COMS 6998 Final Project

Utkarsh Sinha, Sofia Bianchi, Ian Macleod, Imanol Uribe UNI: us2187, srb2225, idm2114, iu2155

December 18, 2021

Introduction

DAOs, or Decentralized Autonomous Organizations, are effectively pools of shared, crowd-driven capital collectively owned and managed by their members. In simplistic terms, DAOs are smart contracts deployed on blockchains such as Ethereum that can be used for a multitude of different projects that require or benefit from a trustless setting. DAOs function as decision engines that operate based on the collective will of stakeholders; because they are so broadly defined, they can be implemented across a broad variety of different sectors and use cases where trust assumptions between parties are weak and can be used for governance, funding, and more. DAOs are fascinating from an economic perspective because they allow individuals to pool resources and collectively access almost unfathomable leverage (some DAOs have been designed to function similarly to risk-free special purpose acquisition companies (SPACs), where all stakeholders' money will be returned to them if the acquisition fails to go through). Additionally, DAOs are intriguing from a political perspective because they present novel governance structures. Most importantly, DAOs are appealing to computer scientists as engineering feats that wield the power of blockchain protocols to create transparent, elegant organizations.

Motivation

As we enter into a new tech frontier in 2022, made possible by the crystallization of blockchain technology in recent years, DAOs, or decentralized autonomous organizations, are becoming increasing relevant for the world of web3-based applications. But what exactly are DAOs? Cara Wu and Chris Dixon of Andreesen Horowitz define them as, "internet-native, global collectives that share resources, build products, and work together towards common goals." In other words, DAOs are organizations whose origins are the web, and whose rules and terms of membership are orchestrated by code-backed protocols, rather than large institutions and "middleman" organizations.

Until recently, DAOs had scarcely been leveraged beyond a means of security for decentralized-finance protocols in the case of Bitcoin or Ethereum. Now, DAOs are being hailed as an integral means of developing web3 applications. For approximately a decade, the landscape of web2 has caused issues of digital ownership and distribution for artists and creatives. Through the creative implementation of DAOs, it is possible to carve a new frontier for digital monetization by eliminating the third party members who tend to benefit most from the popularity of the creator's product or service.

Use Cases of DAOs

DAOs as special purpose acquisition companies

This may be one of the most naive and intuitive implementations of a decentralized autonomous organization, but nonetheless it's worthwhile to mention the power of DAOs to fundraise large amounts of capital across many different parties without the need for any centralized trust assumptions or a mutually agreed

upon treasurer. In 2020 and 2021, special purpose acquisition companies were extremely popular on US-based stock exchanges, with SPAC initial public offerings generating over 600% more investment in 2020 than in 2019 (and far eclipsing previous years as well). [1]. However, SPACs are centrally governed by boards of directors; US regulatory requirements stipulate that SPACs have at least 3 directors, meaning that all shareholders must rely on the expertise and decision making of a small, centralized group of people who are in charge of deciding which company the SPAC should acquire.[2] This effectively divests shareholders of their ability to control their funds, and many SPACs have also been plagued by ambiguity and bad decision-making at an executive level, leaving shareholders with little to show for their investments. The design of DAOs deployed on blockchains is fundamentally different because DAOs are basically computer programs (smart contracts) that are transparent for all to see and their behavior mechanisms are well-defined from the outset.

DAOs use voting mechanisms that allow stakeholders to have a vote (in a simplistic voting mechanism, the weight of the vote is proportional to the size of the stake as a fraction of the total pool of capital), meaning that acquisition-based DAOs are governed, to a degree, by all of their investors. Additionally, the benefits inherited from blockchain protocols such as Ethereum, which provide guarantees about the immutability of the code of deployed smart contracts and offer decentralization without the need for trust assumptions, allow many group acquisition based-DAOs to collect funds and then return them if they don't reach an agreed-upon goal. One SPAC-like DAO that recently made headlines is ConstitutionDAO, which raised over $47 million within a week to buy a rare copy of the US Constitution from $\approx 17,437$ individuals.[3] ConstitutionDAO was ultimately outbid at a Sotheby's auction and offered all of its shareholders the opportunity to exchange $PEOPLE tokens (the DAO's native currency) for ETH at the same fixed rate they invested at, allowing stakeholders to get their money back (minus fees). The sheer speed at which you can create an organization, raise almost $50 million in crowdsourced capital, and then dissolve if the organization's goals are no longer viable is only possible within a trustless, decentralized setting; in this sense, DAOs are poised to disrupt non-profits, investment corporations, and many other types of organizations that manage contributions from the public.

DAOs as digital communities

Another possible use case for decentralized autonomous organizations is the emphasis on decentralized governance to create and maintain communities. This scenario already exists and arises naturally in many social situations: consider a tight-knit friend group that meets someone new and subconsciously decides as a collective whether or not they want the new person to join their friend group. This concept can be codified on blockchain protocols through the use of DAOs, where digital communities can form and entry can be contingent on alignment with the group's collective values and goals. One such example is Friends With Benefits, a DAO that calls itself "a digital city" designed for creative people working with web3.[4] Joining the DAO and being a member requires both a written application, which the community itself reviews and votes on, and a buy-in of $FWB tokens. The pool of capital that Friends With Benefits accrues from entry fees is then managed collectively and can be used for funding various projects. In an ideal design, the financial cost of joining the DAO is far lower than the opportunity cost of not joining because members have access to the collective resources and knowledge of the community (which are presumably far more valuable than the entry fee).

DAOs as a tool for Governance

DAOs have emerged as a powerful tool for the governance of existing organizations. It is easy to see why they are compelling alternatives to more traditional governance structures. DAOs democratize the governance of an organization and ensure that the future steps of the organization truly reflect the desires of the majority

[1] the exact statistics for SPAC growth can be found here: https://www.statista.com/statistics/1178273/size-spac-ipo-usa/

[2] https://www.spencerstuart.com/research-and-insight/board-governance-and-spacs-new-competition-for-capital-and-talent

[3] https://www.constitutiondao.com, also see here: https://twitter.com/ConstitutionDAO/status/1461527516670316544?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1461527516670316544%7Ctwgr%5E%7Ctwcon%5Es1_

[4] https://a16z.com/2021/10/27/investing-in-friends-with-benefits-a-dao/

rather than the goals of a select few. In order to accomplish this decentralized voting, many DAOs have native tokens for governance that they can mint or issue (either as proof of stake rewards or in exchange for a set amount of capital in another cryptocurrency such as $ETH). Anyone with any amount of governance tokens has a say in the future of the DAO project. Governance appear to be one of the most generalizable applications of DAOs; one could even envision a future where entire governmental elections are held on-chain with the power of DAOs where each citizen is issued one token that they can vote on a candidate with; for countries that have trouble securing election integrity, on-chain voting mechanisms that ensure that every vote cast is verifiable would be able to enable new forms of digital democracy.

Examples of DAOs

MakerDAO

One clearly successful implementation of a DAO-based governance architecture is MakerDAO, an algorithmic stablecoin-based lending platform that offers $DAI in exchange for users' assets. The DAO uses the token $MKR as a governance token that allows for weighted voting (each individual shareholder has a vote directly proportional to their share of the total pool of MKR tokens). MKR tokens are available on public exchanges, so anyone who wants to have a vote in the governance and future actions of MakerDAO is enabled to become a shareholder in the company via the acquisition of MKR tokens. In this sense, MakerDAO is analogous to a publicly-traded company whose board of shareholders vote on future decisions for the company; however, the clear contrasting difference is that the MakerDAO shareholders are all pseudo-anonymous and the organization operates perfectly well even when they have no knowledge of one another. The MakerDAO governance structure employs two main types of on-chain votes for coming up with new decisions: Governance Polls and Executive votes.[5] Governance Polls are used as litmus tests to measure the sentiment of MakerDAO stakeholders on different decisions. There can be many polls at the same time, can be created by anyone by using the polling smart contract available in the deployed MakerDAO contract, and stakeholders can vote on as many as they want. These polls are straightforward and sentiment is assessed based on the total amount of $MKR associated with a vote. In order to give a concrete example, consider a question MKR holders might be voting on: *whether or not MakerDAO should accept NFTs as collateral when minting DAI.*[7] This decision will be represented as a binary decision with 1 representing yes and 0 representing no. We can formalize the computational procedure for vote tallying as follows, where S represents the set of all stakeholders who cast votes on the poll, $\alpha_s \in (0, 1]$ represents an individual shareholder's share of the total pool of MKR tokens, and $v_s \in \{0, 1\}$ represents their vote:

$$sentiment = \frac{\sum_{\forall s \in S} \alpha_s * v_s}{\sum_{\forall s \in S} \alpha_s}$$

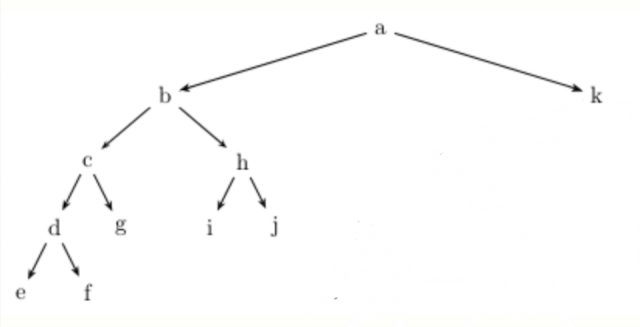
This summation ultimately yields the amount of $MKR staked in favor of the proposal as a fraction of the total amount of $MKR staked by all of the voters on the proposal; if $sentiment > .5$, then there is a simple majority (of the population that voted on the poll, which is often reflective but not necessarily identical to the same total population of stakeholders since the voting population for any given poll is a subset of the total number of stakeholders) in favor of allowing NFTs to be used as collateral for minting $DAI. Further, if $sentiment > .67$, then there is a supermajority in favor of the proposal. We can visualize a simplified decision tree for a series of proposals - all binary decisions - as a left-deep binary tree, where the series of questions posed to the DAOs voting body could be as follows:

Should NFTs be accepted as a viable source of collateral? Should we use the same collateralization parameters for NFTS as for other assets (if no, then another binary with new proposed parameters 1.75 or 2)? Should we continue to use the same price oracles should we use for NFT prices? (if no, then there would be voting on alternative proposals for different price oracles).

[5] `https://makerdao.world/en/learn/governance/how-voting-works/#governance-polls-and-executive-votes`[6]

[7] As it turns out, this question is actually quite an interesting one that is being explored currently. `https://blog.makerdao.com/how-ethereum-smart-contracts-power-dai-the-maker-protocol-and-defi/`

Figure 1: An example of a binary decision tree (every left edge represents a yes to a proposal that occured at a given level of the tree, whereas a right edge represents a no).



MakerDAO Voting Classes

Admittedly, the above tree is an oversimplification of the true complexity of MakerDAO's voting system. It's also important to note that there are two different classes of votes in MakerDAO's implementation: Governance Polls and Executive Votes. A table of the use cases of Governance Polls and Executive Votes is shown on the next page. In general, one could consider Governance Polls as sentiment-based analyses that allow for the proposal of Executive Votes that reflect the popular majority. The two voting schemes have different time scales and different voting consensus protocols.

Governance Poll	Executive Vote
Determine governance and DAO processes outside the technical layer of the Maker Protocol. (*)	Add or remove collateral types.
Form consensus on important community goals and targets.	Add or remove Vault types.
Measure sentiment on potential Executive Vote proposals.	Adjust Vault-specific parameters.
Determine which values certain system parameters should be set to before those values are then confirmed in an executive vote.	Adjust global system parameters.
Ratify risk parameters for new collateral types as presented by Risk Teams. (*)	Replace modular smart contracts.

All of these voting objectives are important, and MakerDAO uses a simple majority for the items denoted by asterisks. However, MakerDAO doesn't actually use Governance Polls to finalize critical decisions but instead tracks the sentiment of stakeholders over time through the use of these polls, this information is informative and allows individuals to gauge interest in an idea before proposing an Executive vote.

An Executive vote is similar to a Governance Poll in many regards – it occurs on chain and can be proposed by anyone via a call to the deployed MakerDAO smart contract – but differs in that Executive votes use continuous approval voting. Furthermore, all of the Executive vote changes have the potential to fundamentally alter the future directions of MakerDAO and change the creation of $DAI, change the assets accepted as collateral, or change the collateralization rate required for assets. Thus, the continuous approval voting system is designed to mitigate the risks of drastic changes or bad ideas that would damage the $DAI ecosystem. The voting system is designed such that there is a list of proposals that are being considered for Executive votes, and stakeholders who vote for an Executive vote with some amount of $MKR have locked their $MKR into the governance system and must change or withdraw their support from the current

proposal that their $MKR is staked in to be able to support a new proposal. This design mechanism is quite idiosyncratic as compared to other voting methods employed by DAOs, but it is pragmatic for MakerDAO for the following reasons.

- Every vote creates a barrier for new proposals.
- Since votes ($MKR stakes) remain in the system continuously, bad proposals are less likely to pass because they would require the reallocation of votes from currently supported proposals (the status quo) to the new bad proposal.
- As the amount of $MKR staked in the Executive vote pool increases, the probability that a rogue proposal passes decreases.

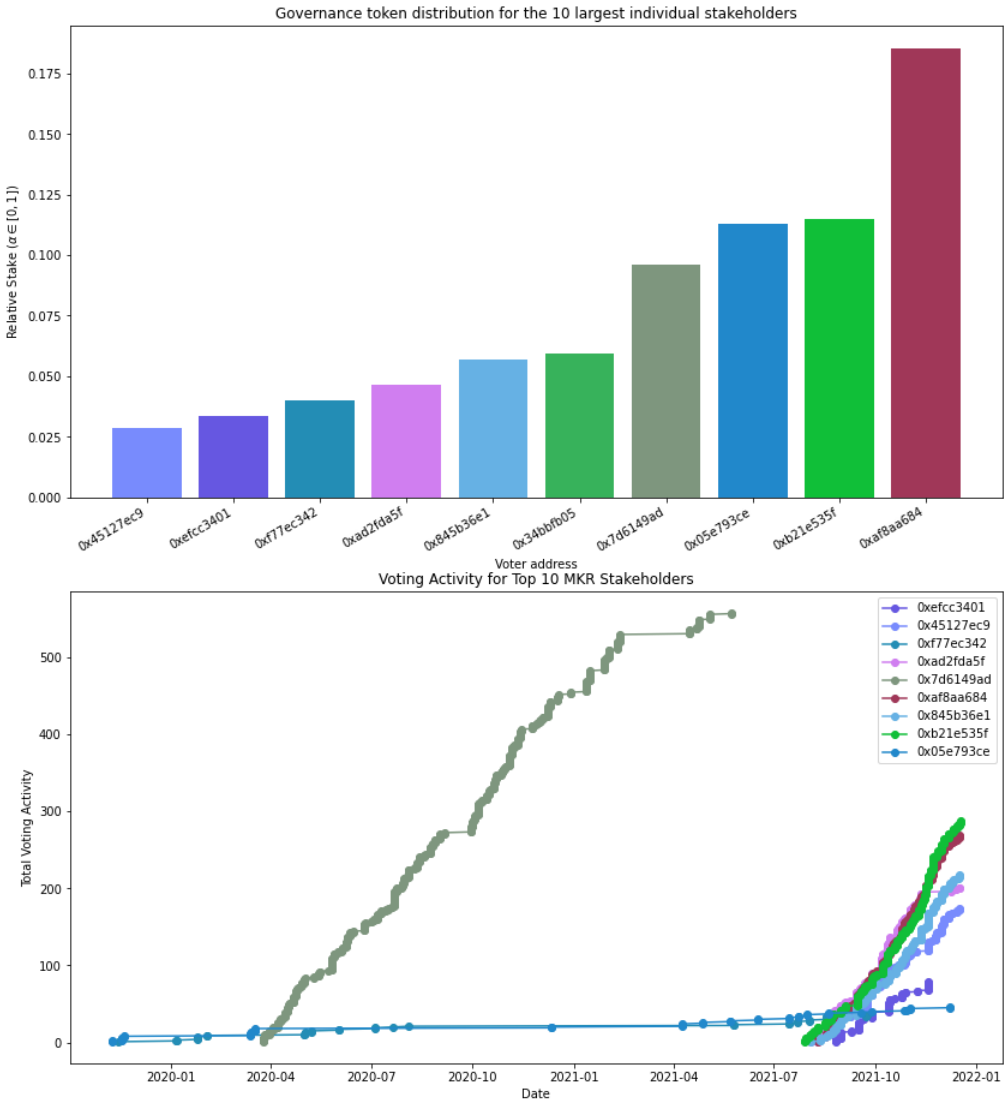
The Executive vote proposal with the largest $MKR stake is the the current status quo in the MakerDAO ecosystem. Anyone can propose a new Executive vote proposal, but the proposal will only be ratified if the MKR token holders that are responsible for the governance of the system and the stability of the peg of $DAI collectively agree that the new proposal is beneficial. This means that the current staus quo will always be defending against any new proposals, and any proposals that are bad or that seem antithetical to the prudent governance of the system are extremely unlikely to garner majority support because this would require stakeholders to change their allocation of $MKR. Additionally, since Executive votes all occur on chain, the votes are secured by the underlying blockchain protocol and the voting record of every stakeholder is publicly available.[8]

Brief analysis of MakerDAO voting activity

In order to more accurately gauge the real-world health of the MakerDAO voting ecosystem, we performed an analysis of the top stakeholders in the system to assess their voting activity over time (although MakerDAO does not require a quorum, it is still interesting to see how funds flow between proposals across time. We used an open-source analysis tool[9] to get CSV data that then yielded the plot shown on the next page (Figure 2). The results from the figure are quite encouraging with regard to the health of the MakerDAO ecosystem. Based on these results, it is clear that "whales" who own large stakes ($\alpha \approx .05$ or something higher) in $MKR are generally very active in voting. It also appears that MakerDAO has garnered recent interest, with stakeholders who began holding $MKR as recently as July 2021 now comprising a significant amount of the voting activity among the top 10 stakeholders. One somewhat remarkable fact is that one whale, the wallet address **0x34bbfb05839c52e9c0356816dca211a55c6d0942**, owns 5.94% of the total governance tokens but has never voted! Additionally, it is clear to see that the top 10 $MKR governance holders have 77.45% of the total governance tokens in the MakerDAO ecosystem. One potential attack vector that is worthwhile to consider if the total share of governance tokens continues to concentrate in the hands of the few is the potential for collusion among whales; however, this attack vector can generally be written off as economically not viable because whales who own $MKR governance tokens would potentially devalue their own stakes through collusion.

[8] https://github.com/makerdao/community/blob/master/faqs/governance.md#what-is-continuous-approval-voting
[9] https://beta.mcdgov.info

Figure 2: A graph of the relative voting share of the 10 whales and the total history of their voting activity. Please note that all voter addresses to the first ten characters have been truncated for visual clarity. Code here: `https://github.com/idm2114/blockchainProject`.



OlympusDAO

Whereas MakerDAO embraces current financial structures and attempts to create a blockchain-based analogue (the algorithmic stablecoin $DAI) to an existing currency (the US dollar), OlympusDAO actively defies traditional, fundamentalist economics and purports to create its own store of value entirely independent from current economic currencies. On the OlympusDAO website, they claim that "a true Store of Value doesn't exist–yet. Stablecoins are vulnerable to inflationary policies, while Bitcoin or Ethereum suffer from market crashes or manipulation. None of these is a true Store of Value."[10] This proclamation is admittedly quite bold; while it is true that the U.S. dollar is not a source of intrinsic value, it is recognized around the world as the de facto global currency.[11] Additionally, the proclamation that OlympusDAO's financial system is

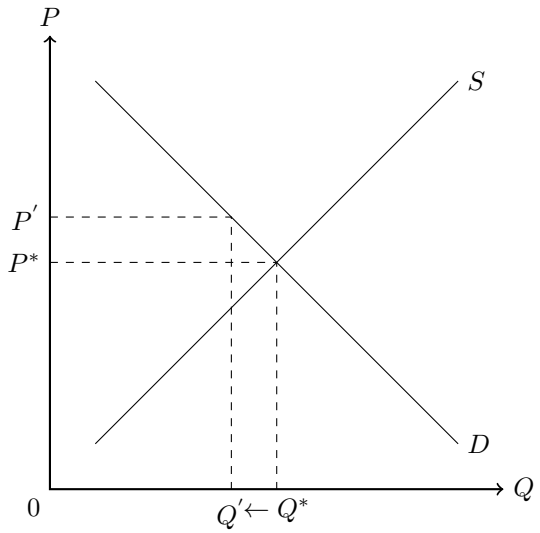
[10] `https://www.olympusdao.finance`

[11] The United States has issued 7.55 trillion dollars in treasury notes to other countries, and the 10- and 30-year Treasury notes continue to be viewed as some of the most stable financial securities instruments for foreign governments. `https://www.statista.com/statistics/246420/major-foreign-holders-of-us-treasury-debt/`

radically different than existing financial systems is somewhat wrinkled by the fact that OlympusDAO is backed by the MakerDAO-issued algorithmic stablecoin $DAI, which in turn is pegged to the U.S. dollar, so it is somewhat ironic that OlympusDAO actively distances itself from and rejects existing currencies as not being innate stores of value when it itself is backed by said currencies. Irony and philosophical questions about "innate" stores of value aside, the protocols behind OlympusDAO are technologically fascinating and serves as an interesting counterpoint to the other DAO that we explored, MakerDAO. Whereas MakerDAO represents an algorithmic approach that attempts to guarantee stability, OlympusDAO seems to be a largely faith-based approach that has the potential for convergence to a stable value at some point in a long-term future time horizon.

OlympusDAO: Ponzi Scheme or Panacea

OlympusDAO is an extremely polarizing blockchain project; some people view the DAO as an extremely high-yield financial investment while others look at the token as a Ponzi Scheme in the making that will inevitably crash.[12] According to the creators the DAO, OlympusDAO aspires to create an intrinsic store of value. In practice, this value creation begins with the acquisition of $DAI – each $OHM is backed by 1 $DAI, but it is not a 1 to 1 peg; instead, the price is modeled as follows: 1 OHM $\geq$ 1 DAI. OlympusDAO plans for its algorithmic currency, $OHM, to stabilize and establish a price floor eventually; currently, however, it embraces volatility as part of it's purported "growth" phase. OlympusDAO proclaims that its initial goal is "not to find a stable price. This may seem antithetical to our currency aspirations, but we ensure it is not. (...) The main tradeoff is volatility and profitability versus stability and consistency. With volatility and profit comes growth; this is what we want early on."[13] Additionally, OlympusDAO promises extremely high-yield returns for stakeholders on the order of 4,500% APY. OlympusDAO generates wealth through two processes: staking and bonding. Staking is the primary accrual method for Olympus and requires that individual stakeholders (owners of $OHM) give their assets back to the protocol by re-investing them into Olympus. The staking process involves a 1:1 exchange of $OHM to $sOHM. This process basically reduces to locking up $OHM within the Olympus ecosystem (trivially, one can observe that it is guaranteed that the price can never fall relative to other currencies if no one ever sells $OHM). The second mechanism for accruing value that OlympusDAO employs is bonding, which allows the $OHM to build reserves in the treasury by selling $OHM at a discount in exchange for other assets such as $DAI. Whereas the first mechanism basically just inflates the price of $OHM artificially by taking currency out of circulation, the second mechanism involves swaps of $OHM for other, more stable currencies to create a asset bundle in the treasury that provides both liquidity and stability to the currency.[14] OlympusDAO's staking mechanism creates inflationary pressure on the value of the $OHM currency.



[12] https://www.coindesk.com/policy/2021/12/05/olympus-dao-might-be-the-future-of-money-or-it-might-be-a-ponzi/
[13] https://twitter.com/RyanWatkins_/status/1447404527326580736/photo/1
[14] https://docs.olympusdao.finance/main/basics/bonding

This diagram shows that the effects on price as a result of a reduction in quantity from Q^* (the equilibrium quantity of \$OHM in circulation) to Q' after the result of an individual stakeholder staking their \$OHM by returning it to the treasury. This action of returning the cryptocurrency effectively amounts to taking the currency out of circulation. One thing that's interesting to consider – and a notion that OlympusDAO has posited that challenges many foundational ideas of economics – is the question of whether or not the currency being taken out of circulation by staking will lead to an inflationary spiral followed by a crash or if it will eventually lead to the stabilization of the price at some new equilibrium price P'.

Is OlympusDAO truly a DAO?

One interesting point to note regarding OlympusDAO is that its voting consensus mechanism is not designed to scale or allow for potentially universal participation. Unlike the MakerDAO contract, which allows for any stakeholder to propose changes to the protocol that can then be voted upon using the governance tokens \$MKR, OlympusDAO has no governance token and is instead constructed with a permissioned majority model that uses a 4 of 7 multisig involving seven whitelisted actors. In this sense, OlympusDAO's governance hews much closer to that of a company with an executive board than a distributed, democratic voting style. Nonetheless, it is worthwhile to note that the protocol plans to make the transition to a fully on-chain DAO "soon." [15]

Different Voting Mechanisms for DAOs

It is worthwhile to discuss some of the different voting mechanisms available for DAOs that are deployed in practice today.

Token-based Quorum Voting

Quorum voting requires a certain threshold of "voters" in order for a proposal's vote to be valid. In reality, this threshold is computed not as a number of voters but as a function of the share of the total amount of governance tokens that are in existence. For example, if a DAO had a 60% quorum, 60% of the governance tokens would need to be allocated in yes or no votes on a given proposal for the proposal to be considered and the resulting majority decision from the vote to be ratified. Let S represents the set of all stakeholders who cast votes, t_s be the number of tokens an individual stakeholder owns, T be the total number of governance tokens available in the ecosystem, $v_s \in 0, 1$ represents the individual stakeholder's vote (either yes to new proposal or no to new proposal), and $q \in [0, 1]$ be the quorum threshold. We can generalize this process in the following algorithm:

if $\frac{\sum_{\forall s \in S} t_s}{T} > q$ and **expiretime == TRUE then**

  if $\sum_{\forall s \in S} t_s * v_s > \left[\sum_{\forall s \in S} t_s - \sum_{\forall s \in S} t_s * v_s\right]$ **then**
    the vote passes (more people voted yes than no)
  else
    the vote fails
  end if
else
  the vote fails to reach quorum

This implementation is quite familiar as it loosely reflects the democratic process used for political elections today. However, it's worthwhile to point out that the variation in the parameter q enables different quorum levels that guarantee participation from the voting body. For example, the Curve DAO requires 30% participation for any given proposal by setting $q = .3$. [16] One potential danger of quorum-based voting is that if ownership of governance tokens is heavily concentrated (i.e. there are some "whales" that own significant portions of the total share of governance tokens), a quorum threshold q that looks quite secure, like .3, could be artificially low if the combined voting power of a few whales surpasses the threshold.

[15] `https://docs.olympusdao.finance/main/contracts/dao`
[16] `https://curve.readthedocs.io/dao-ownership.html`

Setting a value for q that is low, like $q \leq .20$, yields a coarse approximation for the true majority opinion on any given proposal. Of course, $\lim q \to 1$ will yield the most accurate results and reflect the true majority opinion on a proposal, but setting a threshold close to 1 would be highly impractical because it is unreasonable and inefficient to expect full voting participation from all stakeholders on every proposal.[17] Even at a threshold of $q = .3$, Michael Egorov, the CEO of Curve, remarked that "voting does turn into a game of chasing whales".[18] Some DAOs that employ this voting consensus protocol include Curve, Compound, and Kleros.

Conviction Voting

Conviction voting is based on the idea that continuous sampling of the allocation of different governance tokens on different proposals will yield a sense of how much an individual stakeholder cares about a proposal.[19] This notion is loosely related to MakerDAO's consensus mechanism because it involves voting stakes that are continuously present and can be reallocated by moving or switching stake from one proposal to another. The difference with conviction voting than MakerDAO's continuous approval voting is that conviction voting employs an exponential decay function that increases the weight of an individual's stake based on the amount of time that they have left their stake allocated on one proposal. The idea stems from a paper describing "Social Sensor Function" by Dr. Michael Zargham.[20] We replicate the mathematical derivations shown by Dr. Zargham below (note that all credit for the following derivations goes to Dr. Zargham and that we are presenting them here for completeness).
Let x be the observable system state and p_t^i be the preferences of each individual i at time t. We can define a local estimator $y_i^t = E(x_t, p_t^i)$ for each individual stakeholder $i \in \mathcal{I}$ as well as a global decision function $c_t = D(\vec{x_t}, \vec{y_t})$ that represents the choice for each time step. For simplicity, we will assume that the preference of each individual stakeholder $p_t^i \in \mathcal{C}$ belong to the same domain as each choice c_t. Let $t =$ block time and x_t^i be the stake of an individual shareholder at a given block time. Dr. Zargham defined the conviction voting algorithm as follows:

$$y_t^{i,c} = \begin{cases} \alpha * y_{t-1}^{i,c} + x_{t-1}^i & \text{if } c^i = c \\ \alpha * y_{t-1}^{i,c} & \text{if } c^i \neq c \end{cases}$$

Decisions from the algorithm are then represented as an optimization problem where we are choosing the choice that has the maximum sum of all of the convictions across all individuals for that choice at that given time step.

$$c_t = \max_c \sum_{i \in \mathcal{I}} y_t^i$$

A visualization of the results of a conviction voting simulation is shown below in Figure 3. Some DAOs that employ this voting consensus protocol include 1Hive, Panvala, and Commons Stack.

Holographic Consensus

Holographic Consensus is a concept that was first introduced and developed by DAOstack, one of the DAO tooling platforms that will be elaborated on later in this paper. The Holographic Consensus voting mechanism creates a prediction market with each proposal. Predictors can stake funds for or against a proposal they believe will pass or fail. If a predictor who stakes their coins on an outcome predicts correctly, they benefit financially. Proposals that are predicted to pass (i.e. have a prediction market with more money staked on passing than failing) are "boosted" and voting switches from 50% quorum to relative majority, making the barrier to pass proposals much lower than proposals that don't have funds staked on them. One reason that holographic consensus is appealing as an alternative to quorum-based voting mechanisms is that the holographic consensus voting mechanism naturally protects projects from

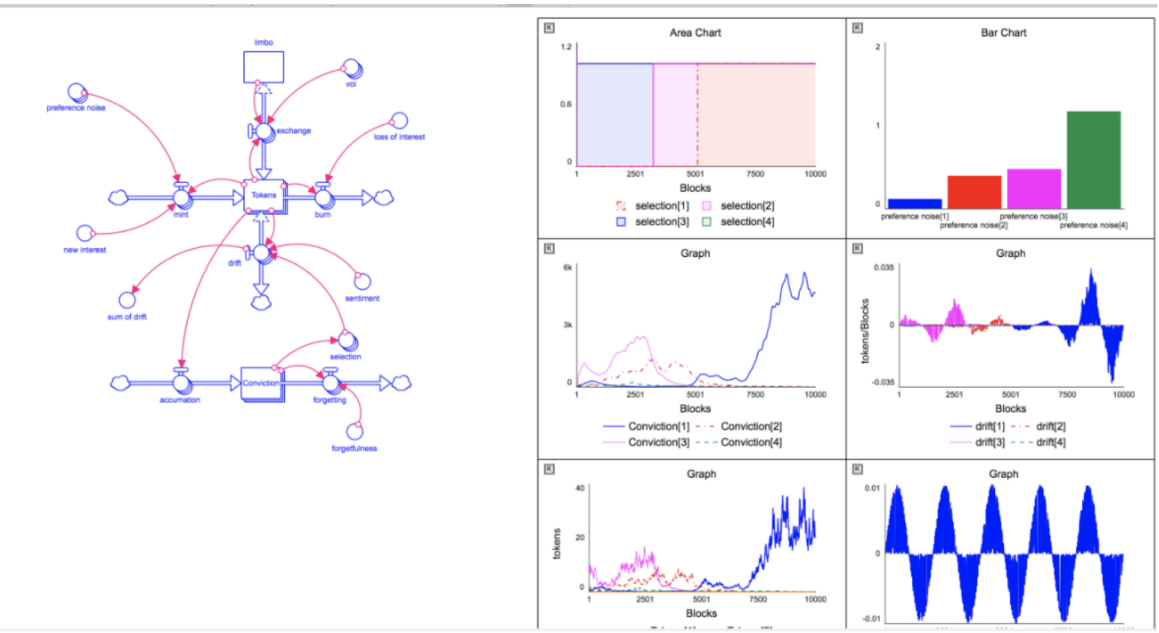
[17] For context, the voting turnout among registered voters in the 2020 US presidential election was 66.9%, a record high but still far short of 100%. https://en.wikipedia.org/wiki/Voter_turnout_in_United_States_presidential_elections

[18] https://medium.com/daostack/voting-options-in-daos-b86e5c69a3e3

[19] https://medium.com/giveth/conviction-voting-a-novel-continuous-decision-making-alternative-to-governance-aa746cfb9475

[20] https://github.com/BlockScience/conviction/blob/master/social-sensorfusion.pdf

Figure 3: A simulation of an ordinary differential equation-based conviction voting algorithm generated by Dr. Zargham.



nefarious proposals; this follows from the fact that any bad actor would need to stake funds on their own rogue proposals in a prediction market and would open themselves up to financial loss if they predicted incorrectly. This consensus design works well for projects that have many proposals because it uses the notion of free-market consensus (no barriers to entry, and the best ideas will garner the most economic support) to determine which proposals are the most important based on the size of their associated stake in prediction markets. Additionally, this consensus mechanism is potentially better than quorum-based consensus because it can eliminate reliance on the "whales" in a DAO's governance structure participating in votes for a given proposal (since if the prediction market suggests that the proposal will likely pass, the quorum threshold q is no longer necessary). This means that good proposals can theoretically pass more quickly. Some DAOs that employ this voting consensus protocol include PrimeDAO and DXdao.

Lazy Consensus

Lazy Consensus is one of the most interesting consensus approaches for voting on new proposals in a DAO's governance structure. It is similar to the idea of an optimistic roll-up in the sense that anyone can immediately motion for a change to occur; if no one objects to it within a given timeframe T, then the change is ratified. However, if someone objects to the proposal, a round of relative majority voting ensues. This system was first designed by Colony and is outlined in their whitepaper, where they suggest a time period of 3 days and use reputation-based slashing and staking system akin to the ETH-based slashing and staking system used in optimistic rollups.[21] Since this consensus mechanism is quite new, Colony is one of the only known DAOs experimenting with lazy consensus.

DAO Tooling

Like many other blockchain developments over the past decade, DAOs had extremely high technical barriers to entry and creation in their inception, requiring a high degree of knowledge about on-chain programming and vigilant programmers who ensure that all deployed contracts are safeguarded against exploitation. This level of technical expertise bars the average person from creating a DAO. However,

[21] Specifically, the lazy consensus model is introduced in section 3.4 of the whitepaper: https://colony.io/whitepaper.pdf

just as the internet grew from a research project to a highly accessible tool that required zero knowledge of underlying mechanisms due to abstractions, DAOs will eventually need to transition to become more user-friendly for aspiring creators without technical knowledge. DAO Tooling, also referred to as DAO Operating Systems, looks to solve this problem by creating modular solutions that can simplify the creation and management of DAOs to ensure that non-crypto-native people are also able to start and run their own DAOs. This requires a simplification from writing smart contract code to using a web interface for the initialization and management of a DAO. There are currently three dominant players in this space - Aragon, DAOstack, and DAOhaus.

Aragon

Founded in 2016 by Luis Cuende and Jorge Isquierdo, Aragon is a software which offers an open source infrastructure used to create and manage DAOs on the Ethereum blockchain. On the DAO deployment platform users can deploy DAOs for a variety of purposes, including virtual worlds, fashion houses, De-Fi protocols, hacker collectives, and subreddits. With DAOs deployed through Aragon's user-friendly interface, DAO stakeholders can attract contributors, pool capital, and govern transparently by leveraging unique, seamless governance plugins. [22]

DAOstack

DAOstack is a modular open-source software stack for DAOs intended to fill the many use cases of web3 developers. DAOstack offers a library of governance protocols paired with friendly user interfaces for generating and managing DAOs. DAOstack offers their services for a variety of template use cases, including grants DAOs for managing existing shared assets; decentralized, DAO-controlled mobile and web applications which can serve a wide variety of purposes; physical DAOs, or management of shared spaces; and alliance DAOs, for sharing terms of coalition towards common causes, such as legal protection and environmentalism.[23]

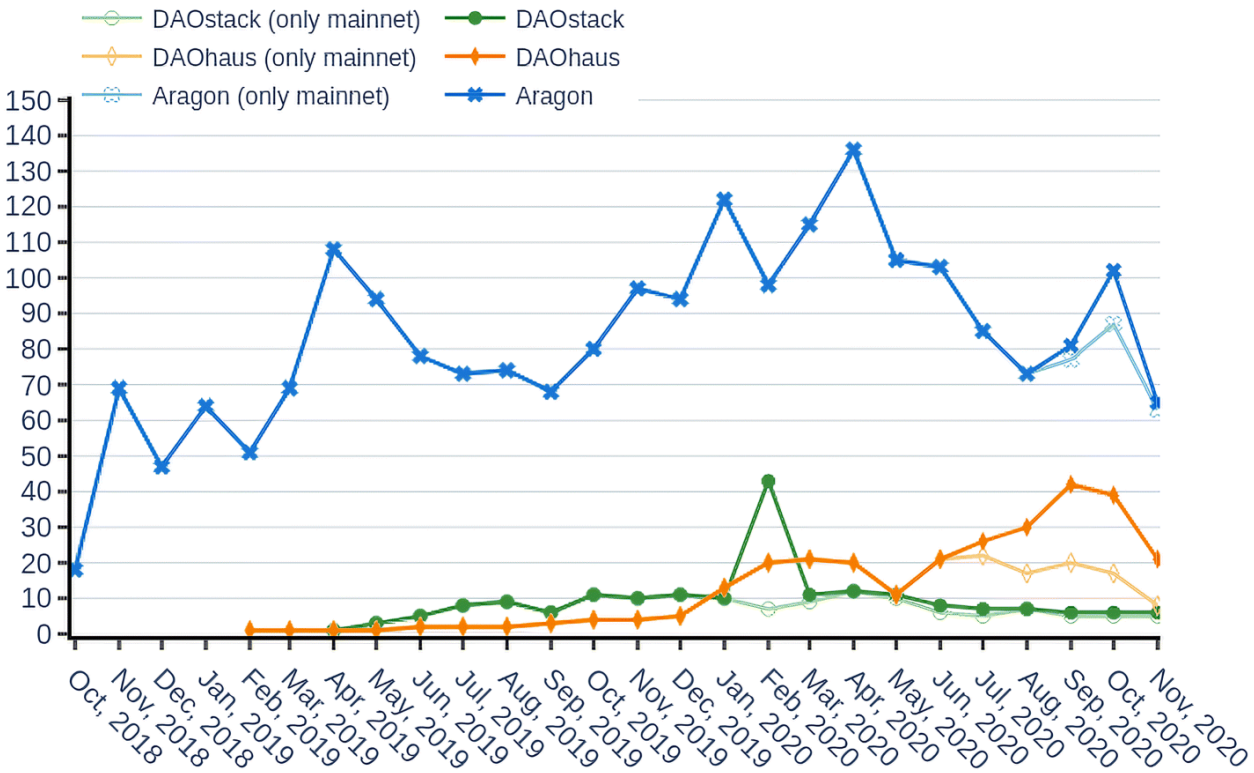
DAOhaus

DAOhaus brands themselves as a "DAO to DAO" economy, a DAO services space built by a DAO, meant for other DAOs, for the purpose of creating new DAOs. Intrinsic to its purpose is to cultivate a social network for the metaverse, founded on metaverse principles of decentralization. DAOhaus emphasizes the transformation of workspaces by allowing freelancers to join forces and to enjoy its elimination of top-down decision making; an outdated tradition long-adopted by corporate culture; through the shared economy of its user-driven decision making process. In many cases, this eliminates the concept of a "salary", as all contributors of a DAO are rewarded on a value-provided basis determined by the DAOs smartcontracts.
Shared by all communities on the platform is the HAUS token. The HAUS token is the native token of DAOhaus, launched in March of 2021. The HAUS token is mainly distributed by a 'Proof of DAO' mechanism. There is a total supply of 1,000,000 HAUS, with a circulating supply of 387,000 HAUS. 605k HAUS belongs to UberDAO, the umbrella DAO controlled by HAUS other DAOs, to be governed by the community. Remaining HAUS may be distributed in a variety of ways, including Mechanism Farming, Delegate/Voting incentives, Liquidity incentives, and Governance mining.
Most DAOhaus contributors belong to at least one of the four main circles of DAOs on DAOhaus, and anyone can become a contributor with no prior qualifications or requirements. These circles are Mage-smiths; or builders, coders who take on the technical responsibilities of DAOhaus; Rangers, or writers, and media creatives; Alchemists, or developers of governance protocols; and Paladins, the project organizers, workshop schedulers, and budget designers of the DAOhaus. Lastly, DAOhaus is currently developing a marketplace, which is coming soon.[24]

[22] urlhttps://aragon.org/
[23] urlhttps://daostack.io/
[24] `https://medium.com/daohaus-club/haus-launch-bd781bbbf13a`

A comparative analysis of the user distribution across DAO Operating Systems

Figure 4: A comparative graph showing the relative popularity of the three different main DAO Operating Systems based on adoption as of November 2020 can be seen below. The image was generated by Youssef Faqir-Rhazoui et al and reflects the total number of DAOs that use each of the different operating systems. https://jisajournal.springeropen.com/articles/10.1186/s13174-021-00139-6



Dangers of DAOs

Up until this point, we've focused almost exclusively on the positive transformative effects of DAOs. However, they are not perfect, and even DAO optimists must acknowledge that there are potential dangers associated with DAOs. In fact, a malicious exploit in the Solidity code of one of the most popular DAOs of all time, The DAO, led to over $50 million in Ethereum being stolen in 2016 and was only restored through a hard fork of Ethereum that resulted in Ethereum Classic and Ethereum diverging.[25] At one point, The DAO's smart contract locked up 14% of all Ethereum in circulation, and the exploit itself revealed the very real vulnerabilities with flawed code for DAO smart contracts. Although an exploit of this magnitude will likely never occur again, it was a critical juncture for DAO development and demonstrated the ways in which malformed DAOs or DAOs that are vulnerable to exploits could have tremendous ramifications, not just for individual stakeholders in a given DAO but for the entire ecosystem of longest-chain blockchains.[26] Truly anyone can make a DAO, so over the next few years it will be interesting to see if the free-market phenomenon of separating the best from the rest will prevail. There are many DAOs today that defy fundamentalist economics, such as OlympusDAO. Additionally, there are many thorny legal issues that regulators must contend with in coming years, such as whether or not DAO tokens (either governance tokens or native tokens issued as currencies, as is the case with $OHM) should

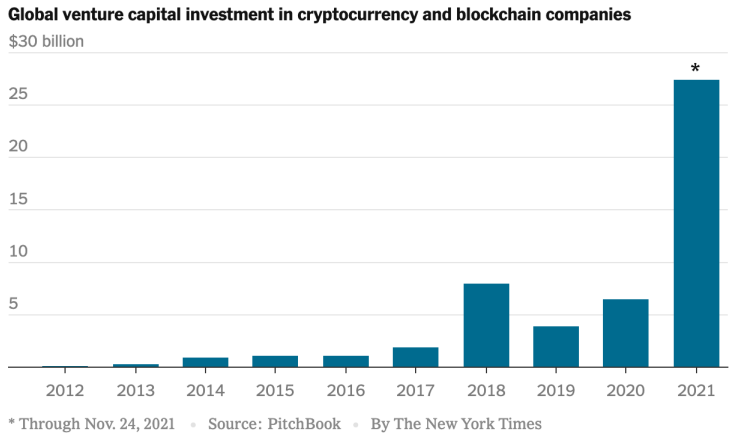
[25] https://www.gemini.com/cryptopedia/the-dao-hack-makerdao
[26] https://medium.com/@MyPaoG/explaining-the-dao-exploit-for-beginners-in-solidity-80ee84f0d470

be considered securities. Nonetheless, despite the many issues that DAOs may face over the coming years, regulatory and otherwise, we view the space as a burgeoning area with the possibility to disrupt traditional financial, social and political systems within the next decade.

A Growing Space

November of 2021 has been perhaps the most exciting and promising month yet in the crypto space. November alone saw $3 billion raised by VC funds, including the launch of a venture fund cofounded by Matt Huang and Fred Ehrsam called Paradigm, the largest crypto fund to exist to date. Five times more venture capital money has been poured into crypto in 2021 as compared to all of 2020, totaling $27 billion globally as of late November. Pitchbook notes that this sum is greater than the total amount invested in crypto over the past decade.[27]

Figure 5: `https://www.nytimes.com/2021/12/01/business/dealbook/crypto-venture-capital.html`



Since the beginning of 2021, 39 crypto unicorns have emerged, totaling 69 as of late November. According to TechCrunch, more than half of the global crypto unicorns have reached the $1 billion dollar threshold in 2021 alone.[28]

Newer, crypto-native launches are not the only participants in the space, either. David Tawil, president of ProChain Capital, finds it unsurprising to see existing venture funds like Sequoia Capital and Table Management getting involved in the space. He points out by "investing in crypto without in fact investing in crypto", institutional investors are exposing themselves to this increasingly accepted asset class without running the risk of experiencing compliance issues and the idiosyncrasies of the regulatory environment. [29].

Introducing: Martian

With the growing acceptance and adoption of investing in crypto/web3 startups, we might begin to understand how useful it can be for a new web3 startup to run its operations like a DAO. Most web3 startups offer a range of tokens - from equity tokens sold to VCs and retail investors in ICOs to NFTs airdropped to loyal users. There will be a need for these new web3 startups to manage all their tokens in one platform. In the next portion of this report, we introduce a whitepaper for our product, Martian which is a token management system for web3 startups.

[27] `https://blockworks.co/paradigm-launches-2-5-billion-crypto-fund/`
[28] `https://techcrunch.com/2021/11/19/as-crypto-unicorns-multiply-the-us-stands-out-as-ground-zero-for-blockchain-winners/`
[29] `https://blockworks.co/novembers-crypto-vc-funding-already-tops-3-billion/`

Product Whitepaper (martian.wiki)
Authors: Ian Dorian Macleod, Imanol Uribe, Sofia Bianchi, Utkarsh Sinha

Contents:

Product Summary

Martian is a token management system for web3 startups

The Problem

Web3 founders need to manage a lot of tokens. Some important use cases are:

1. Issue tokens to VCs for seed funding
2. Pay employees in native tokens as an alternative to ESOPs
3. Airdrop tokens to early adopters as rewards
4. Reward users and investors with governance tokens
5. Host NFT Collection drops
6. Track and visualize all tokens

A token economy is a web3 founder's portal to the world of web3. None of the DAO Tools like Aragon, DAO Stack, or DAO Haus have built a platform for token management for startup founders. The DAO Tooling space will not have a one-size-fits all tool but will rather have multiple horizontal tools specializing on the specific use cases required by that DAO. Hence, a token management system for employees needs a special software tool that we describe below.

Product Demo

User Profile	Use Case
Founders	1. Visualize all tokens on a dashboard 2. Transfer tokens to investors, employees, and users
Employees/Users	Check tokens allotted by a company

Five screens of the web-app are shown below:

1. Dashboard - Equity tokens: Distribution and transaction log of equity (ERC20) tokens
2. Dashboard - NFTs: Track all NFTs (ERC721) airdropped and their current owners
3. Dashboard - Governance tokens: Track all governance tokens
4. Transfer Tokens: Tokens of any form, equity/NFT/or governance, can be transferred from the DAO's account to another account. The receiver of the tokens could be a VC investor, employee, or an early user.
5. DAO Settings: Set the signers of the multi sig wallet. Add employees and add other accounts that the DAO will use.

Dashboard - Equity tokens

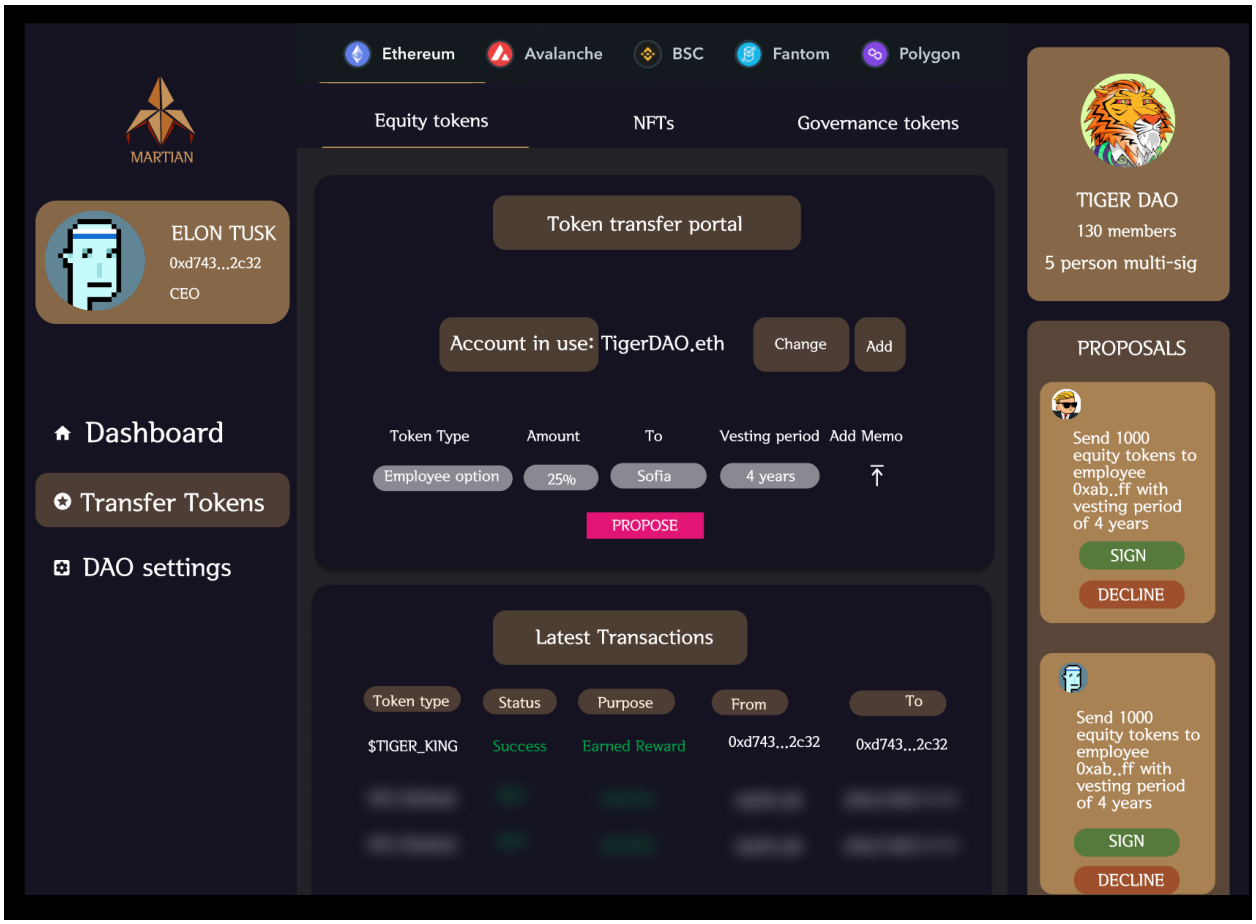
This is an account of the CEO of a web3 startup called TigerDAO. This DAO has an Ethereum account address called TigerDAO.eth which is governed by a multi-sig wallet. TigerDAO has raised a $20M Series B funding through a private token sale to select VCs. They gave out employee compensation in their native tokens. They also airdropped some NFTs to early users. Governance tokens were also sent to board members. All these tokens can be organized and tracked on Martian.

On the right side, the CEO sees requests for token transfer posted by other multi-sig wallet signers.

Dashboard - NFT tokens

The CEO can track all NFT airdrops done by their startup and also monitor current ownership. All NFTs (ERC721 tokens) minted to TigerDAO.eth will be tracked by code to enable this feature.

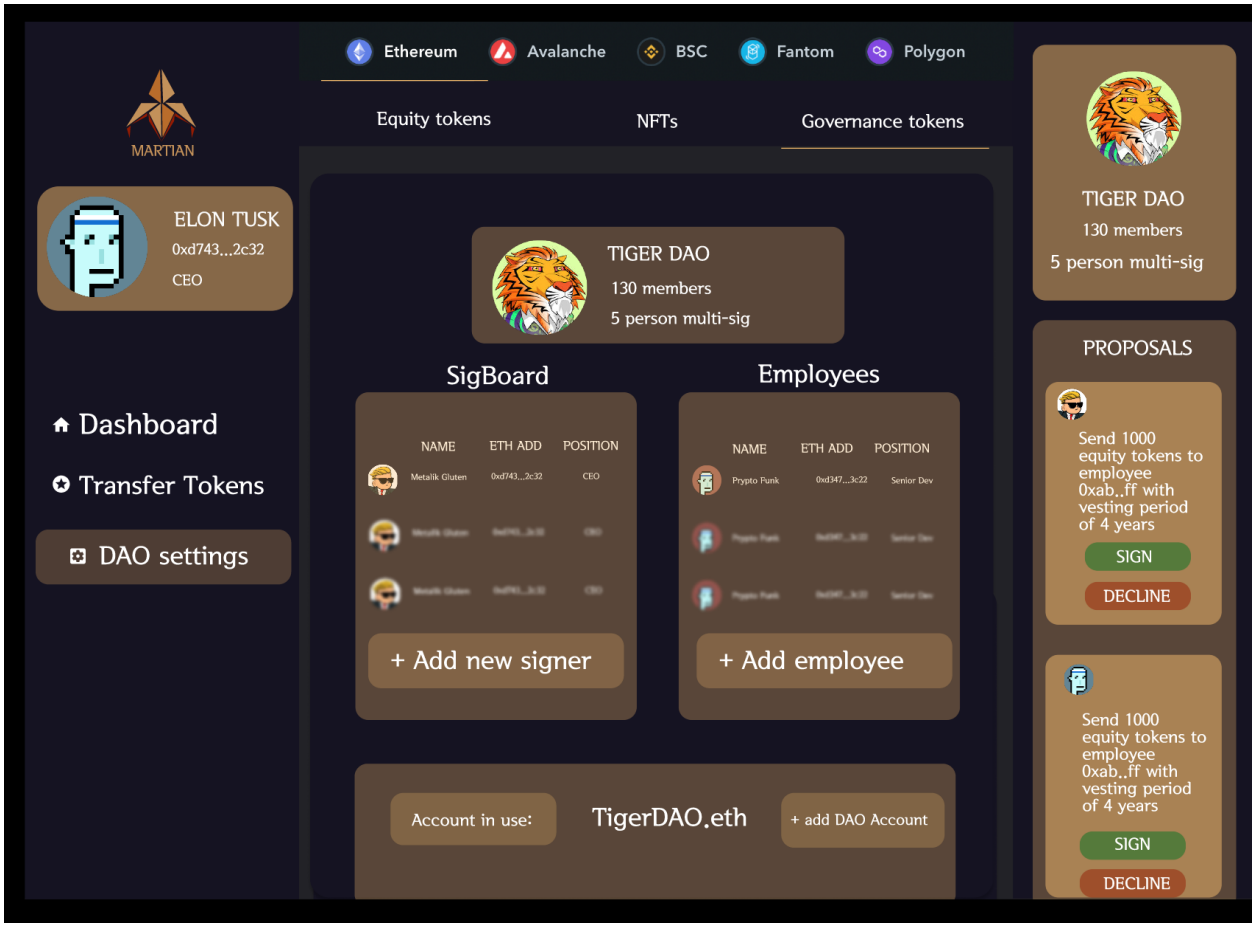
Token Transfer Portal



The CEO can propose token transfers of any form: equity/NFT/or governance, from the DAO's account to another account. The receiver account could be a VC investor, employee, or an early user. Vesting periods could be integrated into smart contracts to ensure correct vesting.

A multi-sig wallet controls all token transfers from the TigerDAO.eth Ethereum address. The CEO can propose a token transfer and other board members would need to sign on it for the transfer to actually happen.

DAO Settings



The CEO can set the signers of the multi sig wallet. Employees with their ETH addresses can also be added. More than one Ethereum account can be connected to the DAO.

Market Potential

Why is now the right time to be building this? A very important question in entrepreneurship is the timing of a product. If you're too early, the market doesn't exist. If the market doesn't exist, then no matter how great your product is, it is destined to fail. If you're too late to the party then you find yourself in a tough competitive oligopoly dominated by well funded competitors with deep relationships with their customers. Besides, the crypto world has historically proven itself to have a lot of tribalism. Early adopters of a product or a protocol are incentivized through native tokens and they become evangelists because they now have skin in the game. Hence, it's even more important to be right on time in the crypto market.

Web3 startups have just started raising seed money. Most web3 startups raise seed capital through SAFT notes. SAFT notes are convertible notes similar to the SAFE note used and popularised by Y Combinator for equity funding rounds. SAFT stands for 'Simple Agreement for Future Tokens' and is analogous to the 'Simple Agreement for Future Equity' instrument in the sense that tokens would now be accepted by investors as a legal tender. This is accepted by the law and VC investors because they are growing increasingly confident in liquidation opportunities through ICOs.

The web3 startups that are raising seed money today, have 8 -10 employees and 3-4 VCs to manage. They are able to account for tokens by storing data in Excel sheets for a quick lookup. Minting or transferring tokens requires firing up a smart contract from the terminal.

As these startups mature, they'll sell tokens to 10+ VCs in Series A,B, and C stages before going for an ICO on the open market. The startups would also employ more people, and easily grow from a 10 member team to 100+ in the next 2-3 years. Now these startups will be managing token compensation for 100+ employees on Excel and will have to write code for every token transaction. Imagine doing all of this on a web-app that runs Ethereum smart contracts in its backend. It's much smoother and more efficient for any founder.

We spoke with some founders of cryptocurrency projects and found significant Product Market Fit. One of our interviewees, Abraham Litwin-Logan, is the founder of a DAO called Reidar DAO that raised around $400K and bought a Bored Ape NFT. He mentioned that none of the existing tools in the market help founders to track and send tokens.

The target customers for Martian are early-stage web3 founders. This market is poised to boom over the next 2 years. A16z have raised a $2.3B crypto specific fund and Paradigm have raised a $2.5B crypto fund. We now have ~$5B VC firepowder lying to flow into early stage crypto/web3 startups over the next 3-4 years. Most web3 startups will raise from token sales and aim for liquidity through an ICO. All such startups would need a token management system, and Martian will be right there.

Let us look at one last point that further strengthens the thesis for Martian - a quick case study on Carta. Carta is a SaaS startup that does cap table and ESOP management for startups on a

web-app. It was started in 2012, does $150M+ in Monthly Recurring Revenue and is valued at ~$7B today. We're working on a very similar use case but for web3 startups.

Tokenomics Design

Martian will have a native token called $MARS. It will be rewarded to early users and would give them governance rights as well. It will be liquidated to raise VC money for some initial rounds and will lead to an eventual ICO if Martian is successful.

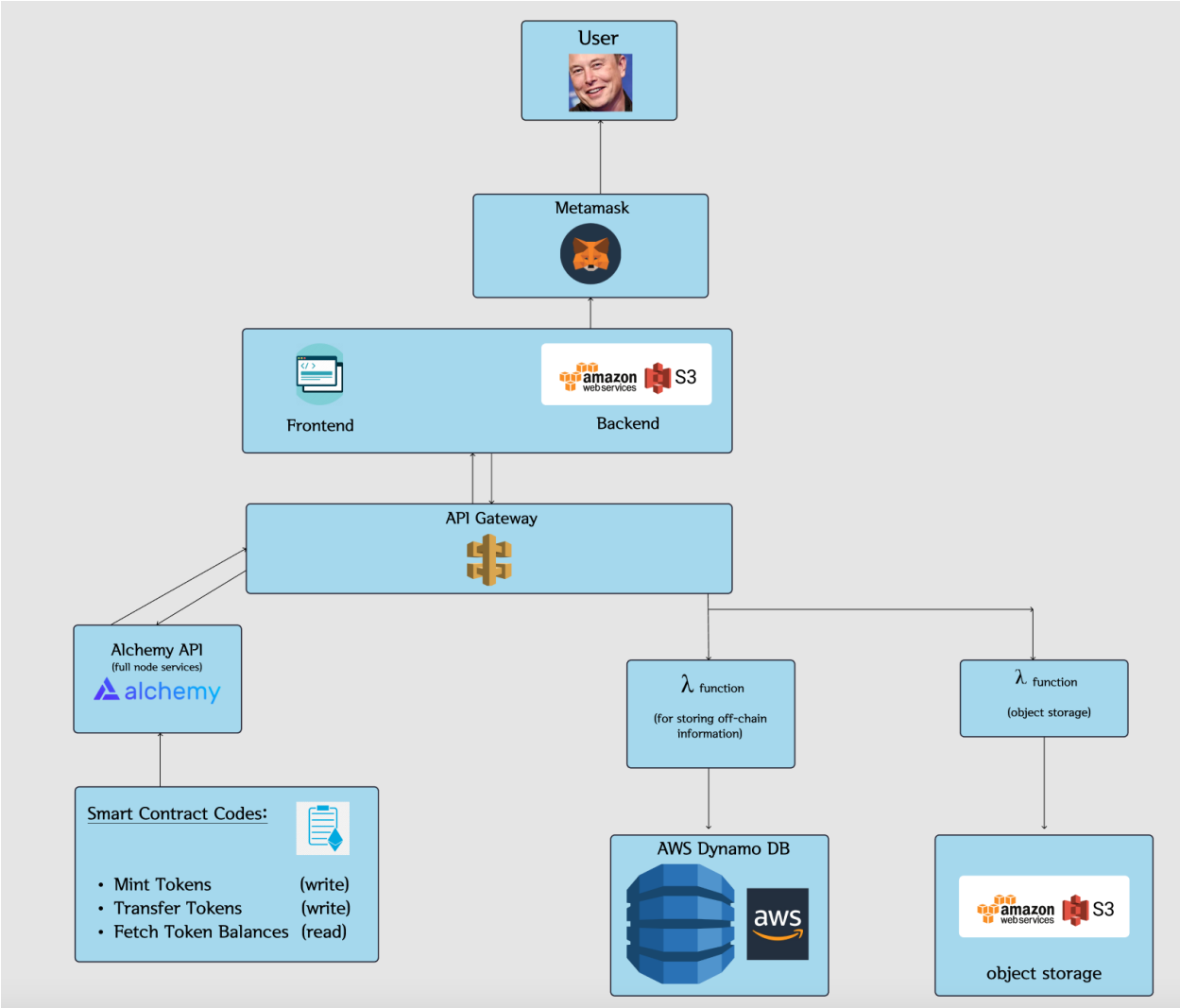
The product will be free to use for the first year. This will lead to organic product-led-growth. $MARS rewards will also incentivize web3 startup founders to use the platform.

After hitting a critical mass of users, Martian will move to a freemium model and will then be sold as a SaaS monthly subscription to web3 startups.

Next Steps

1. Some members of our team have started building the MVP of the product and it should launch by the end of January 2022 for the first user.
2. Community building: Discord server setup to form a web3 founder community of all kinds of projects ranging from just simple NFT projects to new protocols. Founders can request features and discuss pain points.
3. Airdrop of $MARS tokens to most active users
4. Seed round through $MARS sale to VCs: March 2022

Annexure: System Design



Database Schema Design (MySql):

User_info (pk as primary key, username, role, link to dp)
DAO_info (uuid, pk, name, num_of_members, link to picture)
Proposal_info (uuid, timestamp, proposer, subject, link to memo)
Latest_transaction (uuid, timestamp, status, token_type, from, to, reason)
Sig Board (DAO uuid as primary key, name, pk, role)
Employees (DAO uuid as primary key, name, pk, amount)

- Authors: Ian Dorian Macleod, Imanol Uribe, Sofia Bianchi, Utkarsh Sinha