OP Mainnet Security Model

OP Mainnet is a work in progress. Constant, iterative improvement of the security mechanisms that safeguard OP Mainnet 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 Mainnet 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 Mainnet 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 Mainnet and the OP Stack in generalmay also contain unknown bugs that could lead to the loss of some or all of the ETH or tokens held within the system .

OP Mainnet Multisig

The security of OP Mainnet 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 a4-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 Mainnet smart contractswithout upgrade delays to allow for quick responses to potential security concerns. All upgrades to the OP Mainnet system must be approved by both component multisigs and either can veto an upgrade.

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 Mainnet inherently exposes you to the risk of bugs within the Optimism codebase, and that you use OP Mainnet at your own risk.

Work in Progress

Fault Proofs

Fault proofs are a mechanism that allow users to prove if a transaction output published to theL2OutputOracle (opens in a new tab) contract is invalid. Fault proofs are an important part of future of OP Mainnet security and begin to reduce the need for a multisig. An alpha version of the first fault proof mechanism iscurrently in testing(opens in a new tab).

It is important to understand thatfault proofs are not a silver bullet and thatfault proofs do not meaningfully improve the security of a system if the system still has a multisig or security council that can instantly upgrade the system . OP Mainnet is following a multi-client and multi-proof approach designed to eventually remove the need for instant upgrades entirely.

Sequencer Decentralization

The Optimism Foundation currently operates the sole sequencer on OP Mainnet. 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

Does OP Mainnet have fault proofs?

No , OP Mainnet does not currently have fault proofs.Fault proofs do not meaningfully improve the security of a system if that system can be upgraded within the 7 day challenge window ("fast upgrade keys") . A system with fast upgrade keys, such as OP Mainnet, is fully dependent on the upgrade keys for security. OP Mainnet's 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 detailed Pragmatic 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 Mainnet the first chain with true fault proof security.

How can I help make OP Mainnet more secure?

OP Mainnet 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 the Security Policy .

Testing Dapps on OP Mainnet Privileged Roles