Determining a quorum in weighted Fait Accompli with local sortition

This is an adaption of Figures 6 and 3 of the following paper, but with elaboration and additional explanation.

> Peter Gazi, Aggelos Kiayias, and Alexander Russell. 2023. Fait Accompli Committee Selection: Improving the Size-Security Tradeoff of Stake-Based Committees. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23). Association for Computing Machinery, New York, NY, USA, 845–858. https://doi.org/10.1145/3576915.3623194.

Stake distribution

Let $P = (p_1, \ldots, p_{|P|})$ be the set of active stake pools, each with stake $\mathcal{S}(p_i)$, where pools are ordered in a non-increasing fashion, $p_i \geq p_{i+1}$. Furthermore, let $\rho_i = \sum_{j=i}^{|P|} \mathcal{S}(p_j)$ be the total stake for pools p_i and beyond. By definition, the total stake is ρ_1.

Committee size

Let n be the *target* number of seats on the committee. Because of the variability of local sortition, this may not be the exact number of seats determined by the algorithm.

Persistent seats

The number of persistent seats is $n_1 = i^* - 1 \leq n$, where i^* is the smallest $i \in \mathbb{N}$ such that either $\rho_i = 0$ or $\left(1 - \frac{\mathcal{S}(p_i)}{\rho_i}\right)^2 \geq \frac{n-i}{n-i+1}$. The weights of those seats is simply the stake, $w_C(i) = \mathcal{S}(p_i)$ for $i \in [1, n_1]$. Specifically, the first n_1 pools have persistent seats.

Non-persistent candidates

The pools p_i for $i \in [i^*, n]$ are all *candidates* for having a non-persistent seat. The stake distribution among the non-persistent pools is defined as $\mathcal{S}_3 = \mathcal{S}(p_i)/\rho_{i^*}$ for $i \in [i^*, n]$.

Local sortition for non-persistent seats

The *target* number of non-persistent seats on the committee will be $n_2 = n - n_1$. (Figure 6 of the paper uses n_2 for the *actual* number of non-persistent seats, but the local-sortition approach here differs from the paper in that the actual number of non-persistent seats may differ slightly from the target n_2.)

Let $\sigma_i \in [0, 1]$ be the VRF value for party p_i, derived from their signature on the election identifier and the Praos nonce for the epoch.

The number of seats they have on the committee is the value k_i^* for which $P(k_i^* - 1) \leq \sigma_i < P(k_i^*)$ holds, given $P(k^*) = \sum_{k=0}^{k^*} \frac{(n_2 \cdot \mathcal{S}_3(i))^k \cdot e^{-n_2 \cdot \mathcal{S}_3(i)}}{k!}$ for $k^* \geq 0$ and $P(k^*) = 0$ otherwise. (This is simply sampling from a Poisson distribution with mean $n_2 \cdot \mathcal{S}_3(i)$ according to cumulative probability σ_i.) Each of those seats has weight ρ_{i^*} / n_2. (Once again, this scheme differs slightly from the paper in that ρ_{i^*} is divided by the *target* number of non-persistent seats, not the *actual* number of non-persistent seats; note that the *actual* number of non-persistent seats is not publicly known because the sortition is *local*.)

Variability of committee size

The weight of persistent voters is exactly $\rho_1 - \rho_{i^*}$ by construction. Because the sum of Poisson distributions is also Poisson, the expected number of non-persistent seats is n_2 and they have total expected weight $n_2 \cdot (\rho_{i^*} / n_2) = \rho_{i^*}$. Thus the expected total weight is ρ_1, which equals the total active stake.

The number of non-persistent seats varies according to the Poisson distribution, having a standard deviation $\sqrt{n_2}$. Thus the standard deviation of the expected non-persistent weight is $\sqrt{n_2} \cdot (\rho_{i^*} / n_2) = \rho_{i^*} / \sqrt{n_2}$. This is also the standard deviation of the total weight.

In terms of probability distributions, the total weight is $\rho_1 + \rho_{i^*} \cdot \left(\frac{\mathbf{n_2}}{n_2} - 1 \right)$, where $\mathbf{n_2}$ is a Poisson random variable with mean n_2.

Summary

1. The number of persistent seats, n_1 is solely determined by the stake distribution.
   - A pool only occupies at most one persistent seat and the weight of that seat is equal to their stake.
   - Persistent seats stay constant over the epoch.
2. The number of non-persistent seats, whose expectation is n_2, varies according to the VRF values σ_i used for each pool's eligibility.
   - A pool may occupy several seats.
   - Each seat is equally weighted at one n_2th of the total non-persistent stake.
3. The total weight in an election is $\rho_1 \pm \frac{\rho_{i^*}}{\sqrt{n_2}}$. The full probability distribution for the total weight provides guidance on choosing a safe value of the quorum threshold τ.
   - In Peras, τ should be chosen with two constraints in mind:
     1. (safety) The probability that an adversary controlling <50% of stake could, with the help of honest parties, produce two conflicting certificates in the same vote must be vanishingly small. This is because certificate equivocation is assumed to be a

    negligible-probability event in the protocol's safety argument, which must hold even in face of almost-1/2 adversaries. In more detail, if A denotes the fraction of adversarial weight on the committee, then the above constraint results in an inequality $A + (1 - A)/2 < \tau$ (if the adversary splits honest parties in half and adds his votes to both certificates), which results in $A < 2\tau - 1$. Hence, assuming that the adversary has at most a-fraction of stake in the overall population (with a close to $1/2$), we need to choose τ so that the probability that the committee selection on a-corrupted population gives us a $(2\tau - 1)$-corrupted committee is acceptably small.
    2. (optimistic liveness) The downward pressure on τ comes from the fact that an adversary controlling more than $1 - \tau$ weight on the committee can halt certificate creation by just abstaining. This "only" prevents the optimistic path of the protocol, and so it is acceptable to only protect from weaker adversaries here. In particular, one way to parametrize is to first set τ based on the safety requirement above, and then compute the threshold α (this will be $< 1/4$) such that if the corruption in the population is below α then except with negligible probability (say admitting the same error as allowed in the safety case) the adversary will not have enough weight on the committee for the abstain attack.
  - In Leios, τ should be chosen so that there is a vanishingly small probability that <50% adversarial stake could obtain a quorum or veto an otherwise honest quorum.

Numerical example

Consider the stake distribution of Epoch 535 of Cardano mainnet and vary the committee size n . The table below[1] shows that . . .

- The stake of the persistent seats comprises > 80% of the committee's total weight.
- The standard deviation of the total weight is nearly 2% for the smaller committees and a small fraction of a percent for larger committees.
- Noticeable adjustment to the quorum threshold τ is needed to account for a one-in-million chance ("1 ppm tail" in the table) of extremely unlucky sortition (i.e., far fewer seats than expected).
  - For a committee size of 700, Peras would need $\tau \approx 78.52\%$ and Leios would need $\tau \approx 53.52\%$.
  - For a committee size of 1000, Peras would need $\tau \approx 75.76\%$ and Leios would need $\tau \approx 50.76\%$.
  - One part per million may would be an overly conservative setting, since it means that a 25% (or 50%) adversary for Peras (or Leios) would succeed in defeating (or obtaining) a quorum once in a million elections.

Committee Size	Persistent Seats	Persistent Weight	Standard Deviation of Total Weight	1 ppm Tail of Total Weight
500	406	0.8237168	0.0181822269	0.097518383
600	505	0.8964108	0.0106280267	0.056701452
700	601	0.9367007	0.0063618203	0.035166285
800	701	0.9618550	0.0038337146	0.021191655
900	801	0.9770417	0.0023073956	0.012754609
1000	903	0.9864321	0.0013776087	0.007553248
1100	1007	0.9921898	0.0008098848	0.004283038
1200	1107	0.9954256	0.0004743450	0.002508552

[1] See this Jupyter notebook for details of the computations. ↩