Praise

Vitalik’s DAICO idea was badly needed. It’s really good to see the right message propagated from the top.

If I were to describe blockchains in one word, it would be “blockchains make things more accountable”. If I were allowed only a single word, it would be “accountability”.

The fact that ICOs don’t do everything they can to keep themselves accountable is a disgrace to the technology and community. So Vitalik highlighting the issue and proposing a solution is very important.

DAICO

According to the proposal, DAICOs have three extra functionalities, compared to multisig wallets:

“The Tap”

: Owners of the DAICO aren’t able to withdraw all the funds. The DAICO only allows them to withdraw a pre-defined amount per unit time (usually monthly).

“Opening The Tap”

: If the project is doing well, the ICO token holders can increase the monthly allowance by “opening the tap”. However, they can’t reduce it. The process is one way only.

“Closing Shop”

: If the project is not doing well, the ICO token holders can vote to close down the DAICO. In this event all the remaining funds are returned to the current token holders.

Critique

The above proposal is very sensible, and a great step to the right direction. However, it has several weaknesses. I would like to go through them one by one, explain them and propose solutions. The list of weaknesses are below, then a detailed explanation follows.

- Automating The Tap
- Pre-Sale Exploits
- Public Sale Exploits
- “Closing Down” Exploit
- Proposed Solutions

1. Automating the Tap

Asking the community to “open the tap” more every time is not practical.

From one side, a properly planned business will have a sensible and explainable spending curve. It will start low, and then it will increase, according to the business plan. It makes sense to put this expected emission curve into the DAICO, so if the business is going as planned, then there is no action needed from the community.

This also deals with the problem that the business might die or miss opportunities because not enough of the community can be bothered to vote to increase the allowance.

The possibility for the community intervention to open the tap even more should be still implemented, but only be used under exceptional circumstances, when the company needs to deviate from the plan (spend more, with a good reason).

2. Pre-Sale Exploits

This exploit aims to take away the ability of the token holder community to use the “Closing Shop” option. In principle 51% of the token holders must vote “yes” to close shop.

This can be easily circumvented by a fraudulent ICO.

During the pre-sale phase of ICOs there are large percentage of ICO tokens get sold, and it is not always known what the project gets for the tokens. It is inevitable, because pre-sale contributors might pay with cash, fiat currencies, shares, etc. Many of these don’t have a proper representation on the blockchain yet.

The exploit is trivial: A fraudulent team might just do a large pre-sale, where they issue near 50% of all tokens to themselves.

Please note that they don't have to own 50%. Much smaller amount is enough to make it difficult for the rest of the token holders to reach consensus. For example the fraudsters running the ICO only issue 25% of the tokens to themselves — now the rest of the community only owns 75%, so the 51% requirement to close down now was increased to 68%.

3. Public Sale Exploits

Even if there is no pre-sale, an exploit can be carried out during the public sale as well. A fraudulent group can borrow a significant portion of ether, and buy their own tokens on the public sale.

After the sale they can return the ether gradually from the tap, with interest.

This is a less attractive option, but similarly to the pre-sale exploit, it can make the closing down significantly more difficult.

Also, there is no financial risk for the lenders, because the ether is there, it just takes time to get to it.

4. "Closing Down" Exploit

This is an interesting variation of the pre-sale exploit. The fraudsters acquire tokens as described in the pre-sale exploit. Then they trigger the close down. They might even apologize — because of reasons, the project can't continue, but worry not, all eth is accounted for. Except that it's not true.

Then money gets returned to the token holders — including them, since they own a large amount of tokens. They go scott free, having made a potentially large profit.

Proposed Solutions

The "automating the tap" issue contains its own solution: implement a rising emission curve that is in accordance with the project's business plan, and supermajority voting to permit extra raises as an exception if properly explained.

The other issue — meddling with the shutdown — is more complex. Especially when considering the "Closing Down" exploit. The technical solutions for these are all complex and uncomfortable:

Solution 1: No Presale

One solution is to forbid having a presale. This is technically easy, but business-wise difficult, might even be a deal-breaker. It means that it would be enforced that no special business deals could be made. From an idealistic point of view it is defendable, but realistically thinking it might not always be acceptable. Not all private deals are bad.

Also, this does not fix the "public sale" exploit.

Solution 2: Two Tokens

Another natural solution is to mandate that only public sale tokens can be used to vote for the shutdown. Of course, the problem with this is that it implies that we either have two different tokens (presale tokens, public sale tokens) or somehow we make the tokens non-fungible.

Neither of the options are attractive, not to mention that it is dubious if it could be technically carried out. Think about the madness on the exchanges. This is a no-go.

Also, again, this does not address the "Public Sale" exploit.

Solution 3: A Centralized Shutdown Switch

All of the exploits above come from the fact that the number of votes can be manipulated with. There is an obvious solution — using the existing legal framework.

By creating a special account that can be proven to be able to shut down the DAICO, and return the funds to the token holders. Then depositing this key with a known, independent party (lawyer, etc).

In case of fraud, a lawsuit can be launched and the key can be demanded. This shutdown switch would not replace the community's ability to close the shop, it would be added as an extra feature.

The purpose of an ICOs is to raise funds in an accountable, yet easy manner. The purpose of an ICO is not to be above the law. Almost all projects or companies should be exposed to the extant legal processes. The backend key could expire after some period of time.

Conclusion

DAICO is needed, great step to the right direction

Should use an emission curve instead of asking the community to increase the tap

Create a centralized shutdown switch that can be activated by a legal process.

There are other steps that we can take to make ICOs more accountable. For example tokenizing the pre-ICO deals and fiat currencies. I will expand on those and propose a full solution in the upcoming post.

Thanks go to Virgil Griffith for the review and suggestions.

Original post: https://medium.com/@akomba/daico-praise-and-critique-2c5bcee2acfe