TLDR

: We suggest a way to enforce a safe minimum notary pool size.

Background

Two bad things can happen with a notary pool that is too small:

- Overwork

: The amount of work per notary (largely bandwidth) is inversely proportional to the notary pool size. To preserve notary decentralisation, bandwidth requirements for individual notary identities should be manageable by a mainstream internet connection. A given notarisation scheme (parametrised by committee size, collation size, period length, number of shards, minimum deposit, etc.) will have a corresponding safe (minimum) notary pool size relative to a maximum acceptable internet connection speed.

- Takeover

: The amount of capital an attacker has to deploy to take over notorisation (which may include fully notarising withheld or equivocated collations, delaying or stalling notorisation, breaking the RNG, etc.) is proportional to the notary pool size. A given notarisation scheme (parametrised by implicit or explicit voting thresholds) will have a corresponding safe (minimum) notary pool size relative to a minimum acceptable capital threshold for takeover.

Below we suggest infrastructure to enforce a minimum notary pool and mitigate notary overwork and takeover risks.

Construction

When the sharding scheme is first deployed, and more generally whenever the safe notary pool size is increased (e.g. because more shards are instantiated), the SMC managing deposits undergoes a bootstrap phase. Similar to a KickStarter project there are deposit thresholds for system activation. Activation can be all-or-nothing with a single threshold, or be gradual e.g. with shards activated with individual granularity.

After activation the system maintains the safe pool size with a priority queue. Deregistration requests by individual notaries are processed immediately if the pool size stays above the minimum. Otherwise deregistration requests are queued until new notaries add to the deposit pool. At that point deregistration priority is given to the notary with the oldest deposit.

Discussion

The main risk for notaries is “deregistration tail risk”—everyone cannot de-register immediately. In exceptional circumstances the queuing mechanism would be a backstop that provides the sharding infrastructure with a “guaranteed steady state”, buying time for a solution to kick in. Such a solution may be an external intervention by the community (e.g. a hard-fork) or a protocol-level response (e.g. an automatic increase in collation subsidies).