I just came across this paper when discussing multi-signature schemes that do not involve smart contracts and instead would work on protocol-level today. I'm wondering if anyone is doing research and development in that direction as it would save us a lot of multisig pains. It seems that the it is possible to run such a setup on consumer hardware today.

Some motivations:

1. Much more gas efficient multi-signature transactions
2. Much more efficient multisig setup: Today, deploying 1000 multi-sigs would be super expensive. Taking 1000 keys to obtain 1000 threshold addresses would not require any on-chain activity at all.