29 September 2023

REPLY TO THE AMF DISCUSSION PAPER

We thank the Autorité des Marchés Financiers (AMF) for the opportunity to share our perspectives on the potential regulation of decentralised finance (DeFi). We believe that collaborative efforts like this are crucial for the development of a robust and effective regulatory framework that promotes innovation, investor protection, and the overall growth of the blockchain industry.

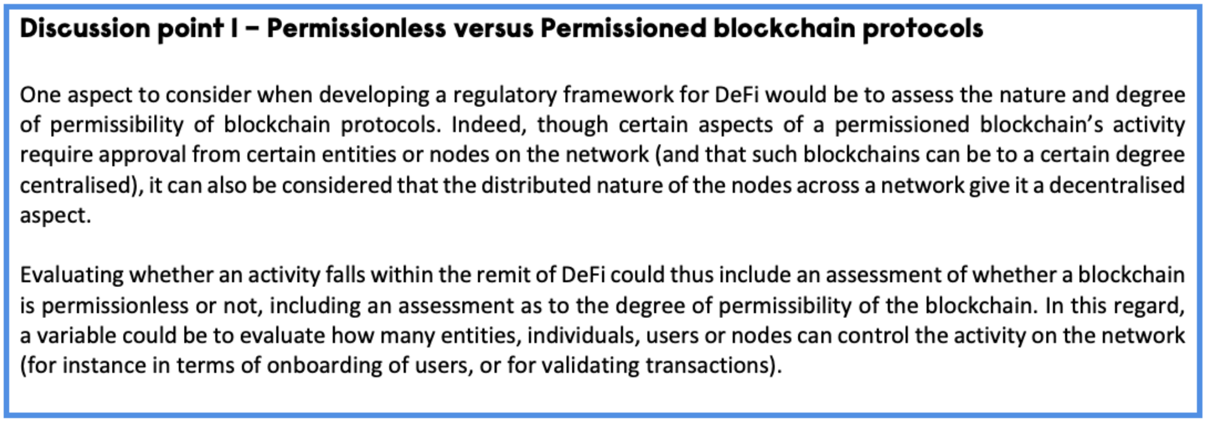
We have carefully reviewed the AMF's discussion paper and are grateful for the comprehensive analysis and insights it provides. The paper addresses several key areas of concern. As organisations deeply invested in the blockchain space, we are happy to provide our perspective and collaborate with the AMF to shape the future of DeFi. Once again, we extend our gratitude to the AMF for the proactive approach and open dialogue.

This is a joint response by the European Blockchain Association, the IOTA Foundation, LlamaRisk and Blockpit, with contributions from Erwin Voloder (EBA), Tom Jansson (IOTA), Svetlin Konsulov (LlamaRisk) and INATBA Board Members Mariana de la Roche Wills (IOTA) and Dr. Max Bernt (Blockpit).

EUROPEAN BLOCKCHAIN ASSOCIATION IOTA LlamaRisk

Blockpit INATBA International Association for Trusted Blockchain Applications

Discussion point 1 – Permissionless versus Permissioned blockchain protocols



Discussion point I – Permissionless versus Permissioned blockchain protocols

One aspect to consider when developing a regulatory framework for DeFi would be to assess the nature and degree of permissibility of blockchain protocols. Indeed, though certain aspects of a permissioned blockchain's activity require approval from certain entities or nodes on the network (and that such blockchains can be to a certain degree centralised), it can also be considered that the distributed nature of the nodes across a network give it a decentralised aspect.

Evaluating whether an activity falls within the remit of DeFi could thus include an assessment of whether a blockchain is permissionless or not, including an assessment as to the degree of permissibility of the blockchain. In this regard, a variable could be to evaluate how many entities, individuals, users or nodes can control the activity on the network (for instance in terms of onboarding of users, or for validating transactions).

The level of decentralisation in the DeFi ecosystem is complex and evolving. While the core ethos of DeFi is rooted in decentralisation, it is important to recognise that decentralisation can manifest itself on a spectrum. At its core, DeFi aims to eliminate the need for intermediaries, thereby enabling instant, secure and efficient peer-to-peer transactions, leveraging blockchain technology and smart contracts.

In response to discussion point 1, we wish to highlight DeFi's potential to offer activities beyond those found in the more traditional financial sector. Hence, in many ways, DeFi represents a paradigm shift in the way that financial services are provided, emerging as an alternative to existing traditional means.

While it might be true that no system is born fully decentralised, it is crucial to acknowledge the goal of achieving a "fully decentralised, automated, and disintermediated" system using decentralised blockchain protocols. So, even if an application or protocol may initially be launched in a (more or less) centralised manner, the potential for (full) decentralisation still exists. This is because the nature of blockchain technology allows for gradual decentralisation over time as the network grows and matures. Particularly, through the participation of a diverse and distributed network of users, governance mechanisms, and consensus protocols, these applications are able to transition towards greater and ultimately possibly "full" decentralisation.

Overall, decentralisation in DeFi encompasses various aspects, including governance, data storage, decision-making processes, and control over funds. As the ecosystem evolves, projects and protocols actively strive to increase their decentralisation by involving the community in decision-making, implementing open-source development, and enabling participation through staking or voting mechanisms.

While the path to full decentralisation may differ for each project, one of the underlying principles is to empower individuals and reduce reliance on centralised entities. This shift towards more decentralisation not only enhances transparency and security but also promotes censorship resistance and fosters a more inclusive and resilient financial ecosystem.

Therefore, it is important for regulators to recognise that decentralisation is generally not a binary state of a certain project that is established from the very beginning, but usually needs to be developed and grow through an ongoing process of implementation.

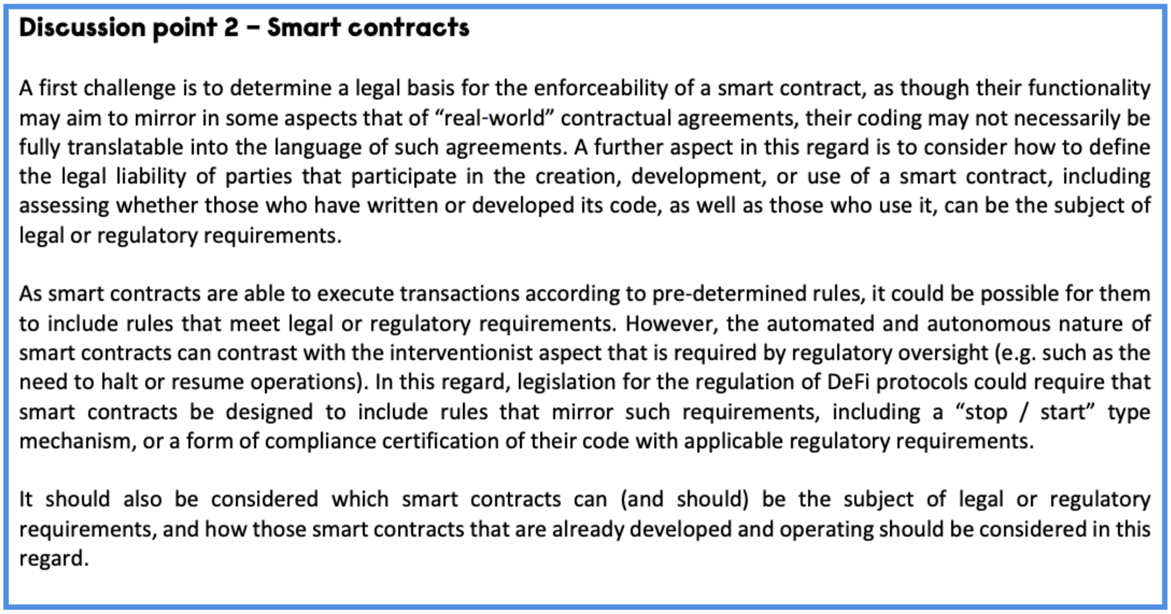
DeFi protocols and applications exist on multiple different blockchains, yet they are still in their infancy. While Ethereum has played a pivotal role in the early growth of DeFi, the landscape is rapidly evolving. New protocols and platforms keep emerging, offering innovative solutions and addressing scalability challenges. This diversification reduces the concentration risk and promotes healthy competition, leading to a more robust and resilient DeFi ecosystem.

DeFi is built on a layered infrastructure, where different protocols and pieces of code interact and integrate to provide various financial services. While Layer 2 solutions have gained attention for their scalability benefits, DeFi applications and smart contracts also operate on Layer 1 blockchains. The existence of smart contracts on both Layer 1 and Layer 2 showcases the flexibility and adaptability of DeFi to leverage different technical solutions based on specific use cases and requirements.

Moreover, DeFi protocols and smart contracts are designed to be interoperable, allowing for seamless integration and collaboration between different platforms and protocols. This interoperability enables the composability of DeFi applications, where different components can be combined to create innovative and complex financial products and services. As a result, DeFi is not limited to a single blockchain or protocol, but rather thrives on the interoperability and integration of various technologies within the broader ecosystem.

In direct response to discussion point 1 regarding permissioned versus permissionless blockchain protocols, we strongly believe that true **DeFi cannot exist within permissioned networks.** While certain aspects of permissioned networks may exhibit decentralisation, the presence of permissioned control by one or multiple parties inherently centralises decision-making power. DeFi, on the other hand, operates on the principle of decentralisation, where governance and control are distributed among participants, allowing for trustless interactions and eliminating the need for intermediaries. Therefore, when evaluating whether an activity falls within the realm of DeFi, it is essential to assess the permissibility and degree of control within the underlying blockchain protocol. The more entities, individuals, users, or nodes can participate in the network's activities and decision-making processes, the greater the potential for a truly decentralised and permissionless DeFi ecosystem to thrive.

Discussion point 2: Smart contracts



Discussion point 2 – Smart contracts

A first challenge is to determine a legal basis for the enforceability of a smart contract, as though their functionality may aim to mirror in some aspects that of “real-world” contractual agreements, their coding may not necessarily be fully translatable into the language of such agreements. A further aspect in this regard is to consider how to define the legal liability of parties that participate in the creation, development, or use of a smart contract, including assessing whether those who have written or developed its code, as well as those who use it, can be the subject of legal or regulatory requirements.

As smart contracts are able to execute transactions according to pre-determined rules, it could be possible for them to include rules that meet legal or regulatory requirements. However, the automated and autonomous nature of smart contracts can contrast with the interventionist aspect that is required by regulatory oversight (e.g. such as the need to halt or resume operations). In this regard, legislation for the regulation of DeFi protocols could require that smart contracts be designed to include rules that mirror such requirements, including a “stop / start” type mechanism, or a form of compliance certification of their code with applicable regulatory requirements.

It should also be considered which smart contracts can (and should) be the subject of legal or regulatory requirements, and how those smart contracts that are already developed and operating should be considered in this regard.

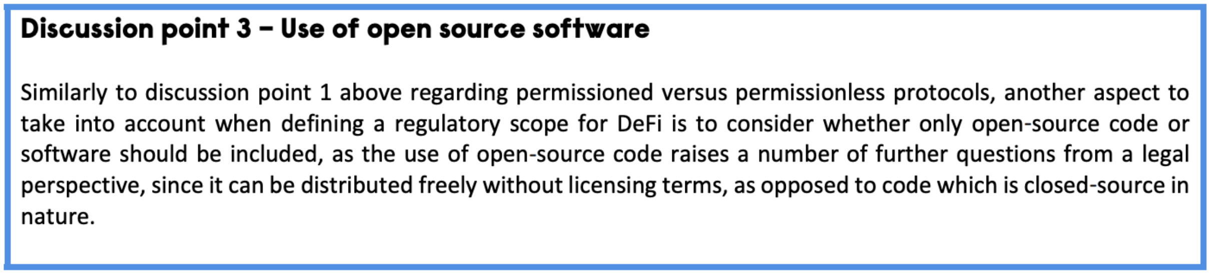
With regard to smart contracts, we see several important considerations to address. Firstly, it is crucial to acknowledge that smart contracts may not necessarily only mirror legal contracts. While it is true that smart contracts can execute transactions based on predetermined conditions, they can also enable other functionalities, such as automatic reporting of suspicious activities to regulators or law enforcement agencies. In essence, a smart contract is a computer program deployed through distributed ledger technology, wherein the execution logic is predefined and deterministic, and the execution happens automatically. Hence, simply put, a smart contract is a tool to automate and execute predefined actions.

Smart contracts may encompass thousands or tens of thousands of lines of code, which makes auditing the code very complex. Audits typically involve both line-by-line analysis and automated reviews, and there are specialised service providers that provide smart contract audits as a service.

In order to safeguard against exploits, one possible approach is to consider a model of certification for smart contracts, ensuring compliance with minimum requirements. Community-led auditing processes can also contribute to enhancing the quality and security of smart contracts, in addition to professional service providers. By establishing mechanisms to certify and audit smart contracts, the industry can promote responsible development and usage, addressing concerns related to liability and potential risks in a self-regulatory manner.

The introduction of centralised features, such as a stop/start mechanism, would not be advisable or practical, as such features would rely on the security and goodwill of a centralised party and remove the decentralised nature of the smart contract.

Discussion point 3. Use of open-source software



Discussion point 3 – Use of open source software

Similarly to discussion point 1 above regarding permissioned versus permissionless protocols, another aspect to take into account when defining a regulatory scope for DeFi is to consider whether only open-source code or software should be included, as the use of open-source code raises a number of further questions from a legal perspective, since it can be distributed freely without licensing terms, as opposed to code which is closed-source in nature.

In response to discussion point 3, the use of open-source software (OSS), we would like to emphasise the security aspects related to OSS. OSS can generally be considered to be safer than closed source software because it is transparent and auditable. In particular, the following factors should be noted:

- **More eyes on the code**: OSS is freely available to anyone to view and audit. This means that there are more people who can look for and fix security vulnerabilities.
- **Faster vulnerability identification and remediation**: When a security vulnerability is found in OSS, it is often fixed more quickly than in closed source software. This is because there are more people who can contribute to the fix, and there is no need to go through a lengthy approval process.

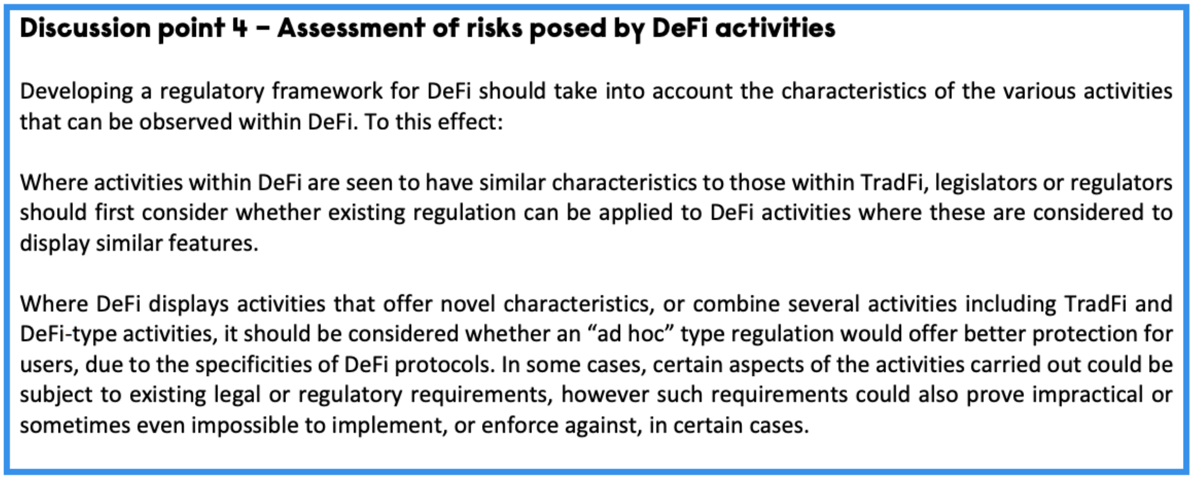
- **Stronger community**: The open source community is very active in identifying and fixing security vulnerabilities.
- **Less risk of backdoors**: Backdoors are malicious code that is intentionally placed in software to allow unauthorised access. Closed source software is more susceptible to backdoors because the source code is not available for public scrutiny.

While OSS is not inherently more secure than closed source software, the transparency offered by OSS means that vulnerabilities can be identified more rapidly. However, when evaluating the security of an OSS project, one should also consider the following points:

- **The reputation of the project**: Does the project have a good track record of security and does it have adequate security policies?
- **The size and activity of the community**: Does the project have a large and active community? A large community can be a sign that the software is being well-maintained and security issues are being addressed promptly.

Overall, OSS can help to ensure safety and security. However, it is important to research and evaluate the project on a case-by-case basis.

Discussion point 4 - Assessment of risks posed by DeFi activities



Discussion point 4 – Assessment of risks posed by DeFi activities

Developing a regulatory framework for DeFi should take into account the characteristics of the various activities that can be observed within DeFi. To this effect:

Where activities within DeFi are seen to have similar characteristics to those within TradFi, legislators or regulators should first consider whether existing regulation can be applied to DeFi activities where these are considered to display similar features.

Where DeFi displays activities that offer novel characteristics, or combine several activities including TradFi and DeFi-type activities, it should be considered whether an “ad hoc” type regulation would offer better protection for users, due to the specificities of DeFi protocols. In some cases, certain aspects of the activities carried out could be subject to existing legal or regulatory requirements, however such requirements could also prove impractical or sometimes even impossible to implement, or enforce against, in certain cases.

In response to the AMF's discussion point 4, we would like to refer to the work done by Llama Risk. We believe that it provides a valuable methodology for the assessment of risks posed by DeFi activities. Llama Risk is an organisation run by volunteers that provides risk assessments of various DeFi activities.

Llama Risk's framework for assessing risks in DeFi was developed in order to assess volatility-prone ERC20 collateral assets added to crvUSD. It differentiates between stablecoins and volatility-prone ERC20 assets as they have different properties and associated risk factors. That is, stablecoins attempt to synthetically keep peg to a reference currency. In contrast, volatile assets have their value determined by market forces, such as supply and demand dynamics, market speculation, investor sentiment, or underlying project developments.

The key dimension of collateral can be summarised as follows:

- **Fundamentals of Collateral**: Evaluating the value of the collateral is essential to ensure that it provides sufficient backing for the stablecoin.
- **Ease of Liquidation**: The ability to liquidate the collateral efficiently is important in ensuring the stability of the stablecoin's value.
- **Persistence of Properties of the collateral**: The persistence of certain properties refers to the stability and predictability of the collateral's underlying characteristics.
- **Risk management**: Risk management refers to the process of identifying, assessing, and prioritising risks, followed by the application of strategies and measures to mitigate or manage those risks.

High-level outline of the framework:

To cover the identified dimensions comprehensively we propose the following framework to assess and quantify the collateral.

Market Risk

This part aims to address the ease of liquidation. It focuses on providing a comprehensive understanding of the volatility and liquidity profile of the asset in question.

- The *liquid staking basis* or the *peg analysis*, reviews the price difference in liquid staking token/underlying cryptocurrency or cryptocurrency and fiat currency/basket of crypto-assets it is pegged to.

- *Volatility analysis* provides insights into how much and how quickly the price of the asset has changed over a given period.
- *Liquidity analysis* delves into evaluating the ease with which the collateral can be bought or sold without affecting its price. This is critical in maintaining stability in times of market stress. Further, we perform a centralised exchange (CEX) and decentralised exchange (DEX) volume analysis to gauge the asset's overall liquidity. Moreover, understanding the asset's usage in DeFi, for example, in lending platforms, can provide additional liquidity insights.
- Lastly, the *liquidation analysis* covers three key areas: speed, size, and velocity of main market assets. The speed considers how quickly the asset can be sold, size looks at the volume of the asset that can be sold without significantly impacting the price, and the velocity considers the rate at which these assets are bought and sold in the market.

Technological Risk

This section is focused on evaluating the technological risk associated with the asset being considered. The purpose of this assessment is to understand if there are any underlying technological issues or risks that could potentially alter the fundamental properties of the collateral.

Quantification of Technical Risk involves assessing various aspects of the asset's technical environment.

- *Developer Activity*: Analysis of developer activity on the project's GitHub, such as commits, stars, and forks, provides an insight into the level of ongoing development and community interest in the project.
- *Smart Contract Maturity*: Measured in days since the contract was deployed, as older contracts are generally considered more reliable due to their longevity.
- *Number of Interactions*: The frequency and number of interactions with the smart contracts can often reflect their stability and the level of trust users have in them.
- *Previous Incidents or Flaws*: A history of incidents, such as hacks or major bugs, could indicate potential vulnerabilities in the system.
- *Scalability*: Evaluating how the system performs under heavy load conditions like high gas prices and transaction spam.
- *Oracles*: Assessing the reliability of the oracles used by the system, as inaccurate or manipulable oracle information can lead to significant system vulnerabilities.
- *Layer Dependency & Composability Risk*: Evaluating the risks associated with dependencies on other chains and risks associated with a product that is dependent on

several underlying protocols. The level of dependency on other systems can potentially increase the risk of the asset.

Risk Mitigation Techniques evaluate the various strategies employed by the project to minimise potential technological risks.

- *Audits*: Regular audits by reputable firms provide assurance of the security and reliability of the smart contracts.
- *Other Measures*: E.g. bug bounties to encourage the identification and reporting of vulnerabilities, or insurance coverage for potential losses can also serve as effective risk mitigation techniques.

Counterparty Risk

Counterparty risk refers to the potential risk of loss due to the failure or default of a party in a financial transaction. In this context, it focuses on the persistence of collateral properties from an ownership rights perspective (i.e., possession, use, transfer, exclusion, profiteering, control, and legal claim).

The aim here is to provide a clear understanding of who holds the legitimate authority to alter the properties of the collateral (e.g., minting additional units), their reputation, and the extent to which changes can be implemented and their potential impacts on the collateral.

- *Administrator/Developer Team*: This section involves assessing the qualifications, experiences, and track record of the team behind the project. It is critical to know if the team has the required competence and capability to run and maintain the project effectively. Any past successes or failures could provide insights into the team's potential performance.
- *Governance*: It's important to understand the governance structure of the project. Who has voting rights? How are decisions being made? Are decisions centralised or do token holders have a say? The governance model can impact the project's long-term sustainability and responsiveness to changes or issues.
- *Token Distribution*: Here, we examine how governance tokens (if applicable) have been distributed. A fair and broad distribution can be indicative of a decentralised network and reduce the risk of any single entity controlling the project.
- *Regulation*: The project operates within a certain regulatory environment. Knowledge of these regulations and compliance with them is crucial. This could involve assessing whether the project has obtained necessary licences or permissions, if it's adhering to reporting and audit requirements, or the legal characterisation of the native token.

- *Legal Establishment*: This section involves a review of the legal structure of the counterparty, which includes the type of legal entity and the country of its establishment. This is important as it impacts the legal obligations and protections for both the project and its users.
- *Licences*: In this section, we identify the relevant laws and regulations applicable to the project based on its jurisdiction. Understanding these legal requirements is crucial as non-compliance can lead to penalties and potentially jeopardise the project's operation.
- *Enforcement Actions*: It's important to investigate any legal enforcement actions brought against the project or the people involved in it. Such actions could signify potential regulatory or legal issues and impact the project's reputation and operation.
- *Sanctions*: A project's adherence to international sanctions obligations is also vital. This involves assessing whether the project has implemented appropriate measures to prevent sanctioned entities from using its services.
- *Liability Risk*: This part deals with evaluating the risk of the project being held liable for harm or financial loss incurred by a third party. This could stem from a range of issues including data breaches, software errors, or contractual disputes.
- *Adverse Media Check*: Lastly, we undertake a comprehensive media scan for any negative press coverage or controversies related to the project. This could include allegations of fraud, involvement in illegal activities, or other damaging information that could pose reputational risks and potentially affect the project's sustainability.

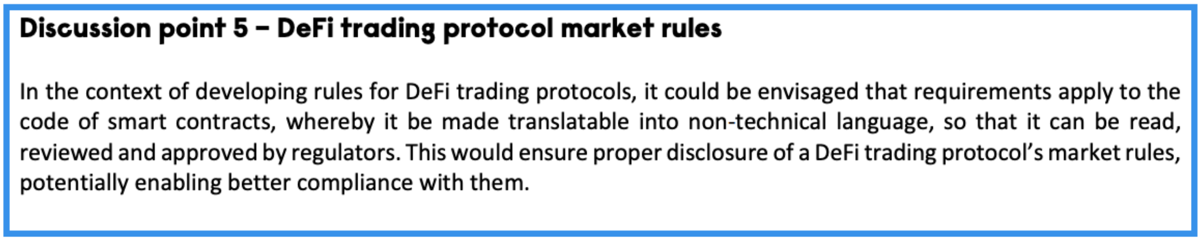
General comment regarding the Terra-Luna crash:

The recent Terra-Luna incident is often used as an example of how risks materialise within the DeFi ecosystem. However, it is important to note that the failure and price crash of Terra-Luna was not caused by the system's degree of decentralisation or its smart contracts, but rather by underlying issues in Terra's tokenomic design. The rapid price decline that occurred can be attributed to investor behaviour, with the flaw in Terra's design exacerbating the situation. It is crucial to differentiate between the platform and its design flaw, as blaming DeFi as a whole can not be justified.

A specific case in point is the Anchor protocol, which promised investors a 'savings account' with perpetually high yields of 19-21%. Coupled with the ease of minting UST, this created an attractive but inherently unsustainable situation. However, it is essential to recognise that while this incident took place within the DeFi space, the latter was not the root cause for the price crash.

In our opinion, even with certain regulatory measures in place, the same result would have unfolded, albeit with potentially lesser magnitude. Thus, it is crucial to approach the Terra-Luna crash as a lesson in refining tokenomic design and implementing appropriate regulatory frameworks rather than blaming DeFi as a whole or using it to advocate for stricter regulatory frameworks in regards to decentralised applications.

Discussion point 5 - DeFi trading protocol market rules



Discussion point 5 – DeFi trading protocol market rules

In the context of developing rules for DeFi trading protocols, it could be envisaged that requirements apply to the code of smart contracts, whereby it be made translatable into non-technical language, so that it can be read, reviewed and approved by regulators. This would ensure proper disclosure of a DeFi trading protocol's market rules, potentially enabling better compliance with them.

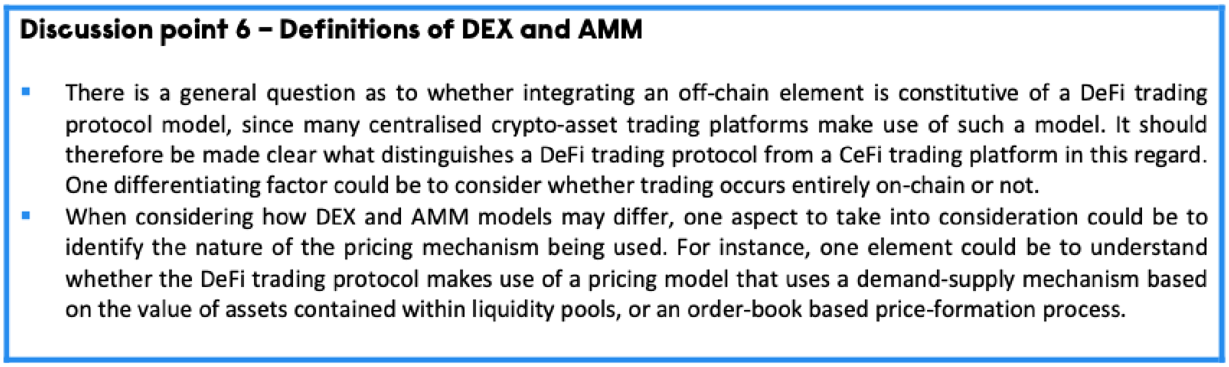
In discussion point 5, the AMF raises the question of whether regulators should be able to read, review and approve smart contracts in a translated, non-technical form. We believe that such pre-approval requirements would significantly stifle innovation.

Firstly, it may be difficult to get regulators to approve smart contracts as they may not be familiar with the technology or the specific requirements in each case, including the functions of the underlying technology. Regulators may also not have the resources to review smart contracts in a timely manner or to review changes that may need to be introduced urgently, e.g. due to vulnerabilities or changes in the underlying technology. The process of translating smart contracts into non-technical documents also raises significant questions, e.g. regarding the accuracy and completeness of the translations and the expertise required to write and review such documents. In addition, several questions would arise regarding such approvals by regulators, including questions about enforcement, jurisdiction and the liability of a regulator who approved a smart contract, which later turns out to be defective. Mandating that smart contracts be read, reviewed and approved by regulators would be inappropriate and a significant restriction of the market.

While it is true that DeFi trading protocols currently operate in an unregulated market, it does not imply a heightened risk of failures or illicit activity. The absence of a regulatory framework does not necessarily equate to an environment rife with market abuse, manipulation, or fraud. In fact, the decentralised nature of DeFi allows for a unique form of self-regulation through transparency, auditability and community-driven efforts to review code. The industry is actively working towards standardisation and certification processes to establish best practices and promote transparency and accountability. Through initiatives like audits, code reviews, and governance mechanisms, the DeFi community is able to address security and compliance concerns.

Furthermore, it is important to acknowledge that the complexity of DeFi protocols may pose challenges for participants, particularly those with limited knowledge or experience in blockchain technology. However, this is not exclusive to DeFi but applies to any innovative and evolving sector. Efforts are being made to enhance user education and provide clear and accessible information about the risks associated with participating in DeFi as well as making it more user friendly. Ensuring financial literacy and understanding the risks is crucial for making informed financial decisions and avoiding negative outcomes.

Discussion point 6 - Definitions of DEX and AMM



Discussion point 6 – Definitions of DEX and AMM

- There is a general question as to whether integrating an off-chain element is constitutive of a DeFi trading protocol model, since many centralised crypto-asset trading platforms make use of such a model. It should therefore be made clear what distinguishes a DeFi trading protocol from a CeFi trading platform in this regard. One differentiating factor could be to consider whether trading occurs entirely on-chain or not.
- When considering how DEX and AMM models may differ, one aspect to take into consideration could be to identify the nature of the pricing mechanism being used. For instance, one element could be to understand whether the DeFi trading protocol makes use of a pricing model that uses a demand-supply mechanism based on the value of assets contained within liquidity pools, or an order-book based price-formation process.

In response to discussion point 6, definitions of DEX and AMM, we would like to highlight that several types of DeFi protocols and composition can be developed with the help of distributed ledger technology.

One example is Synthetix, which operates as a lending protocol, a derivative market, a synthetic asset issuer, and a decentralised exchange (DEX) all at once. Uniswap is another example of a multi-functional DeFi protocol. Initially launched as an Automated Market Maker (AMM), the subsequent development of UniswapX transformed it into a meta-DEX aggregator. This additional feature uses the DLT application layer to connect various DEXs, enhancing liquidity and offering users optimal trading conditions. Furthermore, Uniswap has branched out to include an NFT marketplace, demonstrating the broad spectrum of services that a single DeFi protocol can offer.

Other DeFi protocols, such as Convex or Aura, are classified as yield protocols by DefiLlama. However, within this category, there is considerable diversity in terms of mechanism design and offered services. Some yield protocols focus on optimising yield farming strategies, while others provide auto-compounding functions or operate as yield aggregators.

Off-Chain Elements and DeFi vs CeFi

From an algorithmic standpoint, constant function automated market makers (CFMMs) like Uniswap v2, Balancer, and Curve do not require off-chain components, which sets them apart from both order book-based decentralised exchanges (DEXs) and centralised exchanges (CeFis). In contrast, order book-based DEXs and CeFis do require off-chain components and are thus subject to the same rules and regulations that market makers have in centralised exchanges.

Differentiating Factors

One significant distinction between DeFi and CeFi arises due to the role of arbitrageurs. Currently, most trades occur off-chain first, and are propagated on-chain through centralised-DEX (CEX-DEX) arbitrageurs. However, this model tends to favour centralisation, as only a few players who have privileged access to trading fee tiers on centralised exchanges can effectively carry out CEX-DEX arbitrage. This lack of transparency and potential for under-the-table deals between centralised exchanges and arbitrageurs conflicts with the DeFi ethos of open, permissionless, and transparent financial interactions.

Dissimilar to conventional exchanges, decentralised Exchanges (DEXs) typically do not operate through order books. Instead, the majority of these platforms, including but not limited to Curve, Uniswap, SushiSwap, and Balancer, function as Constant Function Market Makers (CFMMs) - a protocol that maintains a pool of various crypto assets which are supplied by individuals or entities known as liquidity providers. Participants on the platform can propose a trade by offering a specific bundle of assets to the CFMM in exchange for a different set of assets. Upon acceptance of the trade, the offered assets are added to the pool, and the received assets are withdrawn from them. Each successful transaction is subject to a minor fee, the proceeds of which are distributed among liquidity providers in proportion to their contributed liquidity.

The fundamental governing principle of a CFMM is a specific rule that dictates the acceptance or rejection of a proposed trade *(G.Ageris, Constant Function Market Makers: Multi-asset Trades via Convex Optimization)*. This rule is founded upon a trading function that considers both the specifics of the proposed trade and the current pool of assets held by the CFMM. The trade is deemed acceptable if the value of this function, post-trade and after accounting for the transaction fee, equals the value of the function before the trade; in other words, the function remains constant.

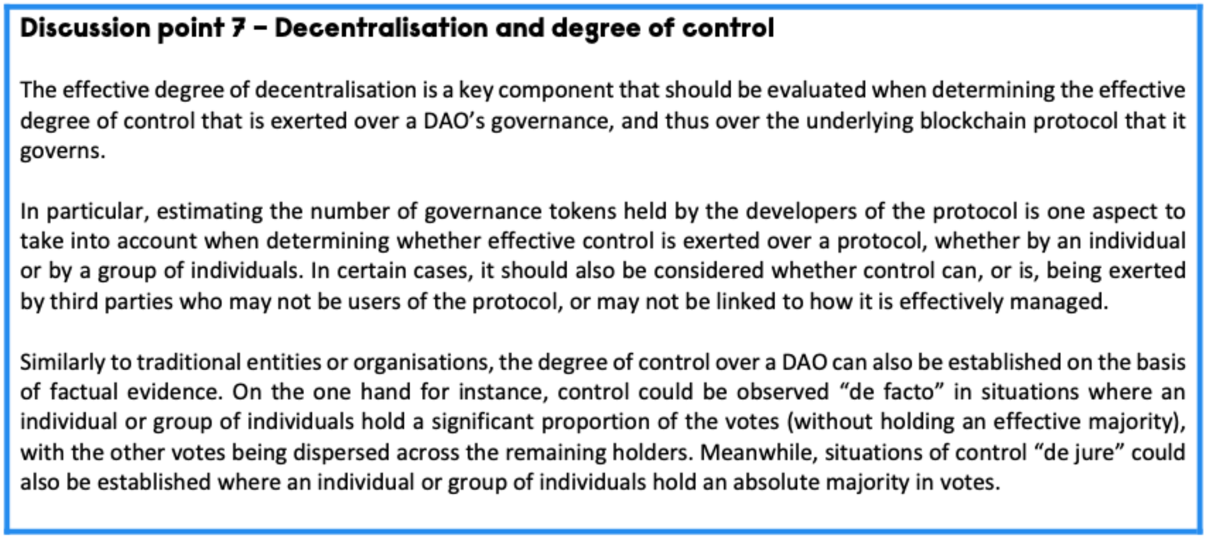
Pricing Mechanisms

In terms of pricing, CFMMs such as Uniswap v2, Balancer, and Curve, operate on a transparent and predictable pricing model determined by the supply and demand influence on the bonding curve. This prevents manipulation from the market maker's side. However, in today's trading landscape, prices are first set by the trading venue with the largest order flow. Once a trade is executed on this dominant market, arbitrageurs then propagate these spot prices across other trading venues. Therefore, CFMMs rely on arbitrageurs to update spot prices across all markets, which ties them to centralised exchanges.

Future Considerations

As on-chain trading volumes increase, pricing power will shift more towards on-chain trading venues. While on-chain order book models may potentially dominate in terms of volume, Constant Function market making algorithms will bring a greater level of transparency to market operations compared to the current centralised pricing models (which exist on Cefi and Defi orderbook models). However, we must carefully consider the balance between decentralisation and operational efficiency in the design of DeFi protocols.

Discussion point 7 - Decentralisation and degree of control



Discussion point 7 – Decentralisation and degree of control

The effective degree of decentralisation is a key component that should be evaluated when determining the effective degree of control that is exerted over a DAO's governance, and thus over the underlying blockchain protocol that it governs.

In particular, estimating the number of governance tokens held by the developers of the protocol is one aspect to take into account when determining whether effective control is exerted over a protocol, whether by an individual or by a group of individuals. In certain cases, it should also be considered whether control can, or is, being exerted by third parties who may not be users of the protocol, or may not be linked to how it is effectively managed.

Similarly to traditional entities or organisations, the degree of control over a DAO can also be established on the basis of factual evidence. On the one hand for instance, control could be observed "de facto" in situations where an individual or group of individuals hold a significant proportion of the votes (without holding an effective majority), with the other votes being dispersed across the remaining holders. Meanwhile, situations of control "de jure" could also be established where an individual or group of individuals hold an absolute majority in votes.

In relation to discussion point 7, decentralisation and degree of control, it is important to recognise that the concept of DAOs has continued to evolve since Vitalik Buterin first described the concept of a Decentralised Autonomous Organisation (DAO). This development has led to several variations and different interpretations of the term.

A DAO can be described as an organisation operating on a blockchain network, where decision-making processes and governance mechanisms are automated through smart contracts. DAOs function in a decentralised manner, without relying on traditional hierarchical structures or centralised control. The rules and operations of a DAO are pre-defined and implemented through code, enabling transparent and trustless interactions among participants.

One widely accepted definition of a DAO, as presented in the "DAO Stack Whitepaper" by DAOstack, a prominent platform for creating and managing DAOs, describes it as "an internet-native, open-source organisation governed by smart contracts and run by rules encoded on a blockchain." This definition acknowledges the decentralised nature of DAOs, their reliance on smart contract technology, and their ability to operate based on predefined rules implemented on the blockchain.

Decentralisation and degree of control

While it is true that DeFi trading protocols may face governance risks, it is important to recognise that these risks are not unique to DeFi. Similar issues exist within the more traditional financial system, where bad actors can exploit their knowledge and position to manipulate prices or execute trades before others. In both decentralised and centralised systems, there might always be individuals seeking to gain an unfair advantage. However, what sets DeFi apart is the potential for increased transparency and the ability to implement innovative solutions to mitigate these risks. The blockchain technology underlying DeFi protocols offer a level of transparency and immutability that can deter such unethical behaviour, as all transactions are recorded and visible on the public ledger. Additionally, the open and community-driven nature of DeFi governance allows for collective decision-making and the implementation of measures to address governance risks. While challenges may still exist, it is crucial to recognise that DeFi is actively exploring ways to enhance governance and mitigate risks, just as the traditional financial system continues to evolve to address its own shortcomings.

In fully decentralised systems, risks to users and market integrity stem largely from technological and cyber vulnerabilities, or risks from integration with centralised systems. This is different from traditional financial systems, where risks primarily arise from data concentration or human errors. "Technology risk" pertains to inherent code safety concerns due to errors and bugs, while "cyber risk" refers to potential protocol loopholes that could be exploited. In traditional finance, a user can lose assets due to their misuse by another party. In decentralised systems, asset loss could occur due to a software bug. Despite the similar risk of loss, the regulatory approaches should differ. In this regard, e.g. Polygon Labs advocates for “different source of risk, same regulatory outcome” approach.

Recently developed innovative compliance tools and solutions could be employed to achieve regulatory outcomes similar to those in traditional financial systems. ERC 7265 is a new standard proposed by a group of Ethereum community members that would enable a "circuit breaker," allowing DeFi protocols to easily add a back-stop in their smart contracts that stops tokens before they leave the contracts in the event of a hack. Moreover, implementing on-chain identity solutions such as Soul-Bound Tokens coupled with an off-chain decentralised identifier (DID) based system could both mitigate pseudonymity risks that can jeopardise sybil resistance (e.g. through vampire attacks), while also leading to new forms of lending based on attribution verification.

There is also additional work being done to create permissionless, nested sub-DAO or ‘para-DAO’ ecosystems such as Maker’s End Game model. Broadly, End Game will enable sub-DAO’s to specialise in different areas and operate their own governance processes. This will help to delegate responsibilities between governance, collateral allocation and operational efficiency. The introduction of Artificial Intelligence (AI) tools will aid in overall governance improvement, with the eventual introduction of delegated voter incentives through consensus staking. Introducing autonomous governance through AI tooling and introduces a new spectrum of open questions related to the degree of control within DAO systems, especially in concert with ‘nested’ environments such as sub-DAOs. This highlights the unique challenge of trying to establish regulatory touchpoints for decentralised systems that may require case-by-case assessment, rather than a boilerplate regulatory framework.

Conclusion

Decentralised Finance is an iterative process undergoing constant change and development. Perhaps the most challenging perspective when compared to the more traditional financial system is its pace of innovation. DeFi is able to iterate parabolically because it is not saddled with technological debt and the need to create channels between old and new systems. Also, from a regulatory standpoint this makes it difficult to ring fence because what we mean by ‘DeFi’ today could be completely different in years to come. In contrast, although there have been innovative solutions in the more traditional financial system, they have been characterised by a predictable ontology, rooted in familiar centralised vectors, allowing regulators to determine rules for financial products and services that in principle, have not changed that drastically. There has been more financial innovation in the span of DeFi existing as a paradigm than there has been from the creation of the mutual fund to the era of high-frequency trading.

That being said, DeFi is still by and large a self contained ecosystem, dwarfed in comparison to legacy capital markets. However, DeFi’s bottom-up approach to financial innovation has produced a blossoming and vibrant community driven approach to value creation. The unique value proposition that public permissionless blockchains, coupled with smart contract technology offer means that DeFi growth may eventually become systemic and will need a regulatory response. In order to promote healthy and responsible innovation, DeFi is working on leveraging this bottom-up approach to introduce self-correcting mechanisms aimed at keeping consumers safe. Smart contracts are becoming more robust, governance processes are being optimised, products fine-tuned and ecosystems algorithmically ring-fenced against endogenous risks. On-chain monitoring and analytics are able to provide a birds-eye view of fund flows, attack vectors and pin-point the build-up of potentially systemic events. These metrics are powerful tools that could also help regulators leverage smart-contract technology to draft robust frameworks that still accommodate innovation and experimentation.

In the more traditional financial system, retail users and institutional users engage along different lines, with different rules applying to institutions especially. It may be the case that we see the same parallelisms exist in the future of DeFi. There is growing talk of a ‘permissioned’ DeFi ecosystem that could allow regulated institutional players to access the permissioned layer of permissionless applications and protocols, governed in a way that adheres to the prudential responsibilities of those entities while leveraging the underlying technology stack to access innovative financial products and services. Just as central bankers have opined in the past that central banks would accept “neither an outcome where central bank money would crowd out private initiative nor an outcome where central bank money is phased out by a market mechanism”, it would be equally onerous to suggest replacing public permissionless blockchains wholesale with private permissioned ones.

Composability and interoperability sitting at the heart of DeFi mechanics would provide for a future where the innovation curve could still be pushed along the frontiers of permissionless blockchains, and integrated based on carefully thought out rules for regulated players to access that innovation on equal footing. Suggesting regulators either pre-approve smart contracts before they are deployed or signal that only permissioned blockchains should be permitted introduces serious market inefficiencies and operational challenges at best and innovation collapse, while breaching the principles of technology neutrality at worst. As the ecosystem continues to mature, education both for policy makers and investors will be key to ensuring that DeFi growth is sustainable and policy measures reinforce rather than reduce development and value creation.