

Hi researchers,

To briefly introduce ourselves, we are DAICO research team organised at Decipher, a blockchain lab of Seoul National University in South Korea. Our goal is to create a formal DAICO model suggested by Vitalik. Currently, our team is working on establishing MVP model and we would like to discuss our project with eth.researchers.

Below is a short summary of our project, so please follow the [link](#) for more details.

Our model is consisted of tap voting and refund voting. The concept of tap is based on the DAICO model proposed by Vitalik. (yes stake) > (no stake)

is the passing requirement for each voting while the minimum voting rate $v\%$

is introduced in order to create an environment that is protected and secured from potential attacks. The characteristics of our model can be elaborated as follows.

1. Modeling with minimal Oracle intervention
2. Incentives-based modelling of token holders

Group settings for Token holders

In order to derive the behavioural incentives of token holders, it is necessary to group the token holders first. In our MVP model, token holders are grouped into two groups which are developer group and public group. The lock on developer group's tokens gets slowly vested over time which distinguishes developer group from public group.

Analysis on behavioural incentives and problem situation of respective groups

1. Tap Voting

Developer

Behavioural incentive

: Developers will try to maximise the size of tap so they can get paid quickly.

Problem Situation

: If developer takes a large portion in total issued tokens, then she/he might call for a vote to raise the size of tap based on their excessive voting right.

Public

Behavioural incentive

: They do not have much incentive to call for a tap voting.

Problem Situation

: If public do not participate in tap voting, then the voting might be cancelled as they fail to pass the minimum turnout rate. Also, the result of voting can be determined by the developer group.

1. Refund Voting

Developer

Behavioural incentive

: Developer group will oppose the refund since they have to refund the raised ETH to public when refund voting takes place.

Problem Situation

: Similar to the aforementioned problem situation in tap voting, excessive voting right might also be a problem in refund voting. Moreover, when the price of the ETH is expected to fall precipitously then developer group might agree with refunding so they could get refund on ETH based on their proportion of tokens.

Public

Behavioural incentive

: In general, the market price will be formed above the price that can be obtained by refund voting, because there is a kind of pegging relationship between tokens and money collected from the refund. Usually, there is no incentive for public group to

agree with refunding due to the greater benefits of selling tokens to the market.

Nevertheless, if it is clear that the price of tokens is expected to decline (i.e. if it turns out to be a scam), they will vote for refunding to get refund as soon as possible.

The causes of the problem situations of voting can be summarized as follows.

- Excessive rights of the developer group
- Volatility of ETH price
- Lack of incentive for public group to vote

Our proposals for Solution

We devised several ways to solve the cause of problems above.

1. Limiting factor q

Limiting factor q

is to lower the voting power of developers by multiplying q

. As a result, their voting power becomes

$$q \cdot p_{dev} = f(p_{pub})$$

$$= Mp_{pub}^2 \text{ (if } p_{dev} > Mp_{pub}^2 \text{)}$$

$$= p_{dev} \text{ (otherwise)}$$

The detailed process is described in the [link](#).

1. Utilizing stable coin

We are considering with utilizing stable coin(e.g. DAI) instead of ETH in fund pool.

1. Incentive pool

This incentive pool is designed to provide incentives for voting participants with incentive tokens.

1. Minimum voting rate

We try to derive the appropriate v

by deriving a probability distribution based on the stake distribution for the calculation of the minimum turnout rate. We judged that voters had a different probability of voting according to their stake holdings and categorized them roughly. An example is the Pareto Optimal. Please refer to the [link](#) for details.

Remaining problems

1) People without ETH

Although we did not reflect on our MVP model, there might be some private sale group who paid with fiat currency instead of ETH, advisor who paid nothing or some shareholders of the previous company. In this regard, there is an issue whether these people should also have a right to vote and get refund in refund voting or not.

2) Reservation Pool

In the real case of the ICO, developer leaves some amount of tokens as reservation in order to give rewards or cover the operation costs which can be distinguished under the management of smart contract. However, the real problem arises after the withdrawal from the reservation pool since it is impossible to trace. Furthermore, if the developer's proportion is relatively large in the reservation pool and owns the reservation token after withdrawal then the power of developer can grow asymmetrically.

Our team have started to build structure on github.

<https://github.com/decipherhub/ICO2.0>

And full doc is [here](#).

We want to embark on discussion with various people so please do not hesitate to give feedback on our MVP model.

Thanks!