

Building Europe's Onchain Financial System

Aave Labs' response to the European Commission's targeted consultation on the review of the Markets in Crypto-Assets Regulation (MiCA)

Date: 30 September 2026

Aave Labs welcomes the opportunity to respond to the European Commission's targeted consultation on the review of MiCA. Aave Labs' group includes the Push entities, which provide onboarding and off-boarding between fiat currency and stablecoins: Push Virtual Assets Ireland Limited, a crypto-asset service provider authorised by the Central Bank of Ireland under MiCA and passported to every other European Economic Area member state except Bulgaria, and Push's UK entities, which are regulated by the Financial Conduct Authority. This response draws on our experience of regulated financial services in the EU and of decentralised finance infrastructure globally.

Executive Summary

Finance is moving onchain. Governments, banks and asset managers are issuing bonds, fund units and deposits as tokens. The Eurosystem now accepts DLT-issued securities as collateral and, through Pontes, settles tokenised transactions in central bank money. Every day, stablecoin liquidity is supplied, borrowed and settled on public blockchains around the clock. The question for this review is no longer whether Europe's financial system will run on distributed ledgers. It is which infrastructure it will run on, and whose rules will shape it.

MiCA gave Europe a head start: the world's first comprehensive rulebook for crypto-assets. This review decides whether Europe builds on that lead or loses it. One path leads to open, interoperable infrastructure that connects European savers, banks and markets to global liquidity under clear, proportionate rules. The other rebuilds the fragmentation of today's markets in digital form, in closed networks that liquidity and innovation will simply route around.

Our message: regulate financial intermediaries, not open-source software

Technology is an instrumentality. Using a smart contract should not take an activity outside regulation, and it should not turn software into a regulated person. What matters is whether there is a financial intermediary: an identifiable legal person that controls an activity and exercises active, ongoing discretion over it, deciding whom to serve, on what terms, and with whose assets. Where such an intermediary exists, regulate it according to the economic substance of what it does. Aave Labs lives by this principle: our subsidiary Push is a MiCA-authorised crypto-asset service provider supervised by the Central Bank of Ireland. But

where open-source software executes pre-disclosed rules that no one can unilaterally change, there is no intermediary for obligations to attach to. Writing or publishing open-source software is not providing a financial service: developers who neither control user assets nor exercise discretion over a service are not intermediaries and should not be treated as such. Trying to force the fit does not protect European users. It cuts them off from a highly beneficial technology that is fast becoming the infrastructure layer of onchain finance, while the rest of the world builds on it.

That is not a call for less oversight. It is a call to put oversight where it works: on the entry points where intermediaries serve EU users, on voluntary, industry-developed disclosure and security standards for protocols, and on supervisors equipped to read the ledger directly.

What Europe stands to gain

Better outcomes for savers. DeFi lending gives EU citizens something historically reserved for institutions: direct access to secured, market-priced lending. A saver who supplies idle stablecoins is paid by borrowers who have posted collateral worth more than their loans, on terms visible to everyone in real time. That is the Savings and Investments Union's ambition for households, delivered in onchain financial markets.

Deeper, more liquid capital markets. As bonds, fund units and treasuries become tokenised, onchain lending markets let holders borrow against them rather than sell, and will evolve into repo, securities lending and margin financing on public, auditable rails.

A genuinely single market. A permissionless lending market is one cross-border pool by default. A saver in Lisbon and a borrower in Helsinki use the same market on the same terms: the integration the EU has pursued for decades, available today.

Better supervision, not less. Public blockchains give supervisors something no traditional system does: real-time, tamper-proof data on every position, collateral balance and liquidation, open to them without anyone's permission. Programmable compliance goes further, enforcing eligibility, sanctions and collateral rules at the moment of each transaction rather than detecting breaches after the fact.

What we ask the Commission to do

1. **Draw the perimeter around control, not technology.** Regulate financial intermediaries, meaning identifiable legal persons who control an activity and exercise ongoing discretion over it. Do not treat open-source, non-custodial software, or the developers who write it, as intermediaries (Q45, Q46, Q61, Q64).
2. **Regulate intermediaries, not the software.** Set proportionate obligations for CASPs that connect their clients to DeFi, not for front-ends that let people use DeFi from their own self-custodial wallets, and support voluntary, industry-developed disclosure and security standards that CASPs can rely on in their due diligence. Do not make protocol certification a de facto licence for software (Q62–Q65, Q67).

3. **Do not extend the interest ban to lending or staking.** MiCA's ban stops issuers and CASPs paying holders for holding a stablecoin. A lending return is different: borrowers pay it to use the asset, and the lender bears the risk, just as with lending euros, bonds or equities. Staking rewards are paid by the protocol for securing the network. Europeans have a right to manage their own finances, and lending their own stablecoins through non-custodial protocols gives them a savings channel beyond bank deposits. Extending the ban would make MiCA stablecoins the least useful in onchain markets, take away institutions' tools for treasury, liquidity and financial risk management, entrench the dollar's dominance, and close a savings channel the Savings and Investment Union should want (Q59).
4. **Keep global liquidity open to Europe.** EU citizens and institutions need access to well-managed stablecoins, including global and multi-issuer ones, and the ability to move quickly between currencies. Measures that fragment that liquidity, such as non-fungible EU tokens or redemption rights conditioned on CASP custody, would cut EU users off from the global liquidity that onchain financial markets run on. Well-supervised multi-issuance is also how euro stablecoins can circulate worldwide, strengthening the euro's international role, including as a global reserve currency (Q27, Q38).
5. **Protect self-custodial finance as a right.** Europeans should be able to hold, use and lend their own assets without an intermediary, a right grounded in Article 17 of the EU Charter of Fundamental Rights. Anti-money-laundering obligations already apply where self-custodial wallets meet regulated firms, under the Transfer of Funds Regulation; supervisory data gaps should be closed through reporting, CASP-level controls and onchain analytics, not by disfavouring self-custody (Q29, Q35, Q64).
6. **Judge digital money by what matters.** Whether it is a central bank digital currency, a tokenised deposit or a stablecoin, digital money should be high-quality, well-managed, widely accessible, interoperable across blockchains and judged on whether it holds stable value, not only on its use for payments. Onchain finance should preserve the two-tier monetary system, with tokenised central bank money as its anchor and tokenised commercial bank money alongside it, and leave room for well-managed stablecoins, rather than rely on central bank money alone (Q10, Q74).
7. **Open public infrastructure to banks and market infrastructure.** Align the EU's implementation of the Basel cryptoasset standard with the Committee's ongoing review and assess networks on their actual resilience, apply DORA at the application layer, and keep Pontes and Appia open to public networks. Large public blockchains are more resilient, not less.
8. **Give tokens a harmonised legal home.** Divergent national property laws leave onchain collateral legally uncertain. We propose an optional, control-based EU regime for the private-law treatment of tokens, and Aave Labs stands ready to contribute to its design (Q80, Q82).

9. **Equip supervisors for onchain finance.** Supervisory observer nodes, shared onchain analytics, voluntary machine-readable risk disclosures, embedded-supervision pilots and supervisory tech sprints, in which Aave Labs would be glad to take part (Q29, Q86).

Where we agree with Europe's supervisors

Much of what supervisors are asking for, we support. Regulatory classification should follow economic substance, not technology. Tokenised financial instruments belong under MiFID, not MiCA (Q1). Custodial crypto lenders that re-lend client assets on opaque terms should be regulated (Q67). And fixed bank-deposit minimums for stablecoin reserves should give way to risk-sensitive liquidity requirements, because concentrated deposits transmit redemption shocks straight into banks (Q29). Our disagreements are narrower than they may appear: they concern whether rules designed for intermediaries should be stretched to cover software that has none.

About Aave Labs

Aave began in Europe. It was founded in 2017 as ETHlend by Stani Kulechov, then a student at the University of Helsinki. It has since grown into one of Europe's first DeFi success stories: the Aave Protocol is today the largest decentralised collateral protocol, deployed across more than fifteen blockchain networks, and Aave Labs is its core service provider. Alongside Push, our MiCA-authorized subsidiary, Aave Horizon, our institutional market, enables qualified investors to borrow against tokenised real-world assets under eligibility rules set by the assets' issuers and enforced onchain. We see every day both what onchain finance can deliver and what regulation needs to get right, and we want Europe, where Aave started, to lead it.

Europe wrote the world's first comprehensive rulebook for crypto-assets. With this review, it can write the first rulebook for onchain finance.

Linda Jeng
Chief Legal & Policy Officer, Aave Labs

Responses to the Consultation Questions

Each question is reproduced as written in the Commission's targeted consultation document, including response options and rating scales where relevant (footnotes omitted), followed by Aave Labs' response. Numbering follows the consultation document; Aave Labs responded to the questions most relevant to onchain finance.

Part 1 — Scope and Definitions (Title II Crypto-Assets)

Question 1

Should crypto-assets that qualify as financial instruments as defined in Directive 2014/65/EU of the European Parliament and of the Council, continue to be governed by sectorial legislation (MiFID/MiFIR/MAR/Prospectus Regulation, etc.), or should all assets that are recorded and transacted on distributed ledgers and that meet the definition of a crypto-asset, or the services provided on such assets, in principle be covered by MiCA?

☒ **Yes, they should remain under the main sectoral legislation**

☐ *No, all crypto-assets, or the services provided on such assets, should be covered by MiCA*

If the answer is "Yes", is the distinction between financial instruments governed by MiFID and crypto-assets governed by MiCA sufficiently clear, also taking into account ESMA's guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments?

☐ *Yes, sufficiently clear*

☒ **No, clarification is needed**

If the answer to the previous question is "No" please explain your response and suggest any policy actions for clarification if needed.

Aave Labs response

Yes, they should remain under the main sectoral legislation; and No, clarification is needed on the distinction. Aave Labs supports maintaining the existing division of labour between MiFID/MiFIR and MiCA rather than collapsing all DLT-recorded assets into a single regime. As with the CASP and DeFi questions addressed later in this submission, the question that matters is where the regulatory perimeter should sit, not which technology happens to record the asset: the distinguishing question should remain the economic function and rights attached to the asset — whether it represents a security, a payment instrument, or a non-security crypto-asset — not the technology used to record and transfer it. Folding financial instruments into MiCA merely because they sit on a ledger would create duplicate, and potentially conflicting, disclosure and conduct regimes for the same economic exposure, and would be a significant step backward for legal certainty at exactly the moment MiCA is trying to establish it.

That said, Aave Labs agrees the MiFID/MiCA boundary is not yet fully settled in practice, particularly for governance tokens, liquidity-provider (LP) positions, and yield-bearing wrapped tokens (such as interest-bearing aTokens generated by lending protocols) that

could arguably be characterised as either a crypto-asset or, in some interpretations, a transferable security or unit in a collective investment undertaking. We recommend that any clarification take the form of guidance and interpretive examples (building on the ESMA Article 2(5) guidelines and the joint ESA classification test) rather than a wholesale re-scoping of MiCA, and that DeFi-native asset types (LP tokens, receipt tokens, governance tokens with no profit-participation rights) be addressed explicitly as worked examples.

More fundamentally, we would encourage the Commission to treat this question as inseparable from the tokenisation of financial instruments themselves, not just of non-security crypto-assets. Keeping MiFID/MiFIR as the home for tokenised financial instruments only works well if MiFID/MiFIR's own trading, clearing, and settlement rules are updated to reflect what DLT actually makes possible – atomic delivery-versus-payment, near-instant settlement, and programmable, smart-contract-executed corporate actions – rather than assuming a tokenised security must still clear and settle through the same intermediated, T+1/T+2 infrastructure built for paper and book-entry securities. The SEC's own review of Regulation NMS and related market-structure and transfer-agent rules to accommodate tokenised (on-chain) securities and round-the-clock trading is a useful reference point: it shows a major securities regulator treating tokenisation not as a side note to existing market-structure rules but as a reason to actively revisit them. We would encourage the Commission to undertake a comparable, dedicated look at whether MiFID II/MiFIR, CSDR, and EMIR's trading, clearing, and settlement provisions remain fit for purpose for tokenised financial instruments, alongside (not instead of) the MiCA/MiFID scope question this question asks directly.

Question 2

To what extent have ESMA's MiCA Article 2(5) guidelines and the joint ESA standardised classification test reduced uncertainty in practice? Which borderline cases remain difficult? Please explain your response and suggest any policy actions for clarification if needed.

Aave Labs response

The guidelines and classification test have helped for the clearest cases (e.g. plainly utility-only tokens, plainly security-like tokens) but leave a meaningful grey zone for DeFi-native instruments that do not map cleanly onto traditional finance categories. Three categories remain genuinely difficult in practice: (i) governance tokens whose value derives partly from control rights over protocol parameters and treasury rather than profit rights, (ii) receipt tokens issued automatically by a smart contract when a user supplies an asset to a lending or liquidity pool (e.g. aTokens), which simply record the user's own supplied assets rather than being a separately designed investment product, but whose treatment under the classification test remains unclear, and (iii) multi-function protocol tokens that combine governance rights with staking roles, such as backstopping a protocol against shortfalls, and whose economic characteristics can change over time as governance evolves the protocol.

The deeper structural issue is that both the financial-instrument test and the standardised EMT/ART/crypto-asset test are built around a discrete issuance event, an identifiable offeror or issuer who can make (and sign, in the case of the Article 17/18 legal opinion for ARTs) a classification declaration at a single point in time, typically when a token is first offered to the public or admitted to trading. That structure fits a traditional token sale reasonably well, but it fits poorly for DeFi-native tokens that are minted or distributed continuously by protocol-level mechanisms rather than sold in a one-time offering – for example, a receipt token issued automatically whenever a user supplies an asset, or a governance token distributed on an ongoing basis through DAO-administered emissions. These same tokens often combine features that the framework assumes belong to separate categories, holding a governance right or economic entitlement that can read somewhat like a security-type right alongside a network-utility or collateral role that reads more like a plain crypto-asset. Neither the 'is it a financial instrument' test nor the EMT/ART/crypto-asset flowchart has a clean answer for a token of this kind, because both presume a 'moment' and a 'someone' to make the call, and a continuously operating, non-custodial, DAO-governed protocol does not straightforwardly have either. We would note this is not a hypothetical concern specific to MiCA: comparable classification frameworks elsewhere (including the covered-investment-contract structure in the SEC's pending proposed Regulation Crypto Assets, which similarly certifies completion of a discrete issuance process rather than addressing tokens that were never issued that way) run into the same structural gap for mature, continuously-distributed network tokens with mixed characteristics.

Rather than new classification templates, we would ask the Commission to clarify that MiCA's white-paper and classification obligations attach to an identifiable offeror or person seeking admission to trading, and do not arise where tokens are minted or distributed automatically by protocol mechanics without any such person. Receipt tokens are the clearest example. When a user supplies assets to a lending pool, the protocol automatically issues a token that does nothing more than record that user's own supplied assets and the interest accruing on them. It is a receipt, not a new investment product, and no one is offering it to the public. MiCA already recognises this logic for crypto-assets offered for free or created automatically as a reward for maintaining a distributed ledger or validating transactions (Article 4(3)). Extending it expressly to protocol-distributed tokens, receipt tokens in particular, and clarifying how CASPs can meet the white-paper condition in Article 66(3) where no offeror exists, would give predictable and consistent answers across Member States without forcing these tokens through templates designed for a one-time issuance event.

Part 2 — Asset-Referenced Tokens and E-Money Tokens (Titles III and IV)

Question 9

Looking 5-10 years ahead, how strongly do you agree with the following visions for the role of stablecoins in the EU?

For each vision below, please indicate on a scale of 1 to 5 where 1 = Strongly disagree 2 = Rather disagree 3 = Neutral 4 = Rather agree 5 = Strongly agree

- *A mainstream digital means of payment for retail transactions within the EU* — **Aave Labs: 4**
- *A mainstream digital means of payment for wholesale transactions within the EU* — **Aave Labs: 5**
- *A complement to existing payment instruments, used mainly in specific use cases especially in international, cross-border payments* — **Aave Labs: 5**
- *A core infrastructure layer for the digital economy and tokenised financial markets especially for settlement* — **Aave Labs: 5**
- *A niche or transitional product, eventually displaced by other forms of digital money (e.g. CBDCs or commercial bank money innovations)* — **Aave Labs: 1**
- *No clear long-term role can be identified at this stage* — **Aave Labs: 1**
- *Others* — **Aave Labs: 5**

If your answer is "Others", please elaborate.

Aave Labs response

Stablecoins' clearest long-term role is as the settlement and collateral asset of onchain finance (5). They already play it: stablecoins are the main unit of account, collateral and borrowing asset in DeFi lending markets, including the Aave Protocol's, and the natural cash leg for tokenised securities settling on public blockchains. Under 'Others' (5), we would add their role as the base savings asset of onchain lending markets, where holders lend them to borrowers at market rates (Q59).

We strongly agree that stablecoins will become a mainstream means of payment for wholesale transactions within the EU (5), particularly where settlement happens onchain against tokenised assets, alongside tokenised deposits within bank networks and wholesale central bank money through Pontes (Q74). We rather agree that they will become one for retail transactions too (4), as programmable, always-available money that works across wallets, applications and borders. We strongly agree that stablecoins will complement existing payment instruments, especially in international and cross-border payments (5), where they already offer faster, cheaper, round-the-clock settlement than correspondent banking, although we see this as one of several roles rather than their only one.

We strongly disagree that stablecoins are a niche or transitional product to be displaced by CBDCs or commercial bank money innovations (1), and that no long-term role can be identified (1). Different forms of digital money will coexist. Tokenised deposits are claims on a particular bank and work best within banking networks; stablecoins are claims on an issuer that pass freely between holders and across blockchains, which is why they are likely to remain dominant in open onchain markets (Q74). Whether euro stablecoins share in that role depends on this review: risk-sensitive reserve rules (Q29), fungible multi-issuance (Q38) and no extension of the interest ban to lending (Q59).

Question 10

The following question explores the current and potential benefits of stablecoins (both EMTs and ARTs) for different use cases. For each use case below, please indicate on a scale of 1 to 5 how beneficial stablecoins would be for EU users:

1: Not Beneficial, 2: Moderately Beneficial, 3: Neutral, 4: Beneficial, 5: Very Beneficial

- International payments (non-EU cross-border remittances or transfers) — **Aave Labs: 5**
- Intra-EU payments (domestic and EU cross-border payments) — **Aave Labs: 4**
- Crypto trading and liquidity provision — **Aave Labs: 5**
- Retail payments - Person to Person — **Aave Labs: 3**
- Retail payments – Person to Business (POI payment to merchants including e-commerce) — **Aave Labs: 3**
- Retail payments – Business to Business — **Aave Labs: 4**
- Wholesale payments (between financial institutions) — **Aave Labs: 5**
- Settlement of tokenised financial instruments (e.g., digital bonds, securities) — **Aave Labs: 5**
- Corporate treasury management — **Aave Labs: 4**
- Access to programmable or smart contract-based financial services (DeFi applications) — **Aave Labs: 5**
- Provision of financial services in underserved regions in the EU — **Aave Labs: 3**
- Others

If your answer is “Others”, please elaborate.

Please explain shortly your assessment and expectations as regards the benefits of stablecoins for EU users and, where relevant, any potential risks.

Aave Labs response

The benefits are greatest for DeFi, crypto trading, international payments and the settlement of tokenised financial instruments. The DeFi use case is a direct instance of the infrastructure-layer point summarised in our response to Q86: MiCA-compliant euro-denominated stablecoins (and well-designed decentralised stablecoins such as the Aave Protocol's GHO) are foundational collateral and settlement assets within DeFi lending markets: they provide predictable unit-of-account exposure for borrowers and lenders, reduce the volatility risk otherwise inherent in crypto-collateralised borrowing, and enable programmatic, 24/7 settlement of interest accrual, liquidations, and repayments without manual intermediation. The single biggest constraint on realising this benefit today is uncertainty about whether EMT/ART issuers and their smart-contract integrations can serve DeFi protocols without inadvertently triggering CASP-style obligations on the protocol itself; regulatory clarity on this point would materially increase the availability of compliant stablecoin liquidity within EU-accessible DeFi markets.

Question 20

In your view, should the MiCA prohibition on granting interest or any interest-equivalent remuneration be modified?

☐ EMTs: Interest and interest-equivalent remuneration should continue to be prohibited

☒ **EMTs: Interest or interest-equivalent remuneration should be allowed (fully or under defined conditions)**

☐ ARTs: Interest and interest-equivalent remuneration should continue to be prohibited

☒ **ARTs: Interest or interest-equivalent remuneration should be allowed (fully or under defined conditions)**

If you selected "allowed", please explain your reasons (including any benefits and risks) and specify the conditions under which remuneration should be permitted.

Aave Labs response

Interest-equivalent remuneration should be allowed under defined conditions, for both EMTs and ARTs. The conditions are those that distinguish a return for using a token from a reward for holding it: (i) the return is paid by third parties for the use of the tokens, such as borrowers in a lending protocol, or by a protocol for consensus participation, rather than by the issuer; (ii) the holder bears the associated risk, so the return is variable and not guaranteed; and (iii) where a CASP intermediates, it discloses the source, risks and variability of the return and applies suitability safeguards for retail clients (Q67). We do not ask here for issuers to be allowed to pay holders out of reserve income, which is a separate question. Articles 40 and 50 prohibit issuers, and CASPs providing services related to the tokens, from granting interest, defined as any remuneration or other benefit related to the length of time during which a holder holds the token, including net compensation or discounts with an equivalent effect received directly from the issuer or from third parties. The ECB would extend the ban to lending, staking and liquidity mining, and the EBA treats lending returns on stablecoins as 'regulatory arbitrage'. We ask the Commission instead to clarify in Level 1 that 'interest' excludes returns paid by third parties for the use of tokens, including through lending protocols, and staking rewards from consensus participation.

A lending return is not a benefit for holding. While the tokens are lent, the lender does not hold them: it supplies them to borrowers, who pay a market price to use them, and holds only a receipt for its claim. Nor is the return granted by an issuer or a CASP: borrowers pay it through a protocol that grants nothing. It is the price of credit, just as lending euros, government bonds or equities earns a return even though banknotes and e-money pay none (Q59). Nor is it arbitrage, which would mean relabelling the same product: a lending return varies with borrowers' demand and exposes the lender to credit and liquidity risk that a holder of the token alone never bears. Staking rewards are paid by the protocol for securing the network, with the staked assets at risk (Q66).

The ban's purpose is to stop stablecoins becoming interest-bearing substitutes for bank deposits. A lending return does not do that: it is variable, uninsured and risk-bearing, the

opposite of a deposit. The evidence that yield drains bank lending is also weak: in April 2026 the US Council of Economic Advisers found that prohibiting stablecoin yield would raise US bank lending by only about 0.02%, at a net welfare cost, largely because stablecoin reserves recirculate through the banking system. The United States draws the line where we propose: the GENIUS Act prohibits stablecoin issuers from paying yield, without extending the ban to returns earned by lending stablecoins to third parties.

Widening the ban would make MiCA-authorized stablecoins the least useful stablecoins in onchain markets. Europeans, who have a right to manage their own finances, would lose a savings channel beyond bank deposits; institutions would lose tools for treasury, liquidity and financial risk management; and euro stablecoins would be unable to compete with dollar stablecoins that holders can put to work. Where intermediated lending raises consumer-protection concerns, the right response is to regulate it as a service, with disclosure and suitability safeguards, as the EBA itself proposes (Q67).

Question 26

How appropriate is it to require EMT-issuing EMLs to hold 30–60% of their reserve assets in bank deposits?

- ☒ **Not at all appropriate / desirable**
- ☐ *Slightly appropriate / desirable*
- ☐ *Moderately appropriate / desirable*
- ☐ *Mostly appropriate / desirable*
- ☐ *Highly appropriate / desirable*

Please explain your ratings and add any suggestions for recalibration or alternative approaches.

Aave Labs response

Not at all appropriate as a fixed requirement. Bank deposits should remain an eligible reserve asset, but mandating that 30% of reserves, or 60% for significant tokens, sit in bank deposits creates the risks it is meant to reduce. It concentrates reserves in a small number of banks, so that large redemptions fall on those banks' funding at the worst moment, as the March 2023 run on USDC after Silicon Valley Bank's failure showed. It turns stablecoin reserves into short-term wholesale bank funding, sharpening the deposit-substitution channel supervisors are concerned about. And it leaves a large share of reserves earning less than short-term government debt, a standing charge on euro stablecoin issuance that makes euro stablecoins harder to sustain against dollar stablecoins backed largely by Treasury bills and repo (Q27).

We support the ESCB's proposal, and the EBA's openness to assessing it, to replace fixed deposit minimums with daily and weekly liquidity requirements, provided that eligible liquid assets include overnight repo, short-dated high-quality sovereign debt and qualifying money-market funds; that the floors are calibrated to observed redemption behaviour,

including outside banking hours; and that concentration limits are proportionate for smaller issuers (Q29).

Question 27

What are the potential benefits of global stablecoins for different use cases? For each use case below, please indicate on a scale of 1 to 5 how beneficial global stablecoins would be for EU holders:

1: Not beneficial, 2: Moderately beneficial, 3: Neutral, 4: Rather beneficial, 5: Very beneficial

- *International payments (cross-border remittances or transfers,) — Aave Labs: 5*
- *Intra-EU payments (domestic and cross-border EU payments) — Aave Labs: 3*
- *Crypto trading and liquidity provision — Aave Labs: 5*
- *Retail payments - Person to Person — Aave Labs: 3*
- *Retail payments - Person to Business (POI payment to merchants including e-commerce) — Aave Labs: 3*
- *Retail payments - Business to Business — Aave Labs: 4*
- *Settlement of tokenised financial instruments (e.g., digital bonds, securities) — Aave Labs: 5*
- *Corporate treasury management — Aave Labs: 5*
- *Access to programmable or smart contract-based financial services (DeFi applications) — Aave Labs: 5*
- *Provision of financial services in underserved regions in the world — Aave Labs: 5*

Other potential use cases (please specify)

Please explain shortly your assessment and expectations as regards the use cases of global stablecoins (EMTs/ARTs) and the benefits for EU users.

Aave Labs response

The benefits are greatest where global stablecoins supply liquidity that has no euro-denominated equivalent of comparable depth today: cross-border payments, crypto trading, DeFi, settlement of tokenised financial instruments and corporate treasury management, and in extending financial services to underserved regions of the world. For domestic and intra-EU retail payments, instant euro credit transfers and euro-denominated tokens are better placed, so we rate the added benefit of global stablecoins there as neutral. Global (non-EU-issued) stablecoins currently supply a large share of the liquidity used as collateral and borrow/lend assets across DeFi money markets, including the Aave Protocol's markets. Restricting EU users' access to this liquidity without an adequate EU-issued or equivalence-qualified alternative would reduce the depth and efficiency of EU-accessible DeFi markets and cut EU users off from the global liquidity that onchain financial markets run on, without making them any safer. We support developing an equivalence or passporting mechanism that preserves EU access to well-managed global stablecoins while addressing

the legitimate reserve-fragmentation and run-risk concerns raised elsewhere in the consultation.

This question is also where the competitiveness point summarised in our response to Q86 bears most directly on stablecoins. Roughly 99% of stablecoin supply in circulation today is US-dollar-denominated, and reserve economics are part of the reason: US issuers can hold reserves largely in short-term Treasury bills and repo, earning close to market rates and supporting a commercially viable business, whereas frameworks that require a large share of reserves to sit in low-yielding or unremunerated form act, in effect, as a standing charge on issuance. Aave Labs raised this with the Bank of England in our response to its stablecoin consultation, where an unremunerated reserve floor would cost a systemic issuer well over 100 basis points of yield on its entire reserve before operating costs. MiCA does not go that far, but its requirement that at least 30% of reserves (60% for significant tokens) be held as bank deposits can leave a large share of reserves earning less than short-term government debt, concentrated in a few banks. We therefore welcome the ESCB's proposal, and the EBA's openness to assessing it, to replace these fixed deposit minimums with risk-sensitive liquidity requirements (Q29), which would narrow the gap. Reserve reform alone will not make euro stablecoins competitive, however: they also need access to deep, fungible liquidity, including through multi-issuance (Q38), and room to be used across DeFi (Q59). Until a genuinely competitive euro-denominated alternative exists, restricting EU users' access to non-EU stablecoins would not strengthen the euro's role in crypto markets; it would simply reduce liquidity and functionality for EU DeFi users. We would encourage the Commission and the ECB to treat reserve economics for MiCA-compliant issuers as a competitiveness question in its own right, not only a prudential one.

We recognise that the predominance of dollar stablecoins also raises a legitimate monetary-sovereignty concern for the ECB, particularly if dollar tokens came to be widely used as a means of exchange within the euro area. In our view the effective answer to that concern is the one set out above: making MiCA-compliant euro stablecoins commercially competitive and deeply integrated into DeFi markets, so that euro liquidity is available on-chain where users need it. Restricting EU users' access to dollar liquidity would reduce functionality without creating a euro alternative.

Question 28

How important is it for EU users (both people and businesses) to be able to access global stablecoins via EU-based and licenced issuers and CASPs? Please indicate on a scale of 1 to 5.

1 Not important at all, 2 Moderately important, 3 Neutral / no clear preference, 4 Rather important, 5 Highly important

- *EU-based and licenced stablecoins issuers* — **Aave Labs: 5**
- *EU-based and licenced CASPs* — **Aave Labs: 5**

Please explain shortly your reply.

Aave Labs response

Highly important for both (5). Global stablecoins supply most of the liquidity used for settlement, collateral and lending in onchain markets, including the Aave Protocol's (Q27). Access through EU-licensed issuers, including EU entities within multi-issuance arrangements, and through EU-authorized CASPs lets EU people and businesses use that liquidity inside the MiCA framework, with EU redemption rights and EU supervision. The alternative is not safer liquidity but thinner markets: smaller EU-only pools, wider spreads and fewer ways to move between currencies. Access should be preserved through fungible multi-issuance (Q38) and an equivalence regime (Q40), not restricted.

Question 29

Based on your experience and assessment, how significant are the following risks associated with a multi-issuance model of global stablecoins for the EU financial system?

Please rate each risk on a scale from 1 (Irrelevant) to 5 (Very significant).

- *Run risk and reserve depletion in the EU (e.g. cross-border migration of tokens during stress leading to sudden increase of redemption pressure on EU issuers)* — **Aave Labs: 3**
- *Unbalanced reserve distribution across jurisdictions (e.g. fragmentation of reserves between EU and non-EU entities)* — **Aave Labs: 2**
- *Cross-border reserve transfer restrictions (e.g. third-country limitations on moving reserves during stress events)* — **Aave Labs: 3**
- *Regulatory arbitrage due to fungibility of tokens (e.g. operation across regimes exploiting differences in prudential or conduct rules)* — **Aave Labs: 2**
- *Supervisory monitoring and data-tracking challenges (e.g. difficulty measuring EU-holdings, especially holdings in self-custodial wallets)* — **Aave Labs: 3**
- *Risks resulting from the stablecoin issuer home jurisdictions not having prudential or conduct rules that meet internationally accepted standards or that are significantly lower than those set out in EU law.* — **Aave Labs: 3**
- *Others*

If your answer is "Others", please elaborate.

Please explain the reasoning behind your ratings above. Describe the nature and importance of these risks, the underlying assumptions, market dynamics, or regulatory factors informing your view.

Aave Labs response

We rate these risks as real but manageable. Self-custodial wallets pose a monitoring and data challenge, not a reason to restrict or disadvantage self-custody itself. The inability of a supervisor to see real-time balances in a non-custodial wallet is a data-visibility limitation inherent to any system that respects self-custody as a legitimate form of asset holding — it is not evidence of elevated risk per se. Reserve, run-risk, and concentration risks are properly

addressed at the issuer level (through the reserve, liquidity, and reporting requirements already in Titles III/IV), not by degrading the treatment or usability of tokens held in self-custodial wallets.

Two kinds of visibility are often conflated: individual attribution (linking a specific wallet to a specific natural or legal person and their jurisdiction) and aggregate systemic visibility (total circulating supply, concentration, transfer flows, and velocity across the whole stablecoin float). Self-custodial wallets genuinely limit the first. They do not limit, and in important respects improve, the second. A public blockchain records every issuance, redemption, and transfer of an EMT/ART on an immutable, real-time, and universally auditable ledger; a supervisor can observe total supply, holder concentration, and flow patterns as they happen, using standard on-chain analytics, without waiting for periodic issuer disclosures or relying on bilateral data-sharing arrangements with custodians. That exceeds the aggregate transparency of bank deposits or custodial e-money, where a supervisor sees only what the institution reports, on a lag.

The Commission should weigh this transparency benefit explicitly, not assess self-custodial holding only by what supervisors cannot see. A run on a stablecoin, a sudden concentration of holdings, or an unusual velocity spike is easier to detect early on a transparent public ledger than in a custodial or bank-deposit system where the underlying flows are only visible to the institution itself. Measures that push holders away from self-custody and toward custodial CASPs in the name of financial stability (such as the redemption-rights restriction discussed in Q38) would trade a data-visibility gap that mainly affects individual attribution for a real loss of the aggregate, real-time transparency that self-custodial, on-chain holding currently provides. The better path is to pair issuer-level reporting and transaction-analytics cooperation (addressing the individual-attribution gap) with continued reliance on, and where useful formal recognition of, on-chain transparency as a genuine financial-stability monitoring tool in its own right.

This approach has institutional support: Raphael Auer's BIS Working Paper No. 811, 'Embedded supervision: how to build regulation into blockchain finance' (2019), sets out how supervisors can monitor compliance by reading a distributed ledger directly rather than relying on firms to collect, verify and report data. We would encourage the Commission to treat embedded supervision as a complement to issuer reporting, a capability public blockchains offer and traditional deposit systems do not.

A further financial-stability concern is deposit substitution: stablecoin growth could shift stable retail bank funding into more concentrated, potentially more volatile wholesale funding where reserves are placed as bank deposits, or move funds out of bank intermediation altogether. MiCA's requirement that 30% of reserves (60% for significant tokens) be held as bank deposits sharpens the first channel, because large redemptions then fall on a concentrated set of banks, as the March 2023 run on USDC after Silicon Valley Bank's failure showed. We therefore support the ESCB's proposal, and the EBA's openness to assessing it, to replace fixed deposit minimums with daily and weekly liquidity requirements, provided that (i) eligible liquid assets include overnight repo, short-dated high-quality

sovereign debt and qualifying money-market funds; (ii) the floors are calibrated to observed redemption behaviour, including outside banking hours; and (iii) concentration limits are proportionate for smaller issuers. Reserve reform would ease the economics discussed in Q27, but will only make euro stablecoins competitive if paired with fungible multi-issuance (Q38) and no extension of the yield ban to DeFi (Q59). Euro-denominated stablecoin supply is today very small relative to euro-area bank deposits, so these risks can be mitigated, monitored and managed as the market grows.

Question 35

MiCA requires that the reserves of the EMTs and ARTs issued, offered or held in the EU should be held in the EU. Can the tokens held in the EU be determined or estimated with sufficient accuracy and frequency?

- ☐ Yes, EU holdings can be determined with sufficient accuracy and frequency
- ☒ **Partially, but with some limitations (e.g., delays, estimation challenges)**
- ☐ No, current methods are insufficient for reliable compliance
- ☐ Uncertain

Please explain your reply to the above question, including any specific remarks with regard to tokens held in unhosted wallets.

Aave Labs response

Partially, but the question conflates the reserves with the tokens. The reserves themselves can be measured precisely: an issuer knows its reserve assets and its outstanding issuance, every issuance and redemption is recorded on-chain, and both can be disclosed in real time. What cannot be determined reliably is where each token's holder is located once tokens circulate, particularly in self-custodied ('unhosted') wallets, since wallet addresses are not linked to residency. The underlying objective is to ensure that tokens circulating in the EU are backed by reserves held in the EU, so that EU holders can redeem against them. That is best achieved by requiring the EU-authorized issuer to hold in the EU reserves covering all the tokens it has issued, which can be measured exactly and continuously. In multi-issuance schemes, where tokens issued outside the EU may be redeemed through the EU issuer, the complement is a binding arrangement for reserves to follow redemptions, backed by supervisory cooperation (Q38). Estimating EU holdings instead, and penalising self-custody users for a measurement gap they did not create, for example through differentiated redemption rights (Q38), would be less accurate and more intrusive.

Closing the attribution gap in the only way that would work — linking self-custodial wallet addresses to the identity and residency of the people who control them — would also raise a serious data-protection problem. It would mean systematically identifying and geolocating natural persons on the basis of their private financial holdings, which sits uneasily with the GDPR's purpose-limitation and data-minimisation principles (Articles 5(1)(b) and (c)); would need a specifically drafted legal basis (most plausibly Article 6(1)(e)) rather than one inferred from MiCA's reserve provisions; would likely require a data protection impact assessment

under Article 35; and would sit in tension with Articles 7 and 8 of the EU Charter of Fundamental Rights. That is an independent reason to anchor the requirement to issuance rather than to holder location.

The ECB/ESCB's own 24 September 2026 response illustrates the tension we describe above. It acknowledges directly that it is 'not feasible to ascertain whether stablecoins held in non-custodial wallets are held by parties within or outside the EU,' yet in the same response proposes a 'Union holder' definition that explicitly extends to non-custodial wallet holdings, framed as anti-circumvention. We would highlight this as a live example of the problem: a definition that reaches a population the ECB itself concedes it cannot reliably identify either goes unenforced in practice, or is enforced only by pushing self-custody users toward exactly the wallet-identity-linkage or CASP-custody requirements we caution against above on both practical and GDPR grounds. We would encourage the Commission to calibrate any 'Union holder' concept to holdings that can actually be attributed – principally custodial and CASP-intermediated holdings – and to anchor reserve requirements to issuance, relying on the aggregate, real-time on-chain transparency described in Q29 for the remainder.

We recognise that supervisors are concerned about holdings they cannot observe or attribute, and we take that concern seriously. But the starting point should be that people have the right to hold and manage their own assets and finances. Self-custody is the digital equivalent of holding cash or other bearer assets oneself, and reflects the right to own, use and dispose of one's possessions protected by Article 17 of the EU Charter of Fundamental Rights. EU law already accommodates self-custody rather than prohibiting it; the Transfer of Funds Regulation, for example, sets specific rules for transfers involving self-hosted addresses. Supervisory data gaps should therefore be closed through issuer reporting, CASP-level controls and on-chain analytics (Q29 and the supervisory proposals in our response to Q86), not by treating self-custody as a disfavoured way of holding assets.

Question 36

Should MiCA redemption rights be explicitly limited to EU holders only?

☐ Yes

☒ **No**

Please explain your response. If you indicated "Yes, what criteria should be used to determine who qualifies as an EU holder? Please also provide a rationale for your proposed approach.

Aave Labs response

No. Limiting MiCA redemption rights to 'EU holders' would require knowing where each holder is located, which, as the ECB/ESCB itself acknowledges, is not feasible for tokens held in self-custodial wallets (Q35). In practice it would become a rule that only clients of EU-authorised CASPs can redeem, penalising self-custody and every EU user who holds stablecoins directly or uses them as collateral in non-custodial protocols (Q38). It would also

make EU-issued tokens less fungible and less useful globally, undercutting the international role of the euro that multi-issuance can support.

The underlying concern, that non-EU holders could redeem against EU reserves in stress, is better addressed at issuer level. EU-authorized issuers should hold in the EU reserves covering all the tokens they issue, which can be measured exactly and continuously, and multi-issuance arrangements should include binding rules for reserves to follow redemptions, backed by supervisory cooperation between home and host authorities (Q35, Q38).

Question 37

In a multi-issuance model, reserve assets may be located across jurisdictions and legal entities. Concerns have been expressed that in times of market stress, the transfer or rebalancing of reserves between issuers may be delayed or restricted. Is this concern valid or substantiated in your view?

☐ Valid-substantiated

☒ **Not valid-not substantiated**

Please explain your response

Aave Labs response

Not substantiated, although the concern is understandable in principle. To our knowledge, no multi-issuance stablecoin has had its reserves blocked from moving between jurisdictions in stress, and the risk can be removed by design rather than managed by restricting the model. First, each EU-authorized issuer should hold in the EU reserves covering all the tokens it has issued, which can be measured exactly and continuously (Q35); EU holders redeeming against the EU issuer are then covered whatever happens elsewhere. Second, where tokens issued outside the EU are redeemed through the EU issuer, arrangements should include binding, pre-agreed rules for reserves to follow redemptions, backed by home-host supervisory cooperation and, where calibrated, a dedicated liquidity buffer (Q38). Third, high-frequency reporting of reserves by location makes any imbalance visible early (Q29). These measures address the concern directly. Making EU-issued tokens non-fungible with their global counterparts, as the ESRB and ECB propose, would not: it would split one liquid market into two thinner ones and remove the benefits multi-issuance brings to EU users and to the euro's international role (Q38).

Question 38

How effective would the following possible additional measures be in mitigating such concerns?

1 = Highly ineffective, 2 = Somewhat ineffective, 3 = Neutral / uncertain, 4 = Somewhat effective, 5 = Highly effective

- *Introducing requirements that would favour or strengthen the redemption rights of holders of stablecoins that are genuinely circulating in the EU, as opposed to*

redemption rights associated with stablecoins transferred to the EU in times of stress to take advantage of MiCA protections (including redemption rights) — Aave Labs: 2

- Restricting direct redemption rights in the EU to holders who are clients of EU-authorized CASPs, while holders that keep the tokens in un-hosted wallets do not have a MiCA guaranteed redemption right in the EU. — Aave Labs: 1*
- Differentiating redemption rights in crisis situations between retail and wholesale/professional holders — Aave Labs: 2*
- Requiring a dedicated liquidity buffer or additional reserve tranche specifically calibrated to cover short-term redemption spikes in the EU — Aave Labs: 3*
- Strengthening real-time or high-frequency reserve and liquidity reporting to EU competent authorities, including granular disclosure of reserve location and transfer constraints — Aave Labs: 4*
- Establishing binding cooperation arrangements between home and host supervisors to ensure rapid approval and execution of cross-border reserve transfers in stress scenarios — Aave Labs: 4*
- Others*

If your answer is "Others", please elaborate.

Aave Labs response

Aave Labs strongly opposes this specific measure as drafted. Conditioning a stablecoin's redemption guarantee on the token being held through an EU-authorized CASP would functionally penalise self-custody and materially disadvantage every non-custodial DeFi protocol that relies on that stablecoin as collateral or borrow/lend liquidity – including the Aave Protocol. Rating: 1/5 (not effective / actively harmful) for this specific measure. A user who supplies USDC or a euro-denominated EMT as collateral into the Aave Protocol, or borrows it out, would lose a core consumer protection purely because the asset passed through a smart contract rather than a licensed intermediary, even though the smart contract's behaviour is transparent and auditable. This would create a strong incentive to route stablecoin activity back through custodial intermediaries, working against MiCA's own objective of enabling safe, transparent on-chain finance.

We would support instead: strengthened real-time reserve and liquidity reporting by issuers (rated 4/5), binding home/host supervisory cooperation on cross-border reserve transfers (rated 4/5), and a dedicated liquidity buffer for short-term redemption spikes (rated 3/5) – each of which addresses the underlying run-risk concern without discriminating against self-custody or non-custodial protocol usage. We rate 2/5 both favouring redemption rights for stablecoins 'genuinely circulating' in the EU, which is hard to define and would undermine fungibility, and differentiating crisis redemption rights between retail and wholesale holders.

More fundamentally, this question should not be assessed only as a risk to be mitigated; multi-issuance global stablecoin models also serve a genuine need that a purely EU-only issuance model cannot. EU institutions and persons – banks and corporates managing cross-border treasury and settlement, and DeFi users and protocols such as the Aave

Protocol relying on deep, fungible stablecoin liquidity as collateral and borrow/lend assets — need access to the same global liquidity pool that non-EU users draw on, not a smaller, EU-only-issued token confined to EU trading venues. This includes the ability to convert quickly and reliably out of a euro-denominated token into other major-currency stablecoins such as US-dollar stablecoins for cross-border payments, multi-currency treasury management, and FX-like liquidity operations, much as institutions rely on deep FX markets today. A multi-issuance structure, in which an EU-authorized issuer and non-EU affiliated issuers jointly issue a single fungible global stablecoin under a shared brand and reserve arrangement, lets EU users tap into that global liquidity depth and currency conversion capability while still transacting through an EU-authorized, MiCA-supervised issuer. Measures that make multi-issuance less attractive to operate, including conditioning redemption rights on CASP custody, risk pushing EU users toward thinner EU-only liquidity or toward non-EU stablecoins with no EU-authorized issuer at all. We would encourage the Commission to weigh this benefit alongside run-risk concerns and to prefer the supervisory-cooperation and reporting measures above.

Multi-issuance also matters for the euro itself. A euro-denominated stablecoin issued jointly by an EU-authorized issuer and affiliated issuers in other jurisdictions can be distributed and redeemed locally around the world, putting the euro in the hands of users and institutions that EU-only issuance would never reach. As dollar stablecoins have shown, that global circulation also builds demand for the currency's short-term government debt through the reserves backing it. Well-supervised multi-issuance is therefore one of the most direct ways to strengthen the international role of the euro, including its standing as a global reserve currency, and a direct answer to the dollar-dominance concern in Q27. Requiring EU-issued tokens to be non-fungible with their non-EU counterparts would close off that opportunity.

We would also flag that both the EBA and the ECB/ESCB go further than the specific redemption-restriction measure addressed above. The EBA proposes a dedicated third-country multi-issuance regime (a new significance criterion, an equivalence baseline with strict reciprocity, prior supervisory non-objection, possibly higher own funds); the ECB/ESCB endorses the ESRB's equivalent recommendation and adds that any EU-issued token in such a scheme must not be fungible with its non-EU counterpart. We share the interest in addressing run and fragmentation risk, but non-fungibility in particular would defeat multi-issuance's core purpose, splitting one global liquidity pool into two smaller, siloed ones — the opposite of the liquidity-access benefit this answer describes. We would encourage any regime to preserve, not foreclose, that access.

Question 40

Do you see merit in introducing an equivalence regime for global stablecoins in the EU?

- ☐ *Yes but only if other mitigation measures are not introduced*
- ☒ **Yes, in addition to mitigation measures**
- ☐ *No*

Please provide reasons for your response, including any perceived advantages or disadvantages of equivalence regimes.

Aave Labs response

Yes, in addition to mitigation measures. An equivalence regime is the most direct way to preserve EU access to well-managed global stablecoins while ensuring that their issuers meet standards comparable to MiCA's (Q27, Q28). It should sit alongside the mitigation measures that address run and fragmentation risk without restricting how tokens are held: high-frequency reserve and liquidity reporting, binding home-host cooperation on cross-border reserve transfers and, where calibrated, a dedicated liquidity buffer (Q38). It should not be combined with measures that would defeat its purpose, such as requiring EU-issued tokens to be non-fungible with their global counterparts or conditioning redemption on CASP custody.

Equivalence should be outcome-based, assessing whether the third-country regime delivers comparable reserve quality, redemption rights, supervision and cooperation, rather than requiring identical rules. It should also be reciprocal where possible, so that euro stablecoins gain comparable access to other markets, supporting the international role of the euro.

Part 3 — Legal Framework for Crypto-Asset Service Providers

Question 45

Is the list of crypto-asset services as defined in Article 3(16) of MiCA adequate to effectively cover crypto-asset markets and provide sufficient legal clarity for businesses?

☒ **Yes**

☐ **No**

Aave Labs response

Yes. Article 3(1)(16) appropriately defines crypto-asset services by reference to specific activities performed for clients — custody, exchange, execution, reception and transmission of orders, advice, portfolio management and transfer services — and that activity-based approach should be preserved rather than expanded to regulate underlying decentralised technology merely because it can be used in connection with crypto-asset services. This is particularly important for decentralised protocols: Recital 22 recognises that crypto-asset services provided in a fully decentralised manner without any intermediary should fall outside MiCA, while MiCA can apply where an identifiable person performs, provides or controls a regulated crypto-asset service, including where elements of that service are decentralised. We consider that distinction fundamentally sound.

Greater legal certainty would nevertheless be valuable as to how that distinction applies in practice. In particular, the Level 1 framework should make clearer that genuinely non-custodial protocols operating through autonomous smart contracts, where no identifiable person provides or controls a listed crypto-asset service on behalf of users, are not themselves CASPs merely because their technology may be used by persons providing

regulated services. The relevant question should remain who, if anyone, is actually providing or controlling the regulated service, rather than whether decentralised technology is involved – and clarifying that distinction would provide considerably greater legal certainty without requiring expansion of the existing Article 3(1)(16) service list.

Aave Labs' own group structure illustrates the practical importance of that distinction. Push Virtual Assets Ireland Limited, an Aave Labs subsidiary, is authorised as a CASP by the Central Bank of Ireland, and its activity is limited to onboarding and off-boarding: converting between euro and stablecoins for its customers, which MiCA classifies as exchange of crypto-assets for funds. Push is an identifiable legal entity that contracts with customers and performs specified services falling within Article 3(1)(16), and is regulated accordingly. By contrast, the Aave Protocol consists of non-custodial smart contracts through which users can interact directly. Where decentralised infrastructure of this kind does not involve an identifiable person providing or controlling a listed crypto-asset service for clients, the infrastructure itself should not be brought within the CASP perimeter.

Question 46

If additional services should be added, what should those be and what requirements should be applied to these services and service providers? If you believe that certain services should be removed, please specify which ones and why.

Aave Labs response

We do not recommend adding 'operating a decentralised lending or borrowing protocol' as a new CASP-licensable service. Doing so would require attributing licensable-entity status to software that, by design, has no operator capable of taking on the obligations (capital requirements, complaint handling, conduct-of-business rules) that a CASP license presupposes. Where a genuine intermediary does exist – for example, a CASP or fiat on/off-ramp that holds client assets or funds and connects retail clients to DeFi protocols – that intermediary is already capable of being captured under the existing service categories (e.g. reception and transmission of orders, or execution), and that is the correct locus of regulation, not the underlying protocol. Front-ends and aggregators that let people interact with protocols from their own self-custodial wallets are not intermediaries in this sense: users sign every transaction themselves and the interface never holds their assets.

Question 49

Is the prudential regime for crypto-asset service providers appropriate to capture the risks associated with the provision of crypto-asset services, or would it be warranted to adjust the prudential stance, e.g. by aligning it with the requirements for own funds applicable to investment firms (including K-factors) that provide services that are broadly similar?

☒ **It is appropriate to capture the risks associated with the provision of crypto-asset services**

☐ *It would be warranted to adjust the prudential stance*

Aave Labs response

It is appropriate to capture the risks associated with the provision of crypto-asset services. Aave Labs answers this from direct experience: our subsidiary Push (Push Virtual Assets Ireland Limited) holds a live MiCA CASP authorisation from the Central Bank of Ireland and is directly subject to this prudential regime. In our experience the existing Article 67 approach — prudential safeguards equal to the higher of the applicable Annex IV minimum capital or one quarter of the CASP's fixed overheads — is broadly workable for a CASP whose activity is limited to onboarding and off-boarding (converting between euro and stablecoins) rather than balance-sheet-intensive activities like proprietary trading or lending. We would be cautious about a blanket move to investment-firm-style K-factors, which are calibrated for position-taking and market risk that an onboarding and off-boarding CASP like Push does not carry; any alignment with K-factors should be targeted at CASP activities that actually take on market or credit risk, not applied uniformly across all CASP classes.

Question 50

Is the amount of minimum capital provided for each class of CASP listed in Annex IV of MiCA adequate or should it be recalibrated?

Please rate each minimal requirement on a scale from 1 to 5, where: 1 = Significantly decreased (much lower than current MiCA requirements); 2 = Somewhat decreased (moderately lower than current MiCA requirements); 3 = Kept roughly as is (current MiCA calibration is broadly appropriate); 4 = Somewhat increased (moderately higher than current MiCA requirements); 5 = Significantly increased (much higher than current MiCA requirements)

- Minimum initial capital for Class 1 (EUR 50.000) — **Aave Labs: 3**
- Minimum initial capital for Class 2 (EUR 125.000) — **Aave Labs: 3**
- Minimum initial capital for Class 3 (EUR 150.000) — **Aave Labs: 3**

Please explain your answer, indicating, if necessary, how the amount of minimum capital should it be recalibrated?

Aave Labs response

We would keep all three minimums roughly as they are. The Class 1-3 structure in Annex IV provides a reasonable starting point, but we would encourage the Commission to consider whether the calibration within individual classes sufficiently reflects the materially different risk profiles of the services grouped within them. Push's own authorisation experience is relevant here: Annex IV places both custody and administration of crypto-assets and exchange of crypto-assets for funds or other crypto-assets within Class 2, and therefore subjects them to the same €125,000 permanent minimum capital requirement. A narrowly scoped CASP such as Push, whose activity is limited to onboarding and off-boarding between euro and stablecoins and which does not provide custody and administration of crypto-assets on behalf of clients, presents a materially different risk profile from a CASP that takes custody of client crypto-assets, yet both currently face the same nominal minimum.

We would encourage any future review to assess whether greater risk sensitivity within the existing classes is warranted, based on evidence of the risks and operating costs associated with different CASP business models, considered alongside Article 67's existing requirement for prudential safeguards equal to the higher of the applicable Annex IV minimum and one quarter of the CASP's fixed overheads (see also our answer to Q49).

Question 51

Should the current approach be maintained or should there be enhanced oversight and coordination in relation to entities that in addition to providing crypto-asset services, offer (1) other unregulated services or (2) other types of regulated services, (3) a combination of crypto-asset services?

☒ **The existing approach should be maintained**

☐ *There should be enhanced oversight and coordination in relation to such entities*

If you chose the second option, which of the following enhanced oversight and coordination mechanisms do you consider may be appropriate?

☐ *Group-level reporting to a centralised authority*

☐ *Enhanced supervisory cooperation between ESAs / NCAs*

☐ *Operation of new supervisory colleges*

☐ *Consolidated supervision*

☐ *Other*

Please provide any comments on the operational feasibility, legal implications, proportionality, or potential unintended consequences of the measures above. If your answer is "Other", please elaborate.

Aave Labs response

The existing approach should be maintained. Regulation of crypto-asset services should remain focused on the legal entity providing those services, rather than automatically extending CASP requirements to other entities within the same corporate group solely by virtue of common ownership. At the same time, supervisors should have sufficient visibility over wider group relationships where these are relevant to the effective supervision of the CASP; MiCA already provides mechanisms for this, including consideration of close links, qualifying shareholders, conflicts of interest, and outsourcing arrangements. We consider this targeted, risk-based approach preferable to a general system of consolidated supervision for all groups containing a CASP.

Aave Labs' group structure is a practical example. Push Virtual Assets Ireland Limited is a separate legal entity authorised by the Central Bank of Ireland as a CASP and is responsible for the regulated crypto-asset services it provides; other entities within the wider group, including those supporting the Aave DAO and the decentralised, permissionless Aave Protocol, undertake different, non-CASP activities. The existence of those activities within the same corporate group should not, by itself, result in those entities becoming subject to

CASP-equivalent requirements. Where wider group arrangements create material risks for the CASP or its clients — for example through conflicts of interest, outsourcing, shared operational dependencies, or arrangements that could impede effective supervision — proportionate supervisory oversight and information-gathering may be appropriate. We would caution, however, against a general consolidated-supervision regime that treats all activities of a group containing a CASP as though they were regulated crypto-asset services; any enhanced framework should be targeted at the particular group relationships and risks relevant to the regulated entity, not applied to groups, like ours, that have already structurally separated regulated and unregulated activity.

The ECB/ESCB's 24 September 2026 response to this consultation endorses transferring CASP authorisation and supervision from national competent authorities to ESMA, a change the Commission itself proposed for all CASPs, irrespective of size, in its December 2025 market integration and supervision package. It adds calls for enhanced prudential requirements for 'significant' CASPs and an EU intermediate-parent-undertaking requirement for non-EU groups. We would note that CASP supervision lies outside the ECB's own statutory mandate: its Treaty role centres on monetary policy and payment systems (Article 127(2) TFEU), and its MiCA tasks concern EMT/ART issuance, not CASPs. How CASP supervision is allocated is a question of institutional design for the co-legislators, to be assessed on its own merits — proportionality (particularly for small, narrowly scoped CASPs), accountability, coordination costs, and proximity to firms such as our subsidiary Push — rather than one on which a central bank's recommendation should carry particular weight.

Question 55

The Payment Services Directive has been substantially reviewed recently, bringing notably more clarity on the interplay between the MiCA rules applying to the transfer services in relation to e-money tokens and the rules under the payment services framework which apply to the provision of payment services. As a result, the PSD3/R will clarify which crypto-asset services may qualify as payment services, including targeted exclusions from the scope of PSD3/R for specific types of transactions/exchanges involving EMTs, and will specify the authorisation process under PSD3 in cases where CASPs are required to obtain a PSD3 authorisation. Do you consider these changes bring sufficient clarity or are there other issues that remain to be addressed? If so, please explain your response.

☐ Yes

☒ No

Aave Labs response

No. We welcome the direction of PSD3/PSR in seeking to provide greater clarity on the interaction between payment services regulation and MiCA, particularly for electronic money tokens (EMTs), but given the practical importance of this boundary for CASPs, further clarity would be valuable. This is relevant to Aave Labs through our subsidiary Push, which is authorised under MiCA and provides only onboarding and off-boarding between euro and stablecoins (exchange of crypto-assets for funds); it is important that straightforward

exchange activity under MiCA is clearly distinguished from activities involving EMTs that constitute payment services and therefore require separate payment-services authorisation. We welcome the EBA's work on the interaction between PSD2 and MiCA, including its recognition that exchange of crypto-assets for funds and exchange of crypto-assets for other crypto-assets should not, without more, be treated as payment services, while certain activities involving the custody or transfer of EMTs on behalf of clients may fall within the payments framework.

We would encourage the final PSD3/PSR framework, and any subsequent EBA guidance, to preserve and make this distinction as clear as possible and to minimise unnecessary duplicative authorisation. Worked examples covering common CASP business models would be particularly useful, including: principal exchange involving EMTs; transfers of EMTs on behalf of clients; custodial and non-custodial models; and cases in which a separate payment service provider handles the fiat payment leg. This would help CASPs determine the applicable regulatory perimeter at the product-design stage and promote consistent interpretation across Member States.

PSD3/PSR's open-banking provisions also matter for onchain finance. Onboarding and off-boarding depend on reliable access to bank accounts and payment rails, and our own experience building Push has shown how difficult that access can be to secure, even for a MiCA-authorized CASP supervised by the Central Bank of Ireland. Banks' reluctance to serve crypto-asset firms remains one of the most practical barriers to regulated on- and off-ramps, and it pushes against MiCA's own goal of bringing activity into the regulated perimeter. MiCA-authorized CASPs should therefore benefit from the same fair, non-discriminatory access to payment accounts that the PSR secures for payment institutions. Payment initiation ('pay by bank') could also give EU users a low-cost, instant route from a bank account into a MiCA-compliant stablecoin. More broadly, the Open Finance goals behind the proposed Financial Data Access Regulation (customer control over financial data and the ability to move it between providers) are native to public blockchains, where positions and transactions are transparent and portable by default. We would encourage the Commission to design FiDA's data-sharing schemes to interoperate with onchain financial markets, so that EU users can combine traditional and onchain financial services rather than treating them as separate worlds.

Question 56

Do MiCA provisions governing crypto asset service providers sufficiently allow, or unduly restrict, access for EU consumers and investors to non-EU and global crypto asset trading and liquidity pools? What are the advantages and disadvantages of focusing on EU liquidity or full access to global liquidity?

Aave Labs response

MiCA rightly requires that crypto-asset services offered to EU clients be provided by authorised firms. That objective should be kept separate from the question of where those

firms and their clients can source liquidity. Crypto-asset liquidity is global, and onchain liquidity is global by design: a lending or exchange pool on a public blockchain is a single pool that anyone can supply to or draw from. Requiring EU users or their CASPs to rely on EU-only liquidity would fragment that pool into smaller, shallower ones, widening spreads, raising borrowing costs and lowering returns for EU users, without a commensurate gain in consumer protection.

The advantage of full access to global liquidity is depth, price quality and resilience; the disadvantage is that some venues sit outside EU supervision. The better answer is to place obligations on the regulated entry point: an EU-authorised CASP should be able to access third-country venues and decentralised liquidity for its clients, subject to best-execution, due-diligence and disclosure obligations, while remaining fully responsible for its MiCA obligations towards those clients. This is distinct from unauthorised third-country firms actively marketing services to EU clients, which MiCA's authorisation requirements and narrow reverse-solicitation exemption (Article 61) already address.

Greater clarity would be useful on when an EU-authorised CASP's use of non-EU venues or decentralised liquidity sources could be treated as the unauthorised provision of services in the Union. We would also caution against ring-fencing liquidity indirectly, for example by limiting CASPs to 'verified' or EU-only pools (Q62.1) or by making EU-issued stablecoins non-fungible with their global counterparts (Q38). Both would leave EU users with thinner markets than the rest of the world. See also Q27 on EU access to global stablecoin liquidity.

Part 4 — Policy Areas Beyond the Current Scope of MiCA

4.1 — Decentralised Finance

Question 59

In case you are aware or make use of DeFi currently beyond the regulatory perimeter of MiCA, what are the main services you (would) use and for which of them do you consider they bring benefits compared to similar intermediated digital assets services?

1. DeFi applications present limited interest and are moderately used for this service; 2. DeFi applications present important potential benefits for this service but their use remains limited due to some non-mitigated weaknesses; 3. DeFi applications present important benefits for this service and are already significantly used, despite important non-mitigated weaknesses; 4. DeFi applications present important benefits for this service, they are already significantly used and present limited risks

- *Exchange services* — **Aave Labs: 4**
- *Payments and transactions services* — **Aave Labs: 4**
- *Trading and Investment services* — **Aave Labs: 3**
- *Lending and borrowing services* — **Aave Labs: 4**
- *Custody services* — *not rated*

Please detail the benefits or weaknesses you associate with the use of DeFi applications for these different services, and the actions you would consider appropriate to optimise these benefits or address the possible issues they raise.

Aave Labs response

We rate lending and borrowing, exchange (spot swaps through automated market makers) and payments (stablecoin transfers on public blockchains) at 4, trading and investment at 3 given the leverage and liquidation risks of onchain derivatives, and do not rate custody: self-custody is the absence of an intermediary, not a DeFi service. In non-custodial lending protocols such as the Aave Protocol, users supply and borrow without ceding custody to anyone; collateral ratios, interest rates and liquidations are enforced by open-source, audited code; and reserves and positions are visible onchain in real time. That removes the commingling, hidden rehypothecation and 'trust us' risk behind the 2022 failures of centralised lenders.

Overcollateralised lending markets are also a standing, always-available source of programmatic credit: users can raise working capital against holdings without selling them, adjust exposure without trading, and deploy idle treasury balances around the clock. As bonds, fund shares and other real-world assets are tokenised, the same infrastructure will support secured lending against them and, in time, securities financing (Q67).

DeFi lending also opens a savings channel that is different in kind from a bank deposit. A saver who supplies idle stablecoins to the Aave Protocol lends directly, through transparent code, to borrowers who have posted collateral worth more than they borrow, and receives the market rate those borrowers pay, less a disclosed reserve factor. The rate is variable, the position is not covered by deposit guarantees, and withdrawals can be delayed when a pool is highly utilised (Q60). In substance, EU citizens gain direct access to secured, market-priced lending of a kind historically open mainly to institutions through repo and securities lending, which is exactly what the Savings and Investment Union seeks for household savings.

This is why we firmly oppose any extension of the EMT/ART interest ban to lending or staking. The ECB proposes extending it to lending, staking and 'liquidity mining incentives embedded in DeFi arrangements'; the EBA treats returns on CASP clients' stablecoins placed in lending protocols as possible 'regulatory arbitrage' of the ban. Both misread its purpose. Articles 40 and 50 stop issuers and CASPs paying holders for holding a token, so that stablecoins serve as a means of exchange rather than an interest-bearing store of value. A lending return is not paid for holding: the lender gives up the token to a borrower, who pays a market price to use it, and the lender bears the credit and liquidity risk. It is also the saver's own decision about their own assets. In a non-custodial protocol no intermediary takes custody or decides anything: the saver chooses to lend, on terms visible in advance, and can withdraw when liquidity allows. Europeans have a right to manage their own finances and to use their own property, including by lending it (Article 17 of the Charter of Fundamental Rights), and they should have access to savings channels beyond bank deposits, which is what the Savings and Investment Union is meant to deliver. A ban would take that choice away without any

intermediary risk to justify it. Euro banknotes pay no interest, and e-money may not either (Article 12 of the E-Money Directive), yet no one concludes that lending euros must go unremunerated. Every asset in the financial system can be lent at a price: government bonds in repo, equities in securities lending, gold, currencies. Denying that price to MiCA-authorized stablecoins alone would make them the least useful stablecoins in onchain markets, and combined with the EBA's proposed ban on lending unauthorized stablecoins, would leave EU clients of CASPs with no stablecoin lending at all. It would also entrench the dollar dominance the ECB is concerned about: euro stablecoins will only compete if holders can put them to work. Institutions would lose tools too: corporates and funds lend idle stablecoin balances as treasury management, borrow against holdings to manage liquidity, and manage financial risk without selling assets. Staking rewards are not interest either: the protocol pays them, from issuance and transaction fees, for helping secure the network, with the staker's assets at risk of slashing (Q66). Liquidity-mining incentives are promotional rewards paid by protocols, not by issuers or CASPs, and are best addressed through clear disclosure of their source, amount and duration. The right response is the EBA's own: regulate intermediated lending as a service, with disclosure and suitability safeguards (Q67), and clarify in Level 1 that 'interest' under Articles 40 and 50 excludes returns paid by third-party borrowers and staking rewards from consensus participation. We address deposit substitution in Q29.

Question 60

What do you consider to be the main risks associated with DeFi?

1. Strongly disagree, 2. Rather disagree, 3. Neutral, 4. Rather agree, 5. Strongly agree

- *Operational risk* — **Aave Labs: 4**
- *Money laundering and terrorist financing risk* — **Aave Labs: 2**
- *Market abuse* — **Aave Labs: 2**
- *Investor protection risk (information asymmetry, no redress, opacity of functioning)* — **Aave Labs: 3**
- *Financial stability* — **Aave Labs: 2**

Please explain your answers.

Aave Labs response

Ratings (the extent to which we agree each is a main risk associated with DeFi): operational risk — 4, rather agree: smart contract vulnerabilities, oracle failures and governance attacks are the principal risk vectors in DeFi, though substantially mitigated in mature protocols through extensive auditing, formal verification, bug bounties and time-locked upgrade governance; money laundering and terrorist financing risk — 2, rather disagree, for protocols themselves, since DeFi transactions are recorded permanently and transparently on public ledgers and are, if anything, more traceable than cash or many traditional finance rails (the AML risk in practice concentrates at fiat on/off-ramps, which are already within CASP/AMLR scope); market abuse — 2, rather disagree, for lending and borrowing specifically (as opposed to trading venues, where this risk is more concentrated); investor protection risk — 3,

neutral: retail users face genuine technical-literacy and redress challenges, but the protocol's rules, code and positions are publicly visible rather than opaque, and the remaining gaps are best addressed through clear disclosure and good interface design rather than intermediary-style licensing of the protocol; financial stability — 2, rather disagree, at current DeFi market scale, consistent with the FSB's assessment ('The Financial Stability Risks of Decentralised Finance', February 2023) that DeFi's interlinkages with traditional finance are to date limited, though this should be reassessed as DeFi, and its interconnection with traditional finance through tokenisation, grows.

On financial stability, we do not claim DeFi lending is free of the vulnerabilities the FSB identifies — leverage, liquidity mismatch, interconnectedness and operational fragility — but each takes a different, and more visible, form. Automatic liquidation of overcollateralised positions can amplify price declines when collateral is correlated, but deleveraging happens early, incrementally and publicly, rather than accumulating as hidden leverage until a disorderly failure, as at the centralised lenders in 2022. The Aave Protocol already operates what is in substance an on-chain macroprudential toolkit: supply and borrow caps, loan-to-value and liquidation thresholds adjusted through governance, isolation mode for riskier collateral, and efficiency mode for correlated assets. Pool liquidity can tighten: near 100% utilisation, suppliers may be unable to withdraw until borrowers repay or new liquidity arrives, a dynamic the interest rate model counters by raising rates sharply and which is observable in real time. Recursive 'looping' and re-use of receipt tokens as collateral elsewhere create leverage chains analogous to rehypothecation, though visible on-chain. And reliance on a small number of oracle providers is a systemic, not merely protocol-level, dependency, which is why we propose oracle robustness standards in Q67.

The March 2023 USDC depeg, which the ECB/ESCB's own response cites as its lead precedent for stablecoin-bank contagion, was a real stress test. As USDC fell to around 88 cents after Silicon Valley Bank's failure, the Aave Protocol kept operating; the Aave Guardian froze stablecoin markets and set their loan-to-value to zero on the most exposed deployment (Avalanche), preventing new positions while allowing liquidations to proceed. Realised bad debt was roughly US\$300,000, confined to two deployments, and the protocol remained solvent (Gauntlet, 'Aave Resilient Through USDC Volatility', March 2023). The shock was transmitted, absorbed and publicly accounted for within days.

This is consistent with the Crypto Council for Innovation's 'Key Elements of an Effective DeFi Framework' (2023), which finds that significant DeFi incidents have concentrated in a narrow set of attack vectors — flash loan exploits, cross-chain bridge compromises (often controlled by a single or small group of parties), and oracle-price manipulation — rather than failures of blockchain consensus, and identifies DAO governance concentration as a distinct operational risk. That supports rating risk by reference to specific, addressable vectors rather than treating 'DeFi' as one undifferentiated category.

Carter and Jeng, 'DeFi Protocol Risks: The Paradox of DeFi' (2021), offer a more cautious counterpoint: automating financial services removes human intermediaries and their discretionary oversight, reducing counterparty and intermediary risk while relocating risk into

blockchain infrastructure, smart contract code, governance processes and interconnections with traditional finance. We consider this framing correct and complementary to our ratings: regulatory attention is best directed at those specific vectors – audit quality, oracle design, governance timelocks and TradFi interconnections – rather than at a blanket characterisation of decentralised protocols as more or less risky than centralised ones.

Question 61

In case you consider the criteria for establishing whether a DeFi application is not fully decentralised not sufficiently clear, which of them should do you consider should be used to assess the degree of decentralisation?

1. Strongly disagree, 2. Rather disagree, 3. Neutral, 4. Rather agree, 5. Strongly agree

- Existence of an identifiable intermediary (person or group of persons) providing a crypto-asset service — **Aave Labs: 5**
- Presence of control by an identifiable person or group of persons (e.g. via admin keys) over the key functionalities of a DeFi protocol (e.g. upgradeability of protocol) — **Aave Labs: 4**
- Significant concentration of governance power over the key functionalities of a DeFi protocol — **Aave Labs: 4**
- Custody of user assets by the DeFi protocol — **Aave Labs: 5**
- DeFi protocol code is not open source — **Aave Labs: 4**
- Marketing of a DeFi protocol by an identifiable entity or person — **Aave Labs: 1**
- Other — **Aave Labs: 5**

Aave Labs response

The right test is whether an identifiable legal person controls the activity and exercises active, ongoing discretion over it: deciding whom to serve, on what terms and with whose assets. Technology is simply an instrumentality. The criteria should be applied to that question function by function, rather than used to score a protocol as a whole. On that basis, the decisive criteria are an identifiable intermediary providing a crypto-asset service (5), custody of user assets that someone other than the user can access or redirect (5), and control of key functions by an identifiable person or group (4). Open-source, independently verifiable code (4) is an important supporting indicator, because users and supervisors can only rely on rules they can read.

Control needs careful definition, because almost every mature protocol retains some safeguards. The question is whether a person can, at their own discretion, change the terms on which users transact or reach their assets, not whether any administrative role exists at all. In the Aave Protocol, upgrades and configuration changes require a public onchain governance vote and a timelock before execution. The Protocol Emergency Guardian and the Risk Stewards act only under limited authorities delegated to them by Aave DAO tokenholders through that same governance process, which can also change or revoke them. The Guardian, a community-elected 4-of-7 multisig, can pause markets and freeze reserves in

an emergency but cannot upgrade contracts, change configuration or move user funds. The Risk Stewards, operated by risk service providers appointed through governance, can adjust specified risk parameters, such as caps and interest-rate settings, only within maximum step sizes and minimum intervals that governance sets and publishes onchain. Bounded, defensive powers of this kind, delegated by and accountable to tokenholders and visible onchain, protect users. Treating them as centralised control would penalise exactly the safeguards supervisors should want protocols to have.

Significant concentration of governance power (4) is a relevant indicator, because a person or small group able to decide governance outcomes controls the protocol in substance. It should, however, be assessed as a spectrum and by its effect on outcomes: a large, permissionless onchain DAO with time-locked execution is qualitatively different from control vested in a small team, even though some token concentration exists in most DAOs. Marketing by an identifiable entity (1) should not, on its own, indicate insufficient decentralisation. Front-ends, documentation and community communications are commonly maintained by contributor organisations, as Aave Labs does for the Aave Protocol, that hold no user funds and cannot change protocol parameters unilaterally; treating visible engagement as control would penalise transparency and push contributors to obscure their involvement.

Under 'Other' (5), we would add one further criterion: whether users can exit without anyone's permission, withdrawing or repaying directly through the smart contracts even if every front-end, contributor organisation and service provider disappeared. This is a simple, testable indicator that no intermediary stands between users and their assets.

This approach matches IOSCO's Recommendation 2 on DeFi (December 2023), which asks regulators to identify the 'Responsible Persons' exercising 'control or sufficient influence' over an activity. We would encourage the Commission to read 'sufficient influence' as the ability to determine outcomes. Writing code, submitting governance proposals or maintaining a front-end should not qualify: that reading would sweep in developers and contributors who decide nothing unilaterally.

Question 62

Do you believe that risks to users of fully decentralised DeFi protocols should be indirectly accounted for by MiCA, e.g. by requiring CASPs to conduct due diligence over DeFi protocols they connect their clients with, or in any other way?

☒ **Yes**

☐ **No**

Aave Labs response

Yes, with important limits. Requiring CASPs that choose to connect retail clients to third-party DeFi protocols to perform reasonable due diligence (audit history, time-locked governance, track record, TVL, incident history) and to make appropriate risk disclosures is a proportionate way to protect retail users without imposing CASP-style licensing obligations directly on

protocols that have no operator capable of bearing them. This preserves the important distinction between regulating points of intermediation (which can bear compliance obligations) and regulating permissionless, open software (which cannot).

The Commission should see such connections as something to enable, not merely tolerate. Integration between regulated intermediaries and DeFi protocols is how onchain financial markets will reach most EU users and institutions. Exchanges and fintechs already offer customers crypto-backed loans and stablecoin savings powered by DeFi lending protocols, and banks will need to integrate with the same infrastructure as tokenised assets and collateral move onchain. The benefits are concrete. EU users gain access through a familiar, authorised firm that provides onboarding, disclosures, customer support and complaint handling. They receive market rates drawn from global liquidity, with collateral and positions visible onchain. The intermediary no longer needs to lend clients' assets on its own balance sheet, the model that failed at centralised crypto lenders in 2022, because it can route them to transparent, overcollateralised protocols instead. Firms can build on shared, open infrastructure rather than each replicating it, lowering costs and strengthening EU fintech competitiveness in line with the Savings and Investment Union. And supervisors get an accountable, authorised entity at the point of access, alongside real-time onchain data on the protocol itself.

Due diligence requirements should be calibrated to support this model: proportionate, focused on the CASP's own processes, and not making the CASP liable for the operation of open-source code it does not control (Q62.1) or conditional on protocol certification (Q65).

Risks can also arise at the front-end, the website or app through which users interact with a protocol. They are real, but they are security and information risks rather than custody or credit risks, because a self-custodial user signs every transaction and the interface cannot move their assets. The most serious harms, such as phishing clones and domain hijacks that trick users into signing malicious transactions, are committed by criminals whom a licence would never reach. The right tools are therefore technical and horizontal: open-source and verifiable front-end code, secure domain and hosting practices, wallet-level transaction simulation and clear signing, and multiple independent front-ends so users can always reach the protocol directly. Operators acting commercially are already bound by EU consumer protection law against misleading presentation, and where a front-end starts to hold users' assets or act with discretion on their behalf, it becomes an intermediary that existing MiCA service categories capture (Q46).

Question 62.1

Please specify how should MiCA account for risks from fully decentralised DeFi applications.

For the purpose of this question, certification of a DeFi application should be understood as verifying that it robustly mitigates against smart contract vulnerabilities, operational risk in general and functions in accordance with its publicised performance.

1. Strongly disagree, 2. Rather disagree, 3. Neutral, 4. Rather agree, 5. Strongly agree

- CASPs should be able to connect their clients to any decentralised DeFi application, subject to giving appropriate warnings and disclosures on risks — **Aave Labs: 4**
- CASPs should be liable for certain types of incidents when they have provided access to the relevant DeFi application and clients have been affected — **Aave Labs: 3**
- CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service global (permissionless) liquidity — **Aave Labs: 2**
- CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service only verified liquidity (verified pools) — **Aave Labs: 1**
- CASPs should only facilitate connection of their clients to decentralised DeFi applications that service global liquidity — **Aave Labs: 2**
- CASPs should be required to discontinue or discourage connecting clients to DeFi protocols that are strongly associated with illicit activity based on blockchain analytics — **Aave Labs: 4**
- CASPs should not facilitate connection to decentralised DeFi applications — **Aave Labs: 1**
- Public bodies should be required, or private organisations incentivised to publish whitelists or blacklists of DeFi protocols based on their risk profile — **Aave Labs: 3**
- Other — **Aave Labs: 5**

Please explain your responses, including your reasoning and any suggestions for improvement, recalibration, or alternative approaches.

Aave Labs response

CASPs are the right place to address the risks of fully decentralised applications, because they hold the client relationship; the question is how, not whether. The answer should be due diligence and disclosure applied by the CASP, not an official list of permitted protocols. A protocol's code, collateral, parameters, governance and track record are publicly visible and can be assessed directly; an exclusive list would instead recreate licensing for open-source software and freeze EU users' choices at whatever the list-keeper has approved.

On that basis, we rather agree that CASPs should be able to connect clients to any decentralised application, subject to their own due diligence (Q62) and appropriate warnings and disclosures (4). We rather agree that CASPs should stop or discourage connections to protocols strongly associated with illicit activity (4), which is consistent with existing AML obligations, provided the analytics criteria are transparent and proportionate, so that widely used protocols are not excluded merely because bad actors have also used them. We are neutral on CASP liability (3): it is appropriate where the CASP's own due-diligence or disclosure failure caused the harm, but not as strict liability for open-source code the CASP does not control. We are also neutral on published whitelists and blacklists (3): useful as voluntary reference tools, harmful if they become a de facto licensing gate.

We disagree with rules that would confine CASPs to a single kind of venue. Verified, permissioned pools are a legitimate design where issuers or institutions require them; Aave Horizon, which enforces issuers' eligibility rules onchain, is one. But requiring CASPs to use only verified pools (1), only certified applications (2), or only applications serving global liquidity (2) would each rule out valid models and fragment liquidity. EU users should be able to reach both permissionless and permissioned markets, with the CASP responsible for matching each client to appropriate products. Prohibiting connections altogether (1) would cut EU retail users off from the most transparent segment of the crypto market and from the infrastructure onchain financial markets run on.

Under 'Other' (5), we propose a tiered due diligence framework. The ESAs would publish objective criteria for CASPs to apply and document: independent audits, governance timelocks and emergency safeguards, oracle design, track record and incident history, and whether users can exit directly through the smart contracts (Q61). Higher-risk products, such as leveraged positions or newly listed collateral, would attract enhanced disclosures and appropriateness checks for retail clients. CASPs would monitor the protocols they connect to and suspend access when a protocol is paused or compromised. Supervisors would then assess the quality of the CASP's process, drawing on public onchain data, rather than certifying the protocol itself.

Question 63

Do you support introducing certification schemes for DeFi protocols and smart contracts?

- ☐ Yes, for all DeFi protocols and smart contracts providing any of the crypto-assets services defined under MiCA, and possibly also other services not in MiCA's scope such as lending and borrowing
- ☐ Yes for the DeFi protocols and smart contracts providing some of the crypto-assets services defined under MiCA
- ☒ **No**

In case you support introducing certification schemes for only certain types of DeFi services, please explain which ones and for what reasons.

Aave Labs response

No, not as a requirement. Aave Labs supports raising security standards across DeFi, and would welcome a voluntary certification or attestation scheme for smart contract security and operational robustness (Q65). What we oppose is making certification a condition for a protocol, including a lending protocol, to be available to EU users or reachable through EU CASPs, for three reasons.

First, a mandatory certificate would promise more than it can deliver. It attests to code at a point in time, while protocols change through governance, add collateral and depend on external oracles and bridges; users and CASPs could treat it as a guarantee it cannot be. Second, it has no one to attach to. A fully decentralised protocol has no operator to apply for, maintain or answer for a certificate, so a mandatory scheme would in practice fall on

contributor organisations that decide nothing unilaterally, the reverse of the control-based test we propose in Q61. Third, it would duplicate, less effectively, what CASP due diligence already achieves: a CASP connecting clients to a protocol can assess audits, governance safeguards, oracle design, track record and exit rights directly, continuously and in public (Q62.1).

Aave's own practice shows what voluntary, market-driven standards already deliver. The Aave Protocol has undergone some 65 independent audits across its versions, by firms including OpenZeppelin, Trail of Bits, Certora, ChainSecurity and Sigma Prime, with formal verification by Certora. Aave V4 alone received about 345 days of cumulative security review under a US\$1.5 million budget ratified by the DAO, followed by a public contest with over 900 participants in which no critical or high-severity issues were found. Standing bug bounties pay up to US\$5 million for a critical vulnerability in the core protocol, and Aave Labs, as a contributor organisation, holds a SOC 2 Type II attestation covering security, availability and confidentiality.

These standards keep rising. In April 2026 an exploit of a third-party cross-chain bridge, not of the Aave Protocol, affected an asset used as collateral on Aave. Aave DAO tokenholders nonetheless adopted two new standards in July 2026: the Aave Risk Framework, which sets binding requirements for onboarding and reviewing collateral assets, bridges and chains, including audit and bug-bounty minimums and at least three independent verifiers on every bridge route carrying Aave exposure; and the Technical Asset Listing Framework, proposed by Aave Labs, which sets a public technical baseline for every asset listed on Aave V3, V4 and Horizon, covering minting controls, privileged roles, oracle paths, bridge topology and audits. None of this was required by regulation, and all of it is public and verifiable. It shows how raising industry standards can strengthen resilience and security while keeping pace with technology, which a fixed certification regime would struggle to do.

The better design is to put accountability where the client relationship sits. Supervisors should hold CASPs to a clear due diligence standard, and a voluntary certificate should count as one positive factor in that assessment, rewarding protocols that invest in security without turning a quality signal into a licence.

Question 64

Which of the following statements about potential certification schemes of DeFi protocols do you agree with?

1. Strongly disagree, 2. Rather disagree, 3. Neutral, 4. Rather agree, 5. Strongly agree

- Instead of a full CASP licence, DeFi protocols that are not fully decentralised should be required to obtain a certification before or soon after making the protocol available to the public — Aave Labs: 3*
- To obtain their certificate, DeFi protocols that are not fully decentralised should be required to integrate specific compliance tools in the design of their protocols — Aave Labs: 3*

- *DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be required to obtain a certificate before making these wallets available to the public* — **Aave Labs: 1**
- *DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be incentivised to obtain a certificate* — **Aave Labs: 4**

Please explain your responses.

Aave Labs response

Where a protocol is not fully decentralised under the control-based test in Q61, obligations should attach to the identifiable person who controls it, and a proportionate certification regime for that person could be a sensible alternative to a full CASP licence. We are neutral on the proposition as drafted (3), because it depends on two conditions: the decentralisation test must be the control-and-discretion test in Q61, so that bounded safeguards delegated by governance, such as emergency pause powers, do not by themselves trigger it; and the certificate must attach to the controlling person rather than operate as a separate gate on the software.

We are also neutral on requiring specific compliance tools (3). Programmable compliance is one of the most important benefits of onchain finance: eligibility rules, transfer restrictions and sanctions screening can be enforced in code, as Aave Horizon does for issuers' investor-eligibility requirements. But regulation should set the outcomes and leave the design of the tools to the market, so that compliance can improve as the technology does.

We strongly disagree that developers of non-custodial wallets should need a certificate before releasing them (1). A non-custodial wallet is a tool people use to hold and manage their own assets, which they have a right to do; the developer never holds the funds, executes transactions or stands between users and their assets. Requiring prior certification would amount to licensing the publication of general-purpose software, and would discourage exactly the self-custody tools that reduce reliance on custodial intermediaries. EU law already manages the relevant risk where it arises: under the Transfer of Funds Regulation, CASPs must collect information on transfers to and from self-hosted wallets and, above €1,000, assess whether the self-hosted address is owned or controlled by their client.

We rather agree that wallet developers should be incentivised to obtain a certificate or security attestation (4). A voluntary scheme, which CASPs could recognise when assessing wallet integrations, would reward good security practice without restricting who can build tools for self-custody.

Question 65

Which of the following statements about potential certification schemes of DeFi protocols or smart contracts do you agree with?

1. Strongly disagree, 2. Rather disagree, 3. Neutral, 4. Rather agree, 5. Strongly agree

- *Certificates should be issued by qualified private sector entities* — **Aave Labs: 4**

- *Certificates should be issued by qualified public sector entities* — **Aave Labs: 4**
- *Any interested party (e.g. persons providing connectivity to or participating in governance of DeFi protocols) should have the possibility to ask for the certification of a fully decentralised DeFi protocol* — **Aave Labs: 4**
- *Only fully decentralised DeFi protocols that reach a certain significance (e.g. based on total value locked) should be required to obtain a certificate* — **Aave Labs: 2**
- *CASPs should not be allowed to connect clients with DeFi protocols that are not certified* — **Aave Labs: 1**

Please explain your responses.

Aave Labs response

Certification can play a useful role only if it stays voluntary and tells users something true. A smart-contract certificate is a snapshot: it attests that code met defined standards at a point in time, while protocols evolve through governance-approved upgrades, add new collateral assets and depend on external oracles and bridges. Many of the largest DeFi losses have involved audited code. A mandatory certificate would risk giving EU users and CASPs false assurance while adding little to what markets already demand: independent audits, formal verification, bug bounties, public disclosure of risk parameters and continuous onchain risk monitoring. Any scheme should build on and recognise these practices rather than replace them with a one-off stamp.

We rather agree that both qualified private-sector entities and qualified public bodies should be able to issue certificates (4 each), provided that criteria and issuer qualification standards are harmonised at EU level to prevent a fragmented, forum-shopped market, and that certificates from either source remain voluntary: a certificate should be a quality signal that users and CASPs can rely on, never a precondition for making open-source software available. We rather agree that any interested party, including a CASP or a DAO governance participant, should be able to request certification (4), because a fully decentralised protocol has no operator to apply on its behalf; a scheme that depended on one would exclude the very protocols it is meant to cover.

We rather disagree that significant protocols should be required to obtain a certificate (2): certification should remain voluntary (Q63), and if mandatory elements were nonetheless adopted, a threshold such as total value locked would be the least harmful design. We strongly disagree that CASPs should be barred from connecting clients to uncertified protocols (1): that would recreate a licensing gate for permissionless software under another name and fragment liquidity for EU users without restricting access to the same protocols elsewhere (Q62.1). Certification should instead count as one positive factor in a CASP's due diligence (Q62), alongside audit history, governance safeguards and track record.

4.2 — Staking, Lending and Borrowing of Crypto-Assets

Question 66

Do you think the current approach whereby staking services are not separately regulated is adequate? If not, what specific requirements should be applied to staking service providers?

☒ **Yes**

☐ **No**

Aave Labs response

Yes. Under MiCA, a firm that stakes crypto-assets on its clients' behalf must already be authorised to hold those assets in custody, and must obtain each client's explicit consent before staking them. That captures the main risk, which is the client's dependence on a firm that holds its assets. Where users stake directly and keep control of their own keys, whether by running a validator or interacting with a smart contract, there is no firm in between, and a staking-specific licence would have nothing to attach to (Q61). Staking rewards are also different in kind from a lending return: they come from the protocol's issuance and transaction fees in return for helping secure the network, not from a counterparty using the staker's assets, so staking should not be treated as lending or as a deposit-like product.

The ECB's proposal to extend the interest ban to 'staking' needs careful reading, because the word covers two different things. Staking in the proper sense, locking a network's native token to help secure a proof-of-stake blockchain, does not involve EMTs or ARTs at all, so the ban has no application to it. Validators are paid by the protocol, in new issuance and transaction fees, for work that secures networks such as Ethereum, and they risk losing part of their stake if they fail or misbehave. Restricting it would keep Europeans from taking part in securing the public networks on which tokenised finance is being built. Where 'staking' is used as a label for stablecoin reward programmes, the right question is who pays: rewards funded by an issuer or CASP for holding a token are already caught by the ban, while returns paid by borrowers for using the tokens are lending returns and should not be (Q59). The ban needs no extension; it needs a clear definition.

The question also matters for DeFi lending, because liquid staking tokens, which represent staked assets and their rewards, are among the most widely used collateral on lending protocols such as the Aave Protocol. Their risks, including validator penalties ('slashing'), withdrawal delays, and the additional smart-contract and bridge layers used by restaking tokens, are real. They are best addressed through issuer disclosure and the collateral standards lending protocols apply, rather than a new licensing regime. The Aave Risk Framework and Technical Asset Listing Framework adopted in July 2026 (Q63) are examples: they set requirements for each asset's contracts, privileged roles, oracle paths and bridge topology before it can be used as collateral.

A precise definition matters beyond the ban too. 'Staking' is used in DeFi for different activities, including locking tokens to take part in governance or to provide a protocol's backstop coverage. Any future rules should be anchored to participation in a blockchain's consensus mechanism, so that unrelated activities are not captured by accident.

Question 67

Do you think that lending and borrowing of crypto-assets should be regulated?

☒ **Yes**

☐ No

If “Yes”, what do you believe should be the main elements of regulatory requirements applicable to lending and borrowing and why?

Aave Labs response

Yes. Lending should be regulated wherever an intermediary takes custody of client assets and exercises discretion over them. The line that matters is custody and control, not technology, and 2022 showed why. Celsius, Voyager and BlockFi took customer assets, re-lent them on undisclosed terms and failed, leaving customers as unsecured creditors. Over the same period the Aave Protocol kept operating as designed: liquidations executed automatically and publicly, a single market-manipulation attack left about US\$1.6 million of bad debt, and every supplier could see the protocol's assets and liabilities in real time. Regulation should close the gap that caused the first outcome without dismantling the architecture that produced the second.

For custodial and intermediated lending, the main elements should be: (i) segregation of client assets and no rehypothecation without specific, informed consent; (ii) disclosure of where client assets are deployed, to which counterparties, and against what collateral; (iii) prudential and liquidity requirements proportionate to the maturity and credit transformation the lender performs; (iv) clear withdrawal and redemption terms, including what happens in stress; and (v) conflict-of-interest and suitability safeguards for retail clients. We support the EBA's proposals to assess adding intermediated lending to the CASP services list and to apply suitability tests to it.

Non-custodial protocols deliver these outcomes by design rather than by supervision. Each user's position is recorded separately onchain; the protocol cannot lend assets beyond what suppliers provide or deploy them on terms other than its published code; collateral, utilisation and liquidation thresholds are visible to anyone, at any moment; and overcollateralisation is enforced automatically, not promised. The outcomes regulators seek from lending rules are already achieved, verifiably, without an intermediary. The residual risks are different in kind (smart contract, oracle and governance risk, the risk of collateral assets that depend on third-party bridges, and liquidity when utilisation is high) and are addressed in Q60.

Regulation of DeFi lending should therefore attach to intermediaries: to any identifiable person who controls a protocol's key functions (Q61), and to the CASPs that give EU clients access, through due diligence, risk disclosures and warnings (Q62). Front-ends that let people use a protocol from their own self-custodial wallets are software, not intermediaries: the user signs every transaction and the interface never holds their assets. Supervisors can monitor protocol-level risk directly from public ledgers (Q29), and industry standards already give CASPs a benchmark for due diligence: in July 2026 Aave DAO tokenholders adopted the Aave Risk Framework and the Technical Asset Listing Framework, which set public requirements for every collateral asset, bridge and chain the protocol supports (Q63). Where

stricter rules are needed, they can be built into the protocol, as Aave Horizon does for issuers' investor-eligibility rules. A licence modelled on bank lending would have no one to attach to.

Getting this right matters beyond crypto. Overcollateralised onchain lending is becoming core infrastructure for tokenised finance: as bonds, fund shares and other real-world assets move onchain, the same protocols can support secured lending and, in time, securities financing, with collateral, margin and settlement handled transparently and continuously. For EU savers it offers direct access to market-rate secured lending (Q59); for EU institutions, a way to mobilise tokenised collateral across markets (Q80). A regime that treats non-custodial protocols as unlicensed lenders would deny EU savers and institutions that infrastructure just as the Savings and Investment Union needs it.

Three proposals would undermine this approach, and the most damaging concern the returns savers earn. The ECB would extend the EMT/ART interest ban to DeFi lending; the EBA treats lending returns on stablecoins as 'regulatory arbitrage' and would ban CASPs from facilitating lending in unauthorised stablecoins, which in practice means USDT. Together they would stop EU savers earning a market return by lending their own stablecoins, the very thing a lending market exists to provide. That return is paid by borrowers for using the asset, with the saver bearing the risk: it is the price of credit, as when euros, bonds or equities are lent, not a reward for holding (Q59). Banning it would take away Europeans' choice of how to manage their own savings, weaken euro stablecoins against dollar ones, strip institutions of tools for treasury, liquidity and financial risk management, and protect no one, since disclosure and suitability rules for intermediated lending, which we support, address the risks. The EBA's certification regime would add a licensing gate for open-source software (Q62–Q65).

4.5 – Tokenised Deposits

Question 74

Tokenised deposits could be deployed in support of a range of use cases across payments, capital markets, and on-chain financial activities. Based on your experience and expectations, please assess the potential relevance and benefit of tokenised deposits for each of the following use cases in the EU.

Scale used: 1 = Not relevant / no meaningful benefit; 2 = Low relevance / limited benefit; 3 = Moderate relevance / moderate benefit; 4 = High relevance / high benefit; 5 = Very high relevance / transformative benefit

- *Person to person payments* — not rated
- *Retail POI payments (domestic, day-to-day point of interaction transactions)* — not rated
- *Intra-EU cross-border payments (non-POI)* — not rated
- *International payments and remittances (third countries)* — not rated
- *Settlement of tokenised securities and other financial instruments* — **Aave Labs: 5**
- *Delivery-versus-payment (DvP) and atomic settlement* — **Aave Labs: 5**

- *Intraday liquidity management (real-time funding and liquidity optimisation)* — **Aave Labs: 5**
- *Treasury and liquidity management services for corporates and financial institutions* — **Aave Labs: 4**
- *Programmable payments and smart-contract-based use cases* — **Aave Labs: 4**
- *On-chain collateral or margining in regulated markets* — **Aave Labs: 4**
- *Improved settlement speed and operational efficiency* — **Aave Labs: 4**
- *Reduction of counterparty and settlement risk* — **Aave Labs: 4**

Aave Labs response

The benefits are greatest in settlement among banks: tokenised securities settlement, atomic delivery-versus-payment and intraday liquidity. Tokenised deposits can also support smart-contract payments and onchain collateral, but how far depends on their interoperability, as explained below. We leave the person-to-person, retail point-of-interaction, intra-EU and international payment use cases to payments-focused respondents.

Tokenised deposits and stablecoins will play different roles. A tokenised deposit remains a deposit: a claim by an identified customer on a particular bank, recorded on that bank's books. Transferring it is in substance an instruction to the bank to debit one account and credit another, and the recipient normally needs an account at the same bank or within the same banking network. That makes tokenised deposits well suited to consortiums of banks settling among known participants, for tokenised securities settlement, delivery-versus-payment and intraday liquidity, which is where we rate them highest. It also makes them less interoperable than stablecoins. A stablecoin is a claim on its issuer that can pass from holder to holder, across wallets and blockchains, without the issuer taking part in each transfer. Outside bank consortiums, in open onchain markets, stablecoins are therefore likely to remain the dominant form of digital money.

Within those limits, tokenised deposits could still become valuable collateral. If a bank or consortium allows its deposit tokens to be posted into non-custodial lending protocols, including permissioned markets, institutional and corporate users could borrow and lend onchain without first converting balance-sheet assets into stablecoins. We see them as a complement to stablecoins, not a substitute. That depends on interoperability: if every transfer must route through a bank-controlled ledger or a licensed gatekeeper, the programmable-payment and onchain-collateral benefits in this question will remain theoretical. We would encourage the Commission to treat interoperability with permissionless smart-contract environments, or at minimum non-discrimination against such interaction, as a design consideration for any tokenised-deposit framework. The same applies, at greater scale, to tokenised real-world assets such as bonds and treasuries.

This reflects the interoperability principle summarised in our response to Q86: Aave Labs is agnostic as to whether digital money takes the form of a stablecoin, a tokenised deposit or, eventually, a digital euro, provided it is high quality, openly accessible and able to move

across the multiple public blockchains, more than fifteen in the Aave Protocol's case, where onchain activity takes place. Multi-chain interoperability does introduce bridge risk, and cross-chain bridge compromises have been among the largest categories of DeFi loss (Q60). Money issued natively on each chain by its issuer, or moved through issuer-operated burn-and-mint mechanisms, avoids concentrating value in a single third-party bridge contract, as wrapped tokens do. Any interoperability framework should favour native multi-chain issuance, which addresses the EBA's concern about wrapped tokens without abandoning interoperability itself.

4.6 — Legal Treatment of Tokens

Question 80

Is there legal uncertainty as to the private law treatment of issuance, holding and transfers of tokens, under national law?

☒ **Yes**

☐ **No**

If you believe there is material legal uncertainty in issuing, holding and transferring tokens (i) which of the following issues are most significant and (ii) what is the urgency with which each issue should be addressed by regulators?

Scales used: Significance of legal uncertainty: 1 = None or Not significant · 2 = Low · 3 = Moderate · 4 = High · 5 = Very high. Urgency of regulatory clarification or action: 1 = None or Not urgent · 2 = Low urgency · 3 = Moderate urgency · 4 = High urgency · 5 = Immediate / critical

- *Issuing a crypto-asset token in compliance with national law* — **Aave Labs: significance 3, urgency 2**
- *Issuing a tokenised financial instrument in compliance with national law* — **Aave Labs: significance 4, urgency 3**
- *Transferring ownership (acquisitions, dispositions, earmarking, etc.) over a token, including good faith acquisition / bona fide ownership* — **Aave Labs: significance 5, urgency 4**
- *Recognising ownership in a token towards third-parties* — **Aave Labs: significance 5, urgency 4**
- *Using tokens as collateral* — **Aave Labs: significance 5, urgency 4**
- *Possibility to differentiate between native and non-native tokens in national law* — **Aave Labs: significance 3, urgency 3**
- *Recognising tokens as objects of property* — **Aave Labs: significance 5, urgency 4**
- *Rights of token holders in intermediated custody chains* — **Aave Labs: significance 4, urgency 3**
- *Enforcement and exercise of rights arising from /over tokens or the underlying assets* — **Aave Labs: significance 4, urgency 3**
- *Custody of tokens* — **Aave Labs: significance 3, urgency 3**

- *Treatment of tokens in insolvency proceedings including intermediary risk* — **Aave Labs: significance 5, urgency 4**
- *Others*

Please explain your reply and provide examples from national law. In particular specify if any of the answers is specifically referring to native or non-native tokens and specify if any of the answers would be different depending on if the token is recording a tokenised financial instrument or crypto-assets.

Aave Labs response

Yes. Legal uncertainty is greatest exactly where onchain finance creates most value: using tokens as collateral. A lender or protocol needs to know that the collateral posted is the borrower's to give, that the transfer is effective against third parties, that liquidation passes good title, and that the position survives a counterparty's insolvency. Each depends on national property law, which MiCA deliberately left untouched, and Member States answer differently. That is why we rate collateral use, recognition as property, transfer of ownership, third-party effect and insolvency treatment as the highest priorities. The issue is not confined to DeFi: as the Eurosystem accepts DLT-based assets as collateral and tokenised securities settle onchain, banks and central securities depositories face the same questions.

Germany shows why this matters. German property law confines 'things' capable of ownership (BGB s.90) to corporeal objects, so a token does not qualify. The only targeted fix, the Electronic Securities Act (eWpG, 2021), uses a legal fiction (s.2(3) eWpG) limited to bonds, fund shares and similar instruments on a securities register, not crypto-assets generally or the DeFi-native tokens used as collateral on the Aave Protocol. Outside that carve-out, scholars disagree whether tokens transfer under the rules for movables (BGB ss.929 ff.) or for assignment of claims (ss.398, 413). Good-faith acquisition from a non-owner has no settled basis, and tort protection is doubtful because tokens generally are not a protected 'other right' under s.823(1). Whether posting a token as collateral has the effect of a traditional security transfer is therefore unsettled at the most basic level. (S. Omlor, 'Germany and the EU', in M. Eggen, L. Jeng and S. Omlor (eds), *Control and Ownership of Digital Assets: A Comparative Law Survey* (Mohr Siebeck, 2026), co-edited by Linda Jeng of Aave Labs.)

France has moved the other way. Its crypto-asset ownership law was split across categories until 2024; in *BitSpread v Paymium* (T. com. Nanterre, 26 February 2020) a court had to treat a bitcoin loan as a 'consumption loan' of fungible objects to resolve a dispute. Ordinance no. 2024-936 now treats digital assets as 'negotiable intangible movables', transfers ownership on registration in the ledger (subject to a custodian-register exception) and protects good-faith acquirers: in substance, a ledger-based model like Model I in Q82. Germany and France have thus reached very different destinations in the same period, which is why this cannot be left to national convergence. French commentary also notes that seizure procedure presupposes a third party who can be served, so a self-custodied asset may be de facto beyond seizure, a gap in the enforcement of rights. (E. Farnoux, 'France', in the same volume.)

The answers differ by type of token. For native tokens, including crypto-assets and DeFi-native tokens such as aTokens and governance tokens, the token is the only record of the asset, so uncertainty goes to the heart of ownership: there is no underlying register to fall back on. For non-native tokens representing securities or other off-chain assets, the question is instead whether transferring the token transfers the underlying right, and how the ledger relates to existing securities registers; national laws such as Germany's eWpG and France's DLT registration regime address this in part, but differently. Model 1, the ideal for native tokens, and Model 3, the realistic EU-wide functional rule (Q82), would together serve both, and we propose an optional, control-based EU regime in Q86.

Question 81

Would you recommend increasing the legal certainty in the treatment of tokens through EU law?

☒ **Yes**

☐ **No**

Aave Labs response

Yes. Legal certainty is a precondition for using tokens as collateral across borders (Q80), and divergent national laws cannot deliver it: Germany and France have moved in opposite directions within the same period. EU action should take the form of an optional, control-based regime of functional rules (Model 3 in Q82), respecting Member States' property systems and aligned with the UNIDROIT Principles on Digital Assets and Private Law, accompanied by a conflict-of-law rule (Q84). It should also give legal effect to automated, smart-contract-executed transfers such as liquidations, for which existing formalities were not designed.

Question 81.1

If YES, what are the 3 most important elements that should be addressed in EU law? Please explain your answer and provide examples.

Aave Labs response

First, entitlement and third-party effect. EU law should determine who is entitled to a token recorded on a DLT register and give that entitlement effect against everyone, including creditors, based on control of the token rather than on national categories of 'things' or 'claims'. Outside the narrow scope of the eWpG, German law may not even recognise a token as capable of ownership (Q80), while the UNIDROIT Principles on Digital Assets and Private Law and Article 12 of the US Uniform Commercial Code already use control as the test.

Second, good-faith acquisition and finality of transfers. A person who acquires a token for value, in good faith and through a valid ledger transfer, should take it free of competing claims, and transfers executed automatically by smart contracts, including liquidations, should be final and effective. Without this, every step in a chain of onchain transactions is

exposed to a prior owner's claim. France's 2024 Ordinance already protects good-faith acquirers, and UCC Article 12 has a comparable 'take-free' rule.

Third, collateral and insolvency. EU law should confirm that security over tokens, and its enforcement by onchain liquidation, is effective against third parties and survives the insolvency of a borrower, lender or intermediary, and that client tokens held in custody do not form part of a custodian's estate. Extending the Financial Collateral Directive to tokens would address much of this. The Celsius bankruptcy, in which customers' crypto-assets in its Earn programme were held to belong to the company, shows what is at stake for users of custodial services.

Question 81.2

If you believe there is a lack of legal certainty regarding tokens, can legal certainty (ownership or entitlement, transfer and enforceability of rights recorded as tokens) be achieved under EU law in one of the following manners?

Rank the below possible measures from 1 to 5. 1. Strongly disagree, 2. Rather disagree, 3. Neutral, 4. Rather agree, 5. Strongly agree

- Implementation of a 28th regime recognising legal effects of DLT registers holding tokens, including good-faith acquisition rules and rules on opposability/enforceability to third parties (erga omnes effects) — Aave Labs: 5*
- Full harmonisation of private law treatment of tokens in Member States — Aave Labs: 2*
- Partial harmonisation of private law treatment of tokens in Member States — Aave Labs: 4*
- Introducing a conflict of law regime for tokens under EU law — Aave Labs: 5*
- Other model*

Please explain your response and provide examples, in particular from national law. Where you favour full or partial harmonisation or the introduction of a conflict of laws regime, please specify which legal instrument would be most appropriate for that purpose (a new Regulation or the use of existing regimes, such as MiFID or MiCA). Also consider if there are risks with establishing an ownership regime at EU level and how these risks could be mitigated.

Aave Labs response

We strongly agree with a 28th regime recognising the legal effects of DLT registers holding tokens, with good-faith acquisition rules and erga omnes effect (5). This is Model 3 in Q82 in optional form, and it extends the approach of the Euroclear/Clearstream '28th regime' proposal beyond issuance. We strongly agree with an EU conflict-of-law regime (5), which is needed whatever substantive approach is taken (Q84). We rather agree with partial harmonisation (4) limited to the functional effects of ledger entries, transfers and collateral set out in Q81.1, and rather disagree with full harmonisation of private law (2), which would collide with Article 345 TFEU and 27 property-law systems for little additional benefit.

The most appropriate instrument is a new, directly applicable Regulation covering all tokens, crypto-assets and tokenised financial instruments alike, rather than amendments to MiCA or MiFID, which each cover only one of those categories and are regulatory rather than private-law instruments. Collateral aspects could be addressed by extending the Financial Collateral Directive to tokens.

An EU ownership regime carries risks: overlap with national property law, parallel regimes that add complexity, and rules that date quickly as technology changes. They can be mitigated by making the regime optional and effects-based rather than constitutive, technology-neutral, aligned with the UNIDROIT Principles, clear about when it applies (for example, by designation in the token or its system), and subject to a review clause.

Question 82

There are different “ownership models” that could be used to increase legal certainty over tokens. Please indicate maximum two models listed below that you think EU law could apply if it were to improve the legal certainty of tokens in the EU.

- ☒ **Model 1: The token is the asset by law, the law recognises a ledger-based asset and the ownership rights are constituted directly by the ledger entry.**
- ☐ *Model 2: The token is the asset by law, where the law recognises that e.g. securities (dematerialised or physical) can be replaced by an entry into a DLT register and by this “replacing” (immobilisation) of the securities the function of the initial security is substituted by entry into a DLT register and the ownership rights are constituted by the representation on the ledger.*
- ☒ **Model 3: Token is the asset by law. In this case the law does not actively regulate legal aspects such as what property is or how transfer of ownership occurs, etc. but instructs on the legal consequences of entries in a DLT register (this is often called a functional approach). The law could at EU level stipulate who may exercise rights, i.e. the person recorded in the DLT register as holder of a tokenised asset, that these rights have full third-party effect and protects from competing claims. This also creates legal certainty for collateral use. The EU law would create a uniform rule of “digital entitlement” that functions across all Member States’ property law structures.**
- ☐ *Model 4: The token is the legal carrier of rights associated with a related (often off-chain) asset. The law defines tokens as legal objects that do not create new rights, but can –like a “container” –represent various kinds of rights, such as membership rights, ownership, intellectual property rights, usage rights or rights of lien, etc.. The token would represent the rights stemming from the underlying assets and the law would ensure that the transfer of a token on the ledger legally transfers ownership of the rights stemming from the underlying asset.*
- ☐ *Model 5: Any other legal ownership structures, for example based on the approaches taken by different countries, including France, Germany, Luxembourg or adopted in other jurisdictions or internationally, that could be implemented in EU law.*

Please explain your answer and provide examples, and in answering the question, please answer the following sub-questions:

- a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?*
- b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?*
- c) Are the different ownership models better suited for native or non-native tokens?*
- d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments) and if not, what would need to be different depending on the type of the token?*

Aave Labs response

Models 1 and 3. Model 1 is the ideal. Where the token is the asset and the ledger entry constitutes ownership, onchain finance works as it is designed to: transfer, collateral and liquidation all happen on the ledger, with no off-chain register to reconcile and no legal fiction to rely on. France's 2024 Ordinance, which transfers ownership of digital assets on registration in the ledger and protects good-faith acquirers, shows that this is workable in a Member State (Q80). We would encourage Member States to adopt it for native tokens.

Model 3 is the more realistic option at EU level. Article 345 TFEU leaves the system of property ownership to Member States, and a constitutive EU ownership rule would have to be reconciled with 27 property-law systems. Model 3 avoids that. Like the Financial Collateral Directive and the Settlement Finality Directive, it would harmonise the legal effects of an arrangement, here a ledger entry, without rewriting national property law: who may exercise the rights, their full third-party effect, priority over competing claims and protection of good-faith acquirers. That delivers the certainty collateral use needs, as the consultation itself notes, for native and non-native tokens alike.

We do not oppose Model 2. It suits tokenised securities that replace existing ones, and it is broadly what Germany's eWpG and Luxembourg's DLT securities laws already do. But it is narrower, and Model 3 would give tokenised securities the same collateral certainty. Model 4 leaves the link between a token and its underlying asset to national law, and Model 5 would preserve the fragmentation that causes today's uncertainty.

On the sub-questions: (a) Model 3 would sit on top of national private law rather than replace it, as the Financial Collateral Directive does, so each Member State keeps its property categories while the EU rule fixes the effects of a ledger entry. (b) Functional rules are preferable at EU level; constitutive rules along Model 1 lines are the better choice for Member States willing to adopt them, as France has. Functional rules also accommodate automated, smart-contract-executed transfers such as liquidations, without formalities designed for manual transactions. (c) Model 1 is best suited to native tokens, where the ledger is the only record; non-native tokens also need rules linking the token to the underlying right, which

Model 3 can supply by giving the ledger entry legal effect over that right. (d) The same functional core can apply to all tokens. For DLT financial instruments it must be aligned with securities law, including the Settlement Finality Directive, CSDR and the DLT Pilot Regime, and with how ledgers relate to existing registers; for crypto-assets, the ledger itself should be decisive.

This functional, control-based approach is already emerging elsewhere. In German reform scholarship, Omlor proposes replacing 'possession' with 'control' for incorporeal crypto-assets, following the UNIDROIT Principles on Digital Assets and Private Law (Principle 6), with transfer by agreement plus ledger entry and good-faith acquisition keyed to the ledger (Q80). The UNIDROIT Principles, Article 12 of the US Uniform Commercial Code and the UK's Property (Digital Assets etc) Act 2025 point the same way. Aligning Model 3 with that work would make the EU's rule interoperable with international practice rather than a competing standard.

Question 82 – Model 1 (a)

MODEL 1 – a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

Aave Labs response

A constitutive EU rule under which the ledger entry itself creates ownership would have to fit 27 property-law systems that Article 345 TFEU leaves to Member States, so its interoperability as an EU-level measure would be limited. It interoperates best where Member States adopt it themselves, as France did in Ordinance no. 2024-936, or as an optional regime that tokens designate. In Germany it would require recognising tokens as a category of property beyond corporeal 'things' (BGB s.90), which the eWpG has done only for crypto securities entered in a crypto securities register. Model 1 is therefore the ideal for native tokens, best pursued nationally, while Model 3 provides the EU-wide layer (Q82).

Question 82 – Model 1 (b)

MODEL 1 – b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

☒ **Constitutive rules of ownership based on the asset being recorded on chain**

☐ *Functional rules regulating the effects of recording an asset on chain*

☐ *Don't know / no opinion / not applicable*

Please explain your answer.

Aave Labs response

For Model 1, constitutive rules. The model's strength is that the ledger entry is the ownership, so transfer, collateral and liquidation all happen onchain with no off-chain record to reconcile.

That is the ideal for onchain finance. As an EU-level measure we prefer functional rules (Model 3), for the reasons of competence and interoperability given in Q82; constitutive rules are best adopted by Member States willing to do so, as France has.

Question 82 – Model 1 (c)

MODEL 1 – c) Are the different ownership models better suited for native or non-native tokens?

☒ **For native**

☐ *For non-native tokens*

☐ *Don't know / no opinion / not applicable*

Please explain your answer.

Aave Labs response

Model 1 is best suited to native tokens, where the token is the only record of the asset and there is no off-chain register or underlying right to reconcile: crypto-assets and DeFi-native tokens such as aTokens and governance tokens. For non-native tokens representing an off-chain asset, a constitutive ledger rule would also need rules linking the token to the underlying right, which Model 1 does not supply by itself.

Question 82 – Model 1 (d)

MODEL 1 – d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

☐ **Yes**

☒ **No**

☐ *Don't know / no opinion / not applicable*

What would need to be different depending on the type of the token?

Aave Labs response

Model 1 fits native crypto-assets well, but not every type of token. For DLT financial instruments, the ledger entry can constitute the instrument, as with Germany's crypto securities register, but the rules must also align with securities and company law, the Settlement Finality Directive, CSDR and the DLT Pilot Regime, and address intermediated holding and the relationship between the ledger and any issuer register. For non-native tokens representing off-chain assets, rules are needed on how transferring the token transfers the underlying right and how that is enforced off-chain.

Question 82 – Model 1 (explanation)

Please explain your answers for MODEL 1 and provide examples.

Aave Labs response

Model 1 is the ideal for onchain finance: transfer, collateral and liquidation happen on the ledger, and ownership follows the entry. France's 2024 Ordinance treats digital assets as

negotiable intangible movables, transfers ownership on registration in the ledger (with a custodian-register exception) and protects good-faith acquirers. Germany's eWpG applies similar logic to crypto securities entered in a crypto securities register, and the UK's Property (Digital Assets etc) Act 2025 confirms that digital assets can be objects of property rights. For users of the Aave Protocol, Model 1 would give certainty that supplying a token, receiving a receipt token or having collateral liquidated onchain transfers ownership exactly as the ledger shows. We encourage Member States to adopt it for native tokens, alongside the EU-wide functional rule in Model 3.

Question 82 – Model 3 (a)

MODEL 3 – a) What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?

Aave Labs response

High. Model 3 would sit on top of national private law rather than replace it, as the Financial Collateral Directive and the Settlement Finality Directive do. Each Member State keeps its own property categories, while EU law fixes the legal effects of a ledger entry: who may exercise the rights, their full third-party effect, priority over competing claims and protection of good-faith acquirers. In Germany it would give ledger entries legal effect without first resolving whether a token is a 'thing' or a 'claim' (Q80); in France it is consistent with the ledger-based 2024 Ordinance. That compatibility with 27 systems, and with Article 345 TFEU, is why Model 3 is the realistic EU route (Q82).

Question 82 – Model 3 (b)

MODEL 3 – b) Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?

☐ *Constitutive rules of ownership based on the asset being recorded on chain*

☒ **Functional rules regulating the effects of recording an asset on chain**

☐ *Don't know / no opinion / not applicable*

Please explain your answer.

Aave Labs response

Functional rules are preferable at EU level. They respect Member States' competence over property ownership, work across different national systems, and can be written to accommodate automated, smart-contract-executed transfers such as liquidations without formalities designed for manual transactions. Constitutive rules along Model 1 lines remain the better choice for Member States willing to adopt them.

Question 82 – Model 3 (c)

MODEL 3 - c) Are the different ownership models better suited for native or non-native tokens?

☐ For native

☒ **For non-native tokens**

☐ Don't know / no opinion / not applicable

Please explain your answer.

Aave Labs response

Model 3 suits both, but it adds most for non-native tokens representing securities or other off-chain assets, where the key question is whether the person recorded on the ledger can exercise the underlying rights with effect against third parties. Model 3 answers that directly. It also works for native tokens, where it can sit alongside a Model 1 rule.

Question 82 – Model 3 (d)

MODEL 3 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

☒ **Yes**

☐ No

☐ Don't know / no opinion / not applicable

What would need to be different depending on the type of the token?

Aave Labs response

The same functional core can apply to all tokens: legal effect of the ledger entry, third-party effect, priority and good-faith protection. What differs is the interface with other law. For DLT financial instruments, the rule must align with securities law, including the Settlement Finality Directive, CSDR and the DLT Pilot Regime, and with how the ledger relates to existing registers and intermediated holding chains. For crypto-assets, the ledger itself should be decisive. For non-native tokens, the rule should provide that the recorded holder may exercise the rights in the underlying asset.

Question 82 – Model 3 (explanation)

Please explain your answers for MODEL 3 and provide examples.

Aave Labs response

Model 3 follows a proven EU technique: the Financial Collateral and Settlement Finality Directives harmonised legal effects without harmonising property law. International work points the same way. The UNIDROIT Principles on Digital Assets and Private Law base proprietary effects on 'control', and Article 12 of the US Uniform Commercial Code lets a purchaser who obtains control of a controllable electronic record for value and in good faith take it free of competing claims. In German reform scholarship, Omlor proposes replacing 'possession' with 'control' for crypto-assets, with transfer by agreement plus ledger entry

(Q80). An optional EU regime along these lines, extending the Euroclear/Clearstream '28th regime' proposal beyond issuance, would give lenders, protocols and institutions a single rule for collateral across the EU (Q81.2).

Question 83

Comparing national laws of Member States, what are the main differences in how national laws governs the issuance, holdings and transfers of tokens? Please explain your answer and provide examples.

Aave Labs response

National laws differ on four points that matter most for issuance, holding and transfer. First, what a token is. Germany confines ownership to corporeal 'things' (BGB s.90), so outside the eWpG a token is neither clearly property nor clearly a claim; France since 2024 treats digital assets as 'negotiable intangible movables' (Ordinance no. 2024-936).

Second, scope. Several Member States have legislated only for financial instruments. Germany's eWpG covers bonds, fund shares and similar instruments recorded in electronic or crypto securities registers; Luxembourg's 2019 and 2021 blockchain laws allow securities to be held in accounts and issued on DLT; and Italy's 2023 FinTech Decree (Decree-Law no. 25/2023) governs financial instruments issued and transferred in digital form. France is unusual in covering digital assets generally.

Third, how transfer happens. In France ownership passes on registration in the ledger for the acquirer's benefit, subject to a custodian-register exception. For German crypto-assets outside the eWpG, scholars disagree whether the rules for movables or for assignment of claims apply, with different formalities and effects.

Fourth, protection of acquirers and creditors. Good-faith acquisition is expressly protected in France and for German electronic securities, but has no settled basis for ordinary crypto-assets in Germany. Enforcement also differs: French commentary notes that seizure procedure presupposes a third party who can be served, leaving self-custodied assets largely beyond it.

The result is that the same token, transferred or posted as collateral onchain, can have different legal effects depending on which Member State's law applies, and for tokens held without an intermediary it is often unclear which law that is (Q84.1). That is why we propose an EU functional rule (Model 3) with a conflict-of-law rule (Q81.2, Q84). The German and French analysis draws on the chapters by S. Omlor and E. Farnoux cited in Q80.

Question 84

Should EU law introduce a conflict of law rule for tokens?

☒ **Yes**

☐ **No**

Aave Labs response

Yes. Even with harmonised substantive rules, a lender needs to know in advance which law governs a token and any collateral arrangement over it. For tokens on a decentralised ledger, traditional connecting factors, such as the location of the asset, an account or an intermediary, often point nowhere or everywhere. EU law should adopt a clear rule that parties can apply in advance, following the approach of the UNIDROIT Principles on Digital Assets and Private Law: the law expressly specified in the token or its system, failing which the law of the issuer's statutory seat where there is an identifiable issuer, with a residual fallback, which could be the optional EU regime itself for tokens that opt into it. The Commission should coordinate with the Hague Conference on Private International Law, which is working on the same question, so that the EU rule is internationally interoperable. For tokenised financial instruments held through intermediaries, the rule should be consistent with the existing conflict-of-law rules in the Settlement Finality and Financial Collateral Directives.

Question 84.1

If you answered "YES" please explain why the current conflict of law rules applicable in EU are not enough or sufficiently clear in its application to tokens?

Aave Labs response

Existing EU conflict rules were built for assets that sit somewhere or are held with someone. Rome I governs contractual obligations, not the proprietary effects of a transfer. The Settlement Finality and Financial Collateral Directives point to the law of the place where the relevant register or account is maintained, which assumes an intermediary maintaining an account, and insolvency rules similarly rely on location. For a token on a decentralised ledger there is no account maintained by an intermediary and no physical location, so the law of the place where the asset is situated has nothing to attach to, and account-based rules apply only where tokens are held through an intermediary. National courts are left to improvise, which is the very uncertainty the consultation identifies (Q80). MiCA itself contains no conflict-of-law rule for proprietary questions.

Question 84.2

If the EU would introduce conflict of law rules for proprietary aspects of tokens, what would be the preferred connecting factors. Rank the below listed connection factors from 1 to 5 (1 being the most relevant connecting factor and 5 the least relevant connection factor).

Connecting factors without a ranking will be considered not relevant.

- *The law of the state specified in the token or in the principles (if any) expressly specified in the token* — **Aave Labs: rank 1**
- *The law of the state specified in the rules or in the principles of the system on which the token is recorded* — **Aave Labs: rank 3**
- *The law of the state in which the legal entity operating the DLT-based system on which tokens are recorded* — *not rated*

- *In relation to a token for which there is an issuer, the law of the state where the issuer is established* — **Aave Labs: rank 2**
- *In relation to tokens for which there is an issuer, the law of the state under whose supervision the issuer operates* — **Aave Labs: rank 5**
- *In relation to tokens for which there is a provider of the technologies creating or issuing the tokens, the law of the state under whose supervision such technology operates* — *not rated*
- *Where a token shall be registered, the law of the state under whose supervision the register is maintained* — **Aave Labs: rank 4**
- *The law of the state of the relevant operating authority/administrator (PROPA), meaning a state authority or a body (e.g., a foundation) that takes over the administration of the system onto which the token is registered* — *not rated*
- *The law of the state of the primary residence of the encryption private master keyholder (PREMA), meaning the seat of a body that holds a system-relevant master key, with the help of which coercive transactions can be carried out, for example, based on a court order.* — *not rated*
- *Any other?* — *not rated*

Please explain your response and provide examples. In answering this question, please consider if the suggested scope of the conflict of law rule in your view is the right one, and whether there are aspects missing.

Aave Labs response

We rank first the law expressly specified in the token (1), which respects the choice made by those who create and use it. Where there is an issuer, the law of the state where it is established should come next (2): for issued tokens such as stablecoins and tokenised securities it is predictable, easy to identify and aligned with the regime that supervises the issuer. The law specified in the rules of the system on which the token is recorded follows (3), consistent with the UNIDROIT Principles on Digital Assets and Private Law, then, for tokens that must be registered, the law of the state supervising the register (4), and the law of the issuer's supervisor (5).

We do not consider the other factors relevant for decentralised systems. Permissionless blockchains have no legal entity operating them, no operating authority or administrator and no master keyholder, so rules built on those factors would either point nowhere or create an incentive to introduce central points of control. A residual fallback is still needed where no law is specified and there is no issuer; the optional EU regime proposed in Q81.2 could serve that role for tokens that designate it.

Question 85

If there are any other issues relating to legal certainty which are not mentioned above, please describe them here.

Aave Labs response

Four further issues deserve attention. The first is enforcement of security by onchain liquidation. In many Member States, enforcing a pledge requires prior notice, a waiting period, court approval or a public auction. Onchain liquidation, executed automatically by a smart contract when a position falls below its collateral threshold, meets none of these formalities, yet it is what protects lenders and keeps DeFi lending markets solvent. The Financial Collateral Directive already disapplies such formalities for financial collateral (Article 4(4)); extending it, or an equivalent rule, to crypto-assets and other tokens would give automated liquidation clear legal effect.

The second is receipt tokens. When a user supplies assets to a lending protocol, it receives a receipt token, such as an aToken, recording its claim on the pool. EU law should confirm that such a receipt simply evidences the user's claim and does not, by itself, create a new financial instrument or change the characterisation of the underlying asset (Q1).

The third is the evidential value of public ledgers. The revised eIDAS Regulation gives legal presumptions to qualified electronic ledgers, but public permissionless blockchains, which have no qualified trust service provider operating them, fall outside that framework. Courts and authorities should be able to rely on records on widely used public blockchains as evidence of transfers and holdings, subject to ordinary rules of proof.

The fourth is remedies that fit immutable ledgers. Where a court finds that a transfer should be reversed, for example after fraud, remedies should operate on persons, through orders to re-transfer or compensate, rather than assume that a ledger can be altered. Legal certainty for users depends on knowing that an onchain record will not be rewritten, and that recourse lies against the person who acted wrongfully.

4.8 – Final Open Question

Question 86

Interested parties that wish to bring other relevant issues, not raised in this consultation, to the Commission's attention, should feel free to communicate them here.

Aave Labs response

Aave began in Europe, and Europe has the chance to lead onchain finance. Our answers rest on six points, cross-referred throughout.

Protect self-custodial finance; regulate intermediaries, not software. Self-custodial finance, holding, using and lending one's own assets without an intermediary, should be recognised as a right for Europeans, consistent with the right to property in Article 17 of the Charter. Classification should follow the substance of an activity, not its technology, which is simply an instrumentality. The decisive question is whether an identifiable legal person controls the activity and exercises active, ongoing discretion over it (Q61). Where one does, it should be regulated; our subsidiary Push is a MiCA-authorized CASP. Where none does, as with the Aave Protocol, self-custodial wallets and front-ends, and DAO governance, intermediary

obligations have nothing to attach to. Obligations should fall on intermediaries that hold client assets, such as CASPs and fiat on/off-ramps, through proportionate due diligence (Q62, Q62.1), not certification of software (Q63–Q65).

Keep savers' returns. The interest ban stops issuers and CASPs paying holders for holding a stablecoin. It must not be extended to lending returns paid by borrowers or to staking rewards paid by protocols, as the ECB proposes, nor should those returns be treated as 'arbitrage', as the EBA suggests. That would close a savings channel the Savings and Investment Union should want, strip institutions of tools for treasury, liquidity and financial risk management, and make MiCA stablecoins the least useful in onchain markets (Q59, Q66, Q67).

Let euro stablecoins compete. Aave Labs is agnostic about the form of digital money, whether CBDC, tokenised deposit or stablecoin, provided it is high-quality, well-managed, openly accessible and interoperable across blockchains; the Aave Protocol runs on more than fifteen. Euro stablecoins need risk-sensitive liquidity requirements instead of fixed bank-deposit minimums (Q29), fungible multi-issuance (Q38) and continued EU access to global liquidity (Q27, Q56). Most euro money is commercial bank money created through lending; tokenised central bank money should anchor that system, not replace it.

Build on open infrastructure. DeFi protocols are an infrastructure layer for onchain finance; as with TCP/IP, regulators supervise the firms building on it (Q45). Banks will need to integrate with these protocols, so DORA's third-party rules should apply to application-layer providers, not public blockchains, and the EU should follow the Basel Committee's review in assessing networks on decentralisation, economic security and controls rather than on whether they are permissioned. Overcollateralised lending will evolve into onchain securities financing as real-world assets are tokenised, complementing the Eurosystem's acceptance of DLT-based collateral, Pontes and Pythagore; Pontes and Appia should remain open to public networks (Q67).

Give tokens legal certainty. Collateral depends on national property laws that diverge sharply (Q80). We propose an optional, control-based EU regime, with Model 1 as the ideal and Model 3 as the realistic EU route (Q82), extending the Euroclear/Clearstream '28th regime' proposal beyond issuance and drawing on the UNIDROIT Principles, UCC Article 12 and the UK's Property (Digital Assets etc) Act 2025. Aave Labs would welcome the opportunity to contribute.

Supervise with the ledger, and keep raising the bar. Public ledgers offer real-time, immutable data, auditable code and visible interconnections. We propose standardised machine-readable risk disclosure, supervisory observer nodes, shared onchain analytics, embedded-supervision pilots and tech sprints, in which Aave Labs would take part. Programmable compliance enforces eligibility, sanctions and collateral rules at each transaction, as in Aave Horizon. Industry standards also keep rising: the Aave Protocol has undergone some 65 audits, and in July 2026 Aave DAO tokenholders adopted the Aave Risk Framework and the Technical Asset Listing Framework (Q63).