DARTE SERIES

Berlin 3.0

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU Markets in Crypto-Assets Regulation (MiCAR). Over time, the series has expanded to cover not only MiCAR but also other emerging regulatory frameworks and region-specific issues relevant to the crypto-asset ecosystem.

The Berlin 3.0 DARTE edition was held on June 13th, 2025, at HTW Berlin, in collaboration with the European Commission, Project Catalyst, and HTW Berlin. It took place alongside the 10th Blockchain@HTW Conference.

The session featured in-depth discussions on three critical themes: the criminalization risks of smart contract development (Judith de Boer, Hertoghs Advocaten), legal pathways for recognizing DAOs as compliant Web3 communities (Joachim Schwerin, European Commission), and the regulatory tension between GDPR and decentralized blockchain infrastructures (Gustav Hemmelmayr, Parity Technologies). We extend our sincere thanks to all speakers and participants for their contributions, and to HTW Berlin for hosting the event.

This report synthesizes the core insights and recommendations from the discussions. It is important to note that the views expressed herein reflect the collective outcomes of the roundtable and not the formal positions of individual participants or their respective organizations.

1. Coding as a Criminal Act?

The first topic of the Berlin 3.0 roundtable, introduced by Judith de Boer of Hertoghs Advocaten, explored the legal implications of developing and deploying autonomous smart contract systems, particularly in light of recent prosecutions such as the Tornado Cash case. The discussion centered on the boundaries of criminal liability for developers whose decentralized tools can be used for both lawful and unlawful purposes.

Participants emphasized that smart contracts, while merely code, can facilitate the transfer of billions in value autonomously. This presents a legal dilemma: at what point does writing immutable and unstoppable code constitute a criminal act? In the Tornado Cash case, a Dutch court concluded that the developers of the protocol, by intentionally designing and deploying an anonymizing privacy enhancing tool without KYC/KYT mechanisms, bore responsibility for the laundering of over 500,000 ETH from criminal origins.

The court argued that the developers' continued involvement in maintaining and promoting the protocol, combined with knowledge of criminal use, amounted to conditional intent ("voorwaardelijk opzet") under Dutch law. The immutability of the smart contracts was deemed a deliberate design choice, not a shield from liability. This finding has sparked concern among developers and legal professionals, who fear that similar interpretations could criminalize neutral or even beneficial tools depending on their use.

Participants discussed whether a tool could be inherently criminal if it is especially suitable for unlawful acts, even when it serves legitimate privacy functions and is not criminalised by law. They also debated the legal consequences of not embedding compliance measures into interfaces and questioned how legal certainty can be preserved in a world of open-source, decentralized innovation.

Challenges Identified

- Traditional concepts of "operator control" do not map well onto decentralized technologies, where governance is distributed and no single entity may have the ability, or legal authority, to halt or modify operations. This disconnect creates legal uncertainty when trying to assign responsibility using frameworks designed for centralized actors.

- Criminal liability frameworks struggle to accommodate code as an autonomous actor, particularly when smart contracts are deployed on immutable infrastructure. This raises foundational questions: Can accountability rest solely with the original developer, or must it consider governance mechanisms, ongoing involvement, and community control?

- Developers face significant legal exposure even in the absence of malintent, particularly when protocols are designed without embedded compliance features even though compliance is not required by law. The absence of

such features, while often a deliberate choice to preserve neutrality or privacy, seem to be interpreted as willful negligence in jurisdictions applying conditional intent standards.

- The lack of ex-ante regulatory guidance exposes open-source contributors to disproportionate post-hoc enforcement risk. In practice, developers operate in a regulatory vacuum where norms are defined retroactively through prosecution, not policy, undermining both legal certainty and innovation incentives.

Moreover, liability may be unevenly enforced across jurisdictions, depending on prosecutorial discretion, the interpretation of intent, and the national stance on privacy tools. This uneven playing field creates fragmentation and forum-shopping risks for developers and platforms alike.

Finally, participants noted a growing ambiguity between tool-building and service-provision. The more a developer maintains a project's interface, markets the tool, or manages relayer infrastructure, the more likely courts are to see them as operators rather than neutral technologists, a distinction that remains blurry and underdefined.

Participants agreed that legal clarity must catch up with technological realities. Developers should not be criminalized for contributing to decentralized ecosystems unless they knowingly enable and directly facilitate criminal activity. Decentralised tools should not be treated differently than other tools that can have multiple uses.

Regulators and courts should distinguish between bad actors and genuine innovators. A technology-neutral, principles-based framework is needed to preserve the benefits of decentralization while addressing legitimate law enforcement concerns. The Tornado Cash precedent underscores the urgency of clear legal boundaries.

Call to actions regarding criminal liability in decentralized development

The key call to actions from the discussion are:

- **Publish clear ex-ante guidance on developer liability:** Urge national and EU authorities to define the limits of criminal responsibility for developers of open-source smart contracts, focusing on intent and the presence of compliance safeguards. A call to action in this regard is the Digital Freedom Declaration (https://digitalfreedom.page).
- **Draw technology-neutral legal standards:** Establish criteria that reflect the unique structures of decentralized systems, ensuring that liability is linked to specific actions and responsibilities, not merely the creation of code.
- **Protect the principle of legal certainty:** Advocate for jurisprudence and enforcement actions that respect lex certa, ensuring that developers are not punished for conduct that was lawful and widely accepted at the time of creation.
- **Recognize dual-use technology:** Promote balanced regulatory approaches that acknowledge both the legitimate and illicit use cases of privacy-enhancing tools like mixers, avoiding overreach that could chill innovation.

2. DAOs as Compliant Web3 Communities

The second topic of the Berlin 3.0 roundtable, introduced by Joachim Schwerin, Principal Economist at the European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW), focused on the legal ambiguity surrounding the status and structure of Decentralized Autonomous Organizations (DAOs) in Europe.

The discussion examined the limitations of current legal wrappers, the absence of a DAO-specific regulatory framework, and emerging solutions that combine collective identity, on-chain governance, and external representation.

Key Regulatory and Structural Challenges

Participants highlighted the growing presence of DAOs across sectors, from DeFi to the social economy, and emphasized their functional similarities to offline cooperatives. Yet, unlike cooperatives, DAOs lack clear legal recognition. This forces projects to rely on suboptimal legal forms or remain outside the formal economy altogether.

Common issues raised included:

1. **Jurisdictional uncertainty:** DAOs operate globally but lack a clear framework for which national rules apply. Formal registration in one country often does not provide cross-border recognition.
2. **Undefined liability:** With no identifiable management or fixed membership, it's unclear who bears legal responsibility. Some participants suggested "collective liability" mechanisms supported by digital governance logs.
3. **Representation gap:** Without physical legal persons to interface with states, DAOs face difficulties in managing taxes, social contributions, or contractual obligations.
4. **Lack of minimum standards**: DAOs vary widely in size and complexity, from chatrooms to proto-states, requiring flexible, horizontal requirements that adapt to their function.

Drawing from sandbox use cases, the BlackVogel & Blockstand DAO studies and 2024 GROW study, the group outlined several building blocks for compliant DAO structures:

- **Digital Collective Identity**: Establish a unique and verifiable identifier for the DAO, combining on-chain membership records with off-chain verification methods such as EBSI-based attestations. This preserves pseudonymity while enabling accountability.
- **On-chain Governance Disclosure:** DAOs should document essential governance parameters, such as voting mechanisms, token distribution models, decision-making structures, and upgrade procedures, in a standardized format. This could resemble MiCAR-style white paper disclosures, ensuring external parties and members can assess the DAO's operational and risk profile.
- **Selective Disclosure with ZKPs:** To balance transparency with privacy, participants explored how zero-knowledge proofs and similar cryptographic tools could enable selective disclosure. These mechanisms would allow DAOs to prove regulatory compliance (e.g., identity requirements, financial controls) without revealing sensitive or personally identifiable information.
- **Orphan Fund Representation:** Use "Sachwalter" structures, where independent entities administer DAO assets without being part of the DAO. These can handle legal duties (e.g. taxes, compensations) on behalf of the DAO without altering its decentralised nature.
- **Flexible Legal Wrappers:** Explore adaptation of existing cooperative statutes (e.g., EU SCEs), foundations, or develop an optional regime. Each option must account for liability, ultimate beneficial owner identification, and AML compliance.

Integration with International Policy Trends

The roundtable echoed findings from broader industry research comparing DAO regulatory frameworks across jurisdictions. While DAO-specific legal forms are beginning to emerge, such as the Wyoming DAO LLC and Marshall Islands structures, these remain fragmented and inconsistent. Participants agreed that uniform standards on AML/KYC, taxation, and legal representation are essential to avoid jurisdiction shopping and to foster the legitimacy of DAOs within existing regulatory systems. It was also noted that regulatory sandboxes and modular legal templates could play a valuable role in supporting DAOs during their early growth stages, offering a pathway to compliance while minimizing legal risk. In this regard, the three DAO use cases in the upcoming third cohort of the European Blockchain Regulatory Sandbox will deepen these reflections.

Participants emphasized that DAOs will persist and scale regardless of recognition, but lack of legal clarity increases risk and stifles legitimate activity. Any European framework must be flexible enough to support experimentation while offering robust protections for DAO participants and third parties.

Call to actions regarding legal frameworks for DAOs

The key call to actions from the discussion are:

- **Establish standardized DAO governance principles and classification models**: Develop a unified taxonomy for DAOs based on their purpose (e.g., Non-Profit, Investment-focused, Community-driven) and governance structure (e.g., member-managed, algorithm-managed). This should be accompanied by core governance standards, such as transparency rules, trustee duties, and baseline documentation requirements, to guide compliant DAO operations across jurisdictions and support legal recognition.
- **Launch an EU-wide cross-jurisdictional DAO sandbox**: Create a regulatory sandbox specifically designed for DAOs, enabling experimentation with novel governance models, on-chain identity, and decentralized financial operations in a supervised, legally coherent environment. This would allow regulators and DAOs to test flexible compliance pathways while gathering the insights needed for broader legal integration.
- **Translate sandbox findings into a future-proof, tech-neutral legal framework**: Use learnings from the DAO sandbox to inform the development of a "28th regime" or optional DAO legal wrapper at EU level. This framework should be

technology-agnostic—relying on broad legal concepts like "Trustworthy Technology"and designed to accommodate rapid innovation while providing legal certainty and enforceable protections for participants and third parties.

3. Personal Data and Blockchain

The third topic of the Berlin 3.0 roundtable, introduced by Gustav Hemmelmayr, Senior Legal Counsel at Parity Technologies, focused on the regulatory tension between GDPR and public, permissionless blockchain infrastructures. The discussion centered on the European Data Protection Board's Guidelines 02/2025 and their implications for decentralized technologies.

Participants noted that although GDPR is a technology-neutral regulation in theory, in practice it remains deeply rooted in centralized data-processing assumptions. Public permissionless blockchains, which do not rely on data collection or identifiable intermediaries, challenge these assumptions. The recent EDPB guidelines fail to account for how decentralized systems actually function and place undue burden on infrastructure-level data like addresses and hashes.

A recurring theme was the distinction between infrastructure data and personal data. While a blockchain address may be seen as personal data when collected and linked to an individual off-chain (e.g., by exchanges or custodians for their KYC processes), that same address used anonymously on-chain should not be treated as personal data. Participants stressed that current interpretations blur this distinction, threatening to classify infrastructure data as inherently personal, undermining the possibility of privacy-by-design implementations.

Three main argumentation lines shaped the roundtable:

1. **Intermediaries and Privacy Risk**: Blockchain transactions generally do not require or reveal personal information unless intermediaries (e.g., custodial wallets, exchanges) collect and link data for regulatory compliance. These off-chain actors, rather than the blockchain infrastructure itself, should be the focus of GDPR compliance and liability.

2. **Infrastructure as Neutral Layer:** Public permissionless blockchains function like public utilities (e.g., a calendar or addresses on a map). Just as a calendar date is infrastructure to measure time independently from individual's links to a certain date (like their birthday), a blockchain address is anonymous infrastructure data on that blockchain even if someone offchain collects certain addresses as part of their data collection around a person. Destroying the infrastructure or restricting its usage due to potential personal data linkage is disproportionate

and ignores the neutral, anonymous and privacy-preserving nature of these decentralized systems.

3. **Expansive Interpretations of Personal Data:** Authorities' tendency to classify nearly all data as personal, even inherently anonymous data like cryptographic hashes, was criticized as impractical and counterproductive. Participants argued that a policy framework rooted in absolute identifiability undermines both technological neutrality and innovation, particularly in contexts where blockchain enhances, rather than threatens, user privacy.

Participants emphasized the urgent need for a recalibration of regulatory interpretations to enable privacy innovation without undermining fundamental rights or system integrity.

Call to actions regarding GDPR and decentralized technologies.

The key call to actions from the discussion are:

- **Reframe the legal interpretation of infrastructure data**: Advocate for a narrow interpretation of GDPR that excludes anonymous, infrastructure-level data from the definition of personal data. Public blockchain addresses or hashes used in privacy-preserving systems should not be treated as inherently personal.
- **Center regulatory responsibility on intermediaries**: Emphasize that GDPR rights and duties should apply primarily to data-collecting intermediaries who establish off-chain links to individuals. Blockchain infrastructure itself should not be held liable for personal data processing it does not perform.
- **Restore and reinforce technological neutrality in privacy regulation**: Encourage regulators to revisit GDPR principles through a teleological lens, recognizing privacy-by-design solutions embedded in blockchain technologies as aligned with the aims of the regulation. Challenge overly broad interpretations that hinder innovation and increase systemic risk.

We thank all participants of the Berlin 3.0 DARTE event for contributing to the discussion:

Arslan Brömme, Ameen Soleimani, Andrew Forson (DeFi Technologies), Bota Jardemalie, Daniela Boback (Bundesblock), Florian Daniel (Westernacher), Frederic Hannesen (M0), Dr.

Friedrich Popp (Popp Law), Gustav Hemmelmayr (Parity Technologies), Jacob Senftinger (SafeWallet), Janine Roemer, Joachim Schwerin (European Commission), Dr. Jörn Erbguth, Judith de Boer (Herthogs advocaten), Mariana de la Roche Wills (BlackVogel), Markus Kluge (tokenforge), Matthias Bauer-Langgartner (Chainalysis), Nuno Lima da Luz (Associação Portuguesa de Blockchain e Criptomoedas), Nurtilek Taalaibekov (CertiK), and Silvan Jongerius (TechGDPR).