October 19, 2023

Public Comment on IOSCO's Consultation Report on Policy Recommendations for Decentralized Finance (DeFi).

We wish to thank IOSCO for the opportunity to comment on the Policy Recommendations for Decentralised Finance (DeFi) (CR/04/2023). IOSCO's work in this area is very important and we appreciate the opportunity for members of the DeFi industry to provide input.

As a general comment, we wish to call on IOSCO to take an active role in providing new regulatory guidelines and recommendations for DeFi. Existing regulatory frameworks for traditional financial services, which are based on centralised systems, are often unsuitable to address the unique challenges and opportunities of DeFi markets. IOSCO's efforts to ensure investor protection and market integrity are very welcome, but we believe that the regulatory approach to achieve those goals must recognize the unique features of DeFi and the wider crypto-asset industry. We believe that existing securities law frameworks are inadequate and inappropriate to address crypto and digital asset markets as a whole.

In particular, crypto and digital asset markets that build on decentralised blockchain technology are inherently different from traditional, centralised financial services. Regulators should take a nuanced approach and only apply Existing Frameworks to assets that clearly qualify as financial instruments and activities related to them. We believe that fungible crypto and digital assets as such should not be treated as securities in most cases.

Existing Frameworks are often unsuitable for DeFi and crypto asset markets in general. Blockchain technology enables crypto and digital asset markets to function in ways that are fundamentally different from traditional, centralised financial markets. For example, blockchain technology enables service providers to settle transactions immediately, without the need for a separate clearing agency. Instead of needing to rely on intermediaries, the underlying blockchain technology can settle transactions securely and users can hold their assets directly.

While it is true that DeFi projects exist on a spectrum of decentralisation and may exhibit centralised areas, the overall approach to DeFi should not be based on regulatory frameworks that assume or require further centralisation. We believe that the regulatory approach should instead encourage and enable DeFi projects to develop towards full decentralisation. For example, regulators should not require DeFi projects to acquire a custody licence, brokerage licence, exchange licence etc. if the project's technology already enables users to trade assets in a decentralised, non-custodial manner.

This is a joint response by the European Blockchain Association, LlamaRisk and the IOTA Foundation with contributions from Erwin Voloder (EBA), Svetlin Konsulov (LlamaRisk) and Tom Jansson (IOTA).

EUROPEAN BLOCKCHAIN ASSOCIATION

LlamaRisk

IOTA

Recommendation #2 - Identify Responsible Persons

A regulator should aim to identify the natural persons and entities of a purported DeFi arrangement or activity that could be subject to its applicable regulatory framework (Responsible Person(s)). These Responsible Person(s) include those exercising control or sufficient influence over a DeFi arrangement or activity.

While it is important to recognise the groups of people or entities involved in a DeFi project, the regulatory outcome should carefully consider the power and influence of each contributing participant. Regulators should not impose the same regulatory framework to such groups or entities as for centralised financial operators, because they individually may not have the same power or influence over the DeFi project overall.

IOSCO's recommendation 2 lacks nuance when it states that "*Once a regulator identifies Responsible Persons, their activities should be assessed using Existing Frameworks or New Frameworks, as appropriate, in accordance with the principle of "same activity, same risk, same regulatory outcome."*" This approach is not sustainable and could significantly deter development in the sector.

For example, Decentralized Autonomous Organization (DAOs) exhibit fluid and dynamic roles, underpinned using smart contracts and decentralized consensus mechanisms. These smart contracts are not a 'management body, board of directors or other fiduciaries commonly found in traditional financial organizations defining how roles are created, modified and dissolved. Participants in certain DAO communities can propose changes (enabled through smart contract configuration) including the creation of new roles or modification to existing contract code. Upon approval by the community, these changes in turn become part of the DAO's operational code and internal dynamism. In other cases, dynamic roles allow participants to transition in and out of roles based on their willingness to actively participate in governance decisions.

Therefore the role of a 'voter' can shift as token holders become more or less involved in governance activities. Smart contracts in turn govern these transitions, allowing the 'community' to adapt roles in real-time. For example, in some DAOs, participants who initially provided liquidity may transition into governance or development roles as the project evolves. These transitions are tracked through smart contracts and are often based on quantifiable contributions to the DAO, where 'rewards' for said roles can be distributed based on how they are occupied and what value is brought to the overall project. This means that the trade-offs between technical skill and any such 'financial' contribution to the overall project are not always cut and dry blurring the lines between IOSCO's guidance on Responsible Person(s) in relation to design maintenance and control, financial and economic control, and/or sufficient influence over a particular activity at the enterprise level.

As DAO governance is defined using smart contracts, they play a crucial role in defining any such roles and governing rules for the project. These smart contracts are overwhelmingly open-sourced (OSS), with a broad contribution from developers dispersed across different jurisdictions and legal regimes. Moreover, the DAO 'community' makes up a constellation of participants using both on-chain and off-chain methods including governance and liquidity provider tokens, online chat rooms, GitHub forums, telegram communities, Discord and other methods. These 'community members' are also geographically dispersed, residing in differing jurisdictions and legal regimes. Furthermore, on-chain participation is driven by pseudonymity as a fundamental characteristic, where participants use for example Ethereum Addresses or other pseudonyms instead of real world identities. The same can be said for off-chain communication across different social media

platforms where avatars are also common. To complicate matters further, recent developments in the DAO ecosystem show experiments involving Artificial Intelligence (AI) assisted governance via so called 'autonomous governance assistance' mechanisms. In such cases, governance improvements and streamlining the internal dynamics of the DAO is delegated to systems/processes that have no inherent legal agency.

Voting procedures may also differ between DAOs (simple majority, delegated and/or quadratic voting). With delegated voting, token holders can delegate their voting power to a representative, relying on trust placed in delegates to vote on their behalf. Shareholders in traditional corporations may delegate their voting rights to another party if they are unwilling or unable to attend the company's annual meeting or in emergency situations. This does not generally extend to delegated voting en-masse in normal circumstances (which in a DAO can be calibrated as a default option). In quadratic voting, a participant receives an allocation of votes with the ability to place more than one vote on a given proposal. In any case, voting mechanisms are defined in advance, hardcoded and are not easily modified. In traditional corporations, c-suite executives (CEO, CFO) may ignore shareholder consensus when coming to a decision, which is contrary to smart-contract based voting and 'liquid democracy' exhibited in many DAOs.

Adhering to 'same risk, same activity, same regulation' as applied in the report suggests regulators can apply either the same regulation or achieve the same regulatory outcome. This may be difficult to achieve in the case of DAOs due to their novel structure, fluid governance and smart contract based automation at various levels of the DAO 'stack.' Moreover, given the geographic disparities of DAO participants across varying jurisdictions, and the inherent pseudonymity of many DAOs in general - it becomes important to underscore that application of boilerplate regulation to all participants is impossible where regulators lack a common understanding, definitions, and visibility on all levels within DAO ecosystems. We therefore recommend that IOSCO help to establish clear regulatory, taxation and registration standards for DAOs while clarifying the specificities of 'locally occurring' within a given jurisdiction. This may further involve clarification of Responsible/Non-Responsible persons, retail vs. non-retail users, and that access to and use of a given DAO by a participant's exclusive initiation does not constitute 'occurring or located within' a jurisdiction.

Recommendation #3 - Achieve Common Standards of Regulatory Outcomes

A regulator should use Existing Frameworks or New Frameworks to regulate, supervise, oversee, and address risks arising from DeFi products, services, arrangements, and activities in a manner consistent with IOSCO Standards. The regulatory approach should be functionally based to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets.

We welcome IOSCO's statement that regulators should consider whether existing requirements need to be tailored or adapted to address DeFi-specific features and risks. However, it is important to distinguish between the technology as such and the (custodial) services offered by a financial operator. As we have outlined above, existing regulatory frameworks for traditional, centralised service providers are often inappropriate for DeFi, which are built for peer-to-peer and disintermediated transactions where users themselves undertake the financial transactions. IOSCO members should therefore consider New Frameworks that take into consideration the unique features of DeFi.

Due to the global nature of the crypto and digital asset markets, we also believe that regulatory frameworks need to be aligned internationally. IOSCO members have adopted contradictory regulatory and enforcement approaches for crypto-assets, e.g. regarding the classification of tokens as securities or non-securities, which have led to a fragmentation at the global level. The same asset may be considered a security in one jurisdiction and a non-security in another. There is a clear need for a consistent, international understanding of what constitutes a regulated financial asset in the context of crypto and digital assets. Ultimately, this lack of consistency weakens both consumer protection and the development of the market.

We believe that financial regulation should not be applied to developers or providers of technology as such. Intermediaries that are technology providers should not be treated as financial intermediaries. Financial regulations should only apply to operators that perform financial services on behalf of users. It would be inappropriate to lump DeFi services together or to apply financial regulations to technology providers merely because the technology as such can be used to make financial transactions. Providers that do not process financial transactions on behalf of users, i.e. non-custodial services, should instead be treated as technology intermediaries and should not be subject to financial regulations.

For example, IOSCO guidance outlines potential issuers of financial instruments including securities as including "aggregators and DEXs offering and selling their own crypto-assets, including governance tokens, LP tokens or other crypto assets."

Aggregators and DEXs function as user interfaces to interact with DeFi protocols, acting as front-end applications enabling users to access various DeFi services seamlessly. They aggregate liquidity from different sources, display token prices, and facilitate the execution of trades and liquidity provisioning. Governance tokens, LP tokens and other crypto assets are integral to the functionality of DeFi protocols (exhibiting voting rights properties and ownership in liquidity pools). These tokens are programmable assets with specific roles and utilities within the DeFi ecosystem. However, at their core, DeFi protocols are smart contracts, with self-executing code scripts deployed on blockchain networks. Aggregators and DEXs operate as seamless entities from the underlying DeFi protocols, which lack legal agency. They do not have control over the issuance and distribution of governance tokens, LP tokens or other crypto assets. Additionally, they do not issue or sell these assets.

Consider Uniswap, a well-known DEX. UNI is the governance token of Uniswap, granting holders voting rights and influence over protocol decisions. However, Uniswap itself consists of smart contracts that autonomously facilitate token swaps. Uniswap DEX platforms, such as Uniswap.info, serve as user interfaces to interact with the Uniswap protocol. They enable users to trade and provide liquidity but do not have control over the issuance or sale of UNI tokens because UNI tokens operate based on smart contract logic.

IOSCO guidance further outlines potential issuers of financial instruments including securities as "the issuance of derivatives/synthetics on traditional financial instruments, as well as the issuance by a cross-chain bridge, wrapping of a token, or in connection with liquid staking."

It is necessary to underscore a differentiation between technical staking and so called 'staking in name only', or SINO-based arrangements before turning to the question of liquid staking. For a more detailed appraisal, some of the contributors to this consultation alongside a consortia of industry partners have released two documents in the public domain "Towards a reliable taxonomy and understanding of PoS and 'related' services in an EU regulatory setting," and

"Understanding Staking: A Structured Taxonomy of Staking Mechanisms." Both are excellent resources we feel would further aid IOSCO in consolidating its understanding and position on the staking ecosystem as a whole.

In technical staking, participants lock their tokens and become validators. The core aim is to ensure network security, while the locked tokens or 'stakes' act as a commitment to the network's well-being. Validators with malicious intentions risk penalties against their stake (slashing), thereby making attacks on the network cost-prohibitive while enhancing overall network security. Technical staking is a penalty based system by design, underscored as **network security through economic value at loss**. Technical staking falls under three main categories: direct staking, delegated proof-of-stake and staking as a service (StaaS) platforms - both of which can also be custodial or non-custodial.

With *direct staking*, token holders/users maintain custody, with direct participation in network security. There is no third party role, with ownership and custody of staked assets belonging squarely to the token holder/user. Rewards are gained directly, and there are generally no fees.

With *delegated proof-of-stake (DPoS),* token holders/users delegate their staking power which can be done directly or through a StaaS platform. Participation is delegated to validators, who propose and vote on new blocks and form consensus on canonical blocks - these are the blocks that the network considers as 'valid.' Custody/ownership remains with the token holder/user, while rewards are proportional to the staking balance. The validator receives a reward if all transactions in the block are currently validated by them and the rewards are shared with users who selected them. The fee is less than the token(s) staked and is charged by the validator.

StaaS platforms are specialized platforms that manage all aspects of staking for users including node setup and maintenance, managing infrastructure and ensuring network security. They are split between custodial staking services, non-custodial staking services, staking pools and liquid staking.

In *custodial staking services*, token holders delegate their staking power with a transfer of ownership to third parties. Custody is handled through a VASP/CASP/wallet provider, while ownership is managed by a VASP/CASP/wallet provider only for the duration of the bonding period. Rewards are passed on to the StaaS provider before being distributed to the user who staked their tokens. There is an associated discounting fee for the VASP/CASP/wallet provider.

In *non-custodial staking platforms*, users/token holders participate in staking directly from their own non-custodial wallets. Providers (as third parties) do not have access to the user's assets and only provide the software application logic that helps users participate in staking from their own non-custodial wallets. Both custody and ownership rest with the token holder/user. If the network supports native delegation, rewards go directly to the staker without charging a fee from the validator first.

With *custodial staking pools*, token holders delegate their staking power to the pool, while a third party provides infrastructure, does the staking and does the distribution of the rewards. Custody rests with the validator while ownership resides with the custodian. Rewards need to be distributed proportionally or as determined by the pool provider. Any fees need to be smaller than the percentage of tokens staked.

Non-custodial staking pools allow token holders to either operate their own validator or delegate validating to a non-custodial StaaS provider without transferring ownership. A third party provides the infrastructure while ownership and custody reside with the token holder/user. Rewards are distributed among token holders based on proportionality of the 32 ETH deposit (in Ethereum-based staking) that is required to operate a validator. Fees can range anywhere from 0-10% depending on the pool.

A *liquid staking protocol* uses smart contracts to pool user tokens before delegating or directly staking them to validators. Additionally, the liquid staking protocol issues a token(s) that represents the staked coins, known as a liquid staking token (LST). In Ethereum-based liquid staking, token holders delegate their ETH to secure a PoS blockchain, while the third party provides the technical infrastructure. Custody is still technically with the end user, however it is delegated to a smart contract for the process of securing a PoS blockchain. Ownership resides with the token holder/user and rewards are distributed periodically as LSTs to those token holders who have pledged their ETH for the purpose of network security. In order to un-stake their tokens, users must first send their LSTs to a 'burner' smart contract. Once validated, the underlying ETH is un-staked. Fees can range depending on the platform and are generally higher than with other types of staking.

Staking in name only or SINO refers to activities that are labelled as 'staking' but functionally operate differently, often mirroring traditional financial operations such as lending, and are not implemented for the fundamental purpose of network security. For example, earn programs lock up specific crypto assets to earn interest over time, with third parties being VASPs/CASPs and wallet providers. These third parties use the locked up deposits to support various activities such as lending to margin traders or staking in PoS networks. The outcome is a share of the generated profits with depositors as interest and/or forms of pro-rata income.

For example, in yield farming, liquidity providers (LPs) are incentivized to provide their tokens to facilitate liquidity on DeFi applications in exchange for interest. Third parties can range from DEXs, automated market makers (AMMs) - which may not be limited to constant product function AMMs - non custodial lending/borrowing platforms, algorithmic based money market systems, automated portfolio managers, and/or automated decentralized aggregation protocols. The third party further facilitates the decentralized infrastructure.

In grouping LSTs as derivatives or synthetic derivatives, it obviates the downstream function of the underlying service provider, in this case the liquid staking platform and may inadvertently funnel the service provider into a market participant definition it does not practically fit with. For example, a central counterparty (CCP) employs advanced risk management techniques. They calculate and monitor Initial Margin (IM) and Variation Margin (VM) based on Value-at-Risk (Var) models. If a trader defaults, the CCP steps in to guarantee the trade's performance. Liquid staking protocols rely on validators to bond a specific amount of crypto-assets (e.g. ETH) as collateral. Validators are at risk of being slashed (leading to collateral loss) if they misbehave. However, liquid staking protocols primarily aim to secure the blockchain rather than manage any counterparty risk the way a CCP would across derivative contracts.

Moreover, in derivative markets, CCPs become the counterparty to every trade, ensuring trade settlement and reducing counterparty risk. Liquid staking protocols enable users to participate in PoS networks and do not engage in clearing and settlement functions. While CCPs are subject to strict regulatory oversight, liquid staking protocols are subject to blockchain network governance.

A closer look at LSTs finds other divergences from what may be considered a traditional derivative or synthetic derivative contract.

(i) liquid staking tokens typically lack explicit contractual terms that define traditional derivatives. They do not provide options or futures contracts with predetermined exercise prices, expiration dates or other contractual features typical of derivatives.
(ii) Traditional derivatives involve counterparties entering into contractual agreements to exchange cash flows or assets based on future market conditions. LSTs are transferable assets that do not require counterparties to engage in contractual negotiations or agreements.
(iii) LSTs serve as a means to participate in staking activities within PoS networks. They enable users to stake their assets and receive tokens that represent their share of the collective staking pool. In contrast, derivatives are designed for hedging, speculating, or managing risk by facilitating price exposure and/or financial obligations.
(iv) In the case of the European Market Infrastructure Regulation (EMIR) derivatives may also be linked to various non-financial variables such as climatic conditions or emission allowances. Although the act of staking itself may be linked to non-financial variables (technical PoS consensus), LSTs are not.

LSTs may be better defined as a 'synthetic crypto asset.' They provide a synthesis of value, combining utility with yield, technical staking with a rewards based system – merging the utility of a native blockchain asset such as ETH with the yield generating capabilities of staking. Liquid staking receipt tokens also exhibit a representational nature as they are created and managed through smart contracts and staking pools. This allows them to serve as digital representations of ownership rights in the staked assets within a given blockchain network. As such, aligning the definition of LSTs with the definition of the underlying asset structure (e.g. ETH) may be a more effective approach and could be tailored to both New Frameworks and Existing Frameworks accordingly.

Recommendation #4 - Require Identification and Addressing of Conflicts of Interest

In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to identify and address conflicts of interest, particularly those arising from different roles and capacities of, and products and services offered by, a particular provider and/or its affiliates. These conflicts should be effectively identified, managed and mitigated. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions. This may include requiring more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.

Toxic vs Nontoxic MEV

We hereby present to your attention clarifications about MEV specifics that are relevant to its treatment as a risk-prone activity. We encourage the distinction between operations that intentionally or unintentionally harm consumers and those that bring balance to the system.

Backrunning occurs when an individual engages in suboptimal trading strategies, such as not diversifying their orders across various markets, resulting in un-favorable execution.

This phenomenon isn't unique to the realm of cryptocurrencies but is a common occurrence across diverse financial markets. In essence, backrunning plays a pivotal role in the market ecosystem, closely aligning with arbitrage practices. It contributes to the correction of market inefficiencies by capitalizing on price discrepancies arising from less than optimal trade executions. The concern should not be so much about the prevalence of backrunning, but rather, its causative scenarios can raise eyebrows. It becomes notable when substantial profits are derived from these activities. Instances where protocols are compromised or funds are illicitly obtained and then swiftly swapped, create ripe grounds for lucrative arbitrage opportunities. These scenarios often accompany significant backrunning activities for which the arbitrator is required to compensate the block-builder generously to prioritize the transaction. It is in these high-stake environments, characterized by substantial fees and considerable profits (see example below), that the scrutiny of backrunning intensifies. This underscores the need for vigilance and ongoing oversight to mitigate potential abuses and ensure market integrity.

Wormhole bridge exploit

Wormhole is communication bridge on Solana that enables the transfer of tokenized assets across blockchains, leveraging Solana's speed and low cost. On February 2nd 2022, the Wormhole bridge was exploited due to vulnerabilities in unpatched contracts in Solana. This allowed the attacker to credit 120k ETH as having been deposited on Ethereum, which enabled them to mint an equivalent amount in wrapped Wormhole ETH on Solana. After the hack, 93,750 ETH was bridged back to Ethereum in three transactions and remains in the hacker's wallet. The Wormhole bridge exploit caused a large backrun opportunity. Observing the bad actor's transactions one could initiate trades that capitalized on the expected market movements caused by the hacker's large transactions.

Opposite to the prevalent issues discussed in the Policy Recommendations, i.e. sandwiching and front-running, often characterized as "toxic MEV", there exists a distinct category termed "nontoxic MEV," encompassing *arbitrage* and *liquidations*. Arbitrage involves the strategic execution of simultaneous asset transactions across diverse markets, capitalizing on price discrepancies to garner profits. This practice is instrumental in maintaining price consistency across decentralized financial landscapes. Arbitrage between centralized exchanges and decentralized exchanges serves to rectify price disparities between on-chain and off-chain markets. Arbitrageurs play a critical role in stabilizing these markets and are rightfully compensated for their essential contributions. Such activities, in their fundamental nature should not be deemed malicious.

Conversely, liquidations are integral to on-chain lending platforms, initiated when the value of collateral underpinning a loan depreciates below the designated safety threshold. In such instances, external actors are permitted to settle the outstanding debt and are incentivized through the option to acquire the devalued collateral at a reduced price. This mechanism is pivotal in insulating lending systems from the ramifications of unrecoverable debts. Fundamentally, liquidations are not designed to be malicious and, therefore should not be considered harmful per se.

Both arbitrage and liquidations are emblematic of nontoxic MEV, characterized by the intrinsic value derived from the exclusive opportunity to capitalize on these financial maneuvers. The crux of this value is contingent upon the capacity to manipulate the sequence of transaction processing within a specific block, a capability that underscores the competitive essence of these strategies.

October 19, 2023

MEV Boost

MEV-Boost is an open-source middleware developed by Flashbots for Ethereum's PoS protocol. It implements a concept known as proposer-builder separation (PBS), providing a framework for validators and builders to interact more efficiently in block production. Validators running MEV-Boost can access a marketplace of builders, thereby maximizing their staking rewards by selling block space to an open market of builders. This open market is essentially a competitive block-building market that aims to optimize block creation and rewards distribution (CoinCashew MEV Boost Guide).

With MEV-Boost, validators in Ethereum's PoS become permissionless. Unlike the previous system, now the validators request blocks from the Flashbots relay through MEV-Boost. This change facilitates a more decentralized and open system for block validation and creation, thus democratizing access to MEV profits and reducing the negative effects associated with MEV.

Legal purview

The European Union's Markets in Crypto Assets Regulation (MiCA) introduces a favorable concept for the fully decentralized and disintermediated provision of crypto-asset services. The Regulation meticulously delineates the rights and obligations incumbent upon a diverse array of stakeholders, including issuers of crypto-assets, offerors, and those endeavouring to secure admission for the trading of crypto-assets, as well as crypto-asset service providers (CASPs).

MiCA outlines that validators do not fall within the CASP definition per Article 3, para 1, item 15: *"a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59"*. The categories of listed services in Article 3, para 1, item 16 focus on the custody, trading, exchange, and management of crypto-assets, along with associated advisory and transfer services on behalf of clients. Validators engage in activities that are inherently different from those defined above. They do not hold or manage crypto-assets on behalf of clients, nor do they operate trading platforms or execute orders for crypto-assets. Their role is technical and operational - focusing on the maintenance of the blockchain network's functionality and security.

Recital 93 of MiCA further asserts the exception, categorically excluding validators, nodes, or miners from the regulatory purview of the act. This exemption is contingent upon the active participation of validators, nodes, or miners in the affirmation of transactions and the consequent augmentation of the distributed ledger's state.

The nuanced dynamics of MEV Boost align synergistically with the overarching ethos of network decentralization and the autonomous evolution of ledger updates. In this context, validators operating with MEV Boost middleware are ostensibly insulated from the regulatory ambit of MiCA. This insulation is attributed to the act's technology-neutral posture, which refrains from imposing prescriptive or prohibitive mandates on specific technological modalities.

Customer safety

Typically, users initiate transactions utilizing wallet software, for instance, MetaMask. A pivotal concern arises regarding the entity to which a user's transaction is submitted. If a user, as is often the case, submits their transaction to a single operator, it elevates the operator to a position of

privilege. This enables the operator to consider user transactions as a form of "private order flow," which could potentially be exploited for MEV extraction.

Transactions are typically submitted through services termed "RPC endpoints" when utilizing wallet software. These endpoints adhere to a specific set of instructions, akin to the nodes within the Ethereum network, but are not mandated to execute functions typically associated with a network node, especially the re-broadcasting or forwarding of the transaction to additional nodes.

Every RPC endpoint operator, upon receipt of a pending transaction, is confronted with a triad of options:

(i) Abstain from action, effectively censoring the transaction.
(ii) Publicly re-broadcast the pending transaction.
(iii) Retain the transaction's privacy and directly forward it to select block-builders or validators.

The third alternative aligns with the operational modality of certain privacy RPCs, exemplified by Flashbots Protect. These privacy RPCs were conceived to shield users from undesirable forms of MEV extraction, serving as a bulwark against potential exploitations.

Within the diversity of DeFi, nontoxic MEV plays a quintessential role in fostering market equilibrium and fortifying the structural integrity of lending paradigms. However, the legal and ethical dimensions of transaction ordering and the monopolization of arbitrage and liquidation opportunities warrant meticulous scrutiny to ensure equitable and transparent financial practices. We therefore suggest a careful appraisal of the differences between toxic and non-toxic MEV in relation to the overall cost/benefit they bring to the DeFi ecosystem as a whole.

Grouping the two types of MEV into one policy outcome would harm consumer protection by reducing the ability of key players to rectify pricing disparities, and therefore introduce structural deficiencies into the operation of DeFi markets as such. As some key IOSCO members were also among the states which adopted MiCA in the Council of the European Union, and whose National Competent Authorities (NCAs) are now working diligently with EU Supervisory Authorities to prepare their domestic markets for its implementation, it would be beneficial for IOSCO to adopt similar positions specifically around the role of validators, nodes or minors - using MiCA as a potential template for the drafting of international standards on these specific topics.

Recommendation #5 - Require Identification and Addressing of Material Risks, Including Operational and Technology Risks

In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to identify and address material risks, including operational and technology risks. These risks should be identified and effectively managed and mitigated. A regulator should consider whether certain risks are sufficiently acute that they cannot be effectively mitigated and may require more robust measures to address this Recommendation.

Each type of blockchain bridge presents distinct legal and risk considerations. The Ethereum Foundation offers a practical classification of different bridge types.

Native Bridges (e.g. Arbitrum Bridge and Optimism Gateway) are integral to specific blockchain ecosystems. They facilitate seamless asset transfer, enhancing liquidity within the ecosystem.

Validator or Oracle-Based Bridges (e.g. Multichain and Across) rely on external validators or oracles. The legal implications revolve around the trustworthiness and accountability of these external entities.

Generalized Message Passing Bridges (e.g. Nomad and LayerZero) facilitate the transfer of assets and arbitrary data. Legal considerations include data privacy, security, and compliance with cross-border data transfer regulations.

Liquidity Networks (e.g. Connext and Hop) focus on asset transfers via atomic swaps. Legal considerations include the security, transparency, and traceability of asset transfers.

MiCA Recital 93 provides an important distinction in the regulatory treatment of Validator-Based Bridges within the broader ecosystem of Crypto-Asset Service Providers (CASPs). This specific recital provides a clear exemption for Validator-Based Bridges from the overarching regulatory ambit that governs CASPs.

To expound, Validator-Based Bridges which are integral in facilitating the seamless interoperability between distinct blockchain networks, are not classified as CASPs tasked with executing transfers of crypto assets from one distributed ledger address or account to another on behalf of a client. Within this regulatory context, the term "transfer service" is defined so as to exclude validators, nodes, or miners that play a pivotal role in confirming transactions and contemporaneously updating the state of the underlying distributed ledger. The exclusion underscores a recognition of the technical and functional distinctiveness of these entities, aligning regulatory frameworks with the practical and operational realities of distributed ledger technologies.

LlamaRisk recently investigated Multichain, a cross-chain router protocol (CRP) that provides the infrastructure for arbitrary cross-chain interactions. The protocol enables cross-chain interoperability of tokens, NFTs, and general data across multiple EVM and non-EVM blockchains. We are pleased to present a comprehensive discourse articulating key findings from our rigorous risk assessment. This assessment evaluates three pivotal vectors: Technology and Smart Contract Risk, Governance Risk, and Custody and Network Risk, with the objective of providing nuanced insights and fostering an informed, secure operational ecosystem.

Technology and Smart Contract Risk

Two security breaches had been encountered by the date of the investigation. Although the financial implications were relatively contained, the incidents underscore the inherent vulnerabilities associated with bridge technologies, a frequent target for cyber adversaries. A rigorous scrutiny of the protocol’s code by noted auditing firms significantly mitigates the risk of compromised smart contracts. However, the latent risk of undetected bugs and vulnerabilities, exacerbated by the intricate nature of bridge operations persists. Despite comprehensive audits the protocol is not immune to technology risks encompassing software failures, human errors, and malicious attacks. This underscores the need for continuous vigilance and risk management.

Governance Risk

Multichain’s governance structure is presently centralized, with decision-making authority vested in the team and the 21 SMPC nodes. The protocol’s indication of transitioning to a Decentralized Autonomous Organization (DAO) remains largely theoretical.

The embryonic stages of DAO integration, marked by the introduction of veMULTI, have yet to manifest into a tangible governance structure. The absence of an operational governance forum and on-chain governance tools underscores the protocol's centralized control.

Custody and Network Risk

The protocol's custody and network operations are governed by the 21 SMPC nodes. This centralized mechanism engenders risks associated with potential collusion and malicious activities that could compromise the network's integrity and users' assets. The team's significant influence over the network, evidenced by the MPC network's fund movement capabilities, raises concerns regarding the decentralization and autonomy of the protocol. Users' confidence in the protocol is anchored in the reputation of node operators. The public disclosure of nodes, many of which are affiliated with the team, underscores the need for enhanced transparency and accountability mechanisms to mitigate associated risks.

Following the insights gleaned from our initial findings, we recommend an extended phase of examination to address specific questions that have arisen, pivotal to ensuring the robustness and integrity of the operational ecosystem. The subsequent analysis should scrutinize: (*A) the potential of a single entity orchestrating a 'rug pull', evaluating the system's resilience and safeguards against such events*. Furthermore, we seek to *(B) assess the project's sustainability and continuity in the hypothetical absence of its founding team*. Are the structures and mechanisms in place self-sustaining and equipped to withstand such a scenario? Lastly, *(C) an in-depth review of the audit reports* is indispensable to identify and evaluate any alarming indications or vulnerabilities that may compromise security or performance. This layered approach ensures a holistic, multi-faceted analysis, underpinning one's commitment to fostering a secure, resilient, and transparent operational environment.

To broaden the understanding of the diverse mechanisms and security postures of cross-chain protocols we present to your attention another risk framework developed by an open community of contributors. Four primary risk categories have been mapped to the cross-chain communication:

Network Consensus Risk pertains to the assurance that the state communicated between networks is validated according to consensus rules. Failures can lead to irreconcilable inconsistent state changes across chains, impacting all bridges connected to the faulty network.

Protocol Architecture Risk highlights the vulnerabilities arising from design assumptions and constraints of layered cross-chain protocols. Risks are especially heightened when new trusted parties are introduced, often leading to weakened security guarantees.

Protocol Implementation Risk encompasses varied programming languages, frameworks, and runtime environments, which may increase the probability of bugs and vulnerabilities, a prominent cause of bridge hacks in recent years.

Protocol Operation Risk stems from the management of cross-chain bridge components, potentially by different actors. Failures in operational activities, like the upgrade and management of bridge smart contracts, present significant risks.

A layer also worthy of exploration is the utilization of off-chain computation, which can provide valuable insights and play a decisive role in relevant due diligence processes. A prime example illustrating the potential of off-chain computations is Off-Chain Reporting (OCR). This innovative

mechanism, primarily associated with the Chainlink network, embodies a transformative step towards accentuating both decentralization and scalability. The architecture of OCR is structured around a cohort of node operators. These nodes are entrusted with the task of sourcing data for designated data feeds. The unique facet of OCR lies in its operational framework, where protocol execution predominantly occurs off-chain. This occurs over a decentralized, peer-to-peer network that interlinks Chainlink nodes.

The procedural communication within OCR employs a streamlined consensus algorithm. In this algorithmic process, every node disseminates its individual data observation, accompanied by a corresponding digital signature. The resultant outcome is an aggregated transaction that encapsulates the collective data observations. Notably, this consolidation results in significant gas savings, enhancing both efficiency and cost-effectiveness.