Hi all,

At Pegasys R&D, we are currently working on a fast

multi-signature aggregation protocol at scale in the presence of Byzantine nodes. Our work lies on top of the San Fermin [0] protocol which is a fast data aggregation protocol with a logarithmic communication complexity. The key insight in San Fermin that the aggregation happens in parallel amongst all nodes, and nodes aggregate larger chunks of data at each phase of the protocol; the number of phase being logarithmic to the number of nodes. San Fermin alone allows for tens of thousands of nodes to aggregate data in a few seconds. Unfortunately, San Fermin is defined in the fail-stop model and we are exploring ways to make it work in the Byzantine model. In that respect, our work-in-progress adds redundancy at each steps of the base protocol to decrease as much as possible the probability of successful attacks such as eclipse attacks

(where contributions of honest nodes are ignored), while keeping the protocol as fast as possible. While we are still in the research phase, we are working on a paper with a clear description of our threat model, our protocol, an analysis and large-scale experiments. At a second time, we want to deliver an open source library implementing our protocol

tailored to the Ethereum 2.0 context using BLS12-381.

We would be very interested to know if anybody else is working on a similar topic; please reach out to us !

Also, we will be present at the Eth2 meeting in Prague next week, and will be happy to discuss our ideas with folks interested by this subject!

Blazej Kolad, Nicolas Gailly, Nicolas Liochon & Olivier Begassat

Pegasys R&D, Consensys

[0] https://www.usenix.org/conference/nsdi-08/san-fermín-aggregating-large-data-sets-using-binomial-swap-forest