addressing questions of liability, transfer, and dispute resolution in decentralized environments.

The discussion also touched on the risks of relying solely on factual abilities (e.g., access to a private key) as a basis for legal recognition, especially in cases of shared or multi-signature control structures. Participants noted that while "custody" and "control" are distinct legal concepts, they often overlap in practice: custodians typically hold not just legal responsibilities, but also technical control over digital assets. This raises questions about who holds entitlement versus who holds power, particularly in custodial arrangements under MiCAR, where CASPs may possess control without being the beneficial owner.

Several speakers emphasized the need for legal frameworks to distinguish between factual control and legal entitlement, especially in light of the growing complexity of custody models in digital finance. In this context, participants also discussed the importance of protecting good faith acquirers and third parties who act in reliance on on-chain data. Without legal presumptions or clear standards around what constitutes effective "control," these actors may be exposed to unjustified legal risks.

A central theme in the discussion was the need to reconcile the technological functionality of DLT systems with the existing legal traditions of civil law countries. Some experts argued that efforts to "force" the concept of control into pre-existing legal categories like possession or ownership may ultimately limit innovation or create inconsistencies in enforcement. Others advocated for a more cautious, incremental approach — for example, by interpreting control as a form of "factual power" that gains legal effect only when combined with intent or contractual context.

There was also discussion around the flexibility of soft law instruments such as the UNIDROIT Principles on Digital Assets and Private Law to support legal systems in adapting to these challenges. As formal legal reform can be slow and politically sensitive, participants viewed soft-law guidance as an essential bridge in the transition phase. Comparative legal experiences, including insights from jurisdictions like Kyrgyzstan and Liechtenstein, were cited as useful models for understanding how digital asset control could be integrated into private law.

Ultimately, there was consensus that implementing the concept of control will require legal innovation, but also careful calibration to avoid unintended consequences in other areas of private law, such as succession, security rights, and good faith acquisition. Participants noted that while national approaches may differ, the creation of a harmonized functional definition of control, even if implemented through soft law, would help reduce legal ambiguity, facilitate cross-border recognition, and support MiCAR's effective implementation.

Calls to Action regarding the "Control" Concept
The key calls to action from the discussion are: • Develop model provisions or interpretative guidance to support the functional recognition of control in civil law jurisdictions, aligned with the UNIDROIT Principles on Digital Assets and Private Law. • Encourage academic and legislative working groups to evaluate whether control should be incorporated as a standalone legal category or treated analogously to possession. • Facilitate comparative law research to document how control is being implemented or interpreted across jurisdictions and identify best practices for convergence. • Establish legal presumptions or safe harbors for good faith acquirers relying on blockchain-based indicators of control, especially in the absence of centralized registries, consistently with the UNIDROIT Principles on Digital Assets and Private Law.

3. Applying the DAPL Principles to Financial Instruments

The third topic, presented by Tecla Rodi, Policy and Regulatory Advisor at Italy's Ministero dell'E conomia e delle F inanze, focused on how the UNIDROIT Principles on Digital Assets and Private Law can inform the treatment of financial instruments issued and transferred via DLT.

Using Italy's Fintech Decree as a case study, participants explored how DLT-based securities could leverage existing book-entry frameworks while adapting key concepts like bona fide acquisition to a decentralized environment.

The Italian approach illustrates how national legal systems can integrate native digital financial instruments into their private law using a combination of traditional rules and digital-specific adaptations. For example, while book-entry and DLT-based securities share many functional similarities, novel issues arise since digital assets are accessed and disposed of through means such as cryptographic keys. The Italian model adopts the concept of "control" from the UNIDROIT Principles on Digital Assets and Private Law over the means of access to the financial instruments, that pertains specifically to the digital world, while mirroring traditional book-entry securities rules for the creation of liens and pledges,

suggesting that hybrid approaches combining traditional and new digital-specific rules may be viable.

Participants noted that one of the innovations of the Italian Decree is the identification of a "manager of the distributed ledger" (*responsabile del registro*) with specific duties related to the integrity of the ledger and the enforceability of security rights. This figure helps ensure that the private law effects recognized in Italian law can be generated, serving as a legal and technical bridge between DLT systems and traditional securities frameworks.

Discussions also covered how the concept of "control" under the UNIDROIT Principles on Digital Assets and Private Law was used to define not only transferability but also enforceability of rights in rem, including the ability to create pledges over digital financial instruments. Participants considered the interplay between such innovations and MiFID II obligations, noting the need to clarify supervisory roles and ensure consistency with EU financial regulation.

The roundtable surfaced open questions about ledger-based registration systems, competing claims, and cross-border recognition of digital securities. For example, what happens when two different jurisdictions recognize two different ledgers as "official" for the same financial instrument? How can claims be prioritized in insolvency or enforcement scenarios involving both on-chain and off-chain claims? Participants agreed that further clarity is needed on how digital control and legal title interact, especially when digital ledgers function as de facto registries of entitlement.

There was also consensus that the UNIDROIT Principles on Digital Assets and Private Law offer a flexible but coherent foundation to address these challenges. Several speakers noted that the P rinciples, by addressing control, good faith acquisition, and third-party effectiveness, could support convergence even in jurisdictions with very different legal traditions. Italy's experience was presented as a promising model for gradual adoption and adaptation of the UNIDROIT Principles on Digital Assets and Private Law in financial markets.

Additionally, the group debated whether DLT-based financial instruments require a rethinking of settlement and clearing models under securities law, particularly when the ledger itself functions as the registrar. Participants emphasized the need for interoperability between DLT registries and central securities depositories (CSDs), and for mechanisms that allow courts and insolvency practitioners to reliably assess ownership and enforceability.

Calls to Action regarding Digital Financial Instruments and DLT
The key calls to action from the discussion are: • Promote the adoption of the UNIDROIT Principles on Digital Assets and Private Law in national financial legislation, especially in areas involving acquisition of digital assets and collateral. • Encourage Member States to expand existing book-entry frameworks to accommodate DLT-based securities without full legal overhaul. • Develop legal guidance on the interaction between on-chain digital registries and off-chain enforcement tools, including in cases of insolvency or default. • Clarify the legal responsibilities and functions of distributed ledger managers or registrars under national law, particularly in relation to evidence of title and compliance with MiFID II.

We thank all participants of the Rome DARTE event for contributing to the discussion:

Alessandro Malventano (European Decentralisation Institute), Alexandru Stanescu (Lexters), Andrea Sacchi, Angelo Maria Galiano (Consob), Antonios Papadimitropoulos (National and Kapodistrian University of Athens, PnP and Associates Law Firm), Antonio Lanotte (Futura Law), Åsa Dahlborn (BlackVogel), Chiara Villani (Lener & Partners), Eesa Fredericks (University of Johannesburg), Eya Abid, Farangis Khasanova (University of World Economy and Diplomacy), Fatima Zahra Zaroui, Francesco Desantis Spasiano (Vision Studio), Georg Harer (Bybit), Giulia Previti (UNIDROIT), Heinz Konzett (Office for Digital Innovation), Ignacio Tirado (UNIDROIT), Irene Tagliamonte (Consob), Joachim Schwerin (European Commission), Klim Omelchenko (International University of Kyrgyzstan), Komil Rashidov (Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan), Kristijan Poljanec (University of Zagreb), Luca Lamanna (Sapienza Università di Roma), Luigi Cantisani (Futura Law), Maria Broulia (JCW), Mariana de la Roche (BlackVogel), Mariolina Colomba (Treezor), Megumi Hara, Natalia Alenkina (Ala Too International University), Nina-Luisa Siedler (siedler legal), Nisrin S. A. Mahasneh (Qatar University), Paolo Gangi (Studio legale Gangi), Rosanna Salonen (UNIDROIT), Rosa Giovanna Barresi (Università degli Studi di Firenze), Salvatore Furnari (Lener & Partners), Satoru (Tomo) Yamadera (Saitama

University Graduate School of Economics and Management), Tecla Rodi (Italian Ministry of Economy and Finance), Teresa Rodriguez de las Heras Ballell (ELI, Universidad Carlos III, delegate of Spain to UNCITRAL), Theodora Kostoula (UNIDROIT), Timur Davlatov (Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan), and Veni Arakelian (Greek Ministry of Finance).