# Intro

We have a desperate need to scale ethereum. The state of smart contract scaling is not as advanced as we would like it to be. As such a lot of projects are leaning towards deploying upon Proof of authority (POA) networks.

These (POA) networks do NOT provide censorship resistance, finality or security of the funds they hold. A super majority of the validators (Authority) can steal these funds, censor transactions or revert finality. However some projects are desperate to scale so these concessions in the short term make sense.

Virtual machine optimistic rollups is an optimistic rollup that contains a fraud proof for every EVM operation. They allow anyone to deploy any ethereum smart contract. So that any observer can proof a fraud and revert. These systems improve upon POA by providing much stronger guarantees.

Here we propose deploying a POA network as a short term solution which will transition to optimistic rollup in stages. We hope to find an Authority (multiple projects) that has high reputation for the short term and then once optimistic rollups are ready replace the authority with them.

# Phase 1: Setup

First we setup a POA chain with our high reputation projects. Each token that wants to use this chain deploys its own token bridge contract. This is registered on the POA side who treat balance made here as POA chain deposits.

# Phase 2: Optimistic rollups join

When optimistic rollups are ready to join they can update token bridges with their fraud proofs. This is opt in for the projects who now can choose when to use optimistic rollups.

Once we enter phase 2 an optimistic token bridge is not secure. A super majority of the Authority can still make data un-available and steal from the token bridges.

# Phase 3: Authorities are replaced with optimistic rollups

In this stage we replace some of the Authorities with optimistic rollups. This means that if an Authorities makes an illegal state transition its attestation can be undone.

If a super majority of Authorities migrate to optimistic rollup then we can roll back illegal state transitions.

# Phase 4: Decentralize transaction ordering

Finally we need to provide some decentralized way to order transactions. We can use something like[MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Value] or [Spam resistant block creator selection via burn auction] where the burn is donated to ethereum public goods funding using quadratic funding or similar.

# Conclusion

One big advantage here is that we will have multiple optimistic rollups proving validity. So if one of them is broken the system is still secure. Its like an M of N multisig. M need to have a critical security bug before we are in trouble.

Having optimistic rollups build on the same chain makes sense to make tooling the same and help them learn and improve each others work. It removes the need for every token to be on the same optimistic rollup in order to benefit from network effect. So instead of having one optimistic rollup winner now we can have many.

# Clarification

To be clear this is not a recommendation that anyone deploy on proof of authority (or proof of stake) side chains. They are intrinsically flawed. If you have no option but to do this you should deploy on one that has a clear path and commitment towards adding fraud proofs.

If you deploy to a proof of authority network. You run the risk of the chain prevent your users from exiting with high fees when you try and upgrade to another solution. There is intrinsic locking here that is very concerning. See [here] fro more information.