# Intro

The adoption of layer 2 scaling solutions could represent the centralization of control over assets stored within them.

[zk/optimistic]Rollup promises to offers 1000's of transactions per second on ethereum. However this comes at removing the miners as the groups involved in transaction ordering AND the group who 51% are able to censor transactions. This power is vested in a coordinator. A coordinator is basically selected as a single entity who has a monopoly on block creation for a given epoch.

The selections of coordinator is a difficult open problem. A few solutions have been proposed

1. Centralized coordinator
2. MEV/ burn auction
3. Proof of stake

Here we describe several attacks against proof of stake coordinator selection on layer 2 and recommend alternative approaches.

# Hardfork to recover from failure modes

On layer 1 POS works well. Huge amounts of capital is placed and used to ensure that data is available. If the system enters a failure mode (a DOS attack or data availability attack) then there can be a protocol level hardfork to remove the deposit from the attacker.

On layer 2 this is very different. It seems very unlikely to be able to coordinate a hardfork in order to slash a misbehaving coordinator of some layer 2 system. Removal of this tool fundamentally limits the ability of POS to be able to respond from attacks.

# DOS attack

If someone with a lot of stake wants to shut down or slow down layer2 system. They can begin staking their tokens and mint only empty blocks. The cost of for them is

1. The opportunity cost on their tokens
2. The reduction in the value of their stake that this attack has.

There are also several ways for users to profit from this attack

1. Charge a high fee in order to process transactions
2. Charge a high fee in order to allow users to withdraw
3. Lock up a bunch of the supply of certain tokens causing the markets to go crazy, for example if you locked up 50% of DAI you could profit if the price of eth fluctuated.
4. Take a short position on the token that is used for staking. Stake -> DOS -> Price Crashes -> Profit.

On layer 1 this is less of a problem because we can always do a protocol level hardfork in order to remove the stake. But on layer 2 it seems like there is no way to punish people for using this attack.

# Fake DOS attack

If a dos attack is happening. Stakers will have a opportunity to not participate in the dos attack and get more rewards. This could push the price of the token higher during a dos attack as more stakers look to increase their stake in order to get more rewards.

An attacker can use this as follows

1. Buy a bunch of token X
2. Start dos attack using some of your token X
3. The market goes up as stakers rush to increase their stake
4. Attacker sells their token X for profit
5. Attacker ends their DOS attack value of token X goes down.

6. Attacker buys token for lower price (Optional)

Repeating this attack an attacker can

1. Discourage other stakers from joining during a dos attack
2. Can start to increase their stake by repeating this attack causing the market to fluctuate.

## Slashing attack

Most of these systems have a slashing condition where stakers get slashes if they don't create a block by time X. The attacker who is also a miner. Refusing to include transactions from other coordinators. They also refuse to build upon blocks containing their transactions trying to uncle them and slash the victim.

Using a relatively small % of the mining power the attacker can significantly increase the chances of another staker getting slashed.

NOTE: There are also network level dos attacks that an attacker can use to prevent the propagation of valid blocks , prevent the staker from producing their blocks in time.

## Coordinator takeover

The ability to slash or buy most of the staking tokens in circulation can lead to coordinator take over. Where they can create almost all the blocks and use this power to impose massive withdraw fees on users wishing to leave. This reduces to almost 0 the value of their tokens.

## Conclusion

The limitations here are based upon

1. The inability to hardfork the token gives no way to recover from failure modes like we can on layer 1.
2. Its possible that attackers with a small % of active stake holders can harm the network as a whole. They can materially reduce the through put of the system by creating empty blocks.

Solutions like MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Valueand Spam resistant block creator selection via burn auction also need more analysis before we can start to recommend what to use for rollup leader election.