given that sharding will very likely use KZG commitments and those require a trusted setup, with the Merge now on the horizon, let's start talking about the setup.

my initial thoughts:

- can we start collecting participants now to have a wide enough scale by the time the MPC ceremony is due?
- can the setup incorporate the results from any previous trusted setups (like Zcash's Powers of Tau, Aztec's Ignition, Tornado Cash's setup) to lower the chances of a reconstructed private key?
- what is the greatest possible damage that someone with a reconstructed private key can do to a sharded Ethereum? can we parametrize the extent of this damage?
- if every participant computes the MPC with the same client, the MPC has a single point of failure (which is, ironically, what an MPC is supposed to guard against). not least in the spirit of a multi-client Ethereum, I think this setup is critical enough to warrant multiple implementations on multiple CPU architectures.