Fault proofs explainer

Fault Proofs are an important part of an Optimistic Rollup system like the OP Stack. Users withdraw ETH and tokens from OP Stack chains like OP Mainnet by submitting a withdrawal proof that shows the withdrawal was actually included in the OP Stack chain. Fault Proofs allow users to permissionlessly submit and challenge the proposals about the state of an OP Stack chain that are used to prove withdrawals.

On June 10, 2024, Fault Proofs were officially added to the OP Stack and were activated on OP Mainnet. This Fault Proofs upgrade moves the OP Stack closer to technical decentralization by:

- allowing anyone to make proposals about the state of the L2
- allowing anyone to challenge proposals made by other users
- allowing users to send messages from L2 to L1 without the need for a trusted third party
- allowing users to trigger withdrawals from L2 to L1 without the need for a trusted third party
- introducing a modular fault proof design that can easily integrate additional proving mechanisms

Although the fault proof game is permissionless, the Optimism Security Council acting as the Guardian 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 a PermissionedDisputeGame, in which only specificPROPOSER andCHALLENGER roles can submit and challenge proposals.

Permissionless proposals

"Proposals" or "State Proposals" are claims about the state of an OP Stack chain that are submitted to Ethereum through theDisputeGameFactory contract. Proposals can be used for many things but are most commonly used by end-users to prove that they created a withdrawal on an OP Stack chain. With the Fault Proofs upgrade to the OP Stack, proposals become permissionless and can be submitted by anyone.

See the permissionless fault proofs diagram below for more details:

Permissionless challenges

Because anyone can submit a proposal, it's important that invalid proposals can be challenged. InOptimistic Rollups like OP Stack Chains there is a ~1 week challenge period during which users can challenge a proposal if they believe it to be incorrect. With the Fault Proofs upgrade to the OP Stack, challenges become permissionless and can be submitted by anyone. Any user can run a node for the OP Stack chain in question and use theop-challenger tool to participate in the dispute process.

Modular design and multi-layer security

The OP Stack Fault Proof System ismodular in design and lays the groundwork for achieving a "multi-proof" system. This allows the OP Stack to support multiple proof systems alongside the initialCannon proof system. With multiple proof systems in place, the OP Stack can be more resilient to potential attacks and bugs in any one proof system.

Additionally, the followingsecurity safeguards have been built around the game, as follows:

- An off chain monitoring system has been set up to monitor all proposed roots and ensure they align with the correct state. Seeop-dispute-mon (opens in a new tab)
- for more details.
- After a root is finalized through a game, an additional delay called the "airgap window" has been added before withdrawals can occur. During this period, theGUARDIAN
- role can reject the root.
- A contract calledDelayedWETH
- has been set up to hold the bonds and only allow payouts after a delay, so that bonds can be redirected towards the correct recipient in the case that a game resolves incorrectly.

Next steps

- Ready to get started? Review theFP Components
- to learn how the different components work together to enhance decentralization in the Optimism ecosystem.
- See theFault Proof Mainnet Security
- to understand changes toOptimismPortal
- andFaultDisputeGame
- contracts.
- For more info about how the FP system works under the hoodcheck out the specs(opens in a new tab)

- .

FAQs

How many steps/transactions are required to settle a dispute (worst-case scenario)?

The maximum depth of a game is 73, but there can be any number of claims and counter-claims within a dispute game. Due to the permissionless structure where many different actors can participate in the same game, a single claim may be countered by any number of different counter-claims, effectively combining multiple disputes into a single game.

Are there any dependencies to consider when proposing a new state root (in the event of sequencer and proposer failure)?

Users can complete the full withdrawal cycle without depending on any privileged action. The Guardian role can override the system by pausing withdrawals, blacklisting games, or reverting to a permissioned system. As a result, the trust assumption is reduced to requiring only that the Guardian role does not act to intervene, inline with the stage 1 requirements.

Since the roles of proposer and challenger will be open to everyone, are guides available outlining the best practices for running them?

It's not expected that normal users runop-proposer to regularly propose output roots. Users would generally just propose a single output root if they need to withdraw and the chain operator isn't proposing outputs for them via direct calls to theDisputeGameFactory via Etherscan or using thecreate-game (opens in a new tab) subcommand ofop-challenger . Documentation forop-challenger is forthcoming.

How much ETH should a chain operator put aside to operate the Fault Proof System?

The nominal operating cost of running FPs (i.e., assuming no invalid proposals or malicious actors) will depend on the initial bond set for theFaultDisputeGame and the frequency of posting proposals. Assuming OP Mainnet parameters, where proposals will be posted hourly, that's 0.08 ETH per hour. Assuming a 7 day dispute window, you'll need roughly 14 ETH (including gas costs) to make proposals. If chains are using the similar FP deploy configs as OP Mainnet, it's recommended to stick to a 0.08 ETH initial bond.

However, the capital requirements for operating a FP chain in itself is much larger than 14 ETH. An operator that secures their chain using FPs must be willing to stake a lot of ETH to secure the chain. One may decide the capital requirements aren't worth it, and use only a Permissioned FP system. The capital requirements will be improved in the later stages of Fault Proofs to make it more feasible for smaller chains.

How large are the bonds expected to be needed to sustain and win a dispute?

The bonds are sized based on the anticipated cost to post a counter claim as well as to deter spamming invalid claims. As an example, on OP Sepolia, the game0xcf8f181497DAD07277781517A76cb131C54A1BEE (opens in a new tab) shows the escalating bond sizes. The list-claims subcommand of op-challenger can also provide a good view of the claims in the game:

./op-challenger/bin/op-challenger list-claims --l1-eth-rpc --game-address 0xcf8f181497DAD07277781517A76cb131C54A1BEE See thespecs(opens in a new tab) for more details.

Fault proofs FP system components