



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) 