Beaumont Capital Markets

www.beaumont-capitalmarkets.co.uk

GERMANY

MiCAR Implementation, eWpG Practice and the Regulation of DeFi and DAOs

PWC

Dr. Michael Huertas
Partner

michael.huertas@pwc.com

+49 160 97375760

www.pwc.com

BIO

Dr. Michael Huertas is a partner and the global and European Financial Services Legal Leader at PwC Legal. Michael advises financial services firms, crypto-asset service providers and issuers, as well as multinational corporations, on a wide range of cross-border banking and finance, capital markets, structured finance and derivatives transactions, as well as complex financial regulatory, supervisory and enforcement matters. He is qualified and practises as a solicitor advocate (England and Wales), solicitor (Ireland) and as a Rechtsanwalt/attorney-at-law (Germany). Michael frequently speaks at conferences and publishes on global financial regulatory issues.

pwc

PWC

Dr. Hagen Weiss
Senior Manager

hagen.weiss@pwc.com

+49 151 1570 8446

www.pwc.com

BIO

Dr. Hagen Weiss is a lawyer and former Federal Government Director and - with a PhD in DLT systems theory - specializes in the law of crypto assets. He is one of the leading lawyers in the field of digital finance and crypto assets - particularly in matters relating to DLT and blockchain in connection with financial institutions and technology companies, as well as issues relating to the German eWpG, the Markets in Crypto Assets Regulation (MiCAR), the EU DLT pilot program, and decentralized finance (DeFi). As a federal official, he has contributed significantly to the regulatory and legal framework for crypto assets in Germany, at the European and international level. In addition, he has been involved with the underlying technology for many years and is familiar with its actual technological features and developments. Having worked as a civil servant for federal authorities and the Federal Ministry of Finance, Hagen Weiss also has extensive knowledge and experience in advising on strategic regulatory decisions.

pwc

MiCAR Implementation, eWpG Practice and the Regulation of DeFi and DAOs

Overview

Germany's digital assets regime in 2026/27 is built upon three pillars: EU harmonisation through MiCAR and related regulations; national financial regulatory law applied functionally to token-based models; and corporate and civil law innovations enabling tokenised issuance and governance, most notably the eWpG. Together, these create a clear, if demanding, perimeter for centralised crypto-asset activities and tokenised securities. This framework is paired with a deliberately cautious approach to decentralised finance ("**DeFi**")-financial services built on public blockchain infrastructure that operate through smart contracts with reduced or absent centralised intermediation- and Decentralised Autonomous Organisations ("**DAOs**")-blockchain-based organisational structures governed by rules encoded in smart contracts and typically administered through token-holder voting. Market development remains robust in the tokenisation of real-world assets and institutional custody, whilst retail-facing activities are increasingly channelled through licensed entities subject to stricter marketing and disclosure controls.

> "
>
> Germany's 2026/27 digital assets regime creates a clear, if demanding, perimeter for centralised crypto-asset activities and tokenised securities, while maintaining a deliberately cautious approach to DeFi and DAOs.

MiCAR in practice: authorisation, disclosure and ongoing supervision

By 2026, MiCAR's regime for CASPs is fully operational. In Germany, BaFin and the Deutsche Bundesbank coordinate prudential, conduct and operational risk oversight for banks and CASPs within their respective remits. To obtain authorisation, CASPs must demonstrate effective governance, safeguarding of clients' crypto-assets, segregation and reconciliation controls, prudential own funds commensurate with operational risk, and outsourcing frameworks with clear responsibility retention. Conflicts of interest-particularly in vertically integrated models that combine exchange, custody, proprietary trading and market-making functions-remain a central supervisory theme, with structural separation or robust controls required to address them.

White paper obligations for public offerings and admissions to trading require detailed risk disclosures covering protocol risks, governance risks, legal enforceability, custody, key management, liquidity, and market manipulation risks. Liability for misleading or incomplete disclosures attaches to issuers and, where applicable, to platform operators facilitating admissions to trading. For ARTs and EMTs, supervisors scrutinise redeemability, reserve composition, investment rules, and disclosure frequency. Reserve assets must be high-quality and liquid, and conflicts of interest in reserve management must be avoided. Significant tokens-those designated by the EBA as posing heightened risks to financial stability, monetary policy or consumer protection due to their scale or interconnectedness-face enhanced oversight and potentially tighter restrictions on non-bank issuers.

NFTs and utility tokens: MiCAR exclusions and supervisory approach

MiCAR excludes certain categories of crypto-assets from its scope, notably non-fungible tokens ("**NFTs**") and utility tokens providing access to specific goods or services. For NFTs, the exclusion depends on genuine non-fungibility; tokens issued in large series or collections, or those that are effectively interchangeable, may not qualify and could fall within MiCAR's perimeter. BaFin applies a substance-over-form approach, examining whether an NFT functions as a unique digital collectible or whether it is, in economic reality, a fractionalised investment, payment instrument, or means of capital-raising. Where NFTs confer rights to underlying assets, revenue streams, or governance participation, they may be recharacterised as crypto-assets, securities, or financial instruments and subjected to the applicable regulatory frameworks.

Utility tokens granting access to a product or service supplied by the issuer benefit from a lighter-touch regime under MiCAR, with reduced white paper requirements and no authorisation obligation, provided the token is accepted only by the issuer or a limited network. However, this exclusion is narrowly construed: tokens tradable on secondary markets, those conferring speculative or investment characteristics, or those marketed with an expectation of profit may lose their utility token status. In Germany, BaFin's functional analysis also considers whether a utility token might constitute an e-money instrument, payment service, or financial instrument depending on its features and use cases. Issuers must therefore undertake careful legal analysis prior to launch, and ongoing monitoring is advisable where token functionality or market dynamics evolve post-issuance.

ESG and sustainability disclosures

MiCAR requires crypto-asset white papers to include information on the principal adverse environmental and climate-related impacts of the consensus mechanism used to validate transactions. For crypto-assets relying on proof-of-work or other energy-intensive validation methods, this disclosure obligation is material and may influence investor and institutional appetite. The European Securities and Markets Authority ("**ESMA**") has developed regulatory technical standards specifying the content, format and presentation of sustainability disclosures, including quantitative indicators where available. In Germany, institutional investors subject to sustainable finance disclosure requirements under the SFDR and related frameworks increasingly factor the environmental profile of crypto-assets into portfolio construction and due diligence, particularly for funds with ESG mandates or sustainability labels.

Beyond mandatory disclosure, market pressure and reputational considerations are driving adoption of more sustainable blockchain infrastructures. Proof-of-stake and other low-energy consensus mechanisms are increasingly preferred for new tokenised issuances, and some institutional custodians have adopted policies limiting exposure to assets validated through high-energy protocols. For tokenised securities under the eWpG, the choice of underlying DLT infrastructure is often influenced by sustainability considerations alongside performance, scalability and regulatory acceptance. As the regulatory landscape evolves, further integration of sustainability metrics into ongoing reporting and supervisory expectations is anticipated.

eWpG and tokenised securities: issuance, registries and lifecycle

The eWpG's legal foundation for electronic securities has scaled materially. Issuers may choose between central electronic registers (maintained by a central securities depository or other authorised entity) and crypto-securities registers maintained on distributed ledger technology ("**DLT**"). The latter requires a registered crypto-securities register keeper, subject to regulatory authorisation and ongoing supervision, with statutory duties regarding the accuracy, integrity, and availability of the register. Legal equivalence between electronic and paper-form securities allows corporate actions, collateralisation, and transfer of title to proceed on-chain with certainty. Conflict-of-law rules clarify the applicable law based on the situs of the register and the governing law specified by the issuer.

"

Legal equivalence between electronic and paper-form securities allows corporate actions, collateralisation, and transfer of title to proceed on-chain with certainty.

In practice, German issuers leverage private, permissioned DLTs for control and performance, with interoperability solutions enabling interface with custodians, central securities depositories ("**CSDs**") operating under the DLT Pilot Regime, and traditional settlement systems. Liability allocation between the issuer, registrar, and technology providers is delineated both contractually and statutorily, with insurance and indemnities being standard for operational errors. As shares and fund units increasingly fall within the eWpG's scope, corporate law matters-such as voting, meeting formalities, and shareholder rights-are being operationalised through smart-contract-enabled registries, with careful mapping to German corporate law requirements.

Market integrity and surveillance

Germany applies market abuse principles to tokenised securities and expects platforms authorised under MiCAR to emulate the surveillance controls of traditional markets, adapted for on-chain idiosyncrasies such as cross-venue fragmentation, pseudonymous activity, and on-chain information asymmetries. Inside information policies must account for on-chain governance proposals, protocol upgrades, and decisions affecting a token's supply or utility. Surveillance tooling must detect wash trading (the practice of simultaneously buying and selling the same asset to create misleading market activity), spoofing (placing orders with the intent to cancel before execution to manipulate prices), and cross-venue manipulation across both centralised and decentralised liquidity pools. Whistleblowing frameworks and incident escalation pathways are an emerging supervisory focus as more activity migrates on-chain.

> “
>
> BaFin has indicated that decentralisation is not a safe harbour; regulatory characterisation is determined by factual control and economic function.

AML/CFT and the crypto travel rule

The integration of the travel rule-the requirement under the TFR for information on originators and beneficiaries to accompany crypto-asset transfers-into German practice has standardised data collection and transmission for crypto-asset transfers. CASPs must screen inbound and outbound transfers for incomplete originator/beneficiary information, manage transfers involving unhosted wallets (also known as self-custodied wallets, where private keys are held directly by the user rather than by a CASP or other intermediary) through risk-based measures, and suspend or reject transfers lacking sufficient information. Banks offering crypto services have harmonised their sanctions screening and transaction monitoring for on-chain activity with existing payment rails, including customer risk-scoring that incorporates wallet heuristics, protocol risks, and typologies such as ransomware, darknet marketplaces, and mixing services (services that pool and redistribute crypto-assets to obscure their transactional history). Whilst cross-border coordination has improved, residual frictions remain with non-EU virtual asset service providers (“VASPs”) not aligned to EU standards.

DeFi: supervisory posture and perimeter issues

No German statute specifically regulates DeFi as such; instead, the supervisory approach is functional and activity-based. Where a protocol or its human promoters perform activities constituting regulated services-deposit-taking, lending, custody, operating a multilateral trading facility (“MTF”, a system bringing together multiple buying and selling interests in financial instruments), portfolio management or placing-licensing and conduct obligations can attach regardless of technological form. If tokens issued or traded through a protocol qualify as securities or financial instruments, prospectus, MiFID II conduct and market abuse regimes may apply. For stablecoin-like instruments deployed via DeFi, MiCAR's ART or EMT rules are implicated where an identifiable issuer exists or where a third party offers the token to the public or seeks admission to trading.

Key supervisory questions include: who exercises control or influence over the protocol; whether front-end operators, governance token holders, or core developers perform regulated intermediation; and whether custody or client asset control is effectively centralised through admin keys, liquid staking (a mechanism whereby users stake crypto-assets through a protocol and receive a transferable token representing their staked position), or vault strategies. BaFin has indicated that decentralisation is not a safe harbour; regulatory characterisation is determined by factual control and economic function. German AML/CFT law can capture DeFi front-ends and facilitators where they act as obliged entities, and MiCAR's CASP perimeter may extend to interfaces that intermediate client orders, safeguard private keys, or charge fees for execution services.

In practice, compliant DeFi models in Germany are moving toward permissioned or semi-permissioned architectures featuring whitelisting, embedded know-your-customer (“KYC”) verification at the interface layer, and governance structures separating protocol parameter-setting from client intermediation. Institutional participation hinges on clarity over liability, the auditability of smart contracts, oracle risk mitigation (oracles being external data feeds supplying off-chain information to smart contracts), and alignment with outsourcing and ICT risk standards under DORA.

DAOs: Corporate law, liability and supervision

DAOs lack an express corporate form under German law. Consequently, they risk being treated as unincorporated associations (*nicht-rechtsfähige Vereine*) or partnerships (*Gesellschaften bürgerlichen Rechts*), with potential joint and several liability for active participants or promoters. Where DAOs issue tokens with economic or governance rights, securities and prospectus considerations arise; where DAOs operate protocols facilitating regulated activities, the individuals who effectively manage or benefit from such activities may be viewed as responsible persons for licensing and compliance purposes. The use of foreign wrappers (e.g., foundations or limited liability companies) to house DAOs does not preclude German regulatory reach where activities target German users or are performed in Germany.

A pragmatic path for DAOs engaging with German markets involves adopting a legal wrapper for limited liability, appointing accountable persons for regulatory interfaces, and segregating protocol governance from client-facing intermediation. Governance tokens offered to the public should be assessed for securities or other financial instrument characteristics, with appropriate disclosures and, where necessary, a prospectus or white paper. AML obligations can attach to the DAO's operational entities, and tax, employment, and consumer protection issues also arise where DAOs remunerate contributors or market services to retail users.

Insolvency and creditor protection

The treatment of crypto-assets in insolvency proceedings has attracted increasing attention as the market has matured and, in some cases, experienced failures. Under German insolvency law (*Insolvenzordnung*), the characterisation of crypto-assets as either assets of the insolvent estate or property held on behalf of clients is determinative of creditor outcomes. Where a CASP or custodian holds crypto-assets on a segregated basis for clients, those assets should in principle be subject to a right of separation (*Aussonderungsrecht*) and not fall into the insolvency estate, provided the segregation is both legally and operationally effective. This requires clear contractual arrangements, technical segregation of wallets and keys, accurate record-keeping, and compliance with MiCAR's safeguarding requirements. Where segregation is deficient or commingling has occurred, clients may instead rank as unsecured creditors with claims against the estate, substantially diminishing recovery prospects.

Recent insolvency cases involving crypto-asset service providers—both in Germany and internationally—have underscored the importance of robust custody arrangements and transparent disclosure of client asset treatment. German courts and insolvency administrators have grappled with practical challenges including tracing on-chain assets, enforceability of multi-signature arrangements, the status of staked or lent assets, and valuation of volatile holdings for distribution purposes. For tokenised securities issued under the eWpG, the register's integrity and the issuer's solvency interact to determine investor protection; the statutory framework provides for the register to serve as evidence of title, but investors remain exposed to issuer credit risk unless additional collateralisation or guarantee structures are in place. Market practice is evolving toward enhanced disclosure of insolvency treatment in client agreements, insurance coverage for custodial failures, and contractual safeguards anticipating administrator scenarios.

> “
>
> DAOs lack an express corporate form under German law and risk being treated as unincorporated associations or partnerships, with potential joint and several liability for active participants or promoters.

Technology risk, audits and assurance

Smart contract audits, formal verification and continuous monitoring are now expected for material protocols and tokenised issuance infrastructure. Change management around protocol upgrades and key rotations is increasingly supervised, with requirements for multi-signature controls (requiring multiple private key holders to authorise transactions), emergency pause procedures (balanced against decentralisation claims), and disclosure of known vulnerabilities and mitigation strategies. Custody models must evidence segregation, key ceremony controls (the formal procedures for generating, distributing and managing cryptographic keys), hardware security module (“**HSM**”) usage, and robust disaster recovery. Insurance markets for smart contract and custody risks have deepened, though coverage remains carefully circumscribed and contingent on security posture and governance quality.

Institutional custody and Spezialfonds developments

Germany's institutional custody market for crypto-assets has expanded significantly, underpinned by regulatory clarity and the entry of established financial institutions. Banks holding crypto custody licences under Section 1(1a) sentence 2 no. 6 of the German Banking Act (*Kreditwesengesetz*) compete alongside specialist digital asset custodians and international players establishing German-regulated subsidiaries. Institutional demand is driven by asset managers, insurance companies, pension funds and family offices seeking regulated access to digital assets within familiar operational and compliance frameworks. The extension of Spezialfonds—Germany's principal vehicle for institutional investment—to permit allocations to crypto-assets (up to 20 per cent of fund assets under certain conditions) has been a significant catalyst, enabling institutional investors to gain exposure without direct custody or operational complexity.

> "The extension of Spezialfonds to permit allocations to crypto-assets (up to 20 per cent of fund assets under certain conditions) has been a significant catalyst for institutional investment in digital assets."

Custodians are differentiating on the basis of security architecture, insurance coverage, asset breadth, staking and yield services, and integration with traditional securities infrastructure. Interoperability with CSDs operating under the DLT Pilot Regime, connectivity to institutional trading venues, and support for tokenised securities alongside native crypto-assets are increasingly important considerations. Operational due diligence by institutional investors focuses on key management practices, disaster recovery, regulatory standing, and the custodian's financial resilience. As the market matures, consolidation among custodians is anticipated, alongside continued innovation in custody technology, reporting capabilities, and value-added services such as collateral management and on-chain corporate actions processing.

Consumer and investor protection

Retail-facing activities attract heightened scrutiny. Risk warnings must be prominent and specific, fees must be transparent, and marketing materials must be consistent with white papers or prospectuses. Staking, yield products and lending services require careful articulation of risks, including counterparty risk, rehypothecation (the practice of using client assets as collateral for the service provider's own purposes), protocol risks and potential loss of principal. Product governance requires identifying target markets, stress-testing for liquidity and redemption shocks, and implementing distribution controls, particularly for complex or leveraged exposures. Complaints handling and redress mechanisms are relevant both under MiCAR and under general consumer protection law.

Intersections with payments, e-money and tokenised deposits

Banks and electronic money institutions ("**EMIs**") exploring tokenised payment instruments must map carefully between e-money, deposit and crypto-asset categories. Tokenised deposits remain deposits in substance and are supervised accordingly; EMTs issued by non-banks must meet redeemability and safeguarding rules; and privately issued payment tokens may fall within MiCAR, with restrictions on scale for significant tokens and additional obligations if used widely for payments. Interoperability with the Single Euro Payments Area ("**t**") and card networks raises additional scheme compliance and chargeback considerations. Programmable payments linked to tokenised assets, escrow and conditional settlement continue to be piloted under bank supervision, often leveraging permissioned DLT for compliance and performance.

Cross border and third country issues

MiCAR's passportability-the ability for a CASP authorised in one EU Member State to provide services across the EU without separate authorisation in each jurisdiction-simplifies intra-EU operations. However, third-country firms cannot directly serve EU clients without establishing an EU-authorised entity, barring limited reverse solicitation (where a client independently initiates contact with the service provider without prior marketing or solicitation). Germany applies these restrictions strictly. Outsourcing to third-country service providers-whether for custody technology, cloud services, key management or market surveillance-must satisfy oversight, data protection and exit requirements. For DeFi and DAOs, geofencing (using technical measures to restrict access based on geographic location) and interface-level controls are common approaches to managing EU user exposure where no EU authorisation exists. Cooperation with foreign supervisors on enforcement, sanctions and AML matters has intensified, with cross-border information exchange becoming a growing feature of investigations.

> “
>
> Third-country firms cannot directly serve EU clients without establishing an EU-authorised entity, barring limited reverse solicitation.

Outlook: policy and market trajectory for 2026/27

Continued convergence between tokenised securities infrastructure and traditional market infrastructures is expected, alongside broader application of the eWpG to equity and fund instruments at scale, and the crystallisation of MiCAR supervisory practice through enforcement and Level 2 technical standards (the detailed implementing and regulatory technical standards adopted by the European Commission on the basis of drafts prepared by the European Supervisory Authorities). DeFi-facing policy is likely to evolve through guidance, consultations and targeted enforcement rather than statute, focusing on custody, intermediation, disclosures and AML/CFT, with potential future revisions to MiCAR informally referred to as “MiCAR 2”. For DAOs, the legal wrapper trend will persist, alongside governance professionalisation and clearer accountability lines. Germany's competitive position will rest on its ability to combine legal certainty with operational scalability-areas where banks and regulated fintechs jointly advancing tokenised issuance, custody and payments appear well placed.