Abstract

The most likely scenario for the collapse of a DAO, in my opinion, is corruption or infighting from within.

To date, many DAOs have been organized, but they are in some ways weaker than traditional joint-stock companies.

For example, they do not have a role equivalent to that of the human resources department of a stock company, and salary and personal disputes have surfaced.

I propose a whistle-blowing method to promote the health of DAOs.

Specifically, a system that establishes account links that link Web 2.0 (Twitter ,Discord) accounts to Ethereum addresses, and when signs of fraud or infighting are detected on Web 2.0, the assets on the Ethereum addresses can be confiscated by majority vote. The following is an example.

There are four main requirements for building this system.

1. the anonymity of DAO participants is guaranteed, and only when a whistleblower is identified, the anonymity of the accused is revoked.
2. introduce a mechanism to link non-anonymous Web 2.0 accounts with anonymous Web 3.0 accounts.
3. detect the signs of fraud before it is committed, and punish those who attempt to commit fraud based on the results of deliberation by the members.
4. Prevent abuse of whistle-blowing.

Account Link

First, let us describe the account link we have devised for this system. This is intended to satisfy requirements 1 and 2.

I believe that fraud and disputes do not surface on the on-chain, but on Web 2.0, such as the discord ch we have established for each DAO.

However, even if there is someone who is planning to cheat, the only thing DAOs can do now is to kick him out of the ch.

Is that really healthy for the DAO?

The ousted person can vote and influence decisions as long as he or she has a governor’s token.

(In the worst case scenario, the value of the governor’s token could be manipulated in retaliation for being kicked out.)

Therefore, I came up with the Akoutlink as a solution that forces all DAO members to participate in that DAO at financial risk, and only if signs of fraud are exposed on Web 2.0, confiscate the anonymity and assets of those members.

This is a simple idea to split the private key that created the Ethereum address (identity in DAO) that holds the governance token (identity in DAO) according to the Verifiable Secret Sharing Method, link it to an account in a Web 2.0 service such as Discord, and distribute it to other members.

Specifically, the process is as follows.

Assume the number of members participating in whistleblowing is n

1. split the private key that created the address into n

shares based on the secret sharing method

1. create pairs of n

shares per Web2.0 account

1. distribute each pair to n

members

If more than the threshold m

shares are gathered, the private key can be recovered.

The gimmick of this account link is that Web 2.0 → Ethereum Address can be recovered, but not Ethereum Address → Web 2.0. This cryptographic trick protects the anonymity and assets of non-malicious members, but if they show signs of fraud, they will be punished by having their private key recovered by a vote of the members.

We believe this mechanism will serve as a deterrent against fraud.

The values of the parameters should be flexible and changeable from DAO to DAO, as it is desirable for each governance to make decisions democratically, such as when consensus is reached by a majority or by 2/3 or more.

Whistleblowing Process

This section describes the overall process (Requests 3 and 4).

Many early-phase DAOs tend to be dominated by the decision-making power of core members, and power tends to be concentrated, but an ideal DAO moves to a phase where it can operate in a decentralized manner, and the overall direction is decided democratically through voting with governance tokens and other means.

We hope to reflect this philosophy in this system as well.

The whistleblowing process, assuming that all participants have submitted the account links mentioned earlier, would be as follows.

[

スクリーンショット 2022-03-04 18.09.07

562×873 43.4 KB

](https://ethresear.ch/uploads/default/original/2X/b/ba57761dee73bf658b7f43811ad5c20ff4223241.jpeg)

Here we assume the existence of a whistleblower contraption. This is responsible for the process of actually writing off the assets of the non-whistleblower based on the results of the vote.

First, the whistleblower gets the signs of fraud and infighting through Web 2.0 message exchanges and so on. For example, “Would you like to play ragpull with us?” These are messages such as

Then, before starting whistleblowing, they lock their own assets into the contract as collateral in advance.

The purpose of this is to secure your credibility to prevent making up fraudulent stories to defraud others.

Voting is then started based on the Web 2.0 account of the accused and the content of the message.

As a result, if more than the threshold n votes are collected, the accused’s assets will be written off, and if not, the accused will be charged with making up the fraud and the assets will be written off.

Although the example here is the write-off of assets as a punishment for fraud, there may be other ideas, such as making it a DAO treasury.

We also believe that the voting phase here could be done simply by sending a pair of Web2.0 and SHARE without a governance token.

This method would match the DAO’s philosophy of democratic decision making through voting and the secret decentralized method.

issue

- Proof that an Ethereum address was generated from the private key
- Proof that the submitted Ethereum address holds a governance token
- Fear of someone colluding to recover the private key outside of a whistleblower
- No signs of fraud caught on registered Web 2.0 accounts
- Cost of using smart contracts for voting and private key recovery

Some issues may be able to use primitives such as zero-knowledge proofs or attribute-based cryptography.

Also, gaps with implementation have not been verified.

Conclusion

I started my research with the idea of changing the current situation where there are no countermeasures against fraud and infighting in DAOs, even if only a little.

However, I believe that there are cases where this scheme itself is abused by fraud.

In the first place, is decision-making by voting democratic?

If you have any suggestions or opinions on how we can improve the situation in any way, please leave a message.