比特币MEV科普：那些你不知道的知识

来源：极客 Web3

比特币网络中的MEV概念大约在2013年开始引起关注。尽管MEV问题更常与以太坊相关联，但比特币也并非没有mev问题。比特币的设计模型和以太坊十分不同，使得自身生态内的MEV未受到太多关注。但随着Ordinals、Runes和各种L2的开发，MEV在比特币中越来越显著。

在本报告中，我们将探讨比特币上日益复杂的MEV，并研究其对生态系统的影响。

## 为什么现在需要关注比特币MEV

在Ordinals火热之前，比特币上的MEV活动并不为人所熟知，主要集中在闪电网络和侧链挖矿等攻击事件中。而Taproot升级带来了更多的可编程性，促进了如 Ordinals和Runes等协议的推出，这使得MEV问题成为了焦点。

比特币10分钟的出块时间进一步加剧了这一问题，因为这会让交易在mempool中的等待时间增长，给MEV玩家留下更多的观测空间，如抢跑交易者可以给矿工提供额外的费用等MEV手段获得更大利益；随着区块奖励的减少，矿工们也可以通过铭文、runes等其他变现渠道寻找收益，这导致了越来越普遍的MEV活动。

下图展示了在备受期待的Ordinals和Runes发布期间，交易手续费相对于区块奖励的激增，有时甚至占据了比特币挖矿总收入的60%以上。



（Source:Dune analytics, transaction fee share % of mining reward, data as of 22 July 2024）

除此之外，在2024年，我们还看到越来越多的BTCfi应用和协议。未来，我们可能会看到比特币的MEV的发展达到更高的规模。

## MEV在比特币和以太坊上的区别

过于关于比特币MEV的讨论比较少，重要的原因在于比特币的架构和以太坊存在着本质区别。

### 比特币的UTXO模型

以太坊通过EVM来执行智能合约，实现了可编程性，并通过维持全局状态来达到这一目的。以太坊采用账户模型，通过管理交易的nonce顺序执行交易。这意味着交易的先后顺序会影响到执行结果，导致搜索者能够轻松识别MEV机会，并在用户交易之前或之后直接插入一笔交易。这类似多个用户同时向数据库写入数据时的竞争态（racing condition）问题。

例如Alice和Bob同时向Uniswap发出相同的：用1ETH换取USDT的交易，但在区块中先执行的交易会获得更多的USDT。

而比特币采用了脚本+UTXO的方式，不带有状态。如果只是一个典型的用于转账的交易，只有接收者能通过自己的签名来解锁，不会存在与其他人读写竞争的问题。

不过比特币上也可以用脚本或SIGHASH构造出来多人均可解锁的UTXO，此时先确认的交易会获得这些钱。但因为每个UTXO的解锁条件仅和自身有关，不会依赖于其他的UTXO，因此竞争态只是局限在这笔UTXO内。

### 引入了BTC以外的资产

除了上述设计的本质区别外，引入BTC外的有价值资产也引发了产生MEV的条件。这些场景产生的MEV，本质上都是协议设计者在BTC上尝试用脚本+UTXO 构建新的资产类别和链上action时，通过顺序来规定资产的所得以及action的合法性与否。有了基于顺序定义的event，就有了竞争顺序的incentive，也就有了 MEV。

在不考虑其他资产的情况下，理性的矿工只会按照交易费率来打包合法交易，并根据交易数据的大小来收取相应费用；但如果一笔交易代表的意义不再是普通转账，而是mint出一个有价值的资产（如Runes等），矿工就可以有多种策略：

1）拒绝这笔交易并自己mint铭文资产；

2）向用户索要更高的手续费；

3）让多个同时发出交易的用户竞价

### Mint

最直接的例子就是在 Runes、BRC20等资产的mint过程中，一般都会约定好资产mint的上限。先确认的mint交易会被认为是成功的，否则会认为无效。那么交易的先后在这种场景中就会至关重要，也就提供了MEV交易的先后排序机会。另外，ordinals引入的稀有聪概念，甚至让一些人担心在减半时矿工为了争抢高价值稀有聪会引发区块重组。

### Staking

除了mint，Babylon等staking协议也会规定每个阶段用户可stake资产的上限。尽管在达到上限后，用户仍然可以构造并发送比特币到staking的锁定脚本中，但此时已无法被认为是成功stake并能在未来获得奖励。也就是说，staking交易的先后排序也至关重要。

例如，Babylon主网上线后很快就到达了phase-1的1000个BTC的上限，导致后面的大约300个BTC超出限额、需要用户手动解锁。



（Babylon主网上线时，费率飙升至超过1k sats/vBytes, Source: Mempool.space）

除了主链上的铭刻/蚀刻资产和staking外，侧链或rollup上的一些活动也会收到影响。我们将在“比特币上MEV的事件”列举更多实例。

## 哪些算比特币的MEV

那么究竟哪些可以算作是MEV，或者更严格的说，比特币上的MEV？毕竟MEV 的定义也在各种语境下并不十分一致。

通常来说，MEV，矿工可提取价值或最大可提取价值，指的是矿工通过操纵区块创建过程以提取最大利润的不同方式。这类活动可以通过多种方式呈现。我们可以按照其参与者和收益去向大概分为以下几类：

用户支付额外费用：例如带外交易加速服务、私密交易池（private mempool）等。交易者也可以通过RBF、CPFP等手段给矿工更高的费用从而确认具有MEV价值的交易。

用户与矿工合谋：用户和矿工合谋对一些有特定意义的交易进行审查或打包。例如作恶的用户与矿工合谋对闪电网络的惩罚交易进行审查，避免其打包从而非法的获取通道内资产。其他新的合约式协议，包括BitVM2的惩罚交易等，也将面临类似的问题。

矿工对L2的挖矿：包括最早的各类合并挖矿方案，矿工在给比特币提供算力的同时将计算的结果也用于其他侧链或L2网络。矿工可能会利用在主链上的算力影响L2的出块、排序等，从而获取超额的L2挖矿收益甚至于影响L2的网络安全。

可以看到，如果是偏向公开市场手段的竞价方式（RBF等），对于整个经济体系仍然起到了比较好的正向激励作用；但无论是用户直接发送交易到矿池，或者是矿池通过筛选交易来牟利，无疑会对比特币社区最为珍视的去中心化和抗审查性提出了挑战，因此也被称为“MEVil”。

## 比特币MEV的典型案例

根据上述的分类，我们可以看到不少相关案例。

### 非标准交易：non-standard transactions

Bitcoin Core软件仅允许节点处理不超过100kvB的标准交易。然而，矿池们仍然将提供高额交易费的非标准交易包含在区块中，这通常以排除其他低费用交易为代价。

其中一些比较典型例子包括：

区块776,884由Terra矿池挖出，包含一个大小为3.38MB的1分钟mp4视频，显示一只青蛙拿着一杯饮料，为矿工赚取了0.5BTC的费用。这一个交易就占了849.93 kvB。

区块777,945包含一张4000 x 5999像素的WEBP图像，占975.44 kvB，为矿工赚取了0.75BTC。

另一个区块786,501，收到了约0.5BTC的费用来刻录一张992.44 kvB， 朱利安·阿桑奇的比特币杂志封面的JPEG图像。

默认的Bitcoin Core节点仅被允许转发标准交易。因此，非标准交易必须通过私有交易池直接接触矿池。私有交易池允许矿池接受非标准交易并提供交易包含的保证。虽然这可以加快交易处理，但随着更多交易转移到私有交易池，这可能导致矿池中心化和增加审查的风险。显然，一些矿池已经在利用运营私有交易池的盈利机会。

例如Marathon Digital引入了“Slipstream”，这促进了私密交易池。这使得Marathon能够向客户提供将复杂和非标准交易提交到网络的能力。

## 侧链或L2上的MEV事件

Stacks侧链此前采用了一个比较特殊的共识方式：Proof of Transfer（PoX）允许比特币矿工挖Stacks区块，并在比特币链上结算其交易。

Stacks参与者在比特币链上转账中进行区块承诺，以此来获得机会得到Stacks 上的出块权和对应的奖励。通过加权随机函数，胜利的矿工能在Stacks网络上挖掘区块。这导致大矿工审查其他Stacks参与者的交易，而只打包自己的 block commit，以此独自获得大量的STX奖励。

随着越来越多的矿工采用这种策略，其他Stacks的参与者基本不太可能可获得奖励。

这种行为对生态带来怎么样的影响呢？

1）通过排除其他诚实矿工的承诺，这减少了最终传递给stackers的奖励

2）如果大矿工持续滥用其算力并排除诚实矿工的承诺，还可能导致中心化问题，使少数矿工完全独占利益。

然而，这个问题现在通过Stacks Nakamoto升级得到了缓解，该升级使这种策略再次出现变得无利可图。此次升级将从简单的矿工选举转变为使用排序算法，Assumed Total Commitment with Carryforward(ATC-C)技巧，降低了 MEV挖矿的盈利能力。由于使用ATC-C，矿工赢得排序的概率现在等于矿工的 BTC花费除以最近10个区块中的中位数总BTC承诺。

另外，未在过去10个区块中的至少5个区块中进行挖矿的矿工，将被取消获得任何Stacks奖励的资格。这减少了矿工通过排除其他矿工的区块承诺来获得不成比例利益的动机。

### 另类资产交易的竞价

对于Ordinals和Runes这些另类资产的MEV，也可以归结到前述的两类：

矿池通过打包区块和交易获取了Ordinals的额外价值或稀有聪等资产

交易者对这些另类资产交易的竞价

对于矿池来说，Runes一开始的出色表现，为矿池提供了额外的利润来源。例如减半时，备受期待的Runes上线推动了网络交易数量和费用达到了历史新高，因为许多用户争相将他们的交易纳入历史性的比特币减半区块中。Post-halving 的交易费用已经突破了1,500sats/vByte（在减半前不到 100 sats/vByte）。

ViaBTC成功利用了这一热潮，挖掘了与Runes上线同时发生的减半区块，在 block 840,000获得了40.75BTC的利润，其中37.6BTC来自与Runes相关的交易费用。





Source: Mempool.space

而对交易者而言，比特币上的Runes和Ordinals交易采用特殊操作码来允许签名的输入和输出被组合，而交易池的透明性也允许许多买家发现潜在的有利可图的交易。

所以对于出现的交易机会，交易者也会频繁使用RBF（费用替换）和CPFP（子为父偿）来竞价，从而使矿工也能够利用这种需求来捕获MEV。例如当卖家列出他们的资产出售时，买家可出价并在有竞争者时使用RBF来提高自己的交易费用，希望自己的交易被确认。

下图中是这种交易者之间的竞争案例：

2ffed299689951801a68b5791f261225b24c8249586ba65a738ec403ba811f0d

这笔交易十分典型。可以看到当卖家挂单之后，成交交易被多次利用RBF的方式以238、280、298、355 sat/vB的费率来替换。



Source: Mempool.space

另一个例子是在Magic Eden平台上OrdiBots铸造过程。几位用户成为了交易池抢先攻击的受害者。OrdiBots的铸造铭文在Magic Eden上使用了PSBT（部分签名比特币交易）。

PSBT和10分钟的区块间隔允许任何潜在买家通过引入不同的地址、签名并支付更高的费用来竞争同一交易。这导致几位白名单用户由于被抢先攻击的机器人干扰而无法铸造（事后团队已经道歉并承诺用定制的 OrdiBots补偿受影响的用户）。

但也并不是所有 MEV 相关技术或事件都是会对用户不利的。MEV 的技术也会在有一些事件中保护用户资产免遭损失。没有启用RBF，错误挂单无法被抢救，被卡住的交易也会长时间保持卡住状态。因此Peter Todd 等也建议全节点启用 full RBF的选项来转发没有标记RBF的交易。

## 比特币上MEV的重要技术组件或手段

那么这些 MEV 都是由哪些比特币上已经提供的技术手段来支撑的？目前涉及到的常见的技术领域包括交易池、RBF、CPFP、矿池加速服务、矿池协议等。

### 交易池（mempool）

和以太坊以及其他典型的区块链网络类似，比特币也有交易池的结构，用于保存 P2P节点收到但还未在区块中确认的交易。和以太坊类似，交易池在比特币的 MEV也可以起到非常重要的作用，可用于查看和估算哪些交易会被打包。

但和以太坊gas机制不一样的是，比特币的手续费（fee）仅和交易体积有关，因此比特币的交易池可以看作是更直接的区块空间拍卖市场，可以看到哪些用户、按照什么样的价格在竞标下一个区块。

因为不同节点收到的P2P传播的交易不一样，比特币网络中并没有唯一的交易池。而且每一个节点也可以主动自定义自己的转发策略（mempool policy），定义自己想接收并转发的交易；

矿池也可以按照自己的喜好来选择打包哪些交易（尽管经济理性上是优先确认费用高的交易）。例如Bitcoin Knots的节点就不接受和转发ordinals的交易，而 Marathon矿池也在浏览器里构建出来一个像素风格的logo。



（区块836361在浏览器中的显示（像素颜色表示该交易的费率），Source: mempool.space）

所以用户可能会考虑将交易直接发送给矿工或矿池，以期待更快的打包，但这样会损害比特币社区非常重视的两个特性：隐私性和抗审查性。

交易通过P2P节点传播而不是直接发送（例如通过一个RPC端点）给矿工或矿池，有助于混淆交易背后的实体信息，使得矿工和矿池无法通过这些被识别出来的身份信息而审查交易。

但有时候我们确实想让交易更快的得到确认，或者因为之前设置的手续费太低而很难被打包进区块的时候，我们仍然有一些工具可以使用，即RBF和CPFP。

### RBF、CPFP

手续费替换（RBF）和子为父偿（CPFP）是用户通常可以使用的提高交易优先级的方法。

RBF (Replace-By-Fee) 允许将交易池中未确认的交易，替换为另一笔与之冲突（也引用到至少一个相同的输入）且付更高手续费率和更高整体手续费的交易。

和前文讨论的交易池策略一样，RBF其实也可以有各种实现规则，但最常用的实现是按照BIP125设计的可选RBF(opt-in RBF），即对专门标记的交易可以替换；另一种是完全RBF（full RBF），无论是否标记，交易均可替换。

而CPFP（Child Pays For Parent） 追加手续费采用了另一种思路。尽管用户先发送了一笔未确认的低费率交易，但此时可以在后续（用前笔交易输出作为输入）交易中付更高的手续费率，以此激励矿工将这两笔交易都打包。

因此有时也可以在浏览器中看到，尽管某个时刻的费率很高，但依然有极低费率的交易打包进了区块，这些交易很可能就是使用了CPFP（因为是由后续交易付费）。



（该笔交易利用CPFP让低费率（7.01 sat/VB）父交易得以打包确认Source: mempool.space）

CPFP和RBF的主要区别在于，RBF是由支付方增加手续费率，而CPFP则允许接收方增加手续费率以加快交易确认，同时对于闪电网络中需要退出的预签交易很有用处（例如锚点输出）。但RBF也有成本上的优势，因为不需要额外的区块空间。

### 额外付费及矿池加速服务

而超低费率交易被打包的另一种可能性是使用了额外付费的方式。

除了RBF、CPFP这些直接交易追加链上手续费的方式外，用户也可以选择采用额外付费（out of band fee payment）的方式来给自己的交易加速。

例如很多矿池都会提供免费和收费的交易加速服务，为用户提交txid的交易进行加速打包。如果是收费的服务，用户需要给矿池支付一笔费用，以弥补矿池在手续费上的差额。因为这类服务在比特币网络之外的体系（例如通过网站充值、信用卡付费等）来支付手续费用，所以被称为是额外付费。

尽管带外付费给无法使用RBF或CPFP的交易提供了一种补救手段，但如果长期大量使用则会影响比特币的抗审查性。

### 矿池协议

我们上述的讨论基本上把矿池和矿工视为了一个群体来讨论，但实际上他们之间也需要分工和协作。矿池集中了矿工的算力来进行挖矿，并根据算力贡献的大小来分配奖励。而这个协作的过程就需要一些协议来进行配合。

目前常见的矿池协议中，例如Stratum v1，矿池只需要给矿工分发一个区块模板（包含区块头、coinbase交易信息），矿工根据这个模板进行哈希运算。目前也有一些工具，如stratum.work能可视化的看到各个矿池的Stratum信息。可以看到，在这个过程中，矿工无法选择要打包哪些交易，而是由矿池来选择交易并构建出模板来给矿工下发任务。

所以在Stratum v1协议中，我们也可以粗略地对标到以太坊生态中：矿池

矿工：承担一部分proposer的职责（计算哈希）

矿池：既是builder，也会利用矿工计算出的哈希，最终propose区块

## 未来如何

一些有前途的解决方案已经被开发出来或正在进行中，以减低 MEV 对比特币的负面影响。

### 新的协议和实现

在一些新的矿池协议中，例如Stratum v2、BraidPool等，矿工也可以自主选择要打包的交易。目前Stratum v2已有一些矿池（如 DEMAND）和矿机（如 Braiins）采用，允许个体矿工构建自己的区块模板，改善了数据传输的安全性、去中心化和效率，同时缓解了交易审查带来的比特币MEV风险。

因此按照这种趋势，未来矿池和矿工的角色分工也未必会按照以太坊PBS分工的方式演进。

另外，Bitcoin Core在交易池相关的新设计可能也会带来新的变化，主要会包括当前讨论最多的v3交易中继策略和族群交易池（cluster mempool）等。不过这些新设计的影响，例如对当前闪电网络通道的退出实现，仍然在讨论当中。

### 挖矿奖励减少的影响

挖矿奖励的减少已不可忽视。随着未来区块奖励的进一步降低，可能会对网络产生各种影响。

一些问题已被比特币开发者较早注意并讨论，例如手续费狙击（fee sniping）问题，矿池可能会故意重挖此前的区块以获取到交易手续费。Bitcoin Core已有一些防手续费狙击的实现，但目前的方法尚不完美。

除了原生手续费外，另类资产可能也是未来补贴挖矿奖励的一种渠道。因此也有一些项目在尝试构建一些基础设施，例如Rebar构建一种替代的公开mempool 来更好地识别出带有价值的另类资产交易。

然而如“带外付费”一节所讨论的，这些非比特币原生的经济激励，会对比特币自洽的激励相容体系产生何等影响还有待未来的进一步观察。

无论如何，比特币上的MEV可能既会从以太坊借鉴，但也会因为架构和设计哲学等因素而有很大差别。比特币日益增长的实用性、不断减少的区块补贴奖励以及不断发展的BTCFi生态系统，都会在未来把注意力集中在MEV上的因素。

特别鸣谢

感谢阿剑对本文的审阅和建议！