

Trust Architecture for European Digital Finance

Regulation Without Collapsing Trust Into Control

Submission to the European Commission targeted consultation on the review of MiCA
Donny Lewis | 27 September 2026

Core proposition. Financial regulation does not eliminate vulnerability. It redistributes it. Good regulation should therefore identify the specific vulnerability at issue, assign only the authority necessary to address it, make the exercise of that authority inspectable and proportionate, and preserve meaningful choice and exit wherever possible.

Executive summary

MiCA was an important attempt to create legal certainty for a market that had grown faster than the institutions around it. The present review is an opportunity to improve that framework without allowing legitimate concerns about consumer protection, financial stability, illicit finance and operational risk to harden into a financial architecture in which control accumulates simply because control is technically possible.

My contribution is based on a framework I call Trust Architecture. I define trust as willingly accepted vulnerability in the presence of risk. The definition matters because it separates trust from verification, compliance and control. Cryptography can prove identity, provenance, signatures, balances and execution. Regulation can compel behaviour. Neither fact, by itself, establishes that the resulting relationship is trustworthy.

The practical implication is simple: different trust failures occur at different layers and need different defences. Issuer risk does not automatically require control of the settlement ledger. Anti-money-laundering obligations imposed on an identifiable intermediary do not automatically justify turning neutral software or non-custodial infrastructure into an intermediary. Identity verification does not automatically require every verifier to retain another complete copy of the person. Smart-contract risk does not automatically justify a gatekeeper deciding which permissionless protocols Europeans may access.

The Commission's consultation itself states that financial regulation should remain technology neutral in order to preserve freedom of choice for market participants. I support that principle. I suggest extending it into an architectural principle: regulation should be neutral not only between technologies, but also between legitimate architectures that allocate trust and control differently while achieving the required regulatory outcome.

1. Trust, verification and control are not the same thing

Trust begins where proof ends. If an outcome is fully guaranteed, no vulnerability remains and trust is unnecessary. Real financial systems cannot eliminate vulnerability: they decide who

carries it, who receives authority over it, what evidence is available and what recourse exists when the relationship fails.

This distinction is increasingly important because digital infrastructure can make control look like trust. A credential may be authentic. Its issuer may be verified. A transaction may be correctly signed. The provenance may be perfect. Yet the weaker party may still have almost no meaningful choice about whether to enter the relationship, what data to disclose, which intermediary to use or whether an alternative path remains available.

The European Digital Identity framework is useful as an adversarial case. The Commission states that use of the EUDI Wallet is not mandatory and that users will control which data they share. Those are important safeguards. At the same time, public services and certain private services will be required to recognise the wallet, and the infrastructure is designed for broad use across banking, employment, travel, education and government services. Formal voluntariness should therefore be protected not only in law but in market structure. A choice can remain legally optional while becoming practically difficult to refuse if essential services converge on one architecture.

This is not an argument against EUDI, cryptography or interoperable credentials. It is an argument for a stronger test: does the architecture preserve meaningful choice for the party carrying the vulnerability? No meaningful choice means no meaningful consent. Without meaningful consent, vulnerability may be imposed or compelled, but it is not willingly accepted trust.

2. Regulation redistributes vulnerability

Every regulatory intervention changes the trust graph. A reserve requirement may reduce one form of issuer risk while concentrating assets in commercial banks and creating another liquidity dependency. A KYC requirement may reduce anonymity at an intermediary while creating durable databases of passports, addresses, biometrics and transaction histories that become attractive targets for compromise or compelled disclosure. A certification requirement may reduce uncertainty about a smart contract while creating a gatekeeper whose approval becomes economically necessary.

The correct question is therefore not simply whether a rule reduces a named risk. It is: where does the vulnerability go after the rule is imposed? Who acquires new authority? What new dependency is created? Can that authority be inspected and challenged? Can a user choose another path without losing practical access to economic life?

This review already contains a contemporary example. European central banks have argued that MiCA's bank-deposit requirements for stablecoin reserves can themselves create financial-stability concerns. Whatever final policy is chosen, the episode demonstrates the general point: controls move risk through a system. They do not make risk disappear.

3. Regulate the actor that holds the authority

MiCA's treatment of decentralised finance should be built around actual control rather than labels. The consultation correctly asks about identifiable intermediaries, administrator keys,

concentrated governance power and custody. These are useful because they identify where authority actually exists.

An identifiable party that can unilaterally upgrade a protocol, seize or freeze assets, alter material economic parameters, misrepresent a product or custody customer funds can reasonably carry obligations corresponding to that authority. The same logic should work in the other direction. Where no party possesses such authority, regulation should not manufacture an intermediary by assigning liability to software developers, non-custodial wallet providers or connectivity providers merely because they are easier to identify.

The regulatory perimeter should follow effective authority and accepted vulnerability. This is more durable than attempting to classify systems as simply 'centralised' or 'decentralised'. A protocol may be decentralised in execution but concentrated in governance. A company may provide a user interface without custody. A wallet developer may publish software without controlling subsequent transactions. Those relationships are different and should not be collapsed into one category.

4. Certification should produce information, not permission

Questions 62-65 consider certification, whitelists, blacklists and restrictions on CASP connectivity to DeFi. Certification can be useful when it produces inspectable evidence: code has been audited, upgrade authority is disclosed, economic assumptions are documented, incidents are reported, and material changes invalidate or update the assessment.

It becomes dangerous when certification changes from evidence into permission. A public or private certifier should not become the de facto authority deciding which otherwise lawful permissionless protocols Europeans may use. That would replace one set of technical risks with institutional dependency and would weaken the very technology-neutrality and freedom of choice identified by the Commission as regulatory objectives.

A better default is evidence plus disclosure. CASPs may perform risk assessments and present clear warnings. Users should be able to distinguish audited from unaudited systems, immutable from upgradeable contracts, concentrated from distributed governance, custodial from non-custodial access, and verified from unverified claims. Restrictions should be tied to specific unlawful conduct or demonstrable regulatory obligations, not to the absence of institutional approval itself.

5. Permissionless settlement and regulated institutions can coexist

The debate should also avoid treating institutional responsibility and permissionless infrastructure as opposites. In September 2026, SoFi Bank and Mastercard announced that stablecoin settlement is live across SoFi's debit and credit card program, with the program expected to process more than USD 25 billion in annualised volume using SoFiUSD. Mastercard describes SoFiUSD as a stablecoin issued by a nationally chartered U.S. bank on a public, permissionless blockchain.

This does not prove that every financial use case belongs on a public blockchain, nor does it establish that the SoFi architecture should be copied in Europe. It demonstrates something

narrower and important: regulation of an issuer does not logically require institutional control of the underlying ledger. Issuance, reserves, redemption, compliance, settlement, privacy and network participation are separable functions.

European policy should preserve the ability to make those separations. Where confidentiality is required, regulate or engineer confidentiality. Where an issuer must hold reserves, regulate reserves. Where an intermediary holds customer assets, regulate custody. Do not infer from one legitimate authority that the same actor must control every layer below it.

6. Privacy: prove what is necessary, possess no more than necessary

Identity and compliance create another recurring trust failure: verification is frequently implemented through possession. A service needs to establish a fact about a person, so it collects and retains a reusable copy of the person - identity documents, addresses, photographs, financial records or other data. The verification event ends; the vulnerability remains.

European digital identity work already recognises selective disclosure and user control as goals. MiCA and adjacent financial regulation should reinforce the same principle. Regulation should specify the fact that must be established and the evidence that must be retained for accountability, while allowing privacy-preserving proofs, attestations and reusable credentials where they satisfy the legal requirement. Verification should not automatically mean universal duplication.

Data minimisation is therefore not merely a privacy preference. It is risk architecture. Every unnecessary copy creates another custodian, another attack surface, another legal jurisdiction and another party capable of exposing or compelling the data.

7. The walk-away test

A useful final test for digital-finance regulation is whether the person or organisation carrying the vulnerability retains a credible ability to leave. Exit does not mean that every regulated service must be anonymous, free of conditions or available without compliance. It means that regulation should avoid unnecessary architectural lock-in when multiple compliant ways of satisfying the same requirement are possible.

The test can be stated plainly: if I reject this intermediary, identity provider, wallet, settlement network or certification authority, is there another lawful route that preserves the essential service? If not, the authority of that component deserves heightened scrutiny because consent around it is becoming progressively less meaningful.

The weakest participant is usually the first to lose exit. Large institutions can negotiate interfaces, licences and exemptions. Individuals and small builders generally accept the architecture presented to them. Preserving plural routes is therefore not only an innovation concern; it is a protection against concentrated vulnerability.

8. Recommendations for the MiCA review

Follow effective control. Attach obligations to identifiable actors according to the authority they actually exercise: custody, unilateral upgradeability, transaction control, material governance power, representations to users, or control over customer assets.

Preserve non-custodial software as software. Do not create an intermediary merely because a developer, wallet provider or interface is identifiable when that party does not control the user's assets or the underlying protocol.

Use certification as evidence, not a licence to exist. Encourage inspectable security and governance assessments, but avoid making public/private whitelists or certificates the default gate through which lawful permissionless protocols must pass.

Make architectural neutrality part of technology neutrality. Specify regulatory outcomes and allow regulated actors to meet them through public, private, permissioned or permissionless infrastructure where equivalent safeguards can be demonstrated.

Require vulnerability-transfer analysis. For material new rules, assess not only the risk reduced but the new concentration, data, liquidity, operational or governance dependency created by the intervention.

Prefer verification over possession. Where identity or eligibility must be established, permit data-minimising proofs and attestations that establish the necessary fact without unnecessary replication of underlying personal data.

Protect meaningful exit. When infrastructure becomes systemically important, assess whether users retain realistic alternative compliant routes and whether switching is technically and economically feasible.

Preserve permissionless innovation. Avoid requiring neutral protocols, open-source code or non-custodial wallets to embed universal compliance controls merely to remain accessible; impose obligations at the layer where regulated authority actually exists.

9. Relevance to the consultation questionnaire

Question 9-10 (future role and benefits of stablecoins): stablecoins can become meaningful payment and settlement infrastructure without requiring a single ledger topology. The SoFi/Mastercard example demonstrates that regulated issuance can coexist with public permissionless infrastructure.

Questions 59-61 (DeFi and decentralisation): assess decentralisation through actual control - custody, administrator keys, unilateral upgrade authority, concentrated governance and identifiable intermediaries - rather than branding or the mere existence of identifiable developers.

Questions 62-65 (indirect regulation and certification): favour transparent risk information, audits and disclosures over mandatory certification gates, whitelists or prohibitions on connectivity to otherwise lawful permissionless protocols.

Questions 66-67 (staking, lending and borrowing): distinguish custodial service provision from autonomous protocol use. Apply obligations to parties that custody assets, make representations, intermediate transactions or exercise effective control, rather than treating the underlying technical action as requiring the same regulatory wrapper in every architecture.

Questions 74-79 (tokenised deposits): preserve competition among settlement architectures. Regulation of deposit liabilities and prudential risk should not unnecessarily dictate whether compliant settlement occurs on institutionally controlled or public infrastructure.

Question 86 (other relevant issues): adopt Trust Architecture as an analytical discipline for digital-finance regulation: identify the vulnerability, locate the party receiving authority, bound that authority, require inspectable evidence, examine where risk is transferred, and preserve meaningful choice and exit.

Conclusion

Europe does not need less trust. It needs to become more precise about where trust is placed.

The promise of cryptography is not that institutions disappear. It is that some things that previously required institutional trust can now be independently verified. The promise of good regulation should be similar: not to eliminate every vulnerability through control, but to place authority where it is necessary, bound it to the vulnerability it exists to address, and leave the rest of the system free to develop.

A weak architecture asks for one master solution. A stronger architecture understands that different trust failures occur at different layers and need different defences.

MiCA can protect consumers and markets without making institutional permission the default trust layer of European digital finance. The Commission's own commitment to technology neutrality and freedom of choice provides the right starting point. The next step is to apply that principle to the architecture itself.

Sources and primary references

- [European Commission - Targeted consultation on the review of MiCA Regulation](#)
- [European Commission - Consultation document \(MiCA review\)](#)
- [European Commission - European Digital Identity Regulation overview](#)
- [European Commission - Q&A on EU Digital Identity](#)
- [SoFi - Stablecoin settlement live across Mastercard card program, 22 September 2026](#)
- [Mastercard - SoFiUSD settlement architecture, 3 March 2026](#)
- [Donny Lewis - The Truth About Trust 3: The Scaffolding We Actually Want](#)