OP Stack security model

Many OP Stack chains, such as OP Mainnet, are a work in progress. Constant, iterative improvement of the security mechanisms that safeguard OP Stack users is a top priority for the entireOptimism Collective(opens in a new tab). The Optimism Collective strives to be clear and transparent about the security of OP Stack chains and the OP Stack as a whole.

Bottom line

The security model of any blockchain system is only as strong as its lowest common denominator. At the moment,it's important to understand that the security of OP Stack chains is dependent on amultisig(opens in a new tab) managed jointly by theOptimism Security Council(opens in a new tab) and the Optimism Foundation. OP Stack chainsmay also contain unknown bugs that could lead to the loss of some or all of the ETH or tokens held within the system .

OP Stack multisig

The security of OP Stack chains is currently dependent on a multisig managed jointly by theOptimism Security Council(opens in a new tab) and the Optimism Foundation. This multisig is a2-of-2 nested multisig(opens in a new tab) which is in turn governed by a10-of-13 multisig(opens in a new tab) managed by the Optimism Security Council and a5-of-7 multisig(opens in a new tab) managed by the Optimism Foundation.

This multisig can be used to upgrade core OP Stack smart contractswithout upgrade delays to allow for quick responses to potential security concerns. All upgrades to the OP Stack system must be approved by both component multisigs and either can veto an upgrade.

Fault proofs

It is important to understand thatfault proofs are not a silver bullet and thatfault proofs provide limited improvements to the security of a system if the system still has a multisig or security council that can instantly upgrade the system . OP Stack chains are following a multi-client and multi-proof approach designed to eventually remove the need for instant upgrades entirely. Users can withdraw ETH and tokens from OP Stack chains to Ethereum by submitting a withdrawal proof that shows the withdrawal was actually included inside of the OP Stack chain. Withdrawals are proven against proposals about the state of the chain that are published through theDisputeGameFactory (opens in a new tab) contract.

Proposals can be submitted to theDisputeGameFactory contract by any user and submissions do not require any special permissions. Each submitted proposal creates aFaultDisputeGame (opens in a new tab) contract that allows any other user to challenge the validity of a proposal by participating in a "fault proof" process. A more detailed explanation of the fault proof game can be found in theFault Proofs Explainer .

Although the fault proof game is permissionless, the Optimism Security Council acting as theGuardian role provides a backstop in case of a failure in the fault proof game. Each proposal must wait for a delay period during which the Guardian can prevent invalid proposals from being used to withdraw ETH or tokens through a number of safety hatches. The Guardian can also choose to shift the system to use aPermissionedDisputeGame in which only specificPROPOSER andCHALLENGER roles can submit and challenge proposals.

Bugs and unknowns

Please also keep in mind that just like any other system,the Optimism codebase may contain unknown bugs that could lead to the loss of some or all of the ETH or tokens held within the system. The OP Stack has been auditedon many occasions(opens in a new tab) , butaudits are not a stamp of approval anda completed audit does not mean that the audited codebase is free of bugs.

It's important to understand that using OP Stack chains inherently exposes you to the risk of bugs within the Optimism codebase, and that you use these chains at your own risk.

Work in progress

Sequencer decentralization

The Optimism Foundation currently operates the sole sequencer on OP Stack chains. Although users can always bypass the Sequencer by sending transactions directly to theOptimismPortal (opens in a new tab) contract, sequencer decentralization can still help mitigate the effect of short-term outages for users.

Security model FAQ

Do OP Stack chains have fault proofs?

Yes , fault proofs are available to OP Stack chains. It is important to note thatfault proofs are not a silver bullet and thatfault proofs provide limited improvements to the security of a system if the system still has a multisig or security council that can instantly upgrade the system . A system with fast upgrade keys, such as OP Mainnet, is fully dependent on the upgrade keys for security. The goal is to be the first system that deploys fault proofs that can secure the system by themselves, without fast upgrade keys.

How is Optimism planning to remove the multisig?

Check out Optimism's detailedPragmatic Path to Decentralization(opens in a new tab)post for a detailed view into how the multisig may be removed in a way that makes OP Stack chains the first with true fault proof security.

How can I help make OP Stack chains more secure?

OP Stack has one of the biggest bug bounties (ever). You can earn up to 2,000,042 by finding critical bugs in the Optimism codebase. You can also run your own verifier node to detect network faults.

Where do I report bugs?

For details about reporting vulnerabilities and available bug bounty programs, see theSecurity Policy .