无需许可故障证明系统在OP主网上线 速览其特性

作者：The Optimism Collective & Op Labs；翻译：0xjs@本站

2024年6月10日，经治理批准的、无需许可的故障证明（fault proof）已在 OP 主网上线，OP Stack 也随之进入Stage 1。这是超级链的一个重要里程碑，很快更多的 OP Stack 链将升级以包含此功能，首先是 Base、Metal、Mode 和 Zora。

无需许可的故障证明(fault proof)系统允许从 OP 主网提取 ETH 和 ERC-20 代币，而无需任何受信任的第三方参与。这也意味着任何想要参与协议的用户都可以挑战和删除无效的提款。虽然参与故障证明系统是无需许可的，但Optimism安全委员会保留在系统发生故障时进行干预并将系统恢复到许可状态的权力。拥有这种后备是负责任且安全地推出故障证明系统的一部分，Optimism安全委员会符合L2Beat 对第 1 阶段的完善的行业标准定义。

## 速览故障证明系统

功能齐全的故障证明系统增强了桥接的 ETH 和 ERC-20 代币的安全性，其功能为完全去中心化铺平了道路。

改进的信任模型

无需许可的故障证明系统使用户能够将 ETH 和 ERC-20 代币从 L2 提取到 L1，而无需涉及任何受信任的第三方（如排序器或任何其他中心化基础设施）。

这意味着提款不再依赖于特权提议者角色发布输出根。相反，现在任何人都可以通过故障争议系统发布输出提案。输出提案对 L2 的状态提出声明。一旦最终确定，该声明可用于促进提款，而无需采取任何特权行动。即便安理会撤销提币。

任何人都可以为安全做出贡献

任何想要参与协议的用户都可以挑战并删除无效的提案。

争议博弈提供了一种确定输出提案有效性的机制。任何人都可以通过参与其相关的争议博弈来质疑输出提案的有效性。每个行动都需要放置 ETH bond，不诚实的bond将支付给诚实的bond持有者以支付 gas 成本。

安全理事会作为安全网

正如Vitalik Buterin 在其Rollup 去中心化愿景中所概述的那样，可以存在临时训练轮，这是一种可以在紧急情况下超越故障证明系统的安全机制。这导致了无需许可的故障证明系统的推出，Optimism Collective 的安全委员会作为后备。在 75% 的签名阈值下，它可以在故障证明系统发生故障或手动升级时进行干预。

该系统减少了信任假设，为全面去中心化铺平了道路。OP Labs 团队的路线图旨在实现 OP Stack 的第二阶段去中心化，当技术被证明是安全的时，将移除辅助轮。

模块化设计，实现多重防护

故障证明系统的模块化特性使其能够集成额外的证明机制，为未来的多重证明系统奠定坚实的基础。得益于此升级中包含的智能合约框架，可以轻松添加额外的证明系统。

这些证明协同工作，将在生产过程中提供增强的安全层。随着 OP Stack 朝着实现第二阶段去中心化的方向发展，这将进一步减少后续升级中的信任假设。

然而，OP Stack 并非仅通过实施故障证明就达到第一阶段。专门针对系统的额外保护措施可确保安全委员会在出现错误时能够迅速有效地采取行动。如果启动了保护措施，提款将被重置，因此需要重新证明所有待处理的提款。安全性是 OP Stack 内置所有内容的首要考虑因素，这些努力与故障证明工作相结合，使 OP Stack 达到第一阶段的功能。

## 下一站：Stage 2

2022 年，Vitalik 概述了一个框架，说明 L2 如何逐步摆脱训练轮，走向完全去中心化。L2 项目通常会在开发的各个阶段尽早启动，并在安全模型完全无需许可之前启动生态系统。随着项目的进展，他们可以摆脱训练轮，从第 0 阶段推进到第 1 阶段，最终进入第 2 阶段去中心化。

现在OP对第一阶段的安全模型充满信心，核心开发团队和生态系统中一些最受尊敬和最勤奋的安全审计员已经彻底审查了安全理事会在任何情况下保持系统安全的能力，下一步就是努力实现第二阶段。接下来是：对争议博弈（Dispute Game）本身的审计，将于 7 月进行。

但展望未来，必须超越第一阶段。

L2s 处于不同的开发阶段，这些项目通常会同时构建生态系统和加强代码。随着项目的成熟，其代码也会不断完善，去中心化进程也会不断推进。早期的安全措施或“辅助工具”已不再必要。

在 OP 主网上启动故障证明、将功能扩展到超级链生态系统中的其他 OP Stack 链以及实现第一阶段的去中心化是重要的里程碑。但终局是第二阶段的去中心化。



目前的故障证明系统为实现“多重证明涅槃”奠定了基础——就像 OP Stack 本身一样，它在设计上是开源和模块化的。该框架旨在使 OP Stack 能够支持多种证明系统，包括零知识证明以及当前的系统 Cannon。将冗余证明方案投入生产，以确保从 OP Stack Chains 提款回以太坊，可以将安全委员会的作用限制为仅在意见不一致的情况下在证明之间进行选择。

故障证明系统由来自 Superchain 的核心开发团队（如 OP Labs、Base 和 Sunnyside Labs）构建和测试。这种协作方式使此次发布成为可能。故障证明提案也得到了Optimism 的 Token House 和 Citizens' House 的批准，通过了 Optimism 治理的两步审批流程。

在接下来的几个月里，我们寻求在测试网上推出其他证明系统，包括 Asterisc 和 Kona。证明这些冗余证明方案的可靠性和稳健性将有助于超级链实现第二阶段的去中心化。

我们正在庆祝故障证明的推出，以及 OP Stack 进入第一阶段，并对超级链实现完全去中心化的未来的道路感到乐观。