GBBC
Global Blockchain
Business Council

STANDALONE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 5.0
DECEMBER 2024

DECENTRALIZED FINANCE (DEFI): OPPORTUNITIES, RISK CONSIDERATIONS, AND KEY PRINCIPLES FOR GROWTH

GBBC GSMI 5.0

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

GSMI 5.0 IN-DEPTH REPORT

DECENTRALIZED FINANCE (DEFI): OPPORTUNITIES, RISK CONSIDERATIONS, AND KEY PRINCIPLES FOR GROWTH

INTRODUCTION

Decentralized Finance (DeFi) is a new trend in commerce that has emerged from the onset and maturation of decentralized networks and blockchain technology. At first DeFi focused on ways to leverage blockchain's programmability, autonomously functioning code to :decentralize" financial activities. This initial foray into traditional finance sought to disrupt and replace the institutions that have traditionally been integral to financial services. As the rise of tokenization expands to encompass various asset types, DeFi has travelled beyond its financial roots, paving the way for innovation across a broad range of financial and commercial markets. This shift brings exciting possibilities, such as enhanced liquidity, broader access to global markets, and entirely new forms of value exchange. However, it also introduces challenges, including regulatory uncertainties, risks of technical vulnerabilities, and the potential for market manipulation.

What exactly defines this new trend, and how might its opportunities and risks shape the future of finance and commerce?

This paper explores the meaning of DeFi, and presents a taxonomy of DeFi concepts, as well as a set of common principles and standards to address the novel issues that DeFi presents. Based on those principles, the paper then proposes a mapping of potential risks and mitigation measures for different types of participants in the DeFi space, followed by a regulatory commentary to identify gaps where there may be no principles or regulatory clarity to address issues of concern that DeFi may raise. Throughout the paper, we identify several common misconceptions about DeFi, and attempt to dispel them with simplified explanations that provide context and clarity.

This paper also seeks to identify what matters most to DeFi protocols for their activities to be legitimized and scale, while recognizing the frenetic pace of DeFi developments. It raises open questions, and provides recommendations for considering the future of DeFi, which forms an approach toward a DeFi playbook.

The reader is encouraged to keep in mind several core themes while reading this paper

First, decentralized blockchain networks arguably remove the need for intermediaries, but that does not mean that intermediaries cannot participate nor does it mean that intermediaries may not eventually become a necessary or practical part of DeFi in the future.

Second, DeFi protocols that utilize decentralized blockchains are automatically global, which means that by design anyone with an internet-connected device can participate. This global access and participation greatly expands the size of the markets but also means that local laws and regulations might be overlooked, or worse, that conflicts between different sovereign laws, standards, and expectations will likely increase.

Third, with fewer or no intermediaries, decentralized blockchains and associated protocols rely heavily and sometimes exclusively on infrastructure (software, hardware, and communication). In traditional markets, both financial services and broader commerce, such infrastructure has not typically been subject to much, if any regulation. Drives to change this paradigm just because transactions in assets happen on or through this infrastructure will often involve a fundamental rethinking of long-held legal and regulatory concepts.

Fourth, in a world built entirely on software, the code becomes of paramount importance because it functions autonomously such that it cannot be stopped or the results of its execution changed. This is not necessarily an argument to regulate the development and deployment of software, but it points to the difficulties associated with determining how to regulate DeFi and reminds us that software suffers from imperfections. Creating incentives to encourage people to code and test carefully and thoroughly, and to solve these imperfections, seem worthy goals.

DEFI OVERVIEW

The DeFi movement often points to a new paradigm for financial services, which can be automated and recorded on a decentralized blockchain. It results from the use of software and emerging technology to facilitate direct, point-to-point value exchange between counterparties, and removal of third party intermediaries. Composable financial services can be carried out through automated transactions enabled by smart contracts that use digital assets including stablecoins as the form of currency.

It is not clear that a universally adopted definition of "DEFi" exists yet. While definitions and common understanding are still evolving, the industry has made progress toward a functional meaning of DeFi.

Let's start with the foundations in the very name:

- **Decentralized:** no single point of failure, no single source of truth, no single authority capable of or responsible for making changes to data
    - This is a natural continuation of trends towards greater automation, leveraging developments in computing, the internet, and global connectivity
- **Finance:** traditional financial services activities such as trading, lending, deposit-taking, custody but with tokenized assets

DeFi does not exclusively involve financial instruments because any asset or bundle of rights can be tokenized and subjected to the functionality of a traditional financial instrument or transaction.

...which lead us to a starting DeFi-nition:

Take traditional financial services activities such as trading and lending, distill them into their component rules and processes, and convert them into self-executing code on decentralized

networks accessible to anyone with an internet-connected device such that any tokenized asset can be utilized on them.

Layering on, "DeFi commonly refers to the provision of financial products, services, activities, and arrangements that use distributed ledger technology (DLT), including self-executing code referred to as smart contracts DeFi aims to operate in a disintermediated and decentralized manner, eliminating some traditional financial intermediaries and centralized institutions, and enabling certain direct investment activities."[1] (IOSCO)

Misconception 1: "DeFi is the opposite of TradFi (Traditional Finance)"

Reality: Rather than attempting to do away with TradFi, DeFi signifies a move towards straight-through processing and universal access to markets with enhanced efficiency and inclusivity, including the ability to subject non-financial assets to those markets. While DeFi arose outside of TradFi and proposes alternative ways to solve problems, including some of the longstanding problems and risk associated with intermediaries (such as counterparty risk), its aim is to make marketplace processes as simple as possible by automating them and removing the need for intermediaries. DeFi also enables integration with TradFi using features like smart contracts, tokenization, and decentralized lending features. DeFi does not remove third parties altogether but allows them access through smart contract integrations. In many cases there can be an integration with an existing centralized TradFi player. For instance, as banks are integrated with a central stock exchange and need its approval to allow trading in traditional assets, they would need to follow a similar process to allow clients who choose to use them to access new protocols. Similarly, for DeFi protocols to integrate tokenized versions of traditional assets, there would need to be at least some integration with traditional players and central exchanges. With tokenization presenting opportunities for markets and liquidity, from event tickets and art to private credit, intellectual property and beyond, innovative business models will have to adapt to these changes.

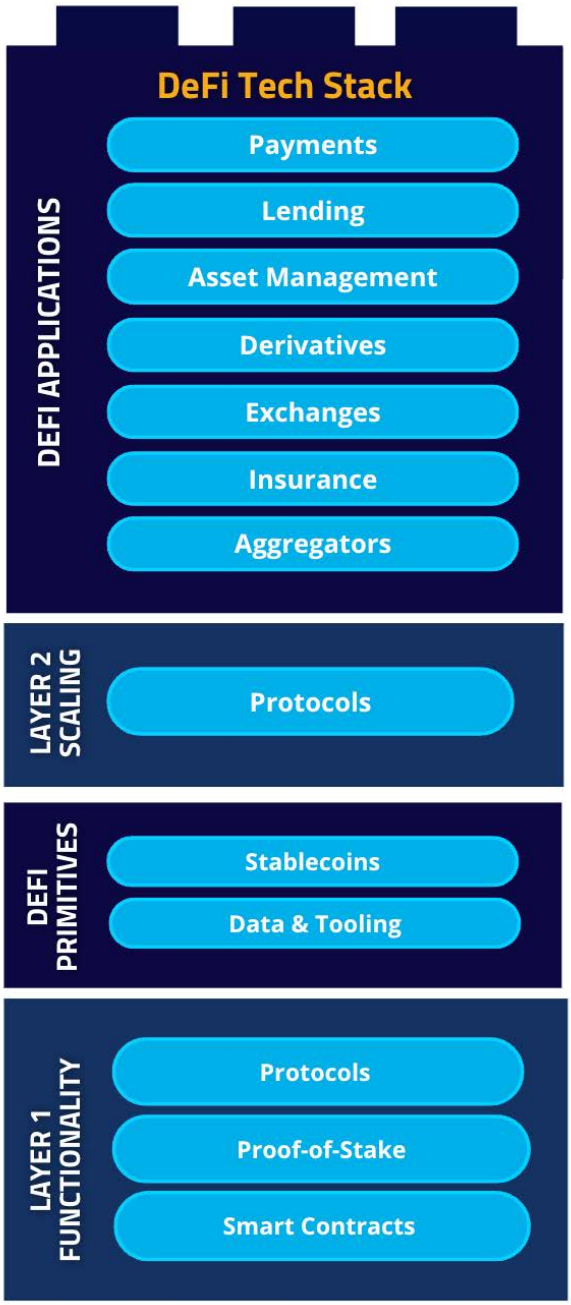
How does this work?

DeFi essentially takes the concept of a traditional financial services activity, such as exchange trading or lending, and breaks it down into basic components. It then recreates that activity in a way that shifts several core traditional functions from centralized market intermediaries to allow individual participants to conduct the activity on their own, on a peer-to-peer basis. Any individual with an Internet connection can access existing DeFi applications or build new ones using open-source code. This open structure has generated a truly global liquidity pool deposited by participants, with which an increasing amount of financial and commercial trading activities are taking place, all by means of automated systems that permit peer-to-peer interactions between counterparties.

DeFi can be envisioned as a "tech stack" that starts with a decentralized blockchain layer on which everything else is built, a Layer 1 comprising basic protocols that allow for the deployment of smart contracts, which create the rules for automating transactions and activities. Operating from the

smart contract layer, DeFi primitives include data, tooling and tokenized assets for composable functionality. With these tools, a wide range of DeFi applications can be built. The full listing of DeFi terms and definitions can be found in the taxonomy in Appendix 1.

FIGURE 1: DEFI TECH STACK



Composable financial primitives can be used to build products with a plug and play architecture. Key features include:

- Protocols define sets of common rules for each financial function
- Total Value Locked (TVL) as the total value of digital assets deposited into DeFi protocols, indicates liquidity, user engagement, and market sentiment
- Liquidity pools combine deposits of digital assets to enable trading
- Automated Market Makers (AMM) provide liquidity management and asset pricing mechanisms
- Flash loans enable borrowing and returning funds within a single automated transaction
- Proof-of-Stake is generally the consensus mechanism to process transactions effected on the protocol, in addition to other consensus mechanisms

It is important to note that DeFi has been developed without an official, or legally agreed definition, nor have the risks been clearly defined. Clarity has yet to be established with respect to ways DeFi should fit within the world of regulated activities, especially for financial services. Yet there are certain principles that its participants have established as foundational for DeFi, which can advance common understanding and also help to define and address risks.

Misconception #2: "DeFi is all about financial markets and financial instruments and is not accessible to all"

Reality: A participant can use any type of token in a DeFi protocol, so long as it is of a configuration, such as ERC20, recognized by the protocol. Layer 1 tokens, governance tokens and memecoins are some examples, as are tokenized stocks, event tickets and trading cards. All assets can be used in DeFi because the software does not differentiate based on the nature of the asset. DeFi essentially allows any activity involving the decentralized trading of assets over blockchain technology, allowing the possibility of activities that are not related to financial instruments but any asset or item tokenized using blockchain technology.

For instance, the regenerative finance (ReFi) movement, considered an offshoot of DeFi, proposes an alternative financial system centered on inclusivity, transparency, and responsibility relative to society and the environment to create net positive effects through regeneration. Another example that can morph into DeFi can be the emerging Decentralized Physical Infrastructure Network (DePIN) trend, which enables a blockchain-based network using cryptocurrency incentives to create and maintain physical infrastructure.

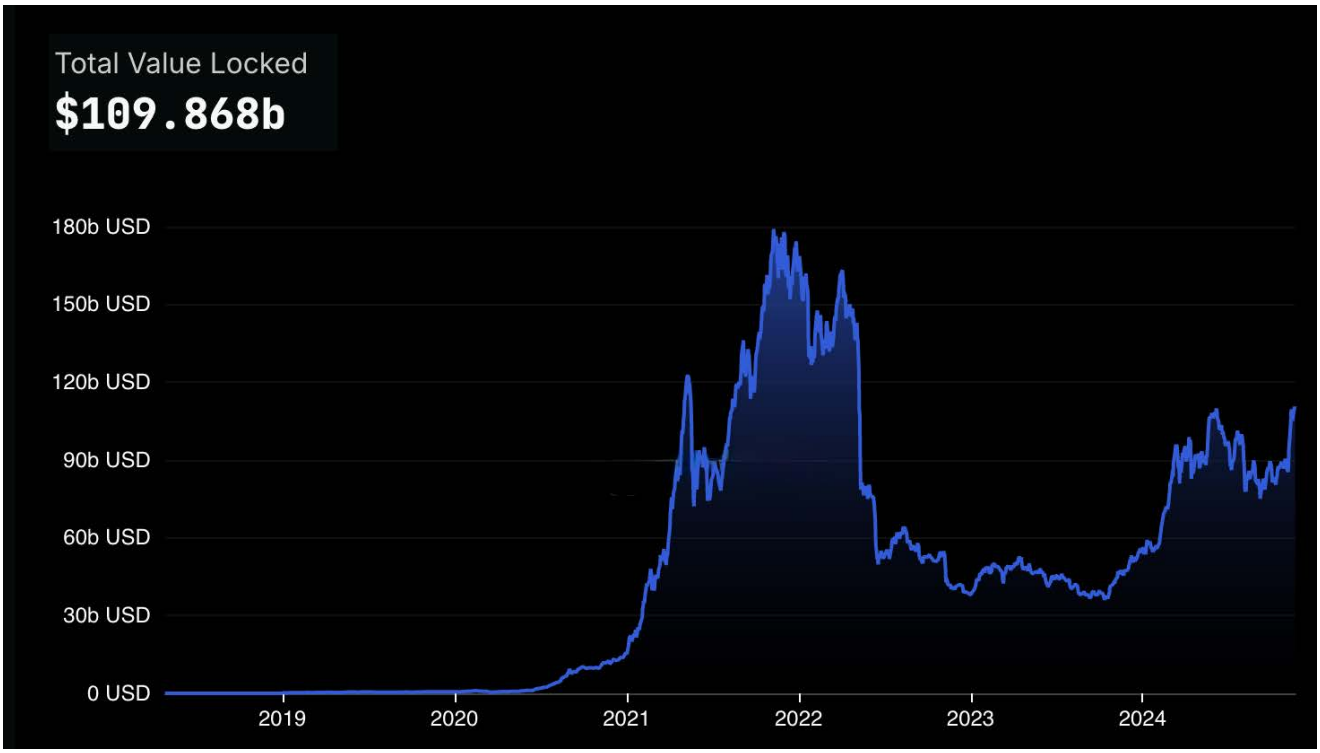
Misconception #3: "Smart contracts are real contracts and are safe because they are automated"

Reality: Smart contracts are nothing more than self-executing code. They are not inherently legally binding contracts, although they could be depending on the facts and circumstances. Moreover, they are not smart in the sense that they do not foresee variations or context apart from the conditions built into them to execute a transaction automatically. They do not account for unforeseen or unanticipated future events that could affect the technology's function or the participants' needs. Therefore, there will always be potential gaps and loopholes, scenarios that smart contracts will "miss" or not account for. It is in the time stamping element on which the safety of smart contracts can be relied.

Smart contracts also have a series of vulnerabilities, including operational risks (e.g., insufficient backup, lack of critical system safeguards, poor governance), technological risks including unintended technological (e.g., vulnerabilities in the code, human mistakes in coding, issues with oracles or sources of information they rely on), cybersecurity risks, and fraud and manipulation (e.g., nefarious code, backdoors). The code may have vulnerabilities to being controlled, and human mistakes may be difficult to reverse if funds are sent to the wrong recipient. Few people may have the technical ability to understand its function or the risks that could be fatal to its functioning.

Who uses DeFi?

FIGURE 2: TOTAL VALUE LOCKED IN DEFI PROTOCOLS



Source: DeFi Lama, Nov 20, 2024 - https://defillama.com

Total Value Locked has increased over the years and normalized following an initial hype. While most early DeFi users have been institutional and professional investors seeking excess returns , early users of DeFi in crisis situations where traditional financial systems have failed are showing real opportunities for financial inclusion. DeFi user growth has been especially significant in emerging markets, with Latin America leading, followed by Sub-Saharan Africa and Eastern Europe respectively. DeFi can reduce barriers to entry, especially for financial services like secondary trading and funding, helping to democratize alternative assets and scale innovations to make Web3 infrastructure more mainstream.

Steps to Scale

In order to achieve the opportunities that DeFi promises, so including the democratization of finance, there are a number of challenges to address and milestones to achieve in its early stages. Finding solutions to these challenges and getting closer to capitalizing on existing opportunities are represented as milestones below:

Functionality

To effectively reach these milestones, it is imperative that the technology functions effectively and securely for all stakeholders. From a technical perspective, an increasing array of tools are being developed to enable DeFi to fulfill its potential. Many of these innovations are driven by partnerships aimed at fostering coordinated progress, relying heavily on shared experiences. These efforts often integrate multiple emerging technologies and establish connectivity with traditional banking infrastructure. Incorporating human-centric design and behavioral analytics, with a focus on diverse populations, will further enhance user experience. Understanding the needs of end users is crucial, particularly as these solutions evolve to serve unbanked and underbanked populations, as well as globally distributed users.

FIGURE 3: DEFI MILESTONES

Interoperability

Interoperability is essential to performing seamless settlements, as the DeFi space often requires exchanging assets of value across chains. Otherwise, when this is not possible beyond a single DeFi protocol, there may be a need to utilize traditional methods. In the traditional approach, one can call upon the example of customers using Visa or Mastercard to settle payments across various systems globally. The DeFi space has achieved collaboration between participants with alliances, public blockchain systems, and secure mechanisms to transact across chains such as bridging technologies. While there are multiple ways to resolve this interoperability need, fragmentation stil exists and a need to ensure an entirely seamless flow of transactions. Moreover, as we move to a multipolar financial system with multiple centers of major activity, it becomes even more important for all participants globally to be in alignment for settlement. Some ways interoperability is being addressed include:

- Decentralized Compute: Blockchain technology can distribute computing power in a secure manner across multiple nodes, enabling networks to rely on multiple servers or data centers to support parallel processing and enhance scalability. This can also make use of underutilized resources at a global level.
- Artificial Intelligence: AI can automate procedures, improve security, and enhance decision making in DeFi. For instance, AI algorithms can detect patterns and predict trends using large data sets, helping investors make better informed decisions.

- API exchanges: Allowing connectivity from API to API, these tools are reducing costs while improving scalability and discoverability for direct-to-consumer applications. They also facilitate rapid deployment of digital solutions to underserved markets. They depend on harmonization around rules, with programmable rules engines that determine data sharing between APIs, and linking protocols to exchange data and facilitate execution.

Privacy and Security

Developers are exploring the use of Privacy-byDesign as a default security feature.

- Zero-knowledge proofs and other tools help manage information sharing by making only necessary information available as needed.
- Sovereign cloud solutions are being designed and launched to provide cloud computing environments that protect data and metadata in compliance with local laws within a particular jurisdiction.

Governance

From a governance standpoint, DeFi has introduced community-driven decision-making structures through the use of Decentralized Autonomous Organizations ("DAOs"). When properly deployed, and at scale, voting and polling, with the use of governance tokens, is meant to ensure stability, efficiency, and agreement on a wide range of topics. Responsible governance and environmental accountability at the Layer 1 level can trickle down throughout the DeFi ecosystem. Governance mechanisms are still not standardized across the ecosystem and there are many challenges associated with various governance models. When governance undermines decentralization, various risks arise.

IN THE ABSENCE OF REGULATION, RISK MANAGEMENT

Most major jurisdictions lack clear regulatory frameworks for DeFi. Policy makers and regulators do not have a ready toolkit for how to regulate autonomously functioning code that allows all asset types to trade together on a peer-to-peer basis (that is, without intermediaries). These three core features of DeFi stand in contrast to traditional market and regulatory paradigms in most of the world. In fact, DeFi often looks and behaves much more like general commerce (which may offer a more appropriate lens for analysis), than financial regulation.

Nor does the laissez-faire approach to software, hardware and communications technologies provide an easy paradigm for activities involving trading, lending, creation of commodity and other derivatives in a mixed asset, automatic and unintermediated commercial environment. As a result, legislators and regulators are still grappling with how to regulate and where regulation is needed.

Without regulatory clarity or a useful toolbox, how should participants act? We propose active, informed risk management. The following sections lay out the different participants and activities core to various types of DeFi protocols and seeks to identify the associated risks. There is a lot of ground to cover and different participants will make their own judgments about what is important to them. Undoubtedly, some will glide along in blithe ignorance, simply happy to ride the waves of the markets and bear all the attendant risks of markets that hopefully function in accordance with their

mandates. Others will want a walled garden so they can ensure that they are doing business only with appropriately checked counterparties on software that has been subject to extensive testing (which might not even be DeFi) and regulatory compliance.

Participants will fall across the spectrum. This paper does not seek to mandate answers or provide guidance on where liability and responsibility should lie. Rather, it lays the foundation for thinking about risk and therefore perhaps about regulation.

As a result, popular considerations and obligations that are broadly recognized at law for intermediaries may not clearly apply for software developers and infrastructure providers, These considerations and obligations point to certain common principles:

- Consumer protection
- Market integrity, addressing market manipulation and fraud
- AML/CFT measures
- KYC best practices
- Security and privacy
- Compliance

What follows are the breakdown of activities and risks.

DEFI ACTIVITIES AND RISK ASSESSMENT APPROACH

There are different categories of participants in the DeFi universe. Some are already regulated, either under traditional regulatory regimes or newer, cryptoasset-specific regulatory approach like Europe's Markets in Crypto-Assets Regulation. Others are not subject to direct regulation. In order to better identify DeFi risks, it is important to begin with identifying what constitutes a DeFi activity, for which we propose a categorization of DeFi activities that have arisen across traditional and non-traditional spheres of financial services. The aim is to identify activities that can be considered true "DeFi" services, to address the question of what makes something "DeFi" in nature. Each category below specifies examples of platforms offering a range of DeFi services, or allowing their customers to access DeFi services.

Note that the actual peer-to-peer individual users are not included as a category or within any category, but they can have significant impact on DeFi in a variety of ways, not least because they provide liquidity and trading interest. They can also be responsible for manipulations and gaming, as well as hacks and other exploits. Because there are multiple laws about these kinds of bad actions, we do not cover them separately in the risk assessment.

One unique aspect about DeFi is the market forces and economic realities that drive demand for, and creation of, solutions to perceived problems. Because the code is usually open source and anyone can launch a protocol that fixes issues, market participants can react almost in real-time to create more fairness, predictability and efficiency when something is identified.

This analysis proposes a high-level approach toward identifying and mitigating risks for DeFi activities across different categories. These risks may range from financial, operational, consumer protection, and regulatory risks. The examples below identify risks, obligations, and issues specific to these categories of services involved in the DeFi ecosystem, as well as mitigation measures.

Category 1: Traditional Regulated Entities

As Centralized Finance (CeFi) dips its toes into DeFi, traditional regulated entities have already begun using DeFi on behalf of clients or providing clients with access to DeFi protocols. For those already regulated entities, an approach toward risk assessments for DeFi services can start with referring to existing standards and how they apply to traditionally regulated entities. The entities listed below have clearly defined responsibilities mandated by regulation or industry standards. If they are to successfully adopt or use DeFi, they need to figure out how those responsibilities apply in the DeFi context of autonomously functioning code. For instance, major global banks assisting clients to access DeFi protocols are expected to assume responsibility for some aspect of connecting them, especially when it involves retail clients. When it comes to risk, it is important to consider that there is a difference between centralized and decentralized technologies, and a difference between tokenized financial instruments and other asset types.

TABLE 1: RISK MANAGEMENT APPROACH FOR TRADITIONAL REGULATED ENTITIES

Type of Entity	DeFi Functionality Offered/Considered	Considerations/obligations for Customers	Risks	Mitigation Measures
Fund Managers & Asset Managers	• Trading tokens and investing as part of money management • Improving the flexibility of accessing decentralized asset investments and sophisticated financial solutions • DeFi ledgering that provides greater transparency into assets' performance	• Regulatory compliance, where there may be regulatory restrictions for fund managers. Rules on custody requirements may also make it difficult to participate in DeFi. • Standards, as defined by jurisdiction	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Insurance policies • Data insurance capabilities to safeguard data • Recovery mechanisms • Centralize KYC • Participation in, or use of, counterparty risk mitigation tools
Brokerage Firms	• Trading and other DeFi activities that can improve liquidity • Considering becoming swap dealers	• Regulatory compliance with functional regulators • Duty of care, acting in the best interest of clients • Separation of customer assets and other requirements may make it difficult for brokerage firms to offer DeFi swap services • Sanctions and AML compliance	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Insurance policies • Data insurance • Recovery mechanisms
Market makers and liquidity providers	• Liquidity provision	• Though acting as a market counterparty, they should maintain market integrity standards • Registration in certain jurisdictions	• predatory trading • Sanctions Violations • AML and Fraud	• strong internal policies and procedures
Central Banks	• Research and pilots on DeFi implications for enabling transactions in the traditional financial system	• Research and pilots on DeFi implications for enabling transactions in the traditional financial system • Adhering to central bank mandates • Preparation measures for crisis management	• Technical risks • Monetary losses • Data breaches	• Extensive research, piloting, and testing of blockchain-based financial infrastructure

Category 2: Registered Legal Entities Offering Digital Asset Services

Legal entities offering digital asset products and services are subject to obligations specified by the jurisdictions in which they are registered to operate. These entities include businesses considered to be crypto-native, offering products and services tailored for the digital asset industry, without directly operating a DeFi protocol. For instance, centralized digital asset exchanges, trading utilities and custodians (including custodial wallet providers) may provide their clients access to DeFi protocols, by trading the assets of, or on behalf of clients in DeFi protocols or providing gateways to such trading. Other entities may provide the basic tooling utilized by DeFi protocols, such as stablecoins.

While these businesses may already provide customers with digital asset opportunities, such as efficiencies for trading alternatives in private markets, DeFi provides opportunities for these customers, adding value to their existing offerings. As these entities increase their engagement in DeFi activities, they should have responsibilities with respect to their customers just as for their other client offerings.

The jurisdictions where the entities are registered and/or licensed may provide stringent or lax requirements for their operations, which can have implications on their overall reliability and risks. On the other hand, these businesses may also be operating without formal licenses, and as such be outside the purview of any regulation. In many cases, it will be important to better define what these services mean in the DeFi ecosystem, and how these entities should envision their obligations to their clients.

Table 2: Risk Management Approach for Registered Legal Entities Offering Digital Asset Services

Type of Entity	DeFi Functionality Offered/ Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Crypto exchanges	• Trading • Staking Services • Self Custody Wallets	• Best practices around product offerings • Risk mitigation programs • Liquidity and market integrity best practices	• Counterparty risk is introduced upon leaving a DeFi platform • Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Transaction monitoring and sanctions screening
Brokers and trading platforms	• Trading	• Best practices around product offerings • Risk mitigation programs • Secure and adequate functioning backend, especially with respect to data management • Liquidity and market integrity best practices	• Counterparty risk is introduced upon leaving a DeFi platform • Monetary losses • Data breaches • Scaling concerns for smaller platforms (e.g., queries, volume, and throughput)	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Transaction monitoring and sanctions screening

Custodians and Wallets	• Custody of tokens • Wallets may allow access to other DeFi services	• Safeguarding funds	• Monetary losses, especially stolen customer funds • Data breaches • Sanctions Violations • AML and Fraud	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Best practices for safeguarding funds (e.g., segregation of funds) • Insurance and recovery mechanisms • Transaction monitoring, sanctions screening, counterparty analysis, and enhanced KYC processes
Market makers and liquidity providers	• See above	• See above	• See above	• See above
Tokenization Platforms	• Tokenization of assets • Trading • DeFi reduces barriers to entry for adoption of tokenized assets	• Compliant infrastructure • Access controls and permissions	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Sanctions screening
Stablecoin and other Token Issuers	• Providing currency used as a key DeFi asset, allowing users to engage in DeFi activities such as lending, borrowing, and yield farming	• Providing currency used as a key DeFi asset, allowing users to engage in DeFi activities such as lending, borrowing, and yield farming - Adequate reserves and transparency • Integration with DeFi platforms using tokens as currency	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud • Collateralization or reserves risks	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Transaction monitoring and sanctions screening • Processes to assure satisfactory reserves

Category 3: DeFi Protocols (truly decentralized per the definition above)

DeFi protocols operate as decentralized platforms, providing applications and services that have arisen and operates outside the purview of traditional regulation or agreed upon obligations. These are interfaces and pure technology providers, in a decentralized context where no single entity or authority is responsible for events taking place, in keeping with the definition presented at the beginning of this paper.

By removing intermediaries, DeFi protocols shift trust from third parties to the protocol itself. A new layer of smart contract risk, which is essentially programming risk plus the risk of "gaming" the system, arises when relying on purely automated functionality. Access also depends on how protocols are set up, which can have implications on risk. The nature of digital assets being exchanged over DeFi platforms also has implications on risk, as do common utilities utilized, such as the availability of data or interoperability mechanisms, including bridge technologies.

Defi protocols raise the question of whether there is there anyone "running the shop" who should have clear obligations to users and/or who should be regulated. While the applications themselves and the software developers behind them may not be regulated, there still need to be risk assessment considerations for these purely technology-enabled DeFi activities as suggested below. In this context, risk will depend on the activity in question. For instance, smart contracts have programming risks and other vulnerabilities. Websites may have flaws that allow bad actors to steal private keys to take control of funds. Moreover, for smaller businesses developing digital solutions, up-front costs and necessary integrations can present risks when there is uncertainty in the market, such as attempting to bank the unbanked.

An important subcategory of this section comprises DAOs, which play a critical role in the DeFi space when introduced for governance. DAOs may not be legal entities in the traditional sense and yet can have a certain level of responsibility associated with a DeFi protocol. Even while operating outside of clear regulatory obligations, the creation of clear roles and responsibilities that should be considered. While most jurisdictions have not yet devised ways of categorizing DAOs, the US State of Wyoming has developed in its laws two different versions of DAO structures. One is similar to a traditional limited liability company ("LLC"), and the other resembles an unincorporated association. The contours of each type are yet to be fully explored. Certain proposed legislation in the U.S. Congress also has sought to address certain requirements for DAOs (e.g., taxation). And, at least U.S. courts are beginning to recognize DAOs as "general partnerships," which (unfortunately for DAO participants) imposes joint and several liability for the acts of the DAO upon each and every DAO participant equally. This "general partner liability" could create significant challenges for the future adoption of DAO approaches to activities that carry significant risk exposure.

Table 3: Risk Management Approach for DeFi Protocols

Type of Entity	DeFi Functionality Offered/Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Layer 1 Protocols	• Smart contract layer on which to build DeFi applications • Sets of common rules enabling composable financial services and governance • Essential functions like security and settlement	• Technical functionality • Security and privacy • True Decentralization	• Technical failures • Monetary losses • Data breaches • Consolidated control that is not fully and practically decentralized	• Code and security audits • Best practices for programming • Full divestment of protocol control by founders and creators
DeFi Applications in general	• Wide range of alternative financial services	• Technical functionality • Security and privacy	• Technical failures • Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Code and security audits • Best practices for programming • Implement next generation RegTech solutions to assure mitigation of Sanctions, AML, and Fraud risks

Decen-tralized Exchanges (DEXes)	• Exchange services	• Liquidity	• Technical failures • Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Code and security audits • Best practices for exchange services • Implement next generation RegTech solutions to assure mitigation of Sanctions, AML, and Fraud risks
Lending Services	• Alternative lending mechanisms	• Responsible and fair lending	• Technical failures • Monetary losses • Data breaches • AML/Fraud • Sanctions Violations	• Code and security audits • Best practices for lending services • Implement next generation RegTech solutions to assure mitigation of Sanctions, AML, and Fraud risks
Bridges	• Interoperability solutions	• Effective transaction recording and verification	• Data breaches • Cross-chain jurisdictional compliance violations between Layer 1s • AML and Fraud • Sanctions Violations	• Code and security audits • Insurance • Recovery mechanisms • Best practices for privacy & security
Layer 2	• Scaling solutions, freeing up space at the L1 level for essential functions	• Offloading transaction execution	• Technical failures • Monetary losses • Data breaches	• Depend on the solutions provided
DAOs	• - Decentralized governance and decision making	• Ensure truly decentralized decision-making power • Mechanisms to overrule single voters	• Technical failures • Monetary losses • Data breaches • Unequal representation of individual participants, leading to information asymmetries and abuses • Concentrations of power in voting and other decision making structures • General Partnership Liability for violations of law	• Enable mechanisms similar to traditional corporate accountability structures • Warn participants of general partnership liability exposure

Misconception #4: The risk of criminal activity is higher in DeFi because there is no AML/KYC

Reality: Theft and fraud, with bad actors engaging in illicit and criminal activities, occur in both DeFi and TradFi. In DeFi, security protocols can be put in place, including AML/KYC and other compliance measures, to provide safe ways of exchanging funds. These measures are particularly important when removing intermediaries, and when integrating tokenized traditional assets with DeFi protocols. In some cases, data may be collected and made accessible only to regulators upon request. That said, this area remains subject to development and discussion. We expect developments here in the coming years. Insights drawn from tracking and tracing technologies have shown a relatively low (or at least comparable) incidence of money laundering in the space. While the data reveals growth in illicit funds sent into DeFi protocols, alongside a reduction in illicit services, this is in the context of DeFi's overall growth in market size. On the other hand, the transparency of fund flows in DeFi makes it harder to obscure fund movements.[4]

Category 4: Sandboxes, Free Zones, and Other Government-Sponsored Innovation Centers

Several governments are taking part in the DeFi space by providing sandbox environments for testing. Many innovations need to go through a sandbox for testing, as registration and licensing services, laws, regulatory frameworks continue to evolve for the DeFi space. These testing environments may also become an informal path for regulators to familiarize themselves with DeFi innovations. The aim is to ensure compliance in the use of smart contracts, algorithms, and processes at the settlement layer, transaction layer, and value/messaging layer while adopting new software.

Table 4: Risk Management Approach for Sandboxes, Free Zones, and Government-Sponsored Innovation Centers

Type of Entity	DeFi Functionality Offered/ Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Sandboxes	• Testing environment and pre go live safety checks • Workshops and Incubation programs with security reviews	• Alignment with laws and regulations • SDKs to support safe testing and innovation • Ensuring balance of speed, security, and ease of use • Reviewing open-source environments and projects • Ensuring audited code	• Providing undue regulatory advantages to participants at the expense of the broader market	• These entities themselves are intended as mitigants for risks
Participating Entities	• Testing a wide range of DeFi functionalities	• Passing regulatory reviews as precursor for acceptance • Maintaining regulatory compliant operations	• Likelihood of operating in breach of rules within testing environment	• Seeking registration and licensing • Participation in sandboxes • Key partnerships

Category 5: DeFi Supporting Services

As a creature of the decentralized internet and blockchains, a range of supporting services have emerged to ensure smooth functionality, though not always accountability or responsibility. Attempts to regulate these support service providers would generally contradict the traditional "hands-off" approach to them by policy makers.

Table 5: Risk Management Approach for DeFi Supporting Services

Type of Entity	DeFi Functionality Offered/ Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Certifiers & Assurance Providers	• Supporting services to ensure practices follow relevant compliance checks	• Certifications that DeFi activities are following compliance checks • Reviews of safety measures including analytics, insights, tracing, and due diligence practices • Transparency on nature of endorsements • Disclosures of 3rd party reviews	• False assurance, inaccurately miscalculating or failing to consider risks	• These activities themselves are intended as mitigants for risks
Decentralized file storage	• Supporting services	• Technical functioning • Security and privacy • Disclosures of 3rd party hosting data	• Technical failures • Data breaches	• Code audits • Best practices for data security, data hosting, backup mechanisms, and recovery mechanisms • Insurance
Layer 1 validators	- Ensure correct functioning of the underlying blockchain	• Under current legal and regulatory regimes, validators conduct this activity in accordance with the built-in consensus mechanism, which should be designed to ensure fidelity through Byzantine Fault Tolerance	• Technical failures • Failures of the consensus mechanism to be truly Byzantine Fault Tolerant	• Code, security and other audits
Internet infrastructure providers	- Providers and developers of software, hardware and cloud services, communications protocols, ISPs, market data providers, oracles	• Under current legal and regulatory regimes, infrastructure providers have few requirements and often are able to escape liability entirely, except when their actions amount to fraud or other types of willful misconduct such as theft	• Technical failures	• Security and other audits • System redundancies and back-ups

REGULATORY CONSIDERATIONS

With respect to regulatory risks and expected regulatory requirements, many open questions remain stemming from DeFi's core of automonous functioning, multi-asset, peer-to-peer nature and how associated activities would properly fit into existing regulatory regimes and expectations. Given that that DeFi protocols and platforms are regulated more by the market than by supervisors and have arisen outside the purview of regulatory supervision, a proper risk assessment seems foundational to any eventual requirements policy makers might seek to impose.

For centuries, the government has regulated intermediaries, not the individuals that design them, or the direct counterparties in peer-to-peer interactions. The implicit assumption is that individuals and counterparties would be in danger of third parties doing them wrong. Regulated activity, therefore, is designed to include the intermediaries all along the chain of custody based on traditional models. Yet DeFi presents a new model that essentially eliminates the traditional players that governments would regulate. Annex 3 below lists regulatory developments globally for DeFi thus far.

As an alternative, the space can start with a self-governance perspective, with structured standards and rubrics for adequate risk assessment and mitigation measures. These standards have made progress identifying best practices that, in the context of several enforcement actions against DeFi protocols in the last few years, could make many DeFi protocols more acceptable to regulators.

Misconception #5: All DAOs are fully decentralized and autonomous

Reality: DAOs come in all shapes and sizes, with their founders making decisions about how they function that may result in an organization that is not truly decentralized or autonomous, or indeed is (as a functional matter) fully centralized. It depends on the architecture and how tokens are distributed, as well as the voting process and other elements of governance. Moreover, few people may in fact read the smart contract behind a DAO, which can become a seemingly black box. Similarly, they may not fully understand their potential exposure to the "general partnership" liability described above. Reread the definition of decentralized at the start of this paper for a framework to think about whether a DAO is decentralized.

DAOs may have a treasury of funds separate from the voting group, which votes on different issues with tokens. If a single entity or a few entities hold a majority of tokens or control decisions in any other form, they essentially have decision making power regardless of how other token holders may vote or what they want. If there are no rules for minimum voting periods, or minimum timeframes from when a vote passes to when a decision is executed over a smart contract, decisions may be determined easily by a few or a single player when not everyone has had the time to vote. If the mechanisms to overrule a single entity casting a majority vote, decentralization may be a mirage.

In fact, litigators have in some rare cases recovered funds from unwilling DAOs. In these cases, these DAOs were not fully autonomous. When one person is the majority token holder, litigation can force them to pay for injustices using traditional measures and standard legal principles.

CONCLUSION

DeFi does not fit comfortably within existing frameworks because it involves autonomously functioning code with transaction finality, multiple asset classes and no central authority or gatekeeper. Peer-to-peer activity is paramount. It also currently suffers from a lack of clear definitions, categorization of actors and activities, and standardization. One might argue that all these features are actually good. They show creative disruption and experimentation on an unprecedented scale, which will drive markets and commerce to better, more global solutions.

On the other hand, just like blockchains provide certainty and predictability, it might be important for DeFi to accomplish those goals. To that end, below is a repository of open questions that the space is addressing, followed by a set of recommendations and considerations for DeFi developments moving forward. The goal at this point is not to specify regulation, which would lead to a jurisdiction specific analysis at too preliminary of a stage, but instead to point to areas that standards might cover. The implications of these questions, considerations and recommendations can then point to specific needs such as new legislation or regulatory developments, new interpretations of such, or necessary exemptions, new sets of expectations, or new technologies (e.g., decision makers investing in analytics solutions tailored for the space).

Open Regulatory Questions for DeFi

1. What constitutes a true DeFi activity?
2. How do DeFi activities fit into existing regulated activities, if at all?
3. For those DeFi activities that may not fit into existing regulations, what are the regulatory expectations for them, and can DeFi protocols satisfy them?
4. What is the appropriate role of government and regulation in a context where there are no intermediaries? Does current law address this effectively in any way?
5. Is having an intermediary sufficient to require regulation? To whom should this point, and what does it mean to remove intermediaries?
6. Should any DeFi protocols, or any elements of protocols (e.g., Dexes) be treated as intermediaries?
7. What makes a financial intermediary, especially for the purposes of being held liable as such?
8. How should regulation address data subjects and counterparties when there are no intermediaries?
9. Who should be held responsible when something goes wrong in the context of no intermediaries?
10. What functionalities should DeFi participants ensure in order to be considered acceptable by regulators and prevent enforcement actions?
11. Should the same principles apply for all DeFi participants, or should there be different rules for different participants?
12. How should regulation address DAOs? Should they be considered legal entities in relation to the law?
13. How to deal with potential “general partnership liability” for DAO actions and activities?
14. What should risk assessments for DeFi entail?
15. What considerations and obligations to customers should DeFi participants be required to have?
16. Should regulators stay out of or lean into regulating the industry?
17. What are the implications of imposing penalties on direct participants (individuals and counterparties), as opposed to exchanges, mixers, and other services?

18. Should an interface providing access to regulated activities (e.g., wallet to access DeFi protocols and make trades) be considered an intermediary and be regulated? Should protocols that provide access to those interfaces be regulated for doing so (e.g., wallet providers)? Where will that end up, if we regulate all layers of access?
19. Should contract participants follow rules to be considered eligible to carry out a transaction? Should a transaction involving an ineligible contract participant be allowed in any circumstance?
20. Should smart contracts be regulated as brokers for carrying out order routing activities, etc.?
21. What new changes does DeFi bring, how do they affect markets, and what would be the implications if DeFi were to scale?
22. Does fully a permissionless and trustless system truly exist, and should it?

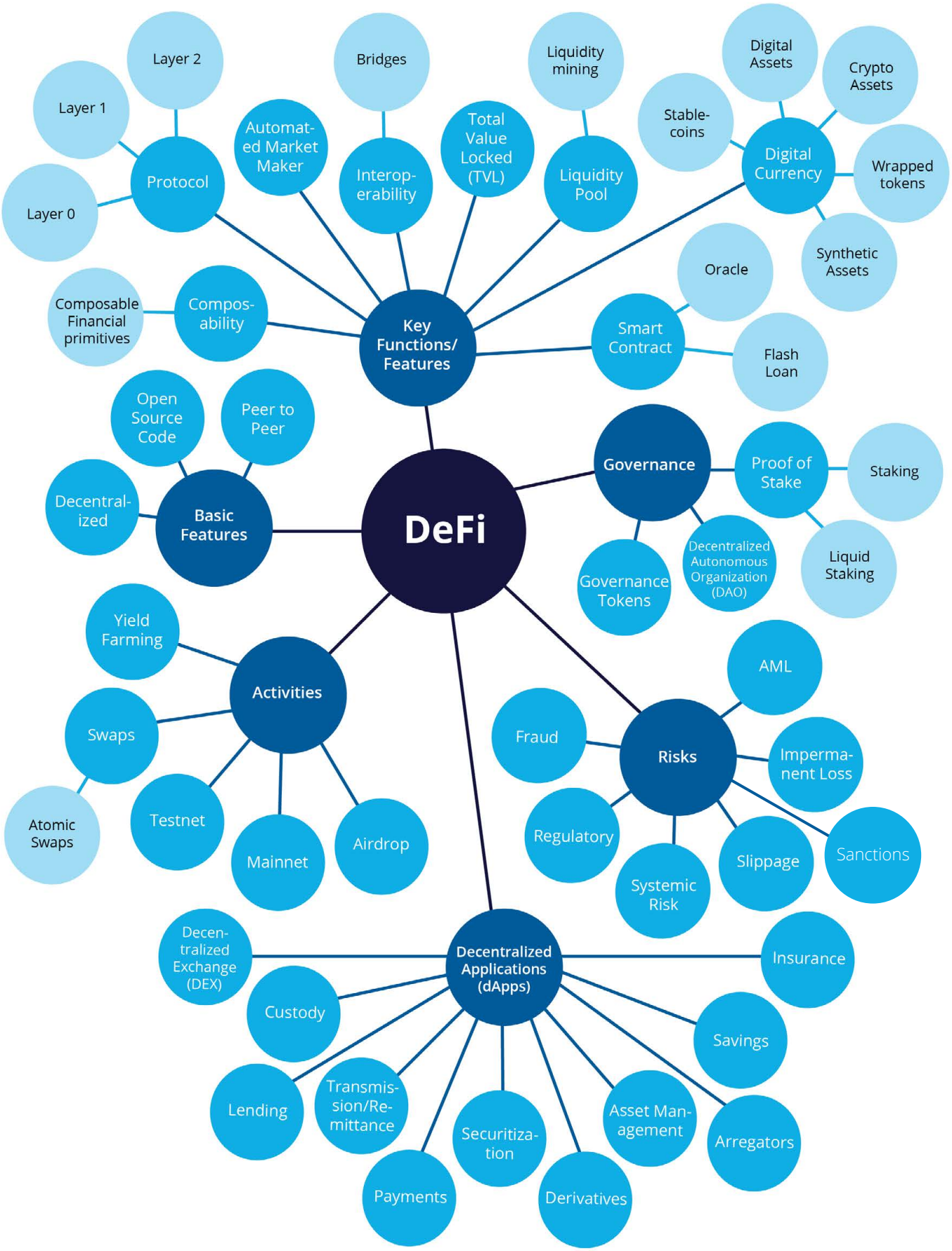
Recommendations and a Skeletal Playbook for DeFi

1. Providing clear definitions in this ecosystem is imperative as a first step to define roles and responsibilities for DeFi players.
   a. There may be a need to define the necessary elements of a DAO in order to merit that name.
   b. A definitional exercise will help the space to identify and approach entities, or subcategories of such, that should or should not be covered by rules
2. Define what standards should be in place for DeFi, and what categories of activity they should apply to, as a precursor for regulation
   a. Define what categories of DeFi activities should be subject to specific standards and best practices, in the absence of regulation at this point
3. Consider that DeFi players, including DAOs, may have a certain level of responsibility will require a certain amount of regulation and what determines when that level is met. a. To determine DeFi players' considerations and obligations to customers, understand what part of the protocol is in question (e.g., smart contract executing transactions, website customers use to access smart contract).
   b. For specific issues (e.g., IP, tax schemes, etc.), consider the actual allocator in a project.
   c. Consider the scope of traditional players and legal entities participating in DeFi, and their regulatory requirements.
   d. Assess the relevance of existing regulations (e.g., regulations for issuance of assets, residence/jurisdiction of defi users, KYC requirements to trade in tokenized assets, etc.)
4. Acknowledge that the activity makes the cases, considering the particular facts and circumstances rather than making sweeping claims. Tokens are separate from the entities and activities using them.
5. If DeFi services replace traditional financial services and processes, they must also be effective at protecting the markets they serve. Define measures for effective AML, protections against fraud, sanctions compliance, and other existing safeguards
6. Implement risk assessments for all types of DeFi activities, identifying the topics they would address and the expectations they give rise to.
7. Consider measures for governance and dispute resolution across categories of DeFi activities
8. Consider services for AML/KYC, verifications, and consumer protection measures.
   a. For instance, protocols may require participants to use secondary digital identity solutions to prove they are not bankrupt, not in a sanctioned country, and have not been convicted of a crime.
   b. Zero knowledge proofs can ensure privacy, and the data can be validated by a legitimate external entity (e.g., US Customs), providing a credentialing solution that any DeFi protocol could accept.

c. This can be operationalized as a layer on which DeFi protocols can function, as an example of harmonizing regulatory technology on top of DeFi solutions. Consider finding ways to obtain legal immunity for using these methods and tools in a DeFi environment.

9. When DAOs are not in reality as decentralized or autonomous as intended, consider a need for broader agreement on DAOs' responsibilities and proper functioning.
   a. Voting and decision making power should not be concentrated in the hands of a few players or a single player.
   b. Assess if a DAO is fully decentralized and autonomous, or partially so, and define an approach accordingly
10. Define the entities that should be held responsible when things go wrong, and solve the "general partnership liability" problem.
11. Define the regulatory risks and consider an iterative process toward legislative and regulatory developments.

Appendix 1: DeFi Taxonomy



Annex 2: Standards and Principles for DeFi and Tokenization

When it comes to basic functionality:

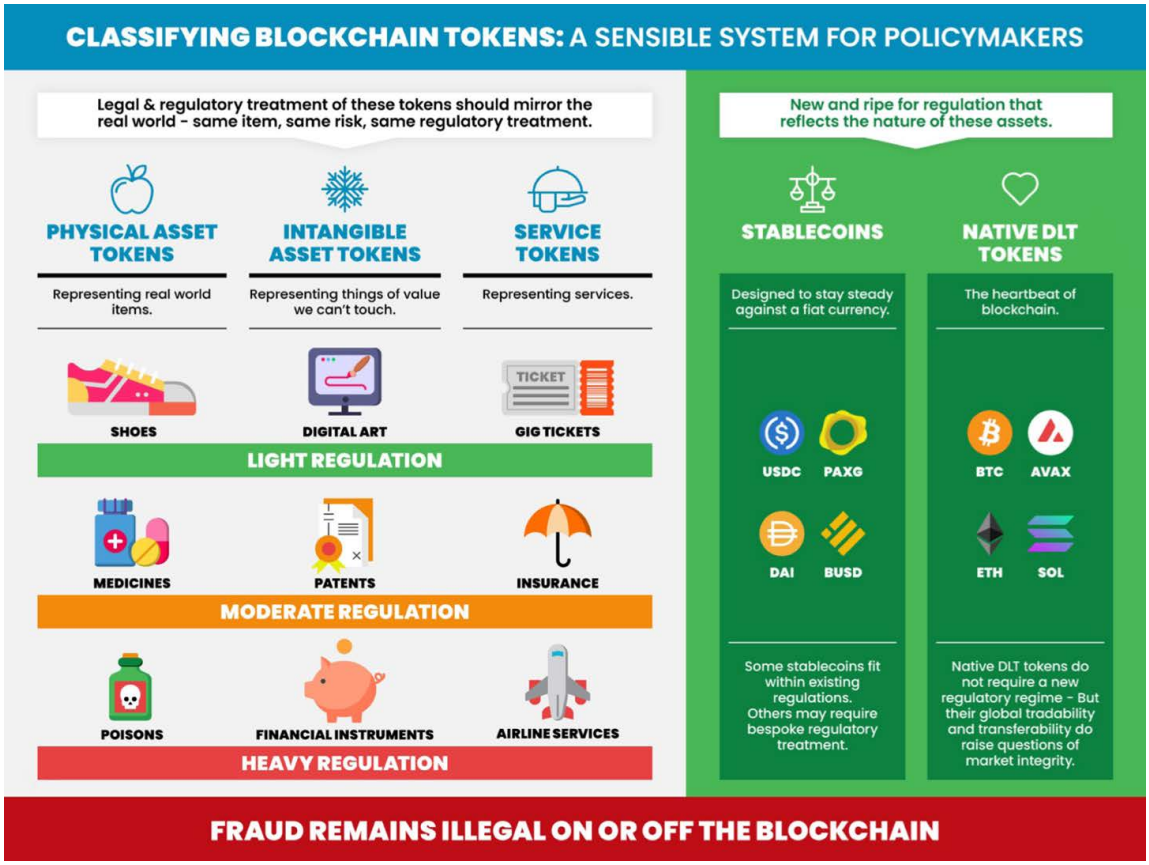
- Quality Management: ISO 9000 is a family of standards for quality management systems. They provide guidance and tools to ensure protocols and services meet external requirements for quality improvement consistently.

There have also been initiatives to develop principles addressing issues presented by the broader blockchain and digital asset space, which are relevant to DeFi, and also principles specific to the DeFi ecosystem.

The recommendations to the US Commodity Futures Trading Commission (CFTC) Global Markets Advisory Committee (GMAC) by the Digital Asset Markets Subcommittee (DAMS) in March of 2024 proposed a Digital Assets Classification Approach and Taxonomy[5] acknowledging that ***"The features of a Digital Asset include, but are not limited to, how the asset: (1) is issued; (2) holds value, (3) confers rights, (4) has fungibility, (5) can be redeemed, and (6) is recorded in books and records. The Subcommittee has endeavoured to define these features below. Digital Assets in this classification have at least one or more of the features captured in the categories, but it should be noted that there may be features developed in the future that have not yet been contemplated at this time. Similarly, not all Digital Assets classified here, have all these features. This is therefore intended as a starting point designed to support regulators and policymakers to take a use case driven approach to evaluate which types of regulations should apply to which type of assets. As these assets evolve and new ones are created, this classification will need to be evolved."*** Digital assets and their various forms are defined and categorized as follows:

Digital Asset Type	Instrument Type	Instrument
Money & Money-Like Digital Assets	Central Bank Digital Currency	General Purpose of Retail CBDC
	Central Bank Digital Currency	Wholesale CBDC
	Bank Deposits	Tokenized Deposits
	Bank Deposits	Deposit Tokens
	Reserve Backed Digital Currencies	Reserve Backed Digital Currencies
	Stablecoins	Stablecoins
Financial Digital Assets	Tokenized Security	Digital Twin
	Security Token	Digital Native
	Tokenized Derivative	Digital Twin
	Derivative Token	Digital Native
Alternative Digital Assets	Tokenized Alternative Asset	Digital Twin
Cryptoassets (e. g. cryptocurrucies)	Platform Cryptoassets (e.g. Bitcoin Ether)	Non-redeemable digital native token with no rights conferred by the issuer (if any)
	Other Cryptoassets (e.g. meme coins)	Non-redeemable digital native token with no rights conferred by the issuer (if any)
Functional Digital Assets	Functional Digital Assets	Cannot be exchanged for value, provides owner with a specific utility
Settlement Controllable Electronic Record	Settlement Token	Solely to transfer or record ownership or perform other middle/back-office financial functions

Another approach to classification of tokens proposed by Owl Explains[6] and published in the International Journal of Blockchain Law[7] is as follows:



"Core Principles for the purpose of setting minimum standards and best practices for the conduct of centralized digital assets businesses that handle customer (or user) digital assets and funds"[8] include:

- Strong Governance and System of Checks and Balances
- Protection of Customer Assets
- Enterprise Risk Management and Stress Testing
- Liquidity Reserves
- Proper Books and Records
- Annual Independent Audit

The "Proposed Information Guidelines for Certain Tokens Made Available in the United States"[9] include proposed guidelines for:

- Token offering and sale information
- Material participants
- Governance
- DLT Technology
- Token information
- Financial information
- Risk factors
- Exhibits

Gibraltar has also released 10 principles for DLT:[10]

1. Honesty and Integrity
2. Customer Care
3. Resources
4. Risk Management
5. Protection of Client Assets
6. Corporate Governance
7. Cybersecurity
8. Financial Crime
9. Resilience
10. "A DLT Provider must conduct itself in a manner which maintains or enhances the integrity of any markets in which it participates."

Guidance for smart contracts

- Smart Contracts: OpenZeppelin has ample guidance for smart contracts on GitHub, as a library for secure smart contract development[11]
- The Smart Contract Primer co-authored by several law firms and TradFi industry groups provides a comprehensive look at the technology of smart contracts and some of their use cases[12]

IOSCO: Final Report with Policy Recommendations for Decentralized Finance (DeFi)[13]

- Recommendation 1 - Analyze DeFi Products, Services, Activities, and Arrangements to Assess Regulatory Responses.
- Recommendation 2 - Identify Responsible Persons.
- Recommendation 3 - Achieve Common Standards of Regulatory Outcomes.
- Recommendation 4 - Require Identification and Addressing of Conflicts of Interest
- Recommendation 5 - Require Identification and Addressing of Material Risks, Including Operational and Technology Risks.
- Recommendation 6 - Require Clear, Accurate, and Comprehensive Disclosures.
- Recommendation 7 - Enforce Applicable Laws.
- Recommendation 8 - Promote Cross-Border Cooperation and Information Sharing.
- Recommendation 9 - Understand and Assess Interconnections Among the DieFi Market, the Broader Crypto-Asset Market, and Traditional Financial Markets.

Additional academic and governmental resources can be found on the EU Crypto Initiative DeFi webpage and the Owl Explains DeFi webpage.

ENDNOTES

1. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf
2. https://www.chainalysis.com/blog/2021-global-defi-adoption-index/
3. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/
4. https://www.chainalysis.com/blog/2024-crypto-money-laundering/#:~:text=In%202023%2C%20illicit%20addresses%20sent,obfuscating%20the%20movement%20of%20funds.
5. https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download
6. https://www.owlexplains.com/en/
7. https://assets.ctfassets.net/eynrhjw8vyk9/6rJQPJfWcdGgp3MYBEndOd/1ccd9500c4ce4dd4939b44ee044a2171/Owl_Explains_-_IJBL_Volume_VIII.pdf
8. https://global-dca.org/core-principles/
9. https://global-dca.org/wp-content/uploads/2024/10/Information-Guidelines-for-Tokens-Available-in-US-FINAL-Oct-20-2024-1.pdf
10. https://www.gibraltarlaw.com/insights/post/102il0f/dlt-regulation-in-gibraltar-the-ten-principles/
11. https://github.com/OpenZeppelin/openzeppelin-contracts
12. https://www.steptoe.com/a/web/gVYaEV4B1drh8mne29DBvC/gfma-gdf-smart-contract-primer-report-2024.pdf
13. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf. One shortcoming of the IOSCO report is its failure to recognize that DeFi allows all asset classes to transact, not just financial instruments. The IOSCO report also lacks a definition of "decentralized" and does not differentiate between protocols that call themselves DeFi even though they are not decentralized. Notwithstanding these and other deficiencies, the IOSCO report's recommendations provide a solid set of reference points for approaching DeFi.

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland