DARTE SERIES

Digital Assets Round Table Experts Series

DARTE SERIES

Consolidated Thematic Analysis

Topics, Problems and Solutions Across the Roundtable Series

Session 1 to 31:
London (March 2024) – Berlin 6.0 (June 2026)

BlackVogel

siedler legal

DAAvern

DARTE SERIES

Digital Assets Round Table Experts Series

In collaboration with the partners and sponsors of the series

3Folio
ADVANTAGE AUSTRIA WKO
AML INCUBATOR
apco
ASENSI ABOGADOS
BERLIN Senatsverwaltung für Kultur und Gesellschaftlichen Zusammenhalt
BERLIN PARTNER für Wirtschaft und Technologie
BINANCE
bitpanda
bitvavo
BNY
BLOCKCHAIN BUNDESVERBAND
BLOCKCHAIN FOR EUROPE
BLOCKCHAIN IRELAND
BLOCKCHAIN FOR GOOD ALLIANCE
LISBOA CÂMARA MUNICIPAL
BLX BIBLIOTECAS DE LISBOA
bpifrance SERVING THE FUTURE
Bocconi Università Commerciale Luigi Bocconi
Bundesblock
BYBIT EU
CARDANO FOUNDATION
TRUSTLESS TECHNOLOGIES ASSOCIATION
CEU CENTRAL EUROPEAN UNIVERSITY
Crystal
CRYPTO FINANCE DEUTSCHE BÖRSE GROUP
CRYPTO RISK METRICS
CV LABS
DLT Finance
DLT GERMANY CONNECT · CREATE · COLLABORATE
European Commission
EUROPEAN BLOCKCHAIN ASSOCIATION
EUBlockchain Observatory and Forum
EMBASSY OF ESTONIA STOCKHOLM
FINTECH GERMANY AWARD
FinPlanet
wirtschaftsagentur wien Für die Stadt Wien
fio
Firi
Frankfurt School of Finance & Management German Excellence. Global Relevance.
GBA
itaú
1inch NETWORK
Linklaters
MERGE
MiCA Crypto Alliance
N26
NÄGELE
NOTA BENE
NORDIC BLOCKCHAIN ASSOCIATION
NORDIC LAW
Project Catalyst
OFFICE FOR FINANCIAL MARKET INNOVATION AND DIGITALISATION PRINCIPALITY OF LIECHTENSTEIN
SPIELFELD
STADLER VÖLKEL RECHTSANWÄLTE · ATTORNEYS AT LAW
sumsub
taxbit
Tezos
TOKEN RECOVERY
trilitech
Trinity Executive Education Trinity Business School
TRM
UNIDROIT
UNIVERSITY of NICOSIA
UNIVERSITÄT LIECHTENSTEIN
VerifyVASP
VIENNA BLOCKCHAIN WEEK
VBANK
web3 foundation
WKO BILDUNGS-KickOff Die Finanzdienstleister
ZUMO

DARTE SERIES

Digital Assets Round Table Experts Series

Table of Contents

1. Introduction and Methodology

The Digital Assets Round Table Expert Series (DARTE), initiated by Mariana de la Roche (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), kicked off in March 2024 as expert platform to increase legal certainty around the Markets in Crypto-Assets Regulation (MiCAR). More than two years later, the series has expanded its scope beyond Europe to encompass the global Anti-Money Laundering framework established by the FATF Recommendations including travel rule, the Digital Operational Resilience Act (DORA), the payment services framework (PSD2/PSD3/PSR and their interplay with the USA and LatAm), tax reporting regimes (DAC8/CARF), data protection, privacy rights and digital identity, private law, and region-specific regulatory questions. Each session has produced a public report containing the discussions held and concrete calls to action.

1.1 Working principles

The roundtables are conducted under a consistent set of working principles, and these principles also shape how the present analysis records their outputs.

First, sessions take place under the Chatham House Rule as applied by the series: participation in a session and the substance of what was discussed may be reported, but statements are not attributed to individual participants. Accordingly, this analysis attributes positions to sessions, never to named individuals, except where a specific, publicly credited output – a published taxonomy, an interpretive note, a named platform – is identified by its author because it exists in the public domain.

Second, the sessions work within the existing regulatory framework: rather than requesting legislative change, they seek workable solutions under the law as it stands. Two sessions departed from this principle, in each case deliberately: Berlin 6.0 (15 June 2026), expressly convened to undertake a critical analysis of the FATF Recommendations themselves and to propose concrete amendments to them, and Munich (September 2025), where the discussion concluded that no solution exists within the existing framework and that a new legal instrument is required.

Third – and most consequentially for how the calls to action in this document are written – the series never aimed to ask regulators for guidance in the abstract but rather to share the industry's guidance with public authorities. Where the sessions identified a need for regulatory clarification, they also proposed what that clarification should focus on. Such calls to action set out below are framed not as requests that a term be defined or a boundary be clarified, but they rather propose a specific clarification of the definition, test or safeguard.

A much welcomed feature of the DARTE series is the triggering of additional instruments by some participants who had been particularly interested in certain topics. On several themes, a problem identified in one session was followed up on by a concrete output that participating

experts produced in addition to the usual DARTE report – a taxonomy, a disclosure platform, an interpretive note. Where this occurred, this analysis highlights it in a dedicated section within the relevant chapter.

1.2 Scope and sources

The analysis covers thirty-one sessions held between March 2024 and June 2026. It is based on the full published report of each edition.

Two sessions followed a format different from the standard editions: London 2.0 (February 2025), a closed forum convening legislators and government officials from multiple jurisdictions together with private-sector representatives to discuss the responsible adoption of blockchain, digital assets and AI, whose report is not public and which is accordingly excluded from the thematic mapping of this analysis; and the Buenos Aires Special Edition (March 2025), a cross-jurisdiction, cross-industry discussion structured around jurisdiction overviews and main takeaways rather than the problem/solution format which is included and treated descriptively.

This consolidated analysis does not summarise the individual reports in sequence. It reads the series transversally: for each recurring theme it reconstructs how the conversation developed and how each session's contribution built on or complemented the last, and what concrete solutions and calls to action emerged. Where a topic was examined from different angles in different cities, those angles are set out as a developing argument rather than a list, so that the cumulative character of the DARTE series' work becomes visible.

1.3 Structure

Chapters 2 to 16 cover the following recurring thematic clusters: the asset and its disclosure regimes (Chapters 2 to 5), money and payments (Chapters 6 and 7), the regulatory perimeter and the compliance stack (Chapters 8 to 12), and institutions, legal foundations and the international dimension (Chapters 13 to 16). The chapters set out the underlying problem, how the conversation developed across the relevant sessions, sometimes the theme's interaction with the rest of the analysis is added, and the solutions and calls to action proposed – with, where applicable, a dedicated passage recording an instrument the community built in response. Chapter 17 draws the cross-cutting findings, and the Annex provides a DARTE session index.

1.4 Thematic overview

Theme (chapter)	The problem in brief	Sessions
Token classification and taxonomy (Ch. 2)	No harmonised classification criteria between MiCAR and MiFID II, or within MiCAR's categories, generating liability exposure, arbitrage and divergence.	Berlin; Buenos Aires; Milan; Vienna 2.0; Madrid 2.0; Paris 2.0
Whitepaper and disclosure obligations (Ch. 3)	Scope, exemptions, liability allocation and procedures raise questions where the issuer is absent, foreign or decentralised.	Vienna; Brussels; Lisbon; Milan
Sustainability disclosures (Ch. 4)	A Day-1 obligation imposed before implementation guidance existed.	London; Dublin; Oslo; Lisbon
Market abuse and market integrity (Ch. 5)	Title VI imports MAR concepts into continuous, fragmented, pseudonymous markets where information lives on-chain and disclosure is informal.	Vienna; Berlin 2.0; Milan; Vienna 2.0; Madrid 2.0; Stockholm
Stablecoins and e-money tokens (Ch. 6)	EMT classification; systemic-risk and reporting duties; permissibility of multi-jurisdictional issuance; reserve and concentration rules.	London; Madrid; Buenos Aires; Helsinki; São Paulo; Paris 2.0
The MiCA–PSD dual-licensing question (Ch. 7)	The dual qualification of EMTs exposes CASPs to double authorisation under MiCAR and PSD2/PSD3/PSR.	Oslo; Helsinki; São Paulo; Paris 2.0
DeFi and the regulatory perimeter (Ch. 8)	MiCAR excludes fully decentralised services without defining decentralisation; surrounding frameworks assume identifiable intermediaries.	Berlin; Vienna; Berlin 2.0; Brussels 2.0; Berlin 3.0; Berlin 4.0; Washington
Self-hosted wallets (Ch. 9)	Their TFR, MiCAR and AML treatment determines whether non-intermediated use of the technology remains practicable in the EU.	Madrid; Berlin 4.0; Paris 2.0; Stockholm
The Travel Rule and AML compliance (Ch. 10)	The duty to exchange originator/beneficiary data collides with non-interoperable infrastructure, divergent standards, self-hosted wallets and privacy.	Madrid; Frankfurt; Dublin; Paris; Madrid 2.0; Berlin 5.0; São Paulo; Stockholm; Berlin 6.0

Privacy, data protection and digital identity (Ch. 11)	Transparency duties confront fundamental rights; GDPR's centralised assumptions meet decentralised infrastructure.	Berlin; Madrid; Berlin 3.0; Berlin 5.0
Tax reporting and accounting infrastructure (Ch. 12)	As DAC8 approaches, the question shifts from legal interpretation to whether reportable data can be generated and classified at all.	Madrid; Vienna 3.0
Supervisory convergence and proportionality (Ch. 13)	A single passport is only as strong as the consistency of supervision behind it; proportionality burdens smaller actors.	Berlin; Vienna; Brussels; Berlin 2.0; Zug; Vaduz; Oslo; Lisbon; Brussels 2.0; Paris; Vienna 2.0; Madrid 2.0; Vienna 3.0
Private law and tokenised capital markets (Ch. 14)	Private law determines what the asset is, who owns it and how rights are enforced – and remains fragmented across jurisdictions.	Munich; Rome
Reverse solicitation and third-country access (Ch. 15)	The solicitation / client-initiated boundary under Article 61(3) is unclear, leaving third-country actors without a workable perimeter.	London; Berlin; Vienna; Brussels; Berlin 2.0; Zug; Oslo; São Paulo
Regional and global cooperation (Ch. 16)	How jurisdictions with different philosophies interoperate, through recognition and equivalence rather than harmonisation alone.	Buenos Aires; Paris; Washington; São Paulo

2. Token Classification and Taxonomy

2.1 The problem

Every obligation in MiCAR hangs on a prior question: what type of asset is concerned. The series encountered this question before MiCAR even applied and never fully escaped it – because existing EU regulation does not fully answer it. There is no truly precise EU definition of "financial instrument". "Utility token", "offer to the public" and "admission to trading" are vague in key details; and whole categories of assets – memecoins, NFTs issued in series, liquid staking tokens, legacy tokens with no issuer left to ask – fit awkwardly into a taxonomy built around identifiable issuers making deliberate offers.

2.2 How the conversation developed

The discussion opened in Berlin (April 2024) at what then seemed the exotic end of the spectrum: NFTs. But the session's real contribution was methodological. Confronted with the question of

when a "non-fungible" token is in substance fungible – and therefore inside MiCAR – the roundtable refused a mechanical answer. It rejected the importation of a Howey-style test, insisted that assessment look beyond mere negotiability to whitepaper intentions and issuer promises, and produced four criteria to be weighed together: artistic uniqueness; the nature of the utility, with non-financial utilities such as DAO voting rights or exclusive content pointing away from financial-instrument status; market dynamics and trading volume over significant periods; and issuance and seriality – with the express caution that the "large series" indication of fungibility is one factor among several, not a verdict. That insistence on substance over form, weighed multi-factorially and developed in dialogue with supervisors, became the series' settled method for every classification question that followed. Berlin also named the stakes: if the same asset can be a security under MiFID in some but not all EU Member States and therefore a utility token under MiCAR (which does not apply to MiFID instruments) in only some but not all Member States, the EU-wide passporting concept is broken at its foundation – a warning that resurfaces in the supervisory-convergence discussion (Chapter 13) and ultimately in the recognition agenda (Chapter 16).

Buenos Aires (March 2025) widened the lens and confirmed that the problem is not a European idiosyncrasy. Across Latin America, securities definitions broadly track the US Howey test or adaptations of the investment-contract concept – yet jurisdictions diverge on the question that matters most in practice: offshore offerings. Some assert authority by reference to the targeted population and others lack reach absent local targeting, with criminal liability for undisclosed securities offerings in certain jurisdictions raising the cost of getting the answer wrong.

Milan (May 2025) brought the question home to the assets dominating retail flows. For memecoins, the undefined perimeter of "offer to the public" and "utility token" leaves platforms unable to determine when whitepaper obligations apply at all – and because publishing a whitepaper for a token with no cooperative issuer means assuming Article 15 liability (a burden Chapter 3 examines in full), the classification gap converts directly into liability exposure. Milan's answer was deliberately conservative: absent an explicit exemption, treat such assets as falling within the Title II perimeter.

The conversation reached its most consequential stage in Vienna 2.0 (September 2025), with liquid staking tokens. Here the taxonomy does not merely blur; it fails. An LST typically has no identifiable issuer, no redemption mechanism and no centralised governance – so it fits neither the ART category, nor the MiFID II/AIFMD frameworks, which presuppose centralised portfolio management. Some NCAs suggested that merely enabling a return could push such assets into alternative-investment-fund territory, an interpretation with drastic consequences for products already widely distributed. The session catalogued what the vacuum costs in practice: retroactive reclassification risk borne entirely by CASPs, because there is no issuer to share it; regulator response times running to months; legacy tokens launched a decade ago, without whitepapers, that no transitional rule addresses; and defensive market practice – voluntary whitepaper

publication paired with liability insurance. Italy's practice of substantively reviewing whitepapers rather than acknowledging receipt captured the dilemma in miniature: clarity for those who file there, fragmentation and forum shopping for the single market.

Paris 2.0 (April 2026) discussions reframed the whole thread programmatically: taxonomy is not a technical afterthought but a core regulatory risk driver, because MiCA and MiFID II operate as parallel frameworks with distinct scopes – and fragmentation arises precisely when markets or supervisors apply informal sequencing that diverges from that legal design.

2.3 Interactions with other themes

Classification is the load-bearing wall of the rest of the analysis. It determines whether a whitepaper is owed and who bears Article 15 liability (Chapter 3); which market-integrity regime applies, with the MiCAR–MAR boundary shifting the moment an asset underlies a derivative (Chapter 5); whether an EMT's dual character drags a CASP into payments law (Chapter 7); whether a protocol's token places it inside or outside the MiCAR perimeter at all (Chapter 8); and what the asset is as a matter of property law (Chapter 14). The passporting-consistency warning first sounded in Berlin recurs as the central fragmentation diagnosis of supervisory convergence in Chapter 13 and as the case for recognition-based approaches in Chapter 16.

2.4 Solutions and calls to action

The sessions' recurring proposal is a substance-based classification standard, as indicated in the ESMA RTS, under which an asset is assessed not by its label or bare negotiability but by a weighted set of indicators the sessions specified for each hard case:

- For assets marketed as NFTs, the four-factor test developed in Berlin – "artistic" uniqueness, the non-financial or financial character of the utility, market and trading dynamics over time, and issuance and seriality – applied together, with seriality treated as indicative rather than decisive, so that a genuinely unique collectible is not swept into Title II while a serialised financial instrument dressed as an NFT is.
- For memecoins and comparable Title II assets, the proposed default rule is that they fall within the Title II perimeter unless a specific exemption applies, paired with the disclosure allocation described in Chapter 3 so that the default does not simply transfer open-ended liability to listing platforms.
- For liquid staking tokens, a dedicated substance-based sub-taxonomy keyed to objective indicators of decentralisation, economic design and technical risk (see the Community in Action passage below), which is aimed to be validated through the ESMA Q&A so that a favourable classification hopefully carries supervisory weight rather than remaining a private legal opinion in the future.

The sessions further proposed that NCAs align their treatment of borderline cases through the same Q&A channel, precisely to prevent the divergent exemption practices – exemplified by Italy's substantive whitepaper review – that drive forum shopping.

COMMUNITY IN ACTION — The MiCA Crypto Alliance token-classification taxonomy

The clearest instance in the series of a call to action producing a built instrument concerns liquid staking tokens. The classification gap identified at Vienna 2.0 (September 2025) was taken up directly: at Madrid 2.0 (October 2025) the MiCA Crypto Alliance announced a working group on crypto-asset legal classification, and by Paris 2.0 (April 2026) the work existed as a published EU legal taxonomy of liquid staking tokens, built on objective indicators of decentralisation, economic design and technical risk.

The taxonomy does more than label assets. It maps each LST against the predicate conditions of three parallel regimes — MiCA, MiFID II and AIFMD — using observable design variables: who controls minting, how yield is generated and distributed, how redemption is governed, and whether any single entity can unilaterally alter outcomes. From these inputs it produces a deterministic classification: most decentralised LSTs fall within MiCA's "other crypto-assets" perimeter, while custodial structures with identifiable issuers and enforceable redemption obligations carry materially higher MiFID II and AIFMD sensitivity. The framework is jurisdiction-neutral and auditable, the same asset description should produce the same classification regardless of who applies it, which is precisely what the current regulatory text does not yet supply.

This is a genuine community output, and it is featured here as such. It is not, however, the whole answer to the classification problem. It addresses one hard case – LSTs – and its supervisory effect depends on validation through the ESMA Q&A mechanism; the wider questions of memecoin perimeter, NFT seriality, MiCAR/MiFID boundary consistency and legacy assets remain open and are the subject of the calls to action above.

For more information on the initiative: https://www.micacryptoalliance.com/reports/legal-classification-of-liquid-staking-tokens-lsts-in-the-eu

3. Whitepaper and Disclosure Obligations

3.1 The problem

Once an asset's classification is settled, the next question is what the market must be told about it. MiCAR replaced prospectus rules with a "lighter" whitepaper instrument – but its scope, exemptions, liability allocation and procedures generate acute questions wherever the issuer is absent, foreign or decentralised, which in crypto is often the place.

3.2 How the conversation developed

DARTE Vienna (May 2024) began with the exemptions. Where a whitepaper is not required under Title II – offers to fewer than 150 persons per Member State, or below €1 million over twelve months – a CASP's client nonetheless needs adequate risk information under Article 66 (3) MiCAR, and the parameters for relying on a third party's whitepaper were simply undefined. The session also flagged a subtle fragmentation source that recurs later: MiCAR's own language versions diverge, so "the same" obligation reads differently across Member States.

The first DARTE Brussels (July 2024) sharpened the liability question and exposed a structural tension. On one hand, the market needs someone to stand behind disclosure for decentralised and issuerless assets; on the other, MiCAR fixes liability strictly on the whitepaper's author and does not let it transfer to those who merely rely on the document – which casts doubt on whether a commercial third-party drafting market can exist at all. The session also identified the timeline mismatch – environmental disclosures required earlier than the full whitepaper mandate, with assets listed before 30 December 2024 grandfathered to 2027 – a thread that becomes central in Chapter 4.

DARTE Lisbon (February 2025) turned to Layer-1 projects and airdrops, where the issuer is typically non-EU and, under Article 3 (33) (c) MiCAR, chooses its home Member State. The session treated jurisdiction selection openly as the strategic decision it has become – weighing experienced but slower regulatory processes in Germany, the Netherlands and France against streamlined approaches elsewhere, the reputational pull of Western Europe, the value of local presence, and the specific hazard of choosing a Member State that has not yet designated its NCA – and worked through the management of material changes arising during the twenty-day review window.

DARTE Milan (May 2025) confronted the hardest version: third-party drafting for tokens with no cooperative issuer. Here a platform that submits a whitepaper assumes Article 15 liability that extends to its management body and survives delisting, with claims considered more likely to succeed in Germany or France than in Italy. The session recorded the appearance of "rogue" whitepapers uploaded by persons unconnected to a project, noted that Article 6 lets "other persons" draft without defining who they are or whether Article 15 reaches them, and observed that AI-assisted drafting removes none of the human liability.

3.3 Solutions and calls to action

The sessions proposed a concrete disclosure architecture rather than a request for clarity:

- A defined liability rule for third-party and "other person" drafters: ESMA to confirm through a Q&A that Article 15 MiCAR liability attaches to a third-party drafter only where it has assumed the issuer's disclosure role, and does not attach to a person whose whitepaper is

reused without the written consent Article 4 (7) MiCAR requires – resolving both the "rogue whitepaper" problem and the free-rider problem in one stroke.

- A single EU digital submission portal for whitepaper notifications, with automatic distribution to all NCAs and a shared notification database, replacing parallel national filings and the duplication they create; and, for non-EU submissions, an explicit procedure for handling material changes during the twenty-day review period.
- Entity-level disclosure for infrastructure operators, excluding individual operator details, so that the disclosure obligation is discharged by the actor that actually exists.
- An industry-run whitepaper benchmarking and quality-validation tool.

4. Sustainability Disclosures

4.1 The problem

The whitepaper is not the only disclosure MiCAR attaches to an asset. Sustainability disclosures form a second, parallel regime – and, unlike the whitepaper, they applied from day one, before any implementation guidance existed. Four sessions traced the consequences from first principle to template detail.

4.2 How the conversation developed

DARTE London (March 2024) framed the question at the level of principle: how MiCAR's sustainability reporting should integrate with the CSRD, SFDR and ESRS E1, and whether it should capture positive sustainability metrics rather than adverse impacts alone. The session worked through the allocation problem that dominates the rest of the thread – the consensus that a CASP can meaningfully report only on metrics it directly influences, the impracticality of a CASP reporting on an entire public chain, and the case for cooperative metrics spanning issuers and Layer 1 / Layer 2 networks – and confronted the tension between reporting flexibility and greenwashing, which it proposed to resolve through standardised quantitative positive metrics accompanied by voluntary qualitative ones.

DARTE Dublin (November 2024) moved from principle to the pain of Day-1 compliance, sharpened by a transitional asymmetry the series returns to repeatedly: sustainability disclosures applied immediately, while whitepaper obligations for non-ART/EMT assets enjoy a grace period to 2027. It surfaced the template's ambiguities – undefined "best efforts" methodological standards, and unclear treatment of multichain tokens, layer-2 architectures and wrapped or bridged assets – and proposed defining "material changes" by quantifiable percentage deviations from baseline.

DARTE Oslo (January 2025) confronted the guidance vacuum directly, and added three structural observations that reframed the problem: jurisdictions with shorter grandfathering periods impose a first-mover disadvantage on their own CASPs; the sustainability rules, introduced late as a response to proof-of-work energy concerns, sit apart from dedicated frameworks such as the CSRD and ISSB; and CASPs must disclose data that the issuers of the very assets they service are not yet required to publish – with ESMA indicating it did not plan further guidance. The session's response was to propose that the industry build the missing guidance itself.

DARTE Lisbon (February 2025) resolved two concrete template questions. It read the requirement of "prominent" placement flexibly enough to cover mobile applications, where the app is the primary interface, with downloadable files for both initial disclosures and material updates; and it addressed the problem of a single asset carrying multiple Digital Token Identifiers across chains – illustrated by a token with more than ten distinct DTIs – through the Functionally Fungible Group methodology developed by the DTI Foundation to consolidate economically identical assets into one disclosure.

4.3 Solutions and calls to action

- A supplementary ESMA guideline on the application of Commission Delegated Regulation (EU) 2025/422 (the sustainability-indicators RTS, now in force), whose content the sessions specified: entity-based disclosures alongside asset-based ones with de-minimis thresholds; a defined methodology replacing "best efforts"; explicit treatment of multichain, layer-2, wrapped and bridged assets; and "material change" defined as a quantified percentage deviation from baseline.
- Standardised quantitative positive metrics alongside the mandated adverse-impact metrics, aligned with the CSRD and SFDR, with voluntary qualitative reporting – the specific mechanism the sessions proposed for reconciling comparability with greenwashing risk.
- A flexible but explicit interpretation of "prominent place" extending to mobile applications, with standardised downloadable disclosure files as the compliance artefact.
- Adoption of the Functionally Fungible Group methodology so that economically identical assets carrying multiple DTIs generate a single, consolidated disclosure.
- Coordinated ESMA–NCA enforcement to prevent regulatory arbitrage in the application of the sustainability disclosure rules, and, as the industry-side response to the persisting guidance vacuum, a shared, non-binding compliance toolkit compiling interpretations, best practices and worked examples.

5. Market Abuse and Market Integrity

5.1 The problem

Disclosure duties shade into conduct rules: where the preceding chapters asked what must be published, Title VI asks what may be traded on before it is published. MiCAR imports Market Abuse Regulation concepts into an environment that differs structurally from traditional finance – trading is continuous, venues are fragmented, participants are pseudonymous, much relevant information lives on-chain, and disclosure channels are informal. The series tracked this theme from the first compliance questions to its newest frontiers.

5.2 How the conversation developed

DARTE Vienna (May 2024) and Berlin 2.0 (August 2024) scoped the terrain: the broad reach of the MAR-inspired provisions, the undefined class of relevant market participants, the meaning of "admission to trading", inside-information disclosure in a DeFi context, and the specific need for CASP controls against price manipulation through automated market makers.

DARTE Milan (May 2025) operationalised insider dealing and revealed how ill-fitting the transplant is. Title VI binds all persons professionally arranging or executing transactions from 30 December 2024, with no grandfathering – yet neither MiCAR nor the technical standards define that personal scope or what "sufficient controls" means. Against a market of millions of assets trading at different prices across hundreds of venues, with cross-chain manipulation, oracle exploits and most trading occurring off-chain on opaque platforms, the session built a graduated compliance ladder: from policies, training and NDAs, through wallet-address declarations, integrated on- and off-chain surveillance, insider lists, pre-clearance and information barriers, to voluntary monthly trade reporting from other venues.

DARTE Vienna 2.0 (September 2025) opened two further fronts. First, disclosure: crypto communication channels – X, Telegram, Discord – are inadequate for the Article 88 duty to disclose inside information "without delay", and an issuer who learns that material information has leaked through unofficial channels must republish it officially without delay. Second, overlap: where the same asset trades in spot and derivative form, MiCAR and MAR apply in parallel with differing definitions of inside information, raising ne bis in idem concerns – compounded because MiCAR's lighter regime, designed with an SME-heavy market in mind, coexists with MAR's full obligations.

DARTE Madrid 2.0 (October 2025) pressed on the operational-standards gap – wallet declarations, insider lists, and whether smart-contract vulnerabilities, DAO governance proposals and protocol upgrades are inside information when disclosed on-chain but not widely understood – and confirmed again an important boundary: MiCAR deliberately implements MAR in lighter form, but once a crypto-asset becomes the underlying of a financial instrument such as a derivative or ETN, the full MAR regime reapplies.

DARTE Stockholm (May 2026) reached the conceptual frontier. When is blockchain data that is technically public but realistically interpretable only by sophisticated actors – through wallet clustering, mempool visibility, treasury tracking, validator-level sight – "inside information" under Article 87 MiCAR? The session recorded a strong strand of opinion that on-chain data is intrinsically public, supported by a traditional-market precedent in which trading ahead of media reporting of a publicly delivered court ruling was not insider dealing, and noted that most real cases combine on-chain analytics with off-chain leaks. It then turned to prediction markets, prompted by reported insider-style activity on a major platform: a position may qualify as a MiFID II derivative while also satisfying MiCAR's crypto-asset definition, pushing the asset into the stronger MiFID II regime until that uncertainty is resolved With national wagering law adding a third perimeter, the discussion concluded that under any classification the substantive market-abuse vocabulary may fail to capture the economic harm.

5.3 Solutions and calls to action

The sessions proposed the substance of the missing standards, not merely their creation:

- A defined personal scope for "persons professionally arranging or executing transactions" and a defined content for "sufficient controls", expressed as the graduated ladder Milan set out – so that an ESMA Q&A or guideline can adopt a concrete, proportionate compliance standard rather than leaving the terms open.
- A "reasonably accessible information" test for on-chain data: information is public, and not inside information, unless deriving it requires professional analytical capacity that is not reasonably accessible – the test Stockholm proposed to resolve the Article 87 MiCAR frontier, with a default that on-chain data is public.
- Treatment of MiCAR/MAR overlapping conduct on a single asset as one offence rather than two, to give effect to ne bis in idem, together with a proportionate SME-calibrated regime reflecting Recital 95 of MiCAR.
- Classification of prediction-market positions by economic substance rather than platform label, and a conduct-based supervisory approach to event-linked markets that targets identifiable abusive patterns regardless of which of the three possible classifications applies.
- On the industry side, a crypto-specific market-integrity taskforce to maintain shared wallet-declaration protocols, simplified insider lists, tiered information barriers and risk-based surveillance integrating on-chain analytics with off-chain data.

COMMUNITY IN ACTION — DAAvern – a disclosure platform for the Article 88 MiCAR problem

DAAvern is a concrete response of the DARTE co-organisers to the disclosure gap set out above. While it cannot replace a firm's existing disclosure obligations, it sits after the disclosure act and provides an evidentiary layer: once information has been made public, DAAvern produces a cryptographically timestamped, multi-blockchain-anchored record of the content and the moment it became available, together with a structured, searchable public archive of disclosures across issuers, CASPs and crypto-assets.

The result is defensible proof of when information entered the public domain, which is precisely the element that informal channels such as X, Telegram and Discord cannot supply on their own, and precisely the element that emerging national requirements are beginning to demand. Germany's KMMV (a regulation specifying disclosure obligations under MiCAR), for example, requires the full text of a disclosure, the exact time, the specific channels used and a named contact, an audit-trail standard that maps directly onto the kind of evidence DAAvern is designed to preserve.

At the time of this analysis, DAAvern is an early working version in a collaborative pilot phase, developed with input from the roundtable community rather than presented as a finished product.

More information: https://daavern.com/

6. Stablecoins and E-Money Tokens

6.1 The problem

Stablecoins are the asset class on which MiCAR's most prescriptive rules converge. Stablecoins, and EMTs in particular, run through the DARTE series from the first session to the most recent, and the problem shifted as MiCAR matured: first how EMTs fit the e-money and payments acquis, then how systemic-risk and reporting obligations would work, then whether MiCAR permits issuing the same token from several jurisdictions, and finally how reserve and concentration rules interact with redemption reality.

6.2 How the conversation developed

DARTE London (March 2024) began with a doctrinal critique of Article 48 (2) MiCAR's equation of EMTs with electronic money, which overlooks that EMTs may be issued by a broader range of entities, enable permissionless rather than permissioned transfers, and function simultaneously as payment instruments and media of exchange – the mismatch that later becomes the dual-licensing problem of Chapter 7 below.

DARTE Madrid (October 2024) addressed systemic risk for significant EMTs against a market then dominated by a few very large issuers, focusing on the heightened capital, liquidity and dual-supervision regime and the reporting burden it imposes. DARTE Buenos Aires (March 2025) added the regional dimension that reframes the asset class: in inflation-affected economies, stablecoins are not a faster rail but an accessible one, with clear potential for remittances and financial inclusion.

DARTE Helsinki (November 2025), a dedicated stablecoin edition, produced the series' most consequential stablecoin work. It established from the text – Recital 54 MiCAR and Articles 38 and 54 to 56 MiCAR – that MiCAR anticipates multi-jurisdictional issuance, requiring reserves corresponding to EU liabilities to be held under EU law, and characterised the resistance to such structures as political rather than grounded in the Regulation, producing a chilling effect in which some NCAs decline to authorise what others process. It examined the "mixing of baskets" problem in redemption stress, burn-and-mint bridging as a route to jurisdictionally clean issuance, and the reserve-concentration question – recording open divergence between the Commission's intention (notified 28 August 2025) to endorse the reserve-composition standards with amendments and the EBA's formal pushback in Opinions EBA/Op/2025/13 and EBA/Op/2025/14 of 10 October 2025, a conflict still unresolved at the time of writing this report (July 2026).

DARTE São Paulo (March 2026) mapped Latin America's fragmentation jurisdiction by jurisdiction – Brazil's developed reserve-and-reporting framework, Chile supervising platforms without addressing issuance, Argentina limited to AML/KYC, Mexico barring financial institutions from public crypto services, Colombia operating only a sandbox – and drew on the FSB's October 2025 thematic review for the resulting race-to-the-bottom dynamic, with the US GENIUS Act's equivalence mechanism adding commercial pressure.

DARTE Paris 2.0 (April 2026) took the legal permissibility of multi-jurisdictional issuance as settled and moved to operational design: it challenged the assumption that faster settlement is the primary use case, framing stablecoins in emerging economies as a substitute for inaccessible rails; identified the structural mismatch between 1:1 reserve rules premised on simultaneous full redemption and the behaviour of holders who never redeem; described the EU's single-bank deposit caps as an international outlier; and left the commercial-versus-central-bank-money question expressly open.

6.3 Solutions and calls to action

- A calibrated, risk-sensitive completion of the reserve-composition standards: the stress-testing machinery now exists at Level 2, Commission Delegated Regulation (EU) 2025/1264 on liquidity management policies and procedures, in force since 23 October 2025, together with the EBA guidelines on liquidity stress testing, and the open question is the contested composition/HLFI layer, where the sessions proposed liquidity stress testing as the central

adequacy criterion, calibrated to each issuer's redemption profile, with proportionate concentration thresholds replacing fixed composition ratios and single-bank deposit caps.

- Shared operational standards for multi-issuance – reserves corresponding to each issuing entity's liabilities, burn-and-mint bridging for jurisdictionally clean issuance, and binding home/host supervisory cooperation for cross-border reserve transfers in stress – so that the "mixing of baskets" risk is managed by design rather than by prohibition.
- A regional minimum standard for Latin America developed through CEMLA, covering reserves, redemption rights and disclosure, explicitly designed to generate the equivalence record needed for access to other markets (see Chapter 16).
- A neutral EU Stablecoin Association to coordinate best practices and supervisory convergence, and engagement with the FSB to ensure global standards reflect the distinct economic function of stablecoins in high-inflation economies.

COMMUNITY IN ACTION — The Joint Interpretive Note on multi-jurisdictional EMT issuance

The Helsinki call to action was not a request that regulators clarify whether multi-jurisdictional issuance is permitted – it was a decision to demonstrate that MiCAR already permits it. The resulting Joint Interpretive Note, authored by Nordic Law and published by BlackVogel and siedler legal, set out why Recital 54 and Articles 38 and 54–56 accommodate multi-jurisdictional issuance provided EU-liability reserves are held under EU law.
By Paris 2.0 the Note was treated as the settled legal foundation for the next phase of work, its conclusion stated in stronger terms: MiCAR neither prohibits nor merely tolerates multi-jurisdictional issuance but in several respects affirmatively accommodates it, and supervisory authorities cannot convert regulatory silence into a substantive ban through interpretation or administrative practice. The Note resolves the permissibility question; it does not resolve the operational-design questions – reserve correspondence, bridging, redemption in stress – which remain the subject of the calls to action above and are now formally posed in the Commission's targeted consultation on the MiCA review, open since 20 May 2026, which asks expressly whether the multi-issuance model should remain permitted.

7. The MiCA–PSD Dual-Licensing Question

7.1 The problem

The moment an EMT moves, a second regulatory universe opens: payments law. Whether a CASP that facilitates EMT transfers also performs a payment service – and therefore needs a PSD2, and later PSD3/PSR, authorisation in addition to its MiCAR licence – became one of the most consequential open questions of MiCAR implementation. Its root is the dual qualification

of EMTs as both crypto-assets and electronic money, and the mischaracterisation of on-chain transfers as conventional payment services.

7.2 How the conversation developed

DARTE Oslo (January 2025) identified the overlap and its cost: double authorisation, inconsistent supervision – some NCAs permitting a single entity to hold both licences, others forcing separate entities – and capital-requirement uncertainty resolved in practice by applying the higher threshold. It isolated four classification grey zones (same-person account transfers, custodial-to-non-custodial transfers, peer-to-peer EMT payments, and EMT payments for goods or services), recorded the Commission's December 2024 request to the EBA and ESMA for a no-action letter, and characterised dual authorisation as an unintended consequence rather than a policy choice.

DARTE Helsinki (November 2025) supplied the doctrine. The confusion rests on two errors: equating wallets – digital vaults, or bearer instruments – with PSD2 payment accounts, and treating on-chain transfers as credit transfers or remittances although no provider handles fiat funds in the PSD2 sense. Anchoring the CASP transfer service in Recital 90 and Articles 48(2) and 70 (4) MiCAR, the session acknowledged that genuine payment services such as fiat payouts and merchant acquiring do belong with licensed PSPs, and noted that the PSD2 minimum capital of €700,000 is unattainable for many CASPs – the observation that later grounds the tiered-pathway proposal.

DARTE São Paulo (March 2026) added the decisive chronology and the third-country lens. The EBA's June 2025 No-Action Letter created a transition period that ended on 2 March 2026, and the EBA Opinion of February 2026 confirmed that a client-named wallet permitting EMT transfers to or from third parties without bank intermediation is a payment account under PSD2, with no derogations. The PSD3/PSR political agreement of 27 November 2025 and final texts of 5 March 2026 kept the dual-regime architecture, adding only a streamlined 60-business-day authorisation channel for Article 63 MiCAR CASPs providing payment services exclusively with EMTs, with full applicability expected around Q2/Q3 2028. Three interim operational models were identified: a pure MiCAR model without EMT transfer functionality, a PSP-as-a-service partnership, and a hybrid group structure.

Paris 2.0 (April 2026) examined the settled PSD3/PSR perimeter and the divergence already visible beneath it – Latvia requiring both licences in one entity while Cyprus requires two, Luxembourg's informal pre-screening delaying MiCAR applications, dual applications running to thousands of pages with time-sensitive documents expiring mid-process, and unresolved EMT tax treatment because MiCAR classifies them as crypto-assets while e-money rules treat them as fiat. Its structural conclusion was that the line between trading and payment functionality is operational, not purely legal: small changes in wallet design, custody model or transfer flow move a service between regimes.

7.3 Interactions with other themes

This chapter is the direct continuation of the EMT analysis in Chapter 6; the self-hosted-wallet exclusions it notes connect to Chapter 9 (Self-hosted wallets), the classification grey zones to the token classification in Chapter 2, and the divergent national implementations to the supervisory-convergence diagnosis of Chapter 13.

7.4 Solutions and calls to action

- A joint EBA/ESMA/Commission interpretive statement, of the content the sessions specified: pure on-chain EMT transfers by a MiCAR-authorised CASP fall under MiCAR and do not require separate PSD authorisation, while genuine payment services – fiat redemption payouts, merchant acquiring – remain within the payments perimeter, with the four Oslo grey zones expressly allocated.
- A proportionate, tiered entry pathway – a small-payment-institution equivalent within MiCAR – allowing CASPs to access payment functionality without the full PI/EMI prudential burden that the €700,000 PSD2 minimum represents, with Hong Kong's dual-licensing model cited as the comparative template.
- An industry-led taxonomy of EMT-related activities and wallet typologies, distinguishing transfers, payments, exchange activities and internal operations – the series' most consistently repeated deliverable in this area – to stabilise the operational classifications on which the regime turns.
- Coordinated NCA supervision under PSD3/PSR to prevent the single-entity-versus-separate-entity and pre-screening divergences from hardening into arbitrage, and a joint interpretive position that using an EMT to purchase another asset is treated consistently for tax across Member States.

8. DeFi and the Regulatory Perimeter

8.1 The problem

The chapters so far presuppose an identifiable obligor. The next three examine what happens at the edges of that assumption. MiCAR excludes fully decentralised services through its Recital 22 without defining decentralisation, and the surrounding frameworks – DORA, AML, criminal law, data protection – were drafted for identifiable intermediaries. The result is a perimeter problem the series examined in seven sessions.

8.2 How the conversation developed

DARTE Vienna (May 2024) named the foundational gap that never closes: no formal definition of decentralisation despite Recital 22's exemption. Rather than await one, the session proposed how

to assess it – through centralisation vectors such as smart-contract access mechanisms (service accounts, kill switches), Web2 interfaces and platform dependence, alongside indicative criteria of return or fee extraction, token concentration, the presence of an identifiable provider and contractual promises – with the guiding insight that removing intermediaries does not achieve decentralisation where indirect control remains. DARTE Berlin (April 2024) had already flagged the corollary at the user-facing edge: non-custodial front-ends risk misclassification as operators, and the custodial/non-custodial distinction must be preserved.

DARTE Berlin 2.0 (August 2024) tested the perimeter against automated market makers, and its reasoning is worth preserving because it shows the method. Grounded in Recital 28 MiCAR (mirroring the Prospectus Regulation), the session concluded that providing liquidity is not in itself a public offer: a liquidity provider neither contracts with buyers nor receives a purchase price and lacks the intent to conclude transactions in specific proprietary assets. But a pool creator who sets the initial price and combines this with public advertising may become an offeror unless the contract is fully decentralised – and MiCAR, unlike MiFID II, offers no proprietary-trading or market-making exemption to fall back on. Money-laundering risk was identified as the principal residual concern.

DARTE Brussels 2.0 (March 2025) exposed a clean gap: DORA, unlike MiCAR, contains no Recital 22-style exclusion, so the legal permissibility of integrating DeFi components is uncertain – protocols fit awkwardly as either ICT assets or ICT third-party providers. The session distinguished infrastructure decentralisation (node number and distribution, clustering, centralised sequencers, common API chokepoints) from application-level decentralisation (access rights, token distribution, governance activity), and proposed engaging validator clusters run by trustworthy consortiums under enforceable SLAs to meet resilience expectations, while warning that compliance pressure can itself centralise DeFi.

DARTE Berlin 3.0 (June 2025) took the discussion to people: the criminalisation risk for developers of autonomous smart contracts after the Tornado Cash judgment, where deliberate immutable design without compliance features, continued maintenance and knowledge of criminal use grounded conditional intent – and the legal limbo of DAOs, with jurisdictional uncertainty, undefined liability, a representation gap and no minimum standards. DARTE Berlin 4.0 (June 2025), a dedicated DeFi edition, examined the tech-provider/service boundary through BaFin's investment-brokerage test against Liechtenstein's technology-neutral and Switzerland's functionality-and-control approaches, using the "postal service" analogy for wallets that merely pass signed transactions to a chain, documenting native DeFi risk management (wallet screening, malicious-token detection, real-time pool scanning) – including a case where a platform's proactive blocking of an illicit wallet was later publicly commended by the US government – and showing, through the loss of a DNS entry that cut off most users of an operational protocol, that front-end gateways are practical enforcement touchpoints even where the backend is decentralised.

DARTE Washington (October 2025) set the EU's principle-based approach against the rule-based CLARITY Act, which judges "mature blockchains" by quantitative thresholds – no entity or group above 20 per cent of governance power or token supply – plus open-source code, permissionless access and community-led upgrades. It recorded the philosophical divide, a proposed multi-vector scoring framework with per-dimension and aggregate thresholds, the counter-view that regulators should target activities and risks rather than degrees of decentralisation, and the warning that, absent guidance, the definition will be set by judges.

8.3 Interactions with other themes

The AMM analysis connects to the offer/whitepaper questions of Chapters 2 and 3; the DORA gap to the operational-resilience discussion of Chapter 13; the developer-liability thread to the private-law and criminal-law questions of Chapter 14; and the native-risk-management practices to the AML and CASP-gateway discussions of Chapters 9 and 10.

8.4 Solutions and calls to action

- A function-based perimeter test the sessions specified in substance: an entity falls within MiCAR only where it exercises control, discretion or access to user funds – assessed through the centralisation vectors identified in the DARTE Vienna and Brussels 2.0 discussions – with defined thresholds for when a front-end operator becomes a regulated entity and safe-harbour treatment for fully decentralised or self-hosted front-ends, preserving the custodial/non-custodial distinction.

- Clarification by the Commission and the ESAs of whether and how DeFi falls within DORA, with the proposed answer that resilience expectations attach to identifiable actors – validator clusters under enforceable SLAs – rather than to protocols that cannot be ICT third-party providers.

- Ex-ante developer-liability guidance linked to intent and specific conduct rather than the act of writing code, technology-neutral and protective of the lex certa principle and of dual-use technology – the substance the sessions proposed to contain the post-Tornado-Cash criminalisation risk.

- A standardised DAO governance taxonomy and an EU-wide cross-jurisdictional DAO sandbox, feeding an optional, technology-neutral EU legal regime for decentralised organisations.

- A shared EU–US decentralisation assessment toolkit blending quantitative thresholds with qualitative oversight, developed jointly by ESMA and US regulators, together with open-source non-custodial risk-mitigation infrastructure and pre-licensing sandboxes for interface providers.

9. Self-Hosted Wallets

9.1 The problem

If DeFi tests the perimeter on the service side, self-hosted wallets test it on the user side. They sit at the intersection of the TFR, MiCAR's service definitions and the AML package, and their treatment determines whether direct, non-intermediated use of the technology remains practicable in the EU at all.

9.2 How the conversation developed

DARTE Madrid (October 2024) raised the verification-threshold question under the Travel Rule and asked for a consistent, risk-based EU approach. Berlin 4.0 (June 2025) reframed it as a perimeter question: whether self-hosted wallet and front-end providers fall within MiCAR's service definitions, with the hazard that user-experience design, fee structures or access facilitation unintentionally convert neutral tools into regulated services – the "postal service" point from Chapter 8 above.

DARTE Paris 2.0 (April 2026) and Stockholm (May 2026) sharpened two structural problems. The TFR's definition of self-hosted addresses is over-broad, capturing smart contracts and DeFi protocols alongside personal wallets and imposing information-collection duties where no identifiable counterparty exists. And the prohibition on transfers above €1,000 to third-party self-hosted wallets is ineffectual – a user can route funds through their own non-custodial wallet first – while legitimate use bears the friction; DARTE Stockholm's answer was to verify the third party directly rather than block the transfer.

9.3 Interactions with other themes

This chapter is inseparable from the Travel Rule analysis of Chapter 10, which it precedes deliberately, and from the DeFi-perimeter test of Chapter 8; the identity mechanisms it invokes are developed in Chapter 11.

9.4 Solutions and calls to action

- A definitional split, reflected in EBA guidance and CASP compliance frameworks, between personal self-hosted wallets and programmatic addresses (smart contracts, protocols), with the risk-based approach under Article 19a AMLD governing the latter so that information-collection duties do not attach where no counterparty exists.
- Explicit clarification that the €1,000 third-party threshold triggers a risk assessment rather than automatic identity verification – the reading the sessions reached of the EBA Travel Rule Guidelines.

- Recognition of external KYC of the third-party counterparty – via eID, remote identity verification or a digital identity wallet – as a proportionate, evidence-based substitute for the blanket restriction on transfers above €1,000, which users can in any event circumvent.

10. AML Compliance

While the Travel Rule and AML Compliance discussions initially focused mainly on the EU implementations, the DARTE São Paulo and the Berlin 6.0 sessions concerned the international AML/CFT standard set by the FATF Recommendations.

10.1 The problem

Non-intermediated holding leads directly into the framework that struggles with it most. The Travel Rule required by the FATF Recommendations and implemented in the EU under the Transfer of Funds Regulation is the most frequently discussed single instrument of the DARTE series, appearing in nine sessions across three continents. The tension is constant: the duty to exchange originator and beneficiary information enhances traceability, but its implementation collides with non-interoperable infrastructure, divergent national and international standards, self-hosted wallets and fundamental privacy rights.

10.2 How the conversation developed

DARTE Madrid (October 2024) reconstructed the June 2022 political compromise on self-hosted wallet thresholds and warned that the EBA's Travel Rule guidelines drift from it by suggesting CASPs gather extra data to verify third-party wallets – a shift that could push transfers to unregulated markets – while rejecting stricter treatment of crypto than cash given blockchain's traceability. DARTE Frankfurt (November 2024) turned to operations: interoperability gaps among EU CASPs (including the unstated assumption that a licence guarantees data quality), the absence of standardisation with non-EU CASPs, and the handling of incoming transfers with incomplete data – where the session worked through the four options pursuant to Article 17 TFR and concluded that rejection is impractical on-chain, returns risk losing funds in omnibus structures, suspension is a last resort, and execution with safeguards is the preferred path. It also exposed why bank–CASP KYC sharing fails in practice: Germany's 24-month re-verification condition renders most existing bank data unusable, and intermediary banks lack wallet data – supporting the view that the transmission duty should rest with the crypto custodian.

DARTE Dublin (November 2024) globalised the problem, mapping the interpretation gap between the EU TFR and FATF Recommendations 15 and 16, including the divergence between FATF's USD 1,000 threshold and the TFR's extension to smaller transfers, and counterparty non-cooperation as a driver of jurisdiction shopping. DARTE Paris (April 2025) observed implementation at scale during the tolerance period: superficial due-diligence practices that risk breaching the GDPR and the TFR at once, FATF-flagged tooling deficiencies prompting banks to cut fiat rails, and Lamfalussy-level inconsistencies leading to the position that Level 1 must

prevail – alongside the reconceptualisation of identity as functional attestations ("over 18", "not sanctioned") rather than names and addresses, which becomes the through-line to Chapter 11 on privacy.

DARTE Madrid 2.0 (October 2025) recorded how divergent national document standards, privacy laws and monitoring requirements undermine auditable compliance; DARTE Berlin 5.0 (November 2025) advanced the identity-based path of reusable credentials and selective disclosure (Chapter 11); DARTE São Paulo (March 2026) identified the absence of open interoperability protocols between VASP systems as the core Latin American bottleneck and the FATF revision as an alignment opportunity. DARTE Stockholm (May 2026) extended the rule into real-world payments: the absence of meaningful third-party verification, the ineffectual €1,000 prohibition, DORA and data-sovereignty exposure where Travel Rule providers face non-EU court-ordered data sharing with little incentive to interoperate, and missing data fields – including a payment-explanation field essential for B2B invoice reconciliation – tempered by the reminders that most EU CASP traffic is closed-loop, that banks needed fifteen years to agree SWIFT standards, and that expanding payloads creates honeypot risk.

10.3 Interactions with other themes

The chapter depends on the self-hosted-wallet analysis of Chapter 9 and flows into the privacy and digital-identity discussion of Chapter 11, whose credential mechanisms are the proposed solution here; its DORA and outsourcing threads connect to Chapter 13. The FATF dimension is taken up at the level of the standards themselves in Sections 10.5–10.6.

10.4 Solutions and calls to action

The proposals evolved in three waves, each with specified content:

- Risk-based calibration: CASPs assess risk at transaction and customer level rather than applying blanket verification; incoming transfers with incomplete data are executed with safeguards – real-time data governance, automated counterparty communication before crediting, transaction monitoring and a staffed AML function – rather than rejected; the transmission duty rests with the crypto custodian that holds the wallet data.

- Standardisation and interoperability: a Wolfsberg-style due-diligence questionnaire for non-EU CASPs, secure interoperable messaging protocols for data resolution, alignment of EU implementation with FATF standards, and – in Latin America – mandated open interoperability protocols anchored to the FATF revision cycle.

- Structural redesign: alignment with eIDAS 2 and the European Digital Identity Wallet; decentralised compliance based on cryptographic attestations and credential reuse; recognition of external KYC to lift the €1,000 self-hosted restriction; a whitelist of DORA-compliant Travel Rule providers; and extension of the data standard to include a payment-explanation field with explicit data-minimisation safeguards.

10.5 The FATF framework under review: Berlin 6.0

10.5.1 A deliberate departure from the series' method

DARTE Berlin 6.0 (June 2026) departed from the DARTE series' method by design. Where the standard editions seek solutions within the existing framework, this edition subjected the FATF Recommendations themselves to critical analysis and proposed concrete amendments. The unifying question was the distinction between measuring how well institutions comply with the standards and asking whether the standards achieve what they were built to do.

The shared diagnosis was stark: the global AML/CFT framework is costly, discriminatory and largely ineffective against its stated purpose; much of it dates in current form from 2001–2003, designed for a vanished technological environment; and stacking further frameworks on a structure that does not work compounds the problem. This is evidenced by an estimated USD 206.1 billion in financial-crime compliance costs of financial institutions worldwide incurred over the twelve months covered by the 2023 LexisNexis Risk Solutions study, with the corresponding cost in EMEA alone estimated at approximately USD 85 billion while public financial-crime enforcement resources remain fragmented and substantially smaller.

10.5.2 The three discussions

The first discussion (Recommendations 10, 15 and 20 – customer due diligence, new technologies, suspicious transaction reporting) argued that the operational core of the regime now constrains rather than enables the fight against financial crime: CDD data siloed across systems weakens AI models and creates black boxes hard to justify in risk-based terms; institutions deploy AI without the formal assessment, testing and inventory Recommendation 15 implies; and rules engines generate low-value alerts that FIUs rarely give structured feedback on. The second discussion (repurposing Recommendation 16) presented the Travel Rule as imposing large permanent costs for negligible return – citing Europol for the assessment that around 1% of EU criminal proceeds are confiscated and that law enforcement accessed under 3% of suspicious transaction reports filed between 2014 and 2023 – while concentrating identity data into multiple honeypots and offering no solution for unhosted wallets. The third discussion (Recommendations 33, 41 and 42) addressed the absence of any mechanism to evaluate whether the regime works, arguing that Recommendation 33 measures activity rather than effectiveness and produces a "success theatre" blind to cost and collateral damage.

10.6 Berlin 6.0: solutions and significance

The session produced three sets of proposals rather than requests – consistent with the series' principle even while breaking its work-within-the-framework rule:

- On Recommendations 10, 15 and 20: move from data sharing to proof sharing, anchored in verifiable credentials, zero-knowledge infrastructure and the European Digital Identity Wallet, so institutions verify what they need (KYC completion, sanctions clearance,

network-level suspicion) without expanding the attack surface; reframe inter-institutional exchange as suspicion sharing rather than customer-data sharing, with a data subject's right to be informed of a flag, to challenge it and to have it removed across the network; require structured FIU feedback; and treat each AI use case as a "new technology" under Recommendation 15, supporting federated learning and secure multiparty computation.

- On Recommendation 16: repurpose the obligation from bulk identity-data transmission into participation in a qualifying, vendor-neutral intelligence-sharing network in which institutions, VASPs, FIUs and law enforcement share risk information only where defined red-flag thresholds are met – modelled on Singapore's COSMIC, the EU's TRACE project and Article 75 AMLR read with GDPR Recital 47, with FATF supplying the qualifying-network criteria and the safeguards (a defined suspicion threshold, pseudonymisation, a mandatory DPIA, joint-controller accountability, independent audit, a redress mechanism) and targeted financial sanctions preserved.

- On Recommendations 33, 41 and 42: reform Recommendation 33 to require effectiveness, cost and exclusion statistics – de-banking and refusal rates disaggregated by customer category, outcome ratios linking SAR volumes to investigations, prosecutions and convictions, and redress outcomes; a new Recommendation 41 establishing independent, evidence-based evaluation of national frameworks against measurable goals; and a new Recommendation 42 requiring fundamental-rights safeguards – no "black box" decisions, written reasons and a right to be heard for denial and termination, effective remedies including reinstatement, minimum access to basic banking, and a reversed burden requiring institutions to justify exclusion.

DARTE Berlin 6.0 was the first session to move from working within the framework to proposing amendments to it. Its output will advance through the FATF's open public consultation on the draft Recommendation 16 Guidance, with responses due 21 August 2026, and the implementation window running to end-2030, and it ties directly back to the Travel Rule analysis of this chapter and forward to the digital-identity and fundamental-rights analysis of Chapter 11.

11. Privacy, Data Protection and Digital Identity

11.1 The problem

Every obligation in the preceding chapter concerns also a data-processing operation, so the AML discussion flows directly into data protection. The tension between transparency duties (AML, market integrity, tax) and fundamental rights recurs throughout the DARTE series, sharpening from individual compliance questions into a structural confrontation between GDPR's

centralised assumptions and decentralised infrastructure – and finally into an agenda built on privacy-preserving identity.

11.2 How the conversation developed

DARTE Berlin (April 2024) began narrowly, with the meaning of "transaction history" for privacy coins under Article 76 (3) MiCAR and its GDPR implications, proposing to limit history disclosure to transactions directly involving the current holder. DARTE Madrid (October 2024) widened this to the combined data-handling risks across MiCAR, AMLD6, TFR, DAC8/CARF – insecure investigative tools, cross-border sharing complexity.

DARTE Berlin 3.0 (June 2025) reached the structural confrontation: the EDPB's Guidelines 02/2025 fail to reflect how decentralised systems work, blurring infrastructure-level data (addresses, hashes) with personal data and threatening privacy-by-design implementations. That DARTE session's position – that GDPR responsibility should centre on data-collecting intermediaries rather than the infrastructure layer – is the privacy counterpart to the function-based perimeter test of Chapter 8 on DeFi.

DARTE Berlin 5.0 (November 2025), a dedicated digital-identity edition examined the systemic risks of centralised eID under the amended eIDAS regulation, sharpened by combination with programmable money and illustrated by comparative cases; the compatibility of decentralised identity with GDPR through the Key Event Receipt Infrastructure, where verifiable event logs replace on-chain personal data; and the absolute-versus-relative identifiability debate, favouring the relative, actor-specific standard supported by recent CJEU case law applying a contextual "reasonably likely means" test. Its central construct – "identity on demand", a verifiable credential proving a KYC check was performed by a trusted third party, with full verification triggered only by flagged activity – is the mechanism the Travel Rule and self-hosted-wallet chapters rely on.

11.3 Interactions with other themes

This chapter supplies the compliance technology proposed throughout the AML and Travel Rule discussions (Chapters 9 and 10) and, at the level of the FATF Recommendations, in DARTE Berlin 6.0 (Sections 10.5–10.6); its intermediary-versus-infrastructure logic mirrors the DeFi-perimeter test of Chapter 8 and the sustainability-allocation debate of Chapter 4.

11.4 Solutions and calls to action

- A narrow GDPR interpretation excluding infrastructure-level data (addresses, hashes) from "personal data", with regulatory responsibility centred on intermediaries who establish off-chain links to individuals – the specific content the sessions proposed for clarification of the EDPB Guidelines.

- A relative, risk-based standard of identifiability sparing processors who lack re-identification capability from disproportionate obligations, aligned with the CJEU's "reasonably likely means" test.
- "Identity on demand" as the reference compliance model: verifiable credentials attesting completed KYC, with selective disclosure and revocation standardised through bodies such as ISO and DIN, full verification triggered only by flagged activity, and removal of the legal barriers that current due-diligence interpretations pose to KYC-certificate reuse.
- Regulator–industry sandbox pilots of decentralised compliance models, and a taxonomy and proportionality matrix for identity use cases so that data collection is matched to risk.

12. Tax Reporting and Accounting Infrastructure

12.1 The problem

Tax transparency completes the triad: after AML and privacy, DAC8 raises the same tension in fiscal form – and adds an infrastructure problem of its own. With DAC8 obligations applying since January 2026 and the first reports due in 2027, the question shifts from legal interpretation to whether the data being generated, classified, converted and transmitted can be produced reliably at all, and whether taxpayers can understand what is reported about them.

12.2 How the conversation developed

DARTE Madrid (October 2024) first raised the privacy and data-security dimension of CARF/DAC8 reporting. DARTE Vienna 3.0 (May 2026), a dedicated accounting and tax edition opened by an overview of the OSCE's virtual-asset work, confronted the operational reality. Traditional accounting and ERP systems cannot process Web3 activity: a single user-visible transaction becomes three to four or more accounting entries, an active user can generate 50,000 to 200,000 accounting lines a year, and practitioners reported non-compliant workarounds – parallel spreadsheets disclosed to authorities as the best achievable approach. The session also identified a structural information asymmetry under DAC8, where authorities receive extensive data while users cannot see how figures are aggregated, valued and classified – recalling the DAC2/CRS precedent of assessments on gross proceeds rather than realised gains, and reaching the central consensus that DAC8 is a transparency framework, not a taxation norm. On classification and conversion – whether an asset is reportable under CRS or CARF, acceptable conversion rates, the contingent treatment of stablecoins as cash equivalents or intangibles – it concluded candidly that, absent a globally unified framework, no complete solution exists.

12.3 Solutions and calls to action

- A standardised upstream aggregation layer at EU level that translates Web3 transactions into transaction-type-specific summary bookings while preserving a revision-safe, drill-down

audit trail – the specific mechanism proposed for the accounting-volume problem – supported by a shared, jurisdiction-aware transaction-mapping library, updated as new DeFi strategies emerge.

- Generic DAC8 explanatory reports across CASPs plus transaction-level drill-down on request together with clear communication to authorities that DAC8 is a transparency framework rather than a taxation norm, cross-border recognition of correction reports, and standardised conversion and valuation simplifications.
- Engagement with the IFRS Foundation on crypto-asset accounting, with consistent treatment of stablecoins and EMTs and a continuity principle protecting good-faith classifications from retroactive challenge, and stronger crypto-native representation in OECD and other standard-setting processes.

13. Supervisory Convergence and Proportionality

13.1 The problem

Across all of the foregoing themes, one variable determines outcomes more than any rule: the consistency of the supervision behind the single passport. Throughout the series, divergent national practice – in authorisation, transitional regimes, passporting, prudential calculation, outsourcing and operational resilience – was identified as the principal threat to MiCAR's harmonisation objective, and disproportionate burdens on smaller actors as the principal threat to market diversity.

13.2 How the conversation developed

The transitional-regime thread (Berlin, Vienna, Oslo) worked through Article 143 (3) MiCAR's ambiguities, reaching consensus that "services in accordance with applicable law" should include unregulated but lawful CASPs, and producing at DARTE Berlin 2.0 a standardised declaration template by which offerors state that past (and potentially non-compliant with MiCAR) communications lose binding effect from 31 December 2024 – addressing the retroactivity problem. In the EEA, delayed adoption left Liechtenstein and Iceland waiting after Norway's late submission. The significant-entity thread (DARTE Brussels) criticised the fifteen-million-user significance criterion as poorly calibrated and proposed supplementing it with market impact and transaction volume, and recast the absence of mandatory regular reporting as a burden – exposing CASPs to divergent ad-hoc national requests. The passporting thread (DARTEs Vaduz, Lisbon) documented how undesignated NCAs blocked notifications in practice, with Portugal as the illustrative case, and recommended proactive notification of all potentially relevant authorities.

The prudential thread (DARTE Vaduz) is where the proportionality diagnosis bites hardest: initial own-funds requirements of €50,000–150,000 are workable, but the ongoing fixed-overheads requirement can reach millions for larger CASPs without the risk-sensitive factors available to banks and MiFID firms; and the classification of crypto-assets as intangibles under Article 36 CRR would force own-funds deductions and risk double deduction under Basel. The outsourcing thread (DARTEs Zug, Vaduz, Brussels 2.0) reconciled the custody sub-delegation rule with cross-border infrastructure by reading "providing custody" to cover only providers with individual private-key access, and pressed for alignment of the overlapping DORA, MiCAR and 2019 EBA outsourcing requirements. The proportionality thread (DARTEs Brussels 2.0, Paris, Vienna 2.0, Madrid 2.0, Vienna 3.0) recurs across the whole series: rules calibrated to large incumbents become market-structure policy by default.

The transitional regime has closed EU-wide on 1 July 2026 and ESMA confirmed that any entity providing crypto-asset services to EU clients without a MiCA licence is now in breach of EU law and must cease, with wind-down plans expected to have been ready in advance.

13.3 Interactions with other themes

This chapter is the supervisory substrate of every other: the classification-passport warning of Chapter 2, the reporting burdens of Chapters 3–5, the prudential feed-through from DORA in Chapter 8, and the dual-licensing divergence of Chapter 7 all resurface here as facets of one problem.

13.4 Solutions and calls to action

- Risk-sensitive own-funds calculation introducing K-factors or comparable risk-weighted approaches aligned with the investment-firm regime, exclusion of unregulated business lines from the fixed-overheads base, recognition of AT1 and Tier 2 instruments alongside CET1, and exclusion of crypto-assets from the CRR Article 36 intangible-asset deduction – the concrete prudential content the sessions specified.

- A narrowed custody definition focused on individual private-key access; alignment of outsourcing obligations across DORA, MiCAR and the forthcoming EBA guidelines with withdrawal of the 2019 guidelines; consolidated outsourcing notifications on the BaFin model; and pooled audit models eliminating redundant ICT-provider audits.

- Prompt NCA designation by all Member States with ESMA/EBA support, respect for the passporting framework with product interventions limited to genuinely risk-posing activities, whistleblowing channels for CASPs facing discriminatory national action, and refined significance criteria supplementing the user count with market impact and transaction volume.

- Formal application of the proportionality principle across Level 1 and Level 2, recognition of intragroup risk-management procedures, and standardised periodic reporting templates

calibrated to size and risk – preferable, for supervisors and firms alike, to the current ad-hoc national requests.

14. Private Law and Tokenised Capital Markets

14.1 The problem

Beneath the regulatory layer lies a question the series confronted late but decisively: what, in law, a crypto-asset actually is. Regulatory law determines who may provide services; private law determines what the asset is, who owns it and how rights are transferred and enforced. However, private law questions remain fragmented across national civil, corporate and property law.

14.2 How the conversation developed

DARTE Munich (September 2025) reached the private-law problem through capital markets. Hybrid securities existing in both certificated and ledger-based form face secondary-market liquidity problems rooted in infrastructure, not regulation: liquidity fragments between exchanges and DLT systems and conversion is opaque. The session weighed three models – trustee-based pooling, a market-maker arrangement, and the preferred bank-intermediated "share-loan conversion bridge" – and asked whether limited-purpose share loans could be exempted from licensing. Because the rights attached to security tokens are governed by national law and unevenly enforceable except under the DLT Pilot Regime, and because decentralised exchanges were examined and rejected as a workaround that does not resolve enforceability, the session concluded – recorded expressly as a first across all DARTE roundtables – that the only viable long-term solution is a new law, preferably an EU regulation: a pan-European Electronic Securities Law.

DARTE Rome (December 2025), convened with UNIDROIT, supplied the doctrinal toolkit, working through three approaches under the express recognition that a regulatory regime cannot be built on a legal fiction: a sector-specific EU instrument modelled on the Financial Collateral Directive, constrained by Article 345 TFEU's reservation of property law to national competence and doubts about Article 114 TFEU as a basis – with a future Article 118-style treaty provision raised for the longer term; soft law, with the UNIDROIT Principles as interim guidance; and mutual recognition of national characterisations, for which e-money and financial instruments provide a precedent. On the "control" concept – a factual notion functioning as the equivalent of possession – the session examined its integration into civil-law systems, the overlap between custody and control where custodians hold technical power without beneficial entitlement, and called for presumptions or safe harbours protecting good-faith acquirers who rely on blockchain-based indicators of control, with Italy's Fintech Decree as the reference case.

14.3 Solutions and calls to action

- A pan-European Electronic Securities Law – preferably an EU regulation, with the Financial Collateral Directive as the alternative model – harmonising civil-law definitions and enforcement for ledger-based instruments; this is the one place in the series where the sessions concluded that work within the existing framework is insufficient and a new instrument is required.

- Recognition by Member States of the proprietary character of digital assets and of control-based transfer, with the control concept integrated into civil law and supported by presumptions or safe harbours for good-faith acquirers relying on blockchain-based indicators of control, and a clarified distinction between control and custody including the insolvency treatment of assets over which a custodian holds technical power without beneficial entitlement.

- Expansion of book-entry frameworks to DLT-based securities with guidance on the interaction between on-chain registries and off-chain enforcement in default and insolvency; advancement of the ESMA DLT Pilot Regime recommendations (raised caps, broader asset scope, a permanent regime); piloting of bank-intermediated loan-backed conversion for hybrid securities, with assessment of a limited-purpose share-loan licensing exemption; and a cross-sector working group on DLT interoperability standards.

15. Reverse Solicitation and Third-Country Market Access

15.1 The problem

The final two chapters look outward, beginning with the narrow gate through which third-country actors may serve EU clients without an EU licence. Reverse solicitation is the most frequently revisited topic of the series' first year. The problem is constant: Article 61 (3) MiCAR and ESMA's guidance determine when third-country actors may serve EU clients without a licence. Yet the boundary between solicitation and legitimate non-solicited activity is unclear – and each session exposed a different facet.

15.2 How the conversation developed

DARTE London (March 2024) raised app-store storefronts – whether app-store interactions could themselves be construed as solicitation, given the absence of geo-fencing and ESMA's narrow reading of "own exclusive initiative". DARTE Berlin (April 2024) worried that ESMA's Guideline 1 could treat social, professional and educational activities – road shows, academic courses – as solicitation, and proposed a class exemption and labelling framework for non-commercial gatherings. DARTE Vienna (May 2024) insisted the exemption remain strictly client-initiated, with indirect solicitation through advertising, influencers and sponsorships captured, and recorded that German and Dutch supervisors had treated active listing on a third-country

exchange as subjecting the issuer to that exchange's home regime. DARTE Brussels (July 2024) flagged the chilling of brand marketing by diversified third-country institutions absent a clear nexus to specific services. DARTE Berlin 2.0 (August 2024) exposed the offeror gap: the reverse solicitation protection runs to CASPs but not to crypto-asset offerors.

DARTE Zug (October 2024) worked through mixed EU/non-EU group structures with shared brand identities, rejecting both geo-blocking (VPN-circumventable and an undue restriction on EU citizens' choice) and brand separation (counterproductive for global brands) in favour of distinct website sections with IP routing, staff training and detailed documentation of how each customer initiated contact – and established that a third-country project's mere token issuance should not per se defeat the exemption, provided the token is not closely tied to the service legitimately offered to EU customers. DARTE Oslo (January 2025) and São Paulo (March 2026) delivered the sober verdict: reverse solicitation may be a cautious interim strategy, not a path to scale in the EU, because under ESMA's guidelines any promotion – targeted advertising, influencer activity, EU-language SEO, retargeting – invalidates reliance on Article 61 MiCAR.

15.3 Solutions and calls to action

- A standardised interpretation of solicitation in digital contexts, differentiated from the MiFID II test, whose content the sessions specified: an explicit exemption – with a labelling framework – for non-commercial and educational activities, so that road shows and academic courses do not invalidate the client-initiative exemption.
- Extension of the reverse-solicitation principle from the Prospectus Regulation to offerors, closing the Berlin 2.0 gap, with parameters preventing misuse.
- Workable rules for group structures allowing global brand consistency alongside clear service separation – distinct IP-routed website sections, staff training and documentation standards evidencing client-initiated contact – in preference to geo-blocking, together with a decisive pre-issuance assessment of the token-service connection.
- Risk-based enforcement by NCAs prioritising activities with genuine consumer-harm potential, reflecting the series' conclusion that a clear, administrable perimeter is itself the most effective enforcement tool against genuinely non-compliant third-country activity.

With the transitional regime closed since 1 July 2026, reverse solicitation is the only remaining lawful basis for unauthorised third-country service into the EU — making the definitional clarity proposed above more consequential, not less

16. Regional and Global Regulatory Cooperation

16.1 The problem

Where reverse solicitation defines the gate, recognition and equivalence define the road between jurisdictions. As the series expanded beyond the EU, a meta-question came into focus: how jurisdictions with different regulatory philosophies can interoperate. Full harmonisation is, in most constellations, politically and culturally infeasible; fragmentation imposes duplicative compliance, invites arbitrage and disadvantages compliant firms.

16.2 How the conversation developed

DARTE Buenos Aires (March 2025) surveyed Latin American regulatory diversity – shared principles but distinct national approaches shaped by inflation and currency instability, institutional gaps where no authority is designated, and the sobering precedent of earlier failed capital-market mergers – while cautioning that the apparent regional alignment observed was an assumption a full jurisdictional review would need to substantiate. Its preferred tools were practical: sandboxes, mutual recognition and regional working groups underpinned by regulator capacity building. DARTE Paris (April 2025) added the competitiveness dimension, warning that without modernisation the EU risks becoming a regulatory "flyover zone", and recording concrete frictions – an implementation timeline described as practically impossible, stricter French requirements prompting relocation, and the departure of traders after a major stablecoin delisting – alongside the FCA's £7.8 million commitment as a positive UK signal.

DARTE Washington (October 2025) articulated the recognition thesis: rather than harmonising, jurisdictions should acknowledge each other's frameworks where baseline standards – governance transparency, market integrity, operational resilience, control-concentration limits – are met, supported by recognition agreements and a regulatory principles index, with harmonisation suiting KYC/AML, promotions and custody, and recognition suiting governance and decentralisation thresholds, and with express guardrails against "arbitrage through recognition". DARTE São Paulo (March 2026) made it concrete through the corridor model – the Brazil–EU relationship as a test case, a CEMLA-based regional stablecoin standard generating the equivalence record for US access, and FATF-anchored Travel Rule convergence.

16.3 Solutions and calls to action

- Bilateral and multilateral recognition agreements built on a shared regulatory principles index, allocating harmonisation and recognition by subject matter – harmonisation for KYC/AML, financial promotions and custody standards; recognition for governance models and decentralisation thresholds – with guardrails against arbitrage through recognition.
- A CEMLA-based regional minimum standard for Latin America (reserves, redemption rights, disclosure) designed to generate the equivalence record needed for EU and US market

access, and structured bilateral corridor frameworks with the Brazil–EU relationship as the test case.

- Recognition by the EU of MiCAR-compliant disclosures across cooperating jurisdictions, and baseline interoperability principles allowing jurisdictional recognition within the EU without full standardisation of compliance tools.

17. Cross-Cutting Findings

17.1 From interpretation to operationalisation to infrastructure

Read in sequence, DARTE sessions trace the life cycle of a regulatory framework. The 2024 editions are dominated by interpretive questions – what counts as solicitation, how transitional provisions apply, how assets are classified. By 2025 the centre of gravity shifts to operationalisation – monitoring insider dealing in continuous markets, implementing the Travel Rule at scale, converging supervision in practice. The 2026 editions confront infrastructure and second-order design – accounting systems, reporting transparency, reserve calibration, the conditions for multi-jurisdictional operation. The recurring conclusion of the most recent sessions, stated explicitly at DARTE Paris 2.0, is that the next phase will be defined not by new legislative text but by the quality of interpretation and the consistency of supervisory practice.

17.2 From regulatory demands to built instruments

The character of the calls to action evolved. Early sessions predominantly addressed regulators; later sessions increasingly assigned work to the industry itself. This analysis reflects a deliberate discipline of the DARTE series in how those calls are framed: the series does not ask for guidance in the abstract but proposes the substance of the guidance it considers necessary, so that each call to action carries the content of the test, definition or safeguard it seeks. On several themes this discipline produced not a proposal but a built instrument: the MiCA Crypto Alliance token-classification taxonomy for liquid staking tokens (Chapter 2); the DAAvern disclosure platform addressing the Article 88 MiCAR disclosure-channel problem (Chapter 5); and the Joint Interpretive Note on multi-jurisdictional EMT issuance authored by Nordic Law and published by BlackVogel and siedler legal (Chapter 6). To these can be added the standardised declaration template on past communications produced at Berlin 2.0 (Chapter 13) and the drafted FATF amendments produced at Berlin 6.0 (Chapter 10). Each shows a complete cycle from problem identification in one session to a usable instrument informing a later one, and together they express the DARTE series' programmatic formulation, from the Paris 2.0 keynote: regulatory quality over regulatory quantity, with industry acting not merely as a consultation respondent but as a co-designer of interpretive frameworks.

17.3 Recurring structural diagnoses

Four diagnoses recur regardless of topic. First, fragmentation through national divergence: whether in supervision, transitional regimes, NCA designation, civil law or tax classification, inconsistent Member-State practice is the most frequently identified threat to the EU single market. Second, the misfit of intermediary-based frameworks: rules drafted for identifiable, centralised actors map poorly onto decentralised infrastructure – visible alike in DORA classification, GDPR controllership, criminal liability and the Travel Rule, and answered repeatedly by the same move, to locate obligations on the actor that actually exercises control. Third, proportionality: from own funds to operational resilience to dual compliance, obligations calibrated to large incumbents repeatedly threaten smaller actors and market diversity. Fourth, the substitution of recognition for harmonisation in cross-border work, both globally and, increasingly, within the EU itself.

17.4 Open questions

Several questions remain unresolved and are likely candidates for future DARTE editions: an agreed assessment framework for decentralisation, raised in Vienna in May 2024 and still open after Washington; the legal form and recognition of DAOs; the boundary of inside information for blockchain-derived data and the classification of prediction-market positions; the private-law harmonisation programme identified in Munich and Rome, for which only a new EU-level instrument was considered sufficient; and the classification challenge in international tax reporting, for which Vienna 3.0 concluded that no complete solution exists absent a globally unified framework.

18. Annex: Session Index

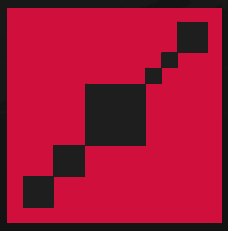
The table below lists the sessions covered by this analysis, with principal themes mapped to the chapters of this document.

Session	Date	Principal themes (chapter)
London	25 Mar 2024	Sustainability (4); EMTs (6); reverse solicitation (15)
Berlin	23 Apr 2024	NFTs and classification (2); reverse solicitation (15); grandfathering (13); privacy coins (11); DeFi front-ends (8)
Vienna	20 May 2024	Decentralisation (8); reverse solicitation (15); whitepapers (3); grandfathering (13); market abuse (5)
Brussels	10 Jul 2024	Whitepapers and disclosures (3); supervision (13); reverse solicitation (15)

Berlin 2.0	20 Aug 2024	AMMs and public offers (8); past communications (13); reverse solicitation for offerors (15)
Zug	2 Oct 2024	Reverse solicitation in groups (15); third-country custody (13)
Vaduz	4 Oct 2024	Own funds (13); gas-fee stations (13); outsourcing (13); passporting (13)
Madrid	10 Oct 2024	Travel Rule and TFR (10); EMT systemic risk (6); privacy across DAC8/CARF (11, 12)
Frankfurt	12 Nov 2024	Travel Rule interoperability (10); incomplete-data transfers (10); KYC sharing (10)
Dublin	25 Nov 2024	Sustainability disclosures (4); EU TFR vs FATF (10)
Oslo	31 Jan 2025	MiCA–PSD2 interplay (7); EEA implementation (13); sustainability (4)
Lisbon	28 Feb 2025	Sustainability reporting (4); passporting (13); L1 and airdrop whitepapers (3)
Brussels 2.0	14 Mar 2025	DORA and outsourcing (13); proportionality (13); DeFi under DORA (8)
Buenos Aires	25 Mar 2025	Special Edition – LatAm regulatory diversity, stablecoins, cooperation (2, 6, 16)
Paris	9 Apr 2025	EU competitiveness (16); UK post-MiCAR (16); Travel Rule at scale (10)
Milan	13 May 2025	Title II uncertainty (2); third-party whitepapers (3); insider dealing (5)
Berlin 3.0	13 Jun 2025	Developer criminal liability (8); DAOs (8); GDPR and blockchain (11)
Berlin 4.0	16 Jun 2025	Tech providers vs services (8); DeFi risk management (8); self-hosted wallets (9)
Vienna 2.0	10 Sep 2025	Inside information and Art. 88 (5); LST classification (2); MiCAR–MAR overlap (5)
Munich	11 Sep 2025	Hybrid securities (14); security token rights (14); DLT Pilot Regime (14)

siedler legal

Madrid 2.0	7 Oct 2025	Cross-border KYC/AML (10); market abuse standards (5); LST taxonomy (2)
Washington D.C.	29 Oct 2025	Decentralisation EU vs US (8); cross-border recognition (16)
Berlin 5.0	11 Nov 2025	eID risks (11); digital ID and GDPR (11); identity in AML/KYC (10, 11)
Helsinki	19 Nov 2025	Multi-jurisdictional issuance (6); dual licensing (7); reserve concentration (6)
Rome	5 Dec 2025	Private law fragmentation (14); the control concept (14); UNIDROIT Principles (14)
São Paulo	17 Mar 2026	LatAm–EU dual licensing (7); regional stablecoin standard (6); Travel Rule harmonisation (10)
Paris 2.0	14 Apr 2026	MiCAR/PSD3/PSR perimeter (7); multi-jurisdictional issuance (6); self-hosted wallets (9)
Vienna 3.0	18 May 2026	Web3 accounting (12); DAC8 asymmetries (12); classification and conversion (12)
Stockholm	25 May 2026	Travel Rule and third-party KYC (10, 9); blockchain data as inside information (5); prediction markets (5)
Berlin 6.0	15 Jun 2026	FATF Recommendations reform – CDD, new technologies and STR (Recs 10, 15, 20); repurposing of Rec. 16; statistics and fundamental-rights safeguards (Recs 33, 41, 42) (10); connections to digital identity (11)



DARTE SERIES

Digital Assets Round Table Experts Series

BlackVogel

siedler legal

DAVern