TL;DR:

A probabilistic proof of custody using only one bit per attestation has been suggested before, and is currently specified for inclusion in phase 1 of the Eth2.0 rollout. It is actually possible to extend this method to make the overhead so small that no separate data structure at all is needed: Instead, a (very small) number of shard block attestations is “poisoned”, and signing a poisoned attestation makes a validator slashable in the same way an incorrect custody bit does. We can therefore simplify the attestation data structures and logic by removing the custody bits.

Background

In order to avoid the “honest but lazy” validator problem, validators have to compute a “proof of custody” that shows that they actually possess a copy of the data that is being signed. @JustinDrake introduced the idea of a 1-bit proof of custody [1] that mixes an ephemeral secret only known to the validator with the data and computes one bit. Later, validators have to reveal their ephemeral secret and everyone can check the custody bit was computed correctly.

A validator has a 50% chance of guessing the custody bit correctly without doing any computation (and thus, without requiring the data). However, since the penalty of slashing is high, this has a negative expected return, and the “lazy” validator is discouraged from doing so.

Current implementation

In order to be maximally MPC-friendly [2], the current implementation is as follows: Let p=2^{256}-189

. During each custody period, a validator computes a custody secret that consists of three numbers s_0, s_1, s_2 \in \mathbb{Z}_p

. The polynomial Universal Hash Function on the data chunks d_0, \ldots, d_{n-1}

is defined as

\mathrm{UHF}(d_0, \ldots, d_{n-1},s_0, s_1, s_2) = \sum_{i=0}^{n-1} d_i s_{i \mod 3}^i + s_{n \mod 3}^n

To compute a single bit from the UHF-output in an MPC-friendly way, we take the Legendre symbol as the custody bit:

\mathrm{custodybit} = L_p(\mathrm{UHF}(d_0, \ldots, d_{n-1},s_0, s_1, s_2) + s_0)

where L_p

is the Legendre symbol [3] normalized to one bit, i.e.

L_p(x) = \left\lfloor \frac{1}{2}\left(\left(\frac{x}{p}\right) + 1 \right) \right\rfloor \text{.}

Suggested updated construction

We start with the observation that any risk of incurring a slashing, with an expected loss that is greater than the average reward per epoch, would deter an honest but lazy validator from attesting without computing the proof of custody. With the current custody bit construction, the probability is 50%. Using the current beacon chain spec, at 0.5M Eth staked (the very low end for security), the reward is around 100k GWei per epoch, but the cost of slashing is 1 Eth (1 billion GWei) (both at 32 Eth staked, proportionally lower if less). This suggests even a 1/1000 chance of getting slashed is plenty of a deterrent, as the expected loss is still ten times the gain per attestation. Since we aren’t concerned about malicious (only rational) behaviour, this analysis suggests we could use a custody bit that is one 99.9% of the time and 0 only 0.1% of the time.

Given this, we can just remove the custody bit from the attestation data entirely, and say an attestation is simply invalid (and slashable) if the custody bit is 0, so that we don’t need to store it. The new custody bit is computed as the logical OR

of the ten Legendre bits

\mathrm{custodybit}*i = L_p(\mathrm{UHF}(d_0, \ldots, d*{n-1},s_0, s_1, s_2) + s_0 + i)

for i=0, \ldots, 9

. This will be zero with probability 1/1024.

Analysis

The main advantage is a slight reduction in spec complexity and smaller attestations.

The only disadvantage of this construction is a tiny loss in the number of attestations. This should not lead to any serious security loss.

The MPC-friendlyness of the construction is preserved, and the overhead will only be increased by a tiny bit from having to compute 10 bits instead of one. Assuming that the Legendre PRF [4] is secure, the OR computation can be done in the open by secret shared validators, so we still only need a single round of online MPC computation.

A further interesting property is that since the information leak is only 0.001 bits per attestation, and with 2048 attestations per custody period, only an expected 2 bits of the custody secret are leaked, making the construction information theoretically secure with respect to recovery of the custody secret (for non-MPC validators).

[1] 1-bit aggregation-friendly custody bonds

[2] Using the Legendre symbol as a PRF for the Proof of Custody

[3] https://en.wikipedia.org/wiki/Legendre_symbol

[4] https://legendreprf.org