The purpose of this post is to describe a coordination mechanism that could be used to better fund public goods in blockchain ecosystems, serving as an alternative to both pure individual donations and on-chain "public funding" schemes of the sort I criticize here. The mechanism does NOT require any in-protocol features, so it could simply be "layered on top" of any existing blockchain.

The mechanism works as follows. Suppose that there is a currency (eg. ETH) with a set of accounts that have balances. Every period (eg. 1 week), a set of N (eg. N = 6) accounts is randomly selected (perhaps by choosing a random address and taking the nonempty account closest to it; note that the randomness should NOT be weighted by account balance). Suppose that there are M registered charities (anyone could register as a charity). Each of the N accounts is asked what percent of their tokens they are willing to contribute to each charity; that is, account i

is required to provide a vector $[p_{i,1}, p_{i,2} \ldots p_{i,M}]$

. At the end of the process, for each charity j

, $\min(p_{1,j}, p_{2,j} \ldots p_{N,j})$

(that is, the minimum of the percentages that the participants are willing to contribute to the charity) is computed. We can then determine the charity with the highest

minimum percentage, and all participants are then required to actually contribute that percent of their balances to the charity.

For example, suppose that the charities are the Apple Fund, the Pineapple Fund and the Kumquat Fund, and the participants that are called out are Alice, Bob and Charlie. Alice specifies {apple: 5, pineapple: 12, kumquat: 0}

, Bob specifies {apple: 15, pineapple: 15, kumquat: 30}

and Charlie specifies {apple: 40, pineapple: 10, kumquat: 9}

. The minima are {apple: 5, pineapple: 10, kumquat: 0}

, so the end result is that Alice, Bob and Charlie all sacrifice 10% of their deposits to the Pineapple Fund.

The mechanism is fully voluntary, because anyone can avoid getting taxed by voting [0, 0... 0]

, and because of this it can theoretically be implemented as a layer on top of existing blockchains (non-participation is equivalent to voting 0). However, there is an incentive to vote higher amounts, because by voting higher amounts you are not only potentially giving up your own money to the charity you vote for, but you also increase the money that the other participants

end up giving up. In every case, an increment to your donation either (i) is a no-op (because someone else voted less) or (ii) donates your money to the charity with N:1 leverage (at least, if all balances are equal).

You might notice that this is similar to the old idea of assurance contracts; the only thing that really differs is the presentation, and the fact that a specific set of participants is "called out" rather than opening participation to everyone. The fact that participants are chosen randomly without taking into account balance, and then called out to give a percentage, is important; it ensures that:

1. Both wealthy and small holders find it attractive to participate, as wealthy holders are large enough that they very significantly benefit from public goods produced, and small holders get very high leverage on their donations

2. Coin holders get called out to donate an amount of funds that is, in expectation, proportional to their balances, so there is no incentive to try to "hide" from being called out by splitting one's funds into many accounts or merging many users' funds into one account