如何看待Optimism欺诈证明因安全问题被调整为受许可？

作者：HAOTIAN

最近，@Optimism由于Fault Proof System出现安全审计问题遭到了海外社区的质疑。原本无许可的欺诈证明的机制，在被发现重大安全问题后，OP Foundation竟然提出要硬分叉修复问题，并将其转为受许可证明？具体怎么回事呢？

1）简单而言：Fault Proof System是一种用于验证Layer2网络状态正确性的机制，任何人可以无许可向L1上的纠纷虚拟机提交L2状态，并接受他人的挑战，如果挑战成功则会触发奖惩机制。

这就是OP-Rollup机制确保安全性而必须存在的欺诈证明机制。6月份Fault Proof System的上线算是弥补了一直以来市场对OP Stack缺乏有效挑战机制的诟病问题。

2）不过，最近一次社区驱动的审计发现了该欺诈证明系统的多个漏洞，Optimism基金会的反应却让人大跌眼镜：

1、将欺诈证明VM opcode级别的漏洞视为小安全漏洞；

2、把欺诈证明系统排除在了外部审计范围之内；

3、暂时将欺诈证明的无许可调整为许可机制，并提出一项名为Granite的硬分叉计划来解决安全问题；

如此这般，让人不得不怀疑所谓Fault Proof System存在意义和有效性，

3）如何看待这件事呢？在我看来：

1、Optimism推出Fault Proof System完全是为了进一步扩大OP Stack阵营所进行的必要的安全挑战机制，市场对Optimism本身是否存在这样的挑战机制已经“乐观化”了；

2、Fault Proof System确实构造精密复杂，大部分状态可在L2本地进行校验，只把一些关键部分推送给L1的故障虚拟机来裁夺，没错是开发了特定op code的虚拟机，这样做既可以确保L1验证的低成本同时又能确保安全性；

3、Fault Proof System从无许可调成许可，并被紧急禁用也暴露了OP基金会和多签安全委员会的过多权利，欺诈证明即使无许可也在安全委员会的控制之下；

4、Optimism实现Stage1的安全和去中心化目标至少相比同阵营的Arbitrum掉队了，ZK-Rollup在技术上的领先优势会进一步得到重视。