coinbase

To:
Directorate-General for Financial Stability, Financial Services and Capital Markets Union
European Commission
1049 Bruxelles/Brussel
Belgium

7 August 2025

Re: European Commission Report on Markets in Crypto Asset Regulation

Coinbase Global, Inc. (together with its subsidiaries, **Coinbase**) appreciates the opportunity to share our views with the European Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (the **Commission**) ahead of the Commission's report on latest crypto developments under Article 142 of MiCA as well as the interim report under Article 140.

We are committed to the EU as one of our largest international markets outside of the US. We believe we are well placed to transition to a MiCA license, and we are excited by the opportunities presented across the region.

MiCA establishes a strong foundation, but the EU must remain adaptable to evolving market developments. As the US accelerates its regulatory framework for crypto, it is crucial for the EU to continue positioning itself as a leading hub for innovation and growth. Global cooperation, not only in regulating centralized markets, but also in the realm of DeFi, is vital to ensure open and interconnected markets. To that end, the Commission's primary focus should be on the effective implementation of MiCA, while preserving the flexibility for future developments.

Coinbase appreciates the opportunity to contribute early considerations on potential areas for further development and review of the MiCA framework.

Yours sincerely,

Tom Duff Gordon, Vice President, International Policy, Coinbase

Scott Bauguess, Vice President, Global Regulatory Policy, Coinbase

coinbase

Introduction

The crypto asset sector is fast evolving. To maintain a leadership role, the EU must remain committed to the creation of an environment for EU companies and individuals to reap the benefits of the next wave of crypto innovation while keeping pace with the changing regulatory landscape, in particular in the US.

The Markets in Crypto Assets (**MiCA**) Regulation marked an important milestone in the regulation of the crypto industry, driving institutional confidence and reducing regulatory uncertainty for centralized crypto markets. These advancements are crucial for fostering long-term growth and stability in the sector and the primary focus should now be on its implementation.

However, the global crypto market has evolved significantly since MiCA's adoption. One notable development is the rise of tokenised assets and their interplay with decentralised exchanges (**DEXes**), is unleashing a new wave of innovation. To fully benefit from these advancements, the EU must stay agile, supporting local innovation, engaging with the global crypto ecosystem, and embracing international cooperation to ensure access to cross-border opportunities.

We welcome the Commission's mandate under Article 140 to produce an interim report on MiCA implementation by mid-2025, and under Article 142 to examine developments in DeFi, crypto lending, borrowing, and NFTs. These reviews offer critical opportunities to ensure Europe's regulatory framework remains fit for purpose.

Our overarching vision

DeFi and permissionless blockchain networks represent a major opportunity to enhance efficiency and reduce intermediation in capital markets. Peer-to-peer or peer-to-pool protocols like DEXes remove the need for brokers, custodians, and clearing agencies, cutting costs and boosting transparency, while providing users greater discretion over their assets. These innovations do not mean that there is no role for intermediaries. Many if not most consumers will still seek intermediaries to act on their behalf, but the option for self-directed activity will nonetheless provide them with benefits by facilitating new products and competition.

For this reason, regulatory frameworks must evolve to recognize and encourage the benefits of self-custody and open infrastructure, and refrain from viewing them as risks to be suppressed. Doing so will advance a more competitive and inclusive EU financial system.

We therefore welcome the targeted consultation on capital markets integration as a valuable opportunity to rethink EU market regulation holistically bridging traditional

finance and crypto, including DeFi. We urge the Commission to await its outcome before proposing new rules on crypto-asset activities.

To deliver on this vision, we would recommend the European Commission to:

1. **Remain focused on MiCA implementation:** MiCA rightly targets centralized intermediaries where most activity and risk reside. These entities are best placed to comply with regulatory obligations. Implementing these rules consistently is the best way to ensure a level playing field for CASPs and issuers across the EU.

2. **Clearly distinguish technology services from regulated financial services :** DeFi protocols are non-custodial and permissionless by design. As the Commission has acknowledged, compliance can be achieved higher in the technology stack, avoiding base-layer regulation that risks stifling innovation. And when considering regulation, it is crucial to clearly delineate between financial services (and other regulated activity, such as payment services) and mere technology services, such as self-hosted wallet software that can be used for many different blockchain functions that are not necessarily related to financial activity.

3. **Safeguard self-custody and user autonomy:** The future of digital markets includes self-custodied assets. Blockchain technology enables users to hold and control assets directly, without intermediaries and regulation should support this innovation. Allowing secure, efficient self-custodial solutions, will promote user autonomy, reduce systemic risk, and advance financial inclusion.

Decentralised and Onchain Finance

DeFi has great potential, offering more inclusive, transparent, and open access to financial services. The EU should ensure that DeFi protocols remain outside of the regulatory scope of MiCA (or MiFID) where certain conditions are met. This approach would be consistent with the approach taken by the US, which is pursuing a nuanced approach to DeFi activities, recognizing a difference between custodial versus non custodial products.[1] Similarly, in the UK, the proposed new crypto regime explicitly carves out genuinely decentralised activities (DeFi).[2] While there is still room to finetune an understanding of what genuine decentralisation means (and we outlined what we think

[1] FinCEN. "*Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies Guidance on Business Models Involving Virtual Currencies*," FinCEN Guidance (May 9, 2019).
[2] Financial Conduct Authority, *DP25/1: Regulating Cryptoasset Activities* (Discussion Paper, 2 May 2025), https://www.fca.org.uk/publication/discussion/dp25-1.pdf.

appropriate criteria are elsewhere[3]), the direction of travel is clear: a financial services regime or CASP-type regime is ill-suited for DeFi.

The same applies to self-custodial wallets (**SCWs**), including DeFi integrations in those SCWs. These are software integrations that facilitate a user using their self-custodial wallet to access permissionless blockchain networks to engage in self-directed transactions involving digital assets and that do not effectuate the underlying blockchain transactions (which are instead effectuated programmatically by third party blockchain protocols), do not exercise ultimate discretion over a user's decision to engage in a particular transaction, do not facilitate the settlement or execution process and do not have unilateral custody or control over the user's assets. SCWs are software (technology), not financial services.

Wallet software can be used for many different blockchain functions that are not necessarily related to financial activity. The wallet software provider does not necessarily know, and should not be expected to know, what activities are conducted by users of the software or the nature of the digital assets or services they interact with. Technologically it makes no difference to the wallet software whether an ERC-20 token represents digital art or a tokenized financial instrument. We expect the US to take a clear, nuanced stance on SCWs in the near future and urge the Commission to keep a close eye on these developments.

We caution against the EU developing its own DeFi rules without consideration for developments in other jurisdictions. Doing so risks negatively impacting the EU's competitiveness in this nascent space. When combined with an extraterritorial approach, the likely impact is to push developers away from the EU and limit the access for EU citizens to DeFi products and services which may not be willing/able to meet EU requirements. Therefore, we would also welcome the EU taking a leading role in a review of IOSCO DeFi policy recommendations.

Decentralisation should be seen as a process and on a spectrum

Recital 22 of MiCA reads that "where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope". Accordingly, MiCA appropriately focuses on centralized exchanges and CASPs, where most business activity occurs and where familiar business models prevail. DeFi, by contrast, requires a distinct approach. We of course would support a consistent and workable interpretation of DeFi at the EU level – e.g. the Danish FSA launched a consultation on defining at what point a project is fully decentralised. Such interpretation

[3] Coinbase Global, Inc., *Response to the U.S. Securities and Exchange Commission's Request for Information: "There Must Be Some Way Out of Here"* (March 19, 2025), https://assets.ctfassets.net/o10es7wu5gm1/1pvwEbI9isoXp6M4UKsodS/f532652769263339ef990dade343b105/Coinbase_SEC_RFI_Response.pdf, 21.

should also be consistent internationally, including through a review of IOSCO policy recommendations for DeFi.

We agree that truly decentralized protocols should not be regulated under MiCA and offer that decentralization should be viewed on a spectrum, and that the presence of intermediaries should not be a factor in determining whether a protocol is centralized.

Decentralisation is not a binary state. It is a process, and it requires time and effort to achieve. In practice, a DeFi protocol is likely to proceed through phases of increasing decentralisation, at each phase enabling greater levels of participation from stakeholders beyond its initial development team. We offered our strong support to a safe harbor (or conditional exemption) proposal in the US and encourage the European Commission to consider adopting a comparable mechanism to foster innovation while ensuring appropriate safeguards.

Under existing EU rules on public offers, token sales are often limited in the first instance to qualified investors. Although this provides a path for developers to raise capital, it does not provide them with an efficient mechanism to distribute the tokens to intended users of the associated network, many of whom do not qualify as qualified investors. However, users generally must first purchase the tokens to gain access to and use a protocol or network. A safe harbor (conditional exemption) for token sales to retail participants, subject to tailored disclosure requirements, would solve this problem.

The ideal outcome for a DeFi project is typically the creation of a network, protocol or application that is collectively governed by a large, widely dispersed community of users. In this model, the development team is financially incentivised not to retain control of a project indefinitely, because its maximal value is realised only after token ownership is widely distributed to the users to whom control is ultimately relinquished. We would also welcome the European Commission initiating a review of capital raising frameworks similar to recent efforts in the US, to foster regulatory modernization that supports the trading of tokenized equity and bonds through decentralized exchanges.

Participating in, interacting with, or facilitating user interaction with, a DeFi protocol is not the same as control over the protocol

Intermediaries should be able to interact with, or facilitate a user interacting with, DeFi protocols, as the participation of one or more intermediaries does not affect the decentralisation of the protocol itself. For example, a centralised cryptoexchange may offer its users an integration with a decentralised exchange (DEX) to provide liquidity or execute trades on the DEX, but this does not mean that the DEX is now intermediated or otherwise centralised. Intermediaries interacting with DeFi protocols do not have control

of the DeFi protocol[4] and should not be regulated as the entity or person considered in control.

Similarly, SCW software providers or providers of APIs also do not hold control over a DeFi protocol simply by providing the SCW software, and should not be regulated as such. Non-custodial software providers that make it easier for users to translate their desired onchain activity into the appropriately formatted code that a protocol can read and execute, which users subsequently sign to send to the DeFi protocol, provide a technology service, not a financial service.

Separately a developer who no longer has unilateral control over a protocol should not bear legal responsibility for that protocol. While there is no obvious or clear threshold to define control, we propose the following broad principles to aid in this determination:

- No person or group of persons under common control has: the unilateral authority, via operation of the token or associated network, to restrict, censor, or prohibit use of the token or associated network; or private permissions, hard-coded privileges, or similar rights granted by the source code of the blockchain protocol or blockchain smart contract of the token or associated network that provide preferential treatment as compared to other similarly situated persons;
- The token or associated network has reached an autonomous state; and no person or group of persons under common control has the unilateral authority, directly or indirectly, to alter or change the functionality, operation, or rules of consensus or agreement of the token or associated network.

Regardless of the concentration of ownership of a token, as long as the associated network on which it functions cannot be altered by the protocol's decentralized governance system and thereby protects against anyone obtaining unilateral authority over others' assets, limit others' access to the token or associated network, or alter the protocol's autonomous operation in accordance with transparently encoded rules without private permissions or privileges, then the token or associated network should be considered sufficiently decentralized.

Whether a person or entity is in control of the DeFi arrangement should be based on clearly articulated parameters. We welcome a review of IOSCO DeFi policy recommendations in this regard.

Smart contract security certification should remain optional

We recognize the French ACPR's work in exploring the feasibility of certifying smart contracts to mitigate cybersecurity and other risks for users. We support initiatives aimed

[4] By definition a DeFi protocol is not controlled by a centralized intermediary (otherwise it is centralized finance, not DeFi).

at enhancing the resilience of smart contracts and note ongoing industry efforts to continuously improve smart contract resilience. Smart contract audits - often multiple audits - and bug bounties are already common practice in DeFi. Any security certification should remain optional, particularly given the rapid evolution of smart contracts and DeFi protocols.

We advocate for a broader, well-balanced security framework that recognizes the effectiveness of independent audits, bug bounties and peer-reviewed code assessments in mitigating risks. Encouraging open-source development fosters transparency and community collaboration, which are crucial for identifying vulnerabilities early. However, any framework should avoid imposing overly strict or centralized legislative controls.

While independent audits are an important component of security and standard industry practice, we caution against mandatory certification systems that could create excessive burdens or restrict access to decentralized financial services. Instead, we believe voluntary, community-driven self-certification mechanisms can provide the necessary oversight, while still allowing room for innovation in security practices.

Support industry-led technical solutions to MEV risks

As we noted in our response to ESMA's Third MiCA consultation[5] MEV is not inherently abusive. Instead, it is the value of ordering in a particular decentralized system, which results from the technical trade-offs inherent in that particular blockchain. While MEV can have certain negative externalities, it is a complex phenomenon that encompasses a wide range of activities that can be both harmful and beneficial. We therefore welcome ESMA's recognition that MEV requires a technical, rather than a prescriptive policy-based, solution.

As ESMA and EBA noted in their joint report on recent developments in crypto assets under Article 142 of MiCAR there are several industry initiatives underway to address negative externalities of MEV. These include the proposal-builder-separation (PBS) framework proposed by the Ethereum foundation,which introduces a mechanism to decouple block-proposing from block-building as well as initiatives to enforce a deterministic order of transactions.

Users also have access to protections on decentralised exchanges. For example, when a user initiates a trade on an automated market maker like Uniswap, they can select the level of slippage (post-order price movement) they are willing to accept, which is akin to specifying the bid-ask spread of a market order in a securities transaction. Users can also choose larger liquidity pools or use private mempools, both which limit the ability of other

[5] Coinbase Global, Inc. and Coinbase Europe Limited, *Response to EBA Third MiCA Consultation Package*, February 8, 2024, https://assets.ctfassets.net/c5bd0wqjc7v0/3nP4WsOnLhTcWl1mAQkkCF/47321cd102ac755ecf1716267a2687bb/Coinbase_-_Feb_2024_Response_to_EBA_Third_MiCA_Consultation_Package-1.pdf.

users to profit from their actions. Users' transactions can only be included in a block if a user's preferences – relating to more than just price – are met. This is a key differentiator of blockchain technology. Only valid transactions that are executed according to the selected preferences of the user can be included in blocks, regardless of their sequencing within the block. For traditional exchanges using permissionless blockchain, the whitelisting of market participants and a code of conduct can be used to mitigate MEV externalities.

We encourage EU supervisors to continue supporting industry-led efforts to mitigate MEV externalities. While we applaud ESMA's focus on technical rather than policy-based solutions for DeFi risks, we caution against mandating specific technological implementations at this stage.

Further explore automated reporting and embedded supervision of DeFi protocols
Public ledgers, such as blockchain networks, provide real-time transaction data that can be leveraged for regulatory monitoring. By tracking liquidity pools and other onchain activity, regulators can gain valuable insights into systemic risks, while supervision tools could assist in identifying suspicious activities that may otherwise go undetected.

There are several challenges in effectively monitoring DeFi markets and on-chain data alone is not sufficient to draw complete conclusions. Additional off-chain data is often needed, but blockchain transparency aids in the surveillance of offchain centralized exchange activity. The ability to identify wallets for inbound or outbound customer activity on centralized exchanges enables the monitoring of potential cross-market manipulation when used with exchange surveillance tools and investigations. The comprehensive consumption of customer-tagged, offchain exchange data from multiple exchanges provides a holistic view in detecting and mitigating cross-market and cross-exchange price manipulation, which is critical for market integrity and user trust.

Many surveillance tools that have been used successfully in traditional securities markets are also being leveraged to monitor offchain crypto exchanges, and in many cases more effectively given the need to surveil markets 24/7/365. A comprehensive monitoring and investigative suite should utilize both centralized exchange surveillance and blockchain analytics to secure user protection.

We support adopting a risk-based approach, focusing monitoring efforts on the largest DeFi protocols and liquidity pools to test the effectiveness of automated reporting. We also support industry efforts in standardising reference data on the blockchain to improve transparency, reducing reliance on complex and expensive off-chain data.

In addition to onchain data monitoring, we encourage the Commission to explore how to make compliance with existing regulatory obligations more efficient through the use of smart contracts. The latter can turbocharge 'RegTech' by making use of smart contract

functionality to help regulated entities comply with existing regulations. However, we emphasize that this should be strictly limited to already regulated entities under existing regulation - not to impose new obligations on otherwise unregulated persons.

Lending and borrowing

Crypto lending and borrowing offer users access to capital and passive income, whether through centralized or decentralized platforms. Centralized platforms provide greater control and support, while decentralized platforms use smart contracts for peer-to-peer or peer-to-pool transactions without a central authority. Both models can improve financial efficiency and inclusivity.

For centralized crypto lending platforms, several principles from MiCA, such as clear custody rules, consumer protection, cybersecurity standards, and transparency in operations, can and should be applied. These measures would ensure consumer protection and enhance trust in the platform.

Decentralized lending and borrowing protocols, however, are DeFi protocols that are non-custodial and permissionless by design. As the Commission has acknowledged, compliance can be achieved higher in the technology stack. The EU should ensure that DeFi protocols remain outside of the regulatory scope of MiCA (or MiFID). As mentioned above, this approach would be consistent with the approach taken by the US regarding custodial versus non custodial products. Interfaces that make it easier for users to interact with these decentralized protocols should be subject to disclosure obligations. However, merely providing software that facilitates a user engaging in self-directed crypto asset transactions that are executed on a blockchain protocol utilizing a self-custodial wallet does not make the non-custodial interface a provider of lending or borrowing services.

Common disclosure requirements can improve consumer protection
Transparency in the crypto lending and borrowing markets is essential to ensuring consumer protection.

For centralized platforms, clear and comprehensive disclosure requirements are critical to helping users understand the risks, terms, and potential outcomes, including possible losses or liquidation. By mandating transparency, consumers can make well-informed decisions when participating in these markets.

To better protect consumers, we believe that common disclosure requirements should be established across crypto lending and borrowing services. These services must provide clear and consistent information on key areas. Users should be informed about all pricing and fees, including any service charges or penalties that may apply. Additionally, transparent disclosure of interest rates, rewards, and yield calculations is necessary to enable users to assess the potential returns or costs of their participation.

Moreover, platforms should be required to disclose the conditions under which additional collateral may be requested, as well as the risks of liquidation if these requirements are not met. Consumers must also be made aware of how their collateral is managed, including whether it can be rehypothecated, staked, or pooled. In particular, users need clear information about the risks involved in the event of disputes or platform insolvency.

For decentralized lending and borrowing protocols, non-custodial user interfaces that merely provide software that facilitates a user engaging in self-directed crypto asset transactions that are executed on a blockchain protocol utilizing a self-custodial wallet should not be subject to disclosure obligations imposed on financial intermediaries. Instead, any obligations should be commensurate with their nature as a software provider. They should give users clear and consistent information on key areas, based on information that is publicly available for the underlying lending or borrowing protocol.

Establish prudential requirements for centralised crypto lenders

Centralized crypto lenders must maintain adequate liquidity reserves to meet customer demands, particularly during times of financial stress or market downturns. Platforms should be required to hold sufficient reserves that can be quickly accessed in cases of liquidation, insolvency, or other unforeseen circumstances. These requirements should mirror the capital adequacy standards imposed on traditional financial institutions, ensuring that crypto lenders are well-equipped to withstand market fluctuations and continue fulfilling their obligations to customers. Such measures will protect consumers from unexpected platform disruptions and provide stability to the broader crypto lending ecosystem.

Decentralised lending and borrowing protocols are non-custodial and therefore any prudential and custody-related obligations should not apply to them.

Safeguarding and cybersecurity standards

Centralized crypto lending platforms that custody customer assets should be held to high standards for cybersecurity practices to protect user funds from fraud, theft, or unauthorized access. Platforms should implement secure storage of assets, conduct regular audits, and have comprehensive protections against cyberattacks and other malicious activities. Clear and transparent disclosures should be required from centralized platforms regarding their custody practices, including whether customer funds are segregated from the platform's own capital and what measures are taken to ensure the safety of these funds.

For decentralised lending and borrowing protocols, we refer to the section on smart contract auditing and certification above.

Staking

Staking is a critical technology that ensures the accurate, secure, and efficient operation of many blockchains. At its most basic level, staking is the process by which users can contribute to the network by securing the blockchain, creating blocks, and processing fees and consensus rewards by the protocol itself. Aside from Bitcoin, most major blockchains today leverage a proof-of-stake model because it is open, secure, and environmentally friendly.

Staking should not be confused with lending

There has been some misuse of the term staking in the market to describe what is in reality lending activity. In a lending transaction, one party gives up ownership of an asset to another party, who promises to return the asset at a later date, usually with interest. The lender puts those assets at risk for the duration of the loan. In contrast, stakers do not relinquish ownership of the assets staked. Instead, they temporarily lock-up these assets by staking them, but always retain the right to un-stake their assets, and always remain the owner of those assets. There is no investment or counterparty risk associated with staking.

Staking does not pose financial risk

There is no investment of money in staking and staked assets do not leave the protocol. Nor are consumers subject to any counterparty risk from staking, since they retain ownership of their staked assets at all times. While network penalties (i.e., slashing) are possible (if the validator behaves maliciously or otherwise violates protocol rules), they are extremely rare. Less than .001% of all staked ETH has been lost to slashing since its inception. In many cases, firms' user agreements typically indemnify the consumer with respect to the loss of assets due to slashing that arise as a result of the service provider's error.

Custodial staking should be regulated as part of custody services

In custodial staking models, a staker never relinquishes ownership or control of the staked assets. They have the same rights and limitations as if they were solo staking at home, and they receive the same protocol rewards and experience the same protocol lockups. This is simple custodial staking, just with the assets held in custody and the instructions to stake being given to the custodian to effect on behalf of the customer. When the client makes an instruction to stake, the firm will directly effect the instruction on their behalf. Assets are not staked without a client instruction, and every instruction results in corresponding activity on the blockchain.

We welcome ESMA's clarification that the provision of custodial staking services is ancillary to custody services and hence any provider of staking services must be authorized under MiCA to offer custody and administration of crypto-assets on behalf of clients.

Stablecoins

Stablecoins have made significant progress at the technological and infrastructure levels, enabling efficient cross-border transactions. MiCA's regulation has played a key role in building trust by providing stability and clear requirements for issuers. However, further work is needed to ensure global interoperability and widespread adoption, as the market continues to evolve and integrate with global financial systems.

Multi-issuance model of global EMTs should be preserved
The multi-issuance model for global E-Money Tokens (EMTs) eliminates friction by allowing the same EMT to be issued and used seamlessly across different jurisdictions, without requiring conversion into another token or currency. This is because the same token can be recognized and accepted globally, regardless of local regulations or reserve requirements. Therefore interchangeability promotes a more efficient, global financial system, enhancing liquidity and reducing regulatory complexities.

Eliminating the multi-issuance model would hinder cross-border payments, would harm EU CASPs and their customers by reducing liquidity and trading options without access to US dollar-denominated stablecoins. These stablecoins offer deep liquidity, and their absence would limit pairing options for euro-denominated stablecoins, resulting in higher costs and slower transactions.

Under MiCA, technical standards will be implemented for reporting obligations related to the volumes of EMTs. This means that EMT issuers will receive data from CASPs about the total number of tokens held by CASPs and their EU-based customers. This information helps EMT issuers accurately assess their reserve requirements in the EU. Specifically, if the issuer markets the same fungible EMT outside the EU, they will need to ensure that their reserves in the EU are sufficient to cover their liability towards EU token holders, based on the proportion of the total EMT supply circulating in the EU market. This ensures that issuers maintain adequate reserves in line with the amount of tokens held and transacted within the EU, creating a balanced and secure system for cross-border operations.

Any review of MiCA should make the EU an even more attractive and competitive market for globally operating issuers. We strongly support the introduction of an equivalence regime for EMTs in a future MiCA 2.0 proposal, ensuring the smooth interchangeability of global EMTs across jurisdictions. This approach would not only benefit global issuers but also enable EU-based EMT issuers to scale and expand internationally. Given the inherently global nature of crypto-assets, the EU must embrace policies that promote cross-border integration, ensuring it remains connected to the broader global markets and liquidity.

Prohibition of interest on MiCAR stablecoins should be removed
Interest-bearing stablecoins provide consumers with additional incentives to hold and use stablecoins, making them more attractive as a store of value. Allowing interest could also increase liquidity and offer consumers better returns on their assets in the digital economy.

Prohibiting interest on stablecoins denies an important benefit to consumers and will stifle the growth of DeFi applications because earning interest is a key feature that attracts users to DeFi platforms. Many DeFi applications, such as lending and borrowing protocols, rely on users earning interest on their assets, including stablecoins. Without the ability to earn interest, stablecoins lose one of their main value propositions, reducing user participation and limiting the development of innovative DeFi services.

Given these potential consequences, the European Commission should consider conducting a new impact assessment of the potential removal of the ban on interest-bearing stablecoins. This assessment should examine the implications for financial stability, the development of DeFi lending and borrowing markets, and the competitive dynamics between stablecoins and interest-bearing tokenised deposits.

Conclusion

As the crypto industry matures, global cooperation is crucial, especially as the true potential of crypto is amplified in its ability to operate across borders. It is crucial for the EU to catch up with the evolving regulatory landscape, in particular in the US, which is fast developing a sophisticated regulatory framework on traditional financial markets and crypto markets, including DeFi. The EU should keep a close eye on those developments, in particular those relating to tokenized equities and non-custodial infrastructure. The EU should also focus on the review and further development of IOSCO DeFi recommendations and subsequently align a future MiCA framework with it. This will ensure the EU fosters DeFi growth while maintaining consistency with global efforts to regulate the sector, helping the EU stay integrated in the evolving global crypto market.

To ensure continued growth and innovation in the crypto space, it is essential for the EU to support open and global markets for stablecoins. A multi-issuance model for global EMTs eliminates friction by allowing the same EMT to be issued and used seamlessly across different jurisdictions. This approach not only benefits global issuers but also allows EU-based EMT issuers to scale and expand internationally. Given the inherently global nature of crypto-assets, the EU must adopt policies that foster cross-border integration, ensuring it remains connected to the broader global markets and liquidity while encouraging competition and innovation.