Regulatory Considerations on Centralized Aspects of DeFi managed by DAOs

Ryosuke Ushida[1] and James Angel[2]

[1]Georgetown University / Financial Services Agency Japan
[2]Georgetown Unviersity
{ru64,angelj}@georgetown.edu

Abstract. This paper focuses on the centralized governance mechanisms of decentralized finance (DeFi) projects managed by Distributed Autonomous Organizations (DAOs) and discuss regulatory considerations. Unlike highly decentralized ecosystems such as Bitcoin, the degree of decentralization varies among DeFi projects. Centralized aspects such as concentrated ownership of governance tokens and admin keys have significant implications on their governance. Concerns include decision-making concentration risk and poor alignment of interests among stakeholders. From a regulatory viewpoint, centralized aspects could make it easier for regulators to impose requirements and therefore increase compliance costs. This might drive the DeFi community to seek further decentralization to avoid regulatory burdens. We conclude that the DeFi ecosystem should learn from the experience of both Internet governance as a partially decentralized system and from traditional corporate governance.

Keywords: Blockchain, DeFi, DAO, Decentralized financial system, Corporate governance, Regulation, On-chain governance, Off-chain governance, and Governance token

1 Introduction

1.1 Background and terminology

Decentralized Finance (DeFi), which generally refers to a decentralized form of financial applications executed by smart contracts on a public blockchain, is proliferating from $660M in TVL (Total Value Locked) in early 2020 to $14.5B at the end of December 2020. A wide range of financial products is available without KYC (Know Your Customers), including crypto-asset exchange, lending, derivatives, insurance, and decentralized stablecoins. In 2019, the Financial Stability Board [2] defined decentralized financial technology as "Technologies that have the potential to reduce or eliminate the need for one or more intermediaries or centralised processes in the provision of financial services" and defined financial systems as "new financial system that decentralized financial technology could bring". On the other hand, there is no widely-accepted definition of DeFi and the word seems to be used arbitrarily for marketing and other purposes. In this

Term	Definition	Example	Reference
Decentralized financial technology	Technologies that have the potential to reduce or eliminate the need for one or more intermediaries or centralised processes in the provision of financial services	Blockchain, DLT	FSB (2019)
Decentralized financial System	New financial system that *decentralized financial technology* could bring	Bitcoin, Ethereum	FSB (2019)
DeFi	Financial application that could consists a part of *decentralized financial system*	Maker, Compound, Uniswap	Defined in this paper
Decentralized Autonomous Organization (DAO)	Organization that is run through rules encoded as computer programs called "smart contracts"	MakerDAO, KyberDAO, Aragon	Chohan (2017)

Fig. 1. Terminology

paper, we define DeFi as a "financial application that could consist of a part of a decentralized financial system". While underlying blockchain platforms such as Bitcoin and Ethereum could be categorized as DeFi in a broad sense, our analysis focuses on smart contract-based applications on such platforms. DeFi protocols are often developed and managed by so-called DAOs, Decentralized Autonomous Organizations. Although the DAO is also not strictly defined, we use Chohan's [15] definition: "an organization represented by rules encoded as a computer program that is transparent, controlled by the organization members and not influenced by a centralized entity." Typical DAOs include The DAO (2016), MakerDAO, and KyberDAO.

The degree of decentralization varies from one DeFi project to another, and many of them are quite centralized, especially in the bootstrapping stage. For example, specific individuals or groups have the authority to change the protocol or freeze locked assets. To mitigate the Single Point of Failure (SPoF) risk caused by dependence on such trusted parties, many communities are heading for bottom-up, decentralized governance by transferring management authority of the protocol to the DAO through on-chain voting. Given the incessant hack incidents and increasing attention from regulatory authorities, the sound development of governance of the entire ecosystem is indispensable if they look ahead to mass adoption beyond niche use cases.

1.2 Related Works

The governance issues of decentralized financial systems are attracting many researchers' attention. Some explore to build sound governance of decentralized financial systems in light of the Internet governance lessons. De Filippi and Wright [5] discuss the applicability of the four regulatory tools (i.e., Law, Market, Norm, and Architecture/Code) in cyberspace proposed by Lessig [9] to control activities in decentralized financial systems. Takanashi et al. [14] points

out the importance of developing an architecture/code that harmonizes with law/regulations, aligns with social norms, and is competitive in the market.

Another point of discussion is the comparison with corporate governance. Hacker [6] argues that complexity-induced uncertainty could be reduced, and stability and order could be strengthened by adapting a corporate governance framework to blockchain-based organizations. Blemus and Guegan [1] analyzes the opportunities and risks posed by tokenization and distributed ledger technology from the perspective of corporate governance. They raised issues related to the responsibility for decision-making by DAOs, which have no management team or board of directors and are determined by token holders without legal framework applicable to DAOs.

Corporate governance and Internet governance are very different in terms of the attributes of governance targets. Nabilou [10] argues that it is misleading to draw parallels between the highly decentralized governance of Bitcoin and corporate governance. On the other hand, Collomb and De Filippi [3] point out that "The DAO", the first DAO initiative that ended in hacking in 2016, was designed to mimic and improve on corporate governance, and the problems caused was rooted in the fact that The DAO was run like traditional corporations. Considering the centralized aspects of the current DeFi applications, an extensive analysis should be conducted from both Internet and corporate governance viewpoints with particular attention to the regulatory implications. However, the ecosystem is fast changing and there is no sufficient academic discussion on it.

1.3 Contributions

This paper has two contributions to the ongoing governance discussion about decentralized financial systems and DeFi. First, we identify and discuss key factors that affects the governance of individual DeFi project managed by DAO and the DeFi ecosystem based on the existing works related to Internet and corporate governance. An emphasis is placed on the difference between decentralized finance with and without DAO and how the centralized aspect of incorporating DAO could affect the governance mechanism of the overall system. Second, we discuss regulatory considerations on the centralized elements of the ongoing DeFi projects/ecosystem for regulators and policymakers to develop a better regulatory framework for its sustainable development.

2 Governance of DeFi managed by DAO

This chapter elaborates on factors affecting the governance of individual DeFi projects, followed by the analysis of ecosystem governance. We stress the importance of understanding dynamic interactions among individual DeFi and the ecosystem at large. In many DeFi projects, relevant protocols are often managed by DAOs, with the community voting on critical decisions such as parameter changes and emergency response. In assessing the governance of the DAO-centered systems, it is vital to consider the direct participants in the project and

the interrelationships among a wide range of relevant stakeholders in the whole DeFi ecosystem.

2.1 Corporate and Internet governance as dual reference points

Overall DeFi ecosystem is a complex structure composed of several elements and stakeholders, including:

- Individual DeFi projects managed by DAOs
- A public blockchain, including scaling solutions, as an underlying platform
- DeFi integrators such as oracle providers and custody solution providers
- DeFi aggregators and curators
- DAO software as a service such as Aragon DAO and OpenLaw
- Centralized financial service providers such as centralized exchanges
- Multiple DeFi ecosystems (i.e., Ethereum, EOS, Polkadot, etc.)

Several researchers indicate the usefulness of analyzing the DAO-based decentralized financial systems from corporate governance perspective. Among others, Hacker [6] argues that token-based venture capital often looks more like companies with principals (i.e., investors) and agents (i.e., managers) than open-source networks. He also mentions that many for-profit token applications share many characteristics with corporations and investment funds, rather than open-source networks. He also observes that token issuance could serve as an alternative way to funding entrepreneurial projects. Also, Kondova and Barba [8] pinpoints that OECD principles [11] on disclosure and transparency and DAO governance share similarities in the decision-making process. In a highly decentralized system such as Bitcoin, corporate governance, which assumes a centralized organization and typically discusses the principal-agency problems and the separation of ownership and management, may not necessarily be applicable. However, there could be a good applicability to the ongoing DeFi projects, which have multiple centralized aspects. In addition, to assess the significance of the factors as means of control in the "apparently" decentralized system, we discuss from the viewpoints of law, market, norm, and architecture presented by Lessig [9] as four regulatory tools in cyberspace and extended by De Filippi and Wright [5] and Takanashi et al. [14] to apply the framework in the decentralized financial system.

2.2 Individual DeFi project governance

A DeFi project typically consists of protocols (i.e., single or a set of smart contracts on the underlying public blockchain), foundation/developer team, initial investors, token holders, and a variety of types of users such as liquidity providers, lenders and borrowers. There is no "one-size-fits-all" solution as each DeFi project varies greatly in many ways such as decision-making mechanism, protocol upgradability, attributes of tokens and types of financial applications. A couple of factors likely influence the governance of many DeFi projects with DAOs. In this section, we elaborate on governance factors that would constrain the activities in the projects to discuss the regulatory implications in the following chapter.

2.2.1 On-chain voting by governance token holders

In order to promote decentralized decision-making, more and more projects are adopting token-based governance. This community-driven bottom-up, decentralized mechanism could eliminate or mitigate the concentration risk of control by certain parties such as the developer team. Tokens can be designed in a variety of ways. Some tokens have not only voting rights and rights to create and submit proposals, but also the rights to receive a portion of the cash flow generated by the protocol. Some can be also used for specific purposes as utility tokens. In this paper, we define a governance token as a token that has a voting right for decision-making which influences the project, regardless of whether it has other rights/functions or not. Hacker [6] argues that token-based systems provide a clear designation of competences and procedures that breaks up the informal power structures and presents an opportunity to distribute power in a fairer and more transparent way. However, in "The DAO" case, the SEC [13] points out the limited influence of the token holders in decision making. While a "DAO Token" holder was given certain voting rights and ownership rights, the Curators, a group of individuals selected by The DAO's developer and a German company "Slock.it", have broad discretion in making investment proposals. Besides, proposals by token holders had to be reviewed by the the Curators before they were voted on. As such, the structure was significantly centralized in favor of the Curators and Slock.it. Token-based voting is just a part of the decision-making process in the existing DeFi projects, and its authority can be restrictive depending on the token design and governance process. Regarding the viewpoint of architecture/code, token holders' degree of control largely depends on the upgradability of the deployed smart contracts.

The distribution of governance tokens is another important issue in assessing the influence of minority token holders on decision making. Governance tokens are distributed in a variety of ways. Some tokens, such as Maker's MKR, are distributed by a specific party, such as a foundation, to early investors and adopters in the form of private sales. Others, such as Compound's COMP[1] and Uniswap's UNI[2], are distributed as rewards or compensations for locking up a certain amount of crypto-assets into a relevant smart contract, which is generally called "liquidity mining". In the case of Uniswap, about 18% is distributed to investors, 21.2% to team members and future employees, 0.7% to team advisors, and the remaining 60% to community members such as liquidity providers over a four-year period. It should be noted that the timing, methods of distribution and distribution ratio are arbitrarily decided by a specific entity in many projects and a large number of voting rights are often granted to particular groups or individuals, the implication of which will be discussed in detail in the following chapter. This is not unlike the super-voting shares often retained by the founders of companies.

[1] https://medium.com/compound-finance/expanding-compound-governance-ce13fcd4fe36

[2] https://uniswap.org/blog/uni/

In terms of the effectiveness and validity of decision-making, the turn-out ratio is an important metric to assess whether token-based voting functions appropriately. Blemus and Gregan argues that decentralized governance is based on the idea of a flat hierarchy, with token holders devoting sufficient time to participate and vote in the community's best interests. In this regard, many DeFi projects are struggling to attract adequate attention from token holders. In the case of the MakerDAO, only 32 voters participated in the emergency voting following the liquidation failure in March 2020, and one address accounted for more than 50% of the total votes. Mechanisms to increase the participation ratio include delegation mechanisms, quadratic voting, and improved UX/UI. Further analysis and experimentation are required to justify the token-based voting system as an appropriate decision-making process for sustainable community development.

From the market mechanism perspective, governance token holders are incentivized to act to maximize their economic benefits. They generally benefit from the capital gain (i.e., appreciation of the token values in the secondary market) and income gain (e.g., distribution from the trading fees generated by the protocol). One concern is that they might prioritize their short-term interests and ruin the long-term development of the project. This is more likely if they have substantial control over the protocol and it is easy to exit by selling the token. For example, some token holders might vote for burning vast amounts of governance tokens and/or increase the distribution ratio of the generated incomes to the stakeholders without engaging in the discussion about long-term strategy. They would expect to benefit from an increase in the token value in the short term while they sell the tokens before deterioration. As Hirschman [7] argues, the easier exit is, the less likely "voice", or voting right, will be used.

2.2.2 Code is law / Governance minimization

Blockchain and smart contract code is written in a formalized language and, unlike law and regulations that leave room for discretion, only actions that follow the rules set in the code are allowed. When the code is adopted as the primary constraint tool, little changes are made to the blockchain protocol except for technical maintenance. The ecosystem is built by relying solely on the original code to minimize human intervention via an on-chain or off-chain governance process. As mentioned in the previous section, the institutionalization of a specific governance process has the risk that the ecosystem could be captured by certain groups such as governance token holders. The ecosystem could be damaged by token holders' behavior that does not align with the incentive of others. In this regard, relying solely on the code could assure certain neutrality that mitigates the risks of SPoFs of specific entities. In a community with a norm that values this neutrality, a code-centric ecosystem will be created, and De Filippi and Loveluck [4] discuss that many in the blockchain community tend to believe that individuals and organizations cannot be trusted and social interactions should be managed solely by computer code.

On the other hand, as De Filippi et al. points out, a formalized rule is easily gamed or exploited by malicious actors. Computer code lacks the flexibility needed to respond to edge cases, such as hacking due to bugs or vulnerabilities in the code, or to comply with incessantly changing regulatory requirements. Zamfir [16], one of Ethereum's core developers, claims that the concept of governance minimization is based on a naive interpretation of how the code interacts with the existing legal system and stands by off-chain governance to intervene to resolve disputes. While computer code is certainly one of the powerful constraints, it is important to position it appropriately in interactions with other constraints such as law and social norms.

2.2.3 Off-chain consensus by community

In the case of the Bitcoin ecosystem, Nabilou [10] describes that "various actors such as mining pools, node operators, users, developers, exchanges, custodians and wallet providers, and eventually the media and advocacy groups have their say and they ultimately decide over critical governance issues either by reaching a consensus or by forking". While some researchers like Nabilou acclaim that their existing governance arrangements have been largely successful in dealing with Bitcoin's major crises, others including Hacker [6] criticize the lack of proper governance mechanism, especially for protocol update for dispute resolution by pointing out that, as an example, the Github repository is maintained by a small group of developers and unpredictability in changes to the protocol result from the lack of an institutionalized process to accommodate dissent from a wide range of stakeholders. The Etherum community, which also does not have a formal governance process such as an on-chain voting mechanism, resorted to an off-chain consensus when they decided to undo the mess caused by "The DAO" hack via a controversial hard fork. Many researchers question the transparency of the undocumented decision-making process and the validity of the judgment. Conversely, Zamfir [16]is opposed to excessively institutionalized governance such as on-chain voting as it could force the community to choose what is against the social norm of the community captured by specific governing forces such as governments, corporates or cartel of specific groups of the community. It is worth noting that law and its potential enforcement could primarily affect the community's decision against the rule of code, as some of the community members would notice the increased attention from authorities.

Off-chain governance mechanisms are put in place even in DeFi projects incorporating token voting systems. The community usually spends quite some time discussing before proceeding to the formal on-chain voting process on their discussion fora such as Discord and website managed by foundation or developer team. Furthermore, some DeFi projects such as MakerDAO have implemented the ability to upgrade the protocol in emergencies without going through the possibly time-consuming voting processes[3]. What needs to be considered in design-

[3] Maker has a dark fix mechanism for handling critical vulnerabilities in the protocol where the trust to its specialist team is required, which has

ing governance mechanisms is to strike a better balance between transparency and security that fits the project's long-term goal in considering the distinct benefits and risks that on-chain/off-chain governance could bring.

2.2.4 Legal compliance/avoidance

One of the differentiating factors among DeFi projects could be the willingness of the community to comply or circumvent the existing legal framework applied to financial services in each jurisdiction. At present, it seems that the primary value proposition of many DeFi is not complying with regulatory requirements such as KYC/AML (Know Your Customer/Anti Money Laundering rules). This purportedly "democratizes" the financial services for financial inclusion while protecting users from the threat of government actions such as taxation and expropriation. In light of growing concerns and scrutiny from regulatory authorities, some of the DeFi projects might choose to further decentralize the project by, for example, dispersing the governance token ownership, anonymizing the developer and community members, or voiding administrative functions to lessen the control points that could be captured by regulators[4].

On the contrary, others might choose to closely work with regulators and other stakeholders outside of the blockchain ecosystem to ensure legal certainty. For that sake, whether or not it should be called "DeFi", they could choose to increase the centralized aspects of the DeFi project to be able to meet regulatory requirements in an effective manner as traditional organizations usually do. One example is Nexus Mutual, a P2P discretionary mutual on Ethereum offering a blockchain-based solution to cover against smart contract failure such as "The DAO" hack. It was established as a company limited in the UK and has received approval by the Financial Conduct Authority. KYC/AML requirements must be fulfilled to become a member of the community and the membership gives legal rights to the assets of the mutual. Residents in some jurisdictions are not able to become a member due to relevant local regulations[5]. Another eye-catching initiative is OpenLaw's LAO, a Limited Liability Autonomous Organization that enables its members to invest in Ethereum ventures projects and generate a profit in a legally compliant manner[6]. The LAO is an LLC (Limited Liability Company) set up in Delaware and it harnesses smart contracts to handle mechanics related to voting, funding, and allocation of collected funds. It intends to ensure legal certainty, limit the members' liability, and streamline complex tax issues. Similar example is the Flamingo, an NFT (Non fungible token)-focused DAO organized

---

never happened as of the end of 2021 [Source: Presentation at BGIN https://www.youtube.com/watch?v=cD717AuLLJo]

[4] SEC charged the founder of EtherDelta with operating an unregistered exchange in November 2018. SEC points out the concentration of power to the founder exampled by his exclusive access to the private key for the "administrator account".

[5] https://nexusmutual.gitbook.io/docs/welcome/use-cases

[6] https://medium.com/openlawofficial/the-lao-a-for-profit-limited-liability-autonomous-organization-9eae89c9669c

as a Delaware LLC that aims to explore emerging investment opportunities for ownable, blockchain-based assets.

In general, there exists a trade-off between regulatory compliance and openness of the project. In the case of the LAO, the maximum number of members is limited to 99, the minimum investment is 120 ETH, and the membership is limited to 9% or for 1,080 ETH. The Flamingo also limits its membership to accredited investors capped at a maximum of 100. Such limitations could curve some of the key value propositions of DeFi, such as composability upheld by its permissionless nature, while paving the way to mass adoption in complying with social requirements. It should be noted that they might need to meet not only securities regulation but also other regulatory requirements regarding AML/KYC and financial stability, which could further increase compliance costs.

2.3 Ecosystem governance

Hacker [6] pinpoints that governance is generally recognized as a system that forms coordination between different actors. The BCBS [12] stated that the "primary objective of corporate governance for banks should be safeguarding stakeholders' interest in conformity with public interest on a sustainable basis, and shareholders' interest would be secondary to depositors' interest." Considering that complex financial products are being offered by DeFi protocols interacting with each other, regardless of the degree of decentralization, it is necessary to take into account the inter-relationships with diverse, relevant stakeholders to align what the DeFi ecosystem would achieve with public interests. In the following, we analyze the interactions with stakeholders that are considered to be particularly important in evaluating the ecosystem governance.

2.3.1 Interdependent DeFi protocols

The DeFi ecosystem is often described as "money Legos" for its philosophical nature of composability, enabling a DeFi protocol to interact with other smart contracts deployed on the same or interoperable blockchain without any permissions or contracts. For instance, a DEX aggregator 1inch.exchange[7] offers the best exchange rate by discovering the efficient swapping routes across a bunch of DEXs on Ethereum, such as Uniswap and Aave. While the open and flexible nature would be competitive advantages against traditional financial services, inadequate security considerations result in a number of hacking incidents, as shown in the previous chapter. A quintessential example is the hack against a decentralized lending and margin lending platform bZx in February 2020. The attacker exploited its collateral pool by taking advantage of so-called flash loans, a technique that combines a complicated set of actions including lending, pooling and selling of tokens in just a single transaction. The hacker used dydx, Compound, Uniswap and Kyber network protocols in the first attack and stole

[7] https://1inch-exchange.medium.com/

$350,000 followed by the $600,000 loss in the second attack after bZx's team updated its protocol using their admin keys after the initial attack[8]. The loss was compensated as the community happened to have enough resources for compensation, but the ecosystem should make clear who is responsible for what with legal certainties to brace for future incidents and dispute resolutions among DeFi projects and other stakeholders. In a simplified on-chain voting system, the opinions of different stakeholders are not reflected in the decision-making process, and there is a risk of decisions being made that are biased towards the interests of token holders. From the banking governance point of view, as BCBS [12] points out, what matters is having the right level of authority, responsibility, accountability, checks and balances among stakeholders. At present, there seems no agreement among stakeholders for the division of responsibilities and no mechanism is put in place to align the interests among stakeholders and fulfill obligations to the outside world. The way of making clear the responsibilities could be a smart contract-based agreement between protocols utilizing the tools such as OpenLaw, which creates and executes legal agreements on blockchain[9].

2.3.2 Underlying blockchain layer

When DeFi protocols are deployed on a blockchain, the security, scalability, native tokens, and governance of the infrastructure layer have a critical impact on the DeFi projects in respective ways. The expansion of the DeFi ecosystem frequently drives Gas prices due to the lack of scalability of Ethereum, and the high volatility of ETH often leads to collateral shortfall and liquidation failures.[10] Conversely, a single DeFi project could significantly affect the underlying layer as The DAO hack ended up in a hard fork of Ethereum to undo the fraudulent transactions. While a tremendous amount of effort is poured into addressing the scalability issues such as 2nd layer solutions and Sharding, the outcomes remain to be seen. Security and governance considerations need to be thoroughly discussed to mitigate the risks that could emerge from the resulting consequences, such as the migration of DeFi projects to the alternative layer. Some governance arrangements should be in place to fill the potential gaps between the blockchain and application layers, examples of which include having regular calls among core developers, working together to build a solution in critical need for the ecosystem such as digital identity, and sharing common financial resources to align the interest of each party.

2.3.3 Existing financial system

The border between the DeFi and centralized finance is likely to become vague

[8] https://blog.coinbase.com/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in-1289f7f77137

[9] https://media.consensys.net/introducing-openlaw-7a2ea410138b

[10] https://blog.makerdao.com/the-market-collapse-of-march-12-2020-how-it-impacted-makerdao/

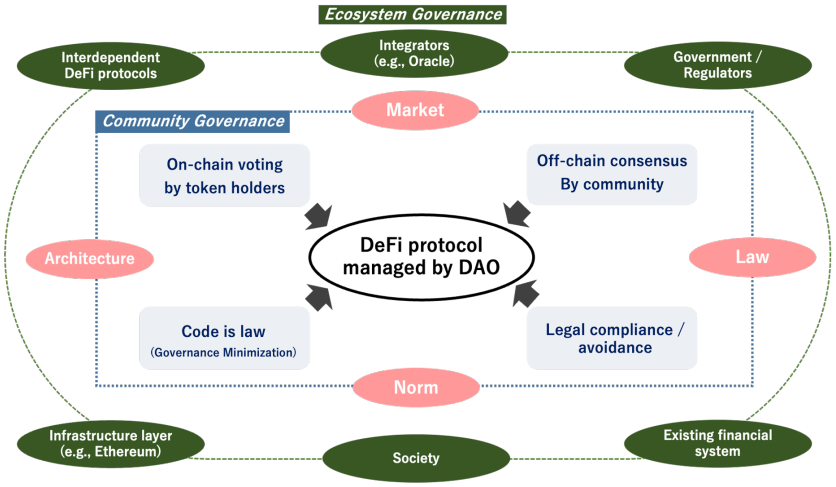

Fig. 2. DeFi governance overview

going forward. It is demonstrated by the fact that centralized exchanges such as Binance and FTX are active to list a wide range of DeFi tokens, including governance tokens, and by the re-centralization of some DeFi projects described in paragraph 2.2.4. An example of the DeFi and centralized finance interaction is Set Protocol, which automatically rebalances the tokenized assets based on customizable algorithmic strategy by tapping liquidity of almost anywhere, including DEXs and centralized exchanges and crypto OTC trading desks. Some governance arrangement should be established between the parties. The division of responsibilities between the decentralized and centralized organizations via smart contract agreement might benefit both if the division of roles fit for each economic purpose and legal requirements are adequately satisfied.

2.3.4 Other governance factors

In addition to the above, there exist several factors that should be considered in ecosystem governance. One of the most decisive factors is the governments and regulators, which will be discussed in detail in the next chapter. Besides, oracle governance is critical as many DeFi protocols rely on it as a price feeder. Furthermore, a variety of types of integrators and aggregators such as wallet providers, DEX aggregators also play an important role in this ecosystem. Digging deeper into these issues is an important research topic for the future.

3 Regulatory considerations on centralized aspects

In this chapter, we demonstrate the multifaceted centralized aspects of the DeFi projects analyze regulatory implications on them.

3.1 Admin keys

Some DeFi projects have a specific party with administrative authorities to modify the protocol by its discretion via private keys called admin keys. The existence of such centralized functions might be accepted by its community members in its bootstrapping stage as it could help facilitate the growth of the community through swift and justifiable updates by the administrators who are strongly committed to the project, such as the initial developer team. Indeed, we saw cases, such as Compound, which issued governance tokens to transfer the authority from admin key holders to token holders as the community grows. On the other hand, some protocols do not have admin keys from the beginning, such as Maker and Uniswap. Taking as an example of the bZx hack discussed in 2.2.1, it could be argued that the bZx developer team was able to fix the bug in a relatively timely manner because they had an admin key. As such, it is not necessarily a bad thing to hold an admin key. However, many projects make only ambiguous statements about the existence and management of such private keys, and even those who claim to be managing them properly have no verification at all. These custody risks are difficult to verify even with external audits, and participants of the ecosystem need to trust the key holders. It would be necessary to follow the security management standards such as ISO/TR 23576 from the operational security perspective. The administrators should strive for appropriate lifecycle management of private keys and transparent information disclosure. In addition, it should be pointed out that the admin key may act as a backdoor and threaten the security of the entire system.

3.1.1 Regulatory considerations

The admin keys and their holders could be one of the control points for regulators as Takanashi et al. [14] argues that backdoor "could facilitate nearly perfect oversight from the government within the network". SEC [13] refers to the fact that eleven "high profile" individuals are selected "as holders of The DAO's Curator "Multisig" (or "private key")" in its investigation report. The EtherDelta examined in 2.1.4 is another proof that regulatory bodies take the admin keys seriously to assess whether the developer is liable for the unlawful financial service provision via smart contracts. If regulators are able to identify the admin key holders, the regulators might ask them to take necessary actions such as freezing of stolen tokens in case of theft or money laundering. As an example, when crypto assets were stolen from the hot wallet of a centralized exchange KuCoin, some ERC-20 token issuers such as USDT and Ocean (government tokens) restricted token movement by administrator's judgement. Though it is not clear whether there was an order or request from the authorities, it is conceivable that the authorities will take similar enforcement actions against future incidents. Moreover, depending on the type of financial product offered, authorities might require the admin key holders to comply with same regulations that existing financial institutions providing comparable services are required to abide by.

Taking a step further, the authorities may decide that uncontrollable projects are unacceptable in order to achieve their regulatory objectives and demand that the adoption of admin keys be required at the launch of the protocol despite the effectiveness of its enforceability. In the early 1990s, the United States National Security Agency (NSA) intended to force telecom companies to adopt a chipset with a backdoor called the Clipper chip so that law enforcement authorities could decode the intercepted voice and data transmissions. The attempt failed due to strong opposition from cryptographers and related groups, but it should be kept in mind that some authorities could have a strong motivation to have control over the protocol, as exemplified by the recent discussion on restricting end-to-end encryption. Since the admin key encompasses issues such as custody risk, as pointed out in the previous paragraph, both developers and authorities should at least conduct in-depth risk assessment analysis before making critical decisions.

3.2 Governance token holders

Blemus and Gregan [1] argue that one of the purposes of distributed governance is to minimize the risk of "tyranny of the majority". However, regarding the degree of concentration of decision-making, governance tokens could work towards increasing the concentration of control over the protocols. Observing the DeFi ecosystem, in many projects, the majority of the governance token is held by the developer team or early investors such as venture capital. For example, 40% of Uniswap's UNI is going to distribute to the inner members such as initial investors and developers, as seen in 2.1.1. Community members usually receive the token via retrospective distribution or as a reward for adding liquidity to the protocol pool. Still, many holders only hold a minority portion of the stake and play only a limited role in governance voting. As a result, large token holders occupy a dominant position in decision-making. It should also be noted that voting rights are often concentrated in specific holders through delegation function.

3.2.1 Regulatory considerations

One of the major regulatory issues is the applicability of governance tokens as securities. While the holders of some governance tokens are entitled to receive a part of the fee income generated by the protocol, others have only voting rights and do not have the right to the treasury of the protocol directly. However, in many protocols, a portion of the tokens is burned as the cash flow to the protocol increases, which is equivalent to a share buyback in the case of ordinary stocks, and can be considered to have the same economic function as dividend. Collomb et al. argue that regulators should assess not only the original nature or function of the tokens being issued but also the underlying motivations of both token issuers and investors, as well as the risks that investors may incur in purchasing these tokens. Given the assumptions that token holders' primary motivation is capital and income gains that would be realized from the growth of the DeFi projects, it is conceivable that some of them are regarded as a kind of securities or

investment contracts, especially for those that have specific centralized party to manage the protocol, though it needs to be examined in the context of the legal framework of relevant jurisdictions. As an example, the SEC [13] has concluded that The DAO token was a security at the time of the issuance, and charged Ripple Labs Inc. and two of its executives alleging that they raised over $1.3 billion through an unregistered, ongoing digital asset securities offering[11].

Given the similarity of the governance tokens to securities, disclosure requirements should be well considered, particularly for the minor token holder protection. In corporate governance, many jurisdictions have put various institutional frameworks in place, such as a requirement to submit statements of large-volume holdings, to mitigate the dominance by large investor regulation to protect minority shareholders' interest. While such regulatory frameworks are not in place as of now, some projects such as Nexus Mutua implement specific voting rules to curve the strong voting power of large holders by, as an example, limiting the maximum voting rights to 5% of the total voting rights. However, this kind of arrangement could also raise concerns about fairness among shareholders.

Another consideration is concerning the possibility of token-based voting mechanisms being captured by authorities. It is conceivable that the authorities could hold a large number of tokens and intervene in the DeFi community's decision-making.

3.3 Other centralized factors

3.3.1 Collateral

Even if the DeFi protocol itself is highly decentralized, there are cases where assets accepted as collateral or locked in its pools are managed in a centralized manner. Maker community decided to add the USDC, custodial stablecoins backed by US dollars, as one of the collateral assets in March 2020 to increase the pool's liquidity after the liquidation failure incidents[12]. As a US corporation, Circle manages the USDC. Enforcement officials may demand the company to freeze the USDC used as a collateral of Dai, a stablecoin issued by Maker protocol, to stop illegal financial transactions. Also, if the Maker community could intervene in the decision via on-chain voting, the voters against the request from authorities could have legal responsibilities. If there is no generally agreed extent of liability of voters, the token holders might choose not to join the voting to avoid getting involved into the complicated situation.

3.3.2 Aggregator

The need for aggregation services is growing as the DeFi ecosystem expands. DEX aggregators enable users to access multiple liquidity pools and offer the best trading price as explained in 2.3.1. Yearn Finance provides lending aggregation by which interest accrual process is optimized by shifting deposited funds

[11] https://www.sec.gov/news/press-release/2020-338
[12] https://forum.makerdao.com/t/proposal-for-collateral-onboarding-of-usdc/1588

automatically between lending pools such as Compound and AAVE. Yearn Finance also helps users to maximize their profit making via liquidity mining or yield firming. Whereas aggregators are yet another protocol like many other DeFi protocols and often do not custody the user's assets, it could be a point of centralization when a lot of users rely on the aggregation services and access the user-friendly front interface. The operators of the website might be deemed liable if it is evident that illegal activities are facilitated by the aggregation protocols.

3.3.3 Legal entity

Chohan [15] discusses the legal indeterminacy of DAO and raises concern about the unlimited liability of the DAO participants if it is structured in the form of a general partnership as opposed to a corporation. As discussed in 2.2.4, legal arrangements lower the risks to investors in starting a business by making the investors have limited liability. Note that this freedom from liability is not affected by how shareholders vote. In addition, legal entity would be necessary to manage intellectual property rights of the community and to deal with jurisdictional-wise issues such as tax issues.

4 Conclusion and future works

There is no need to reinvent the wheel of governance. Whether it is Internet governance or corporate governance, useful mechanisms should be adopted in the DeFi ecosystem. Given the different degrees of decentralization of ongoing projects, the hybrid approach might hit the target. However, it is worth mentioning that it does not mean that we should ignore the existing governance arrangements already in place in the community. It should be also noted that the DeFi ecosystem is rapidly changing and each project seems to be exploring various directions toward further decentralization or re-centralization, which would affects the enforceability of regulation. This would make it much more difficult for regulators to properly assess the risk and implement tailored, risk-based regulatory approaches. Whereas this paper provides an overview of the governance mechanism and regulatory implications, an in-depth analysis should be done in consideration of complicated elements such as jurisdictional regulatory gaps and privacy-enhancing technologies. Besides, salient features of DeFi such as transparency should be examined from corporate governance point of view. It is also necessary to delve into the governance of organizations that are more similar to DAO, such as cooperative financial institutions. Since there is a wide range of issues to be discussed and solved, which neither the DeFi ecosystem participants nor the authorities alone could not sufficiently address, a multi-stakeholder approach should be taken to pave the way for the wider application of innovative financial products for social goods.

References

1. Stèphane Blemus and Dominique Guegan. Initial crypto-asset offerings (icos), tokenization and corporate governance. 01 2019.
2. Financial Stability Board. Decentralised financial technologies: Report on financial stability, regulatory and governance implications. https://www.fsb.org/wp-content/uploads/P060619.pdf, 2019.
3. Alexis COLLOMB, Primavera DE FILIPPI, and Klara SOK. Blockchain technology and financial regulation: A risk-based approach to the regulation of icos. *European Journal of Risk Regulation*, 10(2):263–314, 2019.
4. Primavera De Filippi and Benjamin Loveluck. The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure. *Internet Policy Review*, 5, 09 2016.
5. Primavera De Filippi and Aaron Wright. Blockchain and the law: The rule of code. *Harvard University Press*, 2018.
6. Philipp Hacker. Corporate governance for complex cryptocurrencies? a framework for stability and decision making in blockchain-based organizations. *Oxford University Press*, pages 140–166, 11 2017.
7. Albert O. Hirschman. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*. 1972.
8. Galia Kondova and Renato Barba. Governance of decentralized autonomous organizations. *Journal of Modern Accounting and Auditing*, 15:406–411, 04 2019.
9. Lawrence Lessig. Code and other laws of cyberspace. *Basic Books*, 1999.
10. Hossein Nabilou. Bitcoin governance as a decentralized financial market infrastructure. 04 2020.
11. OECD. *G20/OECD Principles of Corporate Governance*. 2015.
12. Basel Committee on Banking Supervision. Corporate governance principles for banks. https://www.bis.org/bcbs/publ/d328.pdf, 2015.
13. U.S. Securities and Exchange Commission. Report of investigation pursuant to section 21(a) of the securities exchange act of 1934: The dao. https://www.sec.gov/litigation/investreport/34-81207.pdf, 2017.
14. Yuta Takanashi, Shinichiro Matsuo, Eric Burger, Clare Sullivan, James Miller, and Hirotoshi Sato. Call for multi-stakeholder communication to establish a governance mechanism for the emerging blockchain-based financial ecosystem, part 1 of 2. *Stanford Journal of Blockchain Law Policy*, 2020.
15. Usman W WChohan. The decentralized autonomous organization and governance issues. *Journal of Cyber Policy*, pages 1–7, 12 2017.
16. Vlad Zamfir. Against szabo's law, for a new crypto legal system. https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827, 01 2019.