Decentralized Autonomous Finance Organizations in 2021: an Analysis

Andrew Gold
Delft University of Technology
Delft, The Netherlands
a.w.r.gold@student.tudelft.nl

***Abstract*— Decentralized finance has ballooned in transactional volume and value in recent years, leading to numerous protocols of varying levels of complexity being launched to much fanfare and minimal scrutiny. The interconnected nature of decentralized finance, coupled with the high technical and economic complexity of many protocols, signifies that a fundamental weakness in one protocol can lead to unintended side effects or weaknesses in others. This paper explores the past and present landscape of decentralized finance protocols and communities, highlighting past weaknesses that newer protocols have aimed to address, and diving deep into one particularly popular novel protocol, OlympusDAO. The concepts of protocol-owned liquidity, decentralized reserve currencies, and their relationship with complex algorithmic stablecoins are investigated, as are the communities and DAOs that govern and guide them. Various scenarios are expounded upon, particularly those that potentially destabilize one or more of these protocols and/or the broader cryptocurrency market, and how these destabilizing events may lead to cascading negative side effects. Furthermore, the concept of true decentralization and trustlessness in finance is critiqued, followed by the delineation of potentially necessary compromises required for projects to achieve a high degree of security and stability while still remaining sufficiently decentralized.**

I. INTRODUCTION

Decentralized finance has come a long way since its inception soon after the launching of the ERC-20 standard on the Ethereum blockchain. The humble beginnings of tokenization rapidly flourished into a complex, interdependent network of various blockchains and smart contracts with a peak value of over $180 billion stored across various protocols [1]. Beginning as a simple mechanism for value transfer, the introduction of automated market maker (AMM) algorithms allowed for decentralized exchange and liquidity provision, bypassing the middlemen of traditional finance institutions. Since then, numerous decentralized finance ecosystems have launched on various blockchain platforms to varying degrees of success, none more successful than Uniswap - an Ethereum-based decentralized exchange. Uniswap pioneered "trustless" liquidity provision, bypassing the need for finding counterparties in a decentralized exchange and allowing liquidity providers to earn rewards in exchange for locking up their tokens in a smart contract.

However, the inflationary nature and high emission rates of decentralized exchange tokens led these tokens to drop precipitously in value, incentivizing liquidity providers to withdraw their tokens in search of greener pastures with higher frequency. Yield farming, it became known as, became the standard practice for speculative investors as they cyclically pursued high reward rates and new token pairs in the attempt to maximize profits, leading to rapidly shifting liquidity levels in decentralized exchanges. As many cryptocurrency investors began distancing themselves from the diminishing returns of liquidity provision, many began to question the wisdom of denominating the broader cryptocurrency market in US Dollars - an asset that has increasingly become inflated in the wake of the COVID-19 pandemic.

In response to the high-risk nature of providing liquidity to a decentralized marketplace, new protocols with novel mechanics began to appear in early 2021 that flipped the status quo on its head. Aiming to address the two major problems just mentioned, OlympusDAO became the first project attempting to create a digital reserve currency for the broader cryptocurrency market while simultaneously accumulating vast sums of liquid assets to be used as rewards for liquidity providers in what would become known as "DeFi 2.0". The fundamental shift in liquidity provision theory spawned hundreds of copycat projects peaking at over $14 billion in assets becoming staked across Olympus-style protocols within six months. However, numerous questions abound regarding the stability and security of these protocols, as OlympusDAO (along with many others) claim to be governed by their community DAO, even though the anonymous developers hold the majority of the private keys that control the treasury. Additionally, the sustainability of the high yield rewards of staking with these funds is questionable, where complex mechanics governing the variable rates of reward emissions being decided upon by anonymous DAO members may lead to potential conflicts of interest. Such a fundamental ethical mismatch between the ethos of decentralized finance and the inherent complexity in governing an organization in control of billions of dollars worth of assets is worth thorough investigation, which is exactly the purpose of this paper.

The structure of this paper is as follows: Section 2 surveys the landscape of decentralized finance up to and including 2021, investigating the paradigm of decentralized exchanges, liquidity pools, and their intrinsic tokenomics. Section 3 discusses the taxonomy of finance DAOs - the decentralized autonomous organizations that attempt to govern decentralized finance protocols, and discusses the novel concept of protocol-owned liquidity introduced by OlympusDAO. Section 4 dives deeper into OlympusDAO and its major forks and copycats, discussing the relationship between the protocol and the cryptocurrency assets that allow it to exist, particularly the strong interdependence between algorithmic stablecoins and these novel "reserve currencies," and the inherent weaknesses of such a relationship. Section 5 consid-

ers whether or not truly trustless decentralization is possible and whether finance DAO governance is feasible in such an environment, concluding in Section 6.

II. DECENTRALIZED FINANCE AND DAOS

Decentralized Finance was made possible when the Ethereum blockchain launched, where anybody could create their own tokenized digital asset out of thin air, essentially inventing new economic experiments with little to no initial costs. In order to avoid the centralization and regulatory scrutiny that is inherent with centralized exchanges owned by private entities, decentralized exchanges operating primarily on the Ethereum blockchain began offering users the ability to transact their tokens directly in a peer-to-peer manner. Most decentralized exchanges function via automated market maker algorithms, providing liquidity pools in order to facilitate the exchange of tokens without needing to directly find a counterparty to a transaction, performing a similar role to market makers in traditional finance. Stakers in liquidity pools are rewarded with a portion of the transaction fees of the DEX in exchange for locking up their tokens, but staking can be risky due to opportunity loss and impermanent loss. The opportunity loss stems from the friction of or complete inability to withdraw tokens when a positive expected value opportunity arises, and the impermanent loss occurs when the staked liquidity pool tokens (LP tokens) become worth less than the value of the primary token itself if the staker had not partaken in the liquidity pool in the first place.

In order to offset the risk of these potential losses and attract new liquidity providers, decentralized exchanges often offer additional incentives to stakers that usually take the form of proprietary exchange tokens, such as the token UNI for the Uniswap exchange. In addition to transaction fees, stakers are rewarded with these tokens over time in exchange for remaining in the pool. However, if this token has an infinite supply (i.e. they can be minted ad infinitum by the protocol) then the value of the token gradually diminishes as the supply grows large, leading to reduced profits for stakers over time. As more and more protocols launch, exorbitant rewards are offered to new liquidity providers in order to bootstrap new liquidity; rewards which taper off as more liquidity is added to the protocol. When token emissions taper to such an extent that liquidity providers feel that the investment is no longer worth the effort or risk, many providers withdraw and "rotate" their funds into new liquidity pools, oftentimes market-selling their token rewards in the process to lock in profits. Such supply-side tokenomic rewards essentially serve as virtually infinite selling pressure on the market, suppressing the price of the reward token due to the relative lack of demand for the token.

Some decentralized exchanges have attempted to increase buying pressure and/or reduce selling pressure of their proprietary tokens through various means, such as by reducing transaction fees for token holders or by vesting token rewards over longer periods of time - all to little effect. The general price trend of many decentralized exchange tokens, such as UNI and SUSHI, is largely negative - particularly when compared to the value of ETH, a common comparison for many ERC20 tokens that serves to compare the value of investing in an Ethereum-based token versus the native ETH token instead. As such, the broader consensus in the trading communities is that decentralized exchange tokens are largely a poor investment, leading to further negative sentiment surrounding the token.

Preventing Hostile Takeovers

If a DEX token acts as a governance token for the DAO, governance of the DAO is susceptible to hostile takeovers similar to those seen in the traditional corporate world. Even without the possibility of a hostile takeover, the integrity of the DAO can still be undermined via corruption and grift similar to the institutional rot seen in various democracies around the world, as private or individual interests can usurp the interests of the broader community when wealthy individuals accrue enough voting power to influence policy towards their own benefit. This is one of the fundamental weaknesses in token-based governance, especially when voting power is directly proportional to the amount of tokens one holds. The broader DeFi community is largely unaware or seemingly uninterested in addressing the problem, as token-based governance remains the most popular form of DAO governance in existence at this point in time. However, this does not mean that such a model is fundamentally broken; it just remains susceptible to the same ills as many traditional capitalist democracies, where governing power can essentially be purchased. As DeFi continues to grow in scope and scale, it is therefore prudent for new and scaling ventures to carefully consider how they wish to govern themselves, else they become oligarchical.

A significant majority of major decentralized autonomous organizations (DAOs) operate under some form of token-based governance, the largest and most well-known being MakerDAO. MakerDAO is the governance structure and community supporting the DAI stablecoin project, where holders of the MKR token are given voting rights on proposals including internal governance, external investments, official partnerships, and more. There is nothing stopping wealthy individuals from individual purchasing significant amounts of MKR (or colluding with others to do so) to influence the outcome of proposals that financially benefit themselves, a token-based hostile takeover of sorts. MakerDAO is of course aware of this possibility, and even casual observers would be able to see it happening in real-time due to the transparency of the public ledger, but nonetheless would be unable to stop it. There exist a few internal mechanisms implemented to mitigate such a hostile takeover, including the ability to submit emergency proposals that are shorter in duration and require a quorum of voters instead of a clear majority [2].

In the face of a successful adversary, MakerDAO contributors could also fork the project from a block prior to the takeover, and resume where they left off. This would however strand passive investors on a now-inactive fork of the project, where the token's value would ostensibly drop

precipitously as active contributors and investors migrate to the new chain. Additionally, short of major fundamental governance alterations, nothing would stop the adversary from doing the exact same thing on the new fork. Such a process could be repeated ad nauseam as the community attempts to drain a persistent adversary's funds, but would likely lead to a significant decline in community sentiment, and is far from efficient. Similar to a 51% attack on a proof of work-based network, repeated attempts to undermine a token-based network can only be repelled so long as there are sufficient participants willing to continuously rebase and fork, performing a "strategic retreat" attempting to drain the adversary's funds and/or willpower. The question, then, is whether or not traditional token-based governance is sustainable and secure from interference over the long-term.

Navigating the Dark Forest

Poor tokenomics and governance mechanisms are not the only dangers to investors and users in the decentralized finance ecosystem. Ethereum, as with many public blockchains, relies on miners to aggregate transactions accordingly into upcoming blocks, where users compete for blockspace by including fees to miners to place themselves into the queue. Miners are privy to very valuable information contained within the pending and requested transactions, especially when these transactions are of significant size. These miners can inspect upcoming transactions and determine if any pending transactions will affect the market in a noticeable manner, similar to the illegal practice of front-running in traditional finance. As such, miners have the power to organize pending transactions (including their own) such that they can profit from a transaction that is yet to be confirmed. This practice is known as Maximal Extractable Value, or MEV for short.

Such a mechanism has been coined as a "Dark Forest," a reference to the science fiction novel by Liu Cixin [3], wherein a dangerous environment exists such that detection by highly advanced adversaries can lead to one's death. Miners wield enormous power over the Ethereum network and particularly over decentralized exchanges due to their ability to peer into the near future of pending transactions. For example, should an upcoming transaction create or include an arbitrage opportunity, miners can include their own transactions in the same block instead of taking a place in the queue as everyone else does. Furthermore, the upcoming transition of Ethereum to the Proof of Stake consensus model does not entirely eliminate the threat MEV poses [4]. While Proof of Stake introduces a new form of randomness to the creation of new blocks, validators can still take advantage of mempool analysis to front-run transactions. Additionally, validators can collude to extract value and share profits in the case that one of such validators gets chosen to create the next block. This fundamental property of blockchain transactions means that decentralized finance in its current form is inherently inequitable, where those with specific means (e.g. miners and astute programmers) wield disproportionate power over those without such means; an example of oligarchical governance in an ostensibly equitable technological revolution.

Token-based Oligarchy

The more complex a participatory organizational structure becomes, the more knowledgeable and attentive participants must become in order to maintain the integrity of the organization. This leads to the situation where a subset of the participants are more capable of navigating the organizational and social structures within the organization, particularly if they're technologically knowledgeable. Some influential minds involved with decentralization initiatives subscribe to the Iron Law of Oligarchy, which states that all organizations and governments trend towards oligarchy, as the "elites," or those who wield the most influence, tend to become the governors themselves. Additionally, over time organizations tend to become dichotomous where those who govern often serve the establishment itself instead of the establishment's intrinsic goals. With regards to DAO governance, decentralized governance has a natural tendency to centralize around a core of "elites" over time - often those who spend the most amount of time developing the protocol or engaging with the community. This tendency (if it indeed exists) is due to the gradual decline in engagement from the community, where fewer and fewer participants remain focused and engaged with the organization's internal and external functions. Those that do remain, according to the theory, tend to spend more time managing and governing the organization to maximize longevity and profits, rather than achieving the intrinsic goals of the organization.

When a DAO is governed via a token model, any actor who purchases the token on the open market can immediately insert themselves into the governance structure without participating in furthering the DAO's mission or abiding by its ethos. There have been many discussions on this topic in recent months as the number of DAOs has exploded, one of the most outspoken being Vitalik Buterin himself. Buterin has repeatedly pointed out several inherent problems with token-based governance models [5][6], along with several potential options for mitigating negative consequences of such models, but is in agreement that DAOs need to move beyond token-based governance in order to survive. Intrinsically linking economics with governance has often led to both governance and economic problems in the past, and the token-based governance model is no different, the fear being that the same forces that lead to centralization of power in modern society will inevitably happen with blockchain governance. Therefore, one may argue that separating any economic incentives with a governance model is of utmost importance for the long-term viability of decentralized governance, assuming the goal is a participatory democratic model. Such models must not only take into consideration the economic goals and incentives of the organization, it must also consider the social mechanisms and hierarchies of participants, especially acknowledging that it is likely the vast majority of participants of the organization will contribute minimally.

That being said, a counter-argument in support of inextricably-linked economics and governance would suggest that incentivizing participants economically to participate in the organization - particularly when funds are staked as collateral - is for the betterment of all. When a participant stands to lose their funds by behaving in a manner antithetical to the consensus of the community, proponents may argue that they are therefore more likely to behave altruistically, or at least in a manner that does not put their staked funds at risk. Both arguments contain some merit, at least in theory. In order to better understand the consequences of various token-based governance models, Section 3 investigates more deeply the mechanics of a few major DAOs and their inner economies and governance structures.

III. TAXONOMY OF FINANCE DAOS

In this section, the taxonomy and tokenomics of several decentralized autonomous organizations is explored - particularly those whose tokens or software underpin other finance DAOs, such as MakerDAO. Following a brief introduction to MakerDAO, their flagship stablecoin token DAI is examined alongside MakerDAO's governance structure and mechanisms. Considering that the stablecoin DAI serves as the foundation for other DAOs, the relationship between DAI and premier DAO tokenomics is important to the overall stability of any proprietary DAO token's value and economy. However, DAI is far from the only token that underpins the tokenomics of other DAO currencies, therefore symbiotic relationships between tokens and communities plays an important role in the broader DAO ecosystem. Finally, the concept of "DAO tooling," or building modular ecosystems that are designed to be used and recycled in various settings is introduced as a new area of research and development, including a few notable examples.

MakerDAO and the DAI Stablecoin

MakerDAO is one of the first and most recognizable DAOs built upon the Ethereum blockchain ecosystem. Launching in 2017, MakerDAO began with its proprietary token MKR used purely as a governance token with the intent being that the DAO would govern the tokenomics and smart contract operability surrounding their proposed dollar-pegged DAI stablecoin. The purpose of the MKR token was to be used as voting rights within the DAO, as voters would be able to determine facets of the stablecoin's algorithm such as the mandatory minimum collateral ratio. As of December 2021, the current minimum collateral required to mint DAI is 1:1.5 (denominated in ETH), meaning that users must stake $1.50 worth of ETH to mint $1.00 worth of DAI. When a user wishes to recoup their staked ETH they must repay the loan plus interest, and the interest is deposited into the DAO's treasury, which is used to purchase MKR tokens and burn them, effectively reducing the supply and theoretically increasing the value of existing MKR tokens.

MakerDAO officially launched the DAI stablecoin in December 2017; within a week the broader cryptocurrency market would see a massive correction following an enormous bull run that saw the total cryptocurrency market cap increase more than forty-fold from $18 billion to over $800 billion in just one year. Immediately after the blow-off top at the end of 2017, the market experienced prolonged bouts of volatility during a correction that would see the total market cap shrink by over 85% at the bottom of the bear market. During this time, the DAI stablecoin successfully maintained its peg to the dollar with no notable incidents, further bolstering MakerDAO's claim that algorithmic stablecoins were sustainable alternatives to the much-maligned Tether stablecoin (USDT). At the time, MakerDAO founder Rune Christensen lauded the stablecoin's relative stability, pointing out that even though the value of Ether - the only form of collateral available to mint new DAI tokens at the time - had dropped by 80%, the value of DAI had never fluctuated by more than roughly 1%. However, during the March 2020 COVID-19 crash the value of DAI experienced a deflationary spiral that sent the stablecoin's value above $1.10 before settling back down to its original dollar pegging. Such a crash demonstrated that in the face of a black swan event, even the over-collateralization of the DAI protocol wasn't enough to prevent significant fluctuations in value. Since then, DAI has retained its peg to the dollar within a range of roughly one percent.

MakerDAO Governance

Any individual or entity that owns MKR tokens is allowed to participate in the governance of MakerDAO. There are two types of proposals that holders can both propose and/or vote on: executive and governance polls, both of which are conducted on-chain. Members that hold MKR tokens can also propose themselves as delegates, akin to representative democracy. Community members can then stake their MKR tokens with delegates, effectively giving these delegates more voting power. Delegates are approved by the community by a vote, and are publicly tracked and expected to maintain a high participation rate. Delegates usually interact with the community via the MakerDAO forums where they determine the sentiment of the community and how both their constituency and the broader community expect them to vote in an off-chain informal poll. Such an action is called a "signal vote" and is intended to determine whether on-chain action is warranted, especially considering the monetary cost of voting on and deploying changes to the main Ethereum network. After a signal vote is concluded, the proposal is moved to an official on-chain poll, whose results are final and often already include the codified proposed changes to be deployed at a specific block number. Once the vote is concluded, the proposed changes go into effect at the predetermined time.

In this governance structure, large MKR holders have an outsize influence on the direction of the DAO due to the fact that voting power is proportional to the MKR holdings of an individual. As such, MakerDAO is susceptible to many of the pitfalls of token-based governance discussed in Section 2, but with an important caveat: the MakerDAO treasury is already being used to deflate the MKR supply automatically via smart contract, meaning that holders are already profiting

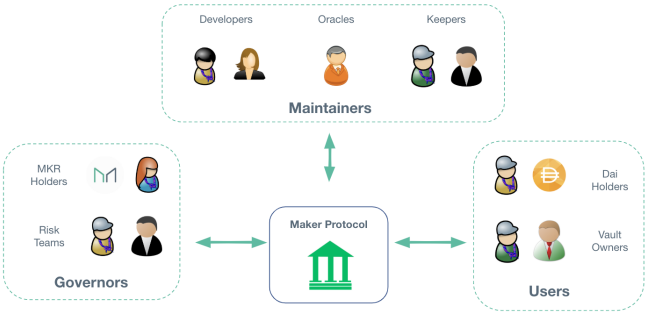

Fig. 1. MakerDAO largely consists of three types of contributors: Governors, Maintainers, and Users. (Source: MakerDAO Documentation)

Fig. 2. OlympusDAO retains nearly 100% ownership over the contents of its treasury, such that the DAO wields enormous influence over the broader DeFi ecosystem due to its rapidly deployable liquidity. (Source: OlympusDAO Dashboard)

from the current paradigm. One of the few possible proposals that could undermine MakerDAO would be to send interest payments directly to MKR holders (or a single specific address) instead of performing token buybacks. However, such a proposal would require broad collusion within the community such that it would be trivial to identify such an effort, allowing non-colluding members of the community to react before going into effect.

MakerDAO's large and active community seemingly acts as a deterrent to malicious behavior, for now. Similar to many traditional institutions, as the DAO grows large the attack vectors for adversaries change accordingly. Smaller DAOs bootstrapping their way through rapid growth phases are more easily undermined from without as wealthy adversaries can purchase their way into power. That being said, small DAOs are also quite nimble and may be able to adjust accordingly should they suffer an attack such as a hostile taker. However, should a small DAO experience rapid growth both in usership and funding, the precarious nature of rapidly bootstrapped growth may attract adversaries as the DAO experiences growing pains.

OlympusDAO and Protocol-Owned Liquidity

OlympusDAO launched in early 2021 attempting to resolve many of the issues mentioned in Section 2 regarding the unsustainable nature of current DeFi liquidity provision protocols. Labeling itself as a "decentralized reserve currency," in less than a year OlympusDAO has acquired a massive war chest of roughly $700 million in various assets, primarily the stablecoin DAI. By minting their currency OHM in a similar bonding mechanism to a central bank, OlympusDAO was able to raise enormous sums of capital in their attempt to create a digital asset backed by a basket of goods, similar to a cryptocurrency "price index." Their goal is to create a free-floating currency that other cryptocurrencies measure their value against, attempting to establish a new paradigm of cryptocurrency valuation that is not denominated in USD.

The explosive growth of OlympusDAO spawned hundreds of copycat projects attempting to capitalize on the new paradigm shift in the broader DeFi ecosystem, most of which turned out to be scams [7][8][10]. The fundamental concern with OlympusDAO is that the treasury is managed by just seven anonymous individuals, four of whom are the founders of the project. Even though the keys to the treasury are guarded in a time-locked Gnosis safe [9], the entire founding team can simply perform a 4-of-7 threshold signature to drain the entirety of the treasury whenever the Gnosis safe is open. Furthermore, the policy contracts are protected in a similar way, though the scheme is 3-of-5, such that a small number of privileged individuals can collude to modify smart contract policy in their favor. This has not happened (yet) with OlympusDAO, but several OlympusDAO copycat projects have had exactly that happen - the code was copied and deployed to a new blockchain, unwitting users purchased new tokens by depositing into the treasury and the founding teams withdrew all the funds and disappeared. The risk of founding teams or trusted insiders with access to the treasury is therefore a persistent threat to the survivability of many finance DAOs, and it is essential that steps be taken to eliminate such a threat before DeFi can consider itself truly "decentralized." Several such steps are discussed in Section 5.

IV. OLYMPUSDAO, DAI, AND WEAKNESSES IN MODERN DAOS

OlympusDAO's meteoric success in bootstrapping enormous amounts of liquidity has shifted the paradigm of decentralized finance away from the highly unsustainable practice of renting liquidity in exchange for rapidly inflating reward tokens. With an enormous number of copycat projects accumulating massive treasuries across various blockchain ecosystems, the DeFi zeitgeist is currently being redefined by the concept of protocol-owned liquidity. DAOs that govern massive treasuries are therefore faced with the imperative of updating their governance strategies to better reflect the greater responsibility in managing such enormous wealth. However, not only do these DAOs face greater responsibility but also significantly greater flexibility in defining both their internal economic mechanisms but also the broader economies into which they integrate. This section highlights

several of the hurdles faced by finance DAOs such as OlympusDAO and MakerDAO, particularly those regarding its long-term viability considering the antithetical compromises DAO participants must make.

Communal Treasuries and Governance

OlympusDAO is currently (at the time of writing) in the process of deploying its "version 2" upgrade, which includes security improvements to their smart contracts based on previous audits [11], as well as transferring total ownership of the private keys controlling the treasury to the DAO - an improvement in securing the funds from insider access. This new update also lays the foundation for the next major focus of the DAO: bootstrapping new DeFi projects by acting as decentralized venture capitalists. In this new program, called Olympus Pro, the OlympusDAO community votes on proposals similar to venture capital investments, where project founders pitch to the OlympusDAO community to provide liquidity in exchange for 3.3% of their new project's tokens to be locked up in the OlympusDAO treasury [12].

Such changes may improve the safety and viability of OlympusDAO, particularly in that the founding developers of OlympusDAO will no longer be able to meet the "K-of-N" threshold for signing transactions from the treasury. However, maintaining a 4-of-7 threshold signature scheme to secure the treasury has both benefits and drawbacks, primarily regarding the integrity of those with access to the seven keys. There is no clear documentation outlining who these seven keyholders are, how they were chosen, or if there are any plans to change the current scheme to something more transparent. No current pending improvement proposals (OIPs) suggest changes to the treasury management scheme in any regard, which could potentially indicate lack of community understanding or concern regarding the topic [13]. Considering that these seven keyholders are anonymous, only a breach of protocol would reveal an adversary in the DAO's midst, and would potentially be catastrophic to the DAO's credibility.

Policy proposals that are accepted via the community are implemented via a quorum of five signatories who sign a transaction to open the Gnosis safe containing the private key allowing changes to the DAO's smart contracts. However, three of the five signatories can theoretically collude to open the Gnosis safe to alter the DAO's contracts, potentially opening a window of time in which the conspirators can alter the behavior of the DAO's mechanisms to benefit themselves. Again, these signatories remain anonymous within the DAO and it is unclear how they were vetted or chosen.

Tendencies Towards Oligarchy

Anonymity within a DAO may resonate with firm believers in the decentralization ethos of the broader cryptocurrency/Web3 crowd, but does little to instill faith in DAOs such as Olympus that are governed largely by anonymous figures. Furthermore, the common ethos of "trustlessness" in the Web3 community is predicated upon the concept of "code is law," where trust in individuals or institutions is replaced by smart contract finality and blockchain consensus. However, such an assumption is largely erroneous as trust is merely shifted from individuals who govern towards individuals who code; those who cannot fully understand the code that forms the foundation of a DAO ultimately place their trust in those who do. Furthermore, this trust extends beyond the first degree of smart contract security, as technical side effects may be born from unintended consequences resulting from complex smart contract architectures. Even those that understand the code at a lower level may not fully understand the resulting broader social and economic implications, leading to a situation where those who understand both the code at a literal level as well as the broader implications are in unique positions of power to manipulate the organization to their own benefit. Therefore, one of the simplest and most straightforward counterweights to such responsibility are based in reducing complexity across the board in order to maximize the number of individuals in the organization that possess a broad understanding of the DAO's technical, social, and political mechanisms.

Achieving such a counterbalance is likely incredibly difficult, because when the DAO grows large the ratio of such highly-attuned individuals will decrease. It may therefore be posited that in order to avoid oligarchical tendencies within a finance DAO, such a DAO must remain small in membership and maintain a high degree of technical capability within its membership.

V. DISCUSSION

Similar to the blockchain trilemma, DAOs face similar inherent trade-offs between decentralization, security, and efficiency. A DAO's decentralization is directly correlated to the "flatness" of the organizational structure, such that a more hierarchical structure leads to a higher degree of centralization around a smaller number of individuals in the organization. When a DAO prioritizes decentralization, often the first casualty is efficiency of governance such that flatter organizational structures have more disjointed and inefficient decision-making processes. Conversely, should a DAO prioritize efficiency, more decision-making power is concentrated around a smaller group of individuals (or around a single person) at the expense of security; these individuals wield disproportionate power over the DAO's governance and treasury. In this case, both decentralization and security are sacrificed for efficiency's sake. Therefore, decentralization and security are more intrinsically linked whereby any governance structure that is not purely direct democracy leads to a concentration of power that inversely affects the remaining two principles in the trilemma.

That being said, as a DAO grows large so too does the difficulty of scaling decision-making processes, assuming that every member wields equal voting power. However, potential avenues exist for DAO governance that may reduce (but not eliminate) the risk of treasury theft or oligarchical tendencies.

Wolves Guarding the Hen House

As decentralized finance continues to grow in market cap and evolve into a complex financial ecosystem, it becomes increasingly important for DAOs managing shared assets to properly engineer their governance mechanisms to avoid the many downsides of decentralization. The DeFi community's obsession with maximizing decentralization has several drawbacks, particularly when it comes to custody of shared assets. Many DAOs use time-locked cryptographic vaults such as Gnosis to store the private keys to shared wallets, but this provides little security if those who have access to the vault retain total control of the contents. When the vault is closed, the funds are theoretically safe from any interference or theft, but there is no technical limitation to preventing those with access from colluding to steal the contents. These time-locked vaults often operate under some kind of (k, n)-threshold scheme, requiring k of n keyholders to sign transactions - however if k keyholders collude, the funds are entirely at risk, meaning the DAO operates under some kind of trust scheme - the antithesis of the "trustless" ethos of decentralized finance.

In order to reduce amount of trust in specific individuals, DAOs with community-managed treasuries can hypothetically increase the number of keyholders k required to sign transactions to the point where collusion between keyholders becomes increasingly unlikely. However, this is not without its own drawbacks as both collusion and coordination of increasingly large groups of individuals becomes more difficult, and within a few short breaths we are back to discussing decentralized consensus mechanisms. It is appropriate, then, that the concept of decentralized consensus is critical not only to the technical security of decentralized networks and the DAOs that they support, but in a social governance manner as well. Should a DAO decide to be governed in a manner such that k of n community members have access to the treasury, deliberate and meticulous governance design is of paramount importance.

...

...

VI. CONCLUSIONS

REFERENCES

[1] *DefiLlama*, http://www.defillama.com/

[2] *MakerDAO Whitepaper*, https://makerdao.com/en/whitepaper/

[3] Liu, Cixin. *The Dark Forest.* Head of Zeus, 2016.

[4] Obadia, Alex and Vemulapalli, Taarush. *MEV in ETH2*, https://hackmd.io/@flashbots/mev-in-eth2

[5] Buterin, Vitalik. *Moving Beyond Coin Voting Governance,* https://vitalik.ca/general/2021/08/16/voting3.html

[6] Buterin, Vitalik. *On Nathan Schneider on the limits of cryptoeconomics,* https://vitalik.ca/general/2021/09/26/limits.html

[7] Haig, Samuel. "Investors Rug-Pulled after Pouring $57m into Dog-Themed Olympusdao Fork." *Cointelegraph*, 1 Nov. 2021, https://cointelegraph.com/news/investors-rug-pulled-after-pouring-57m-into-dog-themed-olympusdao-fork

[8] Malwa, Shaurya. "Wonderland Rattled After Co-Founder Tied to Failed QuadrigaCX Exchange." *CoinDesk*, 22 Jan. 2022, https://www.coindesk.com/markets/2022/01/27/wonderland-rattled-after-cofounder-tied-to-alleged-quadrigacx-190m-exit-scam/

[9] *Gnosis Safe*, https://safe.global/

[10] Fernau, Owen. "OlympusDAO's Success Inspires Dozens of Forks", *The Defiant*, 26 Oct. 2021, https://thedefiant.io/olympusdao-forks

[11] *OlympusDAO Audit Reports*, https://www.olympusdao.finance/audit-reports

[12] *Olympus Pro*, https://docs.olympusdao.finance/pro

[13] *OlympusDAO Proposals*, https://snapshot.org//olympusdao.eth