ZKVM 与 ZK验证的思考

作者：Miles 来源：X，@Miles082510

昨天与国内的ZK芯片厂商讨论了ZK加速的问题。当前，基于ZK的L2只需要几百台GPU机器即可维持日常业务，未来的Asic发展将更加令人期待。那么，现在的加速需求在哪里？哪些部分值得加速？ZK赛道的瓶颈到底是在证明生成还是验证？这些问题会对生态产生什么影响？

基于这条推文，我想分享一些自己的理解，欢迎指正与讨论！

### 过去的ZK技术

早期的ZK解决方案主要基于电路开发。开发者必须使用特定语言构建电路，这种方法既复杂又昂贵。@StarkWareLtd 在这个领域处于领先地位，他们通过STARKs在Cairo中构建了电路，利用STARKs的递归证明优势。然而，这种方法的局限性在于它只能汇总来自单一证明系统或机器的STARK证明。

### 当前的ZK技术

现在，随着通用ZKVM的出现，程序员无需学习新的电路语言，只需编写Rust代码即可开发应用。这方面的代表包括 @RiscZero、@SuccinctLabs 的 SP1、@NexusLabsHQ，以及 @lita\_xyz 和来自 @a16zcrypto 的 jolt。

尽管有很多ZKVM项目，但我认为未来所有的证明聚合系统都将依赖RISC-V ZKVMs或基于Rust的ZKVMs。通过使用RISC-V证明，我们可以轻松合并不同的证明系统，简化复杂的验证过程。

### 问题与挑战

在以太坊上验证证明的成本非常高，且不支持大容量。例如，一个1GB的证明直接在以太坊上验证是不现实的，尽管可以通过递归证明进行压缩，但这同样昂贵且耗时。如果你运行一个ZK rollup，每年的成本可能高达数百万美元。

此外，虽然 @alignedlayer 每秒可验证2500个哈希值，但以太坊无法处理如此大的容量。

### 解决方案

在以太坊上有两种方法可以实现快速且低成本的验证：

证明聚合：提高验证效率的一种方式。

ZK验证层：在 @eigenlayer 上实现低成本、可扩展的ZK验证层，这是 @alignedlayer 的当前做法。

### 讨论与观点

关于ZK赛道的瓶颈，@Ozhar（来自 @zkSync）认为只有5%的成本与验证相关，95%则与生成证明的硬件成本相关。@heslinkim（来自 @gevulot\_network）持不同观点，他认为真正的瓶颈在于证明生成和硬件。

事实上，ZK硬件和证明生成领域也在快速发展中，如 @cysic\_xyz、@Ingo\_zk 和 @lagrangedev 等项目方正在积极推进相关技术。