

INATBA REPORT

by the FINANCE WORKING GROUP

DeFi Self-Regulation: A Proposal for the Industry

February 2025

Defi



INATBA

International Association
for Trusted Blockchain Applications



Authors

Izzat-Begum B. Rajan, INATBA Finance WG Co-Chair, CEO of Imani Partners and Partner at Mosaik Law firm, France

Jean-Christophe Mathonet, INATBA Finance WG Co-Chair, ProSquare, Belgium

Adrian Pollard, HollaEx, South Korea

Alireza Siadat, 1inch Exchange, Germany

Benjamin Bürgi, Cardano Foundation, Switzerland

Georg Brameshuber, Validvent, Austria

Giannis Rousopoulos, IOTA Foundation, Germany

Giles Swan, Blockchain.com, UK

Ismael Arribas, Kunfud, Spain

Ivan Gurtikov, Caisse des Dépôts, France

Jan Klesla, Blockchain Republic, Czech Republic

Jed Grant, KYC3, Luxembourg

Lana Schwartzman, Notabene, USA

Max Bernt, Blockpit, Austria

Mykola (Niko) Demchuk, AMLBot, Hong Kong

Olena Zabrodska, 1inch Exchange, Belgium

Tom Jansson, IOTA Foundation, Germany

Zeno Auersperg, Blockchain Italia, Italy

Reviewers and Advisors

Antonio Lanotte, EU Blockchain Observatory and Forum, Italy

Donna Redel, INATBA Academic Advisory Board, Fordham Law and Business School, USA

Jim Mason, EU Blockchain Observatory and Forum, USA

Maria Del Sagrario Navarro Lérída, INATBA Academic Advisory Board, Universidad de Castilla la Mancha, Spain



Abstract:

Decentralized Finance (DeFi) is redefining financial services by offering automation, transparency, and global accessibility without intermediaries. However, its rapid expansion introduces risks—ranging from smart contract vulnerabilities to governance centralization and financial stability concerns. Traditional regulatory approaches are often ill-suited for DeFi's decentralized nature, necessitating an industry-driven self-regulatory framework.

This report provides a structured DeFi Self-Regulation Proposal, detailing key risk categories and specific best practices to ensure security, compliance, and long-term sustainability. By implementing real-time financial reporting, decentralized governance models, and standardized security audits, the DeFi industry can mitigate risks while preserving innovation. The goal is to create a responsible, transparent, and resilient financial ecosystem, where DeFi protocols can evolve without excessive regulatory constraints while ensuring consumer protection and market integrity.

Table of Contents

Abstract.....	3
1. Introduction and Motivations.....	5
2. Why DeFi Models Matter.....	7
3. Definitions and Key Terms.....	8
3.1 Defining DeFi.....	8
3.2 Defining TradFi.....	9
3.3 Defining CeFi.....	9
3.4 Defining CeDeFi.....	9
3.5 Defining Security vs Non-Security.....	10
3.6 Defining Decentralization and Measuring it.....	10
4. Types of Risks.....	12
4.1 Taxonomy.....	12
4.1.1 Strategic Risks.....	12
4.1.1.1 Strategy.....	12
4.1.1.2 Business.....	12
4.1.1.3 Legal & Compliance.....	13
4.1.1.4 Environment, Negative Impact on Society and Governance Risk (ESG).....	13
4.1.1.5 Reputation.....	13
4.1.1.6 Brand.....	14
4.1.1.7 Capital Risk.....	14
4.1.2 Operational Risk.....	14
4.1.2.1 Internal Fraud.....	14
4.1.2.2 External Fraud.....	14
4.1.2.3 Employment Practices and Workplace Safety.....	15

4.1.2.4	Clients, Products, & Business Practice.....	15
4.1.2.5	Damage to Physical Assets.....	15
4.1.2.6	Business Disruption & Systems Failures.....	15
4.1.2.7	Execution, Delivery & Process Management.....	16
4.1.3	Financial Risk.....	16
4.1.3.1	Credit Risk.....	16
4.1.3.2	Concentration Risk.....	17
4.1.3.3	Liquidity Risk.....	17
4.1.3.4	Market Risk.....	17
4.1.3.5	Insurance Risk or Insurance Underwriting Risk.....	17
4.1.4	Emerging Risks.....	18
	AML/KYC/ATF Compliance for DeFi Protocols:.....	19
4.2	Risk in DeFi vs Risk in TradFi.....	20
4.2.1	Risks that Exist in Both TradFi and DeFi.....	21
4.2.2	Risk in TradFi that Does Not Exist in DeFi.....	22
4.2.3	Risk in DeFi that Does Not Exist in TradFi.....	23
4.2.4	Risk in DeFi that Will Not Exist in “True DeFi”.....	26
4.2.5	Findings & Regulatory Recommendations on DeFi.....	28
4.3	Contagion Policies between DeFi, DAOs, DApps, CASPs & TradFi.....	30
5.	Self Regulatory Proposal for the Industry.....	31
5.1	Basic Administrative Measures.....	32
5.2	Business-Oriented Measures.....	33
5.3	Technical Measures for DeFi Self-Regulation.....	34
5.4	Additional Security Measures.....	36
6.	Conclusions.....	37
7.	Glossary of DeFi Terms.....	38
	(Self-Hosted) Wallets.....	38
	On-Chain Lending.....	38
	Stablecoins.....	38
	Coin.....	38
	Key.....	38
	Voting Rights.....	38
	Liquidity.....	38
8.	Resources and Citation.....	39

1. Introduction and Motivations

One of the biggest narratives in the previous crypto asset investment cycles was the emergence of Decentralized Finance, commonly referred to as DeFi. Even today, more than 5 years since the emergence of the term, DeFi continues to be a new and ever-changing concept that needs to be understood well before it is regulated. As such, this report does a deep dive into what DeFi is today, what it promises to be tomorrow, and how to effectively tackle compliance before top-down lawmaking.

For INATBA and its members, understanding the present and future risks, as well as how to make regulations work for DeFi, is one of the most important tasks that our association can produce, especially since DeFi will be a key topic of upcoming regulatory focus for the new 5 year cycle for the European Commission; a movement that is bound to impact the global policy landscape for DeFi for decades to come.

To be precise, INATBA believes that voluntary self-regulation will be much more impactful in achieving the market safety standard that policy makers aim for, without impacting the growth and development of the whole industry and the competitiveness of Europe within Digital Finance. Self-regulation is not a new concept. It allows industries to establish flexible, industry-specific standards that can evolve with technological advancements and market needs. It encourages innovation by reducing regulatory burdens while still maintaining a focus on safety and transparency. Additionally, by empowering industry participants to monitor and enforce their own standards, self-regulation fosters accountability and builds trust within the market.

Self-regulation exists in traditional financial markets, like in the US, where organizations like the Financial Industry Regulatory Authority (FINRA), a self-regulatory organization, oversees broker-dealers under the supervision of the Securities and Exchange Commission (SEC), allowing for industry expertise to drive enforcement. In Switzerland, self-regulation is similarly integrated into the financial system, with industry associations like the Swiss Bankers Association working alongside the Swiss Financial Market Supervisory Authority (FINMA) to create a collaborative approach that ensures both market integrity and flexibility for growth.

For INATBA members, if self-regulation can exist and positively impact the existing Financial markets, then it should be a starting point for DeFi regulation and a placeholder for additional policy making. Not every aspect of the market needs top-down regulation, and this DeFi report explains why this is especially true for permissionless, on-chain financial applications. Especially as competitiveness is transforming into a key goal of the EU, yet another premature policy expansion may be a step in the opposite direction for Europe's interests.

The scope of this report will start by defining what "true" DeFi is, why it is valuable, how it differs from existing DeFi applications, as well as how it differs from Traditional Financial. The report then shifts to deep dive into DeFi risks, both for today's status quo and for tomorrow's fully decentralized DeFi applications, which primes the third section of the report on how to effectively tackle these risks, now

and in the future. The report will conclude with a proposal to the industry for Self-Regulation; a proposal that seeks both industry feedback and implementation.

This report will exclude a few other key niches, namely consensus and yield staking, on-chain lending, NFT fragmentation and tokenization, emerging niches like Decentralized Science (DeSci), Decentralized Physical Infrastructure (DePIN) and Decentralized Social (DeSoc). These sub-niches of the market deserve their own reports and briefs, some of which will follow this document.

While reading this report, it is crucial to understand that “True DeFi” does not exist as of yet, besides in very few cases.

Considering regulating the DeFi industry today on the basis of non-DeFi incumbents, some of which may have failed or become fraudulent, beats the point of effective regulation. As regulators turn their attention onto DeFi, ensuring that their proposed frameworks support the emergence of true DeFi is a key step in the right direction.

Any entity starts off as centralized. For DeFi, the gradual decentralization of these protocols is crucial for their long term success, yet there is no framework or guidance on how to become compliantly decentralized. As such, there should be recommendations that indicate how the existing risk management frameworks can be applied onto this niche, as well as how these processes can gradually evolve to be implemented in decentralized protocols and during the decentralization process.

To this end, this document serves as a proposal for industry self regulations that will achieve the mission of policy makers, i.e. to ensure investor protections and financial stability, while also allowing the current DeFi niche to become securely decentralized and valuable to the overall economy and society.

The future of finance is unraveling right before our eyes. To grasp and bear its benefits, European policy makers should adopt the perspective of this report and embrace DeFi. Stakeholders should consider the perspective of this report and work towards making DeFi a safe and self-reliable industry that can unleash the benefits of the future of finance

2. Why DeFi Models Matter

DeFi is a disruptive movement within Crypto-assets and Finance that moves the operation of financial services away from centralized models operated by very clearly identified actors, and onto automated, permissionless and transparent processes, controlled by no single entity, but by a collection of stakeholders that, sometimes, upgrade and change a system through clearly defined governance processes. As such, DeFi takes a new path in the industry which allows any participant to be part of the evolution of the system, while truly prohibiting no one from accessing said Decentralized Financial service.

Openness, transparency, immutability and automation are key parameters of DeFi, and the main prerequisites into defining what is truly Decentralized Finance, versus what is aiming or claiming to be DeFi without actually being truly open, transparent, immutable and automated. With that in mind, it is important to ensure that Regulators comprehend the potential of true DeFi, where such Financial systems are flawless and accessible by everyone, everywhere. Similarly, they should know how these systems differ from the reality of the DeFi market today, where we can see various degrees of both decentralization and “flawlessness” in these systems.

As such, INATBA members believe that DeFi protocols should be self-controlled and fully transparent once implemented. The corollary is that DeFi protocols should require fewer controls if they meet or exceed the minimum standards outlined in this paper, as should previously centralized protocols which are now meeting or exceeding these aforementioned minimum standards. Negative outliers and examples of so-called Decentralized protocols which imploded due to fraud or heightened operational risk should not be the motivators for regulatory action, but instead guidelines to the creation of best practices that ensure other protocols do not copy such mistaken behavior on their route to decentralization - something that can and should be achieved through self-regulation and fewer controls.

As DeFi Protocols deserve fewer controls than Traditional Finance, they do not work with legacy systems as of now. However, if DeFi protocols are permitted to operate in a suited compliance framework, they would provide the industry with less frictional costs, faster and more efficient operations and higher transparency than traditional Financial systems. The resources of all participants can thus be reallocated to more value-added tasks, resulting in a better experience for the end consumer.

It is for this reason, therefore, that INATBA and its members would like to see the implementation of a self-regulatory framework that ensures continuous innovation while simultaneously ensuring consumer safety, financial transparency and clear best practices.

3. Definitions and Key Terms

3.1 Defining DeFi

Decentralized Finance, or simply “DeFi”, is a financial system that is built on top of blockchain technology. It allows customers to access crypto-assets-based financial services without the need for a central authority to govern the delivery of said services. DeFi applications utilize smart contracts, which are self-executing deterministic code stored within the programmable blockchains, like Ethereum. By using open source smart contracts, there is no need for a third party to verify or enforce the terms of this service.

Upgrading these protocols, or changing them, comes through on-chain governance operations that are also run on smart contracts with pre-determined governance structures, thresholds and institutions. Governance is an important fraction of what determines a protocol to be DeFi.

Due to the emerging and young nature of the industry, INATBA and the IOTA Foundation conducted a survey in February and March 2023 to solicit feedback from industry stakeholders about how they would define DeFi.¹ Based on both the survey results and additional the literature review, certain key concepts were identified:

1. DeFi is described as a new financial system that operates in a decentralized manner, without the need for intermediaries.
2. DeFi is based on the use of open, permissionless Distributed Ledger Technologies (Blockchain), and open-source smart contracts code.
3. DeFi enables financial freedom, providing universal access and self-reliance.
4. DeFi, as of right now, operates on the assumption of trustless interactions.
5. DeFi decentralizes the governance of the institution that provides these financial services, making them jurisdictionally agnostic by nature.

With the information provided by this research, the current working definition for true DeFi is:

Automated, open-source, trust-less financial systems operating through decentralized, open-source protocols, built on top of decentralized, robust blockchains, and supported by transparent, open-source smart contract code, which executes deterministic operations once certain data fields and on-chain fees have been submitted by any and all wallet address.

¹ The IOTA Foundation requested input from the general public and INATBA directed its survey to members of INATBA. In total, [141 + x] responses were received across the two surveys.



3.2 Defining TradFi

TradFi, short for “traditional finance”, is the established financial system most people interact with in their daily lives. TradFi, a term used primarily by crypto-asset industry participants, is best represented by the banks, investment companies, insurance, and other financial institutions that interact with each other over an intertwined, trust-based industry supported by a collection of isolated operations. In recent times, and due to the interconnectedness of the industry, communication processes and institutions have been established in order to ensure the proper functioning of TradFi, an industry whose potential collapse can have cascading impact in the overall economy. Importantly, traditional finance is the largest and most impactful industry in the globe.

TradFi is often used as a reference point and an example of what can be amended and improved by smart contracts and crypto-assets. Some financial regulation can be used when applicable onto crypto-assets with similar operational characteristics and risks, however, a direct transition of traditional financial regulations onto this new paradigm that is led by the emergence of DeFi and crypto-assets would enforce rules that are not accurately tailored to the needs and operations of DeFi; hindering the potential growth of the industry while also failing to address the true risks that DeFi operations may face.

3.3 Defining CeFi

CeFi, abbreviated for Centralized Finance, represents the vast majority of existing financial operations within the Crypto-asset market. The main characteristic of CeFi is the offering of crypto-assets services through centralized structures, like crypto-asset exchanges and neo-banks. In CeFi, users trust these central authorities (i.e. CASPs) to handle their crypto-assets transactions. These central authorities maintain control over the customers’ funds and personal information and usually require regulatory compliance such as KYC (Know Your Customer) procedures. The central authority also often organizes the custody of the crypto-assets and charges fees for its services.

3.4 Defining CeDeFi

CeDeFi, or centralized decentralized finance, is the merger between centralized and decentralized finance. Due to the perceived complexity of DeFi operations, centralized CASPs have tailored their services to provide DeFi-like operations for their customers. Such CASPs offer a curated, custodial experience when it comes to crypto-asset staking, lending and other core DeFi services, like liquidity provisions. The stated benefits are plentiful, especially since the transaction fees of these operations are significantly lower than popular on-chain alternatives. However, some of the biggest industry collapses in recent times have come from CeDeFi, where overexposure during market downturns have produced significant outstanding liabilities for such CASPs, and imploded their CeDeFi offerings. Examples of this came from platforms like the Celsius Network and BlockFi, which promised inflated returns to their customers, and which both collapsed in late 2022 and early 2024 respectively.

3.5 Defining Security vs Non-Security

Within the European Union, Article 4.44 of the Markets in Financial Instruments Directive II (Directive 2014/65/EU), MiFID II, defines transferable securities as those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as:

- (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
- (b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;
- (c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.

The list provided in MiFID II holds zones of definitional shadows that make it often difficult to know what is and isn't a security. That opens the door to member states having different interpretations of securities in their national laws, which creates a barrier to full capital market integration and cross-border specifications. This also impacts the adoption of financial innovation, as an example, the same crypto-asset that may fall under MiCA in Spain, may also fall under the German interpretation of MiFID II and their definition of a security.

To this extent, this report differentiates Securities from DeFi tokens. In all three of the parameters mentioned above, Securities have an issuer who's fiduciary duty and professional activity is necessary to ensure the increase in the valuation of the transactable security, or the repayment of the outstanding bond. While in DeFi, such activity is neither expected nor necessary for the successful functioning of truly Decentralized Financial protocols and their respective tokens.

3.6 Defining Decentralization and Measuring it

When measuring decentralization, a few key considerations should be taken into account. A decentralized network has different thresholds and specifications to a decentralized financial protocol. What makes a blockchain decentralized does not guarantee that the protocols built on top of it are decentralized. On the contrary, a fully decentralized protocol built on top of a centralized chain is equally far from true decentralization.

As such, in this analysis we will measure the various degrees of decentralization and the key functions that impact the development of a DeFi protocol. Below is a list of these key parameters:

1. Network Selection: The Network that the protocol is built on, and its robustness and permissionlessness.
2. Governance Structure and Operation: How the protocol is built to allow people to vote, as well as how these votes are counted.

3. Governance Token Distribution: Is the DeFi Governance Token, i.e. the token that can be used to control the DeFi protocol, owned by a few major stakeholders, or is its ownership decentralized enough to truly represent the interests of its users and the overall industry?
4. Smart Contract Admin Key Control: Who can change the code, and what are the processes they must go through to do so?
5. Control of non-chain community platforms: Where do people interact to discuss topics related to the DeFi Protocol, and who controls these forums? Can there be top-down censorship?
6. Treasury Deployment and Decentralization: For integral, key funds that are used to develop the protocol, who is in charge of managing these funds and what are the processes they must go through to manage these funds.
7. Oracle Selection and Dependence: For key smart contract operations that need external information sources, which oracles are used and who selects them? Can they be altered? If yes, what is the process to select these oracles?
8. Multiplicity of Touch Points with TradFi: How is the protocol in question affected by other, centralized protocols? How is it impacted by on and off ramps, custodians, and reference assets?
9. Operational Resilience and Need for Centralized Service Providers: How is the protocol in questions affected by operational service providers? How is it impacted by cloud providers, website hosting services, communication platforms and other software service providers?

For each of these parameters, the degree of decentralization and “permissionless-ness” enhances the protocol's potential decentralization and robustness. In short, this creates a spectrum of decentralization, where a clear threshold for decentralization is hard to set. Upon the initial analysis, such a threshold might become clearer, as well as how to measure the direction of a protocol's movement towards decentralization.

This complexity is enhanced by the continuous changes that these verticals may face according to market conditions and off-chain events, like the collapse of Silicon Value Bank or other centralized software outages. To this extent, the proposed self-regulatory threshold should be measured bi-annually, and on an as-needed basis, in cases of major market events.

In this context, protocols at various stages of their decentralization journey are encouraged to use the guidelines of this report to enhance and progressively achieve meaningful decentralization, guided by metrics that reflect their specific characteristics and growth trajectory towards fully decentralized organizations.

4. Types of Risks

To understand the risk profile of DeFi as compared to the traditional financial sector and other non-decentralized financial institutions within the crypto-asset industry, this section reviews existing risks as compiled by international institutions like the Basel Committee, COSO and OSFI-BSIF.

You can find these Compliance and Risk Management Frameworks for [COSO here](#) and for the [OSFI-BSIF here](#). The section will thus produce clear distinctions of risks between DeFi and TradFi, as well as similarities in Risk Profiles.

4.1 Taxonomy

The classification of risks is the basis for the establishment of a risk universe and for the risk assessment. Establishing a risk universe requires a good knowledge of all aspects of the entity under review. The risk universe is made of types of risks, or also called risk dimensions. They are opposed to individual risks that are specific risk elements linked to a specific process. The list below is not completely exhaustive. Some industries might highlight specific risks, however, most of them can be linked back, one way or another to the list below.

4.1.1 Strategic Risks

The Strategic risks category includes the risks that result from the environment of the entity, from decisions of the entity or from specific entity activities.

4.1.1.1 Strategy

This risk relates to the strategic choices of the entity.

A strategy is a careful plan or method for achieving a particular goal usually over a long period of time. In the business sense of the word, the strategy of the entity is the set of high-level actions that the entity will take to meet its objectives.

The tactical actions are more finite actions that allow achieving the strategy of the entity. The strategy risk is the one that is related to the uncertainty of picking a strategy up.

Strategy Risks exist equally in both DeFi and TradFi.

4.1.1.2 Business

The business risk is any risk related to the change in business environment leading to a change of volumes, variation in demand, and other external factors. That covers aspects like client concentration, client evolution (e.g. one goes bankrupt), regulations governing the activity, change in the political context, change in the economic context or change in the client's needs.

Business Risk exists in both DeFi and TradFi, with a heightened risk existing in DeFi due to the expected regulatory movements that will target such activities. For the essence of this report, these will be treated equally.

4.1.1.3 Legal & Compliance

The legal risk is the risk that one event impacting the entity might result in a legal action. It is any risk related to a legal action taken by or taken against the entity. Alternatively, it is the risk that the entity is not adequately protected from a legal perspective.

By default, and as legal actions are usually not core to the business of an entity, this risk falls within the strategy category. Legal also covers the compliance risk. Compliance risk is the risk related to not complying with the laws and regulations.

All Traditional Finance, Centralized Finance and Decentralized Finance suffer from this risk, with DeFi being especially vulnerable to compliance due to the lack of regulatory clarity. On the other hand, once true DeFi protocols are activated, legal risk falls to zero for such automated, self-executable financial operations due to their transparency, automation and immutability.

4.1.1.4 Environment, Negative Impact on Society and Governance Risk (ESG)

ESG Risks are the potential negative impacts that a company's operations or supply chain can have on the environment, society, and its own governance practices. These risks increase in importance as the organization matures.

Although all businesses have ESG Risk, DeFi Protocols are indirectly connected to ESG risk by operating on top of protocols which may, but often do not, have a substantial environmental impact. As with every financial venture, DeFi can have a positive or a negative ESG impact on society depending on its structure and network selection. In fact, the underlying blockchain network plays a key role in determining the environmental impact of a DeFi protocol. For instance, Proof-of-Work (PoW) blockchains require substantial energy to operate, raising concerns about carbon emissions. On the other hand, Proof-of-Stake (PoS) blockchains are significantly less energy-intensive.

Because of the decentralization of protocol governance, DeFi has its own challenges in this field of Governance. This does not mean that DeFi is, de facto, more risky than TradFi models. In other words, DeFi has the potential to improve both financial inclusion and governance structures while minimizing environmental impact if built with ESG in mind. Therefore, the structure of a protocol and the underlying network choice are pivotal in determining the overall ESG impact of DeFi ventures.

4.1.1.5 Reputation

Reputational risk is any event that impacts the image of the entity. Reputational risk is often difficult to measure. Once an entity is sued, for any reason, its reputation may be hit. In this situation, reputational risk is true and accurate, but it is difficult to put a monetary figure on the decrease in the entity's reputation.

All Traditional Finance, Centralized Finance and Decentralized Finance suffer from this risk, with DeFi being particularly vulnerable to reputational risk when specific protocols are found to not be decentralized, automated and transparent. In this sense, DeFi as a term is also vulnerable to reputational risk if it is not defined properly - something that this report aims to help with.

4.1.1.6 Brand

This is the risk that impacts the image of a brand of the entity, and therefore the brand's value. The difference with the reputation risk is that the latter is attached to the entity only, and not the entity's sub-brands.

All Traditional Finance, Centralized Finance and Decentralized Finance suffer from this risk.

4.1.1.7 Capital Risk

The capital risk is the risk of not having the right amount of capital to run the activity.

Due to the nature of smart contracts, Capital Risk is significantly lower in Decentralized Finance than in Traditional and Centralized Finance.

4.1.2 Operational Risk

Operational risk is all the risks related to running an operation. It is a fairly vast domain and probably the most important one in all industries, outside of the Financial Services.

The Basel Committee, an important source of references for risk management, defines operational risk as: "The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

Such risks exist within DeFi, but arguably less so than in TradFi. Operational risk in DeFi is primarily found during crucial points in the protocol's development, such as sybil attacks during major governance votes, or technological attacks during smart contract alterations and upgrades. Due to the immutability and impact of these actions, this risk is higher in DeFi than in TradFi.

4.1.2.1 Internal Fraud

Internal Fraud is the risk of a stakeholder not being in compliance with laws and regulations, exposing the system to a potential fine, as an entity is traditionally responsible for the acts of its stakeholders.

In this category, one may find the misappropriation of assets, tax evasion, bribery instigation of officials and theft of information from computer systems. This risk is very frequent within all organizations that deal with information, including in DeFi, but less so compared to TradFi due to the transparency provided by the Blockchain.

These risks can be alleviated by the creation of self-regulatory standards and industry best practices, more so than additional regulation and requirements.

4.1.2.2 External Fraud

External fraud is the exposure of a system to the wrongdoing of someone external to that system. Common examples of such risk are the provision of fraudulent products by an external provider, the external theft of information, hacking and other related IT damages and forgery.

This risk is very frequent within all organizations that deal with information, including both TradFi and DeFi. However, once a DeFi protocol is deployed on-chain, such external fraud risks have a substantially smaller impact on the operations of the protocol's smart contracts.

4.1.2.3 Employment Practices and Workplace Safety

This risk is very present in all industries, but is not within the scope of risks placed within both Traditional and Decentralized Finance addressed in this document.

Workplace safety is particularly acute in industries where physical activity is present (e.g. metallic industries). Examples of such risk are discrimination, workers compensation, health, excess of structural overtime, dangerous physical activity and use of machinery.

We include in this risk all risk elements related to the pensions of employees. Some Financial Industries assessments (e.g. ICAAP) treat this as a separate item.

4.1.2.4 Clients, Products, & Business Practice

This risk covers items like market manipulation (e.g. Libor manipulation), antitrust, improper trade, product defects, fiduciary breaches, reporting excessive sales contracts to a client to create excessive commissions.

This segment covers the risk of client specific operations or incorrect business behaviors that lead to favoring only one party within a business transaction. This risk is very limited within DeFi due to the industry's code-first structure, besides the manipulation of oracles and other previously mentioned risks, like fraud and operational limitations.

4.1.2.5 Damage to Physical Assets

This risk emerges through the wrong use of assets leading to damaging such assets. This category covers the risks emerging from various hazards like natural disasters, terrorism, vandalism, and strikes.

As of now, this risk is very limited within DeFi but has occurred within TradFi in the past.

4.1.2.6 Business Disruption & Systems Failures

This category covers any unplanned stop of the activity of the company. This might result from utility disruptions, software failures, hardware failures and disruption in the supply chain (e.g. raw materials).

This is a recurring risk with both TradFi and DeFi. For example, private keys might be lost, admin keys to code might also be lost, systems may be hacked or paused due to software viruses, code may feature a bug or the network that a protocol operates on might pause its activity, and other such occurrences.

Overall, this risks features in both TradFi and DeFi, but it is more recognized within DeFi due to the maturity stage of the whole ecosystem.

4.1.2.7 Execution, Delivery & Process Management

This category covers all the unintended events that might impact the operations and delivery of services of the company. In this category, we will find items like data entry errors, accounting errors, failed mandatory reporting, error in the processing on an assembly line, error in maintenance, error in evaluating a new equipment, negligent appropriation of client assets, and other such mishaps.

Such risk exists within DeFi once a smart contract has been deployed, due to the ongoing nature and self-executability of the said smart contract. Software bugs might exist within Smart Contracts that are otherwise operational and active within a blockchain.

But, overall, due to the transparency and immutable nature of Blockchain, these risks are substantially less pronounced than in TradFi, where such checks and balances are not inherently there.

4.1.3 Financial Risk

Financial risk is a section of risks including any risk related to the financial management of the organization. This is an all-encompassing concept as the financial management of the entity is the result of the strategic choices, the zone where the entity sells its products, the way the entity is funded or the way it invests, and how it treats clients and providers.

4.1.3.1 Credit Risk

For all entities, the credit risk relates to the way a company invests its cash or cash equivalents. For example, if a company uses its excess cash to buy bonds of a government or of a business, it has a credit risk versus the said country or company.

Furthermore, this risk encompasses the frequency, timeliness and method that company's clients pay their invoices. Giving excess time to clients to pay their invoices is a form of credit. As such, credit risk can be defined as the risk that one counterpart defaults on the money they owe the entity in question. Defaulting is the mere fact of not paying the full sum of money when this invoice is due.

For simplicity's sake, the securitization risk, which is found in the financial industry, is also included in this category, as is settlement risk.

Within both DeFi and TradFi, credit risk is highly relevant. For TradFi, credit risk has been a topic of recurring focus, while in DeFi, credit risk is mostly related to the interconnectedness of crypto-assets used as collateral, or the reserve investment practices of treasury managers and stablecoin collateral managers. Regardless, credit risk is significantly more pronounced in traditional financial markets, since the programmable nature of smart contracts forces the return of staked collateral to smart contracts that may hold a protocol's assets, as in the case of Celsius Network.

4.1.3.2 Concentration Risk

Concentration risk is the exposure of a company, being in credit, in market or in turnover, to a limited number of counterparties or types of assets.

A simple example is of a company which only has two major clients and outstanding invoices for both, faces the default of one of their two major clients, where material outstanding balances are never paid due to bankruptcy.

The risk of concentration is the opposite of the diversification theory in modern portfolio management. Diversification allows for less correlation between portfolio assets, protecting the total value of the portfolio.

Concentration risk exists in DeFi and TradFi, with major crises occurring in both industries due to the lack of diversification of clients and their assets. Examples of this are the '08 Financial Crisis in TradFi and the collapse of the 2022 Cryptoasset Market due to Terra Luna in DeFi.

4.1.3.3 Liquidity Risk

The liquidity risk is the risk that an organization does not have enough available cash to meet its obligations on time, and hence defaults. Lack or loss of working capital is also reflected by this risk category.

Indeed, cash, client invoices and providers' invoices constitute the natural components of this concept and hence are key parameters of the liquidity risk. However, in both DeFi and TradFi, liquidity risk has been largely alleviated by overnight lending (for TradFi) and by overcollateralization in DeFi. In short, this risk is more pronounced in TradFi than in DeFi.

4.1.3.4 Market Risk

The market risk is the one induced by a variation of the conditions in the financial markets, for example, risk related to currency exposures or interest rates. This also encompasses systemic collapses and sentiment downturns.

When reviewing DeFi Protocols or TradFi institutions, like banks or insurance companies, Market Risk may be equally considered as credit, financial or de-pegging risk, since all of these risks impact market sentiment and have wide-spread influence on financial markets.

For DeFi, this risk may be more pronounced as of right now, since the overall crypto-asset market works in cycles, and sentiment plays a significant role in the market value of collateral assets, lending rates and overall economic activity and revenues.

4.1.3.5 Insurance Risk or Insurance Underwriting Risk

Insurance risk is specific to the insurance companies. It covers all risks induced by a difference in the expected service of the insurance contracts vs. the actual service of such contracts.

For DeFi, such risk is not significant, since insurance is a practice of limited scale as of today. As such, insurance risk is found almost exclusively in Traditional

Financial Markets, with the exception of a few DeFi protocols, like Nexus Mutual, who have yet to attain substantial market reach.

4.1.4 Emerging Risks

These are all the risks that emerge in the environment of an entity but that have not been identified and classified. As expected, emerging risks are very much in scope of DeFi, where a number of operations might produce unexpected risk, and where continuous innovation might produce consequences that few predicted. Examples of such risk are MEV market manipulation risk, rehypothecation (i.e. under-collateralization) risk, and other technical risks.

These risks exist in TradFi too, but impact DeFi significantly more.

AML/KYC/ATF Compliance for DeFi Protocols:

Anti-Money Laundering (AML), Know your Customer (KYC) and Anti-Terrorist Financing (ATF) are core principles of traditional finance that aim to ensure that financial institutions are not utilized to assist criminals, hostile governments and dangerous non-state actors. These measures are mainstays in TradFi. These principles are also aspired by the Crypto-asset industry and DeFi.

However, at present, compliance of the DeFi industry to AML/KYC/ATF requirements is improbable, since accurate requirements, designed to fit the existing technology and its potential, simply don't exist. This increases compliance risks for the whole industry. A part of the consideration that policy makers should have is the need for such stringent AML/KYC and ATF requirements in an industry; an industry which is still extremely young and significantly more transparent than TradFi.

With this in mind, part of the goals of this document is to highlight the proper monitoring of the DeFi industry on such parameters, as well propose the most appropriate measures to mitigate these risks without hindering the future of digital finance and DeFi. Until the creation of such self-regulatory frameworks, the absence of the regulation for DeFi protocols allows these protocols to work without KYC/AML measures, seamlessly providing their service to any on-chain address. To ensure the accurate specification of the degree of such risks, INATBA is producing ongoing work, outside of this report, which aims to highlight the current levels of AML and TF activities.

More information on these levels of risk will be provided in 2025. Until then, it is this report's recommendation that KYC/AML compliance should be conducted by MiCA CASPs, namely on- and off-ramps that connect the real economy with the digital economy, and are already in place through the implementation of MiCA.

INATBA member's final thoughts on this specificity are trifold. For INATBA members, the implementation of KYC/AML controls should not be placed within the technology layer of DeFi. In other words, such compliance should not be force onto smart contracts, since it makes compliant services less competitive than their open source and permissionless alternatives, while also adding technological complexity that can introduce heightened risk. In case such requirements are

introduced in the market, the division of the DeFi ecosystem is highly expected, with some participants choosing to work with non-compliant protocols, while others selecting the compliant alternative.

In either case, the need for a real-time, public and transparent dashboard of DeFi risk, including analysis conducted by analytics firms, like Chainalysis, Crystal Blockchain and AMLBot, will produce a public repository of knowledge that aligns perfectly well with the industry's desire for self-regulation and intelligent compliance.

4.2 Risk in DeFi vs Risk in TradFi

The essential objective of this report is to define whether Decentralized Finance (DeFi) presents the same risks as Traditional Finance (TradFi). This analysis is conducted on the principle of "Same Risk, Same Rules" which has dominated the consideration of regulators while conducting analyses on the need for additional obligations.

In brief, industries which have different risks while conducting the same operations must be accompanied by different rules. In these forthcoming section, we aim to provide more clarity on the need of new rules, whether self-imposed or through regulation, by analyzing four categories:

- A. Risks that exist in both TradFi and DeFi.
- B. Risks that exist in TradFi, but not in DeFi.
- C. Risks that exist in DeFi, but not in TradFi.
- D. Risks that Exist in DeFi now, but should not exist in True DeFi in the future.

The purpose of this analysis is to provide a clear distinction of where risks remain unmitigated by existing regulations and propose a self-regulatory standard that makes technical sense and can be implemented by industry participants effectively and without limiting the industry's potential, as well as highlight the potential of less risky financial application once decentralization is effectively achieved.

The below table assists in this analysis and comparison:

Categories	TradFi & DeFi	More in TradFi	More in DeFi	Not in True DeFi
Strategy	✓	N/A	N/A	N/A
Business	✓	N/A	N/A	✓
Legal	N/A	N/A	✓	✓
ESG	N/A	✓	N/A	✓
Reputation	✓	N/A	N/A	✓
Brand	✓	N/A	N/A	✓
Capital	✓	N/A	N/A	✓
Internal Fraud	N/A	✓	N/A	✓
External Fraud	N/A	✓	N/A	✓
Workplace Safety	N/A	✓	N/A	✓
Practices	N/A	✓	N/A	✓
Damage to Assets	N/A	✓	N/A	✓
Systems Failures	N/A	N/A	✓	N/A
Management	N/A	✓	N/A	✓
Credit Risk	N/A	✓	N/A	✓
Concentration Risk	✓	N/A	N/A	N/A
Liquidity Risk	N/A	✓	N/A	✓
Market Risk	✓	N/A	N/A	N/A
Insurance Risk	N/A	✓	N/A	N/A
Emerging Risk	✓	N/A	✓	✓

4.2.1 Risks that Exist in Both TradFi and DeFi

DeFi and TradFi share a lot of similarities in their risk profiles. After all, they are both financial service providers, either through traditional means or through on-chain, automated and smart-contract based means.

As such, while conducting our analysis, the list of risks that we designated to be both in TradFi and in DeFi are substantial. These risks are:

1. Strategic Risk:
 - a. Strategy
 - b. Business
 - c. Reputation
 - d. Brand
 - e. Capital Risk
2. Financial Risk:
 - a. Concentration Risk
 - b. Market Risk
3. Emerging Risk

In our analysis, it is important to note that the risks found currently in DeFi but which can be alleviated through the proper Decentralization of the protocols are not listed.

Also important to note, this analysis comes primarily from the perspective of the entity in question, and not the consumer and end user of the protocols or financial service, since the report aims to provide recommendations of the self regulation of such entities.

4.2.2 Risk in TradFi that Does Not Exist in DeFi

TradFi risks are outlined in this section. This analysis has a special focus on the risks that emerge primarily through the inefficiencies produced by manual processes and physical operations, it also takes into consideration the follies of human nature.

1. Strategic Risk:
 - a. ESG Risk
2. Operational Risk:
 - a. Internal Fraud
 - b. External Fraud
 - c. Employment Practices and Workplace Safety

- d. Clients, Products and Business Practices
 - e. Damage to Physical Assets
 - f. Execution, Delivery and Process Management
3. Financial Risk:
 - a. Credit Risk
 - b. Liquidity Risk
 - c. Insurance Risk

In this section, it is important to understand that risks, like both internal and external fraud, exist in DeFi as of right now, but would be significantly more pronounced in TradFi, especially TradFi that was at the same regulatory level of clarity as seen in DeFi. As such, the section highlights that such risks are inherently less risky in DeFi than in TradFi, and will become significantly less risky once the protocols in question reach effective and true Decentralization.

Active DeFi projects which are currently DINO's (Decentralized in Name Only), are not considered in this section, and will be discussed in the fourth entry of this chapter. Important to note, that all organizations start off centralized, and strides have been made by the industry towards becoming more and more decentralized.

With that in mind, this section will explore TradFi risk that shouldn't exist within true DeFi.

4.2.3 Risk in DeFi that Does Not Exist in TradFi

DeFi risks are listed in this section. Namely, DeFi risks that will persist after, or are independent of, the emergence of True DeFi, and the self-regulation of the industry. These risks are:

1. Strategic Risk:
 - Legal & Compliance
2. Operational Risk:
 - Business Disruptions and Systems Failures
3. Emerging Risks:
 - (Multiple Outlined Below)

There are several risks that exist in DeFi but not in TradFi mainly due to the technology, business models and geographic disparities; all of which fall under the Emerging Risk label.

These Emerging Risks are primarily created because of the ever-changing and innovative nature of Blockchain, DeFi and other on-chain organizations and innovations.

Some of these risks are:

- **Impermanent Loss Risk:** The design of Liquidity Pools (LPs), which are necessary for the execution of transactions, exposes users to a hidden and non-definitive loss of capital.
- **Forced Overcollateralization Risk:** Even for highly trusted parties, the design of smart contracts inherently forces overcollateralization, creating more inefficient markets compared to TradFi. Fractional Reserve Banking capabilities are not probable under this new paradigm.
- **Cryptographic Risk:** Systemic risk within DeFi. This is the risk of the whole industry collapsing if vulnerabilities are found and exploited within the cryptographic primitives used across the technology and industry. Our analysis indicates that there is a very low possibility of this happening.
- **Smart Contract Finality and Smart Contract Exploitation Risk:** Smart Contract Finality and Exploitation risk are both primarily due to the immutability of blockchain technology. Once a smart contract is deployed, and the admin keys for this contract are burned, there are no changes allowed onto this contract. This means that the addition of any and all new features needs to happen onto a different smart contract. This is a problem since users must manually select to remove funds from the existing contract and to interact with the smart contract, which is both tedious and difficult.
This risk becomes more pronounced when the old smart contract may feature bugs that most users are unaware of. Hence the heightened and related Smart Contract exploitation risk.
- **Architecture complexity:** Despite overall transparency due to the Smart Contracts open source nature, the structural complexity of these operations creates a highly complex process that most users cannot fully understand or fully engage with.
- **Smart contract audits:** Auditing the code of a Smart Contract is an essential best practice adopted by the DeFi industry; yet it breeds uncertainty, since it is not always efficient nor bulletproof. The reality is that many protocols audited by multiple reputable companies have nevertheless been hacked following their audit.
- **New products risks:** In this section we address some of the emerging risks within new products found within DeFi. Again, please note that these risks are primarily caused by the young and innovative nature of the industry, and plenty of these risks will be alleviated once DeFi protocols are truly pushed onto true decentralization.
 - **Flash Loans:** Flash Loans are instant, no-limit loans that settle in the same block that they've been borrowed. This is because same-block settlement produces no risk to the lender(s).

Flash Loans are often used for exploitation hacks, where the attacker takes advantage of unlimited liquidity to drain a smart contract from



its collateral or staked assets.

Flash Loans will continue to be tools that allow for smart contract exploitation, even if protocols are fully decentralized, as long as inefficiencies are found within the smart contract code of said protocols. No other solution than the creation of best practices in the technical development of smart contracts through self-regulation.

- Address Poisoning: Address Poisoning is the risk of complaint addresses intentionally being sent blacklisted funds intentionally.

These attacks were used primarily after the creation of OFAC's Smart Contract Blacklist as a political response by industry participants.

- Bridge Risks: Cross-chain Bridges are frequently used to transfer funds from one Blockchain to another. To achieve this, the smart contract is granted access to the wallet and funds of their user.

This creates a centralized risk point where these contracts can be used by hackers to drain the wallet of the participant on both sides of the Bridge.

Bridge hacks have been favored by malicious actors, being used for the most lucrative hacks that the industry has faced in its existence. The creation of trustless, decentralized alternatives can alleviate these risks, although Smart Contract risk will persist until fully tested.

- Oracle Risks: Oracles feed data onto on-chain Smart Contracts. If the data fed into the smart contract are wrong, the Smart Contract will execute its processes incorrectly. Oracle attacks have historically been the weakest link in Smart Contract security.
- MEV: Minimal (or Miner) Extractible Value is defined as the arbitrage that network validators can enjoy once able to control the transaction included into a block. This can be seen in three forms; front-running, buck-running or the combination of the two through Sandwich Attacks.

These attacks allow the Miner/Validator to manipulate the ordering of transactions in order to extract the most value for themselves in this upcoming block. For example, the miner can see a major sell order coming in for a crypto-asset, allowing him to place his own position first, submit the massive third-party buy order second, and sell his own position first, making a clear arbitrage by manipulating the market.

MEV attacks cannot be stopped by regulation, and only self-regulation, or a major consensus update, can enforce the limitation of this process and risk.

- DAO Risks: In this section we will discuss the risk found within Decentralized Autonomous Organization (DAOs) and so-called DAOs,

which are neither Decentralized or Autonomous. It is important to note that most DeFi protocols are DAOs of their own.

- Pretend Decentralization: The biggest and most pronounced risk in DAOs are the organizations which pretend to be decentralized while being controlled by a few key actors. This is extremely common in today's market environment, where only a handful of Venture Capitalists and the founding teams of the protocols can control the majority of Governance power for the DAOs that control DeFi protocol.

This is especially true when the DAOs may have unknown governance backdoors, producing a riskier environment for retail investors and users of the protocols.

Centralized Governance will likely be solved as the industry matures, and major stakeholders diversify their holdings. This is also not a problem for protocols with minimum governance processes; a key parameter in their journey to long term Decentralization.

Secret backdoors, however, are a major risk that can be alleviated only with Smart Contract best practices and audits, and are the target for the industry's Self Regulatory push.

- Re-entrancy attacks: This is a bot-related attack, where the Smart Contract caller tries to withdraw funds several times in a short timespan, extracting more funds from the protocol than his actual balance and before the protocol is able to verify the addresses outstanding balance.

This is a rare attack, similar to the double spend problem of the underlying infrastructure, and will be alleviated through time.

- Rug pulls: Rug Pulls are coordinated fraudulent attacks by the administrators of a Smart Contract to the financial backers of their token in Automated Market Makers. In short, the founders of the protocol in question dump their token into an exchanging pool, draining the pool of the valuable counterparty asset in exchange for their native tokens, which are then gradually priced at lower and lower prices until they are valued at zero and the second side of the Liquidity Pool is empty.

Although this can occur on TradFi, it is less prone due to the implementation of standards and the absence of founder pseudonymity.

- Liability: Due to the nature of DAOs, there is no clear legal responsibility determined in any potential legal proceedings. In short there is no one to blame for fraudulent activity.

4.2.4 Risk in DeFi that Will Not Exist in “True DeFi”

The main motivation behind INATBA’s push to self-regulate DeFi is two fold. First, the industry is extremely nascent, which means that innovation must be protected, and that the entities and consumers engaged with DeFi are a fraction of the general population with high expertise.

Secondly, the potential of this industry to alleviate risks found both in Traditional Finance and in the current form of DeFi are undoubtable. The protocols themselves can be transparent and self-executable, providing a deterministic outcome for any and all on-chain financial operations without the need for regulatory checks and balances. These attributes increase efficiency and widespread financial access to the persons that need it the most. For jurisdictions that have an underdeveloped financial system, DeFi, in present, offers an efficient and preferable alternative.

With this in mind, it is crucial for this analysis to explain how True DeFi (i.e. truly decentralized protocols on-chain) can remove most of the risks that exist in DeFi today. Therefore, in this section we address how the risks listed in the previous sections can be effectively addressed by INATBA’s proposed self-regulatory proposal, which is expanded upon in the last section of this report.

We start this analysis below, with the list of risks found under the DeFi section:

1. Strategic Risk:

- Business:

DeFi’s automation and over-collateralized nature allows for business risks to be automated away. In short, the protocols themselves will never face the risk of bankruptcy; instead they will operate as usual.

- Legal & Compliance:

The lack of regulatory clarity limits the potential growth of DeFi protocols. It follows that upon the attainment of regulatory clarity, these limitations will disappear.

- ESG Risk:

Out of all three ESG risks, Governance is the only one appropriate for the current form of DeFi. In the long term, governance best practices will emerge only through experimentation and self-regulation. Important note is that governance itself can be decentralized away; since many protocols do not need governance to execute the objectives of their protocol.

- Reputation:

Reputational risk in DeFi is primarily the false presentation of existing protocols as decentralized and permissionless entities. This risk will fade away as the protocols in question continue to decentralize their ownership and governance.

- Brand:

Similar to reputational risk, brand risk will dissipate with time, and as protocols prove their robustness and permissionless through our proposed self-regulatory regime.

2. **Operational Risk:**

- Internal Fraud:

At present, so-called Decentralized protocols may fall victim to internal stakeholders that have oversized control over the protocol and can disrupt and hurt its operations. Again, with self-regulation, time and best practices, these risks can be alleviated entirely in the long run.

- External Fraud:

Fully decentralized protocols will be autonomous, robust and permissionless, avoiding the risk of external fraud entirely.

- Employment Practices and Workplace Safety:

The automated nature of true DeFi protocols removed the need for employees and workplaces, and removed such risks.

- Clients, Products and Business Practices:

The only risk that falls within this category for True DeFi is the manipulation of Oracles, where best practices for the input of off-chain data onto operations can be changed to benefit external market manipulators. Oracle risk is primarily a technological risk, where existing solutions have already alleviated most of these risks.

- Business Disruption & Systems Failures:

This risk is very limited in DeFi presently, and it exists purely because of the industry's early stage of development. With self-regulation and time, such disruption will cease to exist.

3. **Financial Risk:**

- Financial Risk in "True DeFi" does not exist as it does in TradFi. This is primarily due to the overcollateralized nature of the industry, and the automation provided by smart contracts. Risk of simultaneous market downturn due to economic shocks is, however, quite pronounced in autonomous and automated economies, like in on-chain finance.

4. **Emerging Risks:**

- Emerging risks in DeFi, as listed in previous sections, are significantly more detailed and specific risks to DeFi that have not been featured in other risk analyses protocols since they are inherent to on-chain processes, and deserve to be addressed through industry self-regulation before a regulatory framework is imposed onto them.

Most of these risks above can be tackled through the maturing of the industry, the best practices instigated by self-regulation, and, sometimes, by the recognition of new entities which are native to DeFi and on-chain organizations like DAOs.

4.2.5 Findings & Regulatory Recommendations on DeFi

From the identified risks unique to present-day DeFi, it seems clear that current laws were not designed to provide a fair, comprehensive, and safe regulatory framework for DeFi - neither in today's form, which is, expectedly, riddled with risks, nor the potential "True DeFi" that the members of INATBA want to see realized.

In this sense, DeFi requires a specific self-regulatory framework that is enhanced with minimal regulatory activity. The main aspects to consider when drafting new laws is:

- A. Can these risks be alleviated through the implementation of the self-regulatory actions described in the next section of this report? and;
- B. How can regulations help cover additional risks that cannot be addressed through proper self-regulation?

Therefore, below are the actions that must be taken to ensure a safe environment for investors and the transition onto a new paradigm in Finance that is best suited for the future; with less risk and less centralized controls.

As such:

- The framework shall define who is the end beneficiary of a protocol;
 - Is it the early stage DAO developers and associated technical team?
 - Is it the major token holders, including founders and VCs?
 - Is it the DAO itself, under a new or existing incorporation form?
 - And shall the liability claims laws of the country where the end beneficiary is located apply?
- The framework should define what a DAO is, and what a DAO isn't.
- The framework should remove KYC/AML requirements from Smart Contracts and place them onto regulated intermediaries, like on/off-ramps and centralized exchanges (CEXs).
- The framework must include responsibility of the issuer of real-world assets utilized within Smart Contracts and related DeFi protocols. Such issuers may fall under MiFID II.
- The framework shall create an assessment process that labels DeFi products on the basis of their resilience, compliance and security.

A Proposal for the Industry

- The framework must ensure the creation of Smart Contract best practices and audits, with public and trusted results that are easy to understand for both institutional and retail investors.
- The framework shall motivate the utilization of Zero Knowledge cryptographic primitives that allow the end user, especially retail users, to preserve their right to pseudonymity; otherwise, these wallet holders risk being threatened for their holdings.
- The framework shall provide compliant CASPs with the legal authority to block suspicious funds that are sent to their platforms; especially in known cases of theft, fraud and hacks. Authorities should also be able to get KYC information for these suspicious accounts.
- The framework should ensure the proper incentivization necessary for the rapid adoption of trusted, decentralized and verified DeFi protocols that are compliant. These may include:
 - Limited capital protection.
 - Government funding and support.
 - The creation of complaint rails for the deployment of institutional funds.
 - The enshrinement of banking and licensing rights to complaint DeFi entities.
 - The strategic investment into Blockchain infrastructure, such as miners and validators, to ensure the proper governance and processes of the network as a whole (i.e stopping MEVs).
 - Providing best practices and branding educational material that ensures a common level of retail investor comprehension of these technologies.
- Importantly, any regulatory framework should be technologically neutral, ensuring that all Decentralized Consensus technologies and their applications are allowed to flourish with this framework.
- Design a “good conduct” list of rules for DeFi, and of trusted, compliant DeFi operators.

The above targets can ensure the long term safety and adoption of DeFi and Blockchain-enabled Finance. However, some of these goals cannot be achieved only through self- regulation, and may need a coordinated regulatory framework.

The distinction between the processes that need regulations instead of self-regulation will be covered in the final section of this report.



4.3 Contagion Policies between DeFi, DAOs, DApps, CASPs & TradFi

The relationship between decentralized finance (DeFi), decentralized autonomous organizations (DAOs), decentralized applications (DApps), and crypto asset service providers is intricate, with each component playing a role in the broader ecosystem of digital finance.

The intricate relationship in the digital finance ecosystem is due to the high degree of interdependence at both functional and operational levels among various actors. DeFi protocols sometimes rely on DAOs for governance decisions and on DApps for user interaction, while crypto service providers enable access and liquidity.

These interlinkages imply that a shock in one area can ripple through the entire ecosystem, highlighting the importance of comprehensive risk mitigation measures and assurances that lie on the regulated, compliant side of DeFi. Examples of these interconnectedness can be seen by the impact of the collapse of regulated and compliant Silicon Valley Bank to USDC, which led to a minor panic of MakerDAO collateral and the DeFi markets.

The power of DeFi is that, on its own, it is robust enough to be the future of digital finance, with heightened security, efficiency and access. However, policymakers should consider how to protect DeFi markets from instability that may be brought by traditional financial entities that interact with on-chain protocols.

5. Self Regulatory Proposal for the Industry

In this final section of the report, INATBA members propose a set of standards and recommendations that the DeFi industry should consider as it continues to operate and grow. The potential of the industry is incredible, and once done right, it can help create a dynamic financial ecosystem that can benefit billions of people from around the world. It is for this reason that DeFi should be done right, and there is no better place to start than to focus on the first half of the acronym - decentralization.

Decentralization in blockchain systems can occur at various levels, including the protocol layer (Layer 1) - where the underlying infrastructure operates and the core functions are defined - the application layer - where smart contracts and DApps are implemented - or on the business level - where the blockchain acts as a technology layer to provide certain services. A DeFi project issued on a decentralized blockchain does not automatically make this project 'decentralized' from a regulatory perspective.

Some indications, as to what aspects might contribute to the assessment of decentralization in the context of MiCA, have recently been summarized by the Danish Financial Supervisory Authority. They, in particular, make a classification dependent on both legal and technical elements. For a service to be considered decentralized, it must operate without the need for a legal entity or person directly controlling the system. The Danish FSA further emphasizes the need to assess both technical decentralization, such as the use of smart contracts, token ownership structures and governance mechanism, which they consider to be the ultimate signal for the assessment of who controls the protocols' decision-making.

With that in mind, and as the report has stated in the previous sections, decentralization is a gradual process. INATBA members acknowledge that currently, in our view, only very few projects can be considered truly decentralized on all of our proposed indicators. The proposed measures are thereby focused on market participants which are in the process of decentralizing, but are not yet fully there. Furthermore, INATBA members want to clearly state that many compliant projects can not be decentralized due to legal, operational or business limitations, since, at present, no guidance exists on how such compliant projects can transition to decentralized entities that operate solely on-chain.

With that consideration, the following proposed measures aim at establishing standards and best practices to allow a compliant and sustainable transition towards decentralization and to ensure transparent and risk-aware operation of DeFi projects.

5.1 Basic Administrative Measures

- 1) **Real-time Financial Reporting** - The DeFi ecosystem can and should report in near real time on their financial well being, assets, liabilities, and income sources. This will help achieve a high level of transparency and accountability. INATBA will seek to create an open-source and publicly available dashboard that can achieve this in the future. This dashboard will, at a minimum, reflect the financial stability of the operations of the protocol and include the operating income, the cash flow generation and a liquidity ratio. All this information will come from on-chain data to allow an easy build from the operating and accounting systems of the Protocol.
- 2) **Conflict of Interest Policies** - DeFi protocols, or arrangements that seek to become fully decentralized, should establish mechanisms to identify key stakeholders and their competing interests outside of the protocols, as well as address conflicts of interest when it comes to governance and resource delegations. This is a basic rule that the ecosystem is seeking to implement already. At the risk of stating the obvious, this exercise should translate into a document that is publicly available so that both users, prospective investors and policy makers are aware of the nature of the conflict of interests and their consequences.
- 3) **Segregation of Asset** - User funds should be segregated from DeFi Protocols' operating accounts, quite a basic rule, that has already been purported by existing regulations. The non-custodial nature of on-chain, smart contract based protocols allows this quite seamlessly. As it already exists, the assets of each party to the DeFi Protocols should not be mixed with the assets of other participants. For example, the assets of one participant cannot be used for the settlement of an operation of another participant, or for the operations of the protocol.
- 4) **Segregation of Duties** - In DeFi, smart contracts automate the execution of functions without human intervention. These smart contracts are self-executing code that automatically enforces predefined rules and conditions. The use of smart contracts can address the need for Segregation of Duties, as their code (when audited) ensures transparency, prevents tampering, and segregates certain duties across different parts of the process. Reporting on the efficiency of this control, especially while the protocol aims to decentralize, should be part of the governance processes of the DeFi protocol.
- 5) **Prohibition of Insider Trading** - In a decentralized and often anonymous environment, identifying individuals with insider information requires leveraging blockchain's inherent transparency while upholding the ethos of pseudonymity. Rather than identifying individuals, DeFi protocols can prioritize tracking access to sensitive information. Wallet addresses linked to governance roles, developer activities, or privileged data access can be tagged, creating an on-chain record of potential insiders. Smart contracts can log significant actions, such as proposal votes or protocol updates, alongside the involved wallet addresses. This approach enables the

community to identify patterns and flag potential misuse of information without compromising anonymity, fostering both trust and accountability.

Another recommendation involves creating a decentralized whistleblowing mechanism powered by community governance. Participants could flag suspicious activity, such as large trades occurring just before key announcements, for collective review. With programmable incentives, the system could reward individuals who identify credible insider trading cases, encouraging active participation from the broader ecosystem. Although hard to implement, ensuring strict community prohibition of insider trading within DeFi is crucial.

5.2 Business-Oriented Measures

- 6) **Financial Resilience** - Reporting on financial resilience should be made available publicly, and especially so to their governance stakeholders. Ratios like the number of months of operations covered by the level of capital, leverage levels, amount of own liquid assets held versus the capital of the protocol, evolution of the cash flow, number and amount of impairments supported by the protocol should be a few of the indicators to provide. Even if this information is principally for the “management”, when some ratios are hit, market participants should be alerted to major risk thresholds, and the protocol should allow for a predefined halt of operations, if deemed necessary by the community. Effective insurance mechanisms should be reviewed and adopted by the entity’s governance.
- 7) **Users-governance Participation** - Users should have a say in significant platform decisions, employing a decentralized governance model and basic DAO rule. The organization of the protocol should ensure that users who are part of the governance receive all relevant information eluded to here and above.

The process of accepting and evaluating new stakeholders of the governance mechanisms that have the right expertise, knowledge and understanding of the protocol should be established clearly and publicly. The governance structure should have standard procedures to allow this review. The governance structure should have rules to opine on the result of this process. Finally, members of the governance structure should review the character of the candidates and members, and their fiduciary duties.

Best practices on governance should be explored by the community. If innovations, like Quadratic Voting, perform better than traditional governance structures, then these mechanisms should be adopted as best practices to ensure effective decentralization of the protocols.

- 8) **Interoperability Standard** - Cross-platform compatibility and interoperability should be encouraged to promote a cohesive DeFi ecosystem, with cross-protocol liquidity and other characteristics that increase the overall safety and performance of the DeFi ecosystem.
- 9) **Product Description Guidelines** - DeFi protocol can be difficult to understand. Therefore, these offerings should ensure clear communication

and public educational content.

DeFi arrangement must ensure the existence of a clear set of information about the protocol's intricacies, alongside clear descriptions of the related risks. This needs to be done in simple terms to allow anyone to understand.

5.3 Technical Measures for DeFi Self-Regulation

- 10) **Decentralization of Control** - True decentralization requires protocols to transition from centralized control to community-governed systems. This involves implementing governance mechanisms where tokens are widely distributed among stakeholders, enabling transparent voting processes. To eliminate single points of failure, protocols must burn admin keys after achieving operational stability. Permissionless deployment should be prioritized, where any modifications to smart contracts or major decisions are executed through DAO-controlled multi-signature wallets or public governance processes. These measures ensure that no single entity has undue influence over the protocol.
- 11) **Emergency Protocols** - Protocols must be equipped to handle emergencies such as breaches or technical failures. One effective measure is the inclusion of “circuit breakers” that automatically halt abnormal activities, such as excessive withdrawals or price volatility. Recovery protocols should allow freezing of compromised smart contracts while preserving the functionality of unaffected areas. To further enhance resilience, decentralized backups of critical data should be maintained across multiple nodes. These fail-safe measures protect users and ensure protocol continuity during crises.
- 12) **Network Stability Measures** - As DeFi scales, ensuring network stability becomes essential. Layer-2 solutions like zk-Rollups or optimistic rollups can alleviate congestion, reduce transaction costs, and increase throughput while maintaining security. Validator diversity must also be encouraged by distributing staking operations among a wide array of participants, minimizing the risk of centralization. Transaction rate-limit protocols can prevent network congestion caused by surges in demand both legitimate and adversarial in nature, preserving operational efficiency even under heavy load.
- 13) **Identity Verification Processes** - To balance user pseudonymity with regulatory compliance, protocols should adopt advanced identity solutions. Zero-Knowledge Proofs (ZKPs) can enable users to prove attributes like age or jurisdiction without revealing sensitive personal information. Decentralized Identifiers (DIDs) offer another solution, allowing users to verify their identities optionally while remaining anonymous on-chain. However, identity verification requirements should be limited to centralized entry points such as exchanges and fiat on/off-ramps, keeping the core protocol permissionless and accessible.
- 14) **Regular Protocol Updates** - The dynamic nature of DeFi requires protocols to update regularly to address vulnerabilities and incorporate innovations.



Secure development pipelines can ensure new updates are rigorously tested before deployment. Immutable deployment records, such as publishing the hashes of deployed smart contract code to blockchain explorers, provide transparency. Major updates should require community approval via DAO votes, with a built-in delay for implementation to allow sufficient review and feedback from stakeholders.

- 15) **Smart Contract Audits** - To maintain trust and security, all smart contracts must undergo mandatory pre-deployment audits by reputable third-party firms. These audits should identify vulnerabilities, logical flaws, and potential exploits, with results made publicly available. Regular re-audits are also necessary, particularly after significant updates or changes to the protocol. Bug bounty programs incentivize developers and security researchers to proactively identify and report issues, further fortifying the protocol's defenses against exploitation.
- 16) **Transparency in Smart Contract Interactions** - Transparency in DeFi operations fosters user trust. Protocols should publish all smart contract code on open platforms like GitHub, ensuring it is accessible for review. Real-time analytics dashboards can provide users with critical metrics such as total value locked (TVL), governance votes, and transaction histories. Additionally, transaction simulation tools should be offered, allowing users to preview the outcomes of their interactions with smart contracts before committing, reducing unintended errors and risks.
- 17) **Oracle Robustness** - Reliable data feeds are essential for the accurate execution of smart contracts. Decentralized oracles, such as Chainlink, aggregate data from multiple sources to prevent manipulation and ensure accuracy. Time-Weighted Average Pricing (TWAP) mechanisms can further stabilize data inputs, reducing the impact of short-term price fluctuations or malicious attacks. Protocols must prioritize the use of these decentralized and robust oracle solutions to mitigate risks associated with external data dependencies.
- 18) **Decentralization of Control** - DeFi should aim for genuine decentralization. Through this, the level of security and robustness in an internet platform is raised above average besides minimizing chances for frauds

5.4 Additional Security Measures

- 19) **Enhanced Wallet Screening** - Protocols should integrate automated wallet screening tools to flag fraudulent activity and sanction risks in real time. Transactions must be continuously monitored to detect suspicious addresses. When flagged, access should be blocked to prevent money laundering and other illicit activities. Utilizing third-party analytics services for both on-chain and off-chain risk detection ensures that threats are identified promptly and mitigated effectively.
- 20) **Internal Blocklists** - The organization of the protocol should maintain an internal blocklist that continuously incorporates newly identified malicious



addresses and addresses associated with high-risk activities in an automatic manner. This ensures that evolving threats are proactively mitigated, strengthening the security posture of the ecosystem.

- 21) **Verification Against Public Lists** - To maintain security standards, the organization of the protocol should cross-reference known illicit addresses with public blocklists. Regular review and updating of internal blocklists should be conducted using data from publicly available sources, as well as blockchain analytics platforms. Utilizing industry-wide research and dashboards, as mentioned previously, enhances data accuracy and ensures alignment with the broader DeFi community's efforts.
- 22) **Behavioral Pattern Analysis** - Behavior-based blockchain risk monitoring should be employed, allowing screening tools to flag risk based solely on the activity of a given address. This includes integrating the tools that detect whether an account is engaging in unusual behavior or actions typical of fraudulent activities.
- 23) **Malicious Token Detection** - To counteract the proliferation of scam tokens, protocols should implement token verification measures that distinguish legitimate tokens from scams. Suspicious tokens must be flagged for user awareness automatically. Leveraging on-chain tracking, real-time threat detection, and advanced fraud mitigation algorithms will help identify and eliminate fraudulent activities before they affect users and protocols.
- 24) **Transaction Simulation and Validation** - Users should have visibility into transaction outcomes before execution. Protocols should provide transaction simulation features that illustrate expected asset transfers before finalization. This simulation should also be coupled with processes for detecting malicious transactions and warning users before execution is crucial for preventing fraudulent activities. Security tools must be implemented to alert users when interacting with suspicious dApps, ensuring their protection against deceptive platforms.

6. Conclusions

INATBA believes that the evolution of decentralized finance (DeFi) represents a pivotal shift in the financial landscape, offering unparalleled transparency, efficiency, and accessibility. However, as this report has outlined, DeFi's growth is accompanied by unique risks that require a tailored approach spearheaded by the industry. Traditional financial frameworks are inadequate for addressing the complexities of DeFi, underscoring the need for a self-regulatory model that balances innovation with investor protection and financial stability.

A well-structured self-regulatory framework, as proposed in this report, can provide the necessary safeguards without stifling technological progress - something crucial in achieving global competitiveness for any jurisdiction. By fostering transparency, accountability, and security, industry-led initiatives can mitigate risks such as governance centralization, smart contract vulnerabilities, and systemic financial threats. This win-win approach can optimize the adoption of Decentralized Financial technologies and compliance in ways that a rigid regulation never could. Additionally, implementing real-time financial reporting, decentralized governance models, and standardized risk management practices will ensure that DeFi protocols evolve responsibly.

Crucially, self-regulation can be viewed as a legitimate substitute for legislative oversight that aligns with regulatory objectives while preserving the core ethos of decentralization. Regulatory engagement should focus on clarifying legal uncertainties, defining decentralized entities, and ensuring compliance without compromising the efficiency and permissionless nature of DeFi once this self-regulatory framework produces concrete findings that call for further regulatory action. Only then will the policy steps taken ensure the goals of regulators.

As DeFi continues to mature, collaboration among industry stakeholders, policymakers, and technology providers will be essential. By embracing self-regulation, the industry can proactively shape its future, ensuring that DeFi remains a secure, transparent, and sustainable component of the global financial system - which has always been the objective of INATBA and its members. The opportunity to redefine financial systems through decentralized protocols is within reach - if such efforts are approached with diligence, innovation, and a commitment to responsible growth, something that INATBA strives to provide to the industry.

The discussion on the proper regulation and self-regulation of DeFi have just now started. If you and your company seek to participate in these discussions, consider joining INATBA. Together we can help evolve DeFi into the mainstream financial mechanisms that they deserve to be.

7. Glossary of DeFi Terms

(Self-Hosted) Wallets

A digital tool that allows users to store, send, and receive cryptocurrencies and digital assets. Wallets can be custodial (managed by a third party) or non-custodial (controlled directly by the user with private keys). Examples include MetaMask, Ledger, and Trust Wallet.

On-Chain Lending

A DeFi mechanism where users can deposit their crypto assets into lending protocols to earn interest or use them as collateral to borrow other assets. Platforms like Aave and Compound facilitate decentralized lending without intermediaries.

Stablecoins

Cryptocurrencies designed to maintain a stable value, typically pegged to a fiat currency (e.g., USD) or other assets. Stablecoins can be collateralized (USDC, USDT), algorithmic (DAI), or hybrid models.

Coin

A digital currency or asset that operates on its own blockchain, such as Bitcoin (BTC) or Ethereum (ETH). Coins differ from tokens, which are built on existing blockchains.

Key

A cryptographic element used to access and control a blockchain wallet. Private keys grant full ownership of funds, while public keys are used to receive assets. Losing a private key results in permanent loss of access.

Voting Rights

A governance feature in DeFi that allows token holders to participate in decision-making processes of decentralized protocols. Voting rights are often determined by the number of governance tokens held, influencing changes like protocol upgrades and fee structures.

Liquidity

The availability of assets in a market, allowing for efficient trading without significant price fluctuations. In DeFi, liquidity is often provided through liquidity pools, where users deposit assets in exchange for rewards or trading fees. Examples include Uniswap and Curve Finance.

8. Resources and Citation

Barbereau, Tom, et al. “Decentralised Finance’s Timocratic Governance: The Distribution and Exercise of Tokenised Voting Rights.” *Technology in Society*, vol. 73, 1 May 2023, p. 102251, www.sciencedirect.com/science/article/pii/S0160791X23000568, <https://doi.org/10.1016/j.techsoc.2023.102251>. Accessed 1 Dec. 2023.

– “DeFi, Not so Decentralized: The Measured Distribution of Voting Rights)”

Crypto, KAF. “X.com.” *X (Formerly Twitter)*, 5 July 2023, twitter.com/kafcrypto/status/1676645365032820744. Accessed 12 Feb. 2025.

Danish Financial Supervisory Authority. “Decentralised Finance and the Markets for Crypto-Assets: When Is Your Offering Exempt from Regulation?” *Dfsa.dk*, July 2024, www.dfsa.dk/news/2024/jun/crypto-assets_250624. Accessed 12 Feb. 2025.

ELS-CDN. “Economic Metrics of DAOS.” *Els-Cdn.com*, 2023, ars.els-cdn.com/content/image/1-s2.0-S0160791X23000568-gr6.jpg. Accessed 12 Feb. 2025.

Risk Analytica. “Risk Intelligence for DeFi - Block Analitica.” *Blockanalitica.com*, 2018, blockanalitica.com/. Accessed 12 Feb. 2025.

Sandor, Krisztian. “MakerDAO Paves Way for Additional \$1.28B U.S. Treasury Purchase.” *CoinDesk*, June 2023, www.coindesk.com/markets/2023/06/01/makerdao-paves-way-for-additional-128b-us-treasury-purchase/. Accessed 12 Feb. 2025.

Shollaj, Xhoni. “NVIDIA | LinkedIn.” *LinkedIn.com*, NVIDIA, 1 Feb. 2022, www.linkedin.com/pulse/how-measure-vote-decentralization-defi-projects-johnny-shollaj/?trackingId=C%2BSCuvoNQoSOq1xlwACgrg%3D%3D. Accessed 12 Feb. 2024.

Srinivasan, Balaji. “Nakamoto Coefficient: An Accurate Indicator for Blockchain Decentralization?” *Bybit Learn*, 18 July 2022, learn.bybit.com/blockchain/nakamoto-coefficient-decentralization/.



Contact details

Website inatba.org

Contact contact@inatba.org

Join INATBA membership@inatba.org