Optimism“故障证明”系统正式在主网上线

作者：Margaux Nijkerk，CoinDesk；编译：陶朱，本站

Optimism 是领先的Layer 2区块链，旨在帮助以太坊用户快速交易并降低费用。其技术是区块链领域一些大牌企业的基础，包括 Coinbase 交易所广受欢迎的 Base 区块链和 Worldcoin 的 World Chain（由 OpenAI 创始人 Sam Altman 打造）。

但多年来，Optimism 一直存在一个问题。所有使用 Optimism 技术的区块链都是根据一个核心基本前提构建的：它们“借用”了以太坊的安全设备。但事实上并非如此。

到目前为止，Optimism 的安全设计中一直缺少一个核心功能：“故障证明”。周一，这项长期承诺的技术终于登陆 Optimism 的主网。

故障证明旨在确保基于 Optimism 的 Layer-2 链的诚实性。它们有助于防止 Layer-2 链的运营商将不准确的交易数据传递到以太坊的 Layer-1 交易账本，并为 Layer-2 链的“去中心化”提现机制提供支持。

所有Layer 2 Rollup 网络都使用类似的“证明”技术，包括 Optimism 的竞争对手 Arbitrum。它旨在确保Rollup 的用户（无论是 NFT 交易者、散户投资者还是知名金融机构）可以信任以太坊庞大的运营商网络，而不是Rollup 自己的内部系统，以准确记录他们的交易和提款。

随着 Arbitrum 等Layer 2链推出其系统的证明，Optimism 落后了。多年来，这使得 Optimism 成为同行批评的对象，他们声称自己的技术更安全、更先进。

现在，故障证明终于出现在 Optimism 的主网上，该网络的开发人员——以及使用其技术的其他团队不断壮大的生态系统——希望将过去抛在身后。

## “故障证明”如何发挥作用？

在过去两年中，像 Optimism 这样的Layer 2 Rollup 网络已成为在以价格昂贵著称的以太坊区块链上运行的首选方法。

当用户向 Rollup 网络提交交易时，它会与其他用户的交易捆绑在一起，然后再传递到以太坊。这些捆绑包会一次性写入以太坊的交易账本，这种设置可以让用户更快地进行交易，而且费用只是其中的一小部分。

理论上，Rollup 交易由“证明”保护，这是一种加密方法，允许以太坊上的观察者检查交易细节是否被准确记录。这在提款方面最为重要，它允许用户信任以太坊（而不是汇总网络）将他们的资金从Layer 2链中提取出来。

如果没有错误证明，将资金存入 Optimism 的用户需要信任 rollup 的“安全委员会”来归还资金——这个系统将 rollup 暴露在潜在的人为错误或偏见之下。有了错误证明，这些用户只需要信任以太坊即可。

Optimism 的名字源于其“Optimism”证明系统，它在 2021 年首次发布时推出了该技术的一个版本，但在发现问题后迅速废弃了它。

OP Labs 首席执行官 Karl Floersch 在接受采访时表示：“我们实际上删除了整个系统，重新设计了它，并重写了整个系统。”“这很残酷，但绝对是正确的决定。”

Optimism 团队此前在 3 月份分享说，他们正在他们的 Sepolia 测试网上测试其错误证明系统。从那时起，他们接受了区块链安全公司 Sherlock 的审计，发现了一些他们能够修补的错误。

“所以我们修复了所有发现的问题，我们对实际实施的黄金时段充满信心，”Floersch 说。

从本周开始，网络将再次依靠防错系统来为提款提供动力，但它仍将保留“training wheels”，以确保一切顺利运行。安全委员会将保持完整，并在防错系统发生故障时进行干预。这两个实体的结合就是 Optimism 所称的“第一阶段去中心化”。

目标是最终实现第二阶段去中心化，届时网络将完全不必依赖安全委员会。

“第二阶段是一个多重防错系统，足以使系统以某种方式运行，比如自动驾驶。安全委员会没有能力在最后一刻进行干预，”Floersch 说。

Floersch 补充说，该团队正在努力实现第二阶段的目标，但他没有给出实现这一最终愿景的时间表。

随着故障证明最终运往 Optimism 的主网，其他使用 Optimism OP Stack 的区块链也将获得该技术。（据 DefiLlama 称，目前使用 Optimism OP Stack 的两个区块链 Blast 和 Base 在总锁定价值方面超过了 Optimism 的主网。）

“我们将从 OP 主网开始进行这次升级，这是一个相当大的升级，”Floersch 指出。“然而，Coinbase 的 Base 链实施故障证明系统的时间应该不会太长”，Floersch 补充道。