

Decentralized governance in DeFi: Examples and pitfalls.

1st Katerina Stroponiati
Partner, Monday Capital
New York, USA
k@monday.capital

2nd Ilya Abugov
Lead Analyst, DappRadar
Boston, MA
ilya@dappradar.com

3rd Yiannis Varelas
Partner, Monday Capital
New York, USA
y@monday.capital

4th Kostas Stroponiatis
Partner, Monday Capital
New York, USA
ks@monday.capital

5th Modesta Jurgeleviciene
Finance Director, DappRadar
Vilnius Lithuania
modesta@dappradar.com

6th Yashoda Savanth
Raghunatha Rao
Data Analyst, DappRadar
Vilnius Lithuania
yashoda@dappradar.com

Abstract—The DeFi field experienced an incredible surge this year, driven primarily by the popularization of governance token mining. Despite their decentralized infrastructure, most DeFi projects end up highly centralized. In this paper, we analyze the most prominent DeFi DAOs: the structures they have implemented, how they became centralized and the associated risks posed to the projects and the ecosystem.

Index Terms—blockchain, governance, defi, finance

I. INTRODUCTION

Decentralized finance (“DeFi”) has grown into a complex array of platforms on the Ethereum blockchain through which borrowers, lenders and investors can execute financial transactions without the use of traditional financial institutions. The goal of DeFi is to enable an alternative financial system that is built bottom-up, completely decentralized, censorship-free, low-fee, fully-automated and without counterparty risk. DeFi applications strive to be permissionless and open source. Anyone should be able to contribute code and use these protocols no matter where they live or their economic status. This is notably different from the regular banking system. [16]

In practice, there are many limitations to that dream. As the development of the Internet has shown, a decentralized infrastructure does not necessarily lead to a decentralization of powers within that infrastructure. To the contrary, over the years, the Internet network has grown more and more centralized, with a concentration of power in the hands of a few large online operators [4].

The same is true for the blockchain space and the emergence of the DeFi projects on top of it.

In this paper, we will analyze the major DeFi DAOs with the goal of understanding the reasons they fail to properly address decentralization of governance. Also, we will explain why this creates inefficiencies and how it leaves the systems exposed to attacks.

This work is dedicated to Victor, the park musician.

II. BACKGROUND

A. What is Governance

In general, governance defines a framework of rules and procedures that regulates conduct of all participants of a network. It is usually associated with centralized political activity, but it can be applied to everything from commercial interactions to interpersonal relationships.

In practice, governance exists for every system, even if in some it is only implied. Moreover, because systems are hierarchical their governance may be subject to the rules of another system.

For example, the internet as a system follows rules and specific regulations, that determines how different entities interact and how information is transmitted. The different parties using the internet, are subject to both local country laws and international laws, and as such, an internet company does not only need to follow standards for data packaging and transmission, but also laws around data storage, privacy, anti-money laundering and more.

B. Blockchain and Governance

In contrast to the internet, blockchain technology, introduced by bitcoin, was developed with a governance framework embedded in its technology. From the very beginning, this novel technology made it clear that it is not all about code eating the world, it is also about the resultant economy that should make technology autonomous and more meritocratic.

C. DeFi and Governance

Similar to layer 1 protocols, the DeFi protocols that are built on top of Ethereum are being designed with the goal of having as many stakeholders as possible sharing control of the protocol. To that extent, DeFi projects have employed governance tokens to attempt to decentralize the governance of the dapps. Popular distribution models make it so governance tokens can be earned by people who participate in the protocol. These tokens then accrue value due to their ability to be used

to make changes to the project (e.g., make proposals, vote, contribute code, allocate funds etc).

Token voting is a good first step toward transparent, open, on-chain governance but flawed design make it susceptible to large voters controlling the protocols.

III. GOVERNANCE IMPLEMENTATIONS IN DeFi

In this section we are going to analyze the major DeFi projects, how they implement governance, token distribution and token role (if any). We will also display some metrics on participation and also possible attacks that can or have happened.

A. IDEX

IDEX is a decentralized exchange application. A key feature of a DEX is the lack of a centralized custodial entity - users always control their assets. However, IDEX has been developed and is centrally governed by Aurora Labs S.A. What this means is that the company behind IDEX has the power to unilaterally change every aspect of the project: assets listed, fees, integrations and more.

As of the date of publication, IDEX has no governance token. The token is purely used for trading purposes, ie having discounts on fees when trading.

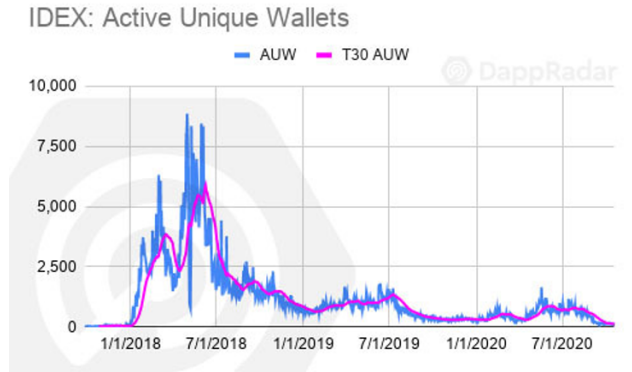


Fig. 3. Source: DappRadar

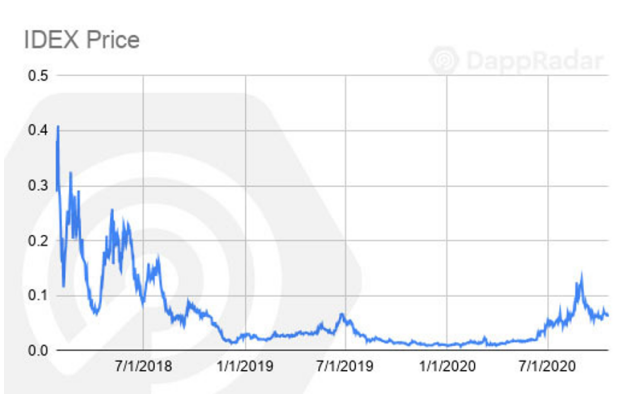
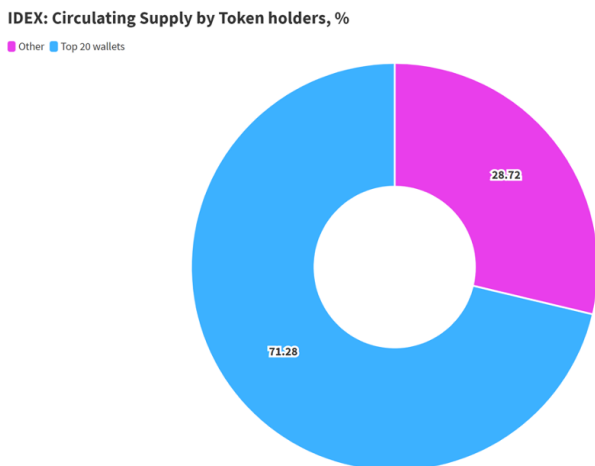


Fig. 1. Source: DappRadar



Source: [Blogs.info](https://public.flourish.studio/visualisation/4099002/) • Note: Smart contracts are eliminated from circulating supply

Fig. 2. Link: <https://public.flourish.studio/visualisation/4099002/>

B. MakerDAO

MakerDAO is one of the oldest dapps in the industry and one of the oldest DAO implementations. The Dai loaning protocol functions as a "pipe" for the number one algorithmic stablecoin in the industry.

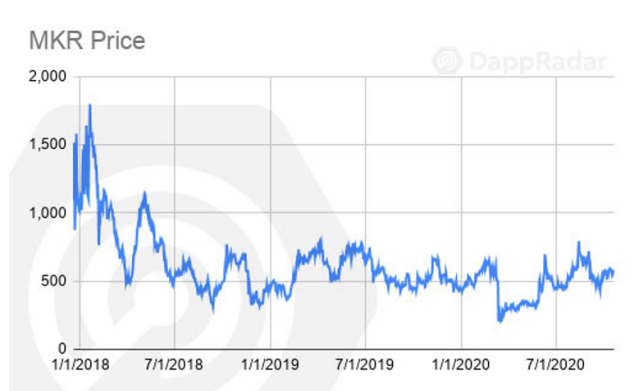
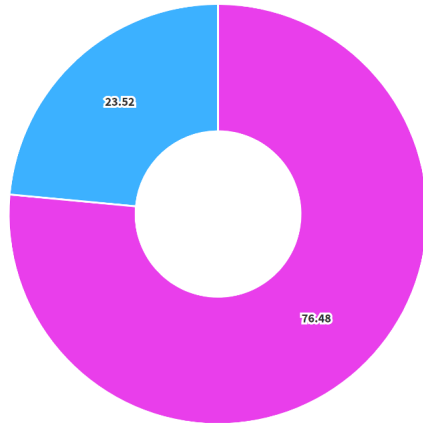


Fig. 4. Source: DappRadar

The governance token of MakerDAO is MKR. Currently the control of the network's contracts is 100% in the hands of MKR holders.

MKR: Circulating Supply by Token holders, %

Other Top 20 wallets



Source: Bloxy.info • Note: Smart contracts are eliminated from circulating supply

Fig. 5. Link: <https://public.flourish.studio/visualisation/4098940/>

The governance process has evolved to be fairly advanced, with separate forum discussion threads before on-chain voting. User get to:

- 1) Determine governance and DAO processes outside the technical layer of Maker Protocol
- 2) Form consensus on important community goals and target
- 3) Measure sentiment on potential executive Vote proposals
- 4) Ratify governance proposals originating from the MakerDAO forum signal threads
- 5) Determine which values certain system parameters should be set to before those values are then confirmed in an executive vote
- 6) Ratty risk parameters to new collateral types as presented by Risk Teams

MakerDAO is very thorough in on-boarding voters, but making proposals is a little bit more vague in terms of procedure.

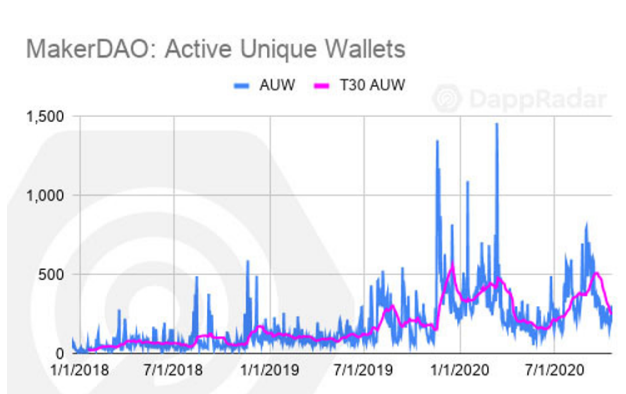


Fig. 6. Source: DappRadar

Voting majority is established with the amount of tokens voting for or against a proposal.

This sounds great, but looking into token distribution, one can easily notice that the majority of MKR tokens is held by only a few wallets. As such, voting power is highly centralized.

C. Compound

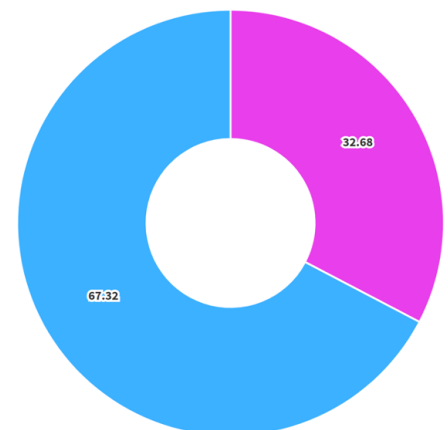
Compound follows a delegated model, which has quickly resulted in plutocracy.¹ Based on the governance model, proposals can only be made by users that have more than 1% of the total tokens delegated to their addresses. [11] Users can delegate their tokens to their own addresses or pick other users' addresses to delegate their tokens to. The model turns naturally to plutocracy though, since the more tokens a user has, the more weight their delegation or vote on a proposal holds. Besides the 1 vote 1 token model, the team and investors own nearly 50% of the total tokens creating an unfair and centralized token distribution from the very beginning.



Fig. 7. Source: DappRadar

COMP: Circulating Supply by Token holders, %

Other Top 20 wallets



Source: Bloxy.info • Note: Smart contracts are eliminated from circulating supply

Fig. 8. Link: <https://public.flourish.studio/visualisation/4098966/>

Currently, there are 50k compound addresses. Considering that exchanges aggregate the compound addresses under one

¹A plutocracy (Greek: ploutos, 'wealth' + kratos, 'power') or plutarchy is a society that is ruled or controlled by people of great wealth or income. The first known use of the term in English dates from 1631.

address, we can't make a precise estimate of the total unique holders. Even ignoring this aggregation that happens on the exchange level, numbers are astonishing. From the 50k holders, 1158 are delegated addresses, which means that 2.3% of the total community currently has the right to make a proposal and vote.²

them to participate in Curve's governance. veCRV can be used to vote on network proposals submitted and those holding high amounts of veCRV can even submit their own proposals. Initially, the founders were planning to distribute 30% to shareholders (team and investors) with 2-4 years vesting).

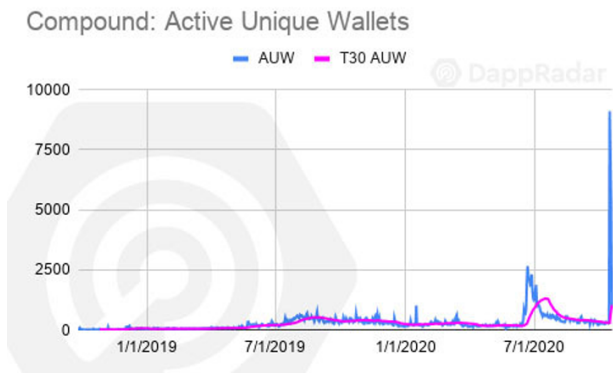


Fig. 9. Source: DappRadar

As we can see from the leaderboard, most of the proposals are made by VCs, team members and a few blockchain projects.

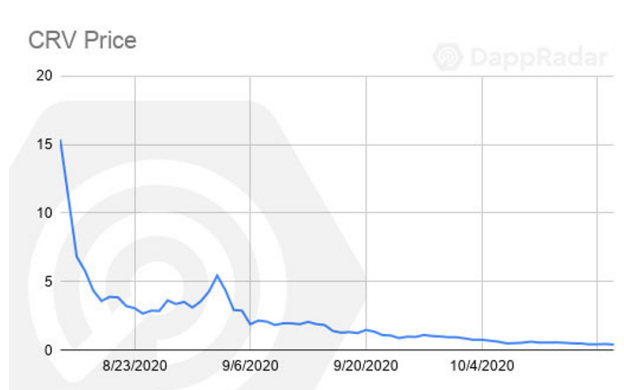


Fig. 11. Source: DappRadar

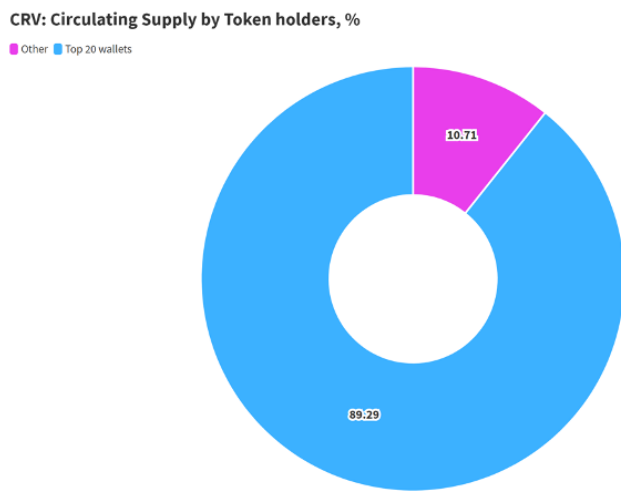
Rank	Address	Votes	Vote Weight	Proposals Voted
1	0x16z	344,964,6835	3.45%	1
2	Polychain Capital	325,768,9184	3.26%	10
3	Gauntlet	125,049,2739	1.25%	17
4	Paradigm	111,088,5237	1.11%	5
5	Robert Leshner	105,004,1599	1.05%	11
6	Geoffrey Hayes	101,000,0219	1.01%	12
7	blck	100,055,0051	1.00%	23
8	Dharma	100,022,6408	1.00%	19
9	Set WBTC Collateral Factor to 60%	71,051,9341	0.71%	1

Fig. 10. Compound top holders.

It is worth mentioning that for a long time Compound operated without a governance token. At some point though, there were disproportionately more lenders than the borrowers, affecting the liquidity of the pools. The governance token distribution incentivized borrowing activity. Users were able to generate profits despite growing interest rates because the COMP token yield more than compensated for, as the governance token (the reward) was tradeable. This led to an increasing interest in COMP token and the protocol is considered the "pioneer" in the liquidity mining idea in DeFi.

D. Curve

On Curve, users and holders of CRV tokens can lock up their tokens to obtain a voting token called veCRV, allowing



Source: [Bloxy.info](https://bloxy.info) • Note: Smart contracts are eliminated from circulating supply

Fig. 12. Link: <https://public.flourish.studio/visualisation/4098989/>

However, Curve's users don't actively participate in the governance process, which leaves decision-making in the hands of a few powerful stakeholders. Users prefer to receive short-term gains, which may explain the significant drop of the token's price.

²Dharma and Gauntlet are at the top holders both here and in Uniswap.

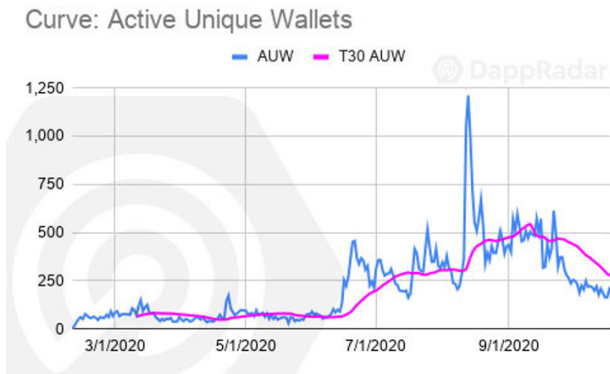


Fig. 13. Source: DappRadar

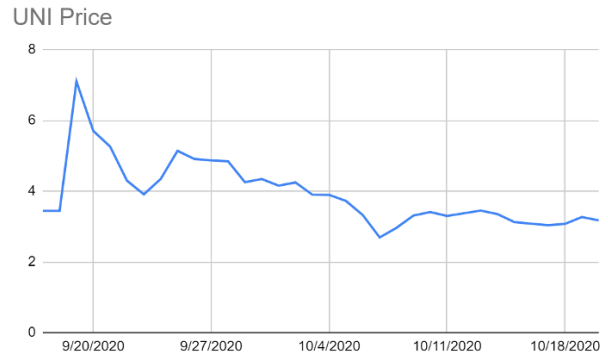


Fig. 15. Source: DappRadar

At one point, it became easy for an address owned by Yearn.Finance – which runs its own liquidity pool – to obtain a significant proportion of the voting power (close to 58%). The founder then decided to buy the 71% of the voting power and maxed out his vote time to four years since the longer a user locks up their tokens, the more voting power they have. This resulted in a major controversy in the community. [12] [13]

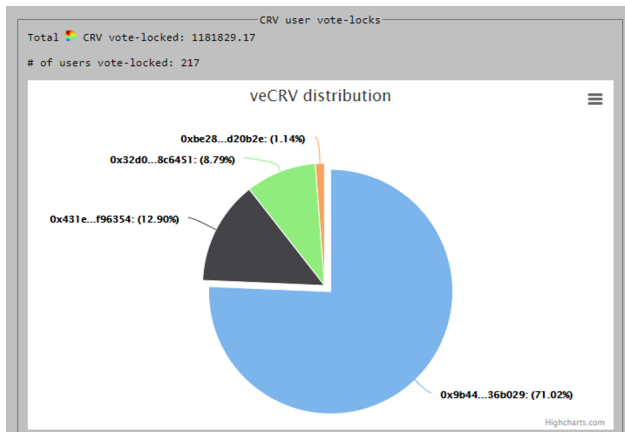
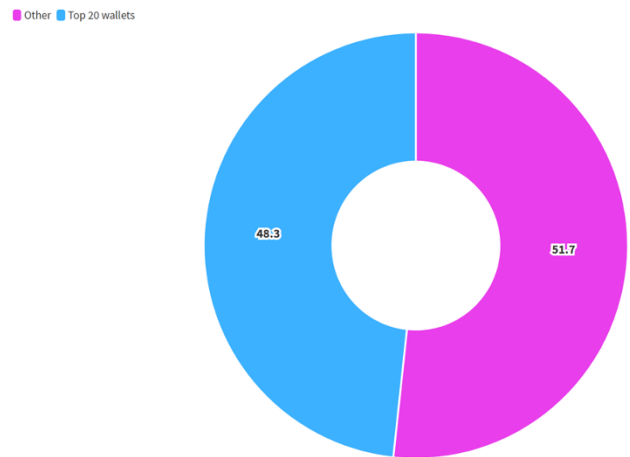


Fig. 14. Curve top holders.

UNI: Circulating Supply by Token holders, %



Source: [Bloxy.info](https://bloxy.info) • Note: Smart contracts are eliminated from circulating supply

Fig. 16. Link: <https://public.flourish.studio/visualisation/4098806/>

Although the team has claimed that the team and investor allocations will vest over 4 years, the tokens allocated to the Uniswap team and to the investors are currently held in regular Ethereum addresses with no transfer restrictions. [14]

E. Uniswap

Uniswap follows a similar model to Compound. A minimum threshold of 1% of the total UNI supply is required in order to submit governance proposals.

UNI holders may delegate their voting power to a representative. Similar to Compound, the team and VC investors own a disproportionate amount of power in the early stages of governance since they own 30% of the total supply. Notice that Dharma and Gauntlet, also appear on Compound's top 10 addresses by voting weight.

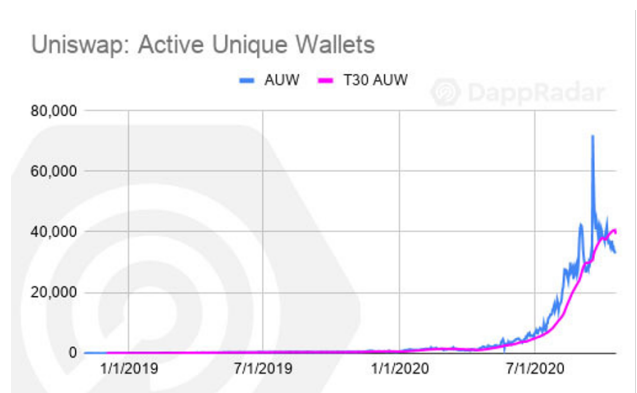


Fig. 17. Source: DappRadar

IV. IMPLEMENTATION ISSUES

Although some projects acknowledge early centralization and high concentration of tokens within the team following a gradual decentralization strategy, that does not mean that in the short to medium term there won't be significant issues that could affect the protocol and user funds.

By looking at the above analysis, one can note that there are few main problems that lead to the majority of the issues with governance in decentralized systems:

- 1) Users see tokens as yield, not voting rights, leading to a very individualist approach to collaboration. Protocols started using their governance tokens as "rewards" for users participating in the network. Although the idea sounds nice - governance goes to those who use the product - in reality the financial incentives have been stronger than the governance incentives. Add the speculative natures of the tokens holders in the equation and we can see why a very small percentage of token holders actually participate.
- 2) No minimum number of participation in order to kick-start the governance. In order for a system to be considered sufficiently decentralized, there needs to be a high minimum number of token holders/participants. Most quorum minimums focus on the number of votes/tokens engaged not the number of voters. The majority of DAOs have less token holders than a privately held company. This leads to "decentralized" systems where decisions are made from a small number of token holders who DO understand the importance of the token they hold.
- 3) Private sales to investors. Most of the DAOs raise money in one way or another. In return, most of the investors get back governance tokens. This creates a high degree of centralization at the start of token distribution, and may actually disincentivize new token holders from directly engaging in project governance.

A. Notable Vulnerabilities

In this section we will discuss some notable cases of projects becoming vulnerable to attacks because of excessive centralization. Community participants and malicious players have figured out ways to attack the protocols by exploiting the design issues we discussed above.

1) *MKR takeover attack scenario:* In MakerDAO's governance framework there are two types of votes. The governance vote is a simple yes/no poll and it is used for solving resolutions and the executive vote which is handled via approval voting to change the state of the whole system through an "executive contract". This contract is also the only entity in the MakerDAO system that contains rules and decisions about the funds locked as collateral. The contract with the most tokens staked (MKR) will be elected and immediately enacted. Given this design, an attacker could deploy a malicious contract and steal all the funds that are locked. This is not very hard to do since the amount of tokens locked in the current executive contract is about 80K




tokens and this amount changes frequently. At the current price of MKR (\$560), an attacker would need about \$44M to take control of the contract, for a potential reward of \$2B (Total value locked as collateral in Maker). The warning and the steps to follow were published by an independent software developer in order to draw immediate attention of the MakerDAO team about a potential catastrophic event for the whole DeFi ecosystem. [7]

2) *Parties with conflict of interest pushing through proposals (Uniswap-Dharma):* A recent example of conflict of interest took place during Uniswap's first proposal, made by Dharma, to reduce Uniswap's existing governance thresholds. Dharma had 32% of the voting power at the time of the proposal while the second biggest voter had 30%. Dharma's made two proposals. One was for a reduction of the amount of tokens needed, in order to submit a proposal, from 1% to 0.3%. The second one was for a reduction in quorum, or the percentage of the total supply which must vote on a proposal in order to pass, from 4% to 3%. Dharma claimed that these two proposals would give the ability to smaller token holders to make proposals and also it would be easier for important proposals to not get rejected since many token holders do not bother voting. Dharma might have had the right intentions but looking at the numbers many could infer that these proposals could easily give more power to Dharma itself on governing Uniswap's protocol. Uniswap total (not circulating) supply is 1 billion. Under the initial protocol rules, 10 million tokens would be needed in order to submit a proposal and 40 million tokens for the proposal to pass. Dharma's proposal was for a reduction of these two numbers to 3 million tokens and 30 million tokens, respectively.

Considering that Dharma's voting power is 15 million tokens or 32% [8] of the total voting power, while the second biggest voter has 30% of the votes or 14 million votes, by reducing the quorum threshold to 30 million, Dharma and the second biggest voter (Gauntlet) could combine voting power to push through any proposal these two believe would be best for Uniswap or them. [9]

3) *Exploiting the composability element:* While DeFi projects may each have individual governance, they are highly interconnected. A collapse of one protocol can cause a domino effect in others. As such it may be a highly profitable endeavor to buy governance tokens of project A in order to crash it by passing hostile proposals, while shorting tokens of projects B (and perhaps C and D) to capitalize on the negative aftershock. Moreover, a clever and lately, quite common strategy, is that the teams of these platforms are employing a "marketing" tactic of offering the possibility to earn governance tokens of other protocols (usually those that have attracted a lot of attention and their price has advanced a lot) to incentivize new users to provide liquidity to their platforms. For example, in order to incentivize users to lock BTC in Curve's sBTC pool, the platform offered users the possibility to earn governance tokens of other platforms

Governance Token and Total Proposals

Dapp	Native Token Image	Governance Token	Proposals
Compound		COMP	27
MakerDAO		MKR	316
Uniswap		UNI	1


 Source: DappRadar

Fig. 18. Proposals and their outcome (Source: DappRadar)

(synthetic, balancer etc). Both platforms had attracted a lot of users and attention from the community, so Curve capitalized on their success. However, indirectly, a user could deposit BTC and get the majority of the rewards of the Curve's BTC pool. By doing so long enough, he/she also becomes a participant in other protocols' governance.

4) *Concept of the Activist Investor*: Similar to traditional industries, activist investors can acquire a significant enough amount of governance tokens to help push through proposals profitable to them. These may be profitable to an investor in the short term, but detrimental to the protocol in the long-term. The LINK short thesis by Zeus Capital, while controversial, may be foreshadowing a future trend. [10]

Highly centralized projects may have governance members take control - recent KuCoin hack showed that projects with a high degree of centralization may freeze assets or create forks. [22] While in this case this was done to benefit the communities, it adds another dangerous precedent.

B. Legal uncertainty

Recent publications from legal enforcement agencies and watchdog groups (SEC, CFTC etc) have clearly highlighted the view these groups have for the space. [19] [20] [21] Tokens that yield interest and also provide voting rights, are by definition securities. Most of the projects have raised money from institutional investors. Those investors need something in return. This is usually translated into a significant sum of tokens, that give them of course governance rights. The lack of sufficient decentralization and token distribution, plus centralization of decision making through whales holding the tokens, puts those projects under high risk. Any government can claim that decisions are made by a few entities/individuals, who are responsible for the project as a whole. Any legal claims against the projects, will be directed towards them, including fines and more. A very recent example involves the founder of y.earn who may be sued by disgruntled users over funds lost in EMN. [18]

Most of the protocol participants(users/investors etc) don't properly understand the governance of the projects that they invest in and the real risks that they take. It is important for participants to be aware of these trade-offs in order to better understand the services they want to participate/invest in and use. If those risks are not properly assessed, the risk of losing funds either via a protocol error or a malicious attack, puts the users funds but also the whole protocol functionality at both financial and reputational risk.

V. CONCLUSIONS

In this paper, we attempted to give an overview of the political governance issues in the DeFi ecosystem of Ethereum. These projects start with a centralized governance structure, where decision making on updates and changes is made by a team or an individual and then they aim to gradually move to decentralization of governance by distributing tokens to the users of the protocol/service. However, the economic incentives of providing liquidity in order to get rewarded with governance tokens, encourages competitive and speculative behavior which leads back to a centralized governance structure, since tokens slowly concentrate in a few hands. In our next paper, we will provide some alternative models of governance to address these dynamics.

REFERENCES

- [1] Wright, Aaron and De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015).
- [2] The digital economy ;rethinking promise and peril in the age of networked intelligence
- [3] Melanie Swan, Blockchain: Blueprint for a New Economy, January 2015. O'Reilly Media, Inc
- [4] Primavera de Filippi. Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream
- [5] Vitalik Buterin. The meaning of decentralization. <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>
- [6] Marcella Atzori. Blockchain Technology and Decentralized Governance: Is the State Still Necessary?
- [7] Micah Zoltu. <https://medium.com/coinmonks/how-to-turn-20m-into-340m-in-15-seconds-48d161a42311>
- [8] <https://ondkloss.github.io/uniswapdelegates>
- [9] Martin Young. <https://beincrypto.com/the-dharma-defi-dilemma-is-uniswap-becoming-more-centralized/>

- [10] Ilya Abugov. <https://cointelegraph.com/magazine/2020/07/20/activist-investors-crypto-blockchain>
- [11] Compound Governance documentation <https://compound.finance/docs/governance>
- [12] Curve token seizure - Decrypt <https://decrypt.co/39599/curve-founder-seizes-71-of-curve-dao-voting-power>
- [13] Curve token controversy- Yahoo <https://finance.yahoo.com/news/founder-curve-now-controls-71-153956022.html>
- [14] Uniswap team tokens controversy <https://cointelegraph.com/news/glassnode-uniswap-team-may-have-misled-community-over-team-token-vesting>
- [15] <https://cointelegraph.com/news/three-birds-one-stone-enhancing-defi-with-political-parties>
- [16] Bitkom Whitepaper - Decentralized Governance https://www.bitkom.org/sites/default/files/2020-07/200729_whitepaper_decentralized-finance.pdf
- [17] <https://www.bankingexchange.com/cards/item/8339-the-rise-of-decentralized-finance-and-why-banks-should-start-paying-attention>
- [18] yearn creator could be sued <https://news.bitcoin.com/defi-community-members-aim-to-sue-yearn-finance-creator-andre-cronje-and-fork-yfi/>
- [19] Howey test and crypto <https://www.sfox.com/blog/howey-test-bitcoin-crypto-regulation-2020/>
- [20] SEC framework for tokens <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>
- [21] SEC Charges blockchain company for unregistered securities <https://www.sec.gov/enforce/33-10865-s>
- [22] Ocean Protocol fork in response to KuCoin hack <https://www.coindesk.com/ocean-protocol-hard-fork-freezes-funds-kucoin-hack>