afme/
Finance for Europe

Association for Financial Markets in Europe

Response to ACPR Discussion Paper:

“Decentralised” or “disintermediated” finance: what regulatory response?

May 19th, 2023

Executive Summary

In April 2023 we welcomed the European Parliament formally adopting the **Markets in Crypto Assets Regulation (MiCA).** As MiCA moves to level 2 and 3 measures, including the European Commission’s planned review of Decentralised Finance (DeFi), we welcome efforts by the ACPR and other National Authorities to continue to contribute to further analysis of DeFi by authorities, and its impact on the financial services industry. Our response to the discussion paper sets out the views of capital markets participants on the importance of regulating DeFi where it intersects with regulated financial markets activities.

We believe that this is a crucial moment for the financial services industry and EU regulators as any potential exclusion of so-called “decentralised activities” would cause a gap in the application of MiCA. This exclusion could create unintended risks to financial stability and potential knock-on impacts. While as noted by the Financial Stability Board (FSB)[1] the current overlap of DeFi and Traditional Finance (TradFi) is not yet significant, this should be actively monitored and managed.

An appropriate regulatory perimeter across Europe is essential, as well as a proportionate and risk-based approach that provides clear perimeter guard-rails but also space for innovation to thrive. AFME believes that this will support the development of a robust digital economy.

AFME is supportive of the development of a thriving digital economy within a clear legal and regulatory framework and hopes our response to this discussion paper will encourage further analysis and consideration of these foundational principles as the EU continues its work on decentralised finance and the governance of digital assets more broadly.

Part 1: DeFi: definition, use cases and schematic structure

Q1: Do you have any comments on the definition of DeFi used in the paper? Does the document correctly reflect the real level of decentralisation of services?

AFME believes that the ACPR’s efforts to work towards these classifications and definitions are welcome and we support the principles put forward. We would note though that to define DeFi as “a set of crypto-asset services, which are similar to financial services and carried out without the intervention of an intermediary” (Pg. 7 of the consultation) is quite a narrow definition of what could be encompassed by the term DeFi. We would encourage regulators to instead focus on the extent of decentralisation, and providing, where possible, clarity for networks with knowable participants (private blockchains) where rules can be enforced, and individuals held accountable.

We agree with the ACPR that there are three main layers that make up DeFi, and while they are in principle the same as those set out in the discussion paper, we would characterise them as follows[2]:

- **Settlement layer (the Infrastructure Layer in the ACPR Consult)**: manages the ledgers by recording changes to the state of the blockchain (e.g. payments) and sets incentives for validators and miners to maintain the chain (e.g. process transactions). It is the core protocols within a distributed ledger infrastructure (e.g. Ethereum). This layer is also responsible for the network’s fundamental operations including the consensus mechanism, dispute resolution, and other technical enablers.

[1] https://www.fsb.org/wp-content/uploads/P160223.pdf

[2] https://finance.ec.europa.eu/system/files/2022-10/finance-events-221021-report_en.pdf

- **Token layer (the Application Layer in the ACPR Consult):** is where crypto-assets are created. This includes non-fungible and fungible tokens like stablecoins, governance tokens, etc. Protocols are built on top of the settlement to extend functionality, typically with regard to privacy, permissioning and performance requirements. The token layer protocols often use processing elements that run outside of the core chain to enhance scalability (e.g. zero-knowledge roll-ups) and cost inefficiencies (e.g. transaction costs) of the settlement layer protocol.
- **Application layer (the User Layer in the ACPR Consult)**: the broad application layer interacts with the underlying network to provide interoperable, functional utility to end-users, including decentralised exchanges, liquidity provisioning, and liquid staking applications. It is where most DeFi protocols are integrated as they rely on both settlement and token layers to execute their associated smart contracts. This layer also may contain applications for services such as credit, decentralised exchange, asset management and derivatives.

In addition to this we would note that as DeFi evolves and potentially new activities are created, these characterisations may need to be updated over time. However, we would still encourage that the ACPR work with European Authorities as well as global standard setters to agree common global definitions for DeFi and how it is characterised. We believe that this will contribute to a more comprehensive regulatory framework both in the EU and globally.

We also believe that the discussion paper does correctly reflect the real level of decentralisation and would agree in particular that many DeFi projects may be mixed or vary over time. We would also suggest however that there are three generally accepted classifications of decentralisation each of which leads to different risks and controls being required:

Type 1 - Smart contracts which are DINO (Decentralised In Name Only) however are still centralised by design. These contracts can be fully upgraded by individuals, multi-signature wallets or multi-party computation (MPC) smart wallet approvals. The person or people who control the private keys are responsible for the actions of the code and can change the beneficial owner used as the output of the contract.

Type 2a - Smart contracts with either a Decentralised Autonomous Organisations (DAO) where voting occurs off chain and the instructions are passed to a Type 1 individual or group who then upgrade the contract or where there is a DAO with majority voting power in the hands of a small number of key individuals. This is essentially a Type 1 level of decentralisation with an additional layer of abstraction as off chain instructions could be ignored by the key holder (no direct effect) and DAO's where the majority of voting rights are held by a small subset of individuals are also similar to Type 1.

Type 2b - Smart contracts with on chain voting by a large number of truly decentralised and anonymous DAO participants. As no upgrades can be made effective without the upgrade being publicly known first through the voting proposal, this is similar to a Type 3 in terms of level of decentralisation.

Type 3 - Smart contracts where the contract isn't upgradable in any way and/or there is no longer a central organisation running it (the number of these will increase as the space matures given the immutability of the blockchain) and/or the private keys for upgrading a contract have been lost.

So in practice and depending on the classification set out above, one could measure "decentralisation" for a DAO by looking at the percentage of ownership of the governance tokens by a wallet or a set of wallets owned by a single party. Or, if that is not possible, one could also look at the liquidity concentration (e.g. measured by density of unique wallets providing liquidity). However, this could be challenging without the verification of ID to prove that it is unique.

Overall, we agree with the definitions set out by the ACPR but would note that those, as well as ours above, are initial categorisations and would need to be accompanied by the appropriate governance and internal controls depending on which type of decentralisation was being employed.

Q2: In your opinion, which use cases of DeFi are likely to develop in the future? Can they serve the real economy ?

First, we would note that this is still relatively unknown, but AFME believes that DeFi that operates within a regulatory perimeter is likely to scale to successful future use cases and achieve broader adoption.

Second, we would note that banks act as a key transmission mechanism for economic and monetary policy and efficiently allocate capital through their borrowing, lending, structuring investment opportunities, providing investment advice and acting as liquidity providers in markets. All these actions will continue and the use of smart contracts to create effective permissions on public permissionless DLT networks (i.e. with appropriate Know Your Customer (KYC)/Anti Money Laundering (AML) mitigations) will create opportunities to increase efficiencies and decrease cross border transactional friction through the application of common global standards. This is similar to how the internet improved for the transfer of information. If used in a responsible manner (i.e. known identity and permissioning of access) blockchain based solutions can also offer improved trust, security, transparency and traceability over alternative legacy methods.
Current DeFi efforts can be seen as outsourced innovation and research and development (R&D) labs for the formal financial system. DeFi efforts can build and test new primitives (e.g. borrowing, lending, trading and investing using different token formats, smart contracts and encryption approaches) on these common standards. While the initial focus has been on DeFi payments, as that has the current highest level activity, we believe the impact real economy will be driven through the impact of these new DeFi like approaches on the processes of borrowing, lending, investing, market making and transferring tokenized assets without the need for counterparty and settlement risk. Real economy tokenized asset types (e.g. property assets, goods and services, collectibles, gaming, metaverse assets, brands, IP) in the future could be lent against, invested in, traded or have conditionality coded into transfer contracts could potentially include:

<u>Tangible Real World Assets on Chain (E.g. investible assets, goods and services)</u>

AFME primarily represents a broad array of pan-EU global and regional banks. As such, the below examples are not necessarily use cases that AFME members would engage in, however we would provide the below views for regulatory consideration based on industry observations potential use cases for DeFi.

Secured deposit tokens backed by Central Bank Digital Currencies (CBDC), HQLA tokenized bonds and tokenized ABS (similar to a vertical slice of the capital structure of a bank) could utilise same blockchain to transfer underlying assets (like mortgages) without credit risk between deposit tokens when a new improved rate is offered based on the metadata the borrower has decided to expose creating a new financial market where previously there was only a bilateral relationship due to the manual nature of transfers.

The settlement of home purchase chains could be coded into a smart contract that transfers the record of ownership removing settlement risk and providing certainty to homeowners as banks involved in lending attest to their willingness to lend prior to the settlement date using cryptography increasing the efficiency of bank's mortgage departments.

Real world assets provided by a custodian or central administrator require regulatory bridges so will probably take the longest but will also have the largest impact. Tokenized investible assets on common cross institution standards could materially reduce the settlement costs when compared to the existing system, in turn reducing costs for end users.

Real world assets linked to a digital token can provide a better experience to consumers in some situations. For example:

- QR code based tickets to sporting events can be replaced by NFTs removing the risk of turning up to an event and finding it has already been used because someone has resold the ticket multiple times (Ticketmaster released token gated event sales in March 2023). This can reduce the risk of purchase disputes over payments.

- NFTs linked to Near-field communication (NFC) tags can prove physical items of clothing are genuine, in a way that holographic stickers are unable to, reducing the market for fake versions of trademarked goods. (Nike subsidiary RTFKT[3] have released multiple NFT linked apparel goods in 2023). The existence of these NFC tags offers opportunities for traceability in supply chain financing.

- Individuals with flexible travel plans could resell a Digital Asset representing a future night in a hotel room peer to peer in the event someone urgently needing to travel is willing to offer them a premium (offers can be made direct to their wallet in a way that is not possible bilaterally today with zk proofs limiting the information shared publicly).

Intangible Real World Assets Represented on Chain (E.g. brands and IP)

There are high levels of friction in IP (Intellectual Property) rights and royalty transactions. The world's largest online royalty marketplace (Royalty Exchange) has only traded 135m USD to date[4] while estimates based on listed US stocks show up to 90%[5] of their value could be attributed to intangible assets. Loyalty point schemes to reward brand loyalty can be created in seconds using open source software on the blockchain (e.g. Starbucks Odyssey released NFTs in 2023[6]). Crowdfunding artists/musicians can raise funds while at the same time use tokens on the blockchain to create token gated online platforms for their fan community in Discord (192m active monthly users[7]). Tokenization using common standards and cryptographic proof of ownership transfer has the potential to create a genuine global marketplace for intangible assets which existing financial primitives can be applied to.

On Chain Only Assets (E.g. collectibles, gaming and metaverse assets)

The gaming industry market size is approximately 250bn USD in 2023[8]. The recent metaverse report from Citi (Money, Tokens and Games – March 2023[9]) highlights that of the existing 3bn gamers globally there could be as many as 50-100m accessing games through Web 3 games (which would require digital assets/wallets) by 2025. The winner of the recent Dookey Dash game by Yuga Labs sold the Digital Asset they received for first place on a blockchain marketplace for 1.6m USD[10] while other players hired professional gamers[11] on a pay-per-result basis in order to get a higher leaderboard position. A recent report by UBS (Metaverse – April 2023[12]) also highlighted the potential for advertising, "in person" virtual music events (for example Travis Scott's Fortnite

[3] https://rtfkt.com/
[4] Royalty Exchange: Buy & Sell Music Rights & Copyrights
[5] WIPO and Intangible Asset Finance
[6] The Starbucks Odyssey Begins
[7] How Many People Use Discord? (Discord Statistics 2023) (thesmallbusinessblog.net)
[8] Gaming Is the Next Super Platform | Accenture
[9] https://ir.citi.com/gps/MG9DEWhoYvQJVWLM9Kr3%2BZmqjoztKJcyNHr83F9Wug2pzAGHPQKfp23RAMrkNts%2FJitXoTNqufOvegUjjXh0IA%3D%3D
[10] Ethereum Transaction Hash (Txhash) Details | Etherscan
[11] The Block: Bored Ape NFT game attracts pros angling for a piece of the Dookey
[12] file:///C:/Users/Elise.Soucie.AFME/Downloads/Longer%20Term%20Investments_en_1588445.pdf

concert had over 12m[13] concurrent viewers generating millions in sales) and interoperable avatars within metaverse games to take an increasing chunk of the 2tn USD global media and entertainment industry revenues.

Q3: What do you think about the concentration phenomena described in section 1-5 of this document?

AFME agrees that there are concentration problem as set out in section 1-5 of the document. Furthermore, this phenomenon could be exacerbated by the fact that Smart contract code is publicly viewable and easy to duplicate.

AFME agrees that there are currently are a few dozen protocols that concentrate the bulk of funds and users, these may continue to be duplicated and used across the market creating even higher levels of concentration as time goes on.

The concentration problem is also often reinforced for public blockchains as there is often a 'winner takes all' market since they profit from a virtuous cycle where they see their security increase with an increase in users (and thus validators), which in turns continues to attract more users, and so on and so forth.

However, despite the problems noted in the discussion paper, we would encourage regulators to take a technology neutral approach and continue to do further analysis of concentration as the market continues to develop. As further level 2 solutions are created, and as the market (and regulatory frameworks) continue to evolve, more participants may engage in DeFi, which could result in more diverse solutions and lower levels of concentration.

Q4: Do you have any comments on or information to add to the schematic presentation of DeFi presented in section 1-6?

AFME believes that this is broadly in line with our characterisation set out under Q1 and are supportive of the schematic set out by the ACPR.

Part 2: The risks associated with DeFi

Q5: Do you have any comments on the description (provided in section 2-1 of this document) as regards risks related to decentralised governance?

AFME agrees with the risks set out by the ACPR in section 2-1.

An additional point that we would highlight with regards to decentralised governance is the tension that can be seen in some DeFi categories such as Decentralised Insurance Protocols between token holders and users. In this example, while the former is often asked to share views, appraise and vote on whether the claim is legitimate and users should thus be reimbursed, they have no interest in doing so since this would decrease the protocol's assets and thus the token's value. We would encourage the ACPR to also take this risk into consideration.

[13] More than 12m players watch Travis Scott concert in Fortnite | Fortnite | The Guardian

Q6: Do you think that layer 1 solutions can exacerbate the security issues of the blockchain infrastructure? What about layer 2 solutions? In your opinion, are there significant differences in this respect between the layer 2 solutions considered?

As section 2-2-1 accurately highlights, all blockchains face a balancing choice between 'decentralisation, security and scalability'. Using the largest smart contract blockchain Ethereum as an example, the solution proposed for using layer 2 solutions like optimistic rollups and zero-knowledge rollups will certainly increase their scalability but, due to increased centralisation arising from their use, will require careful monitoring of the implementation of the new technology. For examples of these risks, we can look at the recent history of bridge attacks that have been reported. As per the response to Q14 section 5 the exact level of monitoring will be a function of the type of bridge interaction between the layer 1 and layer 2 chains as well as recognising that even within the categories there are sub categories with different cost benefits (e.g. zk-SNARKs and zk-STARKS are zero-knowledge proof technologies that allow one party to prove to another that a statement is true without revealing any further information enabling new products which were not possible before). Some bridges which require at least one honest watcher (i.e. centralisation) may need to introduce economic incentives to ensure there is always one incentivised to invest the time and resources required as the size of the value at risk on the L2 chain increases over time. Given the speed of development there may also be further future innovations that have the potential to improve the crypto economic security of other layers (e.g. Eigenlayer restaking i.e. enables staked Ethereum to be used as crypto economic security for blockchain protocols other than Ethereum, in exchange for additional fees and rewards potentially allowing faster bootstrapping of new blockchains). However, we would note that in each case, the security issues that arise will also vary and be dependent on the type of architecture.

Q7: Do you think that the use of rollups or similar solutions will result in less transparency of information for an observer?

Not necessarily, this will still be dependent on the architecture as noted in response to Q6 above. If the Layer 2 rollup approaches are based on public networks and reputable organisations are storing offline copies of the on chain information, then there should be the same amount of transparency. However, each particular type of implementation should be reviewed on its merits and different jurisdictions may wish to maintain their own independent record of transactions. For some innovations which generate blockchain records that are only maintained temporarily (e.g. data blobs) then the method of access to this data in the long term should also be considered (i.e. store the 'working out' and not just the final 'answer').

Q8: Do you have any comments on the description (provided in section 2-3) of the risks related to the application layer of DeFi?

AFME agrees with the risks and description provided in section 2-3. Please also refer to our response to Q14.

Q9: Do you have any comments on the identification of DeFi risks for retail customers (section 2-4-1)?

AFME primarily represents a broad array of pan-EU global and regional banks. As AFME is a capital markets association – our DeFi research has been focused on the risks for wholesale markets and as such is not best placed to comment on this question.

Q10: Do you have any comments or additions to make to the description (provided in section 2-4-2) of the systemic vulnerabilities of the DeFi ecosystem (endogeneity of investments, significant leverage effects, role of automated position liquidation mechanisms)?

We would also note that it may be beneficial to call out the risk management benefits of real-time deterministic liquidation models.

Furthermore, as noted in our response to Q5 we believe it is also important to consider and address wrong way risks in the DeFi space. DeFi's transparency is counterproductive in a liquidation environment, since it can lead to whale hunting (i.e. trying to liquidate a user on purpose). This can also create a negative feedback loop in which everyone wants to leave the system first when there is market instability, which then results in even further instability and market turmoil.

Q11: Do you agree with the proposal concerning the regulation of stablecoins issued by DeFi protocols? (Refer to section 2-4-3: "if a decentralised service claims to create or use a crypto-asset with an official currency as a reference, this crypto-asset must be an EMT within the meaning of MiCA or an equivalent asset)

☒Yes

☐No

Why?

AFME is supportive of this approach and supportive of this further development of the MiCA framework to avoid any unintended gaps. AFME also supports algorithmic stablecoins having the same regulatory treatment as any unbacked cryptoassets.

Q12: Do you have any comments on the description of the potential AML/CFT risks of DeFi (section 2-4-4)?

While AFME agrees with the risks set out by the ACPR, we would still encourage a technology neutral approach to Defi. We would encourage the ACPR and other authorities to consider what new and novel risks are presented by DeFi that may go beyond what is already addressed under existing AML provisions.

For example, we would note for consideration precedent set by a 'tumbler' used for money laundering purposes (Tornado Cash). This was a smart contract with no 'home' jurisdiction. The US authorities could not close it down, so they put the onus on users. It was placed on the OFAC (Office of Foreign Asset Control) sanctions banned list. Usually, this list is reserved for nation states (N Korea, Russia, Iran, etc.) or private individuals. This was used on code (smart contract) for the first time. There are further implications to this lack of 'home' jurisdiction for the smart contract that we would also recommend the ACPR consider as they conduct further analysis.

Q13: In your opinion, are there any other risks that should be taken into account which are not mentioned (or not given sufficient attention) in the document?

AFME agrees with the risks set out by the ACPR. We would also add the following unique challenges presented by DeFi for the ACPR's consideration:

1. *The 'Counterparty' is a smart contract that is executed on all decentralised nodes with no 'home' jurisdiction or 'home' regulator*

- When executing a DeFi trade the trade is executed by the trader's wallet against a smart contract (and not against another trader). In a decentralised public chain with nodes distributed globally this means that the counterparty (a smart contract not a natural person or regulated entity) doesn't have a single physical 'home' location so the only participant in the transaction with a physical location is the end user. The 'middleman' or exchange based smart contract is not regulated.

- One can consider the precedent set by a 'tumbler' used for money laundering purposes (Tornado Cash). This was a smart contract with no 'home' jurisdiction. The US authorities could not close it down, so they put the onus on users. It was placed on the OFAC (Office of Foreign Asset Control) sanctions banned list. Usually, this list is reserved for nation states (N Korea, Russa, Iran etc) or private individuals. This was used on code (smart contract) for the first time. There are further implications to this lack of 'home' jurisdiction for the smart contract.

2. A smart contract will continue to exist even if initial uploading organisation disbands

- When executing a DeFi trade the contract is normally accessed through a front-end web page. This is just a visual interface used for interacting directly with the blockchain in a convenient way. Technically adept individuals can instead interact directly with the smart contract on the blockchain without going through the 'official' web page or indeed other 'non-official' web pages built by third parties to interact with the same smart contract for the same effect.

- Given that smart contracts uploaded to the blockchain are permanent this means that even if the contract is uploaded by an organisation (either a DAO or centralised team) it will continue to exist in use even if the initial team disbands for any reason.

3. Smart contracts can be used by other smart contracts in ways the original creator didn't intend

- Unless restrictions are hardcoded (which as per point 3 these can be removed by copying then editing) it's possible that software built for one purpose on chain can be reused for another purpose different to the original intent when originally uploaded.

- Although not specifically DeFi related, a good example of this is the case where NFT trading platform OpenSea banned smart contracts that used allowed trading of their tokens on its competitor platform Blur from receiving full functionality on their exchange (using a blacklisting of Blur contract addresses[14]). Blur then split its settlement contract for trades on its exchange where the tokens were part of the blacklist. The new settlement flow used the settlement contract of OpenSea itself for its back end infrastructure (same front end Blur website) meaning OpenSea wasn't able to enforce the block as it would involve blocking its own contract from being able to settle the tokens too. In addition, aggregator platforms like 1inch[15] use multiple underlying decentralised exchanges like Uniswap and Sushiswap without needing to ask for permission to use them.

[14] https://www.coindesk.com/web3/2023/02/15/blur-escalates-royalty-battle-with-opensea-recommends-blocking-platform/

[15] https://1inch.io/aggregation-protocol/sushiswap/

- The current state analogy would be someone copying access to the NYSE or LSE and having it run in a different country X without needing the permission of LSE. This is what happens when the exchange is code (i.e. a decentralised smart contract).

- Given the fact that (a) the node operators are decentralised and have no single location, (b) the team that deployed the contract may no longer exist or be known, (c) the effect of the contract is visible to any user and (d) that the contract deployer has no control over other parties choosing to use it this leads to the following outcome: the most centralised point in the chain is the end user and the business offering the web based interface to them in order to generate profit from a service. This may be an avenue for regulators to apply regulations in an otherwise decentralised space.

Part 3: Avenues for a regulatory framework

Section 3-1: Ensuring a minimum level of security with respect to infrastructure

Q14: Should public blockchains be governed by a framework or by minimum security standards (refer to section 3-1, regulatory scenario A)?

☐Yes

☒No

If so, how? If not, why?

No, while AFME is supportive of improved governance in DeFi activities we believe it may be difficult for a public blockchain to be included within a regulatory perimeter at this point in time. Furthermore, it may create unintended financial stability risks.
AFME primarily represents a broad array of pan-EU global and regional banks. As such, AFME members are not using DeFi structures, however we would provide the below views for regulatory consideration based on industry observations of how these now structures function.

We would recommend that the risks related to businesses which interact with smart contracts should be reviewed for each smart contract interaction in terms of: Smart contract type / Economic / Oracle / Governance / Bridge. The risks are cumulative in nature when working out the total risk. AFME has set out considerations for these risks under the below categories:

1. Smart Contracts:
- Level of audit and quality of smart contract audit firm.
- Time stamp record of the snapshot of the codebase reviewed (in case of upgrades which introduce new vulnerabilities).
- Enhanced monitoring shortly after contracts are upgraded (including potentially reduced usage and liquidity requirements).

2. Governance:
- Type of governance. I.e. is it an External Owned Account (EOA), a multi sig or an on-chain DAO. (Recommend against single EOA as too vulnerable).
- Level of distribution of multi sigs (I.e. across different organisations and tech platforms).
- Level of DAO engagement (to avoid malicious proposals passing unexpectedly).
- All smart contract upgrades should have a time lock giving users time to evaluate between submission and execution.
- Monitoring of proposals submitted (to risk model potential impacts).

3. Economic:

- Evaluation of all tokens (Fungible Tokens and Non-Fungible Tokens) used in protocol for both liquidity and fees.

4. Oracle:
- Confirmation if it is on chain oracle (review of details of how the data feeds are aggregated (e.g. for prices does it include a TWAP (Time Weighted Average Price))) or if it is an off-chain oracle (review of risks related to the specific oracle such as chainlink number of nodes etc.).

5. Bridge:
- Type of bridge:
• Natively verified (most secure) – full nodes on each chain verify the transfer.
• Locally verified – only the counterparties verify the transfer.
• Optimistically verified – assume at least one honest operator will challenge the transaction due to economic self-interest.
• Externally verified (least secure) – relies on external verifiers who need to be trusted. We would also conclude by suggesting the following three best practices for DeFi structures:
(1) That a smart contract be audited by an authorised smart contract auditor,
(2) That the degree of decentralisation established and verified when material changes in ownership happens, and
(3) That assets on which DeFi protocol is being applied are also important to determine the risk (e.g. using a smart contract for a traditional financial services derivative).

Q15: Should public authorities supervise the concentration level of validation capacities on public blockchains? If so, through what kind of measures?

☒Supervising concentration in real time

☐Setting caps on concentration

☒Publicly disclosing when specific concentration thresholds are exceeded

☒Taking further action (specify how)

Yes, authorities should monitor concertation risk of validation provision on public chains. If we imagine a future where public chains are being used as infrastructure for permissioned applications on top of them and used by the formal financial system, this is a key risk. For decentralised chains, monitoring concentration in real time and publicly disclosing when thresholds are crossed would be useful in assisting financial organisations with assessing the risks of the different chains to certain kinds of attack mentioned in section 2-2-2. Setting caps on concentration in a truly decentralised chain appears to be impractical but in less decentralised chains may have benefit. We should note the cross over benefit of these approaches to Cyber Risk and Operational Resilience regulations in the wider economy (e.g. the EU Digital Operational Resilience Act - DORA).

However, we would caveat this by noting that technically this may be quite difficult. Currently for most DeFi activities, pseudonymity does not allow for "sybil proofness". In order to have accurate supervision and disclosure KYC would be required for all validators (which is currently not how most DeFi protocols are operationalised).

Q16: Do you agree with the analysis provided in the paper on the merits and limitations of private blockchains (section 3-1, regulatory scenario B)? Should private blockchains operated by private operators be regulated through a supervisory framework, if at all?

☒Yes

☐No

Why?

While we agree that there are both merits and limitations of private blockchains, AFME members do not believe that private blockchains should be mandated for all financial activities. There are many examples of responsible uses of public blockchains or hybrid approaches using a combination of private and public chains such as in the case of the European Investment Bank (EIB) Digital Bond Issuances.[16]

In line with a technology neutral approach, AFME would support private blockchains being regulated in a similar manner to other new technologies implemented by regulated financial institutions. If the technology is implemented it is important that it demonstrates it is meeting the appropriate regulatory outcomes in line with the principle of 'same activity, same risk, same regulatory outcome'.

We would encourage regulators to focus their efforts on private blockchains at the present time and current uses within regulated financial services, while still allowing for innovation and further developments for responsible use of public chains in the future.

Q17: Should public players directly manage the blockchains that provide the infrastructure for DeFi operations?

☐Yes

☒No

Why?

No, per the summary section of the document: of the two proposed solutions the organisational arrangement of public blockchains with "certified" security layer on top e.g. standards (certification of computer code, minimum number of validators, cap on validation capacity concentration as well as applicable 'permissioned' KYC/AML mitigations) would be most similar to how we use the internet today. AFME would support licensed operators managing the blockchains. For example, with the internet today the current public permissionless setup of the internet base layer is augmented with specific security standards being applied to existing traditional finance transactions occurring over the internet architecture. The current setup of the internet has shown itself to be safe for finance organisations while also allowing a large amount of innovation over the last few decades, which no one could have originally predicted, that has been beneficial for the economy.

Q18: Do you have any other regulatory proposals to make with a view to ensuring a minimum level of security for the blockchain infrastructure?

☒Yes

☐No

If so, what are they?

Yes, please see our response above to Q14.

Section 3-2: Providing a suitable oversight framework in view of the algorithmic nature of services

Q19: Is a certification mechanism an effective solution to determine the scope of "safe" smart contracts (for a given state of knowledge)? Would alternative solutions achieve the same result?

Yes, AFME believes that this would be effective and that accountability is key. This is already being done today by some smart contract audit firms and is progressing in a positive way. With regulatory certification mechanisms this could be an effective solution.

Q20: Do you agree with the description (provided in section 3-2-1) of the various techniques offered to audit the computer code of smart contracts, including with their respective strengths and limitations?

[16] https://www.eib.org/en/press/all/2023-030-eib-issues-its-first-ever-digital-bond-in-british-pounds

Yes, we agree with the description set out by the ACPR.

Q21: Can you identify examples of smart contracts that should not be certifiable due to the nature of the services they provide?

☐Yes

☒No

If so, which ones?

AFME members do not at this time have views on specific examples.

Q22: What do you think of the rules put forward in this paper (section 3-2-2, item a) on how to certify smart contracts (pre-certification of called components, certification life cycle)?

Yes, we agree with the rules put forward as a proposal for certification.

Q23: Should smart contracts embed a number of regulatory requirements in their code in the future?

☒Yes

☐No

Why?

Yes, we are supportive of this to the extent that it is possible as it could help reduce the cost of compliance and also support consistent application of regulatory requirements.

Q24: Who should set the security standards for smart contracts (refer to section 3-2-2, item b) and why?

Given the difficulties of regulating public blockchains, we believe that for private blockchains, the selected participants themselves should set the security standards they would like to use and would then be responsible for ensuring that those standards meet the appropriate regulatory outcomes.

Q25: Should interaction with uncertified smart contracts be discouraged or prohibited (refer to section 3-2-2, item c)?

☒Discouraged

☐Prohibited

☐Neither discouraged nor prohibited

Why?

Discouraged, but we would also support having a regulatory sandbox where uncertified contracts could be tested in order to support innovation.

Q26: Who should bear the certification costs of smart contracts (refer to section 3-2-2, item b) and why?

We agree with the arguments set out in the consultation for having developers or managers of the relevant programs bear the costs.

Q27: Do you have any comments on the description made of the risks inherent in the decentralised oracle model? Can these risks be mitigated using a certification mechanism tailored to the specifics of these applications (refer to section 3-2-3)? Do you have any comments or alternative proposals for a framework governing the activities of oracles?

AFME fully agrees with the statement on pages 36-37 of the ACPR paper stating, "It could therefore be argued that the regulatory model of traditional finance is not suited to the specific risks faced by DeFi. This would support the establishment of a framework dedicated to the supervision of (centralised or decentralised) data providers by public authorities."

We would encourage this type of framework be given further consideration.

Q28: Do you have any other regulatory suggestions that could contribute to reducing the risks associated with the application layer of DeFi?

☐Yes

☒No

If so, what are they?

No, AFME members do not have additional suggestions at this time beyond what has been set out in response to the previous questions.

Section 3-3: Regulating the provision of and access to services

Q29: Do you think that in some cases it may be necessary to "recentralise" specific sensitive activities (section 3-3-1)?

☒Yes

☐No

If so, which ones? If not, why?

Authorisation to conduct financially regulated activities

Overview

In order to conduct regulated financial activities, we recommend that DeFi organisations be supervised by the appropriate regulators of specific activities. This will create a more level playing field that is consistent even if the entity is not a regulated organisation, and will also leverage the expertise of regulators to provide appropriate oversight of the activities being conducted. However, we would note that the below recommendations would primarily serve as 'regulatory hooks' and be most relevant for regulated financial services firms who are interacting with DeFi structures. One could argue that the DeFi 'purists' may aim to evade any form of centralisation to the largest extent possible and regulatory intervention and may need to rely on a self-governing model. If this occurs, there may be additional considerations for how a true DeFi structure would interact with the regulated financial services industry.

Recommendations

1. Identification of activities being conducted (e.g. lending etc.)
    a. Determining the nature of operations and taking into account the complexity of the firm's regulated activities, products and how the business is organised.

2. Location and jurisdiction
    a. Financial institutions are required to have an identified place of business. Despite being decentralised, it is critical to know *where* financial products are being offered from and where financial activities are being conducted so that they can meet the regulatory requirements in that jurisdiction.
    b. Regulators are advised to provide clarity on cross-jurisdictional competences, covering in particular cases where investors, DeFi institutions and issuers are not located in the same country in a view to provide clarity on the applicable regime

and hence avoid regulatory arbitrage stemming from the cross-jurisdictional nature of the structure[17].

3. Personnel and decision-making processes
    a. Despite DeFi having varying levels of centralisation it is important for regulators to have oversight of the governance processes for financial activities being conducted. Existing governance regulations could be leveraged.

    b. Furthermore, it is important to have a point of contact. DeFi organisations will need to consider who is accountable for activities conducted and decisions made.

4. Final decision on authorisation made by the supervisory authority who regulates those specific activities.
    a. Taking into consideration the decentralised nature of DeFi activities, maybe different regulatory approaches should be considered too. For example, by offering voluntary compliance for those entities that cannot be recognised under the standard legal identity system (i.e. DAOs), or by introducing a role for regulators in that so-called "self-regulation" by way of validating industry codes or enhancing supervision intensity when necessary.

Choosing the appropriate accountability structure

Overview

Once activities have been identified, DeFi organisations must choose which of the following accountability structures they should adopt. Legal clarity on liability within DeFi is crucial and item 2(b) above also contributes to promoting robust principles.

Our suggestions are supported by research from the BIS. An article from their December 2021 Quarterly review states that all DeFi platforms have an element of centralisation, typically due to the presence of governance tokens. The article proposes that these governance structures mark a useful starting point for recognising DeFi platforms as legal entities.

Recommendations

1. An offshoot of a centralised and traditionally regulated financial institution.
    a. In this case the DeFi organisation would need to adhere to the appropriate regulatory requirements of its parent institution (much like a third country branch).

2. Leveraging the approach of rule applicability from other entities that do not have legal personality (e.g. trusts).
    a. In this case the DeFi organisation should come under the appropriate activity-based regulation.

3. Creating a legal figure for DAOs incorporation, so that this legal figure can be held responsible for legal obligations and therefore, be required to comply with the requirements laid out in MiCA.
4. Establishing clear regulatory principles and rules that can guide the behaviour of DeFi participants, other options? (Formal regulation).
5. In addition to formal regulation, encouraging self regulation within the DeFi community.

[17] Reference to the FSB Regulation, Supervision and Oversight of Crypto-Asset Activities and Market document can be made here - Recommendation 3: Cross-border cooperation, coordination and information sharing

Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication, information sharing and consultation in order to support each other as appropriate in fulfilling their respective mandates and to encourage consistency of regulatory and supervisory outcomes." https://www.fsb.org/wp-content/uploads/P111022-3.pdf

a. Involving industry associations, practice guidelines, any forms of collection action that can help to promote accountability.

Q30: What do you think of the proposals on how to achieve this goal (incorporation requirements, making players with effective control liable, legal status for DAOs)? Do you have any suggestions regarding the legal status of DAOs?

Please see our above response to Q29 which also discusses our suggestions for how this might be achieved.

Q31: Do you agree with the description provided of the risks associated with “CeDeFi” on the one hand and “crypto conglomerates” on the other (box 6M)?

Yes, the risks demonstrated by the recent failures of CeFi has highlighted the benefits of true transparency inherent within DeFi as no such similar problems occurred within the technical protocols. For example, after FTX went insolvent there was no clamour to recode ERC20 tokens or blockchain consensus algorithms.

We should be vigilant against Crypto Asset Service Providers (CASPs) that purport to be DeFi but are not really decentralised. These are DINOs (Decentralised In Name Only) and require due diligence by regulators.

It should be noted that although there have been several instances of smart contracts losing funds, these were due to vulnerabilities in the code which were exploited and show the need for appropriate processes for review of the code prior to release (software development process deficiencies).

Q32: What requirements should apply to intermediaries facilitating access to DeFi?

☒Information requirements

☒Duty of care and duty of advice

☒White paper publication requirement

☒KYC requirements

☒A comprehensive framework inspired by MiCA

☒Other

Why?

We would also support clear risk disclosures including any conflicts of interest.

Q33: Should the same rules apply to all intermediaries in DeFi (including, where appropriate, decentralised web interfaces)?

☐Yes

☒No

Why?

No, DeFi is a vast environment with different uses cases, which will all need a tailormade approach. What is crucial is that authorities take a principles-based, technology neutral approach, that supports different use cases in still meeting the appropriate regulatory outcomes.

Q34: Should access to financial products be conditional on customers' financial literacy level and risk appetite?

☐Yes

☐No

Why?

AFME primarily represents a broad array of pan-EU global and regional banks. As AFME is a capital markets association – our DeFi research has been focused on the risks for wholesale markets and as such is not best placed to comment on this question.

Q35: Do you have any other suggestions for regulating the provision of and access to services?

☐Yes

☒No

If so, which ones?

No, AFME members do not have additional suggestions at this time.

Avenues for a regulatory framework: cross-cutting aspects

Q36: How can proportionality requirements (for small players) be taken into account in the various regulatory avenues put forward by the document (or proposed by you)?

AFME primarily represents a broad array of pan-EU global and regional banks. As AFME is a capital markets association – our DeFi research has been focused on the risks for wholesale markets and as such is not best placed to comment on this question.

Q37: What regulatory avenues -whether or not they are proposed in the document- could overcome the problems related to the possible extraterritoriality of actors (from a national or European point of view)?

Most individuals will not be technically able to access the blockchain smart contracts directly resulting in them needing to use an intermediate app or webpage even if the provider of the service is based outside the territory. This provides an effective regulatory hook through control of this intermediate layer. In addition, co-operation between regulators and standard setters globally is key to preventing bad actors from arbitraging between locations and lowering standards. Facilitating places where real time information can be exchanged between exchanges that act as on/off ramps, owners of widely used smart contracts like stablecoins, blockchain analytic organisations, representatives of regulators and law enforcement in real time will be key to reacting quickly to any situations created by bad actors and freezing any funds generated by extraterritorial actors in violation of the rules.

Q38: Who should, in each case, monitor the implementation of the different regulatory tracks (whether they are put forward in this document or proposed by you)? With what means?

AFME believes that it will be important to ensure European regulations are harmonised globally as this is critical in removing market arbitrage opportunities and benefits large international banks. Who could do this? Possibly a role for IOSCO, FSB, IMF and other supranational bodies.