Cryptoeconomic aggregate signatures (CAS) could be used to reduce forking inRANDAO-based main chains. Here is a concrete protocol for this.

A block must include, along with the other data, a CAS for a random sample of notaries that signed off on the previous block. In general, notaries will refuse to sign off on a block that they do not think is the head, so the only way to make a CAS to revert any blocks is to make a false one, which would lead to every validator making an off-head block sacrificing their deposit (think: ~10-50 ETH per block)

Now, can we improve the properties of the system by going from an honest majority model to an uncoordinated majority model. First, we can incentivize notaries to sign fairly simply by adding a reward to every notary listed in a CAS. This technically incentivizes being listed in a CAS, not signing, but in general CASes will not be willing to list nonexistent signatures so it could be close enough. A more direct approach would be to use the randomness from block N+2 to randomly select one of the validators from the CAS in block N+1, and require the block to contain a proof that the signature from that validator was included in the CAS (notice how as a side effect this makes reverting without notary support even more difficult).

To incentivize not signing off-head blocks, we allow off-head block headers, which contain the CAS, to be included in the main chain as uncles1

. When such a header is included, every notary listed

in the CAS is penalized an amount equal to their expected reward from signing an on-canonical-chain block. If any notary was included in the CAS unjustly, they can get their penalty back and much more by simply going through the CAS challenge process and claiming a share of the proposer's deposit.

1. Uncle = off-main-chain block header included into the main chain, term comes from the idea of an uncle as being an alternate child of one's parent's parent. Here the blocks can also be called "dunkles" (contraction of "dark uncle", and by coincidence "dunkel" is the German word for "dark"), as they are included for purposes of penalizing.