以太坊抗审查之路：BRAID 与 FOCIL 谁更胜一筹？

作者：0xNatalie

在以太坊区块生成和验证过程中，构建者负责从交易池中选择并排序交易，并通过拍卖机制将区块提交给提议者。提议者则从这些提交的区块中选择一个区块进行签名并提议到区块链上。由于提议者作为单一实体，具有最终选择权，这就带来了提议者与构建者之间可能勾结以审查交易的风险。

区块链的核心价值之一在于其抗审查性，即任何人都可以在不受中心权威干涉的情况下进行交易。当提议者能够控制哪些交易被包含在区块中时，这一特性就会受到威胁。损害公平性和透明性。并且可以利用这种权力来操纵区块中的交易顺序，从而获取额外的经济利益，引发 MEV 问题。

## 现有的抗审查解决方案

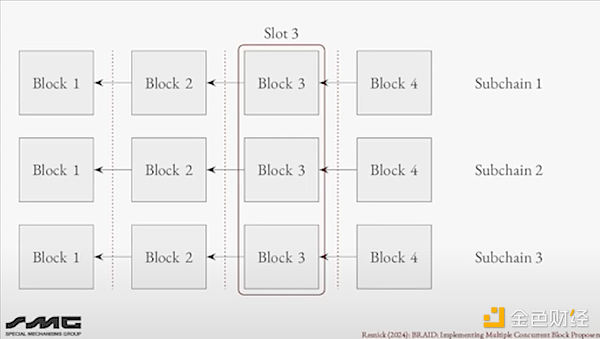
为应对这一挑战，社区提出了多种抗审查解决方案，比如强制包含列表（FOCIL）。在 FOCIL 机制中，每个 slot（时间槽）都会随机选出一组验证者，组成包含列表委员会。这些委员会成员根据各自对交易池（mempool）的主观视图生成本地包含列表，并将其广播。提议者则负责收集并聚合这些本地列表，形成一个聚合列表并包含在区块中。这种机制确保了区块的公正性，因为验证者会依据之前广播的本地列表来验证聚合列表的正确性，只有符合共识规则的区块才会被接受并添加到区块链上。

除了 FOCIL 之外，社区还讨论了多个并发提议者（MCP）的方案。这一概念最早由Max Resnick在Multiplicity机制中提出，旨在通过引入多个并行区块提议者分散权力，降低单一节点对交易审查的能力。在 Multiplicity 机制中，每个验证者都会从自己的交易池中选择一部分交易，构成一个「特殊交易包」。这些验证者将自己选定的交易包签名并发送给当前轮的提议者。提议者收到后，需要将其中至少 2/3 的交易包包含在自己提议的区块中。只有这样，这个区块才会被认为是有效的。这种机制确保了提议者无法单独决定区块内容，从而减少了审查的可能性。为了进一步激励提议者公平地包含交易，此机制实施「条件性小费」规则，即只有那些包含了该交易的提议者才能分得交易小费。交易的小费不是自动地全部给到包含该交易的首个提议者，而是根据一定的条件分配给实际包含了这笔交易的所有提议者。这增加了审查成本，如果想要审查则需要贿赂所有包含了交易的提议者。

## BRAID：改进后的 MCP 实现方案

在 Multiplicity 的基础上，Max Resnick 进一步提出了 BRAID，这是一个更加复杂且完善的 MCP 实现。在 Paradigm 举行的主题为「DeFi in MEV Era」的研讨会上，Max 介绍了BRAID。BRAID 通过允许多个提议者在不同的并行链上提出区块，并利用同步共识机制保持链间一致性，从而实现 MCP。每个链都有自己的提议者，所有提议者在同一 slot 内同时发布他们的区块。以太坊执行层将所有子链在该 slot 内生成的区块交易集合起来，形成一个执行区块，并按照预定的规则对这些交易进行去重、排序并执行，从而降低任何单一实体操纵交易记录的能力。

BRAID 的设计并不引入额外的角色，因此避免了激励/惩罚机制带来的复杂性，但其实施相对复杂，需要协调多个子链的同步和数据处理。



### BRAID 机制的问题

Blockchain Capital 团队Jonahb指出 BRAID 机制中存在的一个问题：「条件性小费」模型对流动性有要求，从而影响用户体验影响。这个模型是一种动态定价策略，要求用户预备一定数量的流动性，以确保交易的抗审查性。用户在提交交易时需要设置两个小费值（T 和 t）。最终实际支付的小费取决于包含交易的提议者数量。

较高的小费 T：代表用户为确保交易不被审查而愿意支付的最高费用。目的是激励提议者在没有其他提议者愿意包含交易时，选择包含。最终如果只有一个提议者愿意包含，则他获得 T。

较低的小费 t：这是用户设置的一个较低的金额，只要交易被多个提议者同时包含，用户就只需要支付 t。t 会在多个提议者之间分摊。如果用户不关心抗审查性，他们可以设置 T=t 并将其交易仅发送给一位提议者。

然而，这种额外的流动性要求增加了参与区块链交易的复杂性和成本，用户需要在交易的当下多预留出一笔资金，只为了保证交易的抗审查性。这些预留的资金在没有被实际使用之前，都是冻结的。

对此，Jonahb 提出了两个解决方案：

Proof of Post-State Liquidity（后状态流动性证明）：用户在提交交易时，提供一个证明，表明在交易执行后将拥有足够的流动性来支付 T（例如，交易后用户会有 $1M 的流动性）。这样，即使交易前没有足够资金支付 T，用户也能通过证明在交易后能够支付。这种方法的挑战在于提议者必须在交易执行前了解交易的最终状态，但大多数金融交易涉及共享状态（如多个交易共享同一账户余额），因此在交易排序确定前，提议者无法准确判断交易后的状态。这需要为每种交易类型提供定制的证明，实操性较低。

Censorship Insurance（审查保险）：引入第三方审查保险提供商（CI 提供商）为用户的 T 提供担保。用户为此支付一个保险费 rT，其中 r 基于交易被审查的可能性计算。此方案不仅降低了用户立即准备大量流动性的需求，还可以通过 CI 提醒用户 T 过低且存在审查高风险。但建立一个用户和 CI 提供商之间的市场需要时间。

## 社区对 FOCIL 与 BRAID 的看法

以太坊客户端 Prysm 开发者terence认为BRAID 的一个显著优点是它不需要额外的参与者。在大多数包括 FOCIL 在内的 Inclusion List (IL)设计中，都需要一个额外的参与者，这增加了以太坊时隙中的时间约束，例如提交 IL 的时间、更新出价的时间以及验证者检查 IL 的时间。不过 FOCIL 方案相比 BRAID 实施起来更为简单和灵活。

Paradigm 研究员Dan Robinson赞赏BRAID 在交易优先级排序上的设计，而不是由领导者（单一提议者）自行决定，有效缓解 MEV。此外，BRAID 中的条件小费机制激励非审查行为，这些在 FOCIL 中并没有体现。

开发者Dev相比 MCP更喜欢FOCIL，他认为 FOCIL 在提供强大的抗抵抗力和简化实现方面更具优势。并提供了一些改进方案使得 FOCIL 更容易实现。

以太坊研究员barnabe.eth认为FOCIL 是一种相当通用且具有可扩展性的机制，他承认 BRAID 有可能在某些方面改善 FOCIL 所提供的保证，但对完全放弃基于领导者的模型持谨慎态度，认为目前这还不是共识，需要更多工作来证明其可行性。