TLDR

: We combine a RANDAO scheme with a threshold mechanism to force-reveal preimages of inactive participants. Thanks to Bernado David (author of SCRAPE) for feedback and suggestions.

Construction

For registration, a participant P

picks a secret s

and posts onchain a hashchain commitment $c = H^{1024}(s)$

. After some time, P

is assigned an honest-majority committee to which he must respond with publicly verifiable shares of s

and a zk-proof that the shares faithfully correspond to c

. Specific constructions:

- PVSS

: We use the SCRAPE construction for the shares of the secret s

. Using $n/2$

exponentiations where n

is the size of the committee we build a DLOG-based commitment of the form h^s

where h

is a random group generator.

- zk-proof

: We build a zkSNARK that s

is the 1024th preimage of c

and that the same s

is the exponent in the commitment h^s

.

At every round a participant is selected to reveal his next hashchain preimage. If he does not, the committee corresponding to the participant reconstructs his secret, submit the preimage on his behalf, and the inactive participant is slashed.

Discussion

With a 50%+ honest majority assumption the above construction yields a fork-free grinding-free RANDAO. In the default case a single message is required to generate the next RNG output. In the exceptional case, $n/2$

messages are required.

The most expensive part of the setup phase is the zk-proof that s

is the 1024th preimage of c

. As benchmarked by Jacob Eberhardt, it takes 5 seconds per 64 hashes. So the setup phase would require ~2 minutes of compute time for each participant.

Assuming 1,000 participants and 5-second periods, the registration phase must be renewed every 1000 * 1024 * 5 / 60 / 60 / 24 ~= 60 days (one “era”).