IOSG | Unichain 的必要性何在？初探 Unichain

撰文：IOSG Ventures

## 前言

多年来，Uniswap 一直在不断推动功能和创新的改革，使交换对用户更加友好和公平。例如，我们看到 Uniswap Mobile 移动版、UniswapX 中的 Fillers Network、用于统一跨链意图标准的 ERC-7682，以及即将在 Uniswap V4 中开放用于定制 AMM 池的钩子等等。

10 月 10 日，Uniswap 宣布了他们的总体乐观 Rollup、 Unichain。该链旨在成为超级链生态系统中的一站式流动性中心，为交易者提供近乎即时的交换体验和更低的价差，同时在此过程中最大限度地保护 MEV 参与者的隐私和完整性，并在此过程中使用 TEE。

虽然这些愿景令人印象深刻，但用户质疑是否需要另一个 L2，包括 Vitalik 在内的一些人评论 Unichain =「每个 Rollup 上的 Uniswap 副本都是如此」。换句话说，他认为在新链上启动 Uniswap 克隆实际上与启动 Unichain 本身具有相同的目的。

那么，Unichain 到底是利好还是利空呢？今天的文章就来探讨一下 Unichain 的架构，了解 Unichain 的「必要性」。



## 1.什么是 Unichain？

Unichain 是一个 optimistic rollup，旨在执行近乎即时的交易，同时使用隐私技术 TEE 来最大限度地减少对链上 LP 和交换者的潜在影响。

由于 Unichain 采用与其他乐观汇总链相同的属性和标准构建，因此它现在可以利用超级链生态系统中的互操作性并访问整个网络的共享流动性。

为此，Unichain 带来了 4 项重大创新：

Rollup-Boost 和 Sequencer Builder 分离

TEE 中的区块构建

Flashblock

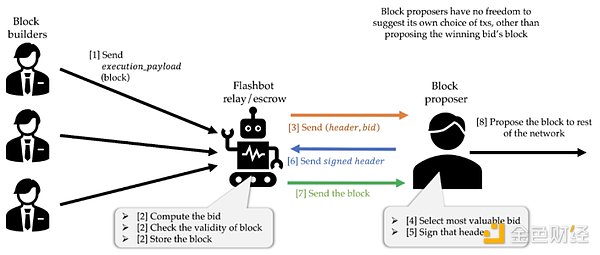
Unichain 验证网络 (UVN)

### 1.1 Rollup Boost：Sequencer Proposer 分离 (SBS)

区块构建 (Block Building) 是解决 MEV 问题的关键。

在 MEV Boost 之前，以太坊受到审查风险和糟糕的用户体验的困扰。由于搜索者之间为利润驱动的订单纳入而展开的激烈竞争，用户面临高额交易费用和抢先交易问题。为了解决这些问题，flashbot 构建了 MEV-boost。

MEV Boost 通过引入中继器来汇总区块构建者和提议者的角色，并将最有利可图的区块提交给提议者进行签名，从而将区块构建者和提议者的角色区分开来。这种设计有效地分散了 MEV 提取过程，并使验证者和专业构建者之间的 MEV 利润民主化。



Rollup Boost 的概念与 MEV Boost 类似，其中启用了 SBS（Sequencer Builder Separation）的 L2 可以通过名为「Block Builder Sidecar」的系统将区块构建过程与序列器的执行引擎分离。

简而言之，系统内部有 4 个主要组件：

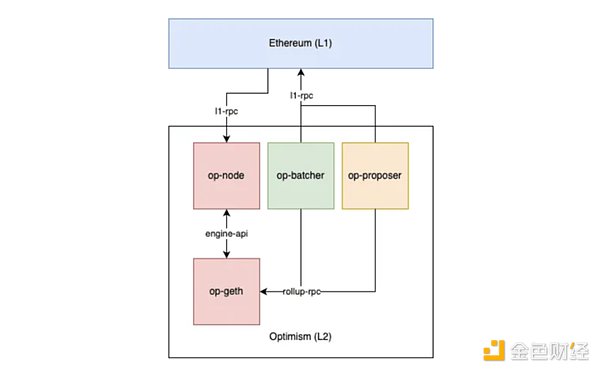
OP-node

OP-geth

Sidecar / Blockbuilder Sidecar

外部区块构建器

下面是 optimism 架构图，我们可以看到序列器节点（又名 op-chain）由 Op-geth 和 Op-node 组成。



为了在排序器中区分区块构建和提议的角色，添加了一个名为 Sidecar 的组件。Sidecar 使 OP 节点能够从外部构建者接收区块，从而在区块构建者和提议者之间创建一个市场。

工作流程如下：

1. OP 节点向 sidecar 发送更新。

2. sidecar 作为中间人将更新转发给 op-geth

3. 当 OP 节点从 OP-geth 请求区块时，sidecar 会拦截请求。

4. 然后，sidecar 将请求转发给外部区块构建者，这是外部构建者可以竞标和竞争的「间隙」。

5. 收到外部 / 获胜者区块后，sidecar 将其发送给 OP 节点。

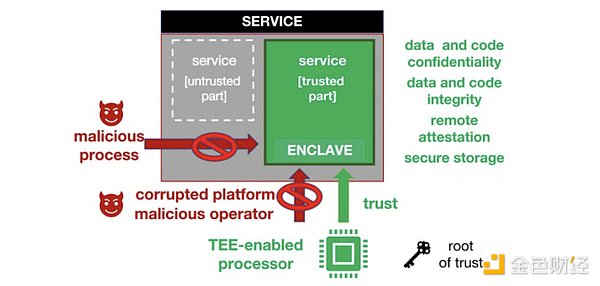
6. 如果没有收到区块，sidecar 将转发本地生成的区块。

区块构建器 sidecar 的主要好处是升级不需要修改 OP 链客户端，同时允许对交易排序规则进行更灵活、更简化和更抗审查。然而，由于添加了中介（sidecar），可能会出现一些延迟。

### 1.2 Rollup Boost：Sequencer Proposer 分离 (SBS)

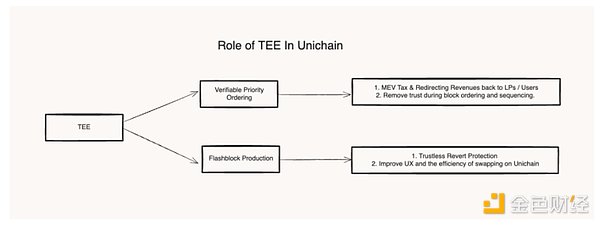
Rollup Boost 通过将可信执行环境 (TEE) 引入区块构建过程来确保交易的完整性，从而使这一过程更进一步。得益于英特尔 TDX 等最新硬件进步，实时性能成为可能。

对于那些不熟悉 TEE 的人来说，它们是处理器或硬件内的安全区域，通过阻止未经授权的实体读取内部数据来提供增强的隐私。同时，TEE 保持高水平的完整性，因为 TEE 内的代码无法修改或替换。



在 Rollup Boost 的背景下，Unichain 将使用 TEE 构建器来降低 MEV 泄漏的风险。这意味着，当将捆绑包或交易发送到 TEE 区块构建器时，TEE 的完整性方面可保证交易到达构建器的顺序不会受到试图提取更多 MEV 的外部方的影响。

此外，TEE 提供无需信任的还原保护，这可以保护用户免受失败交易的影响，因为 TEE 可以运行模拟，并且在处理任何还原交易之前都会被检测和消除。这不仅提高了 AMM 的效率（因为不会有失败的交易通过），而且还改善了整体用户体验，尤其是在交易量大的时候。



为了提高排序和区块构建过程的透明度，区块生成后将向用户公开执行证明。此证明对于验证优先级排序至关重要，这一概念将在后面的段落中解释。

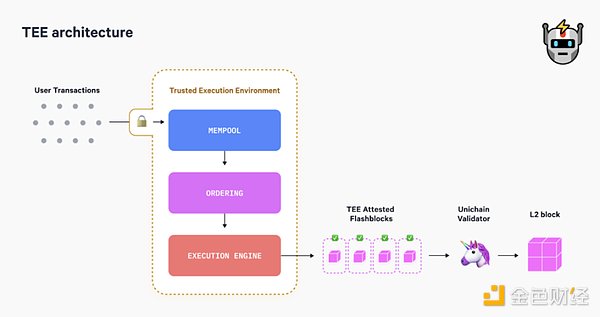
### 1.3Flashblock 和可验证区块构建

以太坊的平均区块时间为 12 秒，非常慢，无法满足当今对可接受交易体验的需求。此外，缓慢的区块时间使网络面临更多 MEV 机会，并使其在垃圾交易攻击下容易受到网络拥塞的影响。

L2 旨在通过捆绑链下交易并提交证明来验证计算正确性，从而提高以太坊的可扩展性。为了提供更流畅的交易体验，Unichain 的目标是实现 250ms 的区块时间。然而，为了实现这一点，Unichain 需要一个能够以低延迟持续传输区块以及近乎即时确认时间的系统。Solana 可以并行处理 440M，但为了实现这样的速度，牺牲了一定程度的去中心化。

以前，在大多数 L2 区块提议过程中，数据的序列化和状态根生成会产生延迟，导致快速区块时间不可行。

为了解决这个问题，flashbot 创建了 flashblock，其理念是将块「分解」成更小的分片，从而缩短块之间的时间，以最大化 UX / LP 优势。



Flashblock 是由 TEE 区块构建器发出的预确认，用于部分但快速的确认。

首先，交易被流式传输到 TEE 区块构建器中。如果 L2 已启用 SBS，则区块构建器将与排序器分离。在排序和捆绑之后，交易将逐步形成称为 Flashblock 的部分确认。Flashblock 将从排序器每 250 毫秒广播到其他节点进行验证。

由于延迟是由 L2 中的状态根生成和序列化引起的，因此 Unichain 通过仅对多个部分块计算一次状态根和共识来摊销区块构建过程的成本，从而大大降低了延迟。

简而言之，Flashblock 之所以强大，是因为：

较短的出块时间降低了 LP 的逆向选择成本风险。

Flashblock 提供现有状态的早期执行状态，使钱包和前端集成更加容易。

快速交易提供出色的用户体验 (UX)。

此外，由于 TEE 可以在每个 Flashblock 中强制执行优先级排序，因此应用程序和智能合约现在可以征收 MEV 税，劫持优先级排序以谋取自身利益，并将 MEV 重新分配给 LP 和用户。

正如 Dan Robinson 在他的推文中强调的那样，允许应用程序和用户「控制」他们的 MEV 是 Unichain 的主要功能 / 目的之一。

更好的是，优先级排序可以通过 TEE 中的公开执行证明进行验证。这让用户可以准确验证他们的交易是如何执行的。这非常重要，因为这是用户确保优先级排序公平进行的唯一方法。

### 1.4Unichain 验证网络 (UVN)

如今，大多数 L2 排序器都是中心化的，单个排序器的行为会影响 MEV 的公平性、区块的活跃度或最终性等。例如，如果排序器发布无效区块，并且提交了欺诈证明来挑战它，则由此产生的链逆转实际上会影响链的速度。

为了应对排序器中潜在的单点故障，Unichain 引入了 Unichain 验证网络 (UVN)。

UVN 通过在提出区块时专注于通过证明规范链 ( 以太坊 ) 的验证者来验证区块，增加了额外的最终性层。这个过程实际上类似于并行化，其中区块构建的不同阶段可以在一个时期内同时发生。

但是，没有文档中的进一步细节，现在就对利弊做出假设还为时过早。

### 1.5$UNI 代币

$Uni 代币现在不仅仅是一个治理代币，它还是一个实用代币。

要成为验证者，运营商必须首先在主网上质押 $Uni 作为抵押品。智能合约将跟踪余额并通过 Unichain 的原生桥更新状态。

在每个时期开始时，当前质押余额都会被快照，费用将按质押权重按比例分配。具有最高 $UNI 质押权重的验证者将被选为活跃集，他们可以发布证明以获得验证奖励的一部分。错过或未发布证明的验证者将不会获得奖励，并且奖励将延续到下一个时期。

根据有限的公开信息，我们可以推断验证奖励将是：

(Unichain 用户支付的 L2 费用 - 应用程序征收的 MEV 税 - 将捆绑包提交到第 1 层的成本）

## 2.Unichain vs Appchain vs General Rollup



Unichain/ 通用 Rollup 和应用链之间的主要区别因素是 MEV、预确认和区块空间竞争。

由于应用链可以灵活地定制其架构，因此它们可以实施不同的 MEV 机制来缓解诸如消除审查风险或减少 MEV 泄漏等问题。

同时，由于 TEE 提供的完整性属性，Unichain 通过确保交易顺序不受任何第三方的影响来缓解和重组 MEV。可验证的优先级排序还确保 MEV 公平，并有可能将 MEV 收入重新分配给用户和流动性提供者。

市场上的大多数排序器都是中心化的，允许它们从订单流中获取最大价值。相比之下，Unichain 采取了更「公共利益」的方法，因为其 MEV 重新分配机制在一定程度上限制了原始排序器可以捕获的 MEV 数量。

Unichain 是基于 OpStack 构建的，OpStack 是乐观链的统一标准，它使 Unichain 能够通过安全消息传递在超级链上读取消息和转移资产，从而通过其原生的乐观互操作性设计实现低延迟（约 2 秒）。另一方面，应用链可以利用不同的互操作性解决方案，例如加入 IBC 生态系统或在 Arbitrum Orbit 上构建 L3（尽管这对于 OpStack 的 L2 来说并不常见）。

## 3.结论

Unichain 是一个有趣的概念，它不仅为用户提供了预先确认的流畅交易体验，而且由于 flashblcoks 启用的更短区块时间，最大限度地减少了 MEV 的利用窗口。这种创新还降低了 LP 的逆向选择风险，并使用户 /LP 受益于更低的滑点等。

另一方面，可信执行环境 (TEE) 的完整性和隐私属性确保链上的用户可以享受公平、可验证或应用程序管理的 MEV 重新分配的保证交易，这要归功于 Unichain 上的优先级排序。

Unichain 的验证过程还可以保护序列器免受单点故障的影响，验证器在快速最终验证区块方面发挥着重要作用，同时将 $Uni 代币转变为具有收益的生产性资产。

然而，通过启用 MEV 重新分配，sequencer 实际上失去了捕获最大数量 MEV 的潜力，但更多的收益正在返回链上的 LP / 用户。

虽然有些人可能会认为 Unichain 可能没有足够的吸引力让资产迁移到新链，但我相信随着 L2 生态系统的不断发展，操作链之间的互操作性将使 Unichain 能够利用更大的流动性池，例如来自 Base 的流动性池。

此外，除了 Grant（Unichain 在 Uniswap DAO 之后也可以以 USDC 形式提供）之外，新的 DeFiApp 有足够的动力在 Unichain 上进行构建，因为他们可以从定制 MEV 重新分配策略中受益。同时，生态系统内的资产可以从 TEE 中受益，以减轻 MEV 泄漏。

因此，凭借其速度、MEV 重新分配的公平性以及该链可能提供的互操作性，Unichain 有可能成为 DeFi 的下一个中心。