For an overview of trustless pools, click here

An extension to the described above is a protocol that enables an abstraction of the pool participants where a large set of participants pool is divided into committees for a defined time period, when that period finishes all participants are rotated to a different pool randomly.

Very similar to committee selection on the beacon-chain.

An overview will look like:

- At every epoch E_i

, from a large set of participants, divide all into fixed sized committees. Each validator pool P_z

at epoch E_i

gets a committee C_{i,j}

than can sign on the pool's behalf attestations and block proposals with a supermajority from C_{i,j}

- C_{i,j}

is dealt with secret shares that can together sign messages (for P_z

) from C_{i-1,j}

in a similar protocol to a DKG. See morehere (Wong&Wing)

Security model: supermajority of honest participants

Benefits:

- Instead of each pool's consensus is siloed, it's the network's responsibility to sign and manage all the pools validators. Basically spreading the risk across many pools.
- consensus is not siloed to pools, but rather is shared across the network
- Risk of slashing bad actors is distributed
- Reduced risk of a pool becoming stuck (no lively)
- Easier onboarding for new participants as they only increase the size of the participants pool, unlike static pools where each new pool decreases the amount of "free" participants, increasing the probability of having the 1/3 byzantine joining a single pool

Risks:

- Every E_i

there is a C_{i,j}

that can sign messages on the behalf of P_z

. That is fixed in time and doesn't change with future rotations. That might increase collusion risk (TBD)

TBD:

- withdrawal protocol. different participants join in different time, each pool has different balances.