

MEV 与 Flashbots

七哥

<https://x.com/0xqige>

思考

- ❖ 如何偷偷的将交易发布到以太坊网络?
- ❖ 如何狙击项目方NFT定时预售?

以太坊黑暗森林

生存是文明的第一需求、资源有限、猜疑链、技术爆炸

《三体》中的“黑暗森林”是指宇宙中各文明为生存而隐匿自身、避免暴露位置的状态，因为任何暴露的文明必将遭到其他文明的打击。

以太坊中的“黑暗森林”指的是网络上充满隐蔽且高度竞争的环境（被来历不明的程序监控），其中交易在未确认前处于被窥探中，一旦有利可图就会被抢跑或被竞争！

MEV

最大可提取价值 Maximal Extractable Value

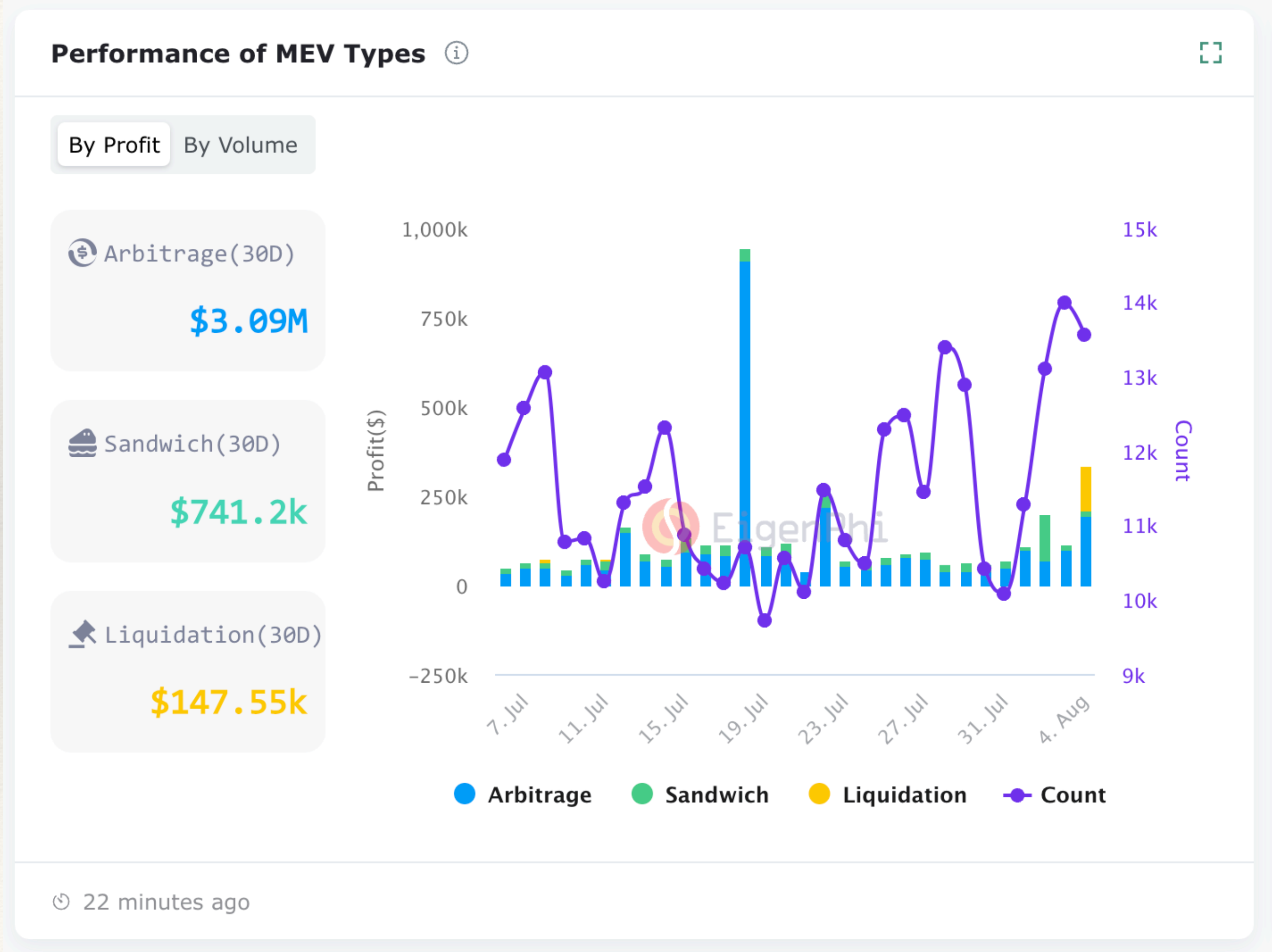
在区块链网络中，具有**排序权**的参与者通过重新排序、包含或排除区块中的交易，能够提取的最大利润，包括抢先交易、套利和三明治攻击等行为。MEV 反映了这些参与者利用交易顺序控制权力所能获得的额外价值。

争夺资源

MEV 策略

- **抢跑交易(Front-running)**: 利用未确认交易的信息, 提前进行相同交易以获取利润。
- **套利(Arbitrage)**: 利用不同交易所或市场之间的价格差异, 进行快速买卖以获取差价利润。
- **三明治攻击(Sandwich Attack)**: 在目标交易前后插入自己的交易, 以操纵市场价格获取利润。
- **清算(Liquidations)**: 通过触发借贷平台上的清算机制, 从清算中获利。
- **矿池提取**: 在去中心化交易所 (DEX) 中, 通过操控流动性池中的交易顺序, 获取最大收益。

MEV 获利



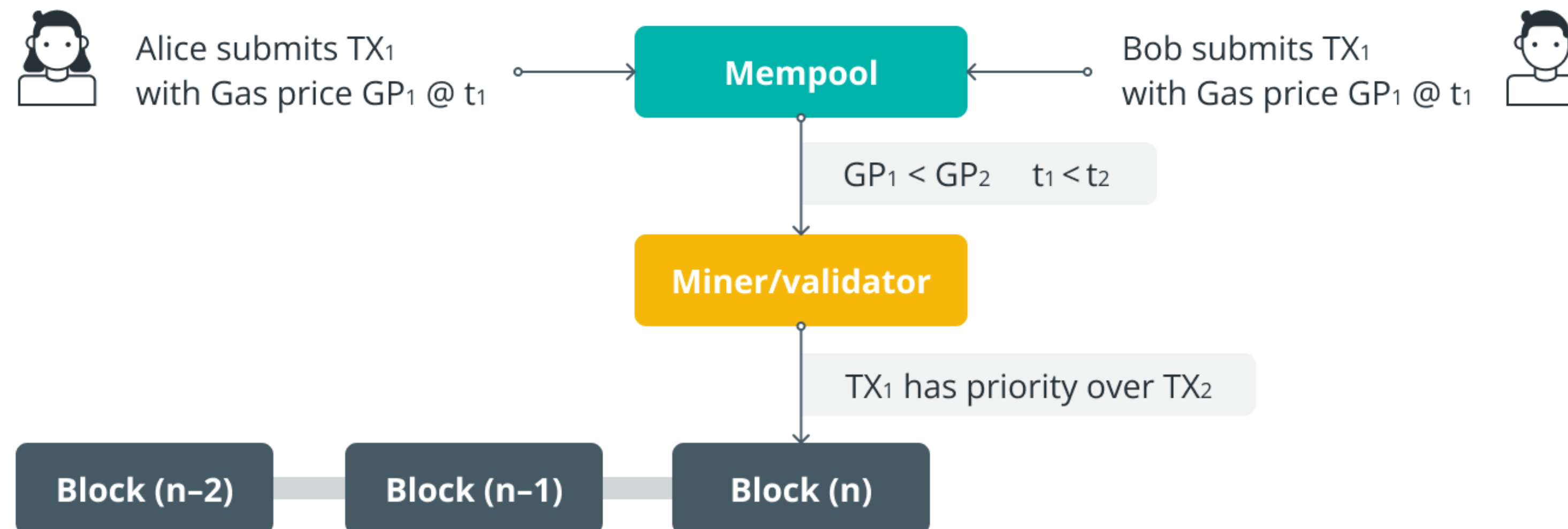
<https://eigenphi.io>

MEV 案例-抢跑

Bob 监听到 Mempool 有一笔有利可图的Alice交易，然后提高Gas抢先交易

```
'{"jsonrpc": "2.0", "id": 1, "method": "eth_subscribe", "params": ["newPendingTransactions"]}'
```

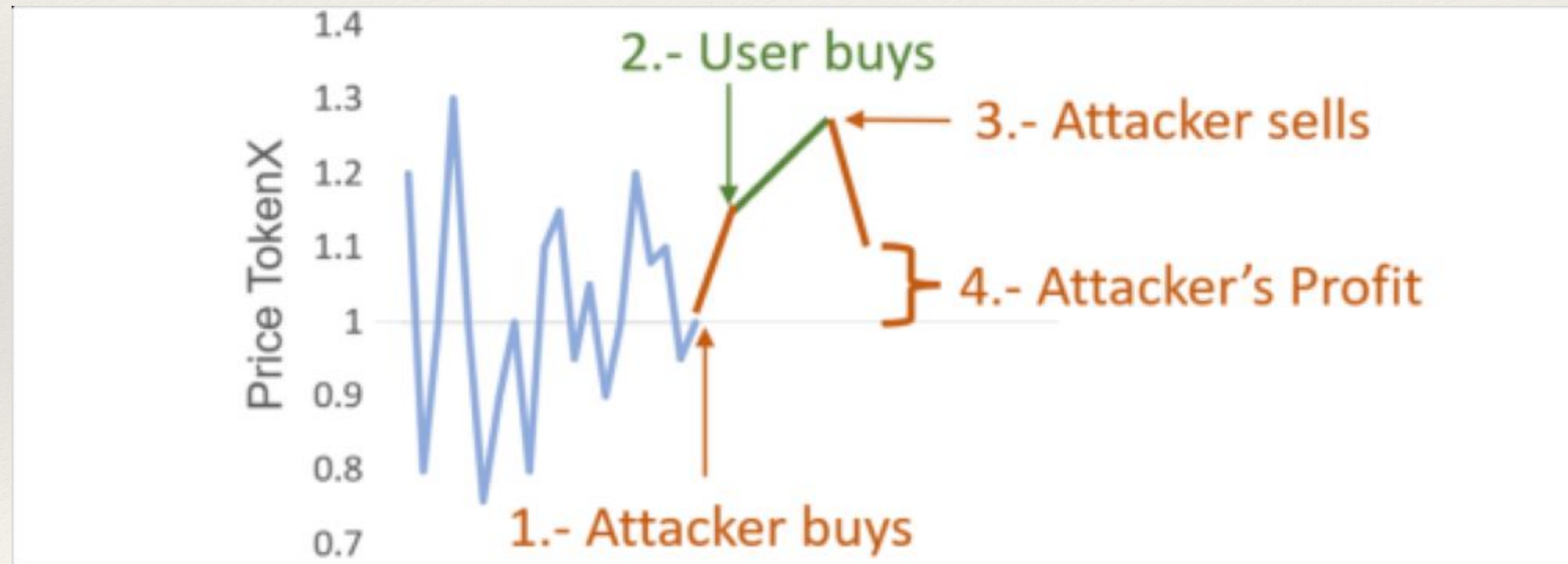
Visual representation of front-running



MEV案例-三明治攻击

$$X * Y = K$$

监控发现机会 -> 攻击者抢先买入资产 -> 受害者买入（Swap时得到的更少） -> 攻击者后置交易卖出资产

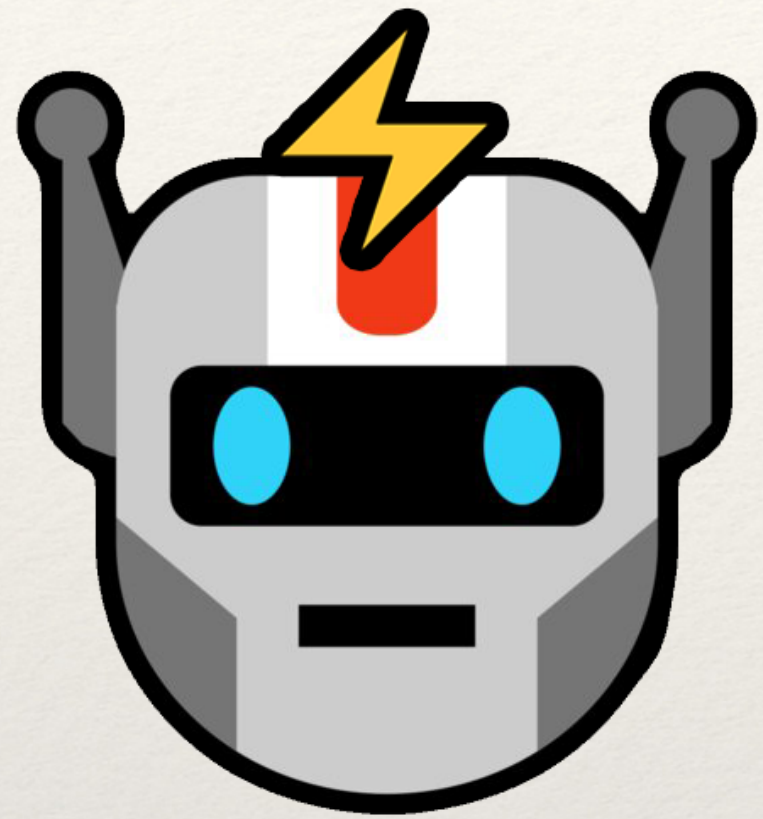


如何攻防MEV

有人的地方，就有江湖

打不过，就加入

什么是Flashbots



Flashbots 成立于 2020 年，是一家研发组织，旨在减轻最大可提取值 (MEV) 带来的负面外部性和生存风险。推出了 mev-geth、Flashbots Protect、MEV-Boost、MEV-Share、开放研究。

为 MEV 建立一个无需许可、透明且可持续的生态系统：

- 照亮：为 MEV 活动带来透明度。
- 民主化：使获取 MEV 收入的途径民主化。
- 分配：实现 MEV 收入的可持续分配。

1. Flashbots Protect：

- 提供抢先交易保护、交易回滚保护、可配置隐私和执行。
- 2023年7月升级，支持选择性交易共享。
- 自2021年10月起开源。

2. Flashbots MEV-Share 节点：

- 重新分配 MEV 给用户、交易发起人或其他目的地。
- 支持可编程隐私和mev_sendBundle标准。
- 自2023年7月起开源。

3. Flashbots Bundle Relay：

- 统一入口点，访问Flashbots Builders和MEV-Share节点。

4. Flashbots 生成器：

- 运行 MEV-Boost 区块生成器实例，最大化利润。
- 合并后2个月开源，2023年3月开源SGX飞地内的原型区块生成器。

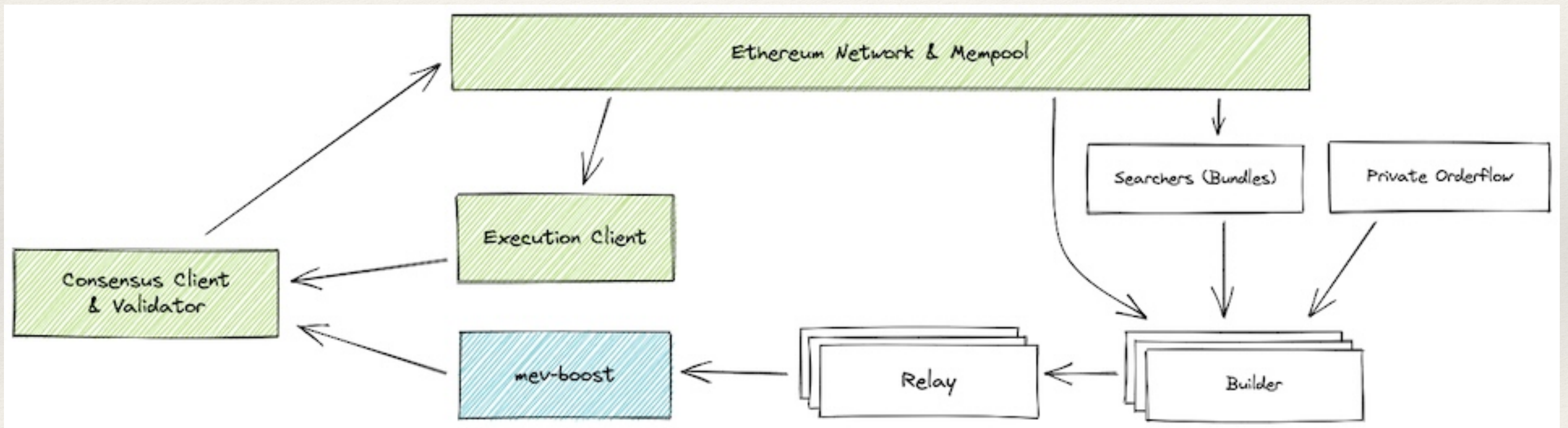
5. Flashbots MEV-Boost 中继：

- 提供数据可用性层和通信接口。
- 第一个运营的 MEV-Boost 中继，支持无权限提交区块出价。

MEV Boost

MEV 是以太坊上的一种中心化力量。无人看管的情况下，对 MEV 机会的竞争会导致共识不稳定，以及搜索者、区块生产者和验证者之间的许可通信基础设施。在 PoS 以太坊中，获取 MEV 的权利更为重要，因为计划中的区块补贴减少将使 MEV 在总质押收入中所占份额更大。


运行 MEV-Boost 的验证者通过向公开市场出售其区块空间来最大化其质押奖励。据估计，运行 MEV-Boost 的验证者可以将质押奖励提高 60% 以上。



现在，以太坊是 POS 质押伪随机轮流出块机制

如何保护Swap交易

<https://protect.flashbots.net/>



A safer way to transact on Ethereum

Use Flashbots Protect to protect yourself from frontrunning and earn refunds.

► Get protected

Transactions processed	Refunds earned
>7.2 million	>220 ETH

Flashbots Protect 具有以下主要优点：

- 高度可配置：自定义隐私、延迟和回扣回报偏好级别。
- 无抢先交易：交易对公共内存池是隐藏的，远离抢先交易和夹层机器人。
- 赚取退款：如果您的交易创建了 MEV，则通过 MEV-Share 赚取 MEV 退款。如果您的交易支付了高优先级费用，则赚取 gas 费用退款。
- 无失败交易：交易只有在不可撤销的情况下才会被纳入区块。用户无需为失败交易支付费用。

将交易发送给构建器时，相信他们不会抢先交易或将其泄露给第三方 MEV 搜索者

<https://docs.flashbots.net/flashbots-protect/quick-start>

如何捆绑交易

```
contract OpenspaceNFT is ERC721 {
    bool public isPresaleActive = true;

    function presale(uint256 amount) payable{
        require(isPresaleActive, "Presale is not active");
        require(amount* 0.01 ether==msg.value, "Invalid amount");
        require(amount+totalSupply()<=1024, "Not enough tokens left");

        _mint(msg.sender, amount);
    }

    function enablePresale() public onlyOwner {
        isPresaleActive = true;
    }
}
```

如何第一时间参与预售?

1. 选择RPC: relay.flashbots.net
2. Tx1:监听 MemPool 中的 enablePresale 交易
3. Tx2: 签名 presale(1024) 交易, 但不发送
4. 捆绑交易, 并发送

```
1  {
2    "jsonrpc": "2.0",
3    "id": 1,
4    "method": "eth_sendBundle",
5    "params": [
6      {
7        txs,           // Array[String], 一个要在原子捆绑包中执行的已签名交易列表。
8        blockNumber,   // String, 此捆绑包有效的十六进制编码区块号。
9        minTimestamp,  // (Optional) Number, 此捆绑包有效的最小时间戳, 自Unix纪元以来的秒数。
10       maxTimestamp,  // (Optional) Number, 此捆绑包有效的最大时间戳, 自Unix纪元以来的秒数。
11       revertingTxHashes, // (Optional) Array[String], 允许回滚的交易哈希列表。
12       replacementUuid, // (Optional) String, 可用于取消/替换此捆绑包的 UUID。
13       builders,       // (Optional) Array[String], 一个用于共享此捆绑包的已注册的区块构建者名称列表。
14     }
15   ]
16 }
```


作业说明

- ❖ 代码在自己的 github 提交
- ❖ 在 decert.me 提交领取证书
- ❖ **不可抄袭作业**，一经发现将不再检查抄袭者作业！

作业

- ❖ 使用你熟悉的语言，利用 flashbot eth_sendBundle 捆绑 OpenspaceNFT 的开启预售和参与预售的交易(sepolia 测试网络)，并使用 flashbots_getBundleStats 查询状态，最终打印交易哈希和 stats 信息

谢谢