**深度研究：MEV 的过去、现状与未来**

[](https://www.panewslab.com/zh/author/1604853782940384.html)链捕手 ChainCatcher ｜2022-11-06 10:22

我们首先介绍什么是MEV以及它为什么重要。然后，我们将解释为什么我们认为MEV是基础，以及如何权衡MEV。

撰文：Amber Group

编译：郭倩雯，链捕手

**导言**

19世纪初，迈尔·罗斯柴尔德（注：历史上最有影响力商人之一，“国际金融业之父”）的五个儿子以法兰克福为起点进行业务拓展，先后在伦敦、巴黎、维也纳和那不勒斯建立了分支。他们建立起信息网络，使用信鸽、信使和租船在欧洲传递信息，速度比任何人都快。通过该网络，罗斯柴尔德家族比任何人都能更快地获得新闻和信息，并利用这些信息在套利和事务中获利。众所周知，这也使内森·罗斯柴尔德比伦敦的官方信使整整早了36个小时，了解到拿破仑滑铁卢战败的消息。

在所有市场中，信息都具有价值的。人们为了能优先接触到信息，进行着非常激烈的竞争。即使在今天，在传统市场上，高频交易机构和对冲基金在世界各地的发射塔和电缆上花费数十亿美元，进行军备竞赛，以获得仅以毫秒为单位的信息优势。

加密世界也不例外。在链上，对订单流和下单权优先访问的竞争愈演愈烈。这种“最大可提取价值”的概念（简称MEV）已从一个小众话题出现在几乎所有加密协议的前沿。我们看到社区内有越来越多关于MEV对协议的透明度、可持续性、去中心化、安全性、审查阻力、估价等的影响的讨论。

在本报告中，我们将讨论围绕MEV的几个关键话题。我们首先介绍什么是MEV以及它为什么重要。然后，我们将解释为什么我们认为MEV是基础，以及如何权衡MEV。我们还总结了MEV的现状和该领域的一些主要参与者。最后，我们讨论未来趋势和一些开放问题。

**要点：**

* **了解MEV很重要。**MEV影响安全性、稳定性和用户体验。这也是区块链代币增值的一个关键组成部分。最重要的是，它影响区块链网络的两个基本属性：去中心化和抗审查。
* **MEV是基础。**有一些解决方案可以减轻某些形式的MEV。但最终，一定量的MEV将永远存在。区块链网络作为智能合约平台，先天具有无限制和无许可的优势，但同样也受到MEV的诅咒。协议和应用程序在处理MEV时需要仔细考虑如何进行权衡。
* 我们估计，在PoW以太坊，**自2020年以来，MEV为矿工贡献了至少8%的总收入。**在主要类别中捕捉MEV机会——套利、清算和三明治攻击——竞争异常激烈，并被少数搜索者所主导。
* 尽管**跨链MEV**目前的影响力可以忽略不计，但它可能成为一股高度集中的力量，影响所有区块链发展。MEV对区块链网络的稳定性也是长远来看日益增长的威胁。
* 我们可以预见，在未来的订单流支付（PFOF）或事务流拍卖的场景，会将一定量的MEV返还给用户。在这些场景下，最有可能的路径是更大程度地集中区块建设者并降低验证者的产量，但要实现这些目的还需更多研究。

**内存池**

Daian等人在开创性的报告中首次定义了MEV。研究人员发现并研究以太坊上的多个机器人，他们相互竞争以获得优先排序，并详细说明了它们对区块链的影响。该论文还首次提出了MEV的定义，即“在给定的时间框架内，以太坊矿工可以从交易操纵中提取的总量，其中可能包括多个区块的交易价值。”

**以太坊交易的生命周期**

假设Joe想在一个去中心化交易所把100 ETH换成USDC。于是他导航到Uniswap的前端并连接他的MetaMask钱包。他指定了交易的输入内容：1000 ETH换130万美元USDC，滑点容差1.0%，然后签署交易。

他的交易首先通过MetaMask的默认RPC端点发送到Infura。Infura将此请求传播到以太坊网络中的其他节点，这些节点再以相似方式传播到它们所连接的节点。

每个验证器都有自己的内存池，内存池是每个验证器维护的待确认交易数据库。它基于自己的内存池构建交易区块。通常，这些交易是按Gas费用排序的。或者，验证者可以运行自定义软件，根据自己的规则和逻辑对交易进行排序。

每12秒，会随机选择一个以太坊验证者来构建和提出一个交易区块。提议者向网络广播新区块的产生。一个由其他验证者组成的委员会会被随机选择，来确定区块的有效性并对其证明。提交交易后，它们将从节点的内存池中移除。

**MEV 是如何产生的**

所有人都可以查看内存池。由于Joe的交易是公开提交的，它创造了几个潜在的盈利机会：

* **三明治**：乔的ETH到USDC的交易有一个异常大的1%的滑点容差。虽然他希望得到130万美元，但他向全世界发出信号表示，他会接受128.7万美元。监控内存池的其他实体可以看到Joe的态度，并试图进行“三明治攻击”，给Joe最坏的执行价格以获取无风险利润。他们先于Joe卖出ETH（抢在他的交易前面），允许Joe以他定义的最低限额卖出，然后以相对便宜的价格回购ETH，来实现盈利。
* **套利**：在Joe的交易之后，Uniswap和其他 DEX 之间的 ETH-USDC 交易对将出现暂时的价差。机器人会不断寻找这些差异，并将在Joe的交易后自动执行套利（回跑他的交易）以获取无风险的利润。

拥有特权的验证者更能获取这种利润。以太坊的共识协议只在区块级别强制执行协议，允许验证者选择每个区块内发生的交易。因此，验证者可以决定包含哪些交易以及这些交易的执行顺序。

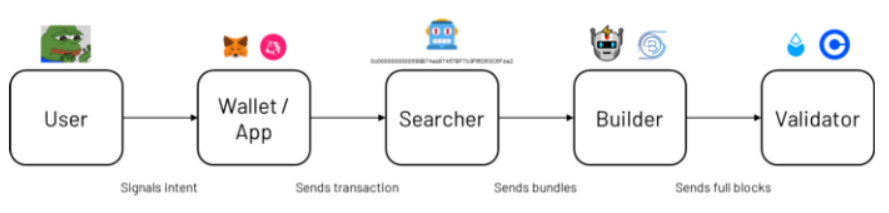
例如，假设有100美元的套利利润可以通过dex获得。Alice可以提交交易，试图从中获利，支付1美元的交易费。但是，内存池对所有人都是可见的。Bob在内存池中看到Alice的交易，复制了她的交易，并提出支付2美元的费用。其他人可能会蜂拥而至。

若不加管控，用户就会受到动态激励，纷纷与验证者/矿工创建链下协议，以保证交易被包含或能被下订单。或者，验证者/矿工自己可以提交并优先处理他们自己的交易，以获取全部100美元的套利利润。

因此有了“最大可提取值”这个术语，简称MEV。该术语在历史上被称为“矿工可提取价值”，但也适用于太坊向PoS的转变以及基于PoS的区块链市场。

**MEV 供应链**

从上面MEV的生命周期，我们可以总结出MEV的供应链：



* 用户：任何想要表达和提交改变区块链状态想法的人。
* 钱包/应用程序：将用户想法转化为区块链交易的用户界面。
* 搜索者：监控内存池并提交交易以提取MEV的实体。
* 建造者：汇总各种来源的交易，创建一个完整的区块，理想情况下是一个能最大化回报的区块。
* 验证者：履行共识职责，如提出和证明区块。

**MEV 的定义**

PoS区块链中MEV的最新定义是：

在给定环境状态和所有可用操作的情况下，验证者可以跨区块（或一系列区块）提取的总值。

验证者通常不能改变其环境的状态，包括区块链规则、区块链上的智能合约代码、其内存池中的交易集等。

可执行的操作包括重新排序、审查和插入交易。它们还可以加入更多的利基策略，比如改变块时间戳、操纵“随机性”、执行其他验证器等等。

**MEV 的类型**

三个最大和最具竞争力的MEV收入池是套利、清算和三明治攻击。

**1) 套利**

套利是MEV收入的最大来源。套利被认为是MEV，因为排序在这里很重要。

套利交易发生在所有市场。传统市场中的交易者面临一些库存不足或时机选择的风险，但许多MEV交易可以自动进行：要么所有想达成的交易都能顺利进行，轻松获得无风险利润，要么所有交易都失败。原子套利在某些情况下，允许搜索者以最少的手头资本进行操作。但也存在具有库存和时机风险的经典统计型套利交易，如CEX和DEX之间的价格套利。

原子套利的竞争异常激烈。套利需要：

1. 运行优化的硬件、软件，在数千组代币对中快速找到机会
2. 提交极其高效的事务，以最大限度地减少Gas费。第二种现象被称为“Gas高尔夫”（Gas golfing），允许MEV搜索者竞标事务。

**2) 清算**

像Aave、Compound和Maker这样的货币市场允许用户存入一些资产作为抵押品，并借入其他资产。随着抵押资产价值的波动，用户的借贷能力也随之波动。

如果借款人超出预算上限，这些协议会依赖市场参与者对借款人进行清算，但需付费。为了激励清算，协议向借款人收取清算费，并将其中一部分费用交给清算人。

这就是MEV的机会所在。搜索者竞相监控所有借款人的头寸，并试图成为第一个清算头寸的人，从而为自己收取清算费。

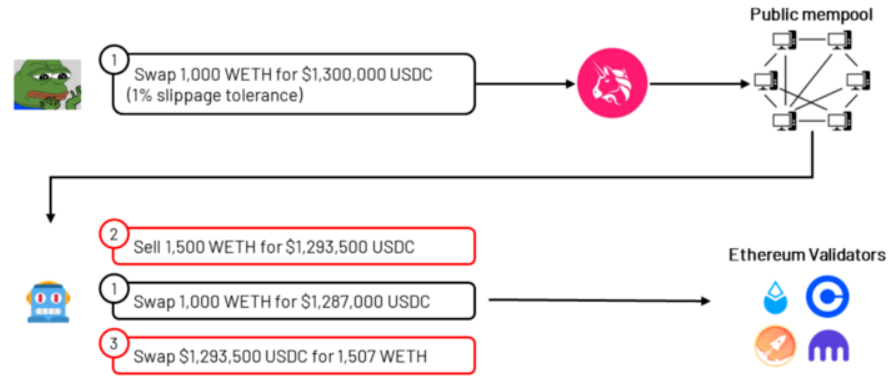
与套利类似，清算事件竞争激烈。在市场急剧低迷期间，清算借款人的竞争导致了巨额Gas费。同样，能优化代码的搜索者更最具竞争力，能去竞标清算。

**3) 三明治攻击**

区块链上的交易并非立即发生。当用户发送Swap交易时，他们定义一个可接受的价格变化百分比（“滑点”），该百分比在提交的交易等待处理时可能发生。

如果用户为他们的交易设置过高滑点，就会发生“三明治攻击”。搜索者利用这些错误，首先将用户的交易提前到最高可接受的滑点，使交易以不利的价格发生。然后执行用户的交易，进一步移动价格。在此之后，搜索者会回跑交易，净赚一笔。

比如，假设搜索者支付了4 ETH的Gas和优先权费用，其无风险利润为3 ETH。



上图为一个说明性的例子：一个用户想用1%的滑点容差将1000 WETH交换到USDC。搜索器在公共内存池中看到交易，于是创建一个抢先和回跑交易包，并通过MEV机器人将其发送给验证者。

如上图所示，三明治攻击更依赖于交易排序特权。如果三明治攻击的任何一半部分未能执行，搜索者将面临损失。

顾名思义，三明治攻击被视为恶性MEV，为大多数加密社区所诟病。套利和清算活动可能是恶性也可能是良性，但三明治攻击大多被视为纯粹的价值提取。一些搜索者甚至公开声明他们不会进行三明治攻击，不然可能会招致批评和反对。

**4) 长尾MEV**

长尾MEV机会比比皆是。比如：

* **Apecoin空投**：Yuga Labs决定向BAYC持有者空投代币。NFTX是一个将NFT标记为可替换令牌的应用程序。一个MEV搜索者用NFTX买下了所有的同质化BAYC代币，将整个池兑换成一个真正的NFT，要求Apecoin空头，然后重新供应NFTX池。这让机器人获得了大约6.1万 APE，相当于当时的27.8万美元。机器人支付了310美元的Gas费用。
* **误操作：**一名用户意外将一个EtherRock NFT标记为444gwei，而非444ETH，一个机器人立即狙击了它，并以234 ETH的价格出售——当时约为60万美元。
* **1inch遗留代币**：1inch偶尔会因某些原因在路由器合约中留下少量代币。一个被编程的MEV机器人会扫描这个路由器合约来获利。

**MEV 很重要**

了解MEV很重要。MEV影响安全性、稳定性和用户体验。这也是区块链代币增值的一个关键组成部分。最重要的是，它影响区块链网络的两个基本属性：去中心化和抗审查。

**1) MEV 产生的负面外部影响**

与MEV相关的活动产生负面外部影响。例如，如果没有有效的费用市场，对MEV的竞争可能会导致**优先Gas费拍卖**（Priority Gas Auctions，有时称为概率费用拍卖“Probability Gas Auctions”）。在PGA期间，搜索者和机器人战略性地设置他们的gas费用来相互竞争，使他们的交易包含在某些交易的前面（或后面）。这导致：

* 网络拥塞，这可能导致其他交易被网络卡住或丢弃
* 高且不稳定的手续费，使其他其他加密用户无法参与，并使不太善于计算的参与者处于劣势
* 失败的出价导致不必要地消耗区块空间（失败的交易也会耗尽块空间）

一个典型案例是Yuga Lab的Otherdeed土地销售。由于拍卖形式的特殊性，手续费用飙升至荒谬的水平，因为投标人争相将他们的交易纳入一个区块。几个用户出价超过2ETH的手续费，最终却交易失败。其他用户因价格过高，连着几小时都无法进入以太坊，不得不等待售卖结束。

PGA还导致了关于延迟性的军备竞赛，因为具有较低延迟的搜索者更有可能中标。随着闪电机器人和其他内存服务的出现，PGA在以太坊上出现的频率降低。但它们仍然经常发生在高吞吐、低费用的链上，如BNB链、Polygon侧链、Aurora等。

**2) MEV 会破坏网络的稳定性**

更宽泛地说，MEV极大地改变了对区块链网络利益相关者的激励。如果数值足够高，MEV奖励可以鼓励验证者和挖掘者参与恶意活动，例如执行重组尝试。事实上，一些社群之前发布的代码导致以太坊矿工能够重组以太坊网络，以获取先前的MEV收入。在当时，以太坊的社交层对矿工的这种实施做出阻止。

然而，这种威胁已出现在其他区块链上。在Avalanche的 之前，任何验证者都可以提出一个区块。在验证者提出一个包含有意义MEV奖励的区块后，另一验证者可以发布一个更长的区块链来“窃取”MEV。因此，一场重组竞赛出现了。显然，这降低了区块链平台的可用性。即使在今天，其他区块链几乎每天都在经历深度重组，这很可能是由MEV推动的。

除了重组，MEV还鼓励在高吞吐量区块链上进行垃圾邮件交易（spam transaction），导致费用市场失效。例如，垃圾邮件交易导致今年早些时候Solana的宕机。由于Solana上存在大量经济活动、交易费用较低、搜索者无法为交易订单偏好进行付费，搜索者受到激励，向验证者发送大量交易来提取MEV，有效地进行DOS攻击。

**3) MEV 是一股集中力量**

MEV是整个区块链的集中力量。

区块生产者可以通过两种方式提取MEV：要么他们自己占领MEV，要么他们把交易的重新排序权卖给别人。

第一种情况在验证者级别高度集中。与单独验证者相比，专业区块生成器更能有效捕获MEV。专业能带来更高回报——专业人士可以更好地投资于基础设施和人力资本，以最佳方式获取MEV。他们还能更好地确保独家订单流，让他们有更多的交易来构建区块，或者与搜索者合作，获得MEV捆绑包的独家访问权。此外，市值较大的机构也可以采用资本密集型MEV战略（如跨链MEV）。

因此，垂直整合（获取并自行运行自搜索器的验证者）和水平合并（组合不同MEV的搜索策略）很容易受驱动出现。

在这种情况下，专业验证者将逐渐从他们自己的利润中获得更大的股份。此外，如果允许协议内委托（也就是用户可以将他们的代币委托给其他验证者），其他用户也会受到激励将他们的代币委托给这些验证者，从而进一步加强他们的领先地位。

在第二种情况下，如果区块生产者自己不能有效地运行 MEV 策略，他们可以将交易的重新排序权出售给其他人。以太坊的路线图有效计划分离区块生产者和区块建造者来体现这一点。这将MEV的集中力量从验证者转移到了区块构建者身上。然而，要找出这种结构的最优解，仍需解决一些问题。

而且，在这两种情况下，MEV奖励都是高度可变的。这种动态有利于大型机构和验证者池，它们可以改变MEV奖励，因为大多数用户更喜欢稳定和可预测的收入。

MEV的利润可能会超线性增长。单个区块内的MEV提取与网络的哈希算力成线性比例。除此之外，随着网络优势的增长，捕获多区块MEV的潜力也在增加。

**4) MEV 有助于经济安全**

MEV收入导致区块链的安全预算增加，但价值需要被提取，才能保持区块链的安全。善意和恶意的行为者都应该试图提取尽可能多的MEV。否则，剩下的MEV将成为恶意行为者攻击协议的补贴。

这并不是说区块链应该盲目增加平台上的MEV来增加经济安全。如上所述，许多类型的MEV会降低用户体验。如果这种类型的MEV继续增加，用户将放弃网络，降低费用和经济安全。尽管如此，一定量的MEV是不可避免的，这是用户活动的结果。

一个良好的区块链设计应使MEV提取民主化，每个验证器都能以大约相同的速率提取MEV。正如Chitra和Kulkarni所指出的，MEV再分配系统也有助于提高经济安全。同时也应努力让新玩家容易进入该领域，推动这个领域的竞争，而不再是寡头垄断。

**5) MEV 降低成本**

MEV还可以降低用户的成本。例如，在DEX上进行掉期交易的用户依赖套利者来确保dex上的价格与CEX一致。事实上，一种名为JIT liquidity的MEV就提高了交易者的执行价格。

MEV还有助于保持算法稳定，限制货币市场协议上的坏账数量，并实现独特的DeFi设计（例如Primitive的RMM，Opyn的Squeeth。）

**6) MEV 创建代币价值**

验证者从发行奖励、基本交易费和MEV/优先费中获得收入。发行奖励实际上是所有权从被动持有人到股东的再分配。基本交易费用在很大程度上非常低，趋向于零。

因此，我们认为L1/L2代币的长期价值在于货币溢价（如BTC、ETH）和/或MEV。从根本上说，区块链出售区块空间。更大的MEV机会意味对块空间的更大需求。

因此，平台需要仔细考虑如何创建和捕获MEV，以免让它泄露给其他实体。

下面，我们列举了当前协议捕获和内化MEV的一些设计示例：

* **Optimism：**进行MEV拍卖。Optimism是以太坊L2。目前，它运行一个集中的序列器来确定交易订单流。根据最新消息，其目标是运行MEV拍卖，将 N 区块窗口内重新排序交易的权利拍卖给出价最高的投标人。这些拍卖的超额利润将通过追溯性公共产品资金用于协议开发。
* **Aurora：**管理和内部化MEV订单流。Aurora是在NEAR上作为智能合约实现的EVM。Aurora过去提供零手续费交易，但后来网络不断受到垃圾邮件交易的打击。Aurora最近宣布一项MEV项目，用于管理MEV流，以减少垃圾邮件交易和对Sybil攻击的激励。他们正在与Kolibr.io合作，为订单流支付创建一个开放和竞争的市场，在交易转移到公共内存池之前，要检查其是否存在MEV机会。
* **Osmosis：**最小化和捕获MEV。渗透是一个Cosmos DeFi应用程序链，旨在通过阈值加密长期降低MEV。它还旨在实施一个允许渗透到“MEV自身”的系统——如大额交易后的套利——利润流向渗透利益相关者。
* **Cosmos**：创造跨链块空间市场。Cosmos是区块链的互联网，创建了几个重要区块链的主干，包括BSC、Polygon和Cronos。但一个常见的批评是，原生令牌ATOM没有从Cosmos的贡献中获取价值。最近，社区成员提出了一个新的建议，寻求提高价值的积累。一个提议包括链间调度器，它创建了一个跨链块空间市场，从跨链MEV活动中产生收入。

**MEV 将增加**

MEV随着复杂性而增长，我们预计MEV在未来十年将呈指数增长。

即使仅在以太坊上，由于新协议和原语的增长，自Flash Boys 2.0发布以来，MEV增长也有了阶跃变化。全新资产类别（NFT）的兴起以及与之相关的各种金融实验也极大地扩大了MEV出现的媒介。

这种趋势必将继续下去。区块链网络作为智能合约平台，先天具有无限制和无许可的优势，但同样也受到MEV的诅咒。

MEV已经单独存在于每个链上。但是因为不同的区块链有不同的信任假设，所以在边界上总会存在额外的MEV。

为了更好地理解MEV动态，需要将区块链分解为三个基本要素：

* **虚拟机：**虚拟机决定维度——协议能做什么：从极其有限到图灵完备。如上所述，更大的复杂性为MEV创造了更宽的向量。允许任何开发者部署价值数十亿美元的智能合约既是好事也是坏事。
* **共识机制：**区块链的一个基本特征是就有效交易及其执行顺序达成共识。加密记录是为了证明交易是有效的，并向我们展示世界的状态。但是同时有很多人试图改变世界的现状。将会有用户对他们提议的世界有所偏好，并且愿意花钱来获得这种偏好。
* **区块空间市场：**区块空间有限。市场需要有效地分配块空间。由于上述因素，如果市场设计不当，用户将转而进行链外订单。

我们认为，由于上述因素，只要区块链允许任何人部署智能合约并转移价值，MEV就会显现。

因此，我们认为，与其考虑如何消除MEV，不如考虑在这三个维度上权衡MEV。下面我们将详细介绍每个因素的一些注意事项。

**1) 区块空间市场**

也许最容易实现的目标是设计一个合适的区块空间市场。设计上的微小变化可能导致用户体验和外部性的巨大变化。

思考不同的设计如何在重大市场事件中发挥作用，例如火热的加密抛售或受欢迎的NFT造币。在这些事件中，订单偏好最为重要。

大多数没有有效拍卖机制的市场鼓励实体向区块链不断发送交易，如果赢得一个MEV机会就可以产生数百万美元的利润，并且链上下订单按照“先到先得”的顺序，搜索者会毫不犹豫地向验证者发送数千笔交易来获得利润。

**2) 共识机制**

减少有毒MEV的更好解决方案之一是加密内存池，如何有效地做到这一点仍有争议。

这里的一个关键权衡是延迟性。委员会的加密是带宽密集型的，特别是对于大型和去中心化委员会。即使使用像SGX这样的可信硬件也会给系统带来额外的延迟。这些系统还为协议引入了更大的复杂性、技术风险和额外的信任假设。

**共识机制的其他考虑因素包括：**

* 实现单一秘密领导人选举防止受MEV激励的DOS攻击
* 单插槽终局性（Single-slot finality）S.中间态到最终性（medium time to finality）V.S. 可能最终性（probabilistic finality）
* 将构建者和提议者的分离体现在协议本身中（例如以太坊的提议者-构建者分离）

**3) 虚拟机**

限制虚拟机的功能会降低MEV。例如，比特币网络在它能做的事情和基于其应用程序的广度方面相当有限，因此平台上存在最低MEV。

开发者还可以决定创建一个许可平台，允许区块链专注于特定的垂直领域，帮助管理用户体验。例如，Osmosis和Sei是为DeFi设计的区块链。开发人员需要提交提案并获得批准，然后才能部署智能合同。这大大降低了MEV可能出现的概率。

**MEV 的现状**

闪电机器人（Flashbots）在不断塑造以太坊上MEV的情况。不久前，美国财政部制裁Tornado Cash 智能合同和相关地址后，在此之后加密社区一直在努力解决其在订单流和块构建中的作用。

**1) 起源**

闪电机器人是一家研发机构，成立于2020年7月，旨在减轻MEV的负面外部影响。

他们在2021年推出了“MEV-geth”，为以太坊创建了一个链外私人事务池，和一个密封区块块空间拍卖。这使得搜索者可以创建和发送事务的“捆绑包”。捆绑包允许搜索者描述在什么条件下应该执行一组交易。值得注意的是，它们具有原子性：要么所有交易都通过，要么一个都不通过。这对于某些类型的交易（例如三明治攻击）尤其有利。

搜索者将包裹发送到一个闪电机器人中继者，用于验证包并减轻DOS攻击。然后，有效包被发送给矿工，矿工可以评估他们收到的捆绑包，创建一个利润最高的区块。

**这种架构的优点包括：**

隐私——交易只有在被包含在一个区块中后才会公开披露。失败的交易不会被公开。它们也不需要手续费。因此，搜索者更有信心能捕捉到MEV，而没有其他机器人识别和抢先发现机会的风险。

效率——该设计为MEV机会创造了一个高效的市场。对最明显MEV机会的竞标将十分激烈，但不会消耗链上不必要的资源。新进入者可以利用长尾或利基机会自由进入市场。

需要注意的重要一点是，该设计不是一个无需信任的解决方案。中继者和矿工都可以看到搜索者提交的捆绑包。他们可能偷了包裹（据称确实偷了）。然而，这种架构也在进行声誉维护，从而使系统尽可能完善完整。

**2) PoW 里的 MEV**

从2020年1月到合并，闪电机器人从部分DeFi协议的套利和清算中获得的MEV总毛利约为6.75亿美元。这个数字应该被认为是MEV的最低估计值，不包括三明治攻击、NFT MEV机会、长尾DeFi活动等。它也只计算闪电机器人数据，但其实搜索者也可以使用其他解决方案。

此外，Chorus One估计，自2020年8月以来，三明治事务的利润接近10亿美元。在同一时期，Messari估计以太坊矿商的总收入约为289亿美元。

这表明，从2020年到合并，MEV贡献了至少5.8%的矿商总收入。

**3) 在 PoS 中提升 MEV**

MEV-geth的设计在合并后无法发挥作用。在PoW以太坊中，只有少数矿池运营商主导算力。任何通过窃取闪电机器人捆绑包进行“欺骗”的运营商都可能受到惩罚。对大多数矿工来说，失去这项业务是不值得的。

合并后，任何人都可以启动验证器。先前的MEV-geth设计无法发挥作用。如果你向单一验证者发送捆绑包，他们偶尔会受到激励，将高价值的MEV事务占为己有。惩罚并不能阻止他们的行为。此外，如前所述，验证者既是构建者又是提议者，因为可以作为一种集中力量——但单独运营商在构建优化区块块方面不太可能像机构运营商那样有效。

因此，闪电机器人合并后，MEV解决方案“MEV-boost”被推出，专业“构建者”的概念出现了。构建者是只专注于接收交易和构建优化块的实体。

验证者可以选择通过中继者从构建者那里接收完整的区块，并获得奖励。这些块是不可见的——验证者在交易被发送到网络之前看不到交易，如果他们试图窃取MEV，就会受到惩罚。

最终，这种架构减轻了MEV对验证者的集中影响，将中心化推向了区块构建者。

**4) 审查和过滤**

这种新的架构引入了新的审查点。只有少数实体经营继电器和建设者，其中一些实体必须遵守当地监管机构。值得注意的是，一些中继者和建设者（包括闪电机器人自己的），都过滤掉了OFAC批准的地址。它们将不包括与美国财政部指定的智能合同或地址进行交互的任何事务。

**事实上，只有占mev-boost市场份额12.5%的3个中继者不审查事务。**

那为什么这件事突然受到人们的关注？在以太坊采用PoW时，审查问题并不普遍，因为矿池就是他们自己的区块建造者。即使闪电机器人试图审查事务，这些矿工也可以在闪电机器人的捆绑包之后附加审查过的交易。

**未来趋势和开放问题**

**1) 跨链 MEV**

假设L1以太坊上的Uniswap和Arbitrum上的Uniswap存在价格差异。ETH在以太坊上售价1400美元，在Arbitrum上售价1300美元。该如何套利呢？

1. **官方桥**：在Arbitrum上购买1个ETH，使用Arbitrum的官方桥将ETH移动到L1以太坊，需要8天。希望到那时价格不会波动太大（或者用永久期货对冲）。然后在L1以太坊出售。
2. **第三方桥**：使用第三方桥将ETH移动到L1以太坊。需要5-20分钟，取决于用户对速度、安全性和收益的优先级考量。
3. **CEX**：一些事务所直接接受Arbitrum的存款。从存款到取款时间不定，但大致在5-20分钟之间。
4. **自营资产负债表**：在两条链上持有ETH和USDC的组合，并在机会出现时在两条链之间进行套利。不时重新平衡，以确保两条链上都有足够的库存。

显然，备选方案4几乎总是能使你获利。但这种策略也是最资本密集型的选择，有利于专业做市商和机构。

事实上，这种动态刺激了跨多个链的共谋。跨链MEV执行是概率事件，一个机构可以在多个链上设置验证者，以最大程度降低风险并更有效地捕获MEV。

**2) 多区块 MEV**

受功率限制，多区块MEV以前在以太坊上是不可行的，因为没有人事先知道下一个提议者是谁。

然而，合并后，任何人都知道谁将在一个 Epoch 内提出接下来的32个区块。目前有超过44.5万个活动验证者，看起来一个验证者似乎不太可能被选中在一个 Epoch 中提出多个区块，更不用说多个连续区块。然而，多个验证器通常存在于一个实体或池下。仅比特币基地就控制了13%的活动验证者——这让他们有大约39%的机会连续提出至少2个区块。

也许，多区块MEV带来的最大威胁就是操纵TWAP价格预言机，从而利用货币市场协议。虽然这不是主要威胁，但当TVL回归时，这些攻击的风险就会增加。

但这只是一个可能，我们还没有看到多区块MEV有这样的动机，特别是持续几个区块都有这种动机。五个连续的区块意味着一个实体可以在以太坊上控制整整一分钟的区块生产。

**3) PFOF 与交易流拍卖**

用户意图和交易流是MEV的主要来源。因此，我们可以想象一个场景，钱包或应用程序将它们的交易流拍卖给构建者。钱包、应用程序和基础设施提供商处于有利地位，可以从聚合和拍卖订单流中受益，从而获得收益。

**结语**

前景似乎十分黯淡——加密货币的市场结构正趋向于传统金融:交易进入黑箱，由特权中介机构管理，将结果从另一端展示出来。

好在，我们看到越来越多的人参与到MEV中，从讨论什么是公平，研究适当的市场设计，到实际实施缓解EV的整个供应链解决方案。

这是一个很长的报告，我们只触及了MEV的表面。因此，我们在下面列出了一些参考资料，供有兴趣深入研究某些主题的读者参考：

* Flash Boys 2.0 — Daian et al.: Seminal report investigating MEV and its impact on Ethereum
* Ethereum is a Dark Forest — Paradigm: Riveting first-hand account of avoiding generalized frontrunners on Ethereum
* Ethereum Blockspace — Who Gets What and Why — Paradigm: First principles based approach to understanding blockspace markets and MEV
* MEV … wat do? — Phil Daian: Arguing why MEV is fundamental and how to manage MEV
* MEV Manifesto — Delphi Digital: Deep dive into MEV design and solutions on Ethereum
* Optimism’s MEVA Proposal: Optimism’s original proposal of MEV auctions on L2
* MEVA (What is it good for?) — Ed Felten: Argument for why MEV Auctions are harmful to user experience and makes centralization worse
* Formalization of Cross-Domain MEV — Obadia et al.: Investigation and formalization of cross-domain MEV

<https://www.panewslab.com/zh/articledetails/veyx9njj.html>