

I had an idea for aggregating votes off-chain and validating them on-chain with Kate commitments and BLS signatures. There is at least one loophole to be closed and potentially lots of ways to make it more elegant, but this should be enough detail to explain the idea in a way that someone with more experience can critique it. Feedback is most welcome!

<https://nikeshnazareth.github.io/vote-aggregation/>