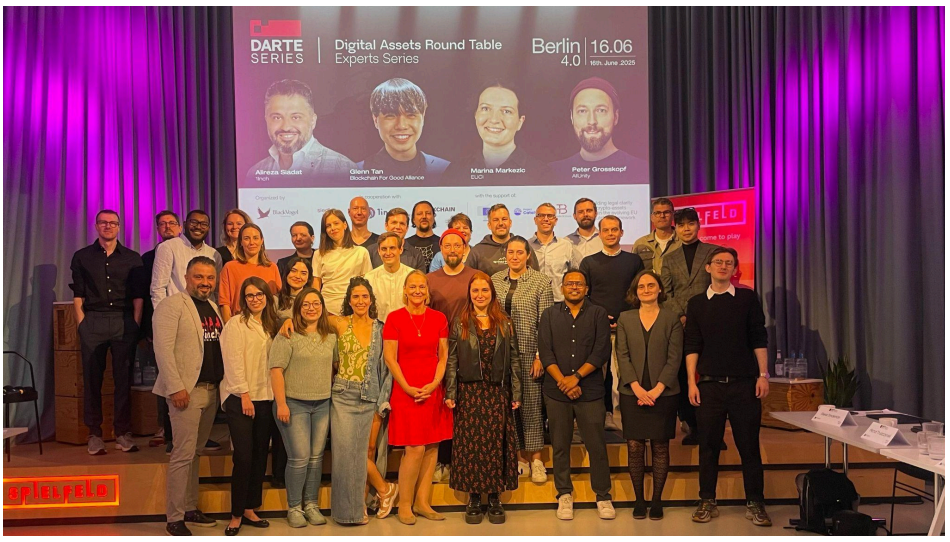
# DARTE SERIES

## Berlin 4.0

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

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

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



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

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

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

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

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

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

Participants flagged several pressing legal ambiguities:

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

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

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

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

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

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

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

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

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

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

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

**Call to actions regarding regulatory clarity for DeFi interfaces**

The key call to actions from the discussion are:

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

2. **DeFi Security and Risk Management**

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

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

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

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

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

**Call to Actions regarding DeFi risk management**

The key call to actions from the discussion are:

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

3. **DeFi Interfaces**

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

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

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

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

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

**Call to Actions regarding DeFi interfaces and decentralization**

The key call to actions from the discussion are:

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

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

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