Special thanks to Dan Robinson for discussion

This post proposes a form of coin voting that mitigates tragedy-of-the-commons issues in traditional coin voting that limit its ability to respond to (potentially obfuscated) vote-buying attacks.

Problem

The core tragedy-of-the-commons problem in coin voting is that each voter only internalizes a small portion of the benefit of their voting decision. This can lead to nasty consequences when it hits against an attacker trying to buy votes: if the voter instead votes in the way that the attacker

wants them do, they suffer only a small portion of the cost of the attacker's decision being more likely to succeed, but they get the full personal benefit of the attacker's bribe.

Suppose there is a decision that the attacker is attempting to push which, if successful, will give the attacker a 20000-point payout but hurt each of 1000 voters by 100 points. Each voter has a 1% chance that their vote will be decisive; hence, in expectation, from each voter's point of view, a vote for the attacker hurts all voters by 1 point. The attacker offers a 5-point bribe to each voter who votes for their decision. The game chart looks as follows:

Decision

Benefit to self

Benefit to 999 other voters

Accept attacker's bribe

+5 (bribe) - 1 (cost to self of bad decision) = +4

-999

Reject attacker's bribe

0

0

If the voters are rational, everyone accepts the bribe. The attacker pays out 5000 points as their bribe, gains the 20000 point payout, and causes 100000 points of harm to the voters. The attacker has executed a governance attack on this system.

Bribes do not need to be direct blatant offers; they can be obfuscated. Particularly, an exchange might offer interest rates on deposits of some governance token, where those interest rates are subsidized by the exchange using those tokens to vote in the governance in a way that satisfies its interests. Even more sneakily, an attacker might buy many tokens but at the same time short that token on a defi platform, so they retain zero net exposure to the token and do not suffer if the token suffers as a result of their governance attack. This is an obfuscated bribe, because what is happening behind the scenes is that users who would otherwise hold the token are instead being motivated (by defi lending interest rates) to hold a synthetic asset that carries the same economic interest as the token but without the governance rights. Meanwhile, the attacker has the governance rights without the economic interest.

In all of these cases, the key reason for the failure is that while voters are collectively accountable for their votes, they are not individually accountable

. If a vote leads to a bad outcome, there is no way in which someone who voted for that outcome suffers more than someone who voted against. This proposal aims to remedy this issue.

Solution: votes as buy orders

Consider a DAO where in order to vote on a proposal with N

coins, the voter needs to put up a buy order: if the current price at the start of the vote is P

, then they need to be willing to purchase an additional N

coins at $0.8 * P$

for a period of 1 week if the vote succeeds (denominated in ETH, as DAO tokens tend to have less natural volatility against ETH than they do against fiat). These orders can be claimed by anyone who votes against the decision.

To encourage votes, a reward for making a vote could be added. Alternatively, anyone who votes against could be required to put up a similar buy order if the against side succeeds, and anyone who votes in favor can claim those orders. Another option is that in each round, token holders can vote on any one of N options, including the “do nothing” option, and if a token holder gets the decision they want their buy order activates and if they do not they can claim other holders’ buy orders.

Analysis

The intended effect of this design is to create a voting style which is a hybrid between voting and futarchy: voting for “normal” decisions that have low effect, and futarchy in extremis. It solves the tragedy of the commons problem by introducing individual accountability into voting

: if you vote for a bad decision that passes, it’s your

responsibility to buy out those who disagree if everything goes wrong, and if you did not vote for that bad decision, you do not have this burden.

Note also that the security of this design does not rely on strong efficient-market assumptions. Rather, it relies on a more direct argument: if you personally, as a holder of the system, believe that decision X is an attack on the chain, then you can vote against it, and if the decision passes then the attacker is required to compensate you with locked funds. In the extremes, if an attacker overpowers honest participants in a key decision, the attacker is essentially forced to buy out all honest participants.