Recently, there were few interesting posts on financing of public goods, exploring different ideas on improving/changing Quadratic Finance (QF) mechanism, originally suggested by Vitalik Buterin, Zoe Hitzig and Glenn Weyl.

These posts ([1], [2]) provoked me to think on these issues myself. I outline my suggestions in this post; all constructions are practical, and if anyone wants to join me in implementing them, or has any ideas / improvements - please be welcome to leave a comment or contact me directly.

I'm tagging authors of these topics, and hope it is not inappropriate.@Filip @llllvvuu

I want to warn the reader that I'm not an expert in the field - I've done some research, but be sure to take my propositions critically. Here is the plan of the post:

1. Motivation outline ("political manifest")

2. What's wrong with QF? Can we increase its scope?

3. My proposal, synthesyzing mutual assurance contracts [1] and revelation approach [2].

4. Closing remarks.

1. Motivation (mostly opinionated politically charged garbage, press [X] to skip)

Funding of public goods (here and after I mean by this goods that benefit large, unrestricted groups of people) is a fundamental challenge for the market economy. Uncooperated rational agents typically don't have marginal benefit justifying the funding of a public good (because while public good benefits a large group of people, it typically benefits each person less than a cost of production).

Typical solutions to these issues are:

1. Taxation. I am not in principle opposed to it, but smaller projects are typically not recognized by a state, so this works only for really large projects. There are expectations that CQF could, potentially, solve this problem. One wouldn't know until blockchain enthusiasts are allowed to run a country; which is not on the roadmap of the most projects yet.

2. Privatizing public goods. In case of digital stuff this involves DRM, copyright enforcement agencies, subscription services and other hellish creatures. It goes hand in hand with "batching" (subscription giving access to a variety of music / films). These subscription services tend to monopolize large chunk of the market, which leads to ridiculous rent extraction, and batching suppresses content which is interesting to smaller groups of people, which, in turn, [angry punk noises

] propels current cultural impotence of media, marching into the late stage of the Society of Spectacle.

Once again, I am not in principle opposed to the forces of Satan either. Privatization of public goods can be a useful mechanism, for example for extra content (like creator making custom NFTs for supporters). But, being the only feasible mechanic for funding, it leaves the creator with the choice of either dying from hunger, or selling her soul.

1. Matching funds. These are basically large organizations matching donations from private donors. (C)QF is an attempt at combining quadratic voting with matching fund, which should, in theory, result in socially optimal fund allocation. CQF is a strong proposition, but once again, external philantropist (or an organization deeply interested in the whole ecosystem) is required. This makes it infeasible for art, and a lot of other stuff (most of IT not related to blockchain too, for example).

Now, suggestion from [1] actually describes an old idea of Mutual Assurance Contract. It is worth implementing by itself, but it can be improved, and this is the main scope of my proposition.

I should also stress that even creating universal

donation service without any fancy mechanisms, yet with decent UX is an extremely valuable proposition for web3: such thing could be a Patreon analogue without taking 12% platform cut. The societal impact of having big, monopolistic donation platform bound by a smart contract, and thus not subject to the ever-growing nature of capital, is extremely valuable.

2. QF - and what's wrong with it?

Let me briefly recall what QF and its different versions are. QF matching fund takes donations $c_1, ..., c_n$

from n

participants and complements them up to the total amount is $x = (\sqrt{c_1} + ... + \sqrt{c_n})^2$

. DIt is proved that in equilibrium, total funding locally optimizes social welfare $\underset{i=1}{\overset{n}{\sum}} U_i (x) - x \rightarrow \max$

, and optimizes welfare globally, provided valuation functions U_i

are concave and sublinear.

There are few issues with QF.

1. It is hard to guess the equilibrium - while there is only one Nash equilibrium, provided $U_i(x)$

are sublinear and concave, guessing optimal contribution might be non-trivial for the participant, as information about other participants is required. This is addressed in the main [paper](#) (as "dynamic QF"), and is the focus of the post [2], which suggests that instead of actually playing

multiple rounds of QF and waiting convergence to the Nash equlibrium, we could use revelation principle

to delegate this tedious step to bots. Every participant is then motivated to reveal $U_i(x)$

truthfully.

1. $U_i(x)$

can be non-concave. Typical example is a "cold start": situation where valuation of severely underfunded project is almost zero, because it requires minimal funding to actually happen. This can (and will) create multiple Nash equilibria, typically with different projects getting nothing, depending on the choice of the equlibrium. I deem this problem inevitable; one can not compare total welfare for different Nash equlibria and choose the best because it will completely break an incentive to reveal true $U_i(x)$

.

1. This is my main concern: QF actually requires

external funding. Moreover, for the big projects funded by thousands of people, it requires enormous matching coefficient (roughly equal to the amount of contributors). There are few known fixes:

3a. CQF - capital constrained QF. This suggests linear interpolation between direct donation and QF. Matching fund should guess the coefficient $\alpha < 1$

beforehand, and then it donates $\alpha((\sqrt{c_1} + ... + \sqrt{c_n})^2 - (c_1 + ... + c_n))$

. This is, indeed, a solution, but more of a fallback - in the mode where there are thousands of similar-sized contributors, underfunding will typically be extreme unless philantropist donates much more than the community, in total.

3b. NQF - this is a term coined[here](#), which refers to the (incorrect) implementation of CQF, used in Gitcoin. The difference is that it chooses α

post factum to spend the whole external fund. As shown, it breaks the incentives in multiple ways.

3c. Taxing participants to amass matching pool. This is discussed in the main paper; I do not think it can work for systems with voluntary participation and non-aligned participants.

There is a [no-go theorem](#) which says that it is not possible to have budget balanced (no external fund), individually rational and incentive compatible mechanism with voluntary participation for funding of public goods.

1. It is trivially attacked by sybils, hence requires strong identity system.

3. Proposal

Let's consider, at first, Mutual Assurance Contract (eloquently described in [1]). This is a contract, in which one can submit n

dollars, and they are spent if and only if there are at least k

contributions of the same size, otherwise money is returned to the original senders. This basic primitive works as an "amplification device" - if my utility of the public good is at least nk

, I'm willing to send n

dollars to this contract: knowing each of my dollars counts as k

.

It is individually rational (by choosing to participate I never lose), but not incentive compatible: if I believe the good will be funded without me with high probability, I might decide to not participate even if my utility is $> nk$

. This is a problem; but I am consciously choosing to ignore it because voluntary participation implies free riding according to the no-go theorem I linked above.

Now, enter the idea of revealing utility functions of [2]. Standard revelation principle requires

that the underlying mechanism is

incentive-compatible. I, however, assume that most of the people participating in the system are happy to reveal their utility functions (after all, they are doing it voluntarily, and mechanism is individually rational). So, revealing utility functions should be treated as a "calibration mechanism" for the upcoming big "mutual assurance contract".

Protocol:

Setup

A list of public goods is determined. Each public good has a manager (possibly a bot), who will play the game on its behalf.

Step 1:

Each donor i

deposits capital and commits to some utility function U^p_i

for each public good p

. Possible UIs for writing down utility functions are discussed in [2]. Donors do not play the game afterwards, they are modelled deterministically.

Step 2:

While

(possible moves are available) do:

Each public good manager creates a slightly modified mutual assurance "contract" by declaring target value v^p

.

A random public good q

is chosen, with probability inversely proportional (? need clarification / empirical data on this) to v^q

.

Contract is filled; donors are modelled to send $[U^q(x^q + v^q) - U^q(x^q)]$

, where x^q

is a current funding level. If a contract overfills, the sends are shrunk proportionally, and the remaining money are returned to the original donors.

end do;

This keeps happening until no possible contract can be filled (there is no subset of donors that are "willing" to pay for any public good).

Closing remarks

While existence of the public good manager basically outsources the complexity of choosing equilibrium, I believe there will be a vibrant system of bots for this mechanism. Also, it ensures rational spending of resources on funding of some

public goods in a individually rational way, which is reasonable expectation for a voluntary participation system.

The in-system incentive compatibility failures (which happen because suggested mechanism for mutual assurance contract is not

incentive-compatible) can be (partially) compensated with a new token, which can be used (burned) on a platform in a normal quadratic voting / auctions in a process of curation / content discovery.

Even if the main system is not immune to collusion, it doesn't seem to break from sybil donors. I am not sure about this (and even in what assumptions could I possibly prove it), but I don't see the direct way it breaks.

This system is compatible with partial pacts with Satan (for example, artists / content creators can give NFTs, exclusive content and other stuff to their supporters through this system). It would be the duty of this platform to keep Satan in check and ensure that these added features are minor enough to not distort the incentives of the main mechanism.

License can be arranged to ensure that the content funded through this mechanism becomes free to copy and redistribute, possibly after a short Satan-flirting delay.