Fault proofs Mainnet security

Source code for Fault Proof Mainnet contracts approved by Optimism Governance can be foundhere(opens in a new tab) . This page details changes to the security model of the OP Stack with the introduction of the Fault Proof Mainnet upgrade. The most significant change introduced by the Fault Proof Mainnet upgrade is the modification of theOptimismPortal to reference theDisputeGameFactory instead of the permissionedL2OutputOracle .

- TheDisputeGameFactory
- contract generatesFaultDisputeGame
- contract instances that each act as a host to a proposal about the state of the OP Stack chain at a given block number.
- Unlike theL2OutputOracle
- , theDisputeGameFactory
- contract offers users the ability to permissionlessly play "fault dispute games" in which the correctness of the proposal is determined programmatically.

Security model

Fault Proof Mainnet is a large contract upgrade that introduces a number of novel components. Given the relative complexity of these novel components, the approach to security for FPM has been to limit the blast radius of potential bugs to very specific contracts and fallback mechanisms that can be easily audited.

Handling invalid game results

All of the security mechanisms put in place generally revolve around the possibility that aFaultDisputeGame contract may incorrectly finalize an invalid game result. There are two variations of this:

1. Resolving that an invalid proposal is valid potentially leading to stolen funds, and
2. Resolving that a valid proposal is invalid causing liveness delays or failures.

Both cases would cause honest challengers to lose bonds (unless theGuardian stepped in). Potential impact is managed through the introduction of a number of safeguards within theOptimismPortal andFaultDisputeGame contracts.

Safeguards withinOptimismPortal

TheOptimismPortal contract includes various security mechanisms that allow theGuardian andSystemOwner roles to collaborate to prevent invalid proposals from impacting withdrawals.

- TheSystemOwner
- can replace theGuardian
- address.
- TheGuardian
- can trigger the global pause mechanism found in the original system.
- TheGuardian
- can "blacklist" specificFaultDisputeGame
- contracts that resolve incorrectly.
- TheGuardian
- can change the respected type ofFaultDisputeGame
- contract in the case that an entire class ofFaultDisputeGame
- contracts is found to have critical bugs. If desired, theGuardian
- can also choose to revert to aPermissionedDisputeGame
- contract that only allows specific roles to submit and challenge proposals.

Safeguards withinFaultDisputeGame

TheFaultDisputeGame contracts store bonds within aDelayedWETH contract that is managed by theSystemOwner . Withdrawals from theDelayedWETH contract are delayed which gives theSystemOwner the ability to manually recover from situations in which bonds would be incorrectly distributed. This delay is set to 7 days on OP Mainnet to give theSystemOwner orGuardian sufficient time to respond to potential security concerns.

Safeguards withinDelayedWETH

- TheSystemOwner
- can replace theGuardian
- address.
- TheSystemOwner
- can hold funds from any specificDisputeGame
- contract.

- TheSystemOwner
- can remove funds from theDelayedWETH
- contract if the issue extends to so manyDisputeGame
- contracts that holding funds from specific contracts is not viable.
- TheGuardian
- can trigger the global pause mechanism to halt WETH withdrawals.

Cumulative security impact

As with the original system, the cumulative effect of these security capabilities is that theGuardian role provides fast response capabilities while theSystemOwner can always step in to resolve all classes of bugs that could result in a loss of funds. The most significant change in security model with the introduction of Fault Proof Mainnet is thatSystemOwner can take a more passive role as invalid proposals will generally be rejected by the Fault Proof System while theGuardian can act as a backstop only in case of a failure in the fault proof game.

Next steps

- See theFP Components
- for an overview of FP system components and how they work together to enhance decentralization in the Optimism ecosystem.
- See thespecs(opens in a new tab)
- for detailed information about the entire FP program, FP virtual machine, and dispute game.

MIPS.sol Transactions