Retroactive Public Goods Funding

Optimism

Follow

Optimism PBC Blog

--

18

Listen

Share

Note: The Optimism team has long been in search of a solution on how to sustainably fund public goods, and we now have the structure of our first experiment thanks to a brilliant design by

[Vitalik Buterin

](https://twitter.com/VitalikButerin). This post is a collaboration with Vitalik as a guest author in section 2.

It's insanely hard to build an ambitious project with no business model. It's hard to get funding, to hire the best, and to persist through the hardships and obstacles of creating something great.

Startups are notoriously difficult challenges even with ample investment funding: the majority fail. But they have one important advantage - the possibility of an exit

. Exits create incentives for upfront funding, hiring, motivation and alignment through equity, a share in the exit. However, for nonprofits, FOSS, and public goods projects, this "light at the end of the tunnel" does not exist.

Given this, it's not surprising that many of the best and brightest rockstar builders, even those who genuinely want

to do maximum good, end up taking a for-profit path, even if it ends up compromising on the mission. For many, it's not simply about wealth, it's about fairness. Why toil building free software that others make massive profits off of, without any upside yourself?

So… what would happen if suddenly, exits did

exist for public goods projects? An exit determined by how much public good

has been created by the project rather than quarterly profit. Would we see more vigorous investment and innovation on technology that maximizes community benefit? Would we see more nonprofits thriving rather than surviving?

We propose a mechanism to achieve these ends below. With protocol generated revenue, retroactive public goods funding, and a Results Oracle, we will create a startup-style funding cycle for public good projects. We, the Optimism team, commit to giving all our profits made from sequencing (prior to decentralizing the sequencer) to public goods funding experiments, including the first public goods exit.

While there aren't any profits to grant yet, and details are still under development, we're excited to make this commitment now and share the foundational ideas of our first experiment!

How the retroactive public goods funding DAO works

By

[Vitalik Buterin

](https://twitter.com/VitalikButerin)

The core principle behind the concept of retroactive public goods funding is simple: it's easier to agree on what was

useful than what will be

useful

. The former is still often a source of disagreement, but it's a type of disagreement where you could still get reasonably good

top-level judgements by using some existing voting mechanism (eg. quadratic voting or even regular voting). The latter is

much more challenging. For the profit-making sector, the best that we can do is to build out an ecosystem where people can create startups and invest in them, and get rewarded if they end up correct. So rather than reinventing the wheel entirely, we will create a public-goods-oriented version of the exact same mechanism.

A DAO, which we can call “the Results Oracle”, funds public good projects. Long term, the results oracle can be funded by protocol fees (eg. if implemented by an L2 project, sequencer auctions are one candidate). But unlike other public goods funding DAOs, the Results Oracle funds projects retroactively

, rewarding projects that it recognizes as having already provided value.

The design of this oracle is a very complicated problem (see also:known long-time problems with naive approaches like coin voting), and is best approached iteratively. A simple early version might be ~20–50 hand-picked technically skilled long-time contributors from the ecosystem that is implementing this scheme. The scheme can be improved from there over time as our understanding of decentralized governance improves.

The results oracle can send rewards to any address. Here are a few possible ideas for what kinds of addresses it can send rewards to:

- A single individual or organization

that was primarily responsible for making the project happen

- A smart contract representing a fixed allocation table

splitting funds between multiple individuals and/or organizations who had contributed time and/or funding to the project

- A project token

, whose supply is distributed among one or more individuals and/or organizations who contributed time and/or money to the project, but which can be traded

In the first and second case, the results oracle would just send funds to the recipients. They could both be implemented as allocation tables, contracts which accept funds and immediately re-distribute them to recipients according to a particular split.

Project tokens are a more radical idea, essentially creating a prediction market for what the results oracle will fund

. The results oracle could use its funds to set a price floor for the token: if it allocates a reward of $X, and the project has a total supply of N tokens, then it publishes an open order to buy up to the entire supply of those tokens at a price of $X/N per token.

Funding by setting a price floor (as opposed to a one-time settlement) allows the oracle to reward the same project multiple times. It also allows a project token to get rewards both from the results oracle and from other sources (eg. other grant mechanisms, NFT-like collectible value, the project’s own economic model if it later gets one). Making multiple rewards can be done by withdrawing the funds from the pre-existing order, and making a new order setting a higher price floor using the combined funds.

Example price trajectory

Because anyone can create an allocation table or a project token for anything, there is the possibility of disagreements on contribution levels within a project leading to multiple competing allocation tables (or project tokens) for the same project. In that case, the results oracle must decide not just which project is valuable, but which project token or allocation table (or what split between multiple tokens/tables) is a better measure of who contributed. This kind of judgement cannot be avoided entirely, though it should hopefully only be required in exceptional cases.