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).