

# DAO: the future or doomed to fail?

Rahim Klabér<sup>1</sup>, Johan Pouwelse<sup>1</sup>

<sup>1</sup>TU Delft

r.e.p@student.tudelft.nl, J.A.Pouwelse@tudelft.nl

## Abstract

### 1 Introduction

The rise of blockchain has led to the idea of the so called Decentralized Autonomous Organizations (DAO). These organizations allow are collectively owned with no one leader [1]. An early example of a DAO was The DAO on the Ethereum blockchain [2]. User could join The DAO by exchanging Ether for DAO tokens. The DAO would act as an investment fund where the members could vote on which project to invest into [2]. However soon after launching, the DAO was exploited and one third of the raised Ether was stolen. Since then many more DAOs have been many exploited [3]. In this paper we try to answer whether DAOs are doomed to fail or a part of the future...

TODO: Make longer??

### 2 Background: DAO

There is no one definition for what a DAO is. The Ethereum foundation describes a DAO as "a collectively-owned, blockchain-governed organization working towards a shared mission" [1]. DAOs do not have a leader and decisions are made through voting. Proposals can be put forward and are executed if enough members voted for it. Due to being blockchain-governed, decisions made by the DAO are transparent and executed automatically [1]. DAOs are often used as a way to govern blockchain-based applications.

#### Membership

There are different ways to model DAO membership. Namely, Token-based membership, share-based membership and reputation-based membership [1].

DAOs with token-based membership model membership with specific DAO tokens on a blockchain. The more tokens a member has, the more their votes are worth. Prospective members can acquire tokens in multiple ways. For example, by buying it on an exchange, by being rewarded for providing liquidity on an exchange or by being rewarded for using a blockchain-based application.

Share-based membership is more permissioned compared to token-based membership as users cannot become members

as easily. Prospective members can join the DAO by submitting a proposal and fulfilling the requirements such as paying the DAO to receive shares. The shares allow members to vote. However, contrary to tokens, shares are non-transferable. An example of a share-based DAO is The Lao [4]. The Lao allows members to collectively invest in projects and is limited to 99 members. Members must pass an Accreditation process and are allowed to buy a limited amount of shares. Members receive proceeds from investments based on the amount of shares they own.

Both token-based membership allows anyone to influence the DAO if they have enough tokens. With reputation-based membership, users gradually gain voting power by participating in the DAO. Reputation cannot be sold or transferred.

#### Proposals

Proposals allow a DAO to make a decision. A proposal can include code that is executed if the proposal passes, this is the autonomous part in Decentralized Autonomous Organization.

Before a proposal is formally proposed, the idea might be discussed with members of the DAO to receive feedback or gather support for the proposal. The proposal is adjusted based on the feedback of the members before being proposed. Chat platforms or internet forums are used to discuss the proposal. There are also specialized DAO platforms, like alchemy [5], that enable both discussion and the possibility to submit and vote on proposals. Figure 1 shows the lifecycle of a proposal submitted in the 1Inch DAO.

There are two main proposals are submitted. First, proposals can be submitted through a smart-contract. The smart contract registers the proposals and allows others to vote on it. Passing a proposal can allow for one or multiple transactions to be executed. Because of this, some DAOs institute a waiting period after a proposal is accepted, so the proposal can be reviewed to make sure no bugs are present. To prevent spam, members might need a certain amount of stake or reputation in the DAO to propose a proposal. Second, a proposal can be proposed by making a post on a forum. In the previous case, the forum might be a front-end for a smart-contract. However, in this case the forum is a website that does not create or mutate a smart-contract. As with the previous case, members can vote on the proposal. However, in this case no transaction is execute in the case that the proposal passes. Instead of being binding, this is a way for members of the DAO to gauge the

support of a particular proposal. However, there are certain DAOs where a small number of members control the smart-contract, in which case they would execute the proposal on behalf of the DAO. For example, in Figure 1 a proposal must be approved by the "DAO Treasury".

### Voting

A proposal can be voted on once it has been created. In general, proposals need a minimum amount of votes and a majority of yes votes to be passed. There are two main ways voting can be done. First, members can cast their vote by interacting with a smart-contract. This records their vote on the blockchain publicly. However, voting by interacting with the blockchain can incur fees. Instead, members can vote through an "off-chain" mechanism like Snapshot [6], which allows DAO members to vote without paying blockchain fees. However, since these votes do not occur on the blockchain, another mechanism must be used to execute the proposal. For example, relying a small group of trusted members or through a more advanced mechanism like oracles [7].

Simple scoring rules like majority voting are susceptible to situations where a small group of members have substantial power. To combat and other situations there are different scoring rules for voting, such as quadratic voting [8] and holographic consensus [9]. Quadratic voting is used to limit a single member's power by using a quadratic formula to price votes. While holographic consensus allows DAOs to scale to members by making voting require less participation(CHECK THIS).

### Delegation

DAOs can be overwhelming for the normal user. DAO proposals can be extremely technical and not all members are qualified to vote on these proposals. Additionally, not all members have the time to evaluate and vote on proposals. A solution to this is Delegation, which allows members to temporarily give their voting power to another member.

## 3 Challenges of DAOs

TODO : Expand section?? and make section flow nicer In theory, DAOs should be decentralized and autonomous. However, this is often not the case. Correctly creating DAOs is very technical, which leads to compromises [10].

### 3.1 Decentralization

Decentralization is hard to implement in practice. For example as shown in Figure 1, 1Inch needs proposals to be accepted by a 7 out of 12 multi-sig before they are executed, to deal with malicious proposals [11]. However, this means that only 7 members need to collude to effectively stop the DAO from doing anything. Migrating an organization to a DAO is not trivial, therefore this technique is often used as a way to start the conversion of an organization into a DAO.

DAOs can have members that control a large portion of the voting power. This can result in scenarios where a small number of members can pass proposals, even if everyone else disagrees. This can occur when the founders are rewarded with DAO tokens, the investors are rewarded with DAO tokens, if large amounts of tokens are available on the open market or

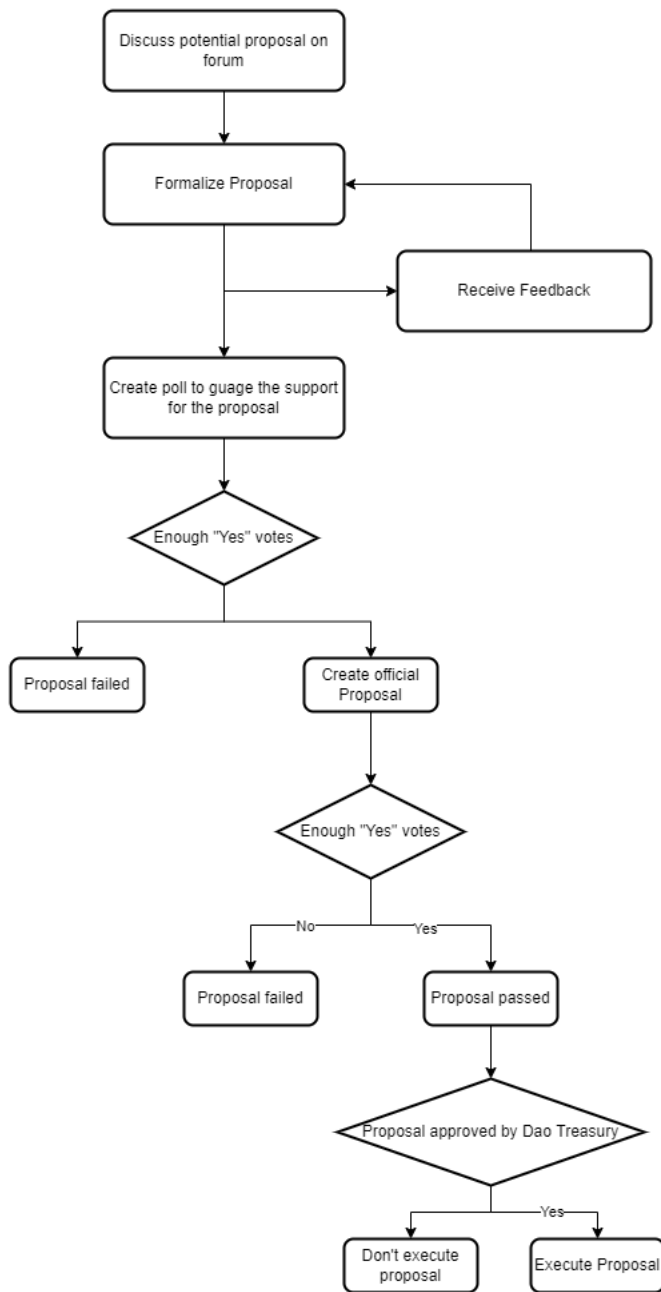


Figure 1: 1Inch Dao Lifecycle

over the counter or if many members delegate their voting power to few members. One example of this is when Justin Sun, the founder of the Tron blockchain, was able to takeover Steemit, a blockchain based social network [12]. By buying a large amount of tokens from the founder and by getting cryptocurrency exchanges to help, Justin was able to effectively take over Steemit.

Even when not controlling a significant portion of voting power, some member can have a large influence on the DAO. For example, the founder or the core team of a DAO are influential for the sole reason that they are trusted. Even if members do not understand a proposal, they might vote just because they trust the submitter of the proposal.

### 3.2 Smart-contract

DAOs rely on smart-contracts to be trustless and autonomous. However, smart-contracts is just computer code, which is error-prone. Many DAOs and blockchain-based application (which may be managed by a DAO) have been hacked due to vulnerabilities found in the smart-contracts [3]. Even when the vulnerability is found before an exploit was performed, fixing the problem is not trivial. A proposal is required to fix a vulnerability. Therefore, attempting to fix a vulnerability will make it known. This is further exacerbated due to the fact that there is often a minimum amount of time before a proposal can be passed, to allow for voting. An example of this is when Compound [13], a lending market, allowed its members to claim more tokens than intended [14]. To fix the problem a proposal was passed, but by then many had already exploited the vulnerability [14].

- [1] E. Foundation, *Decentralized autonomous organizations (daos)*. [Online]. Available: <https://ethereum.org/en/dao/>.
- [2] M. I. Mehar, C. L. Shier, A. Giambattista, *et al.*, “Understanding a revolutionary and flawed grand experiment in blockchain: The dao attack,” *Journal of Cases on Information Technology (JCIT)*, vol. 21, no. 1, pp. 19–32, 2019.
- [3] M. White, *Web3 is going just great*. [Online]. Available: <https://web3isgoinggreat.com/>.
- [4] T. Lao, *The lao*. [Online]. Available: <https://thelao.io/>.
- [5] DAOstack, *An operating system for collective intelligence*.
- [6] Snapshot, *Snapshot docs*. [Online]. Available: <https://docs.snapshot.org/>.
- [7] R. Mühlberger, S. Bachhofner, E. C. Ferrer, *et al.*, “Foundational oracle patterns: Connecting blockchain to the off-chain world,” in *Lecture Notes in Business Information Processing*, Springer International Publishing, 2020, pp. 35–51. DOI: 10.1007/978-3-030-58779-6\_3. [Online]. Available: [https://doi.org/10.1007%2F978-3-030-58779-6\\_3](https://doi.org/10.1007%2F978-3-030-58779-6_3).
- [8] S. P. Lalley and E. G. Weyl, “Quadratic voting: How mechanism design can radicalize democracy,” *AEA Papers and Proceedings*, vol. 108, pp. 33–37, May 2018. DOI: 10.1257/pandp.20181002. [Online]. Available: <https://www.aeaweb.org/articles?id=10.1257/pandp.20181002>.
- [9] Y. El Faqir, J. Arroyo, and S. Hassan, “A scalable voting system: Validation of holographic consensus in daostack.,” in *HICSS*, 2021, pp. 1–10.
- [10] H. Axelsen, J. R. Jensen, and O. Ross, “When is a dao decentralized?” *Complex Systems Informatics and Modeling Quarterly*, no. 31, pp. 51–75, 2022.
- [11] 1Inch, *1inch proposal lifecycle*. [Online]. Available: <https://docs.1inch.io/docs/governance/proposal-lifecycle>.
- [12] T. Copeland, *Steem vs tron: The rebellion against a cryptocurrency empire*. [Online]. Available: <https://decrypt.co/38050/steem-steemit-tron-justin-sun-cryptocurrency-war>.
- [13] *Compound*. [Online]. Available: <https://compound.finance/>.
- [14] M. Sigalos, *Bug puts \$162 million up for grabs, says founder of defi platform compound*. [Online]. Available: <https://www.cnbc.com/2021/10/03/162-million-up-for-grabs-after-bug-in-defi-protocol-compound.html>.