Quadratic Voting Threat Analysis

There's significant merit in the discussion about the need for voting reform (or lack thereof) and looking into and adopting (if feasible) alternative forms of governance systems to put in place as the basis for our voting structure.

No system is perfect in a vacuum, sach system has its own strengths and weaknesses (which I'll briefly touch upon).

Think of it as the Modern MBT problem → Protection, Mobility and Firepower are essential to any Main battle Tank

However, If you want to upgrade the protection then your mobility is adversely affected. If you want it to be more mobile and agile, then you have to compromise on the

If you want better firepower thus better penetration (using APFSDS rounds) then you'll have to upgrade the gun which will increase the weight, would require you to make changes within the hull possibly and also decrease mobility among a myriad of other things.

So it has to be supported by the active measures. I like to think of it as Combined arms warfare which aims to compliment one anothers deficiencies during combat. Just like Armour covers Infantry's advance in urban warfare and in turn the infantry protects the Armour from Anti Tank threats.

Now what does it tell us, Complementing strengths FTW !!

An Ideal voting mechanism has a complex set of criteria which it must uphold in a threat model where no one can be trusted

Now this is esp true in a DAO, which is in essence trustless. (basically we all aren't required to trust each other as individuals to ensure the system is being upheld.)

For more context, read this →https://twitter.com/ThreatT0Society/status/1669948723630342145

There are however, some issues which we have to address regarding that particular implementation, that's what we'll address in this thread.

Please feel free to share your feedback, I'd love to know your thoughts.

I'll Keep it simple and add my condensed insights to this after I sift through all the relevant academic literature. Just the major insights about the relevant topic i.e. possible attack vectors.

This is how the Vote scaling looks like for QV

[

Group 31

1788×900 62.7 KB

](https://global.discourse-cdn.com/apecoin/original/2X/a/a4d585ed296d79cb9064bebc83d0d8b1ad2b9384.png)

The Mathematical formula it was modelled after →

Quadrating Funding, matching contributions to be exact.

In this system, Buying influence (after a certain point) in the traditional manner is pretty much impractical as every consecutive vote you cast, it starts to get more and more expensive.

[

image

780×718 15.6 KB

](https://global.discourse-cdn.com/apecoin/original/2X/0/04859c7d53c1436e6147626f9ba320fdd74f60e3.png)

Possible Attack Vectors :

In this pre eliminatory Threat analysis, I can see 2 glaring attack vectors which would need to be addressed before we even think about anything else.

- Sybil Attack

The way I think of it is, Nothing is ever truly Sybil resistant. It either gets financially, chronologically or technologically infeasible to do so. But as long as the incentive is there, It's worth doing.

The benefits associated with something like that massively outweighs the efforts one has to put in. Incentives shape human behaviour, and in this case the incentive is control over a multi billion $ Treasury.

The incentive to rig something so fundamental to the DAO becomes too too big to overlook and subsequently take actions against those attack vectors.

How to subvert snapshot voting ?

Let's take an example,

Guy 1 holds 1000 $APE in a single wallet and Guy 2 also owns 1000 $APE in 3 different wallets (50/30/20 aa%)

Now let's calculate the weighted voting power for both the individuals

Guy 1 : $10\sqrt{10} = 31.6$

Guy 2 : $10\sqrt{5} + 10\sqrt{3} + 10\sqrt{2} = 22.36+ 17.32+ 14.14 = 53.8$

Now imagine it at a much higher scale, across numerous wallets

We experience such a vast discrepancy while starting with the same $ amount. This is because fundamentally quadratic voting disproportionally affects big voters. The maximum vote scaling (1) tends to → 0, the more APE you hold.

Now the unintended consequence of QV is that big holders are incentivised to fractionalise their holdings, either via capital spread, delegation, or other ways.

Now Imagine this at a much larger scale with lower balances as the number of wallets and the balances in each wallet tend to decrease, the proportional voting power increases exponentially.

You might say that’s a very tedious task, think again. Now credit where it’s due, thanks Amp for bringing this to my knowledge. Turnkey.io allows one to, and I quote Spin-up thousands of wallets and sign millions of transactions, all without compromising on security using Simple APIs.

- Collusion Attacks

No. of Voters	Votes (v) per Individual	Associated Cost	Total Votes
1	100	$ 10,000	100
2	50	$ 5,000	100
5	20	$ 2,000	100
10	10	$ 1,000	100

20

5

$ 500

100

50

2

$ 400

100

100

1

$ 100

100

(For a total of 100 votes, The cost associated with it drops off significantly the more the no of Voters increase while the Voting power remains the same.)

So now the cost of every consecutive vote doesn't scale to the factor of (v) → v^2 $ and instead the cost is divvied up among legit voters and / or aliases of existing one. I've put in aliases to emphasise the sybil attack vectors.

For a vote ranging from 1 → n, the cost of every vote scales from 1 → $(n)^2$

So, it can be determined that the vote scales much more effectively for those with smaller holding. If the amount is small enough, it achieves near parity (if for no. of voters (v) n → 1 , n^2 → 1)

So in short, as QV requires quadratic pricing of votes per individual. Two (or more) colluding individuals can buy v votes for a lower price than one individual alone.

And with the mechanisms in place for Sybil attack that particular effect can be scaled up massively using tools which we talked about in the Sybil section.

Solutions :

Now you might ask, "Why point out all the problems if you don't know what to do about it ?" but rest assured there's a solution for every problem there is. You just have to look real hard

And what that might be? Well, that's a topic for another post.