MEV 与 FLASHBOT

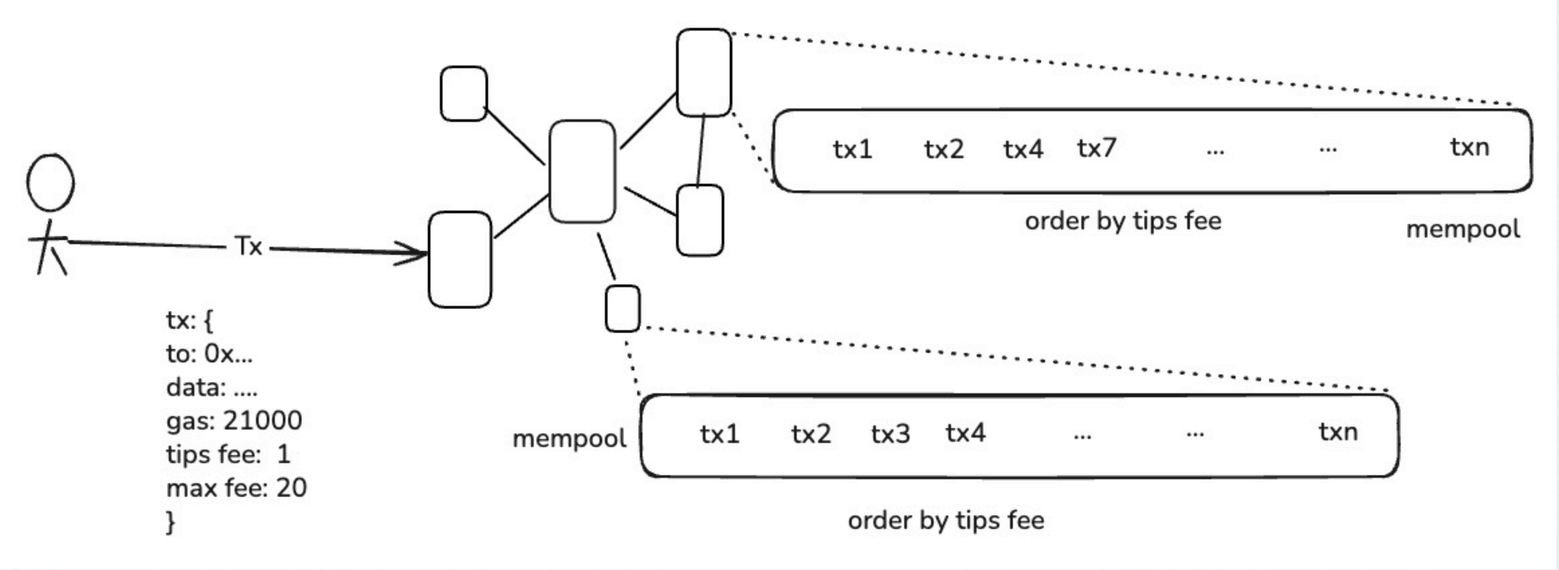
Tiny 熊

要点

- 回顾交易内存池 mempool
- MEV
- FlashBot

回顾 Mempool

- 交易打包之前（pending）会进入 mempool
- pending交易按 tips 费排序
- 节点之间会广播 mempool 的交易（节点有自己的mempool）
  - 用户可监听 mempool： eth_subscribe：newPendingTransactions
- 验证者从 mempool 挑选最有利可图的交易打包（按 Tips 排序 ）



MEV

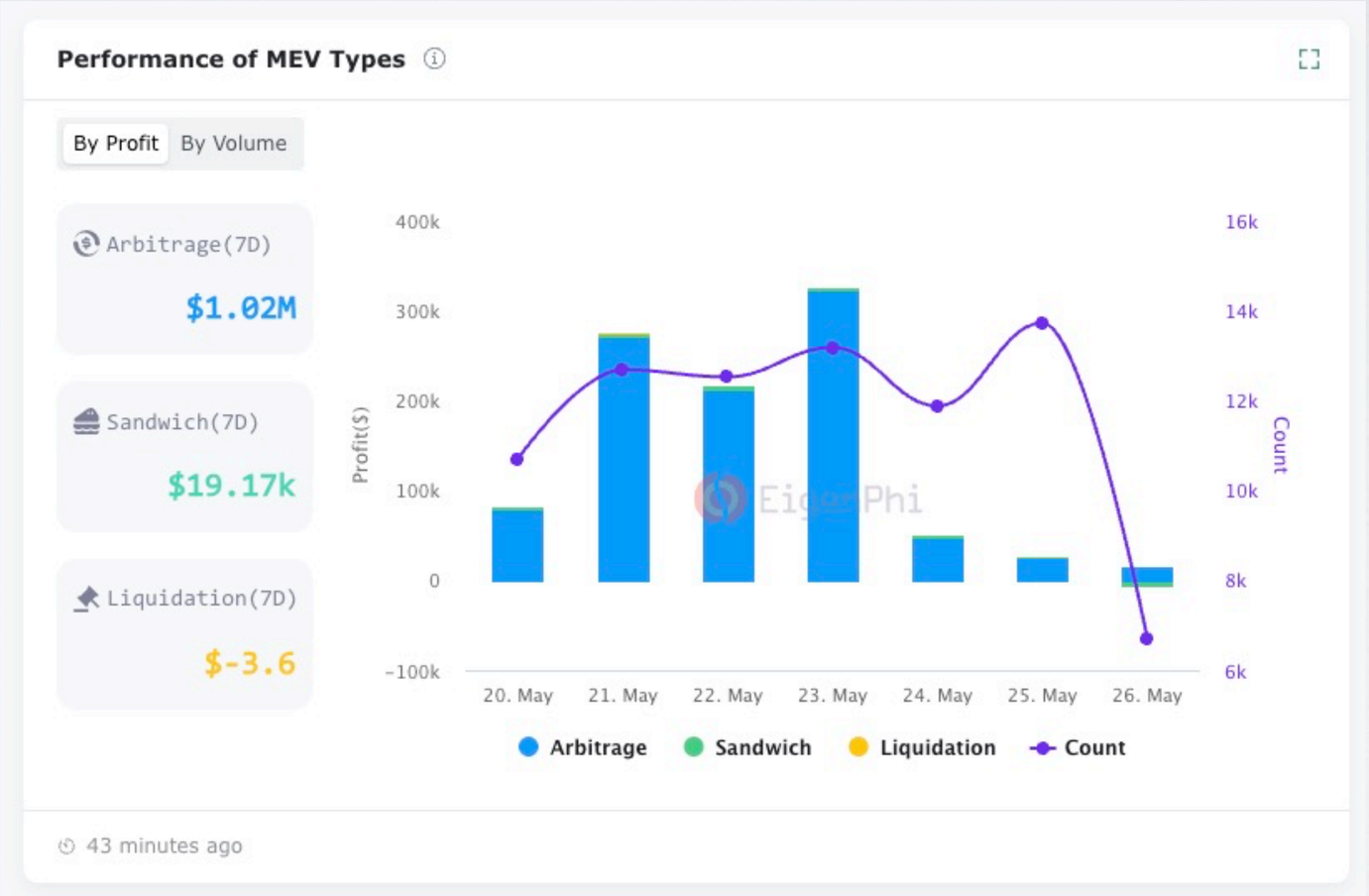
- MEV：Maximal（miner） Extractable Value 最大可提取价值，指的是矿工（验证者）通过对交易排序（或排除交易、额外添加交易）来提取最大可能的收益（除交易手续费之外）
- MEV 策略（或类型）有：
  - 抢跑交易(Front-running)：利用未确认交易的信息，提前进行相同交易以获取利润。（例如某些开奖奖励）
  - 尾随交易(back-running)：紧接在一个未确认的目标交易后面交易，（例如监听新的交易对创建）
  - 三明治攻击(Sandwich Attack)：在目标交易前后插入自己的交易，以操纵市场价格获取利润。
  - 套利(Arbitrage)：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。
  - 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。

以太坊是一个黑暗森林， 一旦暴露就会被打击
（也有针对 MEV 的陷阱）

MEV 利弊

- 利：
  - 帮助 DEFI， 如 及时清算、抹平 DEX 、EX 价差
  - 提升验证者收益
- 弊：
  - Gas 战争及 Gas 不稳定（尤其是提取者的竞争导致）
    - jaredfromsubway.eth 疯狂的时候，MEV 操作几乎覆盖每个区块
  - 对普通用户不公平（被夹、没机会抢购等）
  - 导致更多失败交易浪费链上空间

真实 MEV 获利情况



https://eigenphi.io/

MEV 套利案例

Transaction Description

May-26-2025 13:42:11 UTC

Arbitrage

3

USDC / USDT / WETH / ETH

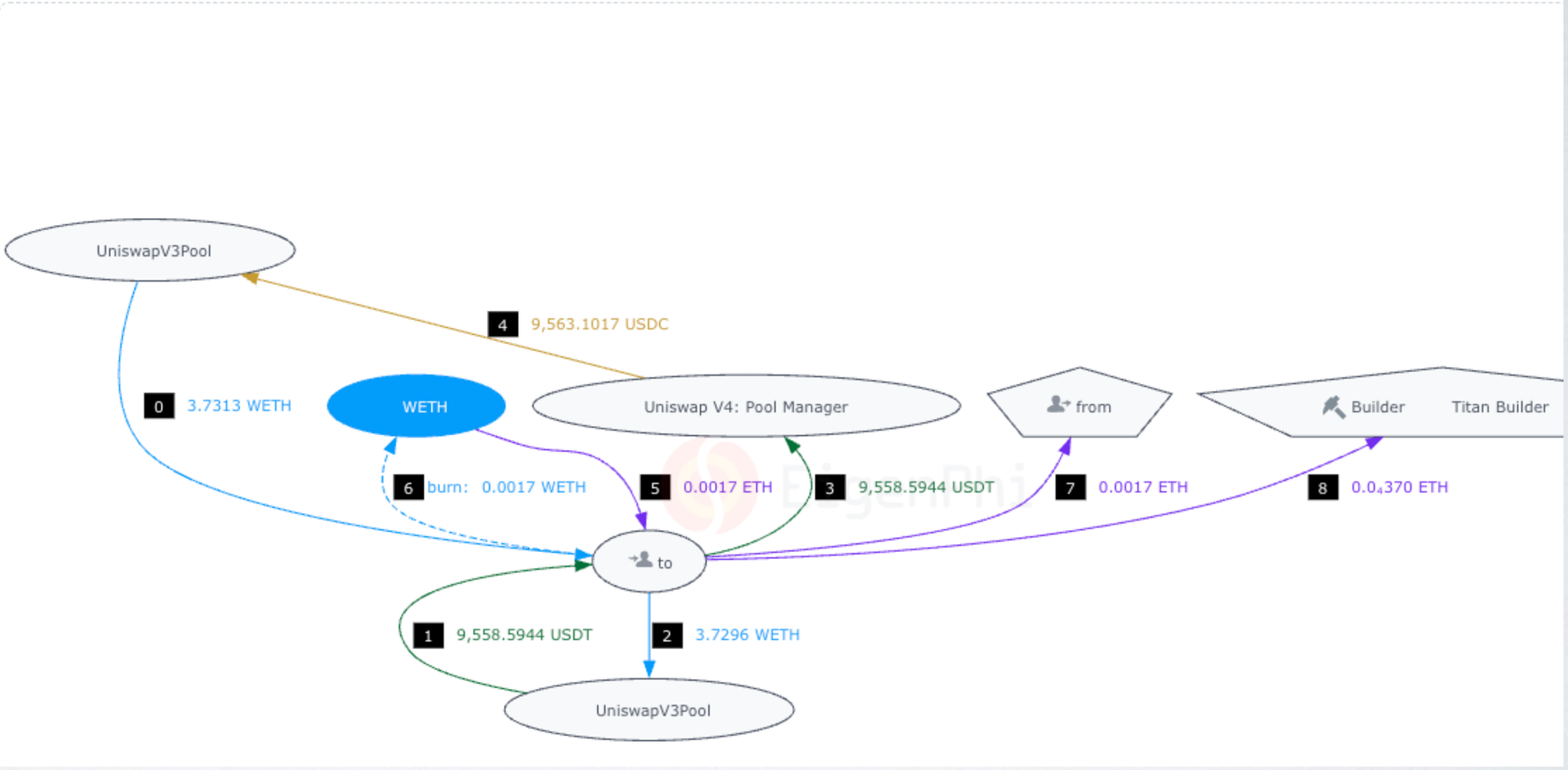
4 tokens swapped in 3 trading venues.

Profit	$3.10
Revenue	$4.46
Cost	$1.36

Token Flow

View Multi-Txs In One Chart

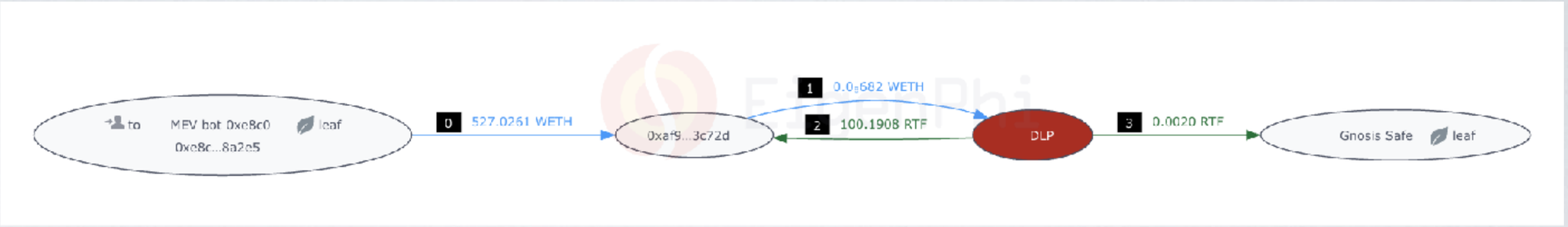
TB



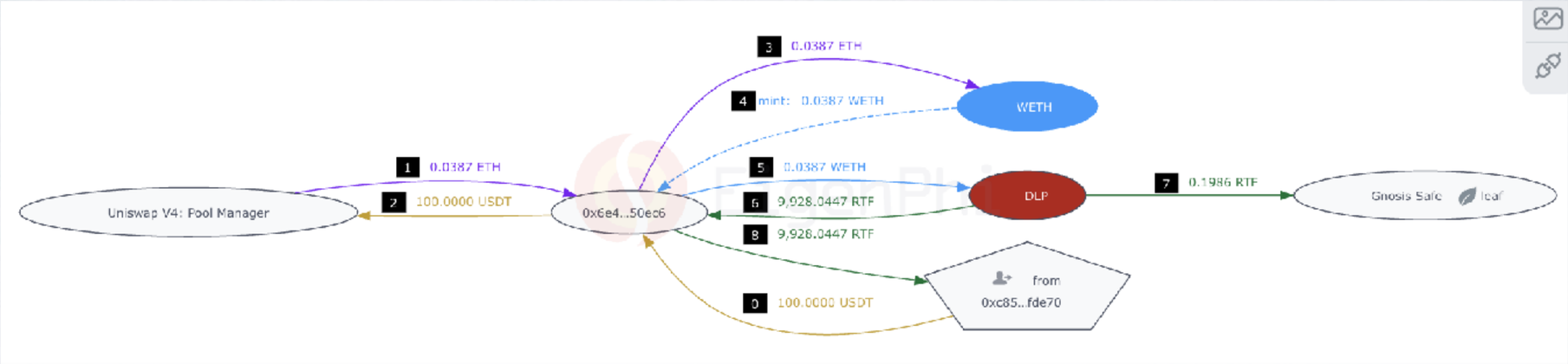
https://eigenphi.io/mev/ethereum/tx/0xd3fdec3185e58be74f6c2f035efc999a1ed84cd06c3b156e8193d7936ab416fb

三明治案例

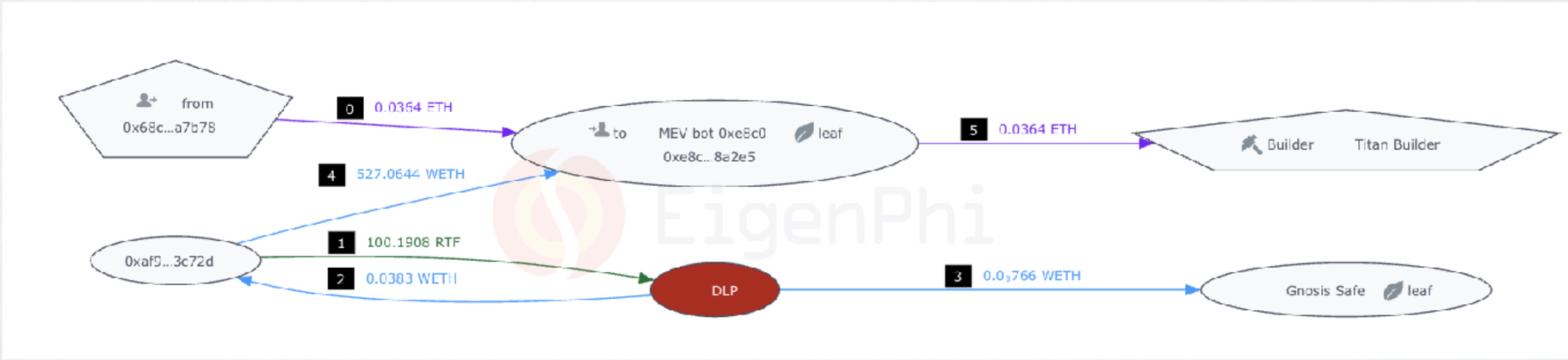
抢跑：
购买 RTF



受害者交易：
购买 RTF



尾随：
卖出RTF



https://eigenphi.io/mev/ethereum/tx/0x7ae27effe1c9c8a4e43411d5520002e25bdaa4b8d5511596756 0dc5da3b8b6e9

如何应对黑暗森林
(如何防范或提取套利)
Flashbots 诞生

Flashbots

- 在 POW 时期 矿工自己 MEV，POS 时期，验证者没有能力提取 MEV
- Flashbots 致力于研究与缓解以太坊 MEV 的研发组织（开始受以太坊资助，后独立融资），目标：
  - 透明化：构建透明的排序市场，不再是黑暗森林，量化影响，优化分配
  - 民主化： MEV 访问更加公平，开放所有人，充分竞争
  - 推动去中心化 PBS（排序权与出块权分离）

Flashbots

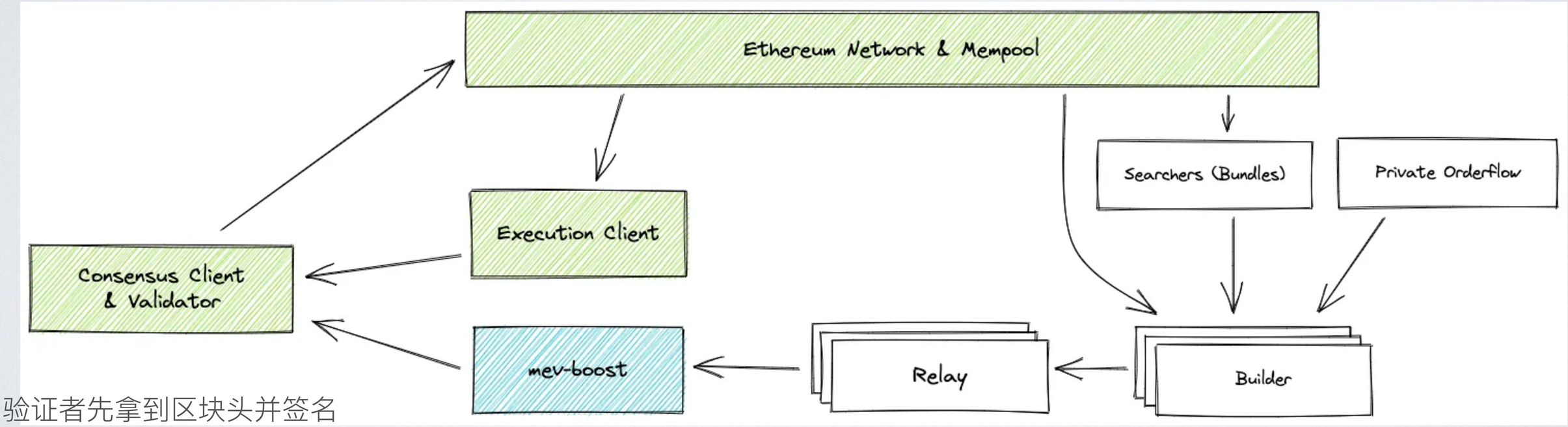
- Flashbots 主要的项目（或产品）：
  - **MEV-Boost**（含 relay）：开源中间件，配合共识层客户端，实现将区块构建工作外包给第三方 Builder
  - BuilderNet / rbuilder： 构建者开源实现及网络
  - Flashbots Protect：提供一个 RPC 端点（隐私节点），帮助用户避免被抢跑和三明治攻击。

通过 Flashbot 可实现

- 通过 Flashbot 在链外构建了一个交易排序市场，支持：
  - 发送隐私交易
  - 发送多个交易
  - 指定交易顺序
  - 指定成交区块/时间
  - 失败交易不上链

Mev–Boost 出块过程

- 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收益。
- MEV-boost 可以连接多个中继， 中继从多个构建者聚合区块，并识别出最有利可图的区块提交给区块提议者。



验证者先拿到区块头并签名
然后再拿到交易体

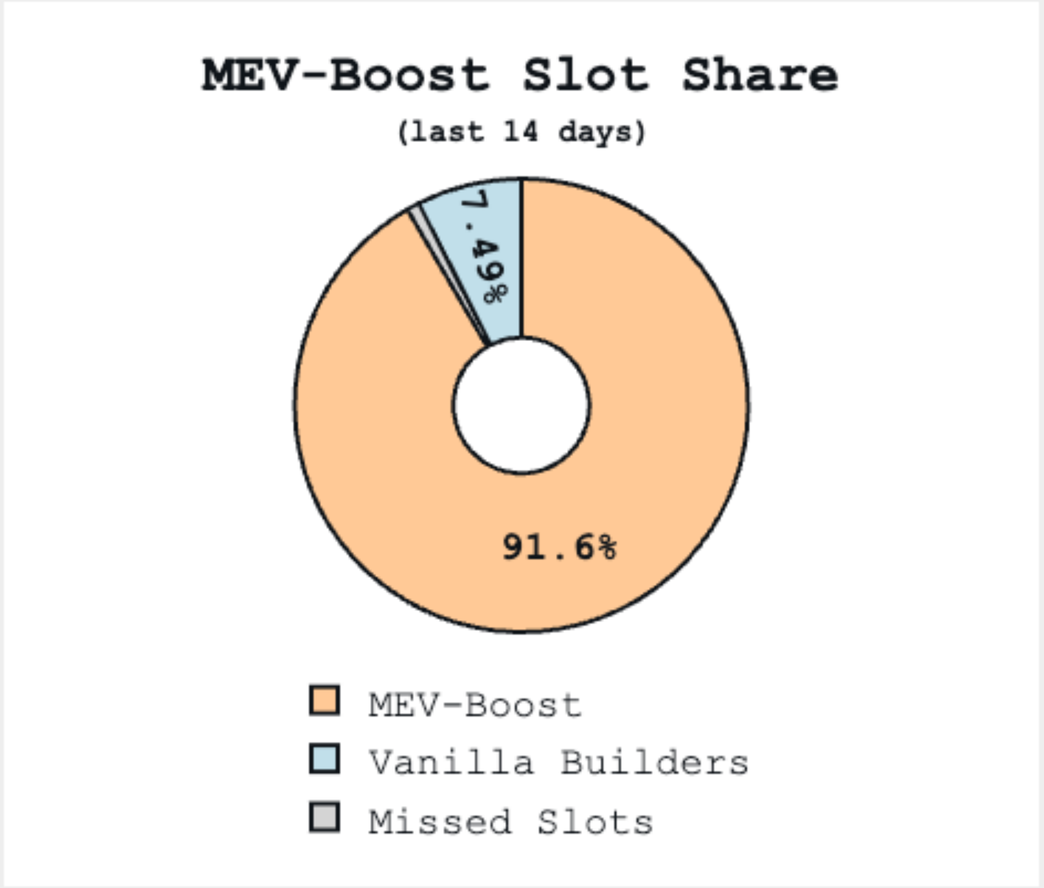
从 Relays 中从选最有利的

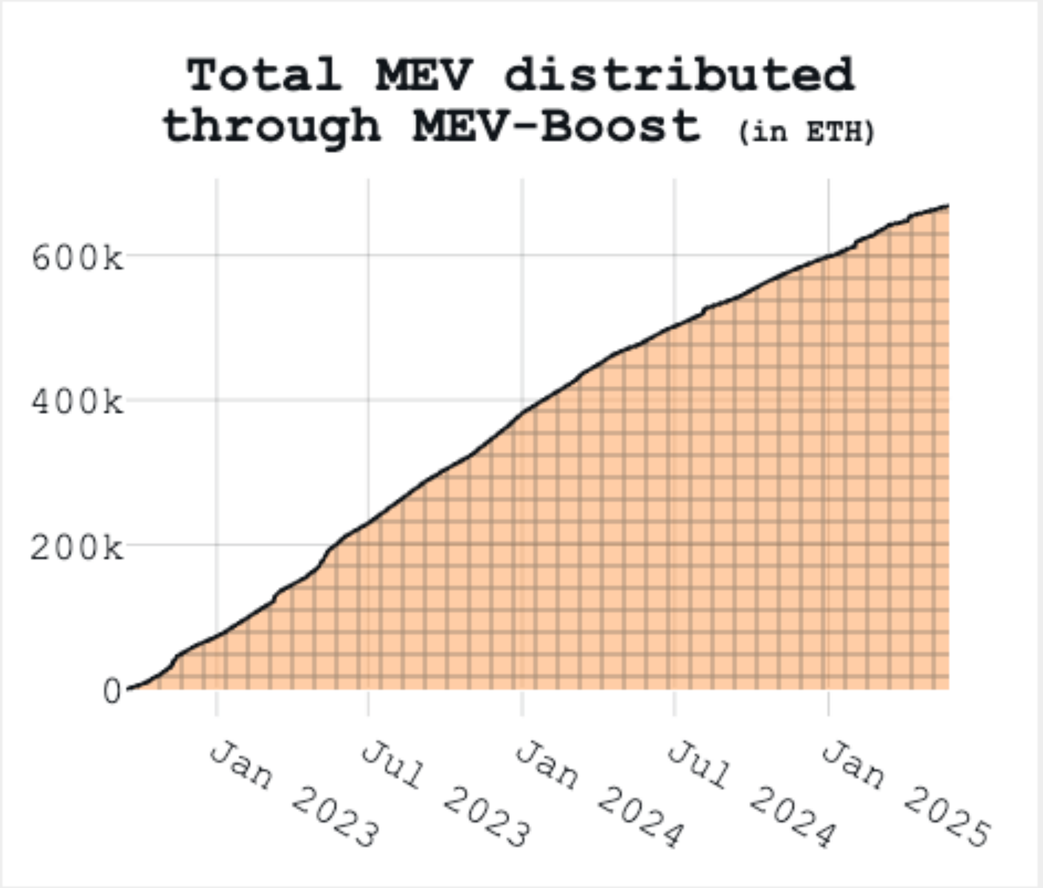
从 builders 从选最有利的

Mev-Boost 出块过程

- searcher（套利者）: 找到有利可图的 bundle ， 例如包含了套利的一批交易。
- searcher 将 bundle 交易发给 builder (可多个) - 隐私交易
- Builder 执行一系列的算法来决定一个区块中应该包含哪些 bundles 和交易来最大化区块的最大利润（Builder 还会接收自己的私有交易，及公开的内存池交易）
- Relayer 检查区块的有效性以及评估 builder打包的块的价值, 挑出价值最大的区块， 发给 mev-boost 。
  - 对比打包某一个区块前后 Buidler 余额差值
- mev-boost 选择谁有利的发给验证者
- 验证者打包区块

Builder


MEV-Boost Slot Share
(last 14 days)
7.49%
91.6%
MEV-Boost
Vanilla Builders
Missed Slots


Total MEV distributed through MEV-Boost (in ETH)
600k
400k
200k
0
Jan 2023
Jul 2023
Jan 2024
Jul 2024
Jan 2025

Builder

MEV-Boost Analytics

Updated at slot 11785299 (2 minutes ago)

Overview · Builder Profitability

7d · **24h** · 12h · 1h

Relay	Payloads	Percent
relay.ultrasound.money	3,638	44.26 %
bloxroute.max-profit.blxrbdn.com	1,850	22.51 %
bloxroute.regulated.blxrbdn.com	1,481	18.02 %
titanrelay.xyz	681	8.28 %
boost-relay.flashbots.net	350	4.26 %
agnostic-relay.net	117	1.42 %
aestus.live	103	1.25 %

Builder (extra_data)	Blocks	Percent
Titan (titanbuilder.xyz)	2,730	41.34 %
beaverbuild.org	2,254	34.13 %
BuilderNet	793	12.01 %
BuilderNet (Beaver)	467	7.07 %
BuilderNet (Flashbots)	180	2.73 %
BuilderNet (Nethermind)	146	2.21 %
rsync-builder.xyz	359	5.44 %
Quasar (quasar.win)	314	4.75 %
Builder+ www.btcs.com/builder	127	1.92 %
bobTheBuilder.xyz	14	0.21 %
https://blockbeelder.com	5	0.08 %
BuildAI (https://buildai.net)	3	0.05 %
Powered by bloXroute	1	0.02 %

各自的隐私网络

https://www.relayscan.io/

如何利用 Flashbot

- 选择一个支持隐私节点 RPC （通常由 Builders 提供）
  - titanbuilder.xyz/ 、Flashbots Protect 、beaverbuild 、bloxroute… 列表
  - 支持额外的 RPC 接口： eth_sendBundle 、mev_sendBundle、eth_sendPrivateTransaction（或 eth_sendRawTransaction 自动支持隐私）
- 构建多个交易，打包发送
  - block.coinbase.transfer(msg.value) 或 提高 gas 以便 Builders 打包

```
{
  "jsonrpc": "2.0",
  "id": 1,
  "method": "eth_sendBundle",
  "params": [
    {
      txs,                // Array[String], 一个要在原子捆绑包中执行的已签名交易列表。
      blockNumber,        // String, 此捆绑包有效的十六进制编码区块号。
      minTimestamp,       // (Optional) Number, 此捆绑包有效的最小时间戳, 自Unix纪元以来的秒数。
      maxTimestamp,       // (Optional) Number, 此捆绑包有效的最大时间戳, 自Unix纪元以来的秒数。
      revertingTxHashes,  // (Optional) Array[String], 允许回滚的交易哈希列表。
      replacementUuid,    // (Optional) String, 可用于取消/替换此捆绑包的 UUID。
      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。
    }
  ]
}
```

捆绑交易场景

- 防止交易在 mempool 被攻击
- MEV，例如监听 mempool 的交易（套利、抢购）
- 拯救被恶意监控钱包的资产
- 减少交易失败带来的损失

```
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

捆绑交易场景

```
nonce = w3.eth.get_transaction_count(sender.address)
tx1 = create_transaction(w3, sender.address, receiver, nonce, network)
tx2 = create_transaction(w3, sender.address, receiver, nonce + 1, network)

tx1_signed = w3.eth.account.sign_transaction(tx1, private_key=sender.key)
bundle = [
{"signed_transaction": tx1_signed.rawTransaction},
{"transaction": tx2, "signer": sender},
]

send_result = w3.flashbots.send_bundle(
    bundle,
    target_block_number=block + 1,
    opts={"replacementUuid": str(uuid4())},
)
logger.info(f"bundleHash {w3.to_hex(send_result.bundle_hash())}")

stats_v1 = w3.flashbots.get_bundle_stats(
    w3.to_hex(send_result.bundle_hash()), block
)
logger.info(f"bundleStats v1 {stats_v1}”)
```

https://github.com/flashbots/web3-flashbots/blob/master/examples/simple.py

https://docs.flashbots.net/flashbots-auction/libraries/bundle-relay

练习题

- 利用 FlashBots 捆绑交易
  - 利用 flashbot API eth_sendBundle 捆绑 OpenspaceNFT 的开启预售和 presale 交易

https://decert.me/quests/70957dea-e3de-4b45-82c2-5c105c56c4ae