For the attention of the European Commission

The DeFi distinction: a blueprint to safeguard decentralised innovation in Europe

Joint recommendations

Introduction

Europe's ambition to lead in digital finance will be tested by how it chooses to address decentralised systems. MiCA has established a credible and widely recognised regulatory framework for centralised crypto-asset services: a genuine competitive advantage for the EU. The question now facing the Commission is whether extending or adapting that framework to decentralised models will reinforce that advantage, or erode it.

As European and global actors operating across the DeFi value chain (protocol development, non-custodial software, hardware security and onchain infrastructure) we bring direct operational experience with the technologies and architectures that any regulatory reflection must account for. We offer this paper as a substantive, constructive contribution ahead of the Commission's anticipated public consultation.

A threshold observation is essential: DeFi is not a single category of activity. The ecosystem encompasses fundamentally distinct functions: immutable smart contract protocols that execute autonomously, non-custodial hardware and software wallets that secure private keys without taking custody, and frontend interfaces that allow users to interact with onchain systems. These layers differ in their technical architectures, their relationship with users, and the degree to which any identifiable actor exercises discretion or control. Effective policy must reflect these distinctions. Treating all activity within the DeFi "stack" as a single regulatory bucket risks producing obligations that are technically unimplementable for some actors and disproportionate for others.

The policy challenge, therefore, is not to define "decentralisation" in the abstract, but to identify where genuine risks to users and financial stability arise within decentralised architectures, and to calibrate any response to those specific risk points. A functional, activity-based approach (grounded in what an actor actually does, and whether it exercises custody or discretion over user assets) would deliver far greater legal certainty than attempts to draw a binary line between "DeFi" and "non-DeFi."

The urgency of getting this right is underscored by the global competitive landscape. Other jurisdictions with equally advanced and innovation-friendly frameworks, particularly across Asia, are moving quickly to attract DeFi activity. The Middle East is also positioning itself as a hub for crypto innovation. Similarly, the United States is also moving rapidly to provide regulatory clarity for non-custodial technology providers, with bipartisan legislation explicitly distinguishing software developers from financial intermediaries. If the EU's regulatory approach is perceived as disproportionate or hostile to DeFi innovation, the consequence

will not be the elimination of DeFi activity: it will be its relocation. Europe would then face the paradox of importing, at greater cost, the very infrastructure it drove offshore.

Open blockchain networks, self-executing smart contract protocols, and non-custodial infrastructure are not financial intermediaries awaiting regulation, they are a distinct technological layer that should remain permanently outside the financial services perimeter. Regulating autonomous code as if it were a service provider is both technically unimplementable and conceptually misplaced. That being said, as institutional adoption deepens (particularly through the integration of tokenised securities and regulated assets) the expectations of authorised financial institutions (and expectations of their respective supervisors) may incentivise software developers and companies to ensure certain security features or new types of configurability in their systems.

What we urge is that the Commission resists the pressure to legislate prematurely on the basis of categories that do not yet reflect technical or market reality, and instead invest in the structured dialogue, interpretive guidance, and evidence-based analysis that will make any future framework fit for purpose.

This paper sets out key principles and concrete recommendations to support that objective. It addresses the clarification of MiCA's existing scope, the need for explicit safe harbours for non-custodial technology providers, a risk-based supervisory approach, the preservation of core architectural features, the conditions for institutional interoperability, and the role of voluntary industry standards.

***

Executive summary

MiCA's regulatory perimeter must be defined by function, not by architecture. The distinction between "DeFi" and "non-DeFi" is not a workable regulatory boundary. What matters is whether an actor exercises custody or discretion over user assets. The Commission should anchor its scope analysis to two clear inquiries: effective control at the protocol layer, and the nature of the service at the application layer. Attempting to define "full decentralisation" further would generate legal uncertainty, inconsistent NCA outcomes, and misplaced obligations.

Developers are not financial intermediaries and must not be treated as such. Writing, deploying, or maintaining open-source, non-custodial smart contract code is a fundamentally different activity from operating a financial service. The EU must establish a developer protection framework that shields contributors from CASP-equivalent obligations where they exercise no effective control over user assets. Without it, EU-based developers face an unacceptable choice between undefined legal exposure and relocation to friendlier jurisdictions.

Supervisory responses must be proportionate to demonstrable, evidence-based risks. DeFi represents approximately 4% of total crypto-asset market capitalisation: it is not a systemic risk today. Any regulatory reflection should target genuine risk points within decentralised architectures, particularly where regulated entities interact with onchain systems, rather than imposing entity-level obligations on infrastructure that operates without custody or discretion.

Core architectural features of DeFi are risk mitigants, not regulatory gaps. Self-custody, open-source development, and permissionless interoperability reduce counterparty risk and single points of failure. Any framework that compels developers to introduce access controls or backdoors into non-custodial tools would actively undermine consumer security and create systemic vulnerabilities. The EU must ensure that regulatory objectives are achieved without altering the foundational integrity of decentralised systems.

Voluntary standards and structured dialogue are the right tools for this stage. In a rapidly evolving technological environment, industry-led mechanisms can address operational and security risks more dynamically and accurately than prescriptive legislation. The Commission should prioritise smart contract audit standards, governance transparency best practices, and market-driven security tools. These must remain genuinely voluntary and must not evolve into de facto certification requirements or new regulatory gateways.

***

Clarifying MiCA's scope to secure DeFi in Europe

Removing legal uncertainty around "full decentralisation"

MiCA's regulatory perimeter should be determined by what an actor does (specifically, whether it exercises custody or discretion over user assets) not by where it sits on a spectrum of decentralisation. The concept of "full decentralisation" referenced in Recital 22 of MiCAR was a useful exclusion at the time of drafting, but attempting to define it further would be counterproductive. It would invite subjective assessments, produce inconsistent outcomes across National Competent Authorities, and frame the regulatory debate around a technical architecture question rather than around actual risks to users and financial stability.

We recommend instead that the Commission structure the regulatory perimeter around two distinct inquiries, which correspond to two different layers of the DeFi stack and raise fundamentally different regulatory questions.

The first concerns the protocol layer (the smart contract infrastructure that enables onchain financial activity). Here, the relevant question is whether any entity retains effective, ongoing control over the protocol's operation. Indicators of such control (including the ability to act unilaterally on user assets, discretion over the execution of individual transactions, or the capacity to modify core protocol parameters without distributed governance) should guide the Commission's assessment. Where no such control exists, imposing entity-level obligations at the protocol layer is both disproportionate and practically unenforceable. The Commission should ensure that protocols which are credibly neutral in their operation are not drawn into the MiCA perimeter solely because they facilitate financial activity, just as the settlement infrastructure of a permissionless blockchain is not itself treated as a financial service provider.

The second concerns the application and service layer (the interfaces, platforms, and infrastructure providers through which users or institutions access and interact with protocols). The relevant inquiry shifts to the nature of the service being provided. A non-custodial wallet that enables a user to interact with a lending protocol, an infrastructure provider that aggregates access to multiple yield sources, or a front-end that displays protocol data: each of these plays a different functional role, and none of them constitute financial intermediation. The Commission should assess whether the entity intermediates between counterparties in a manner that creates counterparty exposure, or whether it is providing a technical service that enables users to interact directly with onchain infrastructure. The ability to operate, maintain, or distribute a software product does not, in itself, constitute a financial service.

Based on this rationale, the following categories should not fall within MiCA's scope:

- Non-custodial wallet providers (hardware and software) that enable users to manage their own private keys without ever taking custody of assets;
- Open-source smart contract developers who write, deploy, or maintain protocol code, as well as application and service layer providers that offer access to such protocols, without exercising operational custody or transaction-level discretion;
- Blockchain infrastructure providers and node operators that validate transactions or provide staking services at the protocol level without holding user funds;
- Interface providers that aggregate transparent, onchain pricing data and relay user-generated and signed messages to blockchain addresses, without exercising intermediary functions such as discretionary routing or execution.

Anchoring the perimeter to these two inquiries (control at the protocol layer, nature of the service at the application layer) would give the Commission a coherent framework that can be operationalised through Level 2 measures, while providing market participants with the directional certainty they need to continue building within the EU.

Establishing a developer protection framework

Developers who write, deploy, or maintain open-source, non-custodial smart contract code should not be treated as financial service providers merely by virtue of having authored that code. Writing software is a fundamentally different activity from operating a financial service: a developer who publishes a lending protocol no more provides a lending service than an engineer who designs a bridge operates a transport company. The Commission should explore the feasibility of a protection framework that would shield developers from CASP-equivalent obligations where they do not exercise effective control over user assets, do not hold the ability to unilaterally modify or halt user transactions, and do not derive revenue from intermediating between counterparties.

Such an approach would be consistent with the EU's technology-neutral principles and with the proportionality standard that underpins the broader MiCA architecture. The relevant regulatory question should not be whether a developer has contributed to a protocol's codebase, but whether any entity retains sufficient control over the protocol's operation to be meaningfully considered a service provider. Where no such control exists, imposing entity-level obligations on developers risks being both disproportionate and practically unenforceable while doing little to advance the consumer protection or financial stability objectives that justify regulation in the first place.

Without a framework that clearly distinguishes between software development and financial service provision, EU-based developers face a stark choice between accepting undefined legal exposure or relocating to jurisdictions that have already moved to clarify this boundary. A well-calibrated developer protection framework would not create a regulatory vacuum: regulated entities that interact with or build upon such protocols (including distributors, asset

managers, and other financial institutions) would remain fully subject to existing prudential, conduct, and AML-CFT obligations. The framework would simply ensure that regulatory obligations attach where control and economic intermediation actually reside, rather than at the code layer.

Advocating for a risk-based and layered supervisory approach

Targeting genuine risk points

Any supervisory reflection should begin with a careful, evidence-based analysis of how decentralised systems operate in practice. Rather than pre-identifying specific technical components as regulatory targets, the consultation should seek to understand where actual user harm or systemic concerns may arise, and whether existing frameworks already address such risks particularly when regulated entities interact with onchain systems.

In particular, the consultation could assess:

- whether already regulated entities integrating DeFi should perform appropriate technical due diligence (audits, code reviews, risk assessments);
- how existing prudential and conduct frameworks can apply to such regulated entities without extending obligations to non-custodial infrastructures and non-discretionary interface providers.

Ensuring proportionality and progressivity

DeFi currently represents a limited share of the overall crypto-asset market and an even smaller share of EU financial markets. According to recent EBA and ESMA reporting, DeFi represents approximately 4% of the total crypto-asset market capitalisation, with total value locked (TVL) of around EUR 78 billion as of September 2024. Moreover, data from Statista further estimates approximately 54 million DeFi users globally, including 7.2 million in the EU (around 1.6% of EU citizens). While the sector is still developing, it is far from being considered systemic, providing a valuable window for proportionate and evidence-based looking policymaking.

Any future policy consideration should remain proportionate, technology-neutral and grounded in demonstrable risks, avoiding structural constraints that would alter the core architecture of permissionless systems.

Preserving core architectural features of DeFi

The consultation should explicitly recognise the legitimacy and value of core architectural components, including self-custody, open-source development, interoperable environments and public networks.

These characteristics are not regulatory gaps: they are structural risk mitigants in certain respects (e.g., transparency, reduced single-point-of-failure risk). Specifically, self-custody empowers users to eliminate counterparty risk entirely. Imposing intermediary obligations on non-custodial tools - such as requiring developers to gate access or build in “backdoors” - would actively undermine consumer security, creating systemic vulnerabilities and honeypots for hackers and malicious actors.

Any future framework should preserve the openness, neutrality and technological integrity of permissionless systems, ensuring that regulatory objectives are achieved without altering the foundational characteristics of decentralised architectures.

Enabling interoperability with traditional finance

An increasing number of financial institutions and Fintech companies interact with onchain markets for liquidity provision, lending, collateral management, and tokenisation more broadly.

The consultation should examine:

- barriers faced by regulated entities when integrating permissionless protocols within existing compliance frameworks, including in the context of the DLT pilot regime;
- how supervisory expectations can remain technology-neutral;
- how DeFi infrastructure can support the scaling of tokenised capital markets in line with the EU’s Savings and Investment Union objectives.

The EU should ensure that permissionless systems are not indirectly disadvantaged compared to permissioned or closed infrastructures, provided institutions appropriately manage operational, legal, and counterparty risks.

Relying on voluntary standards and soft tools

In rapidly evolving technological environments, industry-led initiatives can address operational and security risks more dynamically than prescriptive legislation. A good example is the European Blockchain Regulatory Sandbox, which brings together regulatory authorities and blockchain project operators across EU member states to iteratively assess legal and technical compliance challenges in real time, allowing regulators to develop guidance that is grounded in live use cases rather than theoretical frameworks, and enabling project teams to identify and mitigate risks collaboratively before those risks become codified barriers under rigid statutory regimes.

The consultation could explore:

- voluntary standards for smart contract audits and disclosures. To this end, among possible options raised by the ACRP-AMF Working Group on smart contract certification, we are not favourable to a new mandatory systematic certification;

- best practices on governance transparency and resilience;
- enhanced transparency practices and publicly accessible information on protocol design and usage;
- market-driven security practices (e.g., bug bounties, formal verification).

Such tools should remain voluntary and avoid evolving into de facto certification requirements. Their purpose should be to enhance transparency and informed participation, not to create new regulatory gateways.

Conclusion

The forthcoming consultation, as well as the report to be prepared by the European Commission pursuant to Article 142 of MiCA, represent a critical moment for Europe's digital finance strategy.

The EU does not need to rush toward a bespoke DeFi regime. Its immediate priority should be clarifying MiCA's scope, promoting consistent interpretation across Member States and preserving the ability of institutions and developers to build on onchain infrastructures.

A premature attempt to fit decentralised systems into intermediary-based regulatory categories would risk regulating the wrong layer, discouraging responsible innovation in Europe, and fragmenting the Single Market. Conversely, by adopting a functional, proportionate, and technologically informed approach, the European Union can strengthen trust, safeguard users, and continue positioning itself as a global leader in the responsible development of decentralised financial infrastructure.

***