对比两大跨链互操作方案 AggLayer与Superchain的安全性分析

作者：Brian Seong 来源：X，@BrianSeong99 翻译：善欧巴，本站

以终极声明开篇："无缝的跨链流动性访问是必需的！"

## 1. 轻松部署新的L2

借助@0xPolygon的CDK、@Optimism的OPStack、@arbitrum的Orbit以及其他众多RaaS服务，现在部署L2变得更加容易。然而，链间的流动性变得更加碎片化。这些只是前10名，还有无数更多。



### 2. 跨链用户体验仍然是一个主要问题



由于用户体验问题，跨链交互变得令人头痛。以下是用户的旅程：

通过Layer 1：

从源链提取流动性到L1。等待。（如果是Optimistic Rollup，则有挑战期，大多数链上通常设置为7天）。

从L1添加流动性到目标链。等待。

在目标链上开始交易。

通过桥接：

从源链提取流动性到桥接合约。等待并支付溢价，同时承受信任第三方桥接的风险。

桥接中继器调用目标链上的铸币操作。等待。

在目标链上开始交易，这可能是一个包装的代币。

### 3. AggLayer和Superchain简介



AggLayer解决了流动性碎片化的问题，这导致了资本效率低下并削弱了网络效应。它作为一个统一层，能够在区块链之间实现低延迟的无信任交易，增强了互操作性。

简单来说，可以把它看作是L1和L2之间的去中心化协议。它不能生成新的区块，但它可以聚合连接链的区块。这使得连接到AggLayer的链能够通过在AggLayer上的结算安全地建立异步跨链数据交换。



Superchain，由@Optimism创建的Superchain，是一个基于OPStack的L2链网络，它们共享安全性、治理和标准化的技术堆栈（#OPStack）。通过将链视为可互换的计算资源，它提供了区块链的可扩展性。

简单来说，Superchain为所有#OPStack链提供了跨链数据交换标准，能够通过不同安全性和速度配置的各种消息传递协议，以及通过共享排序器进行的跨链交易排序。

目标：实现链之间的有效通信

### 3.1 支持的L2链堆栈（链的可定制性）

AggLayer将支持：
只要链能够提供适当的输入给悲观证明，它就能连接到AggLayer！

### 3.2 L2安全性

AggLayer由零知识证明（ZK）保障。这允许所有能够生成兼容区块证明的链整合到AggLayer生态系统中。例如，Polygon PoS侧链和Optimistic Rollups链可以生成悲观证明以在统一流动性中建立共享资产状态，zkEVM等链可以生成有效性证明加入AggLayer。AggLayer跟踪所有链上的资产状态。本地链状态用于构建悲观证明，然后在L1上验证。如果某条链尝试提取超出其存入的代币数量，该证明将无法验证。

Superchain严格为OP Stack链构建。所有链都连接到共享的桥接和共享的排序器，因此，所有OP Stack链将通过Optimistic Rollup的挑战期在L1上达到最终确定性。OP Stack链的典型设置是7天的欺诈证明期，而@Blast\_L2（也是OP Stack链）设置为14天。

### 3.3 跨链互操作性

AggLayer的互操作性通过统一桥接和悲观证明实现。

统一桥接：允许所有连接到AggLayer的链访问共享的本地资产池，无需费用抽取中介或额外的信任假设。

悲观证明：所有连接到AggLayer的链的悲观证明将允许用户无需通过L1的中间步骤就能将资产从链A移动到链B。

证明聚合：AggLayer将在源链和目标链的消息队列中检查跨链交易。如果跨链交易在两条链上都有匹配的交易，则接受这些交易；否则，交易将被回滚以确保原子性（这是统一桥接流程的一部分）。有关AggLayer的更多信息，请查看@\_bfarmer的博客。

当AggLayer与共享排序器（如@EspressoSys）一起使用时，它可以有效实现通用的同步组合性。

Superchain的互操作性通过两种类型的跨链交互实现。

共享排序器方法（原子/同步交易）：通过在两个不同链上的两个交易创建引用，并让共享排序器接受两个交易或不接受任何一个交易来实现。共享排序器将承担原子跨链交易接受的风险。

桥接系统（非原子交易，依赖于桥）：这是典型的跨链桥系统。有关不同桥接标准的更多信息，请参阅此推文的图片。

### 3.4 生态系统

AggLayer：

目前连接的链：@XLayerOfficial, @AstarNetwork, @0xPolygon zkEVM, @swellnetworkio等。

@0xPolygon PoS正在连接AggLayer，与@SuccinctLabs合作中。

许多其他非EVM区块链将连接到AggLayer，统一流动性和跨链交互的用户体验，例如@union\_build正在构建连接IBC链到AggLayer的网关。

Superchain：

目前的链：著名的onchainsummer@base, @Optimism, @modenetwork, @ourZORA等。

还有许多其他链也加入了OPStack生态系统。

### 3.5 主权与成本

由于AggLayer不要求与连接的L2共享收入，因此在AggLayer上托管L2的日常成本主要是服务器费用，确保其24/7在线。
所有链都将拥有决定其链主权设置的权利，只要它能提供生成悲观证明所需的输入，就是一个好链！

对于Superchain，除了托管成本外，所有链都必须遵守链法，其中15%的Superchain排序器收入用于资助RFP。

## 4. L2 跨链互操作性的未来

Vitalik 提到：



## 以下是我的一些个人看法：

1.ZK：以太坊 L2 的未来

零知识（ZK）技术正在成为以太坊第 2 层生态系统中去中心化、安全扩展解决方案的终极解决方案。为了在未来的区块链运营中实现真正用户友好的体验，主要的 Optimistic Rollup 可能需要转向采用 ZK 原则。

2. Layer 2 解决方案的聚合

各种 Layer 2 平台的聚合和集成代表着一种不断发展的趋势，反映了当今不同区块链之间日益增强的互操作性——这种发展类似于各国在世界贸易组织 (WTO) 等国际贸易协定下走到一起。通过消除壁垒并增强不同链之间的兼容性，这一趋势为更广泛地采用区块链技术铺平了道路。

3. Rollup 即服务工具和 AppChains 的兴起 Rollup

即服务工具简化了新层创建流程，而 AggLayer 和 Superchain 等基础设施促进了流动性引导工作，因此，从仅仅部署额外的 EVM 兼容层到建立更复杂、专门为各种应用场景量身定制的链，这是一个显著的转变。这种方法旨在为用户在 L2 环境中提供多样化的体验——为所有可以想象的区块链用例提供全面支持。

未来可能各个机构/公司/项目/联盟都有自己的L2，彼此之间可以自由无缝沟通，每个L2只需要专注于自己的产品构建，无需担心引导链级资源。