BGIN SR 010
February 13, 2023

Proposal of Principles of DeFi Disclosure and Regulation

bg in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

This study is a work product of IAM, Key Management and Privacy Working Group of BGIN.

Introduction - Executive Summary -

The crypto-asset industry has seen a surge in DeFi, or Decentralized Finance, transactions since 2020. What does DeFi mean? DeFi itself has emerged recently and thus probably does not have a widely accepted definition (OECD, 2022). Nonetheless, DeFi has been explained in various ways in papers, reports, and speeches by various public organizations and academic researchers. For example, the FSB (Financial Stability Board) (2019) defines "decentralized financial" technology as "Technologies that have the potential to reduce or eliminate the need for one or more intermediaries or centralized processes in the provision of financial services." The BIS (The Bank of International Settlements)(2021) says that the term DeFi refers to the financial applications run by smart contracts on a blockchain, typically a permissionless (ie, public) chain. Ushida and Angel (2021) also define it as a "financial application that could consist of a part of a decentralized financial system" to emphasize the aspect that it is an application. In any case, it is definitely one of the focal points related to crypto-assets, which has attracted a lot of attention from crypto-asset investors, professionals, engineers, financial institutions, and regulators in recent years.

Since DeFi stands for "Decentralized Finance," the first characteristic of DeFi is that it is "decentralized," whether it intrinsically is or not. In other words, monies (in most cases, the crypto-assets) are exchanged or lent through an automatic program without the intervention of traditional financial intermediaries such as banks and securities companies. From a technical point of view, the essence is in the blockchain's feature of not having any single point of failure, meaning that the system will never fail. However, it is clear that this "no single point of failure" is not always realized in DeFi, as is demonstrated when a DeFi system is proven to be vulnerable to hacking and fraud. Under the DeFi framework, the exchange of money (in this case, crypto-assets) is done automatically according to an Ethereum program (in most cases).

In addition, the second characteristic of DeFi is mimicking the transactional aspects of traditional finance such as payments, exchanges, lending, lending/borrowing, investments(asset management/derivatives), and insurance. Table1 shows the summary of existing DeFi initiatives shown in FSB(2022).

This paper will define DeFi as financial applications that are automatically operated by smart contracts or other code on a blockchain. However, this would leave out other services that self-identifiy as DeFi. Thus, this paper will discuss implications for regulatory constructions by further screening it from the perspective of whether it is truly financial or not.

Table1: Summary of existing DeFi initiatives

	Description
Lending	By using smart contracts, users can become lenders or borrowers on DeFi platforms. Users typically post crypto-assets as collateral and then can borrow other crypto-assets. The most prominent platform typically requires $150 of collateral for every $100 of lending. Many platforms set interest rates automatically, depending on demand and supply of liquidity. Some of these platforms have characteristics analogous to commercial and/or central banks.
Investment (Asset Management /Derivatives)	Many projects offer a suite of yield-generating crypto-asset products by automatically routing crypto-asset “deposits” to highest-yield opportunities within a set risk-tolerance for particular pools. Other platforms allow derivative products such as synthetic assets, options or perpetual futures as well as crypto-asset tranches.
Decentralised Exchanges (DEXs)	Decentralised Exchanges claim to be peer-to-peer marketplaces based on smart contracts that allow trading in crypto-assets. They use automated liquidity pools, where investors ‘lock’ in their crypto-assets (in exchange for fees) to facilitate trading.
Payments	Many applications focus on increasing interoperability between blockchains, with the aim to increase scaling. Others focus on increasing the safety of existing means of payment (e.g. through the use of QR codes), by using the blockchain to validate transactions in real time.
Insurance	Some DeFi protocols, called discretionary mutuals, allow members to pool and share risks from smart contract failure, or mutualise premiums into smart contracts that trigger payouts when pre-defined risks or events materialise.

(Source) Excerpt from FSB(2022a)

DeFi has become quite popular among crypto asset investors, and there are several possible reasons for this. The primary justification for using DeFI is that by eliminating counterparties to financial transactions to the bare minimum number of participants, only the customer or investor and the DeFi system that has no possibility of human intervention whatsoever, counterparty risk can be eliminated. The DeFi system itself intermediates financial activity with other counterparties in a manner that generally requires overcollateralization and the automatic liquidation of positions to ensure the system has no possibility for insolvency. Thus, the overall risk profile of a DeFi system can be dramatically lower than for alternatives in a traditional, centralized financial system.

An alternate explanation for DeFi's recent popularity may be due to, the possibility it has been driven by a kind of bubble associated with the creation of many capital surpluses since interest rates had been very low and there was a strong sense of a money surplus due to fiscal and monetary policies in response to COVID-19. Another possibility is that DeFi became the receiver of such surplus money because DeFi had transactions (lending) that allowed users to earn a certain level of yield on crypto-assets just by depositing them.

DeFi is also noted for its cost savings, traceability, and its contribution to financial inclusion. However, while DeFi has these merits, various issues and problems have also been pointed out. For example, the fact that transactions are of varying traceability, the negative effects associated with anonymous transactions (specifically, the use of such transactions for money laundering and illicit activities), numerous hacking incidents, doubts about contribution to financial inclusion, inadequate governance when problems occur, and the protection of general users. In light of this situation, some regulators have argued that official regulation of DeFi may be necessary (Gensler, 2021; Crenshaw, 2021). U.S. Senator Elizabeth Warren has drawn attention to the DeFi market in particular, calling it "the most dangerous part of crypto"[1].

Thus, this paper summarizes the issues surrounding DeFi under these circumstances and presents some discussion points and suggestions for appropriate future regulatory considerations. Ultimately, we would like to propose principles for DeFi disclosure and regulation. Firstly, applying a traditional regulatory strategy to a new technological ecosystem has proved conceptually difficult because there is a policy trilemma called an innovation trilemma for introducing regulation for innovative services and products. That is, when we seek to provide clear rules, maintain market integrity, and encourage financial innovation, regulators have long been able to achieve, at best, only two out of these three goals (Brummer and Yadav, 2018).

Secondly, considering DeFi regulations, whether a DeFi constitutes the "financial service" which participants are subject to consumer/investor protection need to be considered first. Additionally, regulations from the perspective of systemic risk and anti-money laundering may be important regardless of such need for protection.

Lastly, the most important point would be to establish a disclosure system and common platform suitable for the characteristics of DeFi and crypto-assets, as well as an enforcement framework, considering the innovation trilemma. This is because establishing a suitable disclosure system for DeFi and crypto-assets is the most essential infrastructural foundation, when considering self-regulation, enforcement by government agencies, or for investors to pursue their own responsibilities. Establishing an appropriate disclosure framework is, while challenging, necessary to provide all

[1] See the article of The Block (March 2, 2022), " Democratic senators ask Treasury to report on work on crypto sanctions" (https://www.theblockcrypto.com/linked/136064/democratic-senators-ask-treasury-to-report-on-work-on crypto-sanctions) (Last viewed on February 8, 2023)

market participants information about the potential risks and benefits for any particular DeFi applications. To create a common disclosure platform in which national authorities and international standard-setting bodies could also participate and give authority would be desirable. Such a framework would provide basic information regarding a DeFi, such as disclosure of data, governance mechanisms, token information, as well as information on audits, etc., and it is also a convenient way to check for compliance. Designing an appropriate common disclosure platform that also considers participants' incentive structure is very challenging and will be the subject of further research.

This paper is considered to be a publication that further updates the BGIN (2021) produced by the IKPWG (IAM, Key Management and Privacy Working Group) in the BGIN. The structure of this paper is as follows. First, Chapter 1 describes the targets and objectives, and Chapters 2-4 provide terminological and technical explanations and notes on the use of this paper. Chapter 5 presents the issues and problems surrounding DeFi, followed by discussion, implications, and suggestions on regulation in Chapter 6. In Chapter 7, after a brief survey of the current disclosure and regulatory landscape, proposals for DeFi disclosure and regulatory principles are presented. Finally, a summary and further potential topics will be presented.

Table of contents

1. Scope

The targeted audiences of this document are regulators, academia, DeFi participants including developers and engineers, and more generally anyone looking to expand his/her knowledge on the topic.

We are going to introduce the current status and challenges we face in a decentralized finance society. At the first, we explain the benefits, advantages, and possibilities of DeFi and the surrounding ecosystem. Next, we will discuss the problems, risks, and questions of DeFi. Then we will discuss implications for regulatory consideration and propose the principles of DeFi disclosure and regulations.

2. Normative reference

This document has no normative reference.

3. Terms and definitions

This document uses the following terms as the shortcut for more complete wording provided as the definition. When the term appears within this document, it should be read as being replaced by the term.

(1)Decentralized financial technologies

Technologies that may reduce or eliminate the need for one or more intermediaries or centralized processes in the provision of financial services
[SOURCE: FSB (2019)]

(2)Decentralized financial system

A new financial system that could be the result of decentralized financial technology
[SOURCE: FSB (2019)]

(3)Decentralized Finance (DeFi)

Financial applications that are automatically operated by smart contracts or other code

(4)Smart contract

A collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network. The smart contract is executed by nodes within the blockchain network; all nodes must derive the same results for the execution, and the results of execution are recorded on the blockchain

[Source: NIST (NISTIR 8202)]

4. Abbreviations and symbols

In this document, the following abbreviations and symbols are used.

AML	Anti Money Laundering
BGIN	Blockchain Governance Initiative Network
BIS	Bank of International Settlements
DeFi	Decentralized Finance
DAOs	Decentralized autonomous organizations
FATF	The Financial Action Task Force
DEX	Decentralized Exchange
FSB	Financial Stability Board
IOSCO	International Organization of Securities Commissions
KYC	Know Your Customer
SBTs	Soulbound Tokens
SEC	The U.S. Securities and Exchange Commission
NIST	National Institute of Standards and Technology
WEF	World Economic Forum

NOTE: All the abbreviations SHALL appear in this clause.

5. Issues related to DeFi

5.1 Benefits, advantages, and possibilities of DeFi

There are, of course, certain reasons why DeFi is getting so much attention and excitement. This section points out some advantages and possibilities. The expected benefits of DeFi have been pointed out in preceding literatures (Chen, 2019; FSB, 2019, etc.). However, again, and this point is very important, it should be noted that some of the advantages listed below are subject to reality check.

First of all, DeFi can be identified as a potential contributor to promoting innovation and competition. Activities that used to take a lot of cost and effort in existing financial transactions can be done automatically by utilizing smart contracts (persistent scripts). As a result, it is clear that this has the potential to contribute to reducing costs and promoting innovation toward the automation of transactions. Currently, DeFi is mainly limited to crypto-asset trading. However, if the technology is extended to traditional financial institutions, it could encourage competition with existing financial institutions and thus promote innovation.

Secondly, as FSB (2019) pointed out, the DeFi technology may reduce some of the financial stability risks associated with traditional financial institutions and intermediaries. In financial transactions, there is a risk called "concentration risk." "Concentration risk" refers to the risk that entire transactions will be affected if an entity that concentrates most of the transactions is in halt/insolvent. If transactions and systems were decentralized, it would clearly contribute to reducing concentration risk. From a technical point of view, this benefit may be attributed to the feature of having no single point of failure.

Third, DeFi transactions are currently mostly traceable.. As the majority of DeFi protocols currently exist on the Ethereum blockchain, rather than other blockchains, or layer two solutions (FSB, 2019). As a result of this, it is relatively straightforward to trace transactions through tools such as Etherscan. This is rapidly changing, however, as centralised layer two solutions may not necessarily provide the same level of transparency. Zero-knowledge technologies, designed to obfuscate transaction history and promote privacy, are very important in preserving privacy, but may make tracking and traceability more difficult.

Fourth, transactions can take place regardless of national borders, making international transactions easier. While centralised exchanges are often bound by similar laws to banks, DeFi has proved to be a powerful asset in cross-country transactions, particularly for those in crypto-negative countries. Stablecoins aim to denominate a fixed value over time, which is very useful for transactions within the crypto ecosystem, as well as cross-border transactions. These coins are often fully collateralised or over-collateralised with real-world asset backing, such as short term US treasury bonds, crypto-asset backing, or alternatively, maintain algorithmic balance when traded. While they only account for a small part of the crypto market, the most trusted stablecoins hold

this crucial role in payments and cross-border transactions, reducing volatility. They also currently provide most of the liquidity in DeFi applications (Born et al., 2022).

Fifth, their contribution to financial inclusion is often pointed out. It is estimated that about 1.7 billion adults remain unbanked—without an account at a financial institution or through a mobile money provider (The World Bank, 2017). DeFi has the potential to extend the benefits of finance to many more people since financial transactions can be done with a smartphone. The World Bank (2017) indicates that digitalization (technology) contributes to financial inclusion, and financial inclusion is contributing to the wellness of countries. WEF (2021a) also pointed out that decentralized finance (DeFi) was emerging as a tool for smaller businesses in developing markets, particularly for remittances and small loans, and may contribute to financial inclusion.

Lastly, DeFi also may be the basis for a future version of the internet or Web3. Web3 is also being considered as one of the elements of the future Internet, although it has not yet been clearly defined. DeFi forms the basic structure on which a future Web3 internet may grow. By establishing financial structures that are resilient, efficient and permissionless, it could form a foundational infrastructure on which private companies may grow. Easy, trusted transactions allow payment for services, products and use of these systems, and also act as a proof of concept for emerging uses of non-financial token registration, distribution, use and transfer that we are seeing now, such as SBTs and governance. The permissionless, global nature of DeFi means that systems can be built with user bases that aren't limited by geography, political stability, or technological monopoly - as long as effective governance protects these core principles.

In summary, the benefits of DeFi (including potential benefits) are: it may (1) contribute to innovation, with increasing efficiency and potentially a dramatic decrease in the cost and overhead of financial services, (2) reduce the risks of financial concentration and counterparty default, (3) bring the traceability of transactions that blockchain brings (but at the same time raises concerns about privacy, which, at the same time, can be a disadvantage). (4) make international financial transactions easier, (5) contribute to financial inclusion, and (6) contribute to the future of the Internet, Web3

5.2 Challenge, risks, and questions related to DeFi

On the other hand, a number of problems have been pointed out with DeFi, although many of them seem to come from the flip side of the advantages presented above.

(1) Lack of AML/KYC

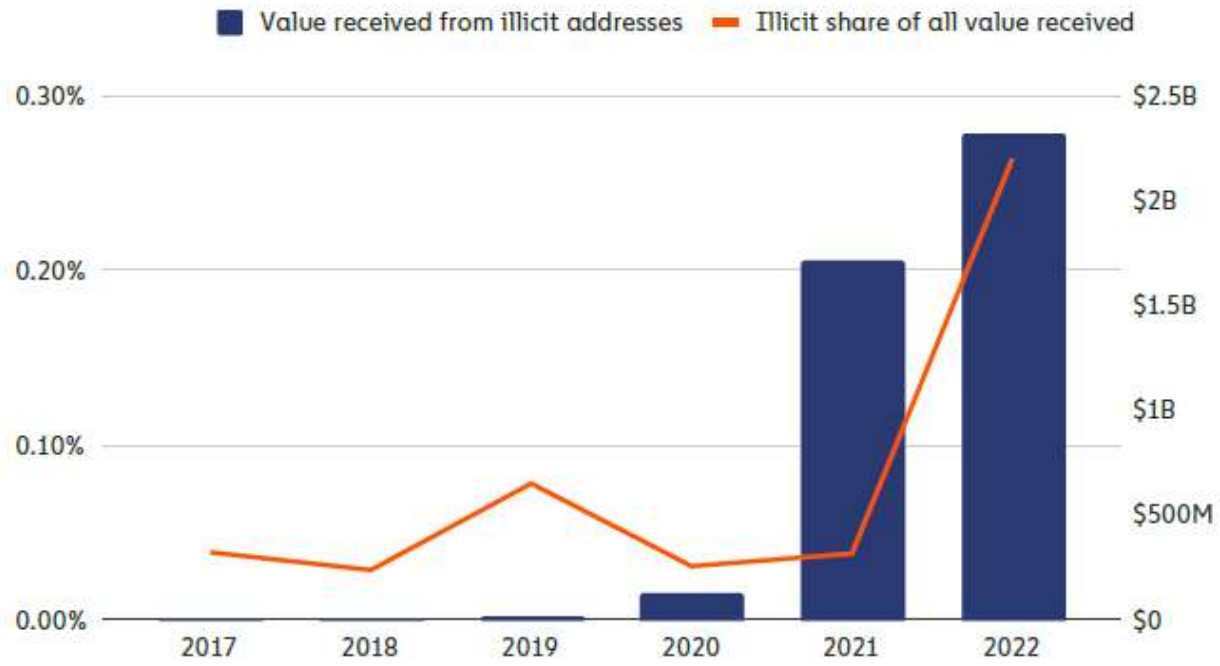
One of the main points of contention with DeFi is the potential for money laundering. Many DeFi platforms do not perform KYC (Know Your Customer) or identity verification for transactions. For example, a decentralized exchange or “DEX”, one of the fundamental DeFi activities, allows the exchange of cryptographic assets and allows transactions across international borders without an intermediary. This may make it easy for money launderers to clean up illegal funds If the DEX's compliance system was

inadequate. In the case of traditional financial transactions, financial institutions such as banks and securities companies perform AML/KYC. In contrast, AML/KYC in the DeFi context is generally only performed by regulated centralized exchanges when fiat currencies are exchanged for digital assets, the on and off ramps to the digital asset ecosystem. Given that DeFi systems typically do not provide for human intervention to verify the identity of participants, KYC is not possible without new capabilities to identify participants in the DeFi context . For example, according to Chainalysis (2022b), illicit DeFi transactions have risen steadily over the last three years, in terms of both raw value and also as a share of all transaction value. Chainalysis (2022b) said that this is primarily in two areas: Theft of funds through hacking, and abuse of DeFi protocols for money laundering (Figure1).

FATF (2021) has identified this as a problem, and AML (Anti Money Laundering) is currently a significant concern in DeFi. However, since a DeFi is enabled by automated application programs, applying AML proves to be a challenge, and this point will be discussed later.

However, there is also the counter argument to increased DeFi regulation, that on and offramps are increasingly monitored and most comply with AML/KYC guidelines. This, along with the inherent traceability of blockchain, and cooperation of many protocols suggest that inherent hard laws requiring KYC/AML for all DeFi protocols may be regarded as overregulation. Many DeFi users also suggest that increased regulation of DeFi protocols may stifle growth of this budding industry, and replicate some of the issues in traditional finance on-chain. This is particularly an issue when laws and regulations are unclear and everchanging - let alone the fact that these protocols would be required to comply with the laws of every single country in which their protocol is used.

Figure 1: Total value received by DeFi from illicit addresses vs. illicit share of all value received by DeFi



(source) Chainalysis (2022b)

(2) Hacking

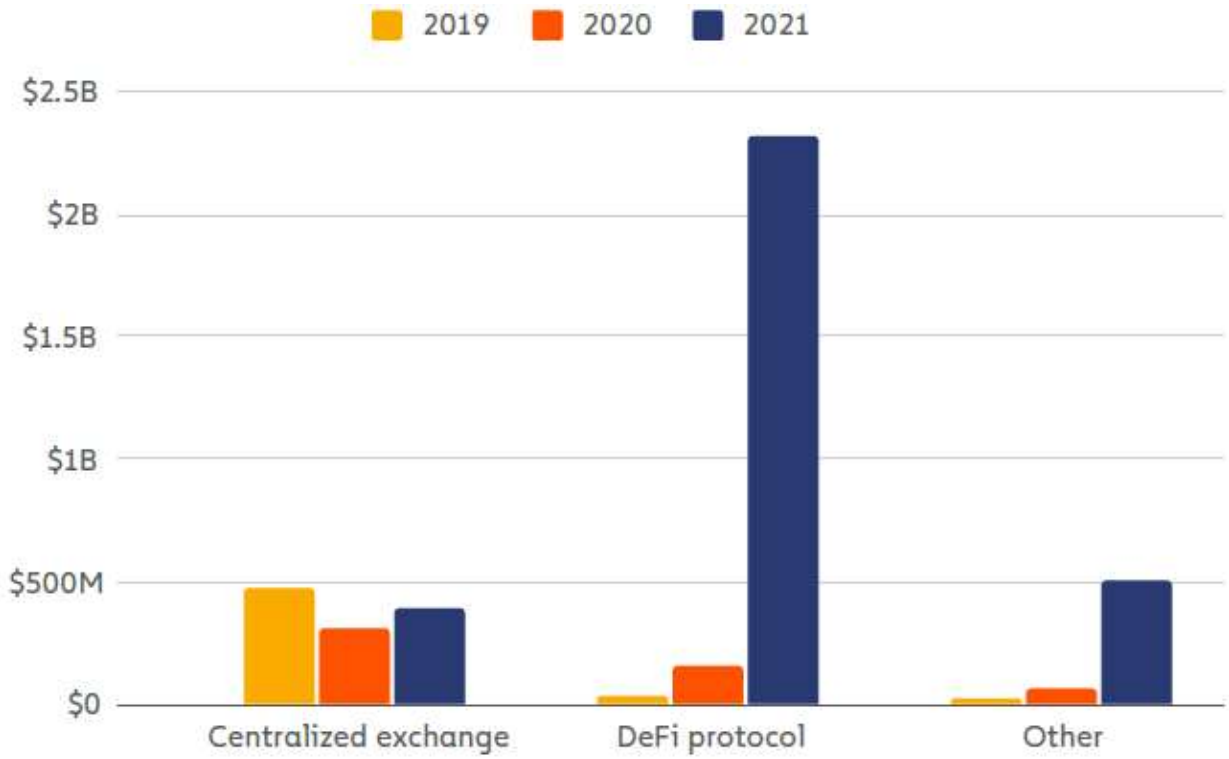
Recently, there has been a lot of hacking related to DeFi platforms in which crypto-assets have been specifically targeted for hacking and successfully stolen. According to Chainalysis (2022a), in 2020, $162 million of crypto-assets were stolen from DeFi platforms, but in 2021, that rose significantly by about 13 times to about $2.2 billion. In 2021, a total of $3.2 billion in crypto-assets were stolen, with DeFi's share of that total nearly doubling from 31 percent to 72 percent, a significant increase.

According to Chainalysis (2022a), most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds. It has also been pointed out that DeFi itself is very new, and the fact that the programs are typically open to the public makes it easier for hackers to find vulnerabilities, which may be leading to increases in hacking.

However, with improved smart contract auditing, and improved education of end users regarding responsible management of funds, and self-custody, it is also pointed out that these hacks will decrease over time (Chainanalysis, 2022a). It is important to remember that in traditional systems, funds are usually managed by sophisticated investors, whereas the onboarding of retail to DeFi means base education is generally lower. While traditionally, retail risk may be constrained to losses on bad investments, there is a larger risk in DeFi, with a diverse range of financial instruments, with varied resilience and safety to hacks. It is also worth mentioning that when hacks occur on-chain, it is easier to track the transactions following the hack than in traditional finance, with an

immutable record of the offenses. In addition, the scale of DeFi hacks must also be compared to losses in traditional financial institutions and funds in order to provide a valid measure of severity.

Figure 2: Cryptocurrency stolen by victim type, 2020 - 2021



(source) Chainalysis (2022a)

Cross-chain bridges are especially at heavy risk, and they are crucial infrastructure of the multi-chain ecosystem. They facilitate and lock a large amount of capital, and provide considerable ease to consumers interacting and moving funds across a multi chain DeFi ecosystem. According to the statistics by Dune Analytics[2], the total locked-in value (TVL) of Ethereum's 15 biggest cross-chain bridges was about $5.58 billion dollars as of February 2, 2022. Currently, the highest TVL is Polygon Bridges ($3.6 billion dollars), with the second largest being Arbitrum Bridges ($1.44 billion dollars), followed by Optimism Bridges ($1.241 billion dollars).

Firstly, due to the high quantity of liquidity and low degree of decentralisation, cross-chain bridges are often an ideal attack vector for hackers. According to SlowMist Hacked data reports[3], as of June 30 2022, there were seven cross-chain bridge security

[2] See Dune site (https://dune.com/eliasimos/Bridge-Away-(from-Ethereum) (Last viewed on February 8, 2023)
[3] See website “2022 Mid-Year Report for Blockchain Security”, (https://slowmist.medium.com/overview-of-blockchain-security-2022-mid-year-report-15078f52b072)

incidents, with losses totalling $1.043 billion, which accounts for 64% of DeFi's total losses and 53% of total losses overall in the first half of the year. Furthermore, the cross-chain bridges create an environment where money laundering can occur without effective mitigation controls in place. Due to the decentralised nature of permissionless bridges, and smart contract technology, the traditional KYC/AML/CTF controls any given centralised exchange must perform and utilize, such as freezing funds or enhanced due diligence are not nearly as possible. As seen in the Elliptic (2021);

> “Proceeds of crime can be transferred between blockchains without going through a centralized service provider such as an exchange, where users’ identities are verified and funds linked to illicit activity might be seized. Decentralized cross-chain bridges have been used to transfer proceeds of hacks, ransomware, darknet market sales and other criminal activity”

As the blockchain enabled economy, and DeFi ecosystems respectively inevitably grow to include more regulated money, such as CBDCs, it will be important to explore ways to both reduce the technical risk of hacking and money laundering risks associated with multichain interoperability performed by cross-chain bridges. These bridges could even represent an ideal vector for regulation of DeFi to place itself, as many straddle decentralised and centralised controlling entities, something regulation can more clearly define outcomes for.

(3) Is it really "Decentralized"?

In transactions through DeFi, there is no primary financial intermediary. However, many have questioned whether DeFi is truly decentralized. In fact, the definition of "decentralized" seems to be unclear. IOSCO (2022) mentioned that what should be considered "decentralized" is not clear. For example, the governance functions of a DeFi, such as voting power, ownership structure, the authority to control the provision of services or products, the authority to manage customer assets, the authority to improve services or products, and so on may or may not be truly decentralized. IOSCO (2022) points out that the extremes of the decentralization spectrum are explained from "Pure Decentralized Protocols" to "Pure Centralized Protocols," and it is unlikely that most DeFi products and systems fall squarely into either extremity, with most sitting somewhere between the two. In practice, it is often the case that some parties can dominate and exert influence in changing the code of the DeFi protocol, that governance is not fully decentralized, or that the revenue that comes from DeFi is not distributed equally. "Decentralized" could be in some cases just a marketing word, and the actual DeFi is often centralized or near-centralized.

For example, BIS (2021) points out that "there is a “decentralisation illusion” in DeFi due to the inescapable need for centralized governance and the tendency of blockchain consensus mechanisms to concentrate power.” BGIN (2021) also points out that the degree of decentralization varies from one DeFi project to another, and many of them

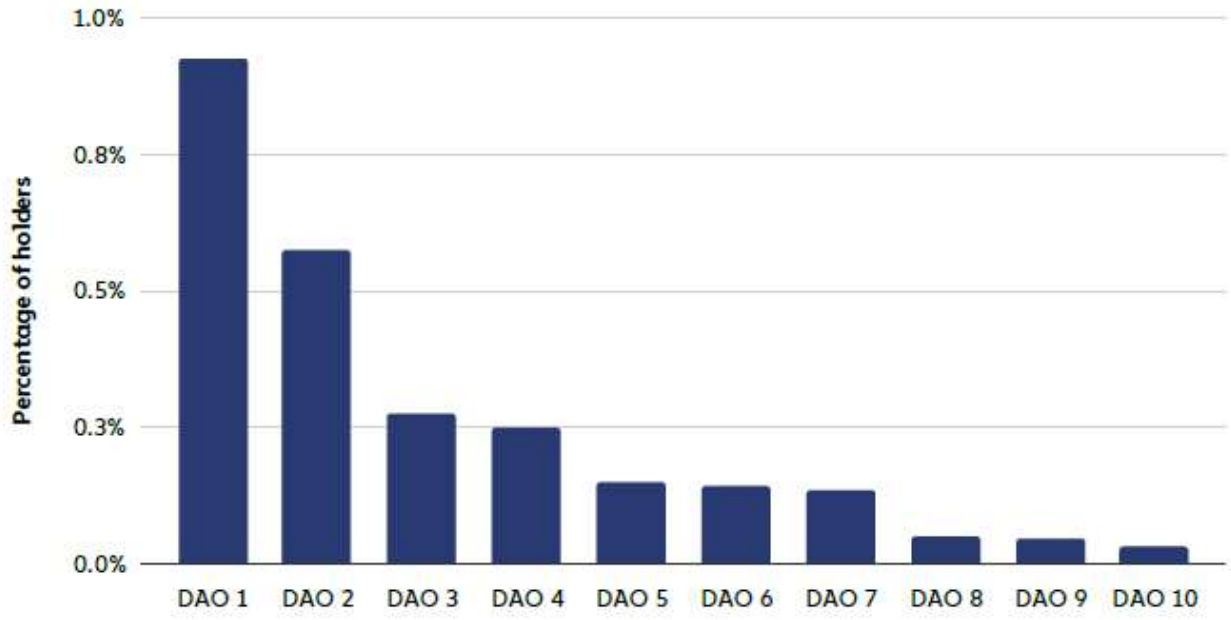
---

(Last viewed on February 8, 2023)

are quite centralized, especially early in their operation. Specific individuals or groups typically have the authority to change the protocol or freeze locked assets. However, given the variety of DeFi forms, it is important to point out that there is no "one-size-fits-all" solution for DeFi governance forms and that the degree of concentration varies from project to project.

Chainalysis(2022b) points out that the governance of DeFi, which is supposed to account for most of the DAOs(Decentralized autonomous organizations), is actually not so much decentralized as promoted and is surprisingly centralized. Figure 3 shows that, across several major DAOs, less than 1% of all holders have 90% of voting power.

Figure 3: Share of users holding 90% of all governance tokens by DAO



(source) Chainalysis(2022b)

In addition, Ushida and Angel (2021) and BGIN (2021) point out that some DeFi projects have a specific party with administrative authorities to modify the protocol at its discretion via private keys called "admin keys," and the existence of "admin key" can be evidence to question decentralization to a certain extent. The owner of the "admin key" may change programs and parameters related to the DeFi project without permission. Moreover, not only that, if this "admin key" is stolen by hackers, the user's assets could be stolen in the worst-case scenario. The existence of "governance tokens" can also be considered from a similar perspective, pointing out that DeFi projects where governance tokens play a major role in governance may be less decentralized.

As a concrete example of centralized governance in a DeFi project, Allen (2021) points out that the "BadgerDAO" has recently suspended smart contracts due to reports of unauthorized access. However, if they were "decentralized" they would not have been

able to do this so quickly[4]. If there is no central operator, then there is no one to comply with enforcement action. Therefore, enforcement action against the DeFi platforms would be impossible, nevertheless there have been cases of enforcement action against the DeFi platforms. Specifically, in August 2021, the SEC issued an enforcement action against a DeFi platform. The SEC imposed a cease-and-desist order on Blockchain Credit Partners (the company that operates the DeFi Money Market) and two others who controlled and operated the company for selling more than $30 million in "securities" through the DeFi Money Market using smart contracts and so-called "decentralized finance" (DeFi) technology between February 2020 and February 2021[5]. According to the SEC's announcement and related press reports, this case is the first time that securities using a DeFi have been the subject of enforcement action (the case ultimately ended in a settlement in which the defendants did not even admit or deny). SEC Chairman, Gensler, referred to this action as a specific example of a case where the DeFi was not actually decentralized in the sense that there was an entity that could be punished. Specifically, based on this case, he pointed out that " These platforms facilitate something that might be decentralized in some aspects but highly centralized in other aspects"[6]. In addition, Gensler points to the existence of a "promoter and sponsor" structure as the core group that creates the software for the DeFi platform and builds its governance, while often also doing the governance and earning the fees, in addition to writing the software programs[7]. BGIN (2021) makes an interesting point about the direction of DeFi's decentralization in the future. Thus, while some DeFi will further promote decentralization to avoid regulation, some will go the other way and become more centralized. As mentioned above, there are numerous indications that DeFi operates on a spectrum of "Decentralization."

(4) Is it really "traceable"?, is it “accessible to all”?

Some argue that a DeFi is not traceable in practice. Crenshaw (2021), who is a commissioner of the U.S. Securities and Exchange Commission (SEC), points out that, as for the lack of traceability, even though all transactions are recorded on a public blockchain, in reality, DeFi investments are not fully traceable, and only a limited small

---

[4] According to Twitter, they tweeted “Badger has received reports of unauthorized withdrawals of user funds. As Badger engineers investigate this, all smart contracts have been paused to prevent further withdrawals. Our investigation is ongoing and we will release further information as soon as possible," (https://twitter.com/BadgerDAO/status/1466263899498377218)(Last viewed on February 8, 2023).

[5] For more information, see SEC press release (https://www.sec.gov/news/press-release/2021-145) (Last viewed on February 8, 2023). The order is as follows.
Blockchain Credit Partners d/b/a DeFi Money Market, Gregory Keough, and Derek Acree, Order Instituting Cease and Desist Proceedings, Securities Act Release No. 10961 (August 6, 2021).

[6] Wall Street Journal (Aug. 19, 2021) " Crypto’s ‘DeFi’ Projects Aren’t Immune to Regulation, SEC’s Gensler Says Some peer-to peer trading and lending projects have features that may trigger the need for regulation,chairman says"
(https://www.wsj.com/articles/cryptos-defi-projects-arent-immune-to-regulation-secs-gensler-says 11629365401) (Last viewed on February 8, 2023)

[7] In the above article（Wall Street Journal on Aug. 19, 2021）, he referred“There’s still a core group of folks that are not only writing the software, like the open source software, but they often have governance and fees,” “There’s some incentive structure for those promoters and sponsors in the middle of this.”

group of people can read and understand the code. Even highly qualified experts miss the flaws and dangers. Thus, these facts raise concerns that (technology) insiders will reap huge profits, while ordinally investors will take more risks, be offered unfairly bad prices, and be exploited over time. It has been pointed out by Popescu (2020) and others that one of the major issues to be addressed in the future is the user interface. In other words, DeFi is still difficult to use for the general public. Certainly, DeFi operates with code that is available to everyone, so it seems that it is more equal and traceable. However, in reality, it is easy to imagine that only a small number of people can read and understand the code. In addition, the content of the code can vary from one smart contract to another dramatically, and that can have a significant impact on investment outcomes and safety. Even if a DeFi aims for a broad range of investment products, the general public could not understand the risks associated with a code as they might with a disclosure prospectus for securities products. It is unreasonable to assume that only technologically capable investors who understand complex codes make up the financial system.

More concretely, many DeFi projects are funded by venture capital and professional investors, but it is not clear how much small investors understand this situation. According to Crenshaw (2021), professional investors bring with them rights such as equity, options, access to project team management, involvement in governance whether formalized or informalized, non-dilution rights, and control rights, which are rarely disclosed. On the other hand, they have a significant impact on investment value. It can be said that venture capital does not necessarily be a good representation for public interest such as investor/consumer protection. Therefore, Crenshaw (2021) pointed out that small investors are at a great disadvantage compared to professional investors, and this information gap will exacerbate the problem.

(5) Market manipulation and difficulties in investigation

It has been noted that market manipulation often occurs in the trading of crypto-assets (Gandal et al. 2018; Griffin and Shams, 2020). Despite the existence of market manipulation, there are few market manipulation regulations and other significant issues exacerbating the problem. In terms of market manipulation investigations, Crenshaw (2021) points out that the feature of pseudonymity can be a problem as well. In many cases, DeFi records all transaction IDs on the blockchain, they cannot be tampered with, and everyone can see them. However, the ID does not actually identify the person who controls the transaction. It merely indicates the address which is controlled by some individual. Since there is often no effective way to identify who is actually the owner of addresses, it is impossible to know, for example, whether a group of people is engaging in market manipulation, or one person is controlling multiple addresses. This makes it difficult for regulators to investigate market manipulation in DeFi market.

Crenshaw (2021) points out that, in the U.S. securities world, sharing identities with participants limits privacy to some extent, but instead makes markets more comfortable, and market participants agree to these practices. In return for a lower degree of privacy, market participants have benefited from a fair, orderly, and efficient market, with less

fraud and market manipulation. DeFi, on the other hand, does not do so (share IDs, etc.) because investors are more privacy-oriented, according to Crenshaw (2021). This is because the use of alphanumeric strings to provide privacy is a core feature of Bitcoin and is typical to most blockchains.

In a recent study, Auer et al. (2022) also noted market manipulation in the DeFi market. Auer et al. (2022) point out that cryptocurrencies such as Ethereum and DeFi built on them rely on validators or “miners” as intermediaries to verify transactions and update the ledger. Since these intermediaries can choose which transactions they add to the ledger and in which order, they can engage in activities that would be illegal in traditional markets such as front-running and sandwich trades. The resulting profit is termed “miner extractable value” (MEV). MEV is an intrinsic shortcoming of pseudo-anonymous blockchains. So addressing this form of market manipulation may call for new regulatory approaches to this new class of intermediaries.

(6) Does it really contribute to "Financial Inclusion"?
The explanation that DeFi contributes to financial inclusion is also somewhat questionable. It is true that even the unbanked people often have smartphones, so allowing financial transactions through smartphones even without a bank account certainly could promote financial inclusion. However, there are two major problems.

First of all, “Competent Knowledge and Literacy” issues can be raised. Even if a person has a smartphone, it does not mean that he or she is capable of trading through a DeFi. Rather, DeFi is likely to require a high level of skill and knowledge/literacy, which may even result in widening the disparity between those who have and haven’t. Especially when DeFi is still a kind of nascent technology. As for stablecoins, which constitute as a DeFi, WEF (2021b) notes that its contribution to financial inclusion is limited at this time. This is after all, due to limited access to the internet and other resources themselves, as well as a lack of digital-related knowledge.

Secondly, usage is currently limited. Even if DeFi could be done through smartphones, it would only be crypto-asset trading. Although there are cases of using a DeFi to avoid high remittance costs, the case is still limited. Currently, most lifestyle-related transactions are not covered, hence this situation is not contributing to financial inclusion.

(7) Operational risk in DeFi

Since DeFi is automatically executed by smart contract, it is generally thought that there is no operational risk, but in reality, there probably is.

First, DeFi cannot be halted or undone basically. The fact that it is automatically executed by smart contract can itself be a major risk. For example, when participants make a wrong transaction, it cannot be easily undone or corrected. This is also a very important point of view for regulators. There is a risk that the program will be

automatically executed, there will be nothing that can be done even if it involves unfair trading or illicit activities where it would be desirable to order a halt or undo the trading.

Second, there is “Oracle risk”. DeFi generally refers to external information, in the form of an "oracle". For example, this information is used to incorporate the price of crypto-assets or other exogenous information not available on a blockchain, into the operation of on-chain code. If the reference price is incorrect or intentionally distorted, the trading price of the cryptocurrency within the service will be greatly dissociated from other services, and participants may unreasonably lose a huge amount of money. This risk is called the "oracle risk."

(8) Characteristics of procyclicality and the potential for systemic risk associated with it

Some DeFi transactions are considered to have characteristics of a so-called "procyclicality". "Procyclicality" was a major theme in the analysis of the financial crisis after the Lehman shock in 2008, and in essence, it means that financial transactions are self-propagating and bring about expansionary effects such as business cycles. Procyclicality tends to occur especially when lending is dependent on the economy and collateral. When the economy is booming and the value of collateral rises, the amount of lending rises further in response to the rise in collateral value, which in turn causes the value of collateral to rise again, leading to further increases in lending. On the other hand, if the economy worsens and the value of a collateral falls, this will lead to a further decline in lending, which in turn will lead to further economic deterioration, creating a vicious cycle.

This mechanism of procyclicality is found in a DeFi's lending as well because it is done with crypto-assets as collateral but has systemic fragility compared to traditional intermediaries who only retain collateral as insurance (Lehar et al. 2022). Since many decentralized finance (DeFi) lending protocols require loans to be over-collateralized, and loans that fall below a certain threshold are automatically liquidated by third parties. Lehar et al. (2022) notes that these liquidations have a sustained cascading effect on asset prices, which often triggers further liquidations. In addition, lack of regulation in leverage ratio may lead to hypercyclicality or rapid contagion. Therefore, when it comes to crypto-asset prices, a rise leads to a further rise, while a fall leads to a further fall. There is another risk that when a large number of financial institutions are involved in DeFi transactions it will spill over to the financial institutions. This is a risk that could lead to systemic risk. As Allen (2021) points out, DeFi is a type of shadow banking system with fragilities that could – if DeFi reaches a significant scale – disrupt our real economy.

(9) Lack of ability to address risks associated with information asymmetry

From a financial theoretical point of view, financial institutions (in this case, assuming a bank) usually exist to deal with the risks associated with information asymmetry between lenders and borrowers. In other words, in the bank's example, it functions to

decrease information asymmetry that exists between depositors and borrowers by analyzing the credit information of borrowers instead of depositors who lack information on borrowers, and by lending only to creditworthy firms. However, in a DeFi, there is no such financial intermediary with critical gatekeeper functions. Analysis of a borrower's credit is often determined by the availability of collateral and not by analysis of other financial information. Only financial transactions are carried out automatically according to the code. In this sense, it would seem to suggest that DeFi is not currently a viable alternative to financial institutions.

In traditional finance, credit or reputation is an important factor. The borrower has the incentive to prove their trustworthiness and the lender needs reliable information to assess the risk of the borrower. Without any reliable information, it would lead to hesitance of lending, setting a high interest rate, or requiring over-collateralization. In fact, Weyl et al. (2022) has raised the problem of a DeFi not being able to replicate real world financial systems because there is currently no ground to build a reputation. They introduce an idea of Soulbound Tokens (SBTs) which are “publicly visible, non-transferable (but possibly revocable-by-the-issuer) tokens held by the soul”. A “soul” is an account or wallet which has linkage with the real world community. Though the idea is still in an early stage, as BGIN (2022) discussed in its study report, it has the potential to diminish unintentional information asymmetry, one of the consequences would be being able to replicate current financial service such as uncollateralized lending in a DeFi. The paper states that it could also have the potential to be used to counter Illicit economic activities, promote regulatory measures such as AML/CFT, and ensure fair, transparent, and accountable governance.

6. Implications for regulatory consideration

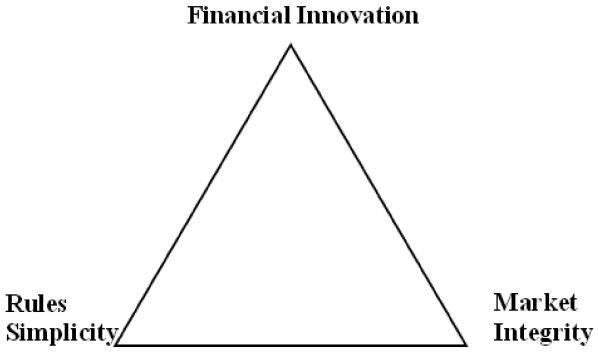
DeFi is not currently regulated as a financial product or trading activity in most countries, but there are many challenges as described above. There is no doubt that market authorities are currently in the process of seriously considering how a DeFi should be treated. In the United States for example, the President's Working Group (PWG) (2021) refers, "Digital asset trading platforms and DeFi also raise broader questions about digital asset market regulation, supervision, and enforcement." and " These questions are under active consideration by the CFTC and SEC." IMF(2022) also calls for more work needs to be done on crypto regulation.

Thus how should DeFi be regulated? What kind of regulations can be considered in DeFi, where "code is law" (De Filippi, 2019)? We discuss the viewpoints to be taken when considering the regulations below.

6.1 Innovation trilemma

First of all, we consider the basic approach in applying regulations to new technologies that create innovations, such as DeFi. Brummer and Yadav (2018) mentioned that applying a traditional regulatory strategy to a new technological ecosystem had proved conceptually difficult because there is a policy trilemma for introducing regulation for innovative services and products (Figure 4).

Figure 4: Innovation trilemma



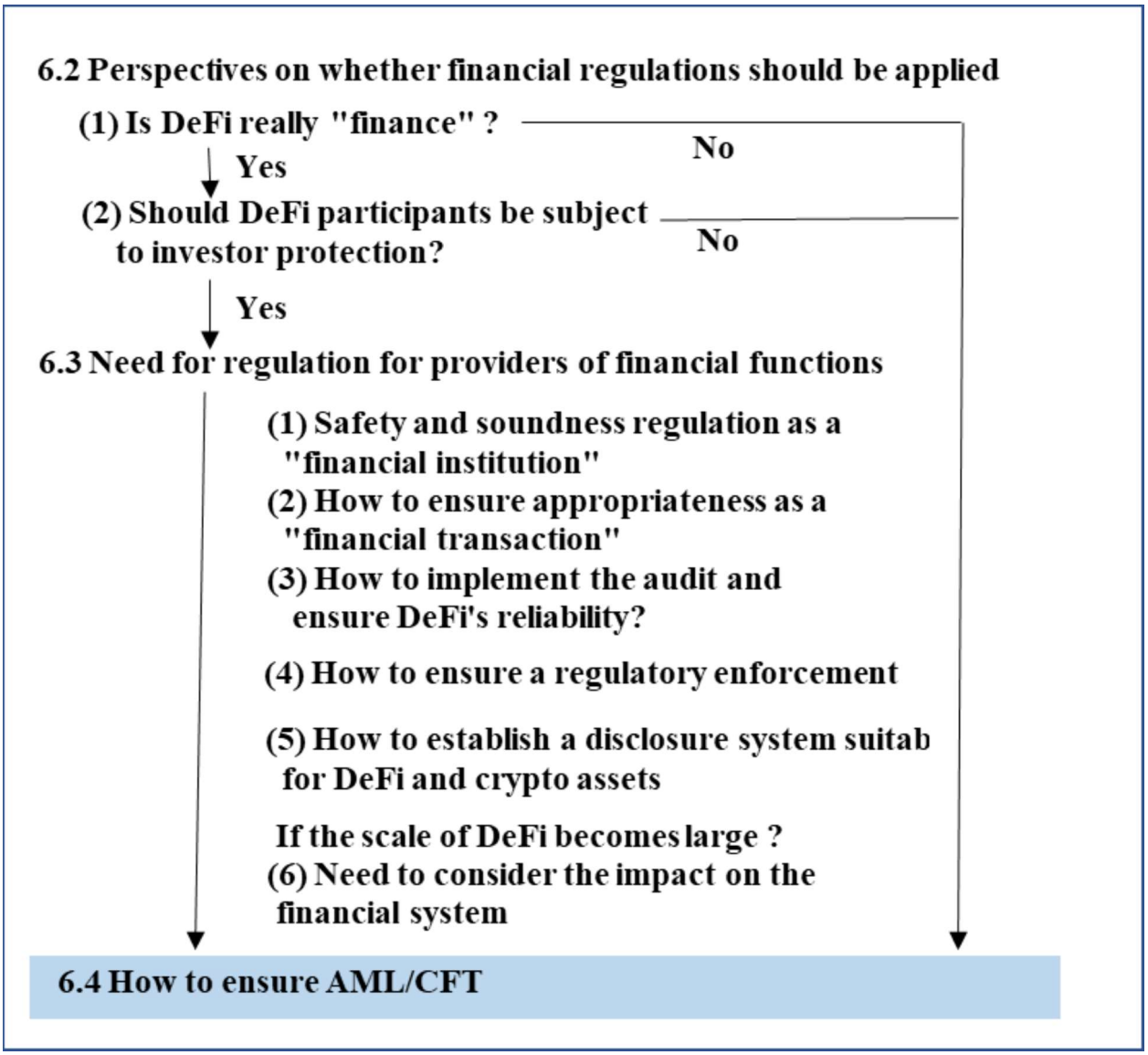
(source) Brummer and Yadav (2018)

That is, when we seek to provide clear rules, maintain market integrity, and encourage financial innovation, regulators have long been able to achieve, at best, only two out of these three goals. For example, if regulators prioritize market safety (integrity) and clear rulemaking, they will have to establish detailed regulations, which may tend to inhibit innovation. Alternatively, if regulators attempt to encourage innovation but also clear rulemaking, they may be forced to respond with brief, high-level regulations, thus increasing the risk of undermining market integrity. Finally, if regulators are focused on

both market integrity and innovation, they will be forced to create complex rules and exemptions, which will ultimately lead to increased difficulties in compliance, international cooperation, and enforcement, which may lead to a lower level of market integrity.

Under these circumstances, what kind of regulatory implications can be expected for DeFi? It is clear that the current regulations on DeFi are almost non-existent, and many problems in the market have been identified. Thus at this point, we could sacrifice two out of the three. Therefore, the vital question will be whether to prioritize market integrity or regulatory simplicity while maintaining ongoing innovation.

Figure 5: Framework for regulatory considerations



(Source) Created by the author

For this reason, as Figure 5 shows, this paper will first examine whether a DeFi can be subject to market integrity in the first place, and more specifically, whether it is regulated as financial and whether participants can be subject to protection. If so, then we will need regulations as required of a financial institution. Nevertheless, given the current revelations of money laundering and the use of illicit funds, it is essential to address these illicit activities in one way or another. And in any case, it is necessary to consider what kind of enforcement will be implemented without clarity about the state and jurisdiction (Figure 5).

6.2 Perspectives on whether financial regulations should be applied

(1) Is DeFi really "finance"?

Since "DeFi" is an abbreviation for "Decentralized Finance," it is natural to think of it as "finance." Moreover, it is precisely whether it constitutes a “financial service”. However, in reality, first of all, we need to consider whether we can really think of it as "financial service". If it is not a "financial service," then there may be less demand to regulate it as a financial product[8]. Specifically, it may not be "financial service," but part of a game. Token lending and investment-like activities in the game are, of course, not subject to financial regulations. Allen (2021) stated that a DeFi is like an “incorporeal casino", and treating stablecoins like regulated deposits will provide implicit government backing to that casino, encouraging its growth. It is inappropriate and should be avoided to legitimize non-financial activities, e.g. lending and borrowing within a “game”, by imposing financial regulations. It would be outside the scope of financial regulations if it is a non-financial transaction.

Above all, it is necessary to confirm whether a DeFi is "financial services" or a kind of "finance" in the sense that it is subject to regulation. It may be possible to identify which parts of the DeFi are "finance" and which parts should not be regulated. The basic principle is "Same business, Same risk, Same rule" as usually said. Thus, if a particular project among a DeFi is not regarded as "financial service," then, of course, there is no need for financial regulation to apply.

(2) Should a DeFi participant be subject to investor/consumer protection?

Even if a DeFi (or part of it) is "financial services," there is also the question of whether its participants are subject to investor/consumer protection. In other words, are DeFi market participants subject to the same protections as ordinary investors in the traditional financial markets? Even in the traditional financial market, qualified investors

[8] See, for example, Armour et al.(2019) for a discussion of what finance is.

with a certain level of knowledge and institutional investors are professional and therefore responsible for their own investment. Nevertheless, for professional investors to make appropriate judgments, solid explanatory documents and disclosures are necessary, so it will be necessary to have a system in place to enable them to make appropriate investment decisions.

In any case, if regulations are to be introduced for a DeFi, it will be necessary to consider what portion of the DeFi participants should be protected.

6.3 Need for regulation for providers of financial functions

If a DeFi qualifies as a “financial service” and investors/consumers should be protected, then the application of financial regulations would need to be considered. Specifically, this would include the following elements.

(1) Safety and soundness regulation as a "financial institution"

When applying protection to a DeFi application, regulations to ensure the safety and soundness of regulation, similar to that of a traditional financial institution, need to be considered. Necessary regulations, such as capital adequacy regulations, entry regulations, restrictions on concentrated transactions, and transaction regulations would be on the agenda if, for example, deposit-like products were to be accepted. Risk management, such as that required of traditional financial institutions, may also be necessary. For example, operational risk, market risk management, and credit risk management are key examples.

(2) How to ensure appropriateness as a "financial transaction"

If transactions in a DeFi are regarded as financial transactions, then various transaction regulations would be required. The most typical regulation would be the market manipulation regulation when trading on the DEX.

(3) How to implement the audit and ensure DeFi's reliability?

Even if a disclosure mechanism for risk, governance, etc., of the code is established, the question then arises as to how to ensure its accuracy. In the normal course of business, listed companies are audited by an external auditing firm and are assured of a certain level of accuracy that investors can rely on. For corporate bonds, there are also rating agencies, such as Moody's and Standard & Poor's, that rate the credit of corporate bonds and provide information to investors. So, does the DeFi ecosystem have the capability to develop such a financial environment that guarantees credibility? Even if it does, how reliable are they?

Currently, it appears that there are indeed companies in the DeFi ecosystem that audit codes, but several issues have been raised. Conflux Network (2020) indicated that audit standards were not standardized, varying from firm to firm, and it was unclear how reliable they were. When a DeFi application is recognized as a "financial service" constituting a “financial system”, it will be necessary to develop an ecosystem that will ensure the reliability of such a financial system. However, the issue of how to tackle this issue will be raised, as it crosses national borders and the affiliation and jurisdiction are not clear.

(4) How to establish a regulatory enforcement framework?

First, DeFi is seen as difficult to enforce because there is no principal entity and therefore no entity for the authorities to order. However, as discussed above, in many cases, there are actual entities to be regulated. After all, some entities benefit economically, and it would be appropriate to consider them as the main operating entities. For this reason, it is necessary to take a close look at the actual governance and operating situation of the DeFi.

Perhaps, the most difficult question regarding DeFi is how these regulations and enforcement can be implemented, and by which authorities. Concerns have often been raised that, since some DeFi projects are further decentralized, there could be no explicit entity subject to regulation. And there may be a DeFi that claims not to belong to any country or jurisdiction. Several ideas have been suggested in this regard.

IMF (2021) mentioned that, although direct bans can have a direct impact on the business of crypto exchanges (for both centralized exchanges and Decentralized exchanges), individuals are still likely to be able to trade and exchange crypto-assets by alternative means. Thus, regulatory arbitrage could exist. Therefore, jurisdictions should actively coordinate with the relevant authorities and international standard-setting bodies to maximize the effectiveness of their enforcement actions and minimize regulatory arbitrage. Greater cross-border collaboration can enhance enforcement actions. Realistically, enhanced coordination of regulation and supervision would be the most that should be done.

There is a suggestion to use soft law, such as a corporate governance code, rather than enforceable regulation by law (OECD 2022). DeFi, which agrees with such soft law, would then sign the agreement, which would effectively function in a self-regulatory manner. Of course, while creating such normative standards and encouraging signatures may have a certain degree of effectiveness, bad actors may not follow these codes and may not sign them even in the first place. Therefore, it will be necessary to have certain authorities in the background of the standard. To this end, it is still essential for national authorities and international organizations to respond in a coordinated manner.

It will also be necessary to deepen research on the possibility that the subject of regulation will be "code (=computer program)," by referring to the recent thinking on

laws and regulations against market manipulation by AI (BOJ, 2018). In the financial markets, recently, there may be a situation where it is unclear who will be responsible for any losses incurred by investors due to algorithmic/AI based trading or trading that harms the fairness of the market. Market manipulation by AI is indeed a crime committed by computer programs, and it will be very helpful to see what measures can be taken against it.

More importantly, it will be important for regulators to develop a system, including human resources and flexible facilities, that will allow them to keep a close eye on areas such as DeFi. There is also a tendency for regulators to be too conservative, which makes it difficult for them to keep up with the application, utilizing cutting-edge technologies, such as DeFi. Regulators need to balance "innovation and efficiency" and "conservatism in security."

In addition, As Zetzsche (2021) points out, DeFi could also take a completely new way of thinking about regulatory design, such as an "embedded regulation" approach. The "embedded regulation" approach is to automate the regulation itself, which may be an efficient way to regulate cyberspace, such as DeFi, and may require further consideration in the future.

However, the question still remains. How should it be handled if it is truly decentralized, for example, the code is the operating entity. In this regard, the August 2022 Tornado Cash incident was highly controversial. On August 8, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash, a leading crypto asset mixing platform, for engaging in money laundering of over $7 billion in crypto assets[9]. Indeed, there is no doubt that money laundering itself is a serious crime, but it is not Tornado Cash that actually laundered the money, but the individual or group that used its mixing service (i.e., in this case, the North Korean money laundering group). Also, if that Mixing platform is computer code and has no governance authority whatsoever, the argument seems to be whether it is appropriate to impose sanctions or arrest the code developer[10]. Regarding the U.S. Treasury Department OFAC sanctions against Tornado Cash, some argue that OFAC sanctions against computer code exceed its legal authority and violate the Constitution (Coin Center, 2022). Moreover, *Coin Center, et al. v. Yellen et al.* pointed out that Tornado Cash did not actually provide a mixing service in that funds of users were not commingled; rather, it allowed for the deposit and withdrawal of digital assets under different, unlinkable addresses in a manner that provided the beneficial feature of privacy in an otherwise fully transparent system.The case is expected to be settled in a future court dispute.

[9] OFAC Press Releases (August 8, 2022), "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats"（https://home.treasury.gov/news/press-releases/jy0768）

[10] FIOD(Fiscal Information and Investigation Service, Netherland)（August 12, 2022）"Arrest of suspected developer of Tornado Cash"
（https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/）

Another controversial issue in the U.S. is the CFTC's administrative action against the Ooki DAO in September 2022[11]. The CFTC filed a lawsuit against a Decentralized Autonomous Organization (DAO) called "Ooki DAO," including those who held and voted for its governance tokens, for providing off-exchange digital asset transactions, registration violations, and non-compliance with the Bank Secrecy Act (BSA). The simple question arises as to whether the tort liability of the DAO should be considered to fall on the voters of the tokens and not on all holders of the tokens, or whether, in the case of a corporation, only the shareholders who exercise their voting rights should be held liable for the tortious acts.The main issue may be what to think about the CFTC approach of determining the liability of DAO token holders based on their participation in governance votes. In any case, the lawsuit (and the court decision based on it) is also considered to have broad implications for the crypto asset industry as a whole.

(5) How to establish a disclosure system suitable for DeFi and crypto assets

One of the most important frameworks for investor protection is the disclosure framework. Blockchain is inherently traceable, so while it is already disclosed to technically sophisticated participants, it is too technical and virtually invisible to the general public and investors, which is one reason why DeFi is considered non-transparent (Brummer, 2022). Ensuring a solid disclosure system will prevent the non-transparent situation that the DeFi has, and will allow investors to make appropriate decisions. Disclosure is considered necessary to a certain extent not only for investors but also for consumers, even if the product is an ordinary product. In this regard, it is essential for DeFi to provide more disclosure.

IMF (2021) and OECD (2022) also pointed out that establishing a disclosure framework including greater data standardization can lead to better oversight of crypto-asset markets, and in this regard, appropriate development of disclosure framework is a necessary measure.

Establishing the structure for how disclosure is to be made can be a very challenging task. Even for traditional financial and corporate entities, international harmonization of accounting standards is a challenging task. The DeFi disclosure system is not defined by one country alone, as it crosses national borders.

In this regard, Brummer (2022) points out that the DeFi disclosure is not suitable for the SEC's EDGAR framework, as used for regular corporate disclosure and institutional investors, and requires a different framework that is preferable for investors and developers of crypto-assets. In other words, the existing disclosure systems used in finance (e.g., EDGAR) are often too detailed and too burdensome for the DeFi system

[11] CFTC Press release,(September 22, 2022) "CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act"
（https://www.cftc.gov/PressRoom/PressReleases/8590-22）

to be suitable at all. Specifically, in terms of the DeFi disclosure requirements, participants should be aware of the issues including those listed below:

- ➢ token governance;
- ➢ conflicts of interest;
- ➢ economic mechanisms (additional issuance, redemption authority, splits, suspensions, etc.);
- ➢ token holder privileges;
- ➢ founder and VC influence;
- ➢ Dapp (Decentralized Applications) business model and risks;
- ➢ risks associated with external references (so-called, "Oracle risk");
- ➢ smart contract code upgrade and bug fixing mechanisms; and
- ➢ DAO (Decentralized Autonomous Organization) decision making and governance.

Above issues are essentially necessary and important information that DeFi participants need to understand, but these are rarely found in the traditional SEC regulatory forms. For this reason, it is desirable to design a new disclosure system aimed at taking advantage of the characteristics of crypto-assets and blockchain.

Establishing an appropriate disclosure framework, while challenging, is the most necessary thing to do in order to get the facts, and for investors to get accurate information as well. This is perhaps the issue that should be addressed most urgently. To create a common disclosure platform in which national authorities and international standard-setting bodies would also participate and give authority would be desirable to have a framework in which access to this disclosure platform would provide basic information regarding the DeFi, such as disclosure of data, governance mechanisms, token information, as well as information on audits, etc., and it is also a more convenient way to check for compliance. Designing an appropriate common disclosure platform that also considers players' incentive structure is very challenging and will be the subject of further research.

(6) Need to consider the impact on the financial system if the scale of DeFi becomes large

Currently, the scale (TVL: Total Value Locked) of the DeFi markets is not significantly compared to traditional financial markets. However, along with the growth of the DeFi markets, many financial institutions would be involved in DeFi in some way. This is because it is difficult to exclude them from the investment portfolios of institutional investors when the scale of the DeFi markets becomes large. In such cases, the impact of DeFi on the financial system should be considered. In particular, as pointed out in the previous chapter, given the evident procyclical nature of the DeFi system, if the DeFi market were to crash, the impact could spread at an accelerated rate and affect the financial system. Allen (2021) noted that, because DeFi still remains largely disconnected from both real-world economic applications and the established financial system, there would be limited pressure on the government to bail it out. However, as

DeFi grows, the possibilities for something to go wrong, and for that something to impact the broader economy, increases.

From a simple point of view, there are two possible ways. The first is to restrict investment in DeFi by financial institutions. In other words, the exposure to DeFi itself should be reduced. This will reduce the negative linkages. Second, some kind of soundness regulation (such as capital adequacy regulation) could be introduced to maintain the soundness of the DeFi system itself. However, since such soundness regulations are entity-based, it is questionable to what extent they will be suitable for DeFi, which is the subject of the computer program.

6.4 How to ensure AML/CFT

Whether or not DeFi is considered financial, and whether or not its participants deserve protection, at this time, the most urgent policy issue regarding DeFi would be the anti money laundering (AML). Regardless of the size of a DeFi, it should not be used to fund crime, and AML is an essential measure. To counter money laundering, KYC, such as identity verification, is necessary to be implemented into DeFi in some form. However, the issue is how to implement AML countermeasures for the DeFi, which is just an application program.

In this regard, The FATF (2021) states that items with significant regulatory uncertainty, such as DeFi and stablecoins, should also comply with the "travel rule." "Travel Rule" is a set of rules for domestic and international wire transfers to prevent money laundering, and requires Virtual Asset Service Providers (VASPs) to collect and exchange information on the sender and recipient of crypto-asset transactions. And in the FATF's view (FATF 2021), almost all DeFi platforms are VASPs. The FATF has warned regulators not to accept without question the crypto-asset industry's marketing technique of broadly calling various platforms "decentralized." This is because DeFi platforms usually have a natural person (maybe not a legal entity) somewhere who "controls or influences" their activities. The point of "control or influence" is the framework for analyzing who is obligated to comply with ALT/CFT regulations.

Addressing the problem of AML may also eliminate the anonymity and pseudonymity features of DeFi, i.e., the privacy of transactions. However, anonymity and pseudonymity make it difficult to maintain fairness in the market, not only for AML but also for market manipulation, as Crenshaw (2021) pointed out. Given that participants in traditional financial markets agree to share some degree of private information with relevant/competent authorities in exchange for maintaining market fairness, it will be necessary to take the necessary measures to maintain a level playing field. As BGIN (2021) also points out, this is a difficult matter and a number of participants expressed concerns about the AML regulations in terms of privacy, level playing fields, financial inclusion, and regulatory enforceability.

However, as will be mentioned below, the key issue is how to enforce AML as the decentralized organization of DeFi further develops. Some have suggested that AML itself be embedded in the code and executed automatically, which is AML Oracle (Coinfirm, 2021). AML Oracle is intended to enable AML through smart contracts, however, is in the early stage of the development and is not clear to what extent this will work practically at this moment.

7. Proposal of Principles of DeFi disclosure and regulation

Based on the risks and challenges seen in the previous chapters, some countries and jurisdictions are also considering regulations on DeFi[12].

For example, in Europe, a regulation on crypto assets called the "Markets in Crypto Assets regulation (MiCA)" is under consideration. However, it appears to focus on stablecoins and other crypt assets, not on DeFi (EU 2022, Coinfirm 2022). Japan was quick to address crypto asset regulation, starting in 2017, but the regulations seems to be relatively strict, because it lists which crypto assets can be traded by crypto asset providers. Other crypt assets, including those on DeFi, are not allowed to serve by those providers. In the U.S. even DeFi tokens are subject to SEC jurisdiction if they are securities, crypto asset futures are regulated by CFTC, but crypto assets in the spot market are not currently regulated. In any event, given that DeFi is characterized as a digital asset, there may be problems in applying similar regulations to DeFi tokens and securities because they are different. The regulation is currently under consideration in Congress (FSOC 2022, Coinfirm 2021). Some countries have banned crypto asset trading itself, hence there are no regulated trading markets in such jurisdictions. Thus, looking at the regulatory developments on DeFi in various countries and jurisdictions, many are currently unregulated, or if they are, they are inadequate. Therefore, it seems unavoidable that new regulations should be considered.

In doing so, in light of the points discussed so far, it would be desirable to establish the following principles for DeFi regulation and disclosure. The reason for the principle is that detailed laws and regulations are highly rigid and difficult to adapt to innovation and technological change, as well as taking a significant amount of time to enact and costing a significant amount of operational costs. Of course, this does not prevent rules and laws if they are enacted in a manner that allows them to adapt to change and operate in a manner that mitigates the disadvantages mentioned above. Several studies are also being conducted by the international organizations and regulators including IMF, FSB, FSOC, and others (see BOX 1-4 in this chapter for reference).

Please note that the following principles do not apply to crypto assets in general, but only to DeFi, which is the subject of this document. The following is a proposal (as of February 13, 2023), which will be refined based on further comments and opinions to finalize the document.

[12] See also the IMF (2022) for a detailed summary of this point.

(Principle 1) Need to establish the Scope of Coverage

(1) Regulators need to identify whether a DeFi constitutes a regulated financial activity and whether its participants fall under investor/consumer protection.

(2) The requirements for whether a DeFi constitutes a financial service should be presented in a form that is easy for participants to understand and appreciate.

(3) This coverage decision could also be considered to be made by the governing body of the globally uniform disclosure platform. once it is established, as described below.

(Principle 2) Establishment of a Disclosure Platform

(1) Disclosure of information on DeFi could be made in a form that is easily understood and grasped by participants in transactions through the establishment of a reliable platform and their voluntary participation in it, taking into account the differences from the disclosure in securities.

Disclosure information in such cases should include the following.

- Factors that have or may have a material impact on the value of the governance token, such as token governance,
    - Founder and venture capital (VC) influence,
    - conflicts of interest;
    - economic mechanisms (additional issuance, redemption authority, splits, suspensions, etc.);
    - token holder privileges;
    - Others
- Dapp (Decentralized Applications) business model,
- Others

(2) It is desirable to establish a globally uniform disclosure platform. The platform should be led by neutral organizations, such as multi-stakeholder organization, international standard-setting bodies, self-regulatory organizations, or international organizations. It is desirable to be approved by regulators in various countries/jurisdictions. Participating in the platform is desirable to have similar effects as registration to a regulator. This would provide an incentive to participate in a proper DeFi disclosure platform.

(3) This globally uniform disclosure platform will have the effect of providing a certain level of trust to trading participants, as only the DeFi that meet the principles will be allowed to participate. In contrast, a non-participating DeFi would also have the potential to have concerns about investor/consumer protection (Name and Shame).

(4) Disclosure platforms should aggregate, publish and provide data from participating DeFi platforms.

(Principle 3) Harmonization with Traditional Financial Regulations

If a DeFi's activity falls within the scope of financial regulatory coverage, the regulations and disclosure rules should be applied under the same risk, same activity, same regulatory outcome, and also under the principle of technology neutrality, considering the balance with normal traditional financial activities. For example, regulation in traditional finance could include:

- Safety and soundness regulation,
- Conflict of interest regulations (e.g., between exchanges and brokerage firms),
- Disclosure regulation (more details below),
- AML/CFT regulation (but this is not limited to financial activities)
- Others

(Principle 4) Consideration of DeFi specialities

Even if a DeFi's activity falls within the scope of financial regulatory coverage, DeFi specific regulations and disclosures should be considered, including the fact that it is a digital activity. Specifically, for example, the most significant differences between traditional finance and DeFi, even if they are the same activity, are the following.

- Electronic activities,
- The ability to easily conduct cross-border activities,
- the existence or non-existence of a central entity that can influence the activity,
- There are cases where there is no central entity at all,
- Even if a central entity does exist, the degree of its influence vary,.
- DeFi's specific risk called oracle risk,
- Automatic execution risk of smart contracts (a kind of operational risk),
- Cyber security,
- Others.

(Principle 5) Addressing the Potential for Systemic Risk

If the connectedness with traditional finance becomes greater, it will be necessary to consider how to deal with systemic risks, such as leverage ratios and capital adequacy ratios.

(Principle 6) Periodical Audit

DeFi participating in the disclosure platform must be subject to an audit at least once a year. A summary of the results should then be disclosed on the disclosure platform, clearly indicating that it is an appropriate DeFi.

It is desirable that a uniform auditing standard be created and that they be approved by the disclosure platform.

(Principle 7) Ensuring Regulatory Effectiveness

A DeFi may not have a central entity or may have a small degree of influence on its activities, and in such cases, conduct regulations that stop the illegal activity itself may be more effective than punishment against the entity to ensure the effectiveness of the regulations.

Since "decentralized" does not allow for the absence of a responsible entity in case of illegal activity, DeFi apps should include a mechanism for correcting or self-discontinuing the activity.

(Principle 8) AML/CFT and other measures to illegal financial activities

Even a DeFi that does not participate in the disclosure platform and is not regulated as financial services, it should comply with AML/CFT and other illegal financial measures as prescribed by FATF standards as they are developed to apply for DeFi.

(BOX 1) IMF's considerations for regulatory frameworks

IMF(2022) points out the following with respect to considerations for regulatory frameworks across crypto assets.

(1) Monitoring
Authorities should first monitor developments to accurately gauge the size of the market and to identify areas of risk,

(2) Prioritization
Authorities should consider the risks of unbacked crypto assets as part of their broader regulatory and supervisory duties and determine whether the crypto asset market presents risks to their mandate that would reflect the considerable resources required to regulate and supervise crypto assets.

(3) Scope
Authorities should determine a clear scope for regulation, that is, which entities, crypto assets, and activities will fall within the regulatory scope

(4) Domestic Collaboration
Regulatory development should be a collaborative effort of financial sector regulators and relevant government departments, taking into account guidance from standard-setting bodies and regulatory approaches in peer countries

(5) Continuous Assessment of Risks
Continuous assessment of risks will be needed to identify shifting risks and business models that may require updating regulations to ensure effective protection of markets, consumers, and financial stability

(BOX 2) FSB report

FSB(2022b, “Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultative document”) proposed 9 recommendations for the regulation, supervision and oversight of crypto-asset activities and markets. The summary of the proposals are below. (Excerpt from FSB, 2022b).

(Recommendation 1: Regulatory powers and tools)
Authorities should have the appropriate powers and tools, and adequate resources, to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers, as appropriate.

(Recommendation 2: General regulatory framework)
Authorities should apply effective regulation, supervision, and oversight to crypto-asset activities and markets – including crypto-asset issuers and service providers – proportionate to the financial stability risk they pose, or potentially pose, in line with the principle “same activity, same risk, same regulation.”

(Recommendation 3: Cross-border cooperation, coordination and information sharing Authorities)
Authorities should cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication, information sharing and consultation in order to support each other as appropriate in fulfilling their respective mandates and to encourage consistency of regulatory and supervisory outcomes.

(Recommendation 4: Governance)
Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place and disclose a comprehensive governance framework. The governance framework should be proportionate to their risk, size, complexity and systemic importance, and to the financial stability risk that may be posed by the activity or market in which the crypto-asset issuers and service providers are participating. It should provide for clear and direct lines of responsibility and accountability for the functions and activities they are conducting.

(Recommendation 5: Risk management)
Authorities, as appropriate, should require crypto-asset service providers to have an effective risk management framework that comprehensively addresses all material risks associated with their activities. The framework should be proportionate to their risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which they are participating. Authorities should, to the extent necessary to achieve regulatory outcomes comparable to those in traditional finance, require crypto-asset issuers to address the financial stability risk that may be posed by the activity or market in which they are participating.

(Recommendation 6: Data collection, recording and reporting)
Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place robust frameworks for collecting, storing, safeguarding, and the timely and accurate reporting of data, including relevant policies, procedures and infrastructures needed, in each case proportionate to their risk, size, complexity and systemic importance. Authorities should have access to the data as necessary and appropriate to fulfill their regulatory, supervisory and oversight mandates.

(Recommendation 7: Disclosures)
Authorities should require that crypto-asset issuers and service providers disclose to users and relevant stakeholders comprehensive, clear and transparent information regarding their operations, risk profiles and financial conditions, as well as the products they provide and activities they conduct.

(Recommendation 8: Addressing financial stability risks arising from interconnections and interdependencies)
Authorities should identify and monitor the relevant interconnections, both within the crypto-asset ecosystem, as well as between the crypto-asset ecosystem and the wider financial system. Authorities should address financial stability risks that arise from these interconnections and interdependencies.

(Recommendation 9: Comprehensive regulation of crypto-asset service providers with multiple functions)
Authorities should ensure that crypto-asset service providers that combine multiple functions and activities, for example crypto-asset trading platforms, are subject to regulation, supervision and oversight that comprehensively address the risks associated with individual functions as well as the risks arising from the combination of functions, including requirements to separate certain functions and activities, as appropriate.

(BOX 3) IOSCO report

IOSCO(2022), “Decentralized Finance Report” point out that financial innovation may lead to benefits for investors and others, but it may also present risks. Then it point out that DeFi appears to present many similar risks to investors, market integrity and financial stability as do other financial products and services, and it also poses specific and unique risks and challenges for regulators to consider. Potential regulatory concerns raised by IOSCO(2022) are below.

- Asymmetry and fraud risks
- Market integrity risks
    - Front-running (or similar frauds)
    - Flash loans
- Market dependencies
- Use of leverage
- Illicit activity risks
- Operational and technology-based risks (Blockchain, Smart Contracts, Oracles)
- Cybersecurity
- Nascent stage of development (Comprehensibility, Scalability, Supportability, Reliability)
- Governance risks
- Spill-over of risks to centralized/traditional markets
    - Centralized Crypto-asset Trading Platforms
    - Traditional Financial Institutions

(BOX 4) FSOC Recommendations

In the U.S., the FSOC (Financial Stability Oversight Council) suggests the following as recommendations for building regulations on cryptographic assets.(FSOC 2022)

(Recommendation 1)
Member agencies (Treasury department, SEC, OCC, FRB, FDIC, etc.) consider these general principles in their deliberations about the applicability of current authorities: Same activity, same risk, same regulatory outcome;

- Technological neutrality;
- Leveraging existing authorities where appropriate;
- Transparency in technology, including through potential future adoption and implementation of federal agency SBOM requirements by industry;
- Addressing financial stability risks before they impair the economy;
- Monitoring mechanisms through which crypto-assets could become more interconnected with the traditional financial system or increase in overall scale;
- Bringing transparency to opaque areas, including through disclosures and documentation of key issues such as interconnectedness;
- prioritizing timely and orderly transaction processing and legally binding settlement;
- facilitating price discovery and fostering market integrity; and • obtaining, and sharing with other agencies, relevant market data from the crypto-asset market

(Recommendation 2)
Continued Enforcements are needed.

(Recommendation 3)
Congress pass legislation that provides for explicit rulemaking authority for federal financial regulators over the spot market for crypto-assets that are not securities

(Recommendation 4)
Regulators continue to coordinate with each other in the supervision of crypto-asset entities, such as stablecoins issuers or crypto-asset platforms, particularly in cases where different entities with similar activities may be subject to different regulatory regimes or when no one regulator has visibility across all affiliates, subsidiaries, and service providers of an entity.

(Recommendation 5)
Congress pass legislation that would create a comprehensive federal prudential framework for stablecoin issuers that also addresses the associated market integrity, investor and consumer protection, and payment system risks, including for entities that perform services critical to the functioning of the stablecoin arrangement

(Recommendation 6)
Congress develop legislation that would create authority for regulators to have visibility into, and otherwise supervise, the activities of all of the affiliates and subsidiaries of crypto-asset entities, in cases in which regulators do not already possess such authority

(Recommendation 7)
FDIC, FRB, OCC, and state bank regulators use their existing authorities, as appropriate, to review services provided to banks by crypto-asset service providers and other entities in the crypto-asset arena

(Recommendation 8)
Member agencies assess the impact of vertical integration (i.e., direct access to markets by retail customers) on conflicts of interest and market volatility, and whether vertically integrated market structures can or should be accommodated under existing laws and regulations.

(Recommendation 9)
Coordinated government-wide approach to data and to the analysis, monitoring, supervision, and regulation of crypto-asset activities.

(Recommendation 10)
Council members continue to build their capacity to analyze and monitor crypto-asset activities and allocate sufficient resources to do so.

8. Conclusion

This paper summarizes the issues surrounding DeFi under these circumstances and presents some discussion points and suggestions for appropriate future regulatory considerations. We proposed principles for DeFi disclosure and regulation. In considering the Principles, there were three major considerations.

Firstly, applying a traditional regulatory strategy to a new technological ecosystem has proved conceptually difficult because there is a policy trilemma called an innovation trilemma for introducing regulation for innovative services and products.

Secondly, considering DeFi regulations, whether a DeFi constitutes the "financial service" which participants are subject to consumer/investor protection need to be considered first. Additionally, regulations from the perspective of systemic risk and anti-money laundering may be important regardless of such need for protection.

Lastly, the most important point would be to establish a disclosure system and common platform suitable for the characteristics of DeFi and crypto-assets, as well as an enforcement framework, considering the innovation trilemma. This is because establishing a suitable disclosure system for DeFi and crypto-assets is the most essential infrastructural foundation, when considering self-regulation, enforcement by government agencies, or for investors to pursue their own responsibilities. Establishing an appropriate disclosure framework is, while challenging, necessary to provide all market participants information about the potential risks and benefits for any particular DeFi applications. To create a common disclosure platform in which national authorities and international standard-setting bodies could also participate and give authority would be desirable. Such a framework would provide basic information regarding a DeFi, such as disclosure of data, governance mechanisms, token information, as well as information on audits, etc., and it is also a convenient way to check for compliance. Designing an appropriate common disclosure platform that also considers participants' incentive structure is very challenging and will be the subject of further research.

These principles will be desirable to be reviewed on a continuing basis, on a regular basis (e.g., every two years) in the future. It is then hoped that the recognition of this Principle will be shared by the participants involved in DeFi and contribute to the development of a healthy market. BGIN would also like to contribute to the healthy development of the DeFi market by communicating these views through gathering and coordinating stakeholder opinions.

Appendix A – Acknowledgement

(Informative)

A.1 Editors and Co-editors

- Tomonori Yuyama (Georgetown University) *
- Ken Katayama (Nomura Research Institute, Ltd.)
- Paul Brigner (Electric Coin, Co.)

*Corresponding editor

A.2 Contributors

- Tetsu Kurumizawa (Yale University)
- Michi Kakebayashi (UC Berkeley)
- Mitchell Travers (Partner, Soulbis Pty Ltd)
- Shinji Sato (Independent researcher)
- Stephanie Bazley (AirTree Ventures)
- Yuji Suga (IIJ)

(Note) The views expressed in this paper are based on the personal views of the authors and not the views of the organizations to which they belong.

Appendix B – Informative reference

(tentative as of 9.15.2022)

1. Allen, Hilary J., “Stablecoins: How Do They Work, How Are They Used, and What Are Their Risks?” Prepared Statement Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, December 14, 2021.
2. Armour, John, Daniel Awrey, Paul Lyndon Davies, Luca Enriques, Jeffrey Neil Gordon, Colin P. Mayer,Jennifer Payne, Principles of financial regulation. Oxford University Press, 2016. BOJ (Institute for Monetary and Economic Studies, Bank of Japan), "Use of Algorithms and AI in Investment Decision Making and Legal Liability (in Japanese)," 2018.
3. Auer, Raphael, Jon Frost and Jose Maria Vidal Pastor, “Miners as intermediaries: extractable value and market manipulation in crypto and DeFi”, *BIS Bulletin* No 58, 16 June 2022.
4. BIS (Bank of International Settlements) (Aramonte, Sirio, Wenqian Huang and Andreas Schrimpf), "DeFi risks and the decentralisation illusion." *BIS Quarterly Review* (2021):
5. BGIN (Blockchain Governance Initiative Network), "Present and Future of a Decentralized Financial System and the Associated Regulatory Considerations," BGIN SR 001, 2021.
6. BGIN (Blockchain Governance Initiative Network),”Soulbound Tokens (SBTs) -Building and Embracing a New Social Identity Layer,” BGIN SR 008, 2022 (Forthcoming).
7. Born, A., Gschossmann, I., Hodbod, A., Lambert, C. and Pellicani, A. (2022), “Decentralised finance – a new unregulated non-bank system?”, Macroprudential Bulletin, Issue 18, ECB, July.
8. Brummer, Chris, and Yesha Yadav. "Fintech and the innovation trilemma," *The Georgetown Law Journal* 107 (2018): 235.
9. Brummer, Chris. "Disclosure, Dapps and DeFi." *Stanford Journal of Blockchain Law and Policy* (Forthcoming) (2022).
10. Chen, Yan, and Cristiano Bellavitis. "Blockchain disruption and decentralized finance: The rise of decentralized business models." *Journal of Business Venturing Insights* 13 (2020): e00151.
11. Chainalysis, "The 2022 Crypto Crime Report," 2022a.
12. Chainalysis, "State of Web3 Report -Your guide to how blockchains are changing the internet “ 2022b.
13. Coin Center, ”Analysis: What is and what is not a sanctionable entity in the Tornado Cash case”, August 15, 2022 (https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case/.
14. *Coin Center, et al. v. Yellen et al.*, 3:2022cv20375 (N.D. Fla., October 12, 2022).

15. Coinfirm, Press release (March 24, 2021), "DeFi AMLT Oracle Integrates World's Most Secure Smart Contract Network RSK." (https://www.coinfirm.com/blog/defi-amlt-oracle-rsk/)(Last viewed on February 8, 2023)
16. Coinfirm,"USA cryptocurrency Regulations", 2021
17. Coinfirm,"MiCA: Markets in Crypto-Assets", 2022
18. Conflux Network, "State of DeFi Audits - Taking a look at the auditing space and its importance in onboarding users by properly securing new DeFi protocols -," Medium.com (Jun 24, 2020), (https://medium.com/conflux-network/the-overlooked-element-of-defi-adoption-e3b29829e3da) (Last viewed on February 8, 2023)
19. Crenshaw, Caroline A. (SEC Commissioner), " Statement on DeFi Risks, Regulations, and Opportunities," The United States Securities and Exchange Commission, 2021.
20. De Filippi, Primavera, Blockchain and the Law,Harvard University Press, 2018.
21. Elliptic, "DeFi: Risk, Regulation, and the Rise of DeCrime", 18 November, 2021 (https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime)
22. EU (Council of the European Union), "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)", 2022. https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf
23. FATF (The Financial Action Task Force), " Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, " FATF, Paris, 2021.
24. FSB (Financial Stability Board), "Decentralised financial technologies-Report on financial stability, regulatory and governance implications -," 2019.
25. FSB (Financial Stability Board), "Assessment of Risks to Financial Stability from Crypto-assets" 2022a.
26. FSB (Financial Stability Board), "Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets Consultative document", 2022b
27. FSOC (Financial Stability Oversight Council), "Report on Digital Asset Financial Stability Risks and Regulation Table" 2022.
28. Gandal, Neil,JT Hamrick, Tyler Moore,Tali Oberman, "Price manipulation in the Bitcoin ecosystem." *Journal of Monetary Economics* 95 (2018): 86-96.
29. Gensler Gary (SEC Chair), Remarks Before the Aspen Security Forum, The United States Securities and Exchange Commission, 2021.
30. Griffin, John M., and Amin Shams. "Is Bitcoin really untethered?." *The Journal of Finance* 75.4 (2020): 1913-1964.
31. IMF(International Monetary Fund), GFSR(Global Financial Stability Report),October 2021, Chapter 2 "The Crypto Ecosystem and Financial Stability Challenges"
32. IMF (Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto), "Regulating the Crypto Ecosystem - The Case of Unbacked Crypto Assets," FinTech Notes 2020/007, (2022).
33. IOSCO(International Organization of Securities Commissions), "IOSCO Decentralized Finance Report," 2022.

34. Lehar, Alfred, Christine A. Parlour, and Calgary Berkeley. "Systemic Fragility in Decentralized Markets." (2022), Paper scheduled at American Economic Association 2022.
35. NIST (National Institute of Standards and Technology) “Blockchain Technology Overview” NISTIR 8202, 2018.
36. OECD (Organization for Economic Co-operation and Development), "Why Decentralized Finance (DeFi) Matters and the Policy implications," 2022.
37. Pitch Book, "DeFi Primer: An overview of DeFi funding activity, concepts, and select protocols," 2021. Popescu, Andrei-Dragoş. "Decentralized finance (defi)–the lego of finance." Social Sciences and Education Research Review 7.1 (2020): 321-349.
38. PWG (President’s Working Group on Financial Markets), "Report on STABLECOINS," November 2021.
39. Schär, Fabian. "Decentralized finance: On blockchain-and smart contract-based financial markets." *FRB of St. Louis Review*, 2021.
40. Schueffel, Patrick. "DeFi: Decentralized Finance-An Introduction and Overview." *Journal of Innovation Management* 9.3 (2021): I-XI.
41. The World Bank, "The Global Findex database 2017," 2017.
42. Ushida, Ryosuke, and James Angel. "Regulatory Considerations on Centralized Aspects of DeFi Managed by DAOs." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2021.
43. Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized finance." *Journal of Financial Regulation* 6.2 (2020): 172-203.
44. WEF (World Economic Forum), "How decentralized finance will transform business financial services – especially for SMEs," July 19, 2021a.
45. WEF (World Economic Forum), "What is the Value Proposition of Stablecoins for Financial Inclusion,"Digital Currency Governance Consortium White Paper Series, November 2021b.
46. Weyl, E. Glen, Puja Ohlhaver, and Vitalik Buterin. "Decentralized Society: Finding Web3's Soul." Available at SSRN 4105763 (2022).