

Once again, nice write up!

Why do the tokens need to be bundled together? Why can't I just buy 100 LST for each of the 5 validators I choose than receiving 1 LST that represents 500 TIA that is evenly distributed across the 5 validators?

If there were only 100 types of LSTs it would make them more fungible than having numerous permutations of LSTs per basket of validators.

Put another way, could the picking and redistribution of stake to validators be something solved in the front end and the chain itself remains simpler.

On a totally different note, given that most attacker will try to exit within the first 10 minutes say, It might be good to have two queues:

- Cumulative diff in validator set can't exceed 1/3 in 3 months; and
- Cumulative diff in validator set can't exceed 5% in 10 minutes

Also, you've mentioned using a cumulative diff queue instead of a net diff queue i.e. if I redelegate 1000 tokens from A to B and then from B to A, the validator set hasn't changed at all however cumulative diff would think it had changed by 2000 tokens. What's your view on the tradeoffs