

Bitcoin Grants Round 6 Retrospective

Round 6 of Bitcoin Grants has just finished, with \$227,847 in contributions from 1,526 contributors and \$175,000 in matched funds distributed across 695 projects. This time around, we had three categories: the two usual categories of "tech" and "community" (the latter renamed from "media" to reflect a desire for a broad emphasis), and the round-6-special category Crypto For Black Lives.

First of all, here are the results, starting with the tech and community sections:

Stability of income

In the last round, one [concern I raised](#) was stability of income. People trying to earn a livelihood off of quadratic funding grants would want to have some guarantee that their income isn't going to completely disappear in the next round just because the hive mind suddenly gets excited about something else.

Round 6 had two mechanisms to try to provide more stability of income:

1. A "shopping cart" interface for giving many contributions, with an explicit "repeat your contributions from the last round" feature
2. A rule that the matching amounts are calculated using not just contributions from this round, but also "carrying over" 1/3 of the contributions from the previous round (ie. if you made a \$10 grant in the previous round, the matching formula would pretend you made a \$10 grant in the previous round and also a \$3.33 grant this round)
3. was clearly successful at one goal: increasing the total number of contributions. But its effect in ensuring stability of income is hard to measure. The effect of (2), on the other hand, is easy to measure, because we have stats for the actual matching amount as well as what the matching amount "would have been" if the 1/3 carry-over rule was not in place.

First from the tech category:

Now from the community category:

Clearly, the rule helps reduce volatility, pretty much exactly as expected. That said, one could argue that this result is trivial: you could argue that all that's going on here is something very similar to grabbing part of the revenue from round N (eg. see how the new EIP-1559 Community Fund earned less than it otherwise would have) and moving it into round N+1. Sure, numerically speaking the revenues are more "stable", but individual projects could have just provided this stability to themselves by only spending 2/3 of the pot from each round, and using the remaining third later when some future round is unexpectedly low. Why should the quadratic funding mechanism significantly increase its complexity just to achieve a gain in stability that projects could simply provide for themselves?

My instinct says that it would be best to try the next round with the "repeat last round" feature but without

the 1/3 carryover, and see what happens. Particularly, note that the numbers seem to show that the media section would have been "stable enough" even without the carryover. The tech section was more volatile, but only because of the sudden entrance of the EIP 1559 community fund; it would be part of the experiment to see just how common that kind of situation is.

About that EIP 1559 Community fund...

The big unexpected winner of this round was the EIP 1559 community fund. EIP 1559 (EIP [here](#), FAQ [here](#), original paper [here](#)) is a major fee market reform proposal which far-reaching consequences; it aims to improve the user experience of sending Ethereum transactions, reduce economic inefficiencies, provide an accurate in-protocol gas price oracle and burn a portion of fee revenue.

Many people in the Ethereum community are very excited about this proposal, though so far there has been fairly little funding toward getting it implemented. This bitcoin grant was a large community effort toward fixing this.

The grant had quite a few very large contributions, including roughly \$2,400 each from myself and Eric Conner, early on. Early in the round, one could clearly see the EIP 1559 community grant having an abnormally low ratio of matched funds to contributed funds; it was somewhere around \$4k matched to \$20k contributed. This was because while the amount contributed was large, it came from relatively few wealthier donors, and so the matching amount was less than it would have been had the same quantity of funds come from more diverse sources - the quadratic funding formula working as intended. However, a social media push advertising the grant then led to a large number of smaller contributors following along, which then quickly raised the match to its currently very high value (\$35,578).

Quadratic signaling

Unexpectedly, this grant proved to have a double function. First, it provided \$65,473 of much-needed funding to EIP 1559

implementation. Second, it served as a credible community signal of the level of demand for the proposal. The Ethereum community has [long been struggling](#) to find effective ways to determine what "the community" supports, especially in cases of controversy.

Coin votes have been [used in the past](#), and have the advantage that they come with an answer to the key problem of determining who is a "real community member" - the answer is, your membership in the Ethereum community is proportional to how much ETH you have. However, they are plutocratic; in the famous DAO coin vote, a single "yes" voter voted with more ETH than all "no" voters put together (~20% of the total).

The alternative, looking at github, reddit and twitter comments and votes to measure sentiment (sometimes derided as "proof of social media") is egalitarian, but it is easily exploitable, comes with no skin-in-the-game, and frequently falls under criticisms of "foreign interference" (are those really

ethereum community members disagreeing with the proposal, or just those dastardly bitcoiners coming in from across the pond to stir up trouble?).

Quadratic funding falls perfectly in the middle: the need to contribute monetary value to vote ensures that the votes of those who really

care about the project count more than the votes of less-concerned outsiders, and the square-root function ensures that the votes of individual ultra-wealthy "whales" cannot beat out a poorer, but broader, coalition.

This raises the question: might it make sense to try to use explicit quadratic voting

(with the ability to vote "yes" or "no" to a proposal) as an additional signaling tool to determine community sentiment for ethereum protocol proposals?

How well are "guest categories" working?

Since round 5, Gitcoin Grants has had three categories per round: tech, community (called "media" before), and some "guest" category that appears only during that specific round. In round 5 this was COVID relief; in round 6, it's Crypto For Black Lives.

By far the largest recipient was Black Girls CODE, claiming over 80% of the matching pot. My guess for why this happened is simple: Black Girls CODE is an established project that has been participating in the grants for several rounds already, whereas the other projects were new entrants that few people in the Ethereum community knew well. In addition, of course, the Ethereum community "understands" the value of helping people code more than it understands chambers of commerce and bail funds.

This raises the question: is Gitcoin's current approach of having a guest category each round actually working well? The case for "no" is basically this: while the individual causes (empowering black communities, and fighting covid) are certainly admirable, the Ethereum community is by and large not experts at these topics, and we're certainly not experts on those specific projects

working on those challenges.

If the goal is to try to bring quadratic funding to causes beyond Ethereum, the natural alternative is a separate funding round marketed specifically to those communities; <https://downtownstimulus.com/> is a great example of this. If the goal is to get the Ethereum community interested in other causes, then perhaps running more than one round on each cause would work better. For example, "guest categories" could last for three rounds (~6 months), with \$8,333 matching per round (and there could be two or three guest categories running simultaneously). In any case, it seems like some revision of the model makes sense.

Collusion

Now, the bad news. This round saw an unprecedented amount of attempted collusion and other forms of fraud. Here are a few of the most egregious examples.

Blatant attempted bribery:

Impersonation:

Many contributions with funds clearly coming from a single address:

The big question is: how much fraudulent activity can be prevented in a fully automated/technological way, without requiring detailed analysis of each and every case? If quadratic funding cannot survive such fraud without needing to resort to expensive case-by-case judgement, then regardless of its virtues in an ideal world, in reality it would not be a very good mechanism!

Fortunately, there is a lot that we can do to reduce harmful collusion and fraud that we are not yet doing. Stronger identity systems is one example; in this round, Gitcoin added optional SMS verification, and it seems like in this round the

detected instances of collusion were mostly github-verified accounts and not SMS-verified accounts. In the next round, making some form of extra verification beyond a github account (whether SMS or something more decentralized, eg. BrightID) seems like a good idea. To limit bribery, [MACI](#) can help, by making it impossible for a briber to tell who actually voted for any particular project.

Impersonation is not really a quadratic funding-specific challenge; this could be solved with manual verification, or if one wishes for a more decentralized solution one could try using [Kleros](#) or some similar system. One could even imagine incentivized reporting: anyone can lay down a deposit and flag a project as fraudulent, triggering an investigation; if the project turns out to be legitimate the deposit is lost but if the project turns out to be fraudulent, the challenger gets half of the funds that were sent to that project.

Conclusion

The best news is the unmentioned news: many of the positive behaviors coming out of the quadratic funding rounds have stabilized. We're seeing valuable projects get funded in the tech and community categories, there has been less social media contention this round than in previous rounds, and people are getting better and better at understanding the mechanism and how to participate in it.

That said, the mechanism is definitely at a scale where we are seeing the kinds of attacks and challenges that we would realistically see in a larger-scale context. There are some challenges that we have not yet worked through (one that I am particularly watching out for is: matched grants going to a project that one part of the community supports and another part of the community thinks is very harmful). That said, we've gotten as far as we have with fewer problems than even I had been anticipating.

I recommend holding steady, focusing on security (and scalability) for the next few rounds, and coming up with ways to increase the size of the matching pots. And I continue to look forward to seeing valuable public goods get funded!