Governance, Part 2: Plutocracy Is Still Bad

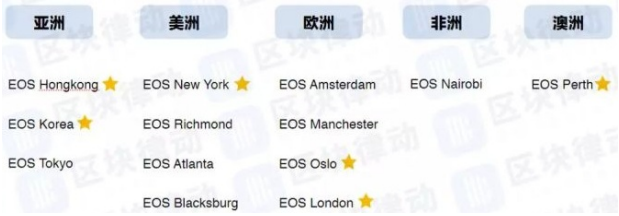
2018 Mar 28 See all posts

Coin holder voting, both for governance of technical features, and for more extensive use cases like deciding who runs validator nodes and who receives money from development bounty funds, is unfortunately continuing to be popular, and so it seems worthwhile for me to write another post explaining why I (and Vlad Zamfir and others) do not consider it wise for Ethereum (or really, any base-layer blockchain) to start adopting these kinds of mechanisms in a tightly coupled form in any significant way.

I wrote about the issues with tightly coupled voting in a blog post last year, that focused on theoretical issues as well as focusing on some practical issues experienced by voting systems over the previous two years. Now, the latest scandal in DPOS land seems to be substantially worse. Because the delegate rewards in EOS are now so high (5% annual inflation, about $400m per year), the competition on who gets to run nodes has essentially become yet another frontier of US-China geopolitical economic warfare.

And that's not my own interpretation; I quote from this article (original in Chinese):

> **EOS supernode voting: multibillion-dollar profits leading to crypto community inter-country warfare**
>
> Looking at community recognition, Chinese nodes feel much less represented in the community than US and Korea. Since the EOS.IO official Twitter account was founded, there has never been any interaction with the mainland Chinese EOS community. For a listing of the EOS officially promoted events and interactions with communities see the picture below.



> With no support from the developer community, facing competition from Korea, the Chinese EOS supernodes have invented a new strategy: buying votes.

The article then continues to describe further strategies, like forming "alliances" that all vote (or buy votes) for each other.

Of course, it does not matter at all who the specific actors are that are buying votes or forming cartels; this time it's some Chinese pools, last time it was "members located in the USA, Russia, India, Germany, Canada, Italy, Portugal and many other countries from around the globe", next time

it could be totally anonymous, or run out of a smartphone snuck into Trendon Shavers's prison cell. What matters is that blockchains and cryptocurrency, originally founded in a vision of using technology to escape from the failures of human politics, have essentially all but replicated it. Crypto is a reflection of the world at large.

The EOS New York community's response seems to be that they have issued a strongly worded letter to the world stating that buying votes will be against the constitution. Hmm, what other major political entity has made accepting bribes a violation of the constitution? And how has that been going for them lately?

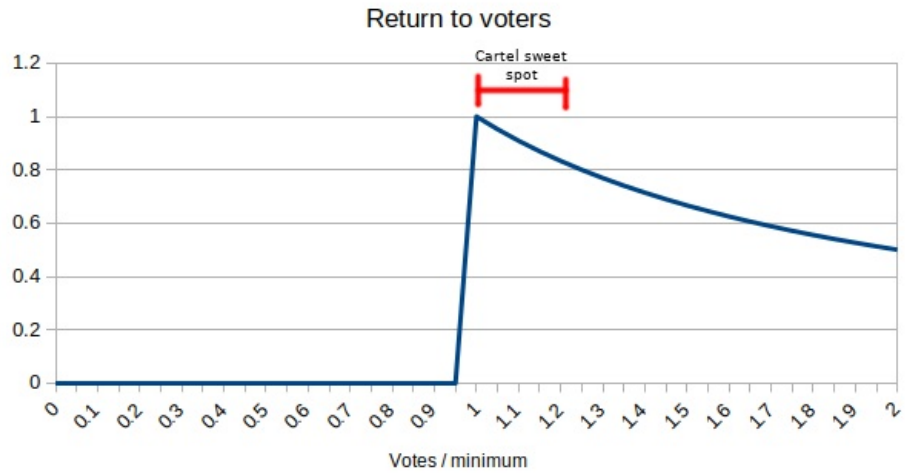
The second part of this article will involve me, an armchair economist, hopefully convincing you, the reader, that yes, bribery is, in fact, bad. There are actually people who dispute this claim; the usual argument has something to do with market efficiency, as in "isn't this good, because it means that the nodes that win will be the nodes that can be the cheapest, taking the least money for themselves and their expenses and giving the rest back to the community?" The answer is, kinda yes, but in a way that's centralizing and vulnerable to rent-seeking cartels and explicitly contradicts many of the explicit promises made by most DPOS proponents along the way.

Let us create a toy economic model as follows. There are a number of people all of which are running to be delegates. The delegate slot gives a reward of $100 per period, and candidates promise to share some portion of that as a bribe, equally split among all of their voters. The actual N delegates (eg. $N = 35$) in any period are the N delegates that received the most votes; that is, during every period a threshold of votes emerges where if you get more votes than that threshold you are a delegate, if you get less you are not, and the threshold is set so that N delegates are above the threshold.

We expect that voters vote for the candidate that gives them the highest expected bribe. Suppose that all candidates start off by sharing 1%; that is, equally splitting $1 among all of their voters. Then, if some candidate becomes a delegate with K voters, each voter gets a payment of $\frac{1}{K}$. The candidate that it's most profitable to vote for is a candidate that's expected to be in the top N, but is expected to earn the fewest votes within that set. Thus, we expect votes to be fairly evenly split among 35 delegates.

Now, some candidates will want to secure their position by sharing more; by sharing 2%, you are likely to get twice as many votes as those that share 1%, as that's the equilibrium point where voting for you has the same payout as voting for anyone else. The extra guarantee of being elected that this gives is definitely worth losing an additional 1% of your revenue when you do get elected. We can expect delegates to bid up their bribes and eventually share something close to 100% of their revenue. So the outcome seems to be that the delegate payouts are largely simply returned to voters, making the delegate payout mechanism close to meaningless.

But it gets worse. At this point, there's an incentive for delegates to form alliances (aka political parties, aka cartels) to coordinate their share percentages; this reduces losses to the cartel from chaotic competition that accidentally leads to some delegates not getting enough votes. Once a cartel is in place, it can start bringing its share percentages down, as dislodging it is a hard coordination problem: if a cartel offers 80%, then a new entrant offers 90%, then to a voter, seeking a share of that extra 10% is not worth the risk of either (i) voting for someone who gets insufficient votes and does not pay rewards, or (ii) voting for someone who gets too many votes and so pays out a reward that's excessively diluted.



Sidenote: Bitshares DPOS used approval voting, where you can vote for as many candidates as you want; it should be pretty obvious that with even slight bribery, the equilibrium there is that everyone just votes for everyone.

Furthermore, even if cartel mechanics *don't* come into play, there is a further issue. This equilibrium of coin holders voting for whoever gives them the most bribes, or a cartel that has become an entrenched rent seeker, contradicts explicit promises made by DPOS proponents.

Quoting "Explain Delegated Proof of Stake Like I'm 5":

> If a Witness starts acting like an asshole, or stops doing a quality job securing the network, people in the community can remove their votes, essentially firing the bad actor. Voting is always ongoing.

From "EOS: An Introduction":

> By custom, we suggest that the bulk of the value be returned to the community for the common good - software improvements, dispute resolution, and the like can be entertained. In the spirit of "eating our own dogfood," the design envisages that the community votes on a set of open entry contracts that act like "foundations" for the benefit of the community. Known as Community Benefit Contracts, the mechanism highlights the importance of DPOS as enabling direct on-chain governance by the community (below).

The flaw in all of this, of course, is that the average voter has only a very small chance of impacting which delegates get selected, and so they only have a very small incentive to vote based on any of these high-minded and lofty goals; rather, their incentive is to vote for whoever offers the highest and most reliable bribe. Attacking is easy. If a cartel equilibrium does not form, then an attacker can simply offer a share percentage slightly higher than 100% (perhaps using fee sharing or some kind of "starter promotion" as justification), capture the majority of delegate positions, and then start an attack. If they get removed from the delegate position via a hard fork, they can simply restart the attack again with a different identity.

The above is not intended purely as a criticism of DPOS consensus or its use in any specific blockchain. Rather, the critique reaches much further. There has been a large number of projects recently that extol the virtues of extensive on-chain governance, where on-chain coin holder voting can be used not just to vote on protocol features, but also to control a bounty fund. Quoting a blog post from last year:

> Anyone can submit a change to the governance structure in the form of a code update. An on-chain vote occurs, and if passed, the update makes its way on to a test network. After a period of time on the test network, a confirmation vote occurs, at which point the change goes live on the main network. They call this concept a "self-amending ledger". Such a system is interesting because it shifts power towards users and away from the more centralized group of developers and miners. On the developer side, anyone can submit a change, and most importantly, everyone has an economic incentive to do it. Contributions are rewarded by the community with newly minted tokens through inflation funding. This

> shifts from the current Bitcoin and Ethereum dynamics where a new developer has little incentive to evolve the protocol, thus power tends to concentrate amongst the existing developers, to one where everyone has equal earning power.

In practice, of course, what this can easily lead to is funds that offer kickbacks to users who vote for them, leading to the exact scenario that we saw above with DPOS delegates. In the best case, the funds will simply be returned to voters, giving coin holders an interest rate that cancels out the inflation, and in the worst case, some portion of the inflation will get captured as economic rent by a cartel.

Note also that the above is not a criticism of *all* on-chain voting; it does not rule out systems like futarchy. However, futarchy is untested, but coin voting *is* tested, and so far it seems to lead to a high risk of economic or political failure of some kind - far too high a risk for a platform that seeks to be an economic base layer for development of decentralized applications and institutions.

So what's the alternative? The answer is what we've been saying all along: *cryptoeconomics*. Cryptoeconomics is fundamentally about the use of economic incentives together with cryptography to design and secure different kinds of systems and applications, including consensus protocols. The goal is simple: to be able to measure the security of a system (that is, the cost of breaking the system or causing it to violate certain guarantees) in dollars. Traditionally, the security of systems often depends on *social* trust assumptions: the system works if 2 of 3 of Alice, Bob and Charlie are honest, and we trust Alice, Bob and Charlie to be honest because I know Alice and she's a nice girl, Bob registered with FINCEN and has a money transmitter license, and Charlie has run a successful business for three years and wears a suit.

Social trust assumptions can work well in many contexts, but they are difficult to universalize; what is trusted in one country or one company or one political tribe may not be trusted in others. They are also difficult to quantify; how much money does it take to manipulate social media to favor some particular delegate in a vote? Social trust assumptions seem secure and controllable, in the sense that "people" are in charge, but in reality they can be manipulated by economic incentives in all sorts of ways.

Cryptoeconomics is about trying to reduce social trust assumptions by creating systems where we introduce explicit economic incentives for good behavior and economic penalties for ban behavior, and making mathematical proofs of the form "in order for guarantee \(X\) to be violated, at least these people need to misbehave in this way, which means the minimum amount of penalties or foregone revenue that the participants suffer is \(Y\)". Casper is designed to accomplish precisely this objective in the context of proof of stake consensus. Yes, this does mean that you can't create a "blockchain" by concentrating the consensus validation into 20 uber-powerful "supernodes" and you have to actually think to make a design that intelligently breaks through and navigates existing tradeoffs and achieves massive scalability in a still-decentralized network. But the reward is that you don't get a network that's constantly liable to breaking in half or becoming economically captured by unpredictable political forces.

---

1. *It has been brought to my attention that EOS may be reducing its delegate rewards from 5% per year to 1% per year. Needless to say, this doesn't really change the fundamental validity of any of the arguments; the only result of this would be 5x less rent extraction potential at the cost of a 5x reduction to the cost of attacking the system.*
2. *Some have asked: but how can it be wrong for DPOS delegates to bribe voters, when it is perfectly legitimate for mining and stake pools to give 99% of their revenues back to their participants? The answer should be clear: in PoW and PoS, it's the protocol's role to determine the rewards that miners and validators get, based on the miners and validators' observed performance, and the fact that miners and validators that are pools pass along the rewards (and penalties!) to their participants gives the participants an incentive to participate in good pools. In DPOS, the reward is constant, and it's the voters' role to vote for pools that have good performance, but with the key flaw that there is no mechanism to actually encourage voters to vote in that way instead of just voting for whoever gives them the most money without taking performance into account. Penalties in DPOS do not exist, and are certainly not passed on to voters, so voters have no "skin in the game" (penalties in Casper pools, on the other hand, **do** get passed on to participants).*