DARTE SERIES

Stockholm

Initiated by Mariana de la Roche W. (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), the DARTE Series is a high-level roundtable format designed to enhance legal clarity around digital assets, focusing on regulation, compliance, data protection, and market integrity.

The Stockholm DARTE edition took place on May 25th, 2026, at the Estonian House (Estniska Huset), in collaboration with the European Commission,Firi and the Nordic Blockchain Association. The roundtable examined three pressing questions at the intersection of AML compliance, market integrity, and the regulatory perimeter of novel on-chain instruments.

The agenda focused on three themes: 1) Travel Rule obligations on third-party KYC and enhanced due diligence, presented by Uve Poom (CryptoSwift); 2) when blockchain data becomes inside information, presented by Karola Xenia Kassai (KassaiLaw); and 3) prediction markets and MiCAR market abuse rules, presented by Dr. Nina-Luisa Siedler (siedler legal and DAAvern). The session opened with welcome notes by Magnus Jones (Nordic Blockchain Association) and Kadri Roosimägi (Estonian Embassy in Stockholm).

We extend our sincere thanks to all speakers, participants, and institutional partners for their valuable contributions. The views presented in this report reflect the collective understanding of the participants and do not necessarily represent the official positions of individual attendees or rapporteurs.

1. Travel Rule – Third Party KYC and Enhanced Due Diligence

The first topic was presented by Uve Poom (CryptoSwift) and addressed three interlocking problems with the current Travel Rule architecture as cryptocurrency transfers move beyond their historical use case of depositing or withdrawing funds to and from exchange wallets, and into real-world payments. This evolution aligns regulatory and operational expectations with those of fiat payments, but it also exposes structural weaknesses in the Travel Rule framework: the absence of meaningful counterparty verification in transactions involving third parties, failures in the Travel Rule service provider market, and gaps in the Travel Rule data standard itself that limit its usefulness for AML, enhanced due diligence, and real-world payment use cases.

On the first problem, the lack of system interoperability between Travel Rule Service Providers represents a market failure that becomes increasingly consequential as stablecoins are adopted for real-world payments. Unsent and unconfirmed Travel Rule messages result in incomplete data, in direct tension with recitals 28 and 33 of the TFR preamble, which require that payer and payee data be complete, particularly for cross-border transactions. Incomplete counterparty data also impedes the traditional AML checks that follow, including sanctions, PEP, and watchlist screening. A related issue arises from recital 39 of the TFR preamble: transfers exceeding €1,000 to third-party self-hosted wallets are effectively prohibited under the TFR, because the CASP is required to verify that the self-hosted address is owned or controlled by its own client. This restriction is largely ineffectual in practice, since users can transfer funds to their own non-custodial wallets first and then onward to any third party from there, while imposing significant friction on legitimate use cases.

On the second problem, not all Travel Rule Service Providers comply with DORA, particularly in relation to data-sharing obligations triggered by non-EU court orders. This raises concerns for European financial data sovereignty and digital infrastructure more broadly. The commercial logic of the market compounds the problem: Travel Rule providers have limited incentive to interoperate, as each is attempting to capture network effects within its own customer base, leaving CASPs exposed to fragmentation and uneven compliance coverage.

On the third problem, the Travel Rule data standard itself lacks fields that would meaningfully support compliance and real-world payment use cases. Current requirements on the beneficiary do not include the data needed for conclusive wallet ownership verification or for sanctions and watchlist screening. The payload is also missing a payment explanation field, which obscures the context of the payment and limits the usefulness of the standard for B2B payments that depend on accountants and auditors being able to reconcile payments against invoices. Real-world adoption of an otherwise robust and inclusive

technology is unlikely to deepen unless this basic measure is taken.

The solutions presented were targeted to each problem. For third-party verification, where third-party beneficiary or originator data cannot be completed through the exchange of Travel Rule messages, CASPs could rely on external KYC: the counterparty would identify themselves using eID, remote ID verification, or a digital identity wallet check. In practice, the originator CASP would ask its client to provide the third party's email address and would then initiate the verification process directly with the third party. Acknowledging external KYC as an adequate measure to complete Travel Rule data would also justify removing the current restriction on transactions above €1,000 between custodial and self-hosted wallets, since the verification objective would already be achieved through a more credible mechanism than the current prohibition. For the data standard, the Originating CASP should be allowed to request and share additional beneficiary data (such as nationality, country of residence, address, date of birth, or personal identification number) to enable conclusive verification, while recognizing the increased privacy risk associated with handling greater volumes of PII online. The Originating CASP may also choose to gather such data on the third party without sharing it with the counterparty VASP, although in that case the counterparty VASP cannot itself verify the data. A payment explanation field should also be added to support real-world payment use cases. For the market failure problem, Travel Rule Service Providers could be whitelisted for use by CASPs, with the whitelist maintained by industry associations or by regulators at national or European level, bringing transparency to DORA compliance, supporting interoperability, and strengthening European strategic autonomy.

The discussion that followed surfaced both support for and significant scepticism about the proposed solutions. Participants observed that for most CASPs operating today, the volume of relevant cross-CASP traffic is limited: many CASPs are running effectively closed-loop transfers and have already integrated with established Travel Rule providers, meaning the immediate utility of new third-party verification mechanisms is greater for the payments sector and for interactions with non-EU CASPs than for the typical EU CASP-to-EU CASP transfer. The example was given that where a Polish CASP has KYC'd its own user, an originator CASP in another Member State cannot access the underlying compliance data and may only receive the name. Where that name matches a sanctions list, the originator CASP still needs additional information to authorize the transfer, which is precisely where a third-party verification layer would provide value.

Participants discussed at length the practical and political dimensions of the interoperability problem. It was noted that banks took fifteen years to agree on messaging standards for SWIFT, and that the crypto industry's lobbying efforts to secure a comparable level playing field have not succeeded. The question of whether interoperability should be solved through regulatory mandate or through

industry collaboration was raised but not resolved, with the observation that a regulatory exemption could be a useful interim measure while the industry develops common standards. New entrants offering quantum-resilient blockchain analytics and risk metrics were noted, and several participants observed that consolidation in the Travel Rule provider market is expected following the July cutoff, which may shift the calculus around interoperability.

A recurring theme was the cost-benefit calculus of expanded data collection. Participants observed that AML officers are currently collecting substantial volumes of information that does not meaningfully support enforcement outcomes, and cautioned that further expanding the data payload risks creating new privacy exposures and honeypot risks without proportionate compliance benefit. The frequency at which third-party verification would need to be repeated was identified as an open question requiring practical calibration. Several participants also stressed that regulatory discussions of this kind, while important, do not substitute for grassroots education of CASPs, AML officers, and users on what compliant practice actually looks like in operation.

A further consequence of operationalizing third-party verification was identified: the same mechanism that allows verification of natural persons could be used to build a whitelist of trusted DeFi wallets and counterparties, addressing in part the parallel problem of how to treat transfers to programmatic addresses where no identifiable controller exists.

Calls to Action regarding Travel Rule Third-Party KYC and EDD

The key calls to action from the discussion are:

- **Recognize external KYC as a basis for lifting the €1,000 SHW restriction:** Regulators and industry should align on a third-party verification mechanism that allows the originator CASP to verify the identity of a non-customer counterparty through external KYC, whether via eID, remote ID verification, or digital identity wallet checks. Where such verification is performed, the current prohibition on transactions above €1,000 between custodial and self-hosted wallets should be lifted, replacing an ineffectual blanket restriction with a proportionate, evidence-based control that better aligns regulation with market practice.
- **Establish a whitelist of DORA-compliant Travel Rule service providers:** A whitelist of Travel Rule Service Providers meeting DORA and EU data sovereignty requirements should be maintained at industry or regulatory level, bringing transparency to compliance posture, supporting interoperability between

providers, and reducing CASPs' exposure to non-EU data access risks under foreign legal frameworks.

- **Extend the Travel Rule standard to include beneficiary identification and payment-purpose fields:** The Travel Rule payload should be extended to allow the Originating CASP to request and share additional beneficiary data necessary for conclusive wallet ownership verification and for sanctions, PEP, and watchlist screening, alongside a payment explanation field to support real-world B2B payment use cases. Such extensions should be designed with explicit data minimisation and privacy safeguards to avoid creating disproportionate honeypot or surveillance risks given the increased volume of PII handled online.

2. When Does Blockchain Data Become Inside Information?

The second topic was presented by Karola Xenia Kassai (KassaiLaw) and addressed a structural ambiguity in MiCAR's market abuse regime: the framework imports concepts developed for traditional financial markets into blockchain-based markets that operate on fundamentally different informational logic.

The core of the problem lies in how MiCAR's definition of inside information interacts with the transparency of blockchain infrastructure. Under Article 87 MiCAR, inside information includes information of a precise nature, not made public, relating directly or indirectly to one or more crypto-assets, which would likely have a significant effect on the price of those crypto-assets if made public. In traditional financial markets, the distinction between public and non-public information is usually relatively clear: information is either formally disclosed to the market or kept confidential within identifiable issuers and regulated intermediaries. Blockchain markets introduce a far more complex informational environment, in which a substantial amount of market-moving information may already exist publicly on-chain, yet remain practically inaccessible or economically meaningless without sophisticated analytical capabilities. CASPs, blockchain analytics firms, validators, and market makers may derive significant informational advantages from techniques such as wallet clustering and attribution, mempool visibility, bridge and liquidity monitoring, treasury wallet tracking, governance activity, stablecoin minting and redemption patterns, validator-level transaction visibility, and ecosystem flow analysis.

This creates a regulatory grey zone around the meaning of "public" information under MiCAR. Information may be technically accessible on-chain while realistically available only to a limited number of sophisticated actors with the analytical infrastructure to interpret it. Blockchain transparency therefore does not necessarily eliminate informational asymmetry; it may instead

shift it toward those with advanced analytical capabilities. The problem becomes particularly acute for CASPs and institutional actors that routinely gain access to ecosystem-level information through listing processes, custody services, liquidity provision, wallet analytics, institutional onboarding, or blockchain monitoring. While MiCAR clearly prohibits insider dealing and unlawful disclosure of inside information, the boundary between legitimate blockchain intelligence and non-public price-sensitive information in transparent yet highly asymmetrical markets remains unclear.

The current framework therefore generates uncertainty on a series of foundational questions: when blockchain-derived information becomes sufficiently precise under Article 87(2); whether technically public but practically inaccessible information should still be considered non-public; how CASPs should identify and wall off crypto-native inside information; and how market abuse rules should operate in markets where informational asymmetry arises from infrastructure access and analytical sophistication rather than from classic issuer relationships.

The solutions presented combined interpretive clarification with operational safeguards. While further regulatory guidance on concepts such as "public information" and "precise nature" would help reduce uncertainty, interpretive clarification alone is unlikely to fully resolve the structural issues created by transparent but asymmetrically interpretable blockchain markets. The industry should therefore work toward shared standards clarifying when blockchain-derived information becomes sufficiently precise to fall within Article 87(2), whether technically public but analytically inaccessible on-chain data may still constitute non-public information (along the lines of a "reasonably accessible information" test), and what practical compliance expectations should apply to CASPs handling crypto-native inside information. In parallel, regulators and market participants may need to adopt stronger operational safeguards, including tiered internal information barriers identifying high-risk informational moments and structurally separating sensitive functions, mantain insider trading lists, provide appropriate training for their personnel, restricted trading and cooling-off periods for personnel with access to market-sensitive operational information, and enhanced surveillance focused on abusive conduct patterns such as front-running or misuse of privileged order-flow visibility. Supervision itself may need to shift gradually toward a more conduct-based approach, focusing less on categorizing every form of blockchain-derived information and more on identifying abusive patterns in practice.

The discussion that followed centered on a foundational disagreement: whether information that can be derived from a public blockchain should ever be treated as non-public, regardless of the analytical sophistication required to extract it. A significant strand of opinion in the room held that on-chain information is intrinsically public, and that the analytical capacity required to interpret it is

comparable to the skill and resource gap that has always existed between sophisticated and retail participants in traditional markets. On this view, information solely derived from on-chain data should never be considered insider information, particularly given that retail participants can themselves learn to read blockchain data and that the tools to do so are increasingly accessible.

A parallel from traditional markets was raised: the case of a publicly traded company where a trader executed a transaction before the media announced the outcome of a court ruling. Because the ruling itself was open to the public, the trade was ultimately not considered insider trading, even though most market participants did not have practical access to the courtroom. This was offered as a precedent for the principle that information formally accessible in public should not be reclassified as non-public merely because access requires effort.

The distinction between insider trading and market manipulation was emphasized as a recurring source of confusion. In crypto markets, the concern most frequently materializes as pump-and-dump activity, which is closer to market manipulation than to classic insider dealing. Participants also noted that the picture is rarely purely on-chain: in most market-moving events such as M&A, token launches, and NFT releases, price movement is typically observable in advance of the public announcement, but this often reflects a combination of on-chain analytics and off-chain information, including leaks and informal disclosures that are not themselves derived from the blockchain. The interaction of on-chain and off-chain data was therefore identified as central to any honest assessment of where insider trading occurs in practice.

Participants also raised the layered nature of access to information across the ecosystem, noting that different actors hold different informational positions at different stages, from token issuers and core developers, to CASPs handling listing and onboarding, to validators with mempool visibility, to analytics firms with wallet attribution capabilities. A meaningful regulatory approach to inside information in this environment would need to account for these layers rather than treating all market participants as occupying a single informational plane. The absence of case law specifically defining insider trading in the crypto and tokenized asset context was noted as a significant gap, leaving the industry to operate on inferences drawn from traditional financial markets jurisprudence that may not transpose cleanly to on-chain markets.

A practical observation closed the discussion: producers of information that may, if leaked, move markets need to be particularly careful about their internal handling practices, regardless of where the formal regulatory line ultimately falls. Investors with sensitive knowledge performing a material transaction which likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset in the crypto market comparable to the traditional market (e.g. crossing specific thresholds of token shares of an issuer)

Investors with sensitive knowledge performing a material transaction which likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset in the crypto market comparable to the traditional market (e.g. crossing specific thresholds of token shares of an issuer) may need to follow similar reporting obligations (e.g. short or long selling disclosure obligations) as investors in traditional finance, provided that NCAs have put in place practical reporting infrastructure and guidance. may need to follow similar reporting obligations (e.g. short or long selling disclosure obligations) as investors in traditional finance, provided that NCAs have put in place practical reporting infrastructure and guidance. The combination of partial regulatory clarity and significant supervisory uncertainty means that internal information barriers, trading restrictions for staff with privileged visibility, and conduct-based monitoring are the most practical tools available to CASPs and other actors in the meantime.

Calls to Action regarding Inside Information in Blockchain Markets

The key calls to action from the discussion are:

- **Clarify the boundary of "public" information for blockchain-derived data:** Regulators and industry should develop shared standards on when blockchain-derived information meets the precision threshold under Article 87(2) and whether technically public but analytically inaccessible data may still constitute non-public information, recognizing that a default treatment of on-chain data as inherently public is the more defensible starting point absent clear evidence of structurally inaccessible analytical capacity.

- **Embed conduct-based supervisory focus and operational safeguards within CASPs:** Supervisors should orient enforcement toward identifiable abusive conduct patterns such as front-running and misuse of privileged order-flow visibility, rather than attempting to categorize every form of blockchain-derived information as inside information. In parallel, CASPs should implement tiered internal information barriers, have insider trading lists completed, train personnel,have insider trading lists completed, train personnel, restricted trading and cooling-off periods for personnel with access to market-sensitive operational information, and enhanced internal surveillance proportionate to their informational position in the ecosystem.

- **Account for the layered structure of informational access in the crypto ecosystem:** Any regulatory or supervisory framework on inside information in

crypto markets should reflect the layered nature of access, distinguishing between token issuers, CASPs, validators, analytics firms, and investorsinvestors, and calibrating obligations to the actual informational advantage held at each layer rather than treating all participants as informationally equivalent. Investors with sensitive knowledge performing a material transaction which likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset in the crypto market comparable to the traditional market (e.g. crossing specific thresholds of token shares of an issuer) may need to follow similar reporting obligations (e.g. short or long selling disclosure obligations) as investors in traditional finance, provided that NCAs have put in place practical reporting infrastructure and guidance. Investors with sensitive knowledge performing a material transaction which likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset in the crypto market comparable to the traditional market (e.g. crossing specific thresholds of token shares of an issuer) may need to follow similar reporting obligations (e.g. short or long selling disclosure obligations) as investors in traditional finance, provided that NCAs have put in place practical reporting infrastructure and guidance.

3. 3. Prediction Markets and MiCAR Market Abuse Rules

The third topic was presented by Dr. Nina-Luisa Siedler (siedler legal and DAAvern) and addressed a regulatory grey zone that has come into sharper focus following recent reporting on alleged insider-style activity in blockchain-based prediction markets: how, and under which regime, market abuse rules apply to instruments that sit between gambling, derivatives, and crypto-assets.

The framing of the problem drew on a recent report published by the data analytics firm Bubblemaps describing alleged insider-style betting on a Polymarket market tied to Iran-war events, including connected accounts that reportedly earned more than $2.4 million with a 98% win rate, alongside a separate case involving betting on military events using what was described as classified information. The core point of the report was that prediction markets can reward access to non-public information in much the same way that securities markets do, even though the products and legal labels are different.

This raises a structural question about the regulatory perimeter. A blockchain-based prediction-market position token could arguably satisfy MiCAR's crypto-asset definition: it is digitally represented, transferable, stored on-chain, economically valuable, and tradable. On that view, many decentralized prediction-market positions may technically qualify as crypto-assets. However, MiFID II financial instruments are not covered by MiCAR but by MAR

which prevails MiCAR even if the financial instrument is tokenized. Within the financial instruments categories, derivative contracts may be the most plausible classification for event-linked outcome shares. MiFID II expressly covers options, futures, swaps, forwards, and other derivative contracts relating to securities, currencies, interest rates, yields, emission allowances, indices, measures, commodities, and other assets, rights, obligations, indices, and measures, including those settled in cash or physically where the legal conditions are met. If the position is a transferable crypto-native position that is not legally a financial instrument, MiCAR may apply as the residual crypto-assets regime. If it is simply a bet on an uncertain event without an instrument or transferable crypto-asset, national wagering law may be the fall-back.

The grey zone is that prediction markets can function like price-discovery markets while escaping the conceptual vocabulary of both MiCAR and MAR. They may be marketed as wagers, built on crypto rails, and traded anonymously, yet the economic harm from insider access is the same as in classic market abuse: unfair informational advantage, distorted prices, and a loss of trust. The current framework therefore risks under-regulating harmful conduct simply because the product sits between regulatory categories.

The framing offered for resolving this was that the behavior is not legally "safe" just because the product is called a prediction market; the real issue is the regulatory classification of the instrument and the venue. If a prediction market falls within MiCAR's perimeter, conduct based on non-public, price-relevant event information would strongly resemble the abuse MiCAR is designed to prevent, particularly where there is deception, unlawful disclosure, or manipulation around a traded crypto-asset. If the market is instead treated as offering financial instruments, MAR would likely be the cleaner fit, since MAR expressly prohibits insider dealing, unlawful disclosure of inside information, and market manipulation for financial instruments. In either case, the conduct itself is the regulatory concern, and the classification exercise should follow the economic substance of the position rather than the label applied by the platform.

The discussion that followed confirmed the problem as genuine and difficult to resolve under existing categories. There was agreement that this is clearly a problem that needs to be addressed, and that it is not currently clear whether the relevant conduct would be governed by MiCAR or by MAR. A significant portion of the conversation focused on whether prediction markets are properly classified as gambling, and whether the event-linked outcome positions they offer could be understood as a form of binary option, which would draw them more clearly into the MiFID II derivative perimeter and therefore into MAR's market abuse regime.

A recurring point was that the analytical exercise of classification cannot be avoided, but that classification alone does not resolve the policy concern. Even where a prediction-market position can be defended as a wager rather than an

instrument under one Member State's wagering law, the cross-border nature of these platforms and the on-chain transferability of positions mean that the protection afforded by national wagering frameworks is fragile in practice. Participants noted that the economic harm at issue, the exploitation of non-public information to take a position before it is reflected in price, is structurally the same whether the underlying instrument is labelled a token, a derivative, or a bet, and that the regulatory framework should be capable of addressing the conduct rather than being defeated by the label.

The discussion also connected this topic to the broader theme of the day. As with the question of when blockchain data becomes inside information, the prediction-market issue is ultimately about whether the regulatory framework can address abusive conduct in markets that did not exist when its conceptual categories were designed. A conduct-based supervisory approach, focused on identifiable abusive patterns regardless of the product label, was identified as the most promising path forward in the short term, alongside clearer interpretive guidance on the classification of prediction-market positions under MiCAR, MiFID II, and national gamblinggambling law.

Calls to Action regarding Prediction Markets and Market Abuse

The key calls to action from the discussion are:

- **Clarify the regulatory classification of prediction-market positions across MiCAR, MiFID II, and national gamblinggambling law:** Regulators and industry should work toward shared interpretive guidance on when blockchain-based prediction-market positions fall within MiCAR's crypto-asset definition, when they qualify as MiFID II financial instruments (in particular as derivative contracts, perpetuals, perpetuals or binary options), and where national gamblinggambling law remains the residual framework, ensuring that the classification follows the economic substance of the position rather than the label applied by the platform.

- **Apply MAR and MiCAR market abuse provisions to prediction markets within their respective perimeters:** Where prediction-market positions qualify as financial instruments, MAR's prohibitions on insider dealing, unlawful disclosure, and market manipulation should be enforced consistently. Where they qualify as crypto-assets under MiCAR, the equivalent provisions on insider dealing and market manipulation should apply. Conduct based on non-public, price-relevant

event information should not be treated as legally permissible simply because the venue is marketed as a prediction market.

- **Adopt a conduct-based supervisory approach to abusive activity in event-linked markets:** Supervisors should focus on identifiable abusive conduct patterns, including trading on non-public information about events affecting outcome positions, regardless of the formal classification of the instrument. This conduct-focused approach is the most practical response to the structural difficulty that prediction markets sit between regulatory categories and may otherwise escape the market abuse vocabulary of both MiCAR and MAR.

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

Alireza Siadat (Deloitte), Cecile Sturich, Dan Haj (Merkle Science), Christopher Grihault des Fontaines (DFNS), Elvins Folkebrant Sababi (Somnia), Erik Vesterlund (Regport), Erika Stanford (CMS), Hanna Raftell (Stratum), Isak Nyberg (Centiglobe), Jacqueline Cooper (DARA), Karola Kassai (KassaiLaw), Kate Voogla (CryptoSwift), Magnus Jones (Nordic Blockchain Association), Marc Oris (GANN Labs), Marcus Mølleskov (Januar), Marie Rinke (Möhrle Happ Luther), Martin Wichman (Kvarn), Mats Brodén (Nordic Powerhouse), Nina-Luisa Siedler (siedler legal and DAAvern), Pawl Laskarzewski (Nomad Fulcrun), Raido Saar (Comply Once), Tommaso Astazi (Blockchain4Europe), Uve Poom (CryptoSwift).