Privacy?

In this post, we ask the question, whether we can achieve privacy-preserving quadratic funding or what privacy guarantees one can even hope for in this context. The post is only intended to be a discussion-starter, so don't expect any rigorous arguments/protocols/solutions! (not yet!)

Quadratic funding is one of the most exciting and important developments in public goods mechanism-design by Buterin, Hitzig, and Weyl since the 1970s. A more accessible primer on quadratic funding (QF) can be foundhere. QF has already been implemented and successfully used in funding Gitcoin's grants. Gitcoin's 9th round has just been finished a few days ago with many fascinating projects.

Motivation

You don't want the whole world to know that, for instance, yousupported Edward Snowden with 10k in DAI. It might be the case, that in your jurisdiction (e.g. in the US.) it is unlawful to support such a "criminal".

Setting: super short background on QF

In QF, we have 3

types of participants.

Senders

: these are the people who wish to fund public goods in the ecosystem.

Recipients

: these are the people who seek to receive funding to be able to deliver their awesome public goods.

Smart contract/Matching pool

: there is a smart contract on chain (or might be a trusted benevolent party) who holds the matching pool. The pool is provided by benevolent actors to match the contributions of the senders according to a quadratic formula detailed below.

Quadratic Funding formula

Essentially, parties want to compute the following formula in a privacy-preserving manner. Suppose a project received k

contributions from senders each sending a contribution with value of c_i

for i\in[1\dots k]

. Then, according to the QF formula the project altogether receives (\Sigma_{i=1}^{k}\sqrt{c_i})^2

funding.

Wanted Privacy Guarantees

Let's briefly review what privacy guarantees one might hope for in a privacy-preserving Gitcoin!

Sender anonymity

Sender's identity unfortunately needs to be known. This has to do withavoiding collusion attacks against the mechanism, which cannot be circumvented without introducing identities. For example, Gitcoin relies on Github identities.

Sender confidentiality

If we cannot hide the fact that we participated in a Gitcoin grant round, can we hide the amount we contributed to a project? Sure! With confidential transactions, this problem can easily be solved.

Receiver anonymity and confidentiality

We also would like to have privacy about the projects we supported. The easiest solution would be to just use stealth addresses for funding the public projects. Imagine that each project publishes a public key on-chain that would allow any sender to contribute to the projects in an unlinkable fashion. However, in that case the smart contract/matching pool would not be able to compute the QF formula at the end of the matching round. This could potentially be solved with some clever zero-knowledge proof system, where you prove that you received k

incoming transactions each of them having value c_i

and you want your rightful matching contributions.

Vision

Most likely, a confidential QF mechanism could be implemented with the help of confidential notes akin to AZTEC confidential notes. Obviously, there might/will be some privacy loss whenever people enter and leave the confidential pool to exchange their funds from/to confidential assets. This is the curse of Ethereum not having privacy/confidentiality/anonymity by default. But, this seems to be the best approach we can hope for.