

Joint proposal with [@cooper-aztecLabs](#). Require knowledge of [non-governance](#) and [The Republic](#)

Summary

This proposal is a combination of non-governance

and The Republic

. It takes the idea from non-governance that there should not be an upgradable Rollup, but acknowledges that not all parts of the Rollup need to be ungovernable.

Namely, the state transition function will be immutable, but the senate

is able to change the gas-pricing

– e.g., the gas used per operation (nullifier insertion, etc.) – and sequencer selection contract through the same mechanism as The Republic

Comparisons

This proposal takes inspiration from [The Republic](#) but limits the Senate's powers by taking inspiration from Uniswap's fee switch - e.g., governance should only have well-defined, scope-limited power.

This proposal is closer to the non-governance side of the spectrum than other alternatives (this proposal has the smallest power scope of any other proposal, besides non-governance). This proposal includes a majority of the republic's dynamics, including the Senate, technical committee, and ability for portal developers to opt-out of governance's ability to update fees and sequencer selection protocols.

[

jedi_compare

3368×753 143 KB

](<https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/fafcf8a10b6a3c163ebc504377e865f24e418a7a.jpeg>)

Details

Looking back at prior Ethereum hard forks, we see that many are related to gas re-pricing of opcodes or changes to how the next block is chosen. In most cases, many of the inner workings of the Ethereum protocol are unchanged, with relatively few points of interest being the most frequent changes.

With that in mind, this proposal keeps the state transitioner constant but changes 'peripheral' values, and as such, the Senate is given a much narrower and more clearly-defined scope of power. Due to the narrower scope of possible changes, it is also possible to reduce the timeframes in which "upgrades" are pending, potentially down to 7 days instead of the 30 days proposed in The Republic.

The Senate still controls the registry, but the registry is simplified – it no longer points to multiple snapshots, but only to the gas pricing, sequencer selection and the Senate implementation itself.

This proposal supports upgrades that impact only the liveness properties of the network, such as repricing gas usage by different operations (nullifier insertions, etc) and the sequencer selection, while ensuring that the safety property is ensured.

In the diagram below (heavily inspired by the Republic), you see that the Senate can only "touch" the state transitioner through the fee and sequencer selection.

[

Model(80)

1920×918 66.7 KB

](<https://europe1.discourse-cdn.com/business20/uploads/aztec/original/1X/7a350a87498a6c30063372011bfd6a232d830133.jpeg>)

Thoughts on malicious governance

To ensure that the rollup cannot be frozen forever by the Senate massively inflating gas costs or changing the sequencer selection to an always-reverting case, the state transitioner must have an alternative route. In the case where block production has been halted for X time, the state transitioner must be able to use “default” pricing and accept blocks from any party with a valid proof (and it is up for discussion if this default should be used until a “normal” block is produced, or whether the timer would reset at every block).

While this could mitigate some of the issues from halting the rollup, it is still possible to upgrade the sequencer selection to a version with only one sequencer that is heavily censoring. In that case, token holders could elect a new Senate and go back to using a censorship-resistant sequencer selection mechanism.

Addressing non-gas or sequencer upgrades

For upgrades such as EIP1559, which altered the gas-model beyond just altering the gas costs of op-codes, migration to a new rollup where the state transitioner supports this would be required, OR the state transitioner should be made such that the gas-model is a module that can be altered and swapped (e.g., by having a separate circuit that handles this, where the verification key is fed into a block at verification time similarly to how the gas costs could be).

Addressing bugs in state transitioner

Ultimately, there's nothing that can be done here, other than a race to exit (if possible).