Unichain：UniSwap 与 Flashbots 能否解决 MEV 问题？

昨天，Uniswap宣布与 Flashbots 合作推出专为 DeFi 设计的以太坊 L2——Unichain，这是一个基于 OP Stack 的 Optimistic Rollup，旨在解决 DeFi 面临的一些挑战。值得一提的是，Uniswap、Flashbots 和 Optimism 都得到了 Paradigm 的投资支持。

当前以太坊 L1 的区块时间为 12 秒，交易速度慢限制了用户体验。此外，MEV 问题也亟待解决，现有的区块构建机制导致某些参与者通过操纵交易顺序获取不公平的收益，进而降低市场效率。针对这些问题，Unichain 推出 1 秒区块时间和 250 毫秒的「Flashblocks」，结合可验证的优先排序机制和可信执行环境（TEE），大幅提升了交易速度，同时增加了交易排序的透明度和公平性，为 Layer 2 的 DeFi 生态注入新的活力。

## Unichain 的技术特点

### 1. Verifiable Block Building（可验证区块构建）

这是 Unichain 引入的一种新的区块构建机制，由 Rollup-Boost 实现。旨在提高区块链的交易排序透明度，减少不公平的 MEV 提取，并提高交易处理速度。其基本思想是使用 TEE 来执行区块构建过程，提供透明且可信的排序机制。Rollup-Boost是 Flashbots 开发的一个用于升级 Rollup 性能的可验证区块构建平台，通过 TEE 来优化区块构建过程。Unichain 是其首个实际应用案例。Rollup-Boost 作为侧车软件（sidecar）集成在 Unichain 上，利用其技术特性（如 Flashblocks 的快速确认和可验证的优先排序）来增强 Unichain 的性能和用户体验。

可验证区块构建的工作原理：

使用 TEE 进行区块构建：TEE 是一种硬件安全技术，能够在隔离的环境中执行计算任务，确保外部环境无法篡改或干扰。在 Unichain 中，区块构建者在 TEE 中运行，确保构建过程安全可靠。TEE 会模拟交易执行，检测是否有交易会失败，并剔除失败的交易，从而防止用户因失败交易而支付高额费用。

生成 Flashblocks（闪块）：Unichain 中每 1 秒生成一个区块，并引入一种预确认机制 Flashblocks ，将每个区块被分为四个闪块（即每 250 毫秒生成一次预确认），并实时传输给定序器。用户可以在交易被正式打包之前就获得早期确认，防止由于区块重组等原因而导致的交易回滚，降低因不确定性导致的额外费用。这一机制加快了交易结算速度，减少 MEV 提取的机会。

优先排序和可验证性：Rollup-Boost 提供了一种可验证的交易排序方法，使用户能够验证其交易在区块中的执行顺序。通过在 TEE 中进行区块构建，交易优先排序可以按照特定规则（如支付的优先费用）透明地进行，并通过验证证明确认区块构建是否符合这些规则。这种机制不仅能防止区块构建者滥用排序权力，还能内化 MEV，即设置规则（如 MEV 税）将一部分 MEV 的收益分配给协议或流动性提供者。

### 2. Unichain Validation Network（Unichain 验证网络）

Unichain 验证网络（UVN） 通过质押和分布式验证，解决单一定序器架构中存在的风险，并加速区块链的经济最终性。

UVN 由多个节点组成，每个节点都可以独立验证区块的状态，确保所有交易记录是合法且未被篡改的。可以防止单一定序器中的冲突区块风险（Block Equivocation Risk）或无效区块风险（Invalid Block Risk），从而增强网络的安全性。成为 UVN 验证节点的运营者必须在以太坊主网上质押 UNI 代币，质押越多的节点拥有越大的权重，更有机会成为活跃的验证节点。

此外，UVN 提供了一种更快的经济最终性机制，通过多节点并行验证来减少单一定序器带来的潜在延迟。每个验证节点在验证周期内都对区块的有效性进行确认，并将验证信息公示到网络上，增加链状态的可信度。一旦区块通过验证，这些交易便被视为不可逆地完成（即经济最终性）。验证者在每个验证周期内需要对区块进行验证并发布公证，否则将无法获得相应的奖励。

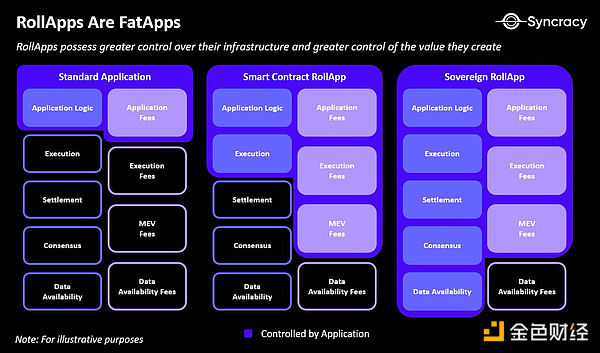
## 社区对 Unichain 怎么看？

Syncracy Capital 联合创始人 Ryan Watkins提出「RollApps are FatApps」的观点，认为 Unichain 所代表的 RollApp 具有更高的控制能力和灵活性，类似于胖应用，拥有更大的控制权和对基础设施的管理能力，能够更好地掌控自己创造的价值。他将应用结构划分为三种类型，并比较了它们的控制范围：

Standard Application：这些应用仅控制应用逻辑和应用费用，执行、结算、共识和数据可用性等层面依赖于区块链基础设施。应用的控制范围相对较小。

Smart Contract RollApp：通过智能合约扩展应用的功能和控制范围，覆盖了执行层面，应用可以管理自身的执行逻辑和费用，但仍依赖于底层区块链（如以太坊）的共识和数据可用性。

Sovereign RollApp：这类应用几乎可以控制所有层面（除了数据可用性），在基础设施上更具独立性，能够为用户和开发者提供更高的定制化控制和功能。



Fenbushi Capital 研究员 Yuki指出将 Unichain 并不是一个专门为特定应用设计的区块链（app-chain），而是一个通用的 L2 解决方案，具有内置的 MEV 再分配机制，不过仍然需要一些自定义的机制（如 hooks）来确保 MEV 收益流向特定的目标群体（如用户或流动性提供者）。

研究员 Haotian认为Uniswap 推出 Unichain 并非背离以太坊，而是进一步推动了以太坊 L2 生态的发展。目前的 L2 生态尚未充分激发 DeFi 的活力，而 Unichain 将在 DeFi 领域的扩展上起到催化作用。与 dYdX 和 MakerDAO 选择完全独立的架构和共识机制不同，Unichain 基于 OP Stack，依然符合以太坊的 Rollup-Centric 扩展战略，同时也为 UNI 代币赋予了更多功能。Unichain 将与其他 L2 共同竞争，有助于提升整个 L2 市场的活力。

也有一些不同的观点，例如 KOL sudo rm认为现阶段的扩展策略忽视了一些核心问题的解决。 L2 扩展了网络的处理能力，但用户的安全问题并没有得到有效解决。与其投入大量资金到 L2 的开发上，不如先解决以太坊生态系统中最基本和最根本的问题，比如用户安全性和抗攻击性。KOL Temmy 对 Uniswap 推出 Unichain 的必要性提出质疑，对是否需要更多的 L2 解决方案感到困惑，因为他认为现有的 L2 已经足够了。Uniswap 这样做可能会导致更多的流动性碎片化，并且如果其他 dApps 效仿，情况可能会比预期的更糟糕。