Thoughts on fees and governance decisions

June 18, 2018

1 Estimates of PNK value by potential jurors

For each court in which a PNK holder could activate her PNK, there will be some fee f paid in ETH per ruling and a cost $w_{\mathcal{USR}}$ of the work (on average) required to make this ruling honestly. Suppose there are N PNK activated in a subcourt, and that there are K PNK required to rule on the cases to be arbitrated in a given period. Assume a prevailing interest rate of r per period.

We make a couple of simplifying assumptions:

- Note that f, K, r, N, and $w_{\mathcal{USR}}$ can all vary from period to period, and in the case of $w_{\mathcal{USR}}$, even from case to case within a period. For now, we assume these variables change slowly enough to be approximated as being constant.
- Sometimes jurors will rule honestly and will nonetheless be in the minority.When this happens, they will lose PNK as a penalty. On the other hand, in other cases jurors will gain PNK from jurors in the minority, whether those jurors are failed attackers or honest jurors who got unlucky. We expect the gains and losses of PNK to mostly average out for an honest juror. For the following computations, we assume these gains and losses exactly average out, and that an honest juror keeps the same amount of PNK from one period to the next.

Then activating a PNK is worthwhile if either

- $f > w_{\mathcal{USR}}$ or
- $f >$ value of PNK deposited $\cdot \frac{\text{number of choices per decision} - 1}{\text{number of choices per decision}}$

depending on whether $\mathcal{USR}$ invests the time to be honest or not. (As a more sophisticated model, you can imagine that the more time $\mathcal{USR}$ devotes to deciding on a case, the higher probability she has of ruling correctly, following some distribution rather than this binary cutoff.)

In the $w_{\mathcal{USR}} > f$ case, $\mathcal{USR}$ essentially receives value of $f - w_{\mathcal{USR}}$ each time she is drawn as a juror.

As K tokens out of N are chosen with replacement, the number of times that $\mathcal{USR}$ is selected as a juror per period X is distrbuted as X Binomial$(K, 1/N)$. In particular, $E(X) = \frac{K}{N}$.

Then the value of the PNK to $\mathcal{USR}$ should be no less than the expected present values of the sequence of future payments of $f - w_{\mathcal{USR}}$ for each ruling for which this PNK is selected:

$$\begin{aligned}\text{Value PNK} &\geq \sum_{\text{period } i=1}^{\infty} E\left((f - w_{\mathcal{USR}})(1+r)^{-i} \cdot X\right) \\ &= \sum_{\text{period } i=1}^{\infty} (f - w_{\mathcal{USR}})(1+r)^{-i} \cdot E(X) \\ &= \frac{f - w_{\mathcal{USR}}}{r}\frac{K}{N}. \end{aligned} \tag{1}$$

2 Heuristics on how rational jurors make fee decisions to maximize returns under different models

The measure of how strong a system is against a 51% attack should be:

What financial cost must a party (possibly an existing token holder) assume in order to obtain 51% of the PNK, minus whatever (presumably reduced) amount can be obtained for these PNK after the attack?

This is heuristically approximated by 51% of the PNK marketcap, or the cost of buying 1 PNK (or a small amount) times half of the number of PNK. In practice, the cost of a 51% attack (at least by someone who does not already hold a large percentage of the tokens) should be higher due to lack of market liquidity causing the successive tokens an attacker buys to increase in cost.

In a liquid voting setup where each PNK holder has the right to vote in the decisions of each subcourt (even those where she is not actively participating), for any given decision PNK holders will fall into two broad camps

- those who participate in the court and want to benefit directly from whatever policy is put in place (e.g. by being paid higher fees)
- those who want to maximize the value of PNK

(A more honest model would allow that any given token holder may begin to participate in a given subcourt if the fees are high enough, and thus has some vested interest in the decisions of each court even if only these decisions are only relevant to that token holder in extreme and unlikely cases.)

Heuristic 1 *If a court only has a minority of PNK actively participating in it, then each decision in such courts should be made to maximize the value of PNK*

if the PNK holders are rational (or more reasonably if they delegate their votes to delegates making such rational choices). Hence choices are made in these courts which maximize the marketcap of PNK, and hence maximize our rough heuristic stand-in for the cost of a 51% *attack as above.*

The assumption that only a minority of PNK holders actively participate is likely a reasonable assumption for all subcourts, namely all courts other than the general court, as users must chose which subcourts they want to activate in.

However, if a majority of (economically rational) token holders are actively participating in a given court, it is not necessarily the case that they will be incentivized to make decisions that optimize for security against 51% attacks, as illustrated in the following (somewhat contrived) example:

Example 1 *Consider we have a system where there are 7 total PNK that are currently held 1 token each by A, B, C, D, E, F, and G.*

Their cost in effort to issue a ruling is as follows:

$\mathcal{USR}$	A	B	C	D	E	F	G
$w_{\mathcal{USR}}$	1	1	1	1	2	2	2

There may be other participants in the market for these tokens, but we assume that their corresponding $w > 2$. Furthermore, some of A, B, C, D, E, F, and G may be interested in buying additional tokens, but due to the marginal utility of their time, their corresponding w for such an additional token would also be greater than 2*.*

We assume that the market for dispute resolution in this court is fairly inelastic up to fees of $f = 2.2$, after which point a competitor offers cheaper dispute resolution and the demand for the services of this court sharply drop off.

Then, it is in the interests of A, B, C, and D (being symmetrical actors) to vote in such a way that maximizes their own returns, which in this case is based on not having their fees paid diluted by the participation of E, F, and G.

Suppose $K = 3$ for all cases and we have some fixed rate of interest r. Then, if fees are set at $f = 1.9$, then the value of a PNK to A, B, C, and D is

$$\frac{1.9-1}{r}\left(1-\frac{5-3}{5}\right)=\frac{.54}{r}.$$

On the other hand, the PNK of E, F, and G are largely worthless as it is not profitable for them to be activated and the resale market is such that there are no other buyers for whom it would be profitable. (If n = number of choices per decision, these PNK may be reasonably valued at

$$f+f\frac{1}{n}+f\frac{1}{n^2}+f\frac{1}{n^3}+....=f\left(\frac{1}{1-1/n}\right)$$

as this is the expected value of fees that a user could gain through random choices before losing her PNK. If r is small, this value can be taken as negligible for these calculations.)

If fees are then increased to $f = 2.2$, the value of a PNK to A, B, C, or D decreases to

$$\frac{2.2-1}{r}\left(1-\frac{7-3}{7}\right)=\frac{.51428}{r},$$

while the value to E, F, and G increases to

$$\frac{2.1-2}{r}\left(1-\frac{7-3}{7}\right)=\frac{.08571}{r}.$$

Then the cost to 51% attack the system when $f = 1.9$ is only the cost to buy one of the tokens of A, B, C, or D - namely $\frac{.54}{r}$ plus the negligible cost to buy the tokens of E, F, and G, while the cost to 51% attack the system when $f = 2.2$ is the cost of buying the tokens of E, F, and G, plus one of the tokens of A, B, C, and D; namely, $3 \cdot \frac{.08571}{r} + \frac{.51428}{r} = \frac{.77141}{r}$.

So we see that it is in the interests of A, B, C, and D to vote so that the E, F, and G do not activate their tokens. As A, B, C, and D constitute a majority, under standard assumptions of economic rationality, they vote this way. On the other hand, this reduces security against 51% attack compared to global optimums.

Remark 1 *Such examples may occur in subcourts where the assumptions of Heuristic 1 fail, particularly the general court. However, by its nature, the general court does not require specific skills, so the sharp increase in w from a small core of expert jurors to the broader population that made Example 1 possible is unlikely to occur there.*

Remark 2 *Consider the following alternative model of voting: after each ruling by the (sub)court, jurors that are ruled coherent can each adjust the fees of the (sub)court up or down by up to some fixed amount. This is akin to the gas voting that determines the gaslimit in Ethereum.*

This model seems a priori reasonable, and one could argue that it is more federal/modular, allowing the decisions of a court to be made by the jurors who are really involved. However, the assumptions of Heuristic 1 would not hold in this model by construction, and we expect that such courts would be much more likely to have situations like that of Example 1 and to produce governance decisions that do not optimize for defense against 51% attacks than the liquid voting model.

Remark 3 *Note how this discussion fundamentally differs from Augur's current model, where there are no subcourts or random selection, and the fees are chosen for the whole system together. Thus there is never a pool of token holders who are actively participating in the system, but indifferent to individual governance and fee choices.*

3 Governance decisions to make and inter-relations

Governance decisions can control a priori all of the following:

- fees
- minimum_deposit (which is lost by a PNK holder for an incoherent decision)
- amount of time to reach decision
- penalty if don't respond at all (higher than amount lost for incoherent decision)
- parent court/where subcourt is in tree
- rules/instructions to be given to jurors - e.g. when a case is out of the scope of the court and should be ruled as non-classifiable, including geographic restrictions etc.
- electoral system (e.g. Condorcet versus IRV if we decide there are multiple good options and want to allow modularity)
- whether to use zk-blinded appeals/ other plug-inable features (to encourage modularity)

Interactions:

- should choose the fees f such that $f <$ value of PNK deposited$\cdot \frac{\text{number of choices per decision}-1}{\text{number of choices per decision}}$ - may require (constant) use of price oracle for PNK versus ETH.
- amount of time to reach a decision is a trade-off between the time required to do a good job (and implicitly influencing the work required to be a juror $w_{\mathcal{USR}}$, particularly if the time is so short that the job becomes more difficult) versus the effectiveness of time griefs. While the effects of the tradeoff here are more subtle than the choice of f versus number of cases tradeoff, ultimately changes that affect the value of $w_{\mathcal{USR}}$ for a large pool of users will affect the value of PNK via equation 1. On the other hand setting a period length that makes time griefs costly and common will decrease demand for the system and decrease the number of cases. So we still expect liquid voting by rational actors to fix optimal values for the period length under the assumptions of Heuristic 1.