Reply to the Discussion Paper: *'Decentralised' or 'Disintermediated' finance: What regulatory response?*

This is a joint response led by the IOTA Foundation, the European Blockchain Association (EBA), and the European Crypto Initiative (EUCI), **with the direct contributions of them, its members and communities, including the members of** INATBA: University of Glasgow, University of Pavia, Cornell University, Research Group in Digitalization and Business Law at Rey Juan Carlos University (DYDEM), La Caisse Des Dépôts, Folks Finance, EthicHub, Tokeny, FeverTokens, AMLBot, Callisto Enterprise, and the members of the expert panel of the EUBOF Iwona Karasek-Wojciechowicz, associate professor and Dr Marcin Pawlowski Iñigo Moré Research Assistant Professor Jagiellonian University; Amit Joshi, Founder HashPrix; Matthew Niemerg, Ph.D. President Aleph Zero Foundation; and, Teaching Assistant University of Chicago Daniel Szego, DLT Architect. **With the support of** the Global Blockchain Business Council (GBBC)

The organizations listed above came together to respond to questions presented in the paper "'Decentralised' or 'Disintermediated' finance: what regulatory response?" written by the Fintech Innovation Hub of the Autorité de Contrôle Prudential et de Résolution (ACPR). Below are our answers.

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

Q1: Do you have comments on the definition of decentralized finance (DeFi) used in the paper? Does the document correctly reflect the real level of decentralization of services?

The document describes the various processes that a decentralized application (dApp) undergoes in order to achieve true decentralization. DApps usually start as highly centralized entities in terms of key management by a core team and only evolve later into decentralized autonomous organizations (DAOs).

In order to define Decentralized Finance (DeFi), it is important to review what has been proposed and understood as its key characteristics by different entities and organizations. The table below presents DeFi definitions used by different institutions.

Paper	**DeFi Definition**
Research Paper. Technical University of Munich & Frankfurt School of Finance and Management	DeFi refers to a **finance protocol** built with **smart contracts** that are 'trustless' (i.e., functioning without intermediaries or third parties) and developed on permissionless, public blockchains.

Decentralized Finance June 2022	
DG FISMA June 2022	Applications in DeFi rely on **automated protocols to produce financial services** including exchanges, credit, derivatives, and portfolio management. In contrast to traditional venues, the specificity of DeFi is that protocols are (i) encoded in universally accessible public **digital contracts** and (ii) maintained by an **open pool of pseudonymous agents** rather than a unique legal entity.
European Blockchain Association	DeFi is a catch-all term used to describe a range of **on-chain activities and services** such as borrowing, lending, derivatives, deposit taking, custody, and exchanges that **use distributed ledgers to connect buyers and sellers** directly without the need for intermediaries. These services are performed by **self-executing smart contracts**, with **no single source of truth, point of failure, or authority** charged with changing the underlying data. Therefore, smart contracts shift counterparty risk away from intermediaries. The open-source software at the root of the DeFi ecosystem and the inherently contestable nature of DeFi as a result of smart contracts enables composability across different platforms and the creation of entirely new ones. It is possible to buy a stablecoin on a decentralized exchange (DEX) and move it to a lending platform to earn interest while additionally leveraging these interest-bearing instruments in an automated market maker (AMM). DeFi is also inherently **cross-border**, existing as a digitally native and jurisdictionally agnostic **ecosystem that is on 24/7** with users around the world.
EUBOF report	DeFi represents a **paradigmatic shift** in financial services provisioning and promises to be one of the most disruptive applications of **blockchain-fuelled decentralization**. The ability to transact peer-to-peer (P2P), i.e. without intermediaries) remotely and trustless (at least as far as trusting one's counterparty is concerned) is a novel phenomenon that is still maturing. The plethora of DeFi applications already in existence may just be the tip of the iceberg compared to the wave of innovation we expect in the near future.
Bank for International Settings (BIS) January 2023	DeFi is a new **financial paradigm** that leverages **distributed ledger technology (DLT)** to offer services such as lending, investing, or exchanging crypto assets **without relying on a traditional centralized intermediary**. A range of DeFi protocols

	implements these services as a suite of **smart contracts**, i.e., software programs that encode the logic of conventional financial operations. Instead of transacting with a counterparty, DeFi users thus interact with software programs that pool the resources of other DeFi users to maintain control over their funds.
Financial Stability Board (FSB) February 2023	DeFi is an umbrella term commonly used to describe a **variety of services in crypto-asset markets** that aim to **replicate** some functions of the **traditional financial system (TradFi)** while seemingly **disintermediating** their provision and **decentralizing** their governance.

When looking at the different definitions, shared concepts emerge. These include:

- DeFi can be described as a financial system that operates in a decentralized manner, without the need for intermediaries.
- DeFi is based on technological innovations, specifically in the form of distributed ledger technology and smart contracts.
- DeFi delivers absolute financial freedom, enabling universal access and self-reliance on the part of the user.
- DeFi operates on the assumption of trustless interactions.

The current definition provided by the ACPR excludes key components identified by other institutions and organizations, such as the authority of the users to control their own assets; the assumption of system-based trusted interactions without relying on intermediaries; and the need for a governance structure, which is mentioned but not considered as a key component.

Moreover, when looking at the industry's understanding of DeFi, a consultation run by the IOTA Foundation featuring contributions from 141 participants (43% from the crypto community and 15% representing VC/investors) reveals that most respondents define DeFi as a new financial system (44%) and often cite this new system's opposition to centralization. Almost one-third of respondents define DeFi as the ability to be financially autonomous (28%), followed by a focus on the involvement of new technologies (18%).

Looking at this survey's results, it is clear that the industry sees DeFi as representing an emerging financial system that offers a wide range of functionalities beyond those found in traditional finance, while also emphasizing the importance of user autonomy. However, it is worth noting that the definition proposed by ACPR misses these essential aspects.

Furthermore, it is important to comment on Box 1 of the report, which fails to provide clarity on these novel concepts. Rather, it presents a misleading and simplified view of them.

1. When discussing whether DeFi represents "decentralized" or "disintermediated" finance, it is important to understand that these are two distinct concepts, although they are often interconnected within the context of DeFi.

   On the one hand, *decentralization* refers to the distribution of control and decision-making across a network of participants rather than being concentrated in a single entity or authority. In DeFi, decentralization primarily involves the use of blockchain technology and smart contracts to create financial applications that operate without intermediaries like banks or other traditional financial institutions. This approach enhances transparency, security, and accessibility for users.

   On the other hand, *disintermediation* refers to the removal or reduction of intermediaries in transactions or processes, typically achieved through the use of technological advancements. In DeFi, disintermediation refers to the elimination of intermediaries such as banks, brokers, or other financial institutions, enabling direct interaction between users and the DeFi protocol.

   While decentralization and disintermediation are related concepts, they are not interchangeable. Decentralization refers to the distribution of control, while disintermediation refers to the elimination or reduction of intermediaries. However, in DeFi, these concepts often go hand in hand since blockchain technology and smart contracts enable both decentralization and disintermediation simultaneously.

   Therefore, DeFi is inherently both decentralized and, in its purest form, disintermediated. It would be unfair to label DeFi as merely disintermediated since its underlying objective and philosophy have always been focused on decentralization. Moreover, DeFi also encompasses disintermediation as part of its philosophy as the goal is for transactions among market participants to occur fully peer-to-peer without intermediaries. As such, DeFi protocols aggregate the offers of multiple market participants (within the same marketplace) by using DLTs with built-in transparent and open accounting.

   DeFi achieves decentralization through various means, such as decentralized infrastructure, smart contracts, open-source code, community governance, and decentralized liquidity. These features empower DeFi protocols to function without intermediaries, resulting in increased transparency, reduced costs, and greater accessibility for users. By leveraging blockchain technology, DeFi can create financial applications that are resistant to censorship, tampering, and control by any single entity.

2. The criticism of the term "smart contract" in the report has some validity, as it can be misleading. However, it is important to clarify that smart contracts are indeed "smart" in the sense that they can execute code based on predetermined conditions. Although

they do not adapt their behavior over time, they are designed to handle complex logic based on predefined conditions.

The statement that smart contracts are not necessarily contracts in a legal sense is partially incorrect. Essentially, smart contracts are self-executing computer programs that include self-executing clauses that are automatically triggered based on specific events or conditions, automatically enforcing the terms of an agreement between parties. The legal status of smart contracts is a complex and evolving issue that varies across jurisdictions. While they may not always meet the legal requirements of a traditional contract, such as being in writing or signed by all parties, they can be designed to mimic the terms and conditions of a traditional legal contract and have the potential to provide a similar level of legal certainty.

Several jurisdictions have taken steps to recognize the legal validity of smart contracts. For example, the Arizona Electronic Transactions Act (Section 44-7031) defines a smart contract as "an event-driven program that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over, and instruct transfer of, assets on that ledger." This law recognizes the legal validity of smart contracts and states that "a contract relating to a transaction may not be denied legal effect, the validity or enforceability solely because that contract contains a smart contract term." Another example is the Swiss Federal Council, which issued a report in 2018 on the legal framework for blockchain and distributed ledger technology. The report established that a smart contract has various characteristics that could influence its qualification and legal effects and discussed some of the potential challenges when applying traditional civil law to them. These two are examples of how different jurisdictions worldwide are taking steps and exploring how to recognize smart contracts as legally valid documents.

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

DeFi is a rapidly evolving sector that has the potential to revolutionize the financial industry by bringing transparency and accessibility to financial services. It is built on blockchain technology, which enables a transparent public ledger that cannot be manipulated, allowing individuals to monitor every transaction. This transparency helps to expose illegal or questionable practices, which can improve fraud protection and deliver more democracy to the financial industry.

The potential applications of DeFi are vast and include cross-chain interoperability, privacy and security, DAOs, real-world asset tokenization, and decentralized identity.

Tokenization involves representing real-world assets on a blockchain, opening up opportunities to access efficient, cost-effective, and real-time financial services without counterparty risks.

Tokenization has gained significant momentum in recent years, with major institutions recognizing its potential and initiating their own tokenization projects.

Real-world assets are set to dominate DeFi use cases, thanks to the emergence of permissioned DeFi and data oracles that address two critical challenges: compliance and asset reliability. DeFi services can restrict access to eligible users by leveraging self-sovereign identities, such as ONCHAINID, while data oracles can provide on-chain proofs that guarantee the existence of the underlying assets, both physically and legally. These mechanisms will enable the use of real-world assets in all kinds of DeFi use cases, such as collateralization, trading, yield farming, and diversifying portfolios.

Examples of such applications include:

- DuneOn Dune: analytic dashboards to monitor exactly what happens in every protocol, on every address that exists:https://dune.com/home
- Artemis is building an analytics platform that aggregates all the crypto metrics: https://app.artemis.xyz/dashboard
- Glassnode provides on-chain and financial metrics, charts, data, and insights: ttps://twitter.com/glassnode
- Dashboards for AAVe lending protocol: https://dune.com/browse/dashboards?q=aave
- Proof of reserves of Cexes: https://dune.com/21shares_research/cexs-proof-of-reserve
- Dex Metrics:https://dune.com/hagaetc/dex-metrics
- Tracking of Wallets that received airdrops https://dune.com/cypherpepe/airdrops-and-wallets
- ETH staking and validator distribution https://dune.com/hildobby/eth2-staking
- Whale wallet tracking https://dune.com/defimochi/token-god-mode
- Deposit tokens, or tokenized commercial bank deposits. https://www.swissbanking.ch/_Resources/Persistent/9/4/1/1/941178de59b98030206fc15ac8c99012f65df30b/SBA_The_Deposit_Token_EN_2023.pdf

As DeFi evolves, products and services will become compliant and secure with the appropriate auditing and monitoring, ensuring the safety and privacy of users. As the technology matures and projects are tested and examined thoroughly, DeFi will play an integral and instrumental role in the evolution of the metaverse, facilitating transactions between the virtual and physical worlds.

Furthermore, DeFi has the potential to democratize financial services and foster financial inclusion, making previously exclusive financial products and services accessible to anyone

with internet access. It has the capacity to create a world where financial services are available to all, regardless of their background or socioeconomic status.

Making definitive predictions about the trajectory of DeFi s challenging. However, by providing a supportive ecosystem that encourages experimentation and technological advancements, we can eagerly await the innovative possibilities that can unfold in the DeFi space.

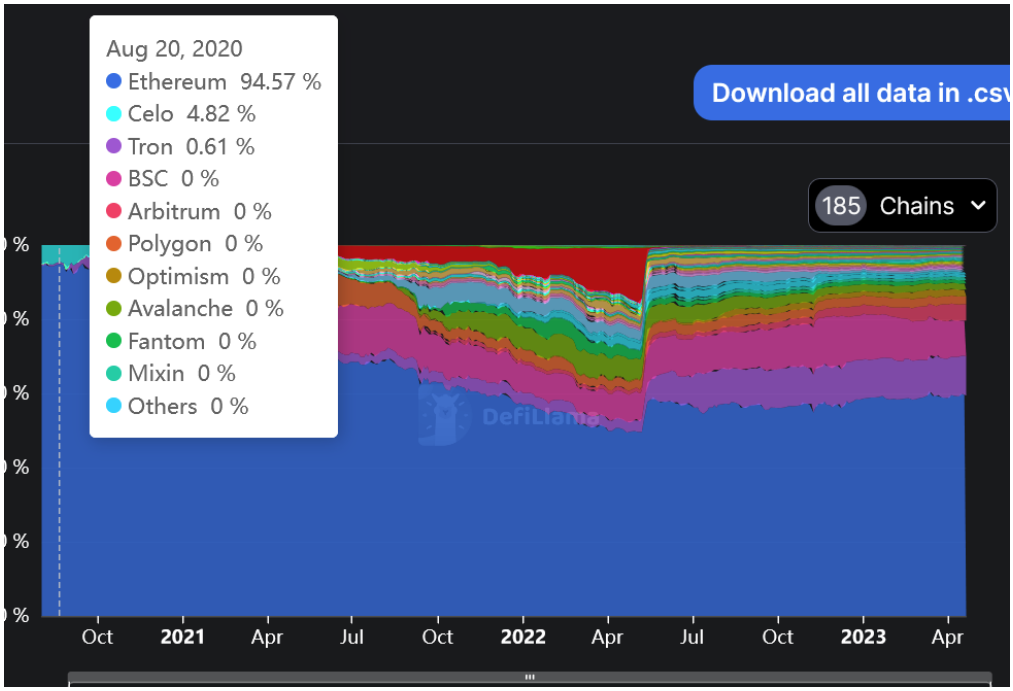
Q3: What do you think about the concentration phenomena described in Section 1-5 of this document?

The governance of DeFi platforms and dApps primarily rests with their founders and teams. Their control is often limited due to the inherently decentralized nature of DeFi platforms, which operate independently of team or token governance. While DeFi governance includes some aspects of centralization (like the distribution of power through tokens that are not very different from traditional stocks), it is fully open, allowing everyone to participate in decision-making based on their voting rights and weight. These decisions can encompass core protocol functionalities.

The degree of concentration cannot and should not be evaluated based on the type of protocol that is used for developing the DeFi apps. Users naturally prefer certain applications or networks, which is typical market behavior. Consumers will always choose the service that gives them the best value, the best experience, the strongest feeling of safety, the highest rewards, and so on. Once competition arises, users will shift to different providers and other services, as it should be in an open market.

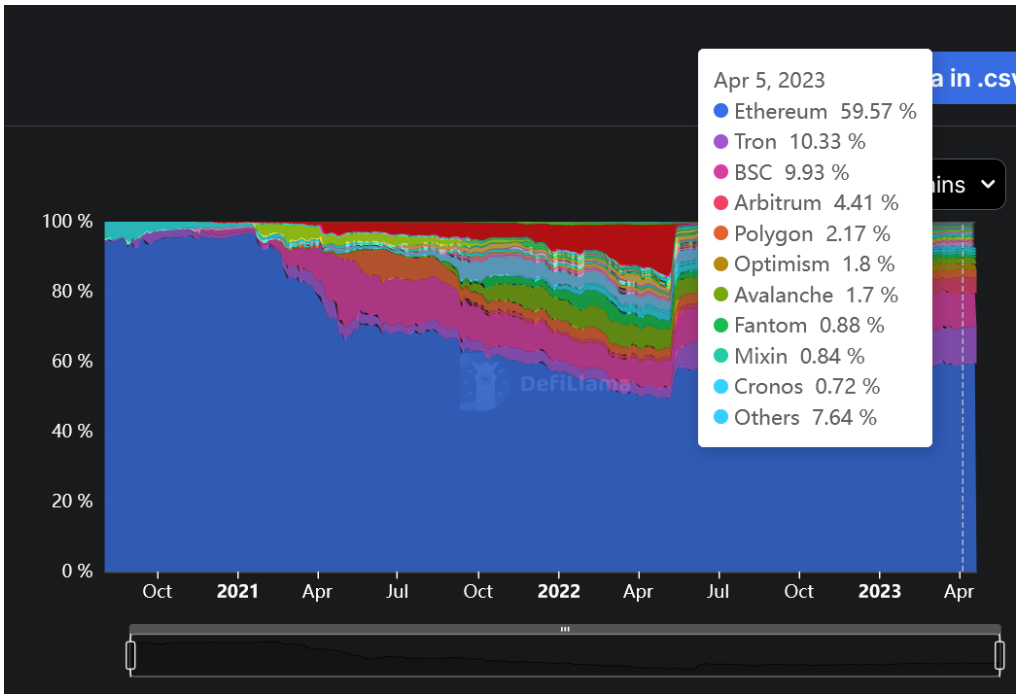
Since DeFi is still in its early stages, widespread adoption has yet to be achieved by most protocols and platforms. Consequently, a few well-established projects currently dominate the market, while smaller-scale projects struggle to gain traction: this is known as the concentration effect. Ethereum, as the pioneer of DeFi, naturally became the foundation for the initial apps. However, as new opportunities emerged, the % market share of DeFi users and the total value locked (TVL) in ETH has consistently decreased. Moreover, it is worth noting that the bear market of the past year has also slowed down the generation of new projects. Now, with the advent of Layer 2 optimistic rollups, a significant shift is expected in the next bull market from ETH to other Layer 2 solutions like Arbitrum and Optimism.

- 94% of Defi was built on Ethereum in 2020.



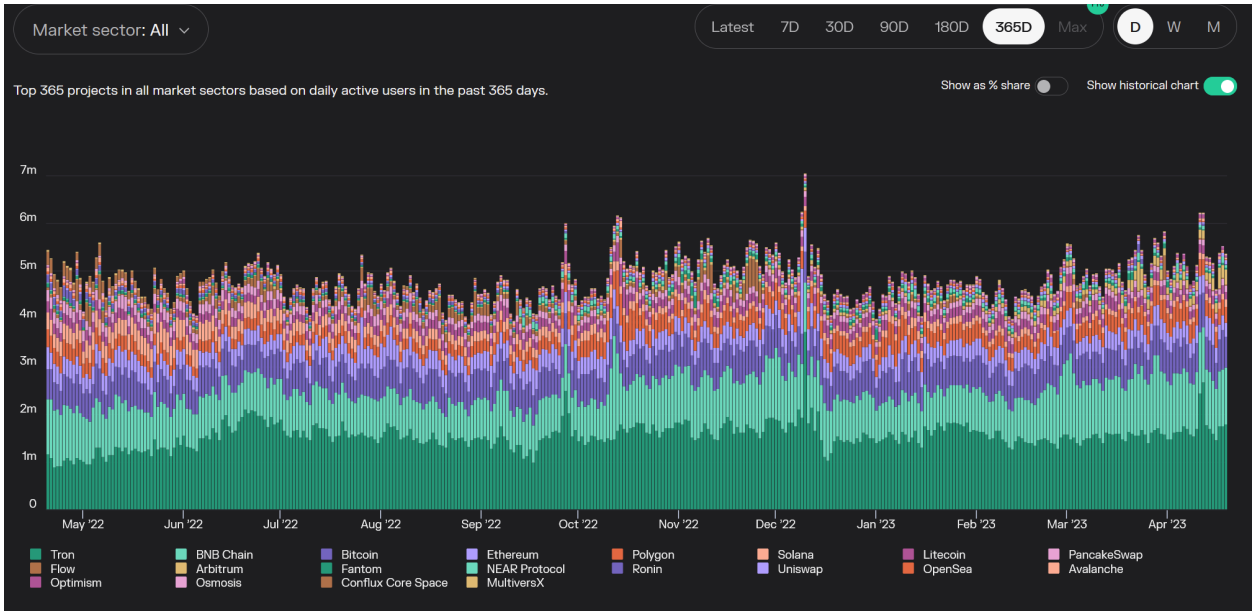
Source https://defillama.com/chains

- While 59.57% was built on Ethereum by April 2023.



Source https://defillama.com/chains

Moreover, by comparing daily active users, we can see that the most used chain is not ETH but Tron.



Source: https://tokenterminal.com/terminal?panel=active_users

Concentration has both positive and negative effects on DeFi. On the positive side, concentration can bring stability and attract new users and investors who are interested in joining well-established and trusted projects. On the negative side, concentration can pose a significant hurdle to innovation and create difficulties for smaller yet promising projects or ideas that struggle to compete with well-established players.

Concentration phenomena in DeFi can be attributed to several factors:

- Network effect: This occurs when the value of a system or platform increases as more users adopt it. In DeFi, larger projects with a substantial user base and liquidity pools become more appealing to new users and potential investors, creating a virtuous cycle that solidifies their dominance.

- Liquidity pools: These pools allow users to contribute funds that facilitate trades on the platform. Concentration arises when users increasingly contribute liquidity to a specific pool, leading to a small number of key users or large players dominating the pool. This decreases platform decentralization and may enhance the influence of these players.

- Governance tokens: Ownership of governance tokens corresponds to the number of votes a user has in the decision-making process. Concentration occurs when a small group of users wields increased power and control over the protocol's decision-making, leading to a concentration of influence.

- Smart contract vulnerabilities: Weaknesses in smart contract code present opportunities for attackers to manipulate the code to extract funds or create fake tokens, leading to a loss of funds for legitimate users. This leads to a “mass exit” of users from the affected protocol towards other, more secure protocols, creating concentration. If vulnerabilities are widespread across multiple protocols, concentration can increase further.

- Limited interoperability: DeFi protocols face challenges in seamlessly communicating and exchanging value with one another due to a lack of standardized protocols and infrastructure. This limitation restricts access for new players, as established protocols have gained traction with users, contributing to concentration.

To conclude, while the concentration effect is significant within specific DeFi protocols and platforms, it should not overshadow the overall decentralized nature of the DeFi industry. DeFi's mission to create a fairer and more inclusive financial system is rooted in openness, accessibility, and decentralization, which are not undermined by concentration effects in specific cases.

As the DeFi industry continues to expand, the development of more interoperable protocols and the emergence of new Layer 2 solutions will help alleviate the concentration effect mentioned in the report. However, fostering an environment conducive to innovation and start-ups in DeFi requires ongoing efforts to establish a regulatory framework that supports innovation, promotes competition, and safeguards user interests. Only through these measures can we encourage the development of a diverse and decentralized DeFi ecosystem that benefits all users. Moreover, it is important to consider that initially, most projects on the DLT space tend to have a centralized structure, but over time, the ownership of governance tokens gradually extends to a larger number of wallets. It is common for technology projects to follow a centralized approach during the initial five years of their lifecycle. However, this dynamic typically shifts as they progress towards becoming publicly accessible. In the case of the crypto industry, this transition has yet to occur due to its relatively small size and youthful stage of development.

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

It is important to note the difference between cold and hot wallets. Cold wallets are completely offline and can be software, hardware, or a paper wallet, whereas hot wallets are connected to the internet and used for interaction with digital keys. Hardware wallets can also be hot wallets but require explicit user interaction to sign requests and never reveal the keys to the outside world.

It is also important to consider the different stakeholders involved in DeFi, including validators, users, borrowers, arbitrators, stakers, traders, liquidity providers, and liquidators. Creating a

specific box for stakeholders can provide clarity on the involved parties and their roles within the DeFi ecosystem. Overall, the representation is clear, but it would be helpful to clarify that decentralized applications can be developed on Layer 2.

Moreover, it is recommended to review the representation of DeFi using the layered DeFi stack, which was originally developed by the EU Blockchain Observatory and Forum. The layered Stack could serve as a valuable foundation for semantic representation and analysis, potentially augmented with additional cross-chain elements. This approach offers several advantages. Firstly, it is widely recognized and utilized in the literature. Secondly, its layered architecture provides a solid framework for conducting cross-layer dependency and risk analysis, enabling a more comprehensive understanding of the DeFi ecosystem. Incorporating the layered DeFi Stack into the examination of DeFi would enhance the analysis of potential interdependencies and risks within the system.

Part 2: Risks associated with DeFi

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

The decentralized governance of DeFi has certain risks that have not received sufficient attention, especially market manipulation and abuse of dominance.

Market manipulation can occur when governance processes are manipulated to interfere with financial markets and stability. Existing market manipulation laws partially address this risk, but further consideration is needed to identify manipulation schemes that may appear legal when considered individually but become illegal when combined. In DeFi, governance has a significant impact on day-to-day operations and can be executed through distributed actions, making manipulation schemes more common.

Abuse of dominance, a concept in competition law, typically focuses on hindering competition through methods other than regular competitive practices. In traditional finance, interfering with internal decision-making processes may not be relevant for establishing abuse of dominance. Recognizing and addressing this form of abuse will help authorities identify and prosecute such conduct.

DeFi also faces risks related to cyber-attacks and platform interconnectedness. Due to its reliance on outsourced and cloud computing, the likelihood of cyber-attacks increases. The use of cloud computing has been associated with an increase in cyber risks across various economic sectors. The youthfulness of the industry contributes to these challenges, as regulatory solutions alone may not be sufficient to address them. The responsibility to address and resolve these issues lies primarily with the industry itself, which has the ability to adapt, innovate, and develop effective solutions over time.

Furthermore, the high interconnectedness among economic actors in DeFi amplifies systemic risks stemming from contagion. Several studies have discussed these risks and proposed methods to measure them, highlighting the need for risk management in DeFi. To mitigate these risks and enhance decentralization, new governance models are emerging.

One such approach is to randomly select individuals or entities to serve as governors through a lottery or sortition system. This approach aims to decentralize decision-making and prevent the concentration of power. Compound and Uniswap are examples of DeFi protocols that have implemented new governance models, incorporating community grants, reward programs, and sortition for representative selection.

Other innovative governance frameworks include **liquid democracy**, **quadratic voting**, **decentralized autonomous organizations** (DAOs), and **futarchy**.

- Liquid democracy combines elements of direct and representative democracy, allowing token holders to participate directly or delegate their voting power.
- Quadratic voting gives more weight to participants with a greater stake in the protocol, ensuring decisions are made by those most invested.
- DAOs automate decision-making through smart contracts controlled by token holders, eliminating the need for intermediaries.
- Futarchy combines prediction markets with decision-making, basing decisions on market signals rather than individual opinions.

While decentralized governance in DeFi introduces risks related to market manipulation, abuse of dominance, cyber-attacks, and platform interconnectedness, new governance models are emerging to address these challenges. These models aim to enhance decentralization, fairness, inclusivity, and transparency in decision-making processes within the DeFi ecosystem.

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 under consideration?

We lay out two different positions or points of view on Layer 1 and Layer 2 solutions for scalability. The first position primarily focuses on scalability concerns and the need for improved Layer 1 technologies, while the second position emphasizes the security of Layer 1 and the significance of diligence in application development, along with the value of interoperability between blockchains.

Position 1: Layer 1 solutions will ultimately provide better scalability than Layer 2 solutions. This position emphasizes the need for an alternative to Ethereum on Layer 1 that can handle higher transaction volumes. It suggests that Ethereum's roadmap, including sharding, could be a potential solution, although its implementation is still in the distant future.

Position 2: Layer 1 blockchains like Bitcoin and Ethereum offer greater security compared to Layer 2 blockchains. This position highlights the vulnerability of Layer 2 bridge infrastructure to bugs and hacking and suggests that building applications on Layer 1 are considered more secure. Moreover, Layer 2 solutions primarily serve the purpose of scaling. This position suggests that platforms should inherently embed interoperability across networks in their Layer 1 infrastructure to fully leverage the benefits of blockchain and Web 3.0. It also emphasizes the importance of diligence, rigorous code development, technology assurance tools, code auditing mechanisms, and ongoing monitoring to ensure security and reliability.

Considering both viewpoints, it is evident that both Layer 1 and Layer 2 solutions have their respective roles and considerations in addressing security issues. Layer 1 solutions are crucial for establishing a secure foundation and providing inherent security features, while Layer 2 solutions primarily facilitate interoperability between blockchains, but may introduce additional vulnerabilities through their bridge infrastructure: for example, Layer 2s can create vulnerabilities associated with centralized actors controlling the order of transactions. While some designs exclude the possibility of censorship, determining the order of transactions allows these parties (often the teams themselves) to engage in value-extracting behavior at the expense of their users.

In our view, it is important to strike a balance between scalability, security, and interoperability when designing blockchain infrastructure. Layer 1 solutions provide the necessary security foundation, while Layer 2 solutions offer opportunities for scalability and interoperability. Diligence in development practices and ongoing monitoring is essential for ensuring security in both Layer 1 and Layer 2 solutions. Ultimately, a comprehensive approach that carefully considers the strengths and limitations of both layers is vital to mitigating security issues and enhancing the overall blockchain infrastructure. It is crucial to highlight that the security of Layer 2 solutions is relatively less understood than Layer 1 security. Given that Layer 2 technology and its applications are still in their early stages, it would necessitate several years of intensive research to comprehensively analyze the security guarantees offered by Layer 2 solutions.

Q7: Do you think using roll-ups or similar solutions will result in less transparency of information for an observer?

The level of transparency in the use of roll-ups or similar solutions can vary. While rollups can enhance blockchain scalability and decrease gas fees, they may compromise the transparency of information available to external observers. This is because these solutions group transactions together before finalizing them on the main chain, making it harder to track individual transactions. This is a data availability problem: while a transaction can be observed on Layer 2, Layer 1 can only offer an assumption (in the case of optimistic rollups) or proof (in the case of ZK-rollups) that the transaction exists. When viewing an individual transaction, the risk is whether or not the Layer 2 continues to give access to the underlying data.

However, the degree of transparency also depends on the specific implementation of rollups. Some implementations, like Optimism, Polygon, and Arbitrum, offer block explorers similar to Ethereum that enable comprehensive transaction tracking. Nonetheless, analyzing off-chain activity can be more complex as oracles are required to include off-chain activities on-chain.

Furthermore, the development of other Layer 0 solutions (such as those being researched and tested at Cosmos) that may offer more flexibility but could include approaches that hide transaction data can pose issues. However, data transactions in Layer 2 solutions are not completely hidden from observation. While individual transactions may appear obfuscated when viewing only the Layer 1 blockchain, connecting to the corresponding Layer 2 that aggregates the transactions allows the observer to see individual transactions.

In summary, the level of transparency when using roll-ups or similar solutions can vary depending on the specific implementation. While some rollups may reduce transparency, others offer similar levels of transparency as Ethereum. The development of Layer 3 solutions may offer more flexibility but may also introduce transparency and data privacy challenges.

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

The description highlights the risks associated with using DeFi services and stresses the importance of users having knowledge of these risks and taking appropriate measures to protect themselves. It also highlighted the value of thoroughly testing and auditing smart contract code before deploying it.

However, it is important to acknowledge that there are additional risks specifically related to the application layer of DeFi services. One such risk is **transaction reordering**, where individuals or entities with privileged roles (e.g. miners, stakers, or validators) choose the order of transactions and exploit that position for their own benefit. Another risk is **flash loan attacks**, where attackers exploit flaws in smart contracts to borrow large sums of money and manipulate the market. Finally, there is the risk of **oracle manipulation**, where hackers manipulate external data used by smart contracts to produce unfavorable outcomes.

These risks underline the importance of designing and implementing secure DeFi protocols and taking all necessary advance measures against potential attacks. The layered DeFi stack model would also be helpful here, as it encompasses various sublayers, including the tokenization layer, protocol layer, application or display layer, and aggregation layer. Each of these layers introduces different risk factors that must be thoroughly assessed. By evaluating the risk factors associated with each individual layer, a holistic understanding of the risks within the complex application can be achieved. This approach allows for a systematic analysis of the different components and their potential vulnerabilities, enhancing the overall risk management in the DeFi ecosystem.

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

Most of the observations regarding risks to retail customers in DeFi are accurate. The complexity of these products does indeed pose challenges. However, there is a divergence of opinions within the DeFi community about who should determine whether an individual user is capable of understanding and managing these risks.

At one extreme, there is a steadfast belief within the DeFi community in the liberal free market where 'caveat emptor' serves as a guiding principle: to enter at own risk without restrictions. Moving towards the middle, there are those who believe that the company issuing the products or a supervisory authority should provide clarity on the complexity of a protocol and the products built on top of it. However, both perspectives agree that the ultimate decision on whether to engage and transact with these products and protocols should rest with the individual user. Unlike traditional finance, there is no lender of last resort (LOLR) in DeFi.

However, traditional finance has also witnessed some of the worst instances of financial misconduct of retail investors. Brokers acting as middlemen sold 'opportunities' and 'safe' investments made up of toxic products (too-big-to-fail institutions pre-GFC, faulty credits, real estate syndicated mortgage scams, etc.), costing people their livelihoods.

Financial advisors in commercial banks may use brochures and charts to persuade retail investors to invest their savings in certain products. These advisors may be motivated by their bank's range of products, which can earn them higher commissions. They might also be driven by monthly targets related to credit approvals and credit card sales, which compels them to steer clients toward meeting these quotas. This puts the advisor in a challenging position where they have to generate profits for the client, the bank, and themselves. It's an impossible trinity and, more often than not, it's the client who ends up losing out. Therefore, even with all of the facts presented up front, people are at the mercy of trusting the person who is selling them these products. However, some individuals possess the necessary knowledge and can independently conduct due diligence on investment products.
Decentralized Finance (DeFi) eliminates the need for advisors and intermediaries, as there are no broker fees or hidden motivations influencing investment pitches.

The DeFi ecosystem is built on the principles of radical transparency and self-agency. Individuals have the right to invest their savings in products of their choice. While it is important to consider warning labels in line with the concept of "buyer beware," it is ultimately up to individuals to take responsibility for their investment decisions. Without a lender of last resort (LOLR), there are limitations to the amount of warning that can be provided. The outcome, whether positive or negative, depends solely on the choices made by individuals. It is

essential for product creators to strike a balance by informing customers about the complexity of their offerings while recognizing that the final decision lies with the user.

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)?

Information asymmetries bound DeFi directly to the information structures possible through smart contracts. While these asymmetries introduce endogeneity risk as described in the paper (including omitted variables, simultaneity, and measurement error), a similar risk exists in traditional finance, where exploits related to endogeneity have been seen as strengthening market conditions.

As an example, we could compare the recent flash loan attack discovered in the Aavegotchi (GHST) price calculation method with the 1992 Sterling crisis, where currency speculators triggered a run on the British pound, forcing sterling out of the European Exchange Rate Mechanism.

Aavegotchi is an NFT platform that uses a price oracle to determine the GHST price which invokes the 'convertVGHST' function of the Vault GHST pool. The flash loan attack happened as follows:

First, the attacker deposited 294,000 aGHST (Aavegotchi's interest-bearing tokens) into the Vault GHST pool and minted 283,000 vGHST (Vault GHST tokens). In tandem, the attacker also deposited around 6.15 million USDT into the 0vix protocol, allowing them to borrow multiple assets from 0vix lending pools, using their deposited USDT as collateral. The attacker subsequently transferred 24.5 million USDC and the previously minted 283,000 GHST and borrowed ovGHST which is the 0vix version of the Aevegotchi GHST token, which spiked the total GHST supply. This price manipulation of the GHST token led to a price increase from US $1.17 to US $2.01. The attacker profited roughly US $2 million, 1.45 million USDC, and 9.5k GHST. The attacker exploiting the endogenous glitch in the Aaevegotchi price calculation method was an example of omitted variable bias leading to exploit the potential.

It could be argued that endogeneity played a similar role in 1992 in the case of the pound sterling. The European Monetary System was a multilateral adjustable exchange rate agreement where most nations of the European Economic Community (EEC) linked their currencies to prevent large fluctuations in relative value. The EMS operated by adjusting nominal and real exchange rates (exogenous and imposed on the model) and created the first European Exchange Rate Mechanism that calculated exchange rates for each currency (endogenous to the model), alongside an accounting currency, the European Currency Unit

(EMU) acting as a weighted average of the currencies of all 12 participating states (also endogenous to the model). The ERM was the logical conclusion to the 1972 Werner Report and establishment of the 'currency snake' and single currency fluctuation band of +/- 2.25%.

It could be argued that the endogenous risks posed by the exogenous influence of German monetary policy in the EMS were a feature rather than a bug of the system. Although Britain did not sign up for the ERM in 1979, Chancellor of the Exchequer Nigel Lawson followed a semi-official policy of shadowing the Deutsche Mark between 1987-88. Lawson was replaced by John Major, who convinced the British cabinet to sign the UK up to the ERM in 1990, effectively guaranteeing that the UK government would follow an economic and monetary policy preventing the exchange rate between the pound and other member currencies from fluctuating by more than 6%. The pound entered into the ERM fixed at £1 to DM 2.95, meaning that if the pound ever bottomed at the permitted range of DM 2.773 the government would have to intervene. When the Bundesbank raised rates in the early 1990s to counter inflationary effects related to excess expenditure from German reunification it put stress across the whole ERM. Britain (already suffering from inflation three times the rate of Germany in 1989, interest rates at 15%, lower labour productivity, and double deficits spurred by a depreciated US dollar) felt the compression brought by the rigidity of the commitment to fixed exchange rates under ERM. Conversely, the pound came under huge pressure from currency traders.

The British government authorized the spending of billions of pounds worth of FX reserves to prop up sterling in the currency markets but in the end not even a rise in the base rate from 10-12% was enough and Britain left ERM in September 1992. Ironically, 'Black Wednesday' was viewed by some as 'Golden Wednesday' ushering in a new economic revival and the outgoing conservatives handing Tony Blair's incoming Labour government a much stronger economy in 1997 than there was in 1992.

To summarise, it might not be a stretch to assume that both the endogenous and exogenous factors that contribute to risks in DeFi and TradFi are features rather than bugs inherent in any environment where value exchanges hands. Exploits leading to flash loan attacks have parallels in the broader context of our political economy, such as how the ERM has been described as a de-facto Deutschmark Zone (Weber 1991) because the policy adopted a fixed exchange rate with short-run effects. Like the Aevegotchi case, this was another example of omitted variable bias – the implications of which, by contrast, changed the course of history. Therefore, it would be important to also consider the relative scale/size of DeFi and its spillover effects when considering the spillover effects in the traditional financial and political system more often than not leading to tidal shifts in the global political economy.

Q11: Do you agree with the proposal concerning the regulation of stablecoins issued by DeFi protocols? (refer to Section 2-4-3: "If a decentralized 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)

No. A decentralized service that claims to create or use a crypto asset with an official currency as a reference is not concrete enough as a system that supports EMTs. E-money is characterized by the following criteria:

- It is an electronically stored monetary value as represented by a claim on the issuer.
- It can be acquired against payment of a monetary amount.
- Its purpose is making payment transactions, i.e., primarily to transmit sums of money to others.
- Third parties, i.e., not just the issuer, accept these assets as payment.

Points 1 and 2 are related to the system of stabilization aiming to avoid the inconveniences of liquidity and setting a deposit guaranteeing redemption at any time while impeding liquidity stress. A decentralized service that claims to create or use a crypto-asset with an official currency 'as a reference' is more exposed to liquidity risk and could easily de-peg in value. Barthélémy, Gardin, and Nguyen (2023), explained in a recent Banque de France working paper the challenges in creating a system of stabilization of value while being a uniformly accepted model partly because the nature of systemic liquidity risk differs significantly across countries. Even systems of value stabilization within 'short-term assets' like those currently used for DeFi stablecoins are presumed to be less prone to liquidity stress. Yet, developing a systemic liquidity stress testing tool is challenging due to data constraints and hard-to-model behavioral factors.

There are also complications as the EU's Markets in Cryptoassets (MiCA) regulation eludes any definition of a fully decentralized protocol. For example, MiCA Titles III and IV were designed to prevent a foreign-issued and non-euro-backed stablecoin from becoming a widely used means of payment and store of value in Europe, thereby undermining the European Economic Area and competencies of the ECB as regards to monetary policy. The use of this type of asset as a means of payment is very niche as it is not recognized by sovereign states, and therefore does not require merchants to accept them to pay for goods and services offered. When they do so, it's purely voluntary. It follows that this new form of "money" must therefore be regulated as this would give them credibility and reassure users. Users' protection is fundamental but shall not form a severely restricting environment for the issuing companies so they can expand in a healthy ecosystem that fits their assets (hence the creation of a specific category).

The current EMT regulation does not consider the technological realities of stablecoins like DAI, which maintains its peg with an over-collateralization of a basket of crypto assets. Therefore, DAI does not require assets to be held in a credit institution nor the need to invest assets in liquid securities as assets are crypto assets and can be held on the Blockchain. How would this be applied? Nor can we target holders of DAI: European users represent only a

fraction of users. The ECB has opined that the drawback of stablecoins like DAI is the lack of an identifiable entity liable for crypto assets. A DAO acting as an issuer has no legal standing at law, and therefore applying the definition of an EMT or equivalent under MiCA fails due to the lack of both a definition of a fully decentralized protocol and legal status for DAOs full stop. The argument becomes a feedback loop.

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

AMLR offers a comprehensive regulatory framework that applies to a wide range of financial services and institutions. While DeFi is a growing area of the crypto industry, it still represents a small portion of the overall financial landscape. Therefore, it is premature to add DeFi into the AMLR at this time, given that there is still much to learn about this emerging ecosystem. Moreover, Section 2-4-4 presents DeFi as a huge risk for ML and FT: however, it is important to note that cash remains the most common medium of exchange used in money laundering. According to the United Nations, roughly $800 billion to $2 trillion of fiat is used for laundering yearly while crypto in 2022 was close to $23.8 Billion, which means that the estimate of cryptocurrency used for money laundering is less than 2% of the lower end of the estimated range of fiat currency used for money laundering.

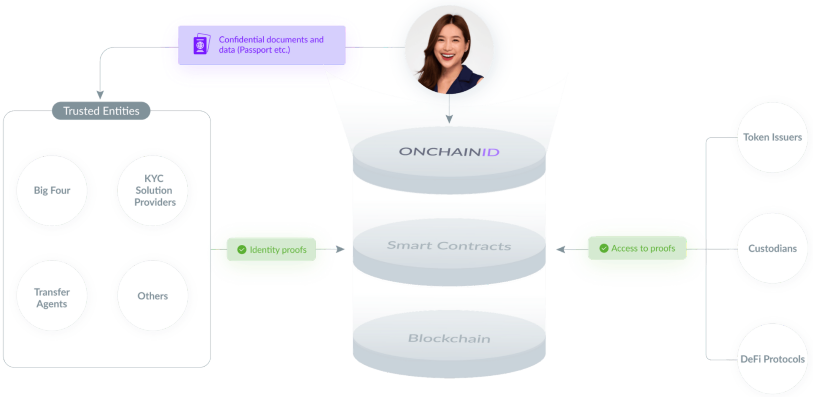
Blockchain analytics can help identify patterns and anomalies in transaction data that may be indicative of ML or TF activities, they can also help identify and trace the flow of funds through the DeFi ecosystem, including between different dApps and protocols. The implementation of AML requirements within existing legal systems focuses on preventing the use of tools that enhance anonymization, such as mixers, in order to maintain the ability to track and trace users. The primary objective of AML regulations today is to minimize pseudonymity and limit anonymity. Simultaneously, personal data regulations push personal data administrators and processors to prioritize maximum protection of personal data, which entails maximizing pseudonymity to safeguard user information from being tracked by third parties. This scenario exemplifies how applying traditional approaches and regulations to the DeFi space may not be suitable for DeFi participants. Furthermore, complying with most regulations would necessitate centralized governance, contradicting the direction DeFi is aiming for. Consequently, the existing legal framework discourages public and permissionless network communities and actors from undergoing various legal certification and supervision processes, given the complex and conflicting regulatory landscape.

DID solutions can help verify the identities of users when connecting with a dApp. Furthermore, regulatory compliance can be built into DeFi protocols through smart contracts, which can enforce specific rules and requirements related to KYC/AML (Know Your Customer/Anti-Money Laundering) and other regulatory obligations. Smart contracts can also enable the automatic reporting of suspicious activities to regulators or law enforcement agencies.

Regardless of a specific regulation that requires DeFi space to become compliant with KYC, there are already platforms innovating in this area, one example is Aave, which is a decentralized lending platform that allows users to borrow and lend cryptocurrencies without intermediaries. In order to comply with KYC requirements, Aave has implemented a "know your customer" (KYC) process for users who wish to borrow or lend above a threshold amount. Users are required to provide personal information such as their name, address, and government-issued ID, which is verified through a third-party KYC provider.

The argument presented in Section 2-4-4 that the lack of KYC and control mechanisms in DeFi "quite logically" generate money laundering and terrorist financing risks is misleading and an exaggeration of reality. While digital assets have been used in certain areas of crime, it is not accurate to suggest that the growth of these crimes is due solely to DeFi or a lack of KYC measures.

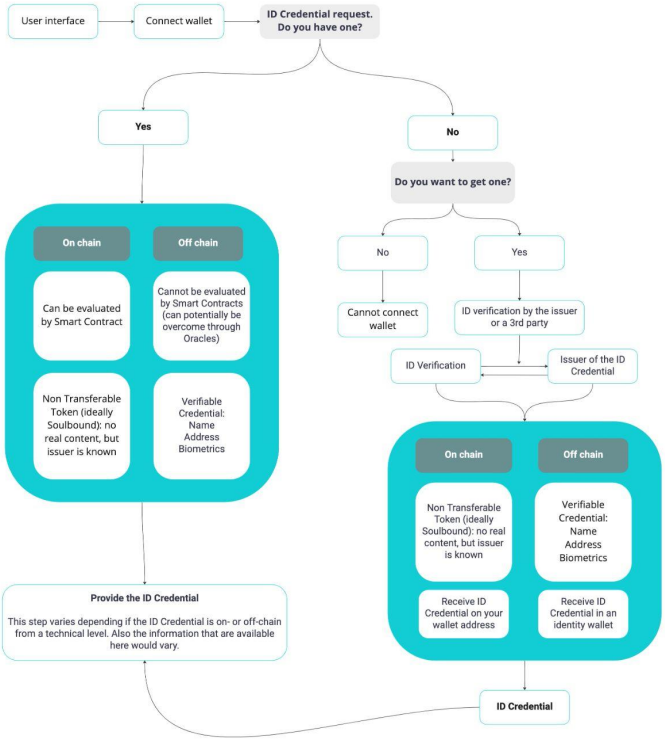
It is important to recognize that wallet addresses are not equivalent to identities. In fact, anyone who knows the wallet's private key can access the wallet, making it almost impossible to prove the true owner of a wallet. Hence, there is a lot of potential for Identity-based permissioned solutions in DeFi. Self-sovereign blockchain identities give users control over their identity by acting as their passports on blockchains. One identity can link to multiple wallets, and only verification proofs from trusted parties are published on the blockchain. There are multiple solutions exploring this potential. For example, ONCHAINID provides a framework for implementing identity in smart contracts. In their solution, identity proofs are issued by trusted parties and hashed as credentials managed by the owner, which allow DeFi protocols to verify if users meet their KYC/AML requirements to access DeFi platforms. Such identity ensures user pseudonymity by using on-chain identity addresses similar to wallet addresses but with the capability to identify the identities of users.



Source: ONCHAINID

The crucial component of a decentralized identity is the verification of user eligibility by authorized parties acting as trust anchors. They provide trustworthy verification through credible credentials, allowing DeFi smart contracts to seamlessly enforce compliance.

Additionally, these parties hold accountability and regulators can approach them to investigate any suspicious activity and identify users' real-world identities. This is what the IOTA Foundation calls "identity on demand", which refers to the ability to reveal the identity of authenticated subjects on demand and allows authorized parties (e.g. law enforcement) access to the actual identity data in case of a valid claim.



Source: IOTA Foundation Sandbox presentation

The implementation of Self-Sovereign Identity (SIS) and Decentralized Identifiers (DID) provides a solution for efficient and secure authentication for off- and on-chain applications. Those solutions will allow service providers to fulfill their legal obligations while providing their customers with secure, ergonomic, and privacy-preserving authentication mechanisms. This ensures transparency and integrity in DeFi, ultimately safeguarding users' on-chain privacy while ensuring compliance.

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?

The following risks were not mentioned in the report and should be taken into account:

- **Technology risk:** Bear in mind that DeFi is a software application. Thus, it can have bugs or loopholes in the code, which even if they are not necessarily intentional could be exploited. Many botched DeFi projects have been launched with unaudited code, resulting in losses like the YAM code bug disaster. To mitigate technological risk, the

industry (i.e., the ecosystem) could, through an association, self-regulate to audit an application before uploading it to a blockchain. In addition, there could be an audit process by, for example, a committee or verified developers assigned by the association. Such an approach could also be designed through an open source channel such as GitHub, with a verified code or smart contract requiring majority approval of the network. Code that has been audited and verified could receive a special mark/grade that is easily identifiable to everyone. Code that is not approved by the network would not be allowed to launch an application on the blockchain, with an algorithm preventing such an application from operating.

- **Liquidity risk:** The crypto market is highly illiquid, so every small quantity of "buy" or "sell" of these assets could have a huge impact on their value. Failing to assess this risk and inappropriately evaluating the DeFi application can cause severe losses even to sophisticated investors. Billionaire Mark Cuban showed that he is not immune to risk when he traded a DeFi app that crashed in one day. He later admitted to Bloomberg: "Even though I got rugged on this, it's really on me for being lazy. The thing about DeFi plays like this is that it's all about revenue and math and I was too lazy to do the math to determine what the key metrics were." Although this problem might subside as DeFi applications gain more adoption and become mainstream, in the short term, some applications may experience this type of risk.

- **Product risk:** Like any product or service you engage with, it is important to engage with a reputable, transparent product. DeFi is still a nascent industry without an established brand or reputation. Because anyone can create a cryptocurrency or a DeFi application, it can be difficult to parse what is serious and what is a joke. Meme coins, in particular, are incredibly volatile. One of the fundamental features of blockchain technology is transparency. Therefore, if developers of a DeFi application prefer to remain anonymous (like the botched protocol Harvest Finance, developed by an anonymous team) that should raise a red flag about its trustworthiness or whether it may be a scam. Each application should go through a rigorous evaluation of its product, its use case, and its team of developers.

The application of quantum computing to Proof of Work and Proof of Stake protocols could also significantly alter the validation system, creating fraudulent validations and taking control through 51% attacks, which allow double-spending by recovering previously spent cryptocurrency. Custodial risks could arise from the increased ability to perform brute-force attacks to decrypt private keys. Quantum computing poses a significant threat to the security of discrete log-based public-key cryptography, which is commonly used to protect user addresses (wallets) in DeFi. Therefore, the most significant threat to DeFi could lie in the potential accessibility of user funds stored in wallets. Quantum computing could enable unauthorized access to these funds, allowing attackers to impersonate wallet owners or compromise validator nodes, thereby undermining the security assumptions of Proof of Work (PoW) or Proof of Stake (PoS) mechanisms. In essence, quantum computing provides a way to gain

access to the "key" instead of breaking through the main door or windows. This threat persists until the adoption of post-quantum cryptography in the DeFi ecosystem. Yet that same quantum computing capability could more quickly and easily scan for code vulnerabilities in smart contracts.

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)?

No. Given the vast number of public blockchains and the extensive diversity of activities they support, along with the inherent difficulty in predicting future use cases for consensus protocols and cryptography, we believe that implementing a set of minimum standards or a regulatory framework would be inefficient. Without a proper examination of various use cases, a strong set of minimum standards or a regulatory framework around blockchain characteristics could further negatively impact blockchain development and de facto limit and prevent further investments and innovations. To address the risks effectively, public authorities should engage in a thorough examination of best practices and standards adopted by the market participants. These practices include smart contract audits, bug bounty programs, code verification, and rigorous testing.

To elaborate on the above, it should be noted that by design, blockchain infrastructure boasts a unique blend of features: immutable on-chain data, advanced cryptographic security, decentralized validation, swift transactions, and a built-in consensus mechanism for seamless upgrades. Each feature comes with a specific set of parameters, which can be implemented in different ways. Over time, this led to the development of a plethora of consensus protocols, each with distinct mechanisms for validating on-chain data and varying levels of encryption and other features. Despite the efforts to find the best possible combination of features, it has been challenging to achieve a high level of decentralization, security, and scalability of the network at the same time. This challenge has been often referred to as the blockchain 'scalability trilemma' (a term coined by Vitalik Buterin), which states that one can only have two out of three – decentralization, security, and scalability – at a time, with trade-offs being inevitable. Different blockchains and consensus mechanisms thus present different trade-off scenarios, each serving different preferences and objectives. As it is with numerous other technologies, diversity allows for the necessary trial and error, enabling further innovation and an indispensable learning experience, which provides for greater security and efficiency in the future.

Some consensus protocols allow greater scalability of the blockchain by relying on light nodes, which require reduced blockchain data. As a full node contains an entire copy of the blockchain

ledger (i.e. all blockchain transactions) at all times, it is deemed to be providing a higher degree of security. However, due to such vast data requirements, a network of full nodes is often considered as not scalable (thus the creation of lightning networks, Layer 2, rollups, etc.). Similarly, a huge number of validators may offer greater security of the network, yet at the expense of making it slow and completely dysfunctional.

These are just a few examples of the code itself providing for different (minimum) security standards. Consensus mechanisms are by design already adapted to the minimum required for the operations to be performed in a certain manner. Therefore, it is not advisable to set a minimum number of validators required in a public blockchain. Instead, a strong understanding of each specific consensus protocol, features thereof, and related cyber-security resilience mechanisms should be examined and taken into account.

The authors of this Discussion Paper correctly observe that a shutdown of the infrastructure cannot always be implemented. Indeed, with regard to the decentralized protocols a shutdown is impossible. Such restrictions, along with a requirement of obligatory intervention or termination are impossible due to the disintermediated and decentralized nature of blockchain infrastructure. As argued in the European Crypto Initiative's Position Paper on the Data Act, such requirements may have the opposite effect and expose users to additional risks as the shutdown feature may be abused or otherwise damaging for the blockchain users if inappropriately executed.

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

By taking further action. It is important to consider the concentration level of validation capacities on public blockchains, as it can have serious implications for the security and decentralization of the network. Public authorities should play a role in supervising this concentration and implementing measures to address potential issues. Potential approaches include monitoring and reporting, anti-monopoly regulations, initiatives or incentives for decentralization, and collaborative governance.

It is important to note that direct supervision by public authorities might not be the most effective approach, especially if the blockchain network operates in a decentralized and autonomous manner. However, authorities can still have a role in ensuring that other regulated entities, such as DAOs or entities providing access to DeFi services, meet certain requirements to promote fair and secure access to these services.

In a nutshell, public authorities should consider supervising the concentration level of validation capacities on public blockchains through measures such as monitoring, anti-monopoly regulations, initiatives for decentralization, and collaborative governance. The specific approach may vary depending on the characteristics of the blockchain network and the broader regulatory framework. It's important to note that excessive regulation could stifle

innovation and growth in the blockchain sector in general. Regulation should be carefully considered to strike a balance between the decentralization and security of public blockchains and encourage their development and adoption.

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?

Private blockchains operated by private operators should not be regulated through a supervisory framework. Compared to public blockchains, private blockchains encompass different types of governance. Transaction validation and the ability to operate a node may further be reserved for those with permission (permissioned blockchains). As such, private blockchain often reflects the features enabled by a privately operated database or a private cloud solution. The EU Database Directive defines a database as a 'collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.' In this sense, private blockchain presents a methodical way in which data can be arranged. Instead of regulating private blockchains through a new supervisory framework, existing regulations and sui generis rights should be examined.

This perspective (private blockchains operated by private operators) undermines the concept of DeFi. There are two main arguments to consider on this point.

1. Artificial intelligence and quantum computing: The advancement of these technologies poses a potential threat by enabling techniques that can circumvent traceability. These technologies can potentiate the risks associated with money laundering practices highlighted by the Financial Action Task Force (FATF) in their document on countering ransomware financing, particularly when it comes to key management.

2. Limitations of private networks: Private networks lack the partitioning mechanisms found in public networks. In public networks, the community creates defense mechanisms by identifying and sharing lists of addresses associated with malicious or suspicious activities through social networks. These lists, known as blacklists, serve as a means of exchanging information among users. However, controlling these "self-generated" mechanisms raises concerns. There is a danger of being unjustifiably blacklisted or facing challenges in ensuring the accuracy and fairness of these mechanisms.

In summary, while private DLTs aim to address the issue of traceability and reduce money laundering risks, advancements in technologies like AI and quantum computing introduce new challenges. Additionally, the limitations of private networks hinder the effectiveness of defense mechanisms established by the community. Finding solutions that balance privacy, security, and effective control mechanisms is crucial to mitigate risks associated with money laundering and maintaining a fair and reliable system.

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

No. Within a free market economy, the principles of economic freedom and individual liberty dictate that private actors should have the autonomy to engage in commercial activities. This fundamental concept, recognized in French Public Law as the "*Liberté du commerce et de l'industrie*," underscores the importance of allowing private entities to operate and innovate without undue interference.

Public actors can contribute to the growth of the private sector and blockchain infrastructure by providing services that are primarily in their domain and prerogative. By leveraging their expertise and resources, public entities can foster an environment conducive to innovation ensuring a level playing field and supporting the development of a robust blockchain ecosystem. However, it is crucial to maintain a clear separation between the roles and responsibilities of public and private actors. Thus public players should not directly manage the blockchains that provide the infrastructure for DeFi operations. Below we provide expanded reasoning.

As further observed by Primavera de Filippi, the rules and procedures of a blockchain-based network are primarily defined by the developers and are subsequently “adopted” by a variety of actors who willingly agree to submit to these rules. Anyone is free to exit the system or even fork it (i.e., copy it) into a separate system operated by a different protocol. No one has the legal authority to coerce anyone into submitting to the rules of a particular protocol. Participation in any blockchain-based system is purely optional and voluntary.

In order to ensure the smooth governance of a blockchain-based system, it is crucial to address the management of technological constraints. This responsibility lies with either the entire network participants or a substantial majority, or in the case of PoS systems, a party that holds a majority stake. Public entities are unable to directly oversee public blockchains that serve as the foundation for DeFi unless they possess such a significant majority themselves.

The private sector has embraced privately operated blockchain solutions as valuable technical tools. However, it's important to note that there is no universally accepted definition of a "private blockchain." This term can encompass a permissioned blockchain, which restricts participation in transaction validation to specific validators. On the other hand, it can also refer to a fully closed DLT that resembles privately owned databases or cloud computing services, rather than public and decentralized ledgers. It is evident that the latter type of private blockchain cannot serve as the infrastructure for DeFi operations. Even in cases where private blockchains support DeFi activities, it doesn't necessitate public entities to involve themselves in managing these private blockchains. Similarly, Apple Pay, Google Wallet, and Mozilla

browser offer technical solutions and interfaces that enable users to access certain DeFi operations, but they do not provide public access to their underlying infrastructure.

In conclusion, we deem it unnecessary and inappropriate for public actors to have access to manage the infrastructure of privately operated blockchain solutions solely because they are used for financial operations or DeFi facilitation.

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. Blockchain protocols have gained trust in various applications due to their verifiable code, auditability, and other mechanisms that enhance security. Rather than relying solely on stringent compliance processes that enforce minimum security standards, security can be effectively entrusted to stakeholders who provide core infrastructure, even when they operate under self-regulation or regulatory guidance. To offer an alternative to regulation, we present an overview of a (self) certification process.

The blockchain protocol's technological design guarantees the execution of operations on the blockchain, thus it's important to consider how the minimum level of security is ensured with other internet protocols. One such protocol is HTTP (Hypertext Transfer Protocol), widely used for data transmission over the internet. However, HTTP is not secure as it lacks data encryption and is susceptible to eavesdropping, man-in-the-middle attacks, and data tampering. To enhance security, HTTPS (Hypertext Transfer Protocol Secure) is employed, which adds an additional layer of protection by encrypting data and ensuring server authenticity. Creating a secure website involves using SSL/TLS (Secure Sockets Layer/Transport Layer Security), a protocol that encrypts internet traffic and verifies server identity. SSL certificates, issued by trusted third-party certificate authorities (CAs), play a crucial role. CAs digitally sign the certificates with their private keys, enabling client devices to verify them. Activating SSL on the origin server enables the website to load over HTTPS, ensuring encrypted and secure traffic. It's worth noting that self-signed certificates can be created by generating a public-private key pair, but browsers may not consider them trustworthy and may display a "not secure" warning or terminate the connection altogether, blocking the website altogether, despite the "https://" prefix.

In addition to the above, the minimum security standard could be further promoted through the Security Management System (ISMS) framework, designed to manage and mitigate the risks associated with information security. ISMS provides a structured approach to protecting sensitive information and ensures that appropriate controls are in place to safeguard against security breaches and cyber-attacks. The main goal of ISMS is to minimize risk and ensure business continuity by proactively limiting the impact of a security breach. Further, consider the ISO/IEC27001:2013, an internationally recognized standard for information security

management systems. The standard does not mandate specific actions but instead includes suggestions for documentation, internal audits, continual improvement, and corrective and preventive action. The main goal of ISO 27001 is to reach an organization's desired level of information security. An organization must comply with specific requirements to become ISO 27001 certified, including providing the following assessments: (1) the risks the information assets face; (2) the steps taken to protect the information assets; (3) a plan of action in case a security breach happens; and (4) identification of individuals responsible for each step of the information security process.

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?

A certification mechanism can be an effective solution to determine the scope of "safe" smart contracts. It can help standardize the development process and ensure that smart contracts meet quality and security requirements, ultimately safeguarding user security. To ensure the effectiveness of certification, it is important to consider the following factors during the review process:

- Industry or regulatory requirements: Smart contracts must comply with relevant regulations, such as data protection or financial regulations, specific to the industry or use case.
- Risks and vulnerabilities: The certification process should address the potential risks and vulnerabilities associated with the particular use case or application of the smart contract.
- Certifying entity expertise: The expertise and qualifications of the individuals or organization conducting the certification should be taken into account to ensure reliable and accurate evaluations.
- Testing and validation: The certification process should include thorough testing and validation procedures to ensure the reliability and robustness of the smart contract.

The formal verification of smart contract security requires certified tooling, as vulnerabilities in the tooling can undermine the effectiveness of smart contract audits (as demonstrated by the breach of the Dexter exchange platform on the Tezos blockchain). This approach offers increased scalability and only necessitates the involvement of a few knowledgeable engineers and scientists,

It is important to note that certification alone may not be sufficient. It should be complemented by continuous monitoring, bug bounty programs, and regular security audits to ensure the ongoing safety of smart contracts. The three dimensions mentioned in Section 3-2-2.a (static analysis, dynamic analysis, and software composition analysis) are important components of a certification process for smart contracts, but may not be adequate on their own to ensure the safety and security of the smart contract. Other considerations for certification include:

- **Open-source development:** Encouraging open-source development and community-driven auditing can lead to more secure and reliable smart contracts, as developers worldwide can contribute to finding and fixing potential issues.
- **Continuous education and training:** Ensuring that developers are up-to-date with the latest security practices and vulnerabilities can help minimize risks associated with smart contract development.
- **Bug bounty programs:** These programs incentivize independent security researchers to find and report vulnerabilities in smart contracts, which can help identify and resolve issues before they become critical.

In the case of modular smart contracts, it's important to not only ensure the safety and security of each individual module but also to ensure that the different modules can interact with each other correctly and safely. Beyond the mere request of certification on previous modules, it is important to consider the following during the certification review:

- **Identification of individual modules:** Each module should be identified and evaluated separately for compliance with security and quality standards.
- **Identification of module interactions:** The certification process should identify the interactions between the different modules, ensuring that they are compatible and secure.
- **Verification of module compatibility:** The certification process should verify that each module is compatible with the other modules it interacts with and that it operates as intended.
- **Analysis of potential vulnerabilities:** The certification process should analyze potential vulnerabilities that may be introduced by the interaction of modules.
- **Integration testing:** The certification process should conduct integration testing to verify that the modules interact correctly with each other.
- **Final certification:** Once all individual modules and their interactions have been evaluated and verified, the modular smart contract can receive its final certification.

Implementing a life cycle for the certification process and requesting updates when the code has been modified is a sound strategy. However, it is important to determine how much the composition of the smart contract needs to change in order to be submitted again to the certification process.

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 their respective strengths and limitations?

Although the code behind smart contracts is often published for transparency purposes, this does not necessarily make it easier for end-users to assess their safety and functionality. Moreover, developers may choose to protect their code for intellectual property purposes, as publishing smart contract code exposes it to third-party exploitation. As such, formal verification using certified tools is a preferred method for verifying that a smart contract is consistent with its specifications and error-free. This can be done without the need to publish the contract and formal method auditing can be automated and scaled to reduce cost. Additionally, it is important to verify the governance of the smart contract and other off-chain components, such as oracles, in a traceable manner. This verification ensures that the contract functions as intended and reduces the risk of errors or vulnerabilities. Human auditing methods are often impractical and cumbersome, making formal verification with certified tools the preferable approach for ensuring smart contract security.

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

There are several reasons why certain smart contracts may not be certifiable. These include contracts facilitating illegal activities, fraudulent schemes such as Ponzi or pyramid schemes, and contracts designed to exploit users or commit other malicious activities. Additionally, smart contracts that are experimental or too complex for human audit may also be challenging to certify.

For instance, the diamond standard architecture used in some smart contract implementations (such as the smart contract store developed by FeverTokens) can be difficult to certify by humans. Instead, the industry needs to develop automated tooling and formal verification to verify these contracts as needed, especially when updates occur.

Overall, formal verification tooling is a crucial direction for the DeFi industry, providing highly available, consistent, and scalable smart contract audits to ensure the security and integrity of DeFi protocols and platforms.

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)?

Pre-certifying components is important but not sufficient to ensure the safety and correctness of a system. This approach assumes that the certification process is holistic, but that is not always the case. To ensure the overall safety and correctness of a system, extensive formal verification of the entire system is required. While pre-certification can be faster and less

expensive than a full certification life cycle, it has limitations. For instance, it may not provide complete assurance that the overall system is secure and reliable, particularly when there are interactions between components. Additionally, it can be challenging to coordinate multiple components that are certified by different entities. As a result, a more comprehensive approach to certification, including a full certification life cycle, might be necessary to ensure the safety and correctness of a system.

In some cases, a pre-certification of called components may be sufficient, while in other cases a full certification life cycle may be necessary. The life cycle provides comprehensive assurance that the entire system is secure and reliable and can be customized to the specific requirements of the smart contract, including a review of the interactions between components, which can identify vulnerabilities. However it is time-consuming and it can be difficult to apply to systems that are constantly changing, such as those using upgradable smart contracts. **The best approach to certifying smart contracts depends on the specific requirements of the system. and the resources available. The choice of approach for pre-certification and certification life cycle will depend on several factors, including the complexity of the smart contract, the level of risk involved, and the available resources.**

New smart contract architectures, such as the upgradable pattern of the diamond standard, have made smart contracts more dynamic and subject to change. As a result, changes to smart contracts must be transparent and subject to regular audits. Automated audits through formal verification are needed to keep track of these changes in a timely manner, especially when changes are made while the smart contract is in use. This could be implemented with hybrid methods that can also be used for pre-certification, combining the strengths of both human auditing and automated formal verification. For example, human auditors can review and test the code while automated tools can assist in detecting potential vulnerabilities and errors.

Dynamic smart contracts can also benefit from custom governance policies with advanced role-based access control (RBAC) to control their changes. For example, some stakeholders could have the right to pause the smart contract that is being modified until the new configuration is properly validated. By implementing these policies, changes to smart contracts can be made more transparent and subject to ongoing audits, ensuring the safety and correctness of the system.

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

Yes. There are several benefits to embedding regulatory requirements in smart contracts:

- Compliance: Including regulatory requirements directly in the code ensures that the smart contract operates within the legal framework. This reduces the risk of non-compliance and potential legal repercussions.

- Transparency: By defining rules and requirements within the contract, all parties involved gain clarity and transparency. They can easily understand the obligations and limitations set forth by the regulations.
- Trust: Adhering to regulations helps build trust among users. When smart contracts demonstrate compliance with regulatory requirements, it instills confidence and encourages broader adoption of blockchain technology and its applications.
- Ecosystem benefits: Embedding regulatory requirements in smart contracts contributes to the overall ecosystem. It enhances transparency and certainty, particularly for applications like DeFi where compliance is crucial. Stakeholders can rely on the smart contract to automatically comply with applicable laws and regulations.
- Dispute mitigation: By incorporating regulatory requirements into smart contract code, the risk of disputes arising from disagreements over compliance is minimized. Clear and predefined rules reduce ambiguity and provide a basis for resolving potential conflicts.

On the other hand, regulating self-regulated and stateless systems like smart contracts can be quite complex. Translating legal language and regulatory requirements into code can be challenging as there might be implications in the law that are difficult to capture in a smart contract. Universal regulations require an international authority with enforcement power. Implementing regulations in one country alone could hinder its ecosystem development. A voluntary code of conduct or charter for smart contract developers could be beneficial. Still, without any punitive measures, compliance may be limited. Developing a specific framework risks redundancy with solutions already in place.

Summing up, embedding regulatory requirements in smart contracts promotes compliance, transparency, trust, and overall ecosystem benefits. It can mitigate disputes and ensure that all stakeholders can confidently engage in transactions while adhering to applicable regulations. Still, if not universally applied, it could create risks for the ecosystem development in the countries that would decide to apply it.

Q24: Who should set the security standards for smart contracts (refer to Section 3-2-2, Item B) and why?

A dedicated harmonized European Norm (hEN) for smart contracts is being developed. The European Commission is bringing together ETSI and CEN CENELEC to develop technical specifications in line with requirements laid out in the Data Act, further in line with the Annual Union Work Programme 2022. It could follow that both ETSI and CEN CENELEC could establish a Joint Technical Body (JTB) following Mode5 collaboration. The industry specification by ETSI PDL-11 was also designed in collaboration with European SMEs for example. There is also important work being done in ISO CT307 WG7 on the issue of interoperability, alongside ETSI PDL-6. Taken together, if such an approach were further instrumentalized beyond the level of smart contract standardization for IoT devices, it could serve as a blueprint for public-private collaboration on setting security standards for DeFi-related smart contracts. This is where industry associations like Gaia-X could help coordinate with different institutional

industry-related bodies (e.g. ESMA) to drive the smart-contract technical standards for DeFi. It could also follow that Gaia-X or other players in a similar position could mirror the aforementioned Joint Technical Body approach.

Q25: Should interaction with uncertified smart contracts be discouraged or prohibited (refer to Section 3-2-2, Item C)?

Interaction with uncertified smart contracts should be discouraged. While it may be too restrictive to prohibit uncertified smart contract interactions altogether, it is important to discourage such interactions and make users aware of the potential risks and downsides. This can be done by promoting cautiousness and due diligence before proceeding with any uncertified contracts.

When high stakes are involved, users should be particularly discouraged from interacting with uncertified smart contracts. However, providing automated formal verification processes for smart contract audits is also crucial so that a greater proportion of contracts can be certified. This will allow users to access simplified audit reports and make informed decisions on whether or not to interact with a smart contract.

It is important to notice that prohibiting uncertified smart contract interactions altogether may seem like the safest option, but it may not be practical or feasible in some cases. Prohibition would require a high level of control and regulation over DeFi, which is inherently decentralized and aims to provide financial services to anyone with an internet connection.

Prohibition may also hinder innovation and limit the potential benefits of DeFi by restricting access to new and experimental smart contracts. By discouraging uncertified interactions instead of prohibiting them, users can still have the freedom to explore new opportunities while being aware of the potential risks and taking necessary precautions.

Furthermore, promoting caution and due diligence encourages responsible behavior by users and encourages the development of better audit tools and formal verification processes for smart contracts. This, in turn, can improve the overall security and trustworthiness of DeFi and contribute to its long-term success.

Q26: Who should bear the certification costs of smart contracts (refer to Section 3-2-2, Item B) and why?

The costs of certification for smart contracts should be borne by the developers who create them. This is because they are responsible for ensuring that their smart contracts are secure and reliable for their users. Certification provides an additional layer of assurance that the smart contract functions as intended and is free of vulnerabilities or errors.

Certification can also serve as a competitive advantage for smart contract developers, as it demonstrates their commitment to providing secure and reliable smart contracts to their users. Furthermore, certification can be mandatory for regulatory compliance purposes, such as in the financial industry, and may be necessary for smart contracts to be adopted by users. However, it is important to note that mandatory certification costs may act as access barriers to new players in the field. Therefore, regulatory bodies could consider providing financial assistance or incentives to reduce the cost of mandatory certification for smart contract developers, especially those who are new to the industry.

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?

In the DeFi ecosystem, the reliability of oracle services is critical in determining adoption and stability. Trust in oracles involves two dimensions: trust in the production of information by the oracle and trust in the transmission of the information from the oracle to the smart contract. While the first dimension may be driven by economic incentives, the second dimension relates to risks such as operational failure or cyber-attacks.

To ensure trust in oracles, standardized frameworks for data production, processes, and APIs could be established. This would promote competition, innovation, adoption, and coordination among various participants, including consumers, protocol designers, and oracles. By standardizing these frameworks, public and open information would be readily obtainable and reliable, making it easier for users to trust the information provided by oracles.

Legal frameworks for oracles would also introduce liability and improve efficiency and trust. For example, specialized oracles could produce non-fungible tokens for Know Your Customer (KYC) or credit-scoring purposes. This would expand the contracting space for lending protocols while keeping identities private on-chain. Such initiatives would ensure conflicts of interest are avoided, provide reliable information, and make DeFi protocols more accessible to a wider range of customers.

Furthermore, establishing a legal framework for oracle operations could substantially improve efficiency and trust. It would introduce liability for the activity of an oracle and ensure that licensed oracles produce reliable information on candidate customers, which could then be used by DeFi protocols. In addition, security standards and disclosure guidelines could be developed to ensure that conflicts of interest are avoided between oracles and other contracting parties. Overall, public support for establishing standardized frameworks and legal frameworks for oracles could enhance the efficiency, trust, and adoption of DeFi. By doing so, we can ensure that information provided by oracles is verifiable in the real economy, public, open to all interested parties, readily obtainable, and reliable.

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

No. The regulatory concerns have been highlighted in the different questions. In particular on the questions provided to answer under Section 3-2*: Providing a suitable oversight framework in view of the algorithmic nature of services.*

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

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

No. We believe a “recentralization” of some cases is not necessary for the following reasons. First, it is not clear what sensitive activities are and how they are defined. Secondly, we deem that the MiCA regulation holds sufficient requirements for “recentralization” and incorporation not only when sensitive activities are engaged or provided, but specific crypto assets or financial instruments are provided to the individuals. And thirdly, we believe any “recentralization” poses risks to security, reliability, trust, and governance, especially if applied to Layer 1 blockchain solutions. The pursuit of decentralization aims to distribute power, enhance security and remove the risks linked to the “single point of failure”. It also creates a more resilient and inclusive blockchain ecosystem that aligns with the principles of transparency, immutability, and user empowerment. As mentioned above, we deem it necessary to adopt a ‘substance over form’ approach and prevent too many restrictions or regulations from impacting the further development of blockchain technologies.

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?

Because DAOs do not have a clear legal status, it can be complicated to impose regulations on them, especially in cases of regulatory arbitrage. To apply regulations, legal entities must be clearly defined. It is important to note that any regulatory measures must balance innovation and investor protection and may need to evolve as the DeFi and DAO landscape continues to develop. Incorporation requirements, making players with effective control liable, and legal status for DAOs, are aimed at bringing more clarity and legal certainty to the regulation of DeFi and DAOs. These proposals could potentially help to address some of the legal and regulatory challenges that DeFi and DAOs currently face, such as uncertainty around liability, governance, and compliance requirements. Incorporation requirements could also help ensure that DAOs are registered and regulated appropriately, providing greater legal certainty for investors and users. Making players with effective control liable could help to ensure accountability and prevent abuse of power within DAOs. Legal status for DAOs could help clarify their legal position and provide more certainty around issues such as liability and governance.

In general, it is important for regulators and policymakers to work together with industry players to find the right balance between innovation and regulation. Clear and consistent regulatory frameworks can help to support innovation and protect users, while also providing legal certainty for investors and businesses.

It could also be important to evaluate the progress of other regimes and jurisdictions with a regulatory framework. For example:

a. **The Republic of the Marshall Islands:** The Marshall Islands has passed DAOs Revolutionizing Enterprises Act (REA), which recognizes DAOs as a distinct form of a legal entity. Decisions of the DAO can be legally taken by DLT-based votes, and no single human has any special powers that they could abuse to execute decisions that go against the will of the DAO's members.

   The REA defines a DAO as an entity managed through rules encoded as computer programs on a blockchain, with decisions made by a consensus of its members. This means that the decisions of the DAO are made through a voting process among the members, which is recorded on a blockchain and executed automatically through the code of the smart contract governing the DAO. Since there is no central authority or human decision-maker in a DAO, the decisions are made solely by the members of the DAO through their voting power. This ensures that no individual has special powers that they could abuse to execute decisions that go against the will of the DAO members.

   However, it is important to note that the REA also provides for certain legal requirements for the operation of a DAO, including registration, reporting, and disclosure requirements, as well as provisions for the protection of the rights and interests of the members. It is important for those interested in establishing or operating a DAO to comply with these legal requirements and seek legal advice in the relevant jurisdictions.

   The Marshall Islands have emerged as a leading jurisdiction for registering DAOs, offering legal entities tailored to the unique needs of DAOs. These entities, including for-profit and not-for-profit DAO LLCs, are based on the LLC structure. They provide several advantages, such as limited liability for members, corporate personhood, and tax benefits. For-profit DAO LLCs are subject to a 3% gross revenue tax. While the Marshall Islands currently lack specific laws or regulations pertaining to digital assets, tokens, or protocols, they have plans to introduce innovative legislation in these areas.

   The jurisdiction adheres to international standards and requires KYC completion by DAO members holding more than 25% governance rights or any managing members. Annual reporting is mandatory, and Marshall Island DAO LLCs can open accounts with

various banks. Other corporate entities are available in the Marshall Islands, and MIDAO maintains a list of local lawyers offering legal advice and consulting services.

Notably, Marshall Island DAO LLCs are unique as they do not have to follow typical requirements that other corporate entities may require, such as having board members or directors with special powers, keeping full member information on record, submitting extensive annual filings, and more. MIDAO serves as the exclusive registered agent responsible for creating and maintaining DAO LLCs in the Marshall Islands, providing standardized template documents.

The Marshall Islands place certain limitations on DAO engagement in specific sectors, such as direct participation in adult entertainment, gambling, or the custody of digital or financial assets. For-profit DAO LLCs are subject to a 3% gross revenue tax but may be exempt from capital gains and dividends. Most DAO members can remain anonymous unless holding over 25% governance rights. Marshall Island Series LLCs are permitted, and MIDAO can help identify options for moving a DAO entity to the Marshall Islands. Digital asset laws and regulations in the Marshall Islands are limited to companies involved in the custody of digital assets on behalf of others. The jursidiction is not on any international blacklist and is included on the white list established by the Organisation for Economic Co-operation and Development (OECD). The creation of a DAO LLC in the Marshall Islands can be completed in as little as 30 days once the necessary paperwork is submitted.

The EU can draw on the Marshall Islands' DAO regulations to inform its own regulation of DAOs and other decentralized digital entities. Firstly, the EU could recognize DAOs as a distinct form of a legal entity, as the Marshall Islands have done. This would require establishing a legal framework for the establishment and operation of DAOs, including registration and reporting requirements, as well as provisions for the protection of the rights and interests of the members. Secondly, the EU can consider adopting a regulatory framework that supports the use of DLT and smart contracts to govern DAOs. This would involve recognizing the unique characteristics of DAOs, such as the absence of a central decision-maker and the use of consensus-based decision-making processes. Thirdly, the EU could consider implementing tax policies that are conducive to the growth of DAOs, such as the 3% gross revenue tax levied on Marshall Islands for-profit DAO LLCs (and which applies to earned income and interest but does not apply to capital gains and dividends). It is also important to consider that the Marshall Islands' KYC requirement for DAO members with 25%+ governance rights and managing members aligns with the desire of the EU to make DeFi compliant with KYC and AMLR.

b. **Wyoming DAO LLC:** It could also be interesting to examine the development of DAO legal wrappers, such as the Wyoming DAO LLC model in the United States. Wyoming allows the registration of profitable DAOs and the distribution of those profits among

its members. In March 2021, the Wyoming Senate passed a DAO supplement that introduced a new type of entity called a Wyoming DAO LLC. To be classified as a DAO LLC under this supplement, an LLC must indicate in its articles of organization that it is a DAO. By establishing a DAO LLC, members of the DAO are safeguarded against unlimited liability for the DAOs actions and can interact with the off-chain world (enter into contracts, manage the treasury, etc.).

If the Wyoming DAO LLC is member-managed, the management responsibility must be vested in its members, similar to the classical model of LLCs. Alternatively, if it is managed algorithmically, the management responsibility must be vested in the smart contract, similar to the classical DAO model, where decision-making is encoded in the protocol. The articles of organization should indicate the method of management, whether it is member-managed or managed by smart contracts. Typically, members of the DAO LLC do not have any fiduciary duty to the organization or any member, except for the implied contractual covenant of good faith and fair dealing (unless otherwise specified in the articles of organization or operating agreement)

The articles of organization and smart contracts govern the operations of the DAO LLC, similar to the role of an operating agreement. However, an operating agreement can supplement the DAO LLC's operation to the extent that the articles of organization or smart contract do not provide for it. Under the applicable law, a DAO LLC that is managed algorithmically can only be formed if the underlying smart contracts can be updated, modified, or upgraded. Both the articles of organization and operating agreement of the DAO LLC are authoritative statements. In case of a conflict between the articles of organization and the operating agreement, the articles of organisation shall prevail over any conflicting provisions. On the other hand, if there is a conflict between the articles of organization and the smart contract, the smart contract shall take precedence over any conflicting provisions of the articles.

Therefore, it is advisable to construct the governance and management provisions consistently and comprehensively across all the constitutional instruments of the DAO LLC, including the smart contract, articles of organization, and operating agreement. Each article of organization of the DAO LLC must contain certain statements about the DAO, including information on:

- The rights and voting rights of members.
- Transferability of membership interests.
- Relations among the members and between the members and the DAO LLC.
- Activities of the DAO LLC and the conduct of those activities, etc.

The DAO LLC also has a ‘pass-through’ taxation system, giving DAO LLC’s pass-through treatment and allowing allocated profits to be taxed only once on the

individual tax return of each memberIn summary, the EU could consider a blended approach to the legal entity recognition of different DAOs as they are by and large aiming to achieve different ends, with governance arrangements curated towards those specific ends. The fact that there are grants DAOs, investment DAOs, media DAOs, social DAOs, or more general decentralized cooperatives without an economic overtone would hold that a flexible regime is best suited. The examples provided of the Marshall Islands and the State of Wyoming are two models out of a constellation of DAO structures and showcase the heterogeneity at work. The EU could consider this blended approach and also the introduction of a DAO taxonomy to underscore that there may exist different DAOs for different reasons within the EU. As such, the EU could after identifying a DAO based on its taxonomy, apply the appropriate legal wrapper.

In conclusion, addressing the regulatory challenges associated with DAOs requires a comprehensive approach that balances innovation and investor protection. Incorporation requirements, making players with effective control liable, and providing legal status for DAOs are proposals aimed at bringing more clarity and legal certainty to the regulation of DeFi and DAOs. These measures can help address issues such as uncertainty around liability, governance, and compliance requirements.

For example, the Marshall Islands recognize DAOs as a distinct form of a legal entity, enabling decision-making through DLT-based votes. This approach can inform the EU's regulation of DAOs, encouraging the recognition of DAOs as unique entities and establishing legal frameworks for their operation. It is important for the EU to consider the experiences and progress of other jurisdictions, such as the RMI and the State of Wyoming, to shape its regulatory approach effectively.

The EU could explore options like establishing a legal framework for DAOs, incorporating tax policies that incentivize DAO growth, and adopting a DAO taxonomy to differentiate between various types of DAOs based on their purposes and governance arrangements. Furthermore, the EU could consider the Wyoming DAO LLC model, which provides liability protection and allows interaction with the off-chain world.

Overall, the EU should adopt a flexible regulatory approach that accounts for the diverse nature of DAOs and their respective goals. By applying appropriate legal wrappers and considering the experiences of other jurisdictions, the EU can foster innovation while ensuring compliance, investor protection, and legal certainty within the DeFi and DAO landscape.

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 6)?

CeDeFi presents risks that are not specifically related to crypto assets but to the companies offering these services. These companies should be subject to additional regulations and obligations related to accounting, auditing, disclosure, and so on. However, it is common for

these companies, including conglomerates, to take advantage of regulatory uncertainty and create complex legal structures. By operating across multiple jurisdictions with either lax or non-existent crypto asset regulatory regimes, they can arbitrage their way out of compliance obligations while launching products and services that would otherwise be subject to much stricter rules. The prevalence of off-shoring in CeDeFi, especially with regard to derivatives products, is one such example. Given the overlapping business areas of CeDeFi companies, they are also often harder to pin down from a regulatory perspective.

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

Information requirements, Duty of Care and duty of advice, and white paper publication requirements. When engaging with DeFi, individuals may rely on multiple third-party service providers. While users may access a smart contract deployed by those who own and operate the interface, these two activities may as well be held by different entities or individuals. Further on, decentralized user interfaces often don't require a user account creation. A website may be considered a DeFi intermediary, and yet it only paves the way to other payment service providers allowing users to top-up their digital wallets by purchasing crypto-assets with their credit card (such as https://flexa.network/; or https://www.moonpay.com/).

Certain service providers may be less finance-oriented but nonetheless crucial for the DeFi access and services to be executed successfully. Users may rely on services provided by decentralized storage providers, there may be additional voting regimes and smart contracts developed and deployed by others, through which one collects verifiable credentials and conducts the identity verification, etc. While such DeFi intermediaries may present an interface for payment, very similar to Apple Pay or Google Wallet which do not demand a KYC from their users. The application of regulations should be applicable to payment service providers, crypto exchanges, and those who offer financial services. On the other hand, the regulation should not apply to those who do not conduct such services, but act merely as technology intermediaries. Given the diverse range of intermediaries involved in facilitating access to DeFi, it would be imprudent to lump them all together and pursue a one-size-fits-all solution.

When examining the requirements for DeFi intermediaries, it is important to acknowledge the layering hierarchy of the blockchain infrastructure and the application architecture of the DeFi diagram provided in the Discussion Paper. The base layer (Layer 1 blockchain protocols) establishes the rules for validators and confirmation of transactions on-chain. Users engage with Layer 1 blockchain protocols indirectly, most usually through the higher layers of the infrastructure. Higher layers (aggregators such as wallet providers, applications, and others) allow users to access products and services and expose themselves to greater risks. By focusing regulatory efforts on the upper layers, regulators can strike a balance between

safeguarding user interests and maintaining the principles of decentralization, cyber resilience, security, and innovation inherent in blockchain technology. It allows for targeted oversight of the areas where user protection and regulatory compliance are most critical, without stifling the underlying technology and its potential for transformative impact across various industries.

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

No. The question of whether to apply the same rules to all intermediaries in the DeFi ecosystem is complex, and each option has its own benefits and drawbacks. Applying the same rules to all intermediaries could help prevent regulatory arbitrage, promote fair competition, protect consumers, and reduce systemic risk. However, it could also stifle innovation, limit the potential benefits of DeFi, and discourage participation. A one-size-fits-all regulation may not address the different characteristics of intermediaries involved in DeFi. Therefore, any regulatory framework will need to balance the need for consumer protection with the potential benefits of innovation and decentralization. For example, the decision to leave DeFi out of MiCA was strategic, recognizing the rapidly evolving nature of the industry and the need to avoid premature regulation that could stifle innovation and hinder growth potential. Regulators are actively monitoring developments in DeFi, and as the ecosystem matures, they will work towards developing a regulatory framework that balances innovation and investor protection. Therefore, any future regulatory framework should consider the fast development of DeFi and the variety of applications that are being created.

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

No. Financial literacy and understanding the risks involved in financial products are essential to ensure that customers make informed decisions about their finances and avoid negative consequences. However, imposing requirements for financial literacy and risk appetite may further exacerbate financial exclusion, particularly for low-income individuals and those without access to traditional banking services.

Furthermore, subjective assessments of financial literacy and risk appetite may not be an accurate or effective means of ensuring consumer protection, as these characteristics can change over time and may be influenced by various factors. Enforcing such limitations could also require significant resources and infrastructure, and could be seen as a violation of the right to access financial services. It is important to consider that at the moment, there is no standardized way to measure financial literacy or risk appetite, and assessments may be influenced by factors such as language barriers, cultural differences, and educational background. Also, enforcing those types of limitations could require significant resources and infrastructure, as well as allocated entities such as regulatory bodies or financial institutions that are equipped to assess and monitor individuals' financial literacy levels and risk appetites and the changes in those behaviors through time per individual.

Considering how traditional finance regulations manage financial literacy could be useful to set an ethical standard for the DeFi industry. Protecting vulnerable customers, such as elderly users, from being sold financial products they don't understand should be a priority.

One potential solution could be to utilize advances in technology, such as Artificial Intelligence, and embedded rules within smart contracts to customize applications, products, and services to cater to customers' sophistication and risk appetite. For example, customers could be asked questions before purchasing a product; the smart contract could determine whether to allow the purchase based on the answers. However, automated algorithms should be carefully tested for biases and ethical concerns and audited and certified by self-regulated auditors or a decentralized audit mechanism. Applications should also be monitored, and if the risk level changes due to economic or geopolitical conditions, the smart contract should cease operations until reassessment is established, or a risk threshold could be set for customers below which they will not have access to the product.

In summary, while financial literacy and risk assessment are essential, we must be mindful of the potential negative consequences of imposing such requirements on access to financial products. By utilizing technological advancements in AI and embedded rules within smart contracts, we can customize applications, products, and services to cater to customers' sophistication and risk appetite, mitigating situations where customers may be taken advantage of due to their lack of knowledge. When limiting access to services, it is important to consider that this type of measurement could increase financial exclusion and reduce competition in the financial sector. Moreover, individuals who are deemed to have low financial literacy or risk appetite may be excluded from accessing certain financial products, even if they are capable of making informed decisions about their finances. This could further widen existing inequalities and limit individuals' opportunities to improve their financial well-being which can have significant implications for human rights.

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

No. All our suggestions have been made through the other questions. In the end, our recommendations advocate for a balance between fostering innovation and protecting users' interests when regulating DeFi. The focus should be on designing a framework that promotes responsible growth, safeguards against risks, and ensures a fair and secure environment for participants in the DeFi ecosystem.

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)?

Regulatory requirements can be implemented in DeFi in ways that recognize the differences in resources and capabilities between small and large players. One approach is to use a tiered regulatory system, where smaller players are subject to less stringent regulatory requirements than larger players. This can be achieved by setting different thresholds for regulatory compliance based on factors such as the size of the player, the type of activity, and the level of risk. For instance, smaller DeFi platforms could be subject to simpler compliance requirements, while larger platforms would be subject to more complex and stringent requirements.

Another approach is to leverage blockchain-based solutions that can reduce the burden on smaller players. Regulators can use blockchain-based compliance tools to automate compliance tasks, reducing the cost and complexity of compliance. This would make it easier and less expensive for smaller players to comply with regulatory requirements. For instance, record-keeping, transaction monitoring, reporting, or DID solutions can be used to create secure and decentralized digital identities that can be used to verify user identities and ensure compliance with regulations such as KYC requirements for DeFi lending and borrowing platforms.

Additionally, regulatory sandboxes can be used to provide a controlled environment for smaller players to test and develop their DeFi products and services. This approach allows for the testing of new innovations under the supervision of regulators while reducing the regulatory burden on smaller players. It can encourage innovation and competition in the DeFi space while protecting consumers and ensuring that regulatory objectives are met.

It's important to note that regulatory requirements should be proportional for small players. By implementing different approaches such as tiered regulatory systems, blockchain-based compliance tools, and regulatory sandboxes, regulators can strike a balance between protecting consumers and fostering innovation and competition in the DeFi space.

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)?

DeFi should be regulated with a focus on user protection while preserving privacy and self-data management capabilities and avoiding regulatory and structural aggregation leading to centralization. An efficient balance can be achieved through a widely adopted European blockchain-based identity, such as DIDs or SBTs, which offers flexible solutions to different users in the markets. The European Union has a chance to institutionalize this through projects like the EUDI wallet or by evolving EBSI in the context of European DAOs. By identifying European users, regulators or intermediaries can identify non-compliant users and access Europe's blockchain-based services, potentially alerting or asking for compliance amendments.

One way to achieve this is through international regulatory standards and frameworks developed through collaboration between different countries or regions, providing a common set of rules and guidelines for DeFi actors to follow. This would reduce the potential for conflicting regulations and extraterritoriality issues, providing greater legal certainty for DeFi actors operating across borders. Another way is through regulatory cooperation agreements between different jurisdictions, ensuring regulations are consistent across different jurisdictions and reducing the potential for regulatory arbitrage.

Regulatory sandboxes can also be used to test new DeFi products and services across different jurisdictions. These sandboxes provide a controlled environment for smaller players to test and develop their DeFi products and services under the supervision of regulators while reducing the regulatory burden on smaller players. This approach encourages innovation and competition in the DeFi space while protecting consumers and ensuring regulatory objectives are met.

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), and by what means?

A combination of voluntary compliance and public observatories can be used to regulate DeFi in a way that promotes user protection. Voluntary compliance can incentivize DeFi service providers to comply with policy requirements in exchange for public signals of quality and good intentions. This approach can be made feasible through the public licensing of supervisor-approved non-tradable and non-fungible tokens that serve as legally recognized proof of compliance. However, this requires incentives and supervisory powers to make compliance attractive. Third-party auditors can independently verify compliance and help ensure DeFi actors are following best practices and standards.

Furthermore, the unique structure of DeFi projects calls for a public observatory of DeFi activity operated by a public authority. This institution would deploy public investigations and issue opinions and warnings about specific DeFi protocols, practices, and public address activities. It can also cover the entire range of public protocols and provide supervision adapted to the transparency of protocols and historical activity.

Self-regulation within the DeFi and blockchain ecosystem can also be effective due to the strong sense of community and the high reputational risks associated with non-compliance. Self-regulation can establish best practices for security, data privacy, and transparency and can be enforced through peer review and self-reporting that later on could become standards. By combining these approaches, DeFi can be regulated in a way that protects users while promoting innovation and growth in the ecosystem.