Intelligence Economy
INSTITUTE

Regulating Decentralised Finance in the European Union: Compte rendu and Analysis of a Closed-Door Roundtable on the MiCA Review Consultation

Zakaryae Boudi
Intelligence Economy Institute

June 2026

Abstract

This note records and analyses the substance of a closed-door roundtable held in May 2026, convening regulators, supervisors, legal practitioners, academics, exchange operators, protocol builders and policy specialists around the European Commission's consultation on decentralised finance (DeFi), launched ahead of the mandatory review of the Markets in Crypto-Assets Regulation (MiCA). The discussion was conducted under a non-attribution convention; positions are therefore reported without ascription to individuals or institutions, except where named protocols or public documents were invoked as examples. The roundtable converged on several structuring findings: that the threshold question is not how to regulate DeFi but whether identified risks justify regulation at all; that "sufficient decentralisation" remains undefined and would benefit from analytical tools borrowed from competition economics; that the consultation in fact bundles four distinct questions—protocol certification, gatekeeper obligations, circumvention by "fake DeFi," and the treatment of yield on e-money tokens—which must be disentangled; and that Europe's competitiveness position leaves little margin for regulatory error. The note further develops two contributions advanced by the Intelligence Economy Institute: the need for a shared, machine-readable catalogue of cybersecurity risks and verifiable properties of on-chain systems—a need addressed by the Blockchain Property Ontology—and a proposal for an EU taxonomy of function and control in on-chain financial arrangements, designed expressly to avoid the failure modes of past classification efforts, as the analytical precondition for any proportionate regulatory intervention.

1. Context and purpose

The European Commission has opened a public consultation on decentralised finance, the first formal step in a sequence that participants expect to unfold over several years: consultation now, a mandatory report on the functioning of MiCA within roughly a year, a possible legislative proposal thereafter, and then negotiation between the Commission, the Council and the European Parliament. One participant with prior experience inside a national supervisor estimated the fastest realistic path to binding rules at three years. The roundtable was convened to test the consultation's premises against the views of those who supervise, advise, build and operate in the sector, and to begin shaping coordinated responses.

Two framing facts recurred throughout the discussion. First, DeFi remains a small fraction of crypto-asset markets—figures between one and four per cent of overall market activity were cited—which

several participants regarded as dispositive on the question of systemic risk, while others cautioned that small relative shares can still represent large absolute numbers of investors and money. Second, MiCA itself deliberately left DeFi out of scope: its Recital 22 exempts crypto-asset services provided "in a fully decentralised manner without any intermediary," a formulation that was helpful at negotiation time precisely because the framework was designed for centralised intermediaries, but which now leaves the central interpretive question—what counts as full or sufficient decentralisation—unresolved.

2. The threshold question: regulate against which risks?

The most consistent discipline imposed on the discussion was the demand that any regulatory move be traced back to an identified risk. Participants repeatedly listed the classical objectives—market integrity, consumer and investor protection, anti-money-laundering and counter-terrorist-financing (AML/CFT), financial stability—and then asked, objective by objective, whether DeFi as it exists presents a problem proportionate to a multi-year legislative process. One participant added competitiveness explicitly to that list of guiding objectives, alongside implementability: rules must be specifiable, free of internal contradiction, and resistant to circumvention, since regulation is not merely text but an operational protocol that courts and markets must be able to execute.

A thought experiment offered early in the session crystallised the risk logic. Compare two entities performing economically similar functions: a licensed investment firm that custodies client assets and executes transactions, and a small identifiable team paying for servers and running an execution engine over decentralised exchanges, with no custody of client assets. If the first fails, clients lose their money and chaos follows; that is why it is regulated. If the second disappears, the service stops but every client retains exactly the assets they held, because the protocol, not the operator, holds them. Identifiability, the participant argued, is therefore not in itself a ground for regulation; the ground is the presence of a risk that regulation can actually mitigate. Several speakers extended the point: an erroneous calibration produces errors in both directions—under-regulation tolerates a residual level of crime, as every free society does, while over-regulation imports concerns from adjacent policy fights (platform regulation, artificial-intelligence liability, child protection online) into a domain where they do not belong, regulating "the people you can catch" rather than the matter itself. One speaker memorably described this as the *Casablanca* approach: when in doubt, round up the usual suspects—interfaces, front-end operators and developers—because they are the only identifiable parties.

A legal academic placed the consultation in the wider Brussels conjuncture: following the Draghi report on European competitiveness and the Commission's subsequent simplification agenda, a formal de-prioritisation strategy has shelved the level-two implementation of legislation already adopted, because the European supervisory authorities lack the resources to execute their mandates. Launching a new regulatory workstream for a market segment of this size, the argument ran, sits uneasily with that posture, and risks repeating what several participants regard as MiCA's own pattern: regulation presented as innovation-enabling that in practice has not made Europe a more attractive place to build.

3. Decentralisation: criteria, critiques, and the contestability lens

The consultation advances a set of criteria for assessing whether a protocol is genuinely decentralised. As reconstructed in the discussion, these cover, among others: the existence of identifiable persons exercising influence over the protocol, including developers who deployed the code; control over economic and technical parameters through administrative keys; significant concentration of governance power; custody of, or effective power over, user assets; the open-source character of the code; and the protocol's marketing posture. Each criterion drew substantive critique.

On identifiable persons, participants noted that identifying a developer who deployed open-source code tells the regulator very little: the relevant question is what that person can still do—whether they can unilaterally modify the protocol or merely once contributed to it. On administrative keys, practice shows peer-controlled arrangements analogous to corporate governance: key holders frequently cannot act alone, and changes to economic parameters such as protocol fees require broader token-holder involvement, so a registry of key holders is not a measure of control. On governance concentration, a recent European Central Bank paper identifying the largest delegates in major protocols was criticised for failing to distinguish delegates acting as revocable proxies from parties holding effective, legally cognisable control—a distinction one participant described as fundamental, since a token holder who lazily delegates voting power while retaining the right to revoke it at any time has not ceded control in any meaningful sense.

The most analytically generative intervention proposed importing the toolkit of competition economics. Whether a market is contestable is a question economists and antitrust authorities answer daily, using concentration indices of the Herfindahl–Hirschman family and merger-control heuristics about the number of effective competitors. Sufficient decentralisation, on this view, is not a count of governance token holders against some textbook fiction of infinitely many agents; it is a question of whether control is contestable—whether a small group, even of four or five participants, must genuinely compete and can be displaced. A counterpoint was immediately offered with a named example: the Morpho lending protocol, whose base layer is plausibly decentralised, but where a small number of vault curators—two groups were said to control on the order of eighty per cent of lending activity—effectively run the operations built on top of it. Concentration and contestability, a third participant observed, are distinct concepts, and governance can be concentrated yet contestable where delegation is freely revocable; the interaction of the two is an open research question on which at least one participant is preparing academic work.

4. Four questions hiding inside one consultation

A structuring contribution disentangled what "regulating DeFi" actually means in the consultation, identifying four distinct fronts that the roundtable then debated in turn.

4.1. Certification of protocols

The consultation floats a certification regime—deliberately not called a licence, and described in the room as a "half-licence"—as a lighter-touch pathway for protocols that are not fully decentralised but should not be forced into full crypto-asset service provider (CASP) authorisation. In principle the idea of a graduated pathway found some sympathy; in practice, scepticism dominated. Participants doubted that the EU could specify such a regime correctly and in time, stressed that the cost, duration and predictability of the certification process would matter more than its text, and noted that industry feedback gathered in past responses to the French authorities (AMF and ACPR) shows builders are not opposed to standards as such—they object to year-long opaque processes. The deeper objection was constitutional: no jurisdiction in the world has yet regulated DeFi as such, and the EU would be the first mover in an experiment whose downside is borne by its own ecosystem.

4.2. Gatekeepers and "CeDeFi"

The second front does not regulate protocols at all but the regulated entities that give access to them. CASPs are already licensed; the question is what their existing obligations mean when they intermediate access to DeFi—disclosures and warnings to users, due diligence on integrated protocols, and so

on. The roundtable flagged a consequential subtlety: one consultation question asks whether CASPs should be permitted to interact *only* with certified DeFi. Formally this imposes nothing on protocols; substantively it is an indirect certification mandate, and as drafted the question contains no carve-out for fully decentralised protocols, which could find themselves excluded from regulated distribution precisely because they have no entity capable of seeking certification.

The institutional context makes this front the economically significant one. A recent Ipsos survey in France was cited indicating that, among respondents interested in accessing DeFi, roughly half would prefer to do so through their bank and a quarter through a crypto exchange, with fewer than a third comfortable operating a self-hosted wallet. Institutionalised DeFi—regulated entities providing liquidity, integrating protocols and distributing products—is therefore likely to be the channel through which adoption actually occurs, which means DeFi is already substantially regulated *de facto* at its points of contact with the regulated perimeter. Exchange representatives, however, pushed back on formalising a gatekeeper role: it would force them to select which protocols may exist commercially, expose them to liability for decentralised systems they do not control, and add regulation to entities that are already heavily regulated. An alternative, advanced from the builder side, located the natural control points at the gateways more broadly understood—exchanges, but also wallets and RPC infrastructure—on the argument that regulating entry and exit points captures whatever innovation emerges on-chain without chasing each new protocol, though others warned that this risks regulating future innovation by definition.

4.3. Unmasking "fake DeFi"

The third front commanded the broadest consensus: distinguishing genuinely decentralised systems from crypto-asset service providers in disguise—entities using the DeFi label to avoid authorisation. As one participant put it, if regulation comes, "it will not be a regulation on DeFi; it will be a regulation on fake DeFi." Supervisory experience supports the concern: the French regulator, reviewing a product built with DeFi partners, asked whether the partner held a MiCA licence on the ground that what it provided was, in substance, a MiCA service with identifiable centralisation. A complementary observation from the trading-platform side held that DeFi is not binary but a spectrum of degrees, with full decentralisation at one rarely attained end; on this reading, much of what is marketed as DeFi already falls within MiCA's listed services, and a leading decentralised exchange operating a trading interface was offered as an example. The political-economy warning attached to this front was sharp: when centralised exchanges walk into regulators' offices claiming to represent decentralisation, the credibility of the entire industry's case suffers, much as it would if dominant platforms claimed to speak for the open internet.

4.4. Yield on e-money tokens

The fourth front concerns the prohibition—inherited from the e-money framework that preceded MiCA—on granting time-based interest on e-money tokens (EMTs), and what it means when a stablecoin is deployed into a DeFi protocol that generates yield. Is yield earned by taking risk in a lending protocol "interest" within the prohibition? Is a CASP that intermediates, smooths or aggregates such yield itself granting prohibited interest? A concrete position was advanced: risk-bearing deployment of an EMT into a protocol is not the passive remuneration the prohibition targets and should be specified as outside its scope. The competitive stakes were framed bluntly: in a world where other jurisdictions permit such yield, an absolute European prohibition could be "the nail in the coffin" of euro-denominated stablecoins in on-chain finance—particularly as agent-to-agent, algorithmically optimised payments emerge, since autonomous agents will route to whatever asset optimises returns without regard to monetary geography. The American debate around the GENIUS Act was cited as the mirror image: a prohibition on issuers offering yield, a banking-sector fear of deposit flight, and an emerging compromise turning on whether

rewards flow from bona fide third-party activity rather than from the mere holding of the token.

5. The transatlantic dimension

A practitioner advising large global banks summarised the United States debate under the Clarity Act, which allocates digital assets between securities and commodities regimes and interacts with the GENIUS Act on stablecoins. The core dispute is whether developers of DeFi protocols should bear legal responsibility when their code is used for illicit purposes; advocates seek safe-harbour language for non-custodial software developers, while law-enforcement bodies oppose carve-outs they believe would impede prosecution. The drafting has converged on *control* as the operative concept—who can exercise it, over what, and when—which is precisely the axis along which the European discussion of admin keys, governance and custody is also moving. The forward-looking prediction was structural: as banks obtain permissions to act as market makers and trade crypto directly, the regulatory treatment of DeFi will be determined less by doctrine than by whether incumbents perceive a level playing field; pressure for heavier DeFi regulation will track banks' fear of disintermediation, exactly as it has with stablecoins and deposit flight.

6. Smart contracts, security assurance, and the missing catalogue

A distinct thread of the discussion, opened from the product-engineering side, proposed that the most workable regulatory primitive is not the entity but the artefact: require that the smart contracts users interact with be published, and equip supervisors with tooling and templates against which a contract can be checked—"a programmatic, programmable way of verifying whether what I am doing is acceptable." By definition, if you know what the contract does, you know what you are dealing with, including the existence and scope of any administrative rights. The proposal drew two qualifications. First, technical analysis of the contract does not answer who uses the protocol and how—a decentralised exchange with a single liquidity provider raises questions no code review resolves. Second, a participant active in litigation defending privacy protocols warned that once regulators hold a discussion about smart contracts, dirigiste ideas follow: proposals reportedly circulating in the European political space would define one canonical smart contract per activity per country—the logic of a centralised system transplanted onto an open one—and in an era when conversational AI can produce a bespoke contract on demand, regulating intermediated contracts while identical unintermediated ones proliferate is not a coherent basis for law. A further intervention, looking past current threats to AI-driven agents and the prospect of state-level quantum attacks, called for voluntary cybersecurity standards that developers and operators could contribute to and reference even outside any registration regime.

What all three positions presuppose, and what none of them supplied, is a shared reference: a common, rigorous statement of *which properties* an on-chain financial system is supposed to satisfy, what each property means precisely, how it fails, and by what method it can actually be verified. Today that knowledge is scattered across audit reports, incident post-mortems and the tacit expertise of a few specialists; every audit re-derives its requirements from intuition, every analysis tool encodes its own private notion of a problem, and supervisors are left choosing between trusting prose attestations and commissioning bespoke expertise. A regulator's "template" for analysing a published contract, a voluntary cybersecurity standard, and any honest certification regime all require the same missing layer: a catalogue of cybersecurity risks and correctness properties with stable identities, machine-readable structure, and an explicit account of what each verification method can and cannot establish.

This is the layer the Intelligence Economy Institute and Tokenfrastructure are building with the

Blockchain Property Ontology (BPO),[1] a living, machine-readable catalogue of the properties blockchain systems are supposed to have—safety, liveness, access control, economic soundness, cryptographic and zero-knowledge guarantees, governance, cross-chain integrity, and the behaviour of autonomous on-chain agents. Each entry describes one property in plain language, in precise mathematics, and in a structured form that verification tools and automated auditors can consume directly; records its relationships to other properties (implication, dependency, reinforcement, conflict); maps the attack patterns that exploit its absence, with references to historical incidents; and cross-references established weakness registries and engineering standards so that existing knowledge flows in rather than being discarded. Two design principles are directly responsive to the failure modes aired at the roundtable. The ontology is honest about verification—it states what is mechanically achievable by which method, refusing the category error of treating single-trace tools as capable of establishing hyperproperties, and thereby refusing to manufacture the false assurance that certification regimes are most at risk of institutionalising. And it treats assumptions as first-class: every guarantee exposes the assumptions it rests on and whether each is discharged or merely accepted, so that "we verified solvency" is forced to also say "assuming the oracle is honest and the chain is live." A certification or supervisory-tooling regime anchored to such a catalogue would replace assurance theatre with conditional, inspectable, machine-checkable claims—which is the only form of assurance worth mandating.

7. A proposal: a taxonomy of function and control in on-chain finance

The single most damaging feature of the current debate, evident throughout the roundtable, is that "DeFi" is doing the work of at least a dozen distinct concepts at once. Participants observed that protocols, front-ends, gateways, governance bodies, liquidity providers and integrating institutions raise entirely different regulatory questions; that exchange, lending, staking, derivatives and insurance are different financial functions with different risk profiles; that decentralisation is a spectrum, not a binary; and that a survey of practitioners found more than half conflating DAOs with DeFi altogether. When regulators hear one word for all of this, they reach for one instrument—and the instrument is invariably calibrated to the most centralised, most visible, least representative actors in the room.

The instinctive answer is a taxonomy, and the Intelligence Economy Institute believes a classification effort is indeed the correct first deliverable of the review period. But the proposal must be made with open eyes, because the idea carries a history. IOSCO considered and explicitly declined to build a prescriptive DeFi taxonomy, adopting instead a functional, economic, outcomes-focused approach in its 2023 policy recommendations, on the stated ground that no generally accepted definition of DeFi exists even among industry participants. The European Supervisory Authorities have already produced the descriptive layer: the joint EBA–ESMA report under Article 142 of MiCA maps DeFi adoption, lending, borrowing and staking business models and the associated ICT and financial-crime risks, and supervisory practice has already settled on substance over form—a project's claim to be "fully decentralised" is assessed against its technical architecture, ownership logic and governance rules, not its marketing. On the academic side, the canonical layered "DeFi stack" is itself contested: recent scholarship reconstructs it on different modular principles and rejects entire layers of the standard diagram. And the Union possesses, in the Sustainable Finance Taxonomy, a fully worked cautionary precedent: a flagship classification system criticised within a few years of adoption for complexity, reporting burden, limited usability and poor international alignment, with only a small fraction of its criteria quantitative and anchored to a standard metric, and now itself the object of a simplification exercise. The mechanism of that failure is general and must be designed against from the outset: the moment a classification becomes an eligibility gate—certified versus uncertified, permitted versus excluded from regulated distribution—classification turns adversarial, boundary-gaming dominates, and a compliance industry grows around the cells rather than

[1] https://github.com/TKNFRA/blockchain-property-ontology

around the risks. A consultation question that would permit CASPs to interact only with "certified DeFi" is precisely such a gate, and a taxonomy bolted to it would rot in exactly the way the green taxonomy did.

The Institute's proposal therefore incorporates four corrections that distinguish it from both the naïve taxonomy and the IOSCO refusal. First, the object must be renamed: not a taxonomy *of DeFi*—which presupposes the definition the field cannot agree on, and which would violate the Commission's own stated principle, restated in this very consultation, that financial regulation remain technology-neutral—but a **taxonomy of function and control in on-chain financial arrangements**. Two axes carry the structure. The axis of *financial function* asks what economic function is performed and who enables it—payment, exchange, lending and borrowing, staking, derivatives, insurance, asset management—deliberately operationalising, rather than reinventing, the functional vocabulary in which IOSCO, the FATF and the recent Emirati guidance already work, so that the EU contribution is interoperable specification rather than unilateral invention. The axis of *control* asks where effective power over the arrangement sits and how it is held: upgrade paths and administrative keys, governance arrangements and the revocability of delegation, oracle and data dependencies, front-end and distribution chokepoints, and custody or effective power over user assets. A layered description of the stack remains useful as supervisory pedagogy, but it should be treated as an explanatory annex, not a load-bearing legal structure, precisely because the layers themselves are unstable.

Second, the taxonomy must be *diagnostic, not eligibility-bearing*. It supplies the shared language in which supervisors, courts and operators describe an arrangement—the language that makes guidance cumulative, makes the fake-DeFi disguise legible, and makes consultation responses commensurable—but legal consequences attach to the financial functions performed and the control facts established, never to membership of a taxonomy cell. This single design rule is what separates a classification that ages like the joint ESA financial-instrument test, which reduces uncertainty at the margin, from one that ages like the green taxonomy, which manufactured a verification industry.

Third, the treatment of decentralisation must be *evidentiary rather than scored*. The contestability concepts aired at the roundtable are the right analytical lens, but converting them into a computed index—a Herfindahl threshold over governance tokens, a number of independent key holders—would be an error of the first order: such indices are trivially gameable through sybil-split holdings and decorative delegation; on-chain measurement does not capture effective control exercised through off-chain coordination, multisignature arrangements, front-ends or oracle dependencies, the very concentration channels the BIS identified in its "decentralisation illusion" analysis; concentration and contestability are, as one participant noted, distinct concepts that a single score conflates; and any numeric threshold becomes a target, inviting structuring just below the line—a European replay of the gaming that "sufficient decentralisation" invited in the United States. What the taxonomy should require instead is a *structured disclosure of control points*: a standard, machine-readable statement of who can do what to the arrangement, under which conditions, with which revocation rights. This is assumption disclosure—the assume–guarantee discipline in regulatory form—and it is the precise point at which the taxonomy couples to the property catalogue of the preceding section: the taxonomy's control disclosure states which powers exist and on which assumptions the arrangement's guarantees rest; the Blockchain Property Ontology states which properties an arrangement bearing those functions must demonstrably satisfy and by what method each claim can actually be verified. Together they make supervision programmable—machine-readable classification on one side, machine-checkable assurance on the other—which is the only supervisory model that scales to a domain where a new protocol can be deployed in an afternoon.

Fourth, the taxonomy needs *maintenance machinery*. A classification frozen in a legislative annex is a snapshot with legal force; MiCA's own drafting history, dominated by the NFT questions of its negotiation years, shows how quickly a snapshot dates. The taxonomy should live as versioned, openly

published, machine-readable data under the stewardship of a standing body with structured industry input, on review clocks, in the manner of an engineering standard rather than a recital—so that when agentic payments, restaking or whatever follows them cut across today's categories, the classification is amended in months, not re-legislated in years. So designed, the taxonomy is future-proof in a way that activity-specific rules are not, and it converts the guidance, sandbox and supervisory-dialogue machinery that participants preferred over new level-one text into something cumulative rather than anecdotal. Figure 1 summarises the architecture of the proposal and its coupling to the property catalogue.

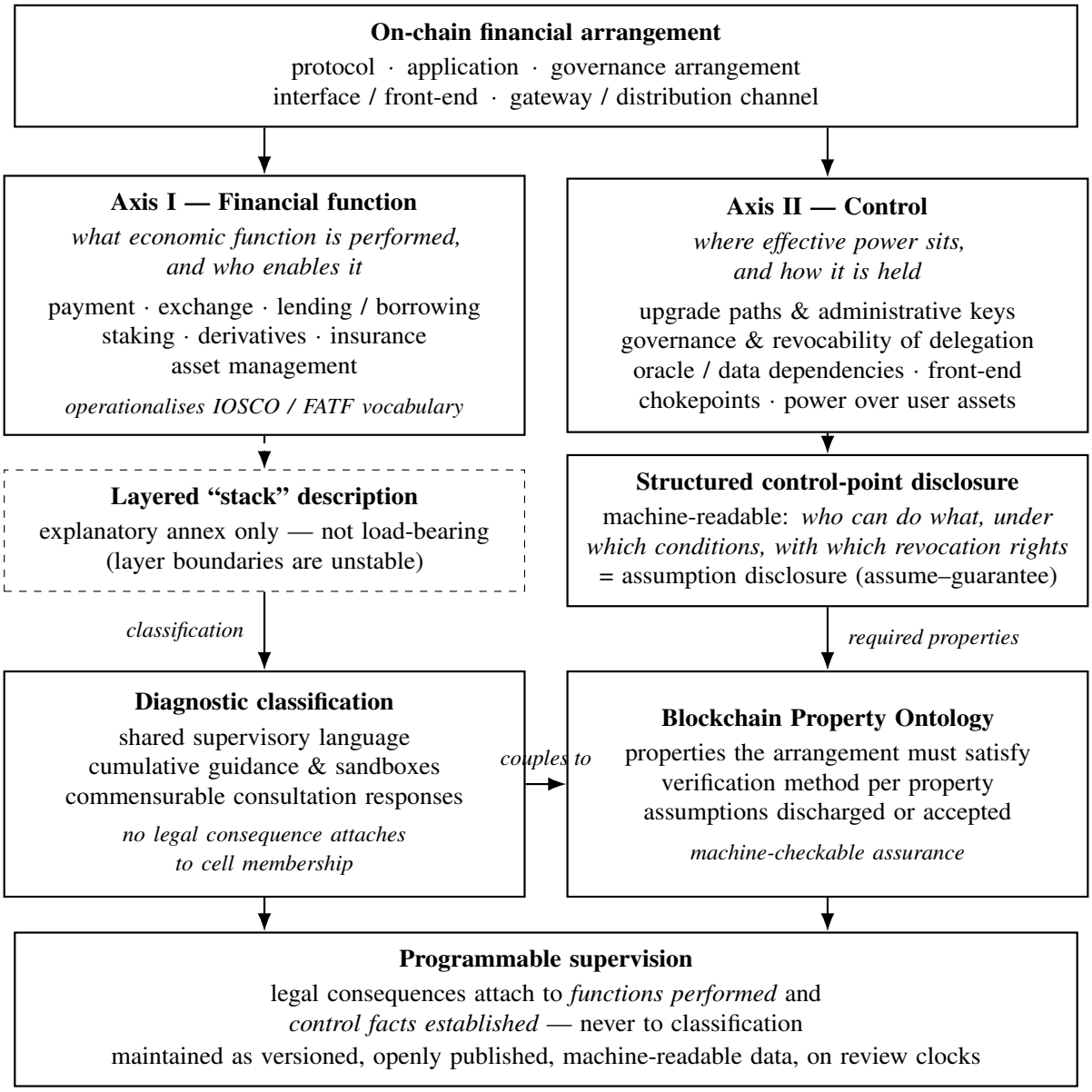

Figure 1: Architecture of the proposed taxonomy of function and control in on-chain financial arrangements, and its coupling to the Blockchain Property Ontology. Classification is diagnostic; assurance is machine-checkable; consequences attach to functions and control facts, not to cells.

8. Competitiveness and timing

The competitiveness assessment offered around the table was stark. European liquidity in DeFi is marginal and largely supplied from elsewhere; guidance on reverse solicitation has driven significant

non-EU projects to withdraw from European events, sponsorships and public engagement altogether; and one participant argued that MiCA and the surrounding discourse have built "a regulatory moat around an empty castle." Opinions divided on intent—one speaker suggested the ambiguity is deliberate, ambiguity being a more effective deterrent than any hard rule, while another, with long legislative experience, attributed it to process: three years, thirty governments, thousands of last-minute amendments, and no single reader of the final text. Against this, a more positive note was sounded: EU licensing retains genuine reputational currency, with investors and partners outside Europe still asking first whether a firm holds a European authorisation, and Europe hosts genuine DeFi champions, including a unicorn lending protocol cited as the second-largest of its kind globally. The synthesis most participants could endorse was sequencing: there is no emergency, the market is small, the technology and its use cases are moving faster than any legislative cycle, and the rational course is to push the substantive decisions back twelve to eighteen months while investing now in the analytical groundwork—definitions, taxonomy, supervisory education—without which any text adopted will be wrong.

9. Concrete steps voiced in the room

Asked to translate the discussion into actionable recommendations for the consultation period, participants converged on a programme that can be summarised as follows. Begin from risk, not from perimeter: every proposed obligation should name the harm it addresses, and proposals that cannot should be resisted. Educate before legislating: supervisory boards that cannot distinguish lending from liquidity provision cannot regulate either, and structured education of regulators and stakeholders was repeatedly named as the genuine first step. Categorise the activity before answering whether to regulate it—the taxonomy argument in its practitioner form. Prefer guidance, worked examples and sandboxes to new level-one text, on the model of the UK Financial Conduct Authority's published examples of when an interface or protocol falls within existing regulation, since changing legislative text "always makes it worse" while most regulatory friction is interactional rather than textual. Specify what existing law already covers—including the EMT yield question and the anti-circumvention rules—before inventing parallel regimes that would leave operators caught between MiCA and a certification track. Consider a safe harbour for neutral front-ends meeting defined non-discrimination criteria, mirroring the American debate. Give DAOs a European legal home, so that decentralised governance has a compliant form available rather than an offshore default. Develop voluntary cybersecurity standards anchored in a shared catalogue of properties and risks. And respond to the consultation in numbers: the Commission counts responses one by one, so ten aligned submissions from ten entities outweigh one joint letter.

10. Concluding observations

Three structural conclusions emerge from the roundtable. First, the centre of gravity of this consultation is not DeFi but the perimeter: the genuinely contested questions concern circumvention, gatekeeping and the treatment of regulated entities touching decentralised infrastructure, and these can be addressed through interpretation and guidance under existing law. Second, the questions that do concern DeFi proper—what decentralisation is, how it is measured, what assurance about on-chain systems can honestly be given—are not legal questions at all but analytical and technical ones, and they will be answered well or badly depending on whether the Union invests in shared infrastructure: a taxonomy that makes the object legible, and a property catalogue that makes assurance verifiable. Programmable finance, to state the Institute's standing thesis, must be provable finance; a regulator that cannot say what must be proved, of what kind of object, has no business certifying anything. Third, the window for getting the groundwork right is the review period itself. The legislative machine, once engaged, will run for years on whatever definitions it is fed at the start; the work of the coming twelve months is to make

sure those definitions exist, and that they are right.

This compte rendu was prepared by the Intelligence Economy Institute on the basis of notes taken by Zakaryae Boudi during the proceedings. Remarks are reported without attribution. Any errors of transcription or synthesis are the author's own. The Blockchain Property Ontology referenced in Section 6 is maintained at https://github.com/TKNFRA/blockchain-property-ontology.