Last weekend, we decided to use quadratic funding to distribute a $14,000 prize pool at one of our on-site hackathons, DoraHacks ETH Hackathon Beijing — DAO, NFT, Layer-2. We deployed a quadratic funding grant on HackerLink, and let the community votes decide who the winners are.

Previous DoraHacks hackathons used a voting scheme that can be described as "one-team-three-votes + one-judge-three-votes". Teams can cast their votes to any other teams except themselves. Judges can vote any team. A prize pool will be distributed proportionally according to the final voting results.

It's new to combine quadratic funding and a physical hackathon.

The grant was setup prior to the hackathon. It started 12:00 pm Saturday March 6 GMT+8 and ended 4pm Sunday March 7 GMT+8.

The rules of the hackathon are as follows:

- Hacking time is from 12:00 pm Saturday to 12:00 pm Sunday
- Hackathon hackers can submit their projects to the grant between 12:00 pm Saturday and 12:00 pm Sunday
- Between 12:00 pm and 4:00 pm Sunday, a demo fair and a project demo show were hosted
- Anyone can vote any project, voting cost starting from 0.01BNB and every additional vote to a particular project costs 0.01BNB more than the previous vote, therefore total cost is quadratic.
- Projects receive direct donation from the community, plus a portion from the prize pool based on quadratic voting results (detail see)
- After voting ends, there is a grace period. If there is obvious sybil attack found, the project is disqualified from receiving any funding from the prize pool (however it's still eligible to redeem fund from the community contribution). This is how obvious sybil attack can be identified.

In the first place, we were mostly concerned that our smart contract could be sybil attacked because we did NOT require any ID verification. After all, when it's close to the end time, every project would have incentive to create a bunch of addresses and vote 0.01 BNB from each of the addresses to gain maximum return from the prize pool.

The grace period was set up to prevent sybil attack, although it will be pretty hard to totally oust sybil attack in the end. Given that we do NOT have an easy-to-use & effective DID product so far, an investigation to prove any sybil attack is doable, but comes with high costs (an investigation needs to look into transfers between the voting accounts).

The result was pretty surprising. On Sunday morning, many crypto communities started talking about this hackathon and how they can participate in the grant to support early-stage blockchain projects. People started to flood in from ~10:00 am, and the traffic increased at a growing speed. By 12:00 pm, there have been a few hundred votes being casted among all the projects.

In the end, there were 11207 votes casted to 19 projects, 341.19BNB donated from community (worth ~74,000 USD), 5x larger than the 61.5BNB prize pool (worth ~$14,000) sponsored by Binance Smart Chain. A summary of the results is here, a real-time leaderboard of the quadratic funding grant is on HackerLink.

There were 5.5k smart contract interactions, which means there were actually quite a lot of people casted more than 1 vote to a single project.

It's my first time to see a quadratic funding grant with community donation 5 times larger than the prize pool. There are a few interesting observations.

1. Sybil attack

With large number of community votes, sybil attack became less feasible — it takes much more than the total of prize pool to dominate the prize pool. A sybil attack here needs large amount of funding to complete.

Fees can prevent sybil attack too. If we charge a fee upon donation, say 0<p<1, it has cost to donate. Still an attacker can make the following calculation.

If the attacker uses D BNBs to conduct a sybil attack, then there will be a fee of Dp charged. If its expectation to receive funding from the prize pool is smaller than D

p, the attacker will have incentive to do it.

For example, if the attacker prepared for 100 BNB for a sybil attack, he needs to pay a fee of 5 BNB. If the expectation to receive funding from prize pool is less than 5 BNB, the attacker will have no incentive to do so.

When quadratic voting becomes highly competitive, the becomes uncertain. At the hackathon, projects received far more community donation than prize pool, it was costly to conduct sybil attack — the attacker needs to prepare for a large amount of BNBs.

1. Collusion

If an attacker doesn't have large amount of BNBs, one way to attack is through collusion — "Vote for us and we will return BNB to you plus an interest".

This might happen during large-scale voting events (such as general election), but costly to do so at a hackathon or a grant.

We can introduce mechanisms lie MACI (introduced by Vitalik Buterin) to prevent this from happening.

In practice, we found a benevolent form of collusion — some projects promise future airdrops to donor addresses in communities.

1. Voting on Ethereum

We deployed the quadratic funding contract on Binance Smart Chain because BSC is the main sponsor of the event.

What will happen if voting happens on Ethereum? We can expect the following.

A. Gas fee can further prevent sybil attack by increasing cost of votes.

B. High gas fee will prevent many people from actually vote, unless the donation is much larger than the voting cost. Currently, smart contract interaction could cost ~30 USD.

1. Winners Take All

Because of the way quadratic funding algorithm distributes the prize pool, the result is winners take all. Top 5 projects took X percent of the prize pool.

Is this good or bad? It's rather a philosophical question. On one side, there are many high-quality projects at the hackathon that received less community votes. For example, Ethsign has received wide interests from judges and venture funds after the hackathon, ranked 7th on the leaderboard among the 19 projects, but only received 235 community votes (26.67 BNB) and 0.15 BNB from prize pool, because of less community votes, and received much less from the prize pool.

** comparing to NASH Protocol Meta Universe, received 2193 community votes, 123 BNB community donation and 14.9 BNB prize pool funding.

If some hackathon organizer wants a more even distribution of the fund, the algorithm can be adjusted to fit. For example, take square root or logarithm of the support area will smooth the curve and end up with an even distribution.

1. Is the community right or wrong?

Quadratic voting is community driven, we already know that. The result proved it. Two of the top-three projects are NFT games, they certainly look fancier and attract more attention.

When we fund public good, experts and community will most likely give different answers. Experts will take an "elite" view, and the community will take a "popular" view, and these two views are complementary to each other.

For a public chain, it's important to sustain a developer community that actively develop projects on the infrastructure and get funded. Quadratic funding grants can fund community spawned projects very well. A combination of expert grant and community QF grant is going to help the ecosystem development.

Currently, the BSC Grant Round-1 on HackerLink is still going on, and we will soon organize DoraHacks Global Hackathon Series in multiple countries. It will be super interesting to continue observing the dynamics of community and gradually develop the quadratic funding scheme.