Settlement Hacks

⚠ OP Stack Hacks are explicitly things that you can do with the OP Stack that arenot currently intended for production use.

OP Stack Hacks are not for the faint of heart. You will not be able to receive significant developer support for OP Stack Hacks — be prepared to get your hands dirty and to work without support.

Overview

This guide teaches you how to modify the default Settlement Layer module for an OP Stack chain. The Settlement Layer includes modules that are used by third-party chains to establish aview of the state of your OP Stack chain. This view can then be used by applications on those chains to make decisions based on the state of your OP Stack chain. Third-party chains can be any other blockchain, including other OP Stack chains. One common Settlement Layer mechanism is a withdrawal system that allows users to send state from your OP Stack chain to the third-party chain. Modifications to this layer typically involve introducing new modules or tweaking the security model of existing modules.

Default

The default Settlement Layer module is currently the Attestation Proof Optimistic Settlement module. This module allows a third-party chain to become aware of the state of an OP Stack chain through an Optimistic protocol where challenges can be executed alongside a threshold of attestations from a pre-defined set of addresses over a state that differs from the proposed state. With a Cannon fault proof shipped to production, this default module can be replaced with a module that allows anyone to challenge proposals by playing the Cannon dispute game.

Security

Modifications to the Settlement Layer can strongly impact the security of common mechanisms like user withdrawals. A decreased withdrawal delay can, for instance, open the door to gas spam attacks that make challenges exceedingly expensive. It is generally not recommended to modify the Settlement Layer unless you know what you're doing.

Modding

Tweaked parameters

One simple modification to the Settlement Layer is to tweak the parameters of the default Optimistic state withdrawal mechanism. For example, the withdrawal period can be reduced if a smaller withdrawal period would be sufficient to secure your system.

Custom proofs

Settlement Layer modules use a proof system to verify the correctness of the state of your OP Stack chain as proposed on the third-party chain. In general, these proofs are either Optimistic proofs that require a withdrawal delay or Validity proofs that use a mathematical proof system to assert the validity of the proposal. The current Attestation Proof Optimistic Settlement module could be replaced with a fault proof system.

Multiple modules

There is no requirement that a system only have one Settlement Layer module. It is possible to use one or more Settlement Layer modules on one or more third-party chains. A system that aims to bridge state between two chains will likely need to use one Data Availability Layer module and one Settlement Layer module per chain.

Execution Hacks Overview