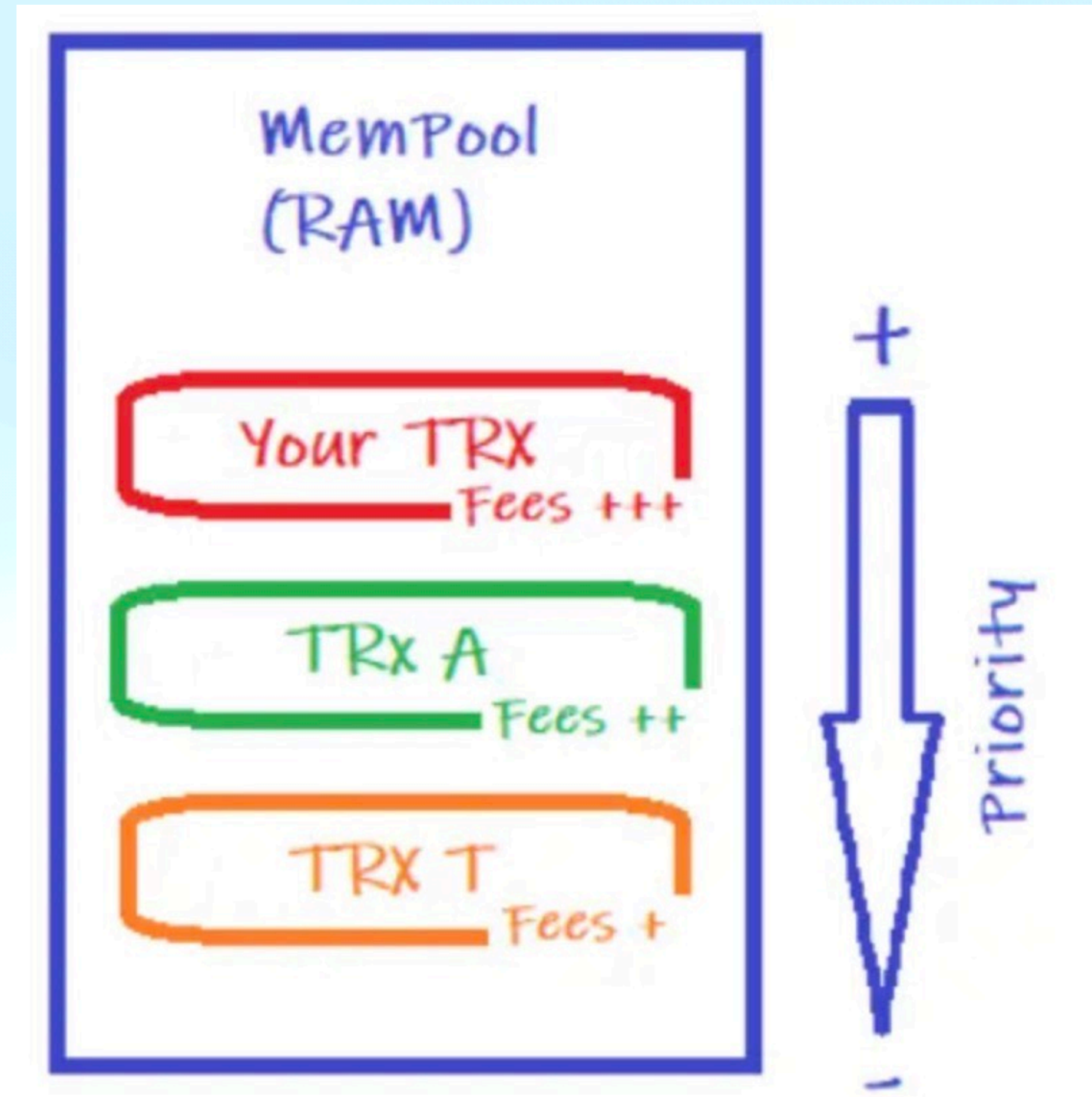


flashbots隐私节点的运用

write and speak by 33357

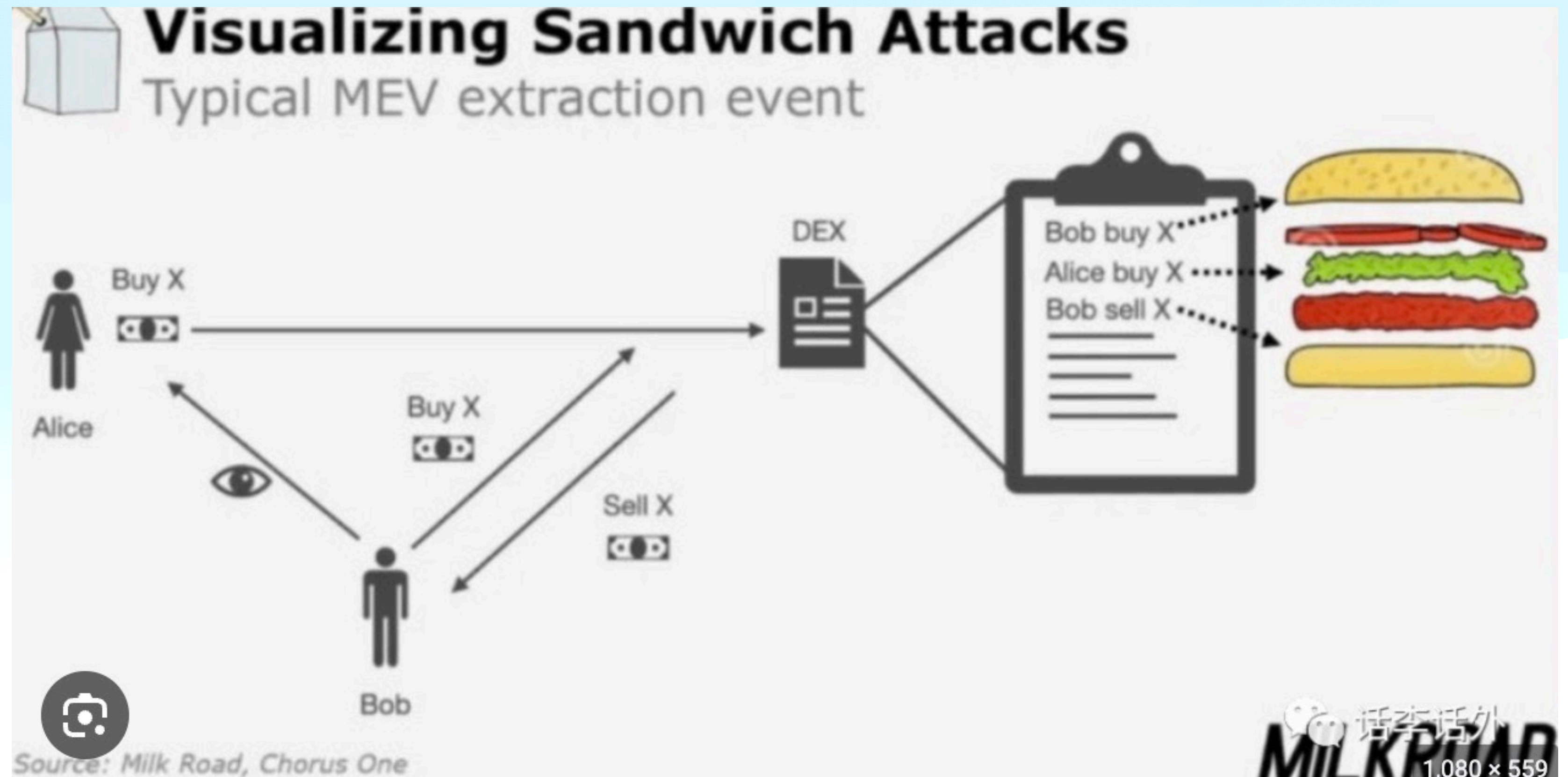
mempool的功能

- 筛选交易进入pending阶段
- pending交易按gasprice进行排序
- 广播pending交易
- 提供pending交易给矿工打包



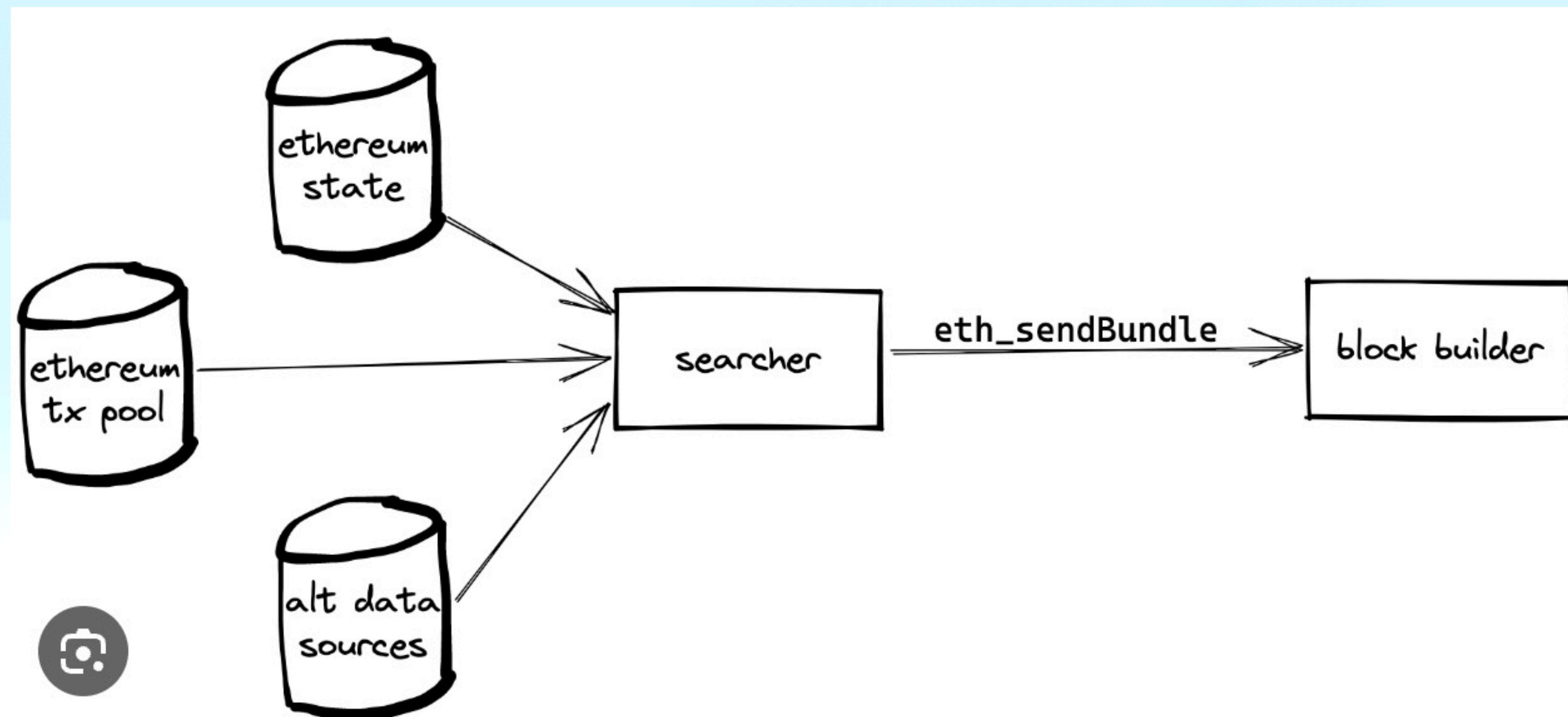
mempool引发的攻击

- 交易抢跑
- 交易跟随
- 三明治交易



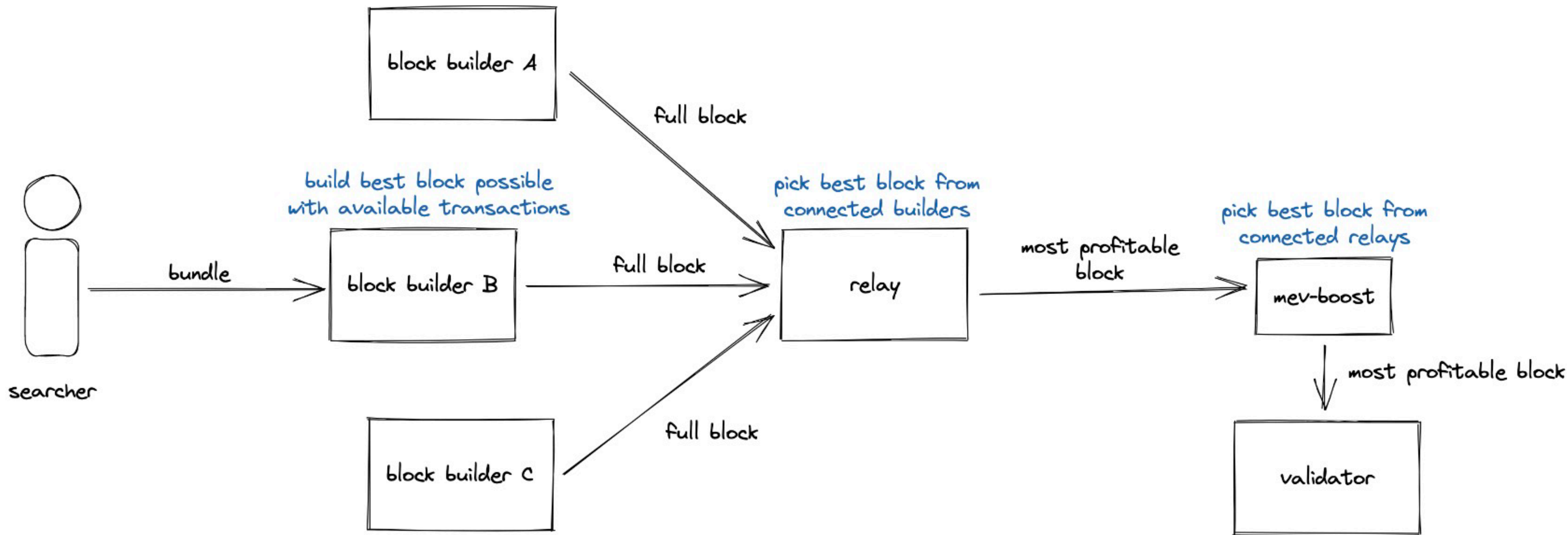
flashbots的功能

- 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
- 撤回失败交易



flashbots的结构

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



隐私节点接口

<https://beaverbuild.org/docs.html>

RPC docs

Beaver doesn't care about your authentication headers and signatures.

eth_sendRawTransaction

Sends a transaction to beaver. The transaction will stay private.

Also supported under the name: `eth_sendPrivateRawTransaction` (exact same RPC).

This RPC accepts a single argument: the hex-encoded, raw transaction.

隐私节点接口

`eth_sendBundle`

Sends a bundle to beaver. It will stay private.

This RPC accepts a dictionary of:

`txs`

List of hex-encoded, raw transactions. Can be empty for cancelling a bundle.

`blockNumber`

The block that this bundle will be valid for.

`minTimestamp`

Optional. If specified and >0 , the bundle will only be valid if the block timestamp is greater or equal to `minTimestamp`.

`maxTimestamp`

Optional. If specified and >0 , the bundle will only be valid if the block timestamp is smaller or equal to `maxTimestamp`.

`revertingTxHashes`

Optional. A list of transaction hashes contained in the bundle, that can be allowed to revert, or be removed from your bundle if it's deemed useful.

`uuid`

Optional. An arbitrary string (make it hard to predict!), which allows you to update/cancel your bundles: if you specify an `uuid` and we already have a bundle with an identical one, we'll forget about the old bundle. So we can only have a single bundle with a certain `uuid` at all time (and we keep the most recent).

`replacementUuid`

Optional, deprecated, alias for `uuid`.

`refundPercent`

Optional. An integer between 1–99. How much of the total priority fee + coinbase payment you want to be refunded for. This will negatively impact your prioritization because this refund is gonna eat into your bundle payment. Example: if a bundle pays 0.2 ETH of priority fee plus 1 ETH to coinbase, a `refundPercent` set to 50 will result in a transaction being appended after the bundle, paying 0.59 ETH back to the EOA. This is assuming the payout tx will cost beaver 0.01 ETH in fees, which are deduced from the 0.6 ETH payout.

`refundRecipient`

Optional. You can specify an address that the funds from `refundPercent` will be sent to. If not specified, they will be sent to the `from` address of the first transaction.

Bundle cancellation: Say that you sent a bundle with `uuid` "10ba43b9c689ed0242b3". If you want to cancel it entirely, you can send a bundle with the same `uuid`, and an empty list of transactions.

隐私节点的使用场景

- 防止交易在mempool被攻击
- 攻击mempool的交易
- 拯救被恶意监控钱包的资产
- 减少交易失败带来的损失



粉丝发在微博的感谢信
感谢认可，我继续努力 🙏



微博正文



阿水愉快的度过了她的23岁

+关注

24-3-3 01:28 来自 微博轻享版
发布于 广东

Blast上项目好多，质押的号之前被盗了，都不想接着玩了
😭。

找科学家AA取回质押的以太，u本位没亏😭还承诺后续的空投也帮我抢，本以为我这个小韭菜是没希望被搭理的，找回资产真的是中彩票般开心。

再次感谢🙏科学家@0xAA科学家，技术没有被用来做恶，还能帮助别人，这才是币圈的(3,3) 🍏🍏

隐私节点市场份额

<https://www.rated.network/builders>

ENTITY	BLOCKS	MARKET SHARE	RELAY DISTRIBUTION	AVG TXS INCLUDED	EXCLUSIVE ORDER FLOW %	MEDIAN BLOCK VALUE (IN ETH)
Beaverbuild	2,888	43.34%		155		0.0851
Titan Builder	1,736	26.05%		178		0.0618
Rsync	1,382	20.74%		179		0.0835
Flashbots	158	2.37%		169		0.071
jetblidr.xyz	130	1.95%		180		0.0431
rpc.tbuilder.xyz	101	1.52%		151		0.0328
f1b.io	92	1.38%		158		0.0428
Builder 0x69	39	0.59%		160		0.0678

隐私节点使用案例

```
async function sendAll(sign: string, targetBlockNumber: number) {
  providerUrlList.forEach(async (providerUrl) => {
    sendProviderUrl(providerUrl, sign, targetBlockNumber);
  });
  sendFlashbots([sign], targetBlockNumber);
  log(`sendAll, targetBlockNumber: ${targetBlockNumber}`);
}
```

```
async function sendProviderUrl(providerUrl: string, sign: string, targetBlockNumber: number) {
  try {
    await axios.post(providerUrl, {
      jsonrpc: '2.0',
      id: 1,
      method: 'eth_sendBundle',
      params: [{ txs: [sign], blockNumber: `0x${targetBlockNumber.toString(16)}` }],
    });
  } catch (error) {
    log(`sendProviderUrl ${providerUrl} ${error}`);
  }
}
```

flashbot节点使用案例

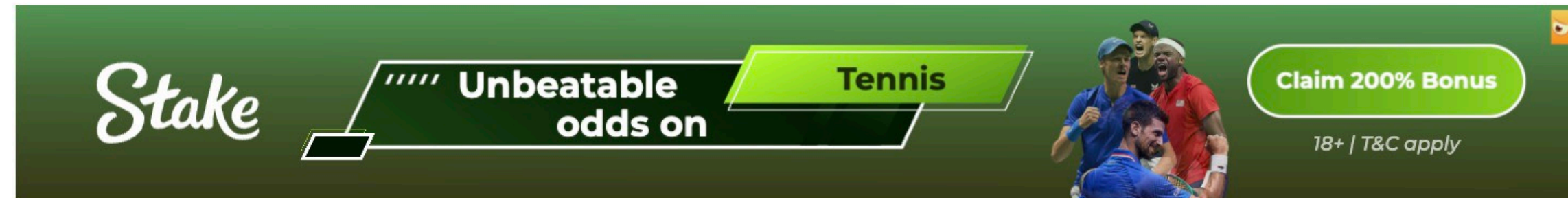
```
async function sendFlashbots(signedBundle: string[], targetBlockNumber: number) {
  try {
    const flashbotsProvider = await FlashbotsBundleProvider.create(provider, wallet);
    const bundleReceipt = (await flashbotsProvider.sendRawBundle(signedBundle,
      targetBlockNumber)) as FlashbotsTransactionResponse;
    log(`send flashbots, targetBlockNumber: ${targetBlockNumber}`);
    const res = await bundleReceipt.wait();
    if (res == 1) {
      log(`useFlashBot ${targetBlockNumber} Revert`);
    } else {
      log(`useFlashBot ${targetBlockNumber} Success`);
    }
  } catch (error) {
    log(`send flashbots ${error}`);
  }
}
```

Dex套利交易

Transaction Action:

- ▶ Swap 0.08588683038866112 ETH For 8,775,822.161147301904515072 FINALE On Uniswap V2
- ▶ Swap 8,775,822.161147301904515072 FINALE For 4,073,001.819911515220568478 LOYAL On Uniswap V3
- ▶ Swap 4,073,001.004125515375228678 LOYAL For 0.089119425398319744 ETH On Uniswap V3

Sponsored:



From:

0x76F36d497b51e48A288f03b4C1d7461e92247d5e

Interacted With (To):

0x2d2A7d56...039447B4D

The net movement of tokens (whether sent or received) per address involved in this transaction

ERC-20 Tokens Transferred: 4

All Transfers Net Transfers

- ▶ From Uniswap V3: LOYAL 9 To 0x2d2A7d56...039447B4D For 0.089119425398319744 (\$300.25) Wrapped Ethe... (WETH)
- ▶ From 0x2d2A7d56...039447B4D To Uniswap V2: FINALE 3 For 0.08588683038866112 (\$289.36) Wrapped Ethe... (WETH)
- ▶ From Uniswap V3: LOYAL-FINALE To Uniswap V3: LOYAL 9 For 4,073,001.819911515220568478 Loyalty Labs (LOYAL)
- ▶ From Uniswap V2: FINALE 3 To Uniswap V3: LOYAL-FINALE For 8,775,822.161147301904515072 Bens Finale (FINALE)

Value:

0 ETH (\$0.00)

Transaction Fee:

0.003190571274444204 ETH \$10.75

Gas Price:

15.549502283 Gwei (0.000000015549502283 ETH)

flashbot explore

https://flashbots-explorer.marto.lol

Bundles in #19339334

Hash	From	To	Assets	Gas used	Gas price	Coinbase transfer	Miner reward
0xac8c91a2a...	0x91e0...3924E1	0xF3dE...509127	USDT 693.39 WETH 0.20 (\$685.37)	207061	25 gwei	≡ 0.0000	≡ 0.0052
#1				207061		≡ 0.0000	≡ 0.0052
0xb7f432d05...	0x5CC2...85B9C1	0xF3dE...509127	WETH 0.20 (\$685.37)	169325	22 gwei	≡ 0.0000	≡ 0.0037
0x89c5d0bd...	0x2001...a7da4A	0x7D23...3B69A5		30974	17 gwei	≡ 0.0000	≡ 0.0005
0x483b50ab...	0x75e8...1dcB88	0xC759...4BCfb2		21000	17 gwei	≡ 0.0000	≡ 0.0004
0xafb18d3d9...	0x75e8...1dcB88	0xB332...1aec4e		21000	17 gwei	≡ 0.0000	≡ 0.0004
0xef0ae472c...	0x75e8...1dcB88	0xC1a3...0DE481		21000	17 gwei	≡ 0.0000	≡ 0.0004
0x5e056162...	0x75e8...1dcB88	0xdAC1...831ec7	USDT 4000.00	46097	17 gwei	≡ 0.0000	≡ 0.0008
0x95b3f97e7...	0x75e8...1dcB88	0x3f7F...571eb5		21000	17 gwei	≡ 0.0000	≡ 0.0004
0xacb2ee67a...	0x75e8...1dcB88	0x4677...a5E5f3		51559	17 gwei	≡ 0.0000	≡ 0.0009
0xf68e47975...	0x75e8...1dcB88	0x4f2d...Da2dF1		21000	17 gwei	≡ 0.0000	≡ 0.0004

回购抢跑

https://etherscan.io/address/0x410e10C33a49279f78CB99c8d816F18D5e7D5404

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x4368b174ef3...	Buyn Burn	19359850	18 mins ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01017741
0xb9fdc69fae1...	Buyn Burn	19359550	1 hr ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.0101765
0x71b137478b...	Buyn Burn	19359249	2 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0x4e7f207d1b5...	Buyn Burn	19358950	3 hrs ago	0x00B700B9...251002aF3	IN 0x410e10C3...D5e7D5404	0 ETH	0.0109835
0xb613ecabdd...	Buyn Burn	19358650	4 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0x5e82da6c46...	Buyn Burn	19358355	5 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0xb8fb54e51a0...	Buyn Burn	19358054	6 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0x82b3be5d64...	Buyn Burn	19357754	7 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0xf8644b21ef6...	Buyn Burn	19357442	8 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0x8ee1dc91d4...	Buyn Burn	19357141	9 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399
0x1d577bc30a...	Buyn Burn	19356843	10 hrs ago	0xca29358a...23A3eE4a7	IN 0x410e10C3...D5e7D5404	0 ETH	0.01098399

From: [0xca29358a0BBF2F1D6ae0911C3bC839623A3eE4a7](#)

Interacted With (To): [0x410e10C33a49279f78CB99c8d816F18D5e7D5404](#)

Transfer 0.010989 ETH From [Wrapped Ether](#) To [0x410e10C3...D5e7D5404](#)

Transfer 0.010989 ETH From [0x410e10C3...D5e7D5404](#) To [0xca29358a...23A3eE4a7](#)

ERC-20 Tokens Transferred: 3

All Transfers Net Transfers

From [Uniswap V3: TITANX](#) To [0x410e10C3...D5e7D5404](#) For 17,011,618,306.059065991145625626 (\$11,654.68) [TITAN X \(TITANX\)](#)

From [0x410e10C3...D5e7D5404](#) To [Uniswap V3: TITANX](#) For 3.319011 (\$11,516.41) [Wrapped Ethe... \(WETH\)](#)

From [0x410e10C3...D5e7D5404](#) To [Null: 0x000...000](#) For 17,011,618,306.059065991145625626 (\$11,654.68) [TITAN X \(TITANX\)](#)

Value: 0 ETH (\$0.00)

Transaction Fee: 0.010177412025 ETH (\$35.31)

Gas Price: 48.001 Gwei (0.000000048001 ETH)

Gas Limit & Usage by Txn: 333,333 | 212,025 (63.61%)

Gas Fees: Base: 46.336156443 Gwei | Max: 48.001 Gwei | Max Priority: 48.001 Gwei

Burnt & Txn Savings Fees: Burnt: 0.009824423569827075 ETH (\$34.09) Txn Savings: 0 ETH (\$0.00)

Other Attributes: Txn Type: 2 (EIP-1559) Nonce: 14469 Position In Block: 34

Input Data: Function: `buynBurn()`

防打废

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0xb521d08b52...	Set Approval ...	19359988	24 secs ago	0x72e156E4...e08D068EB	0x42537d4E...e569d9e9D	0 ETH	0.00298356
0xa3a8a48911...	Set Approval ...	19359988	24 secs ago	0x8BB6784F...FcD549D55	0x42537d4E...e569d9e9D	0 ETH	0.00298449
0xc1dede5660...	Set Approval ...	19359987	36 secs ago	masamii.eth	0x42537d4E...e569d9e9D	0 ETH	0.0028958
0x6079d25b93f...	Set Approval ...	19359987	36 secs ago	0xa8a54e27...Aa510570c	0x42537d4E...e569d9e9D	0 ETH	0.00291795
0x6b2397eca5...	Mint	19359987	36 secs ago	0xe1fB8486...F26627c65	0x42537d4E...e569d9e9D	0 ETH	0.00205867
0xae1b39b937f...	Mint	19359986	1 min ago	0x64A19966...2d0Cc90F6	0x42537d4E...e569d9e9D	0 ETH	0.00172121
0xa958c0bfc01...	Mint	19359986	1 min ago	0xA2E74D33...B6a2b4AAB	0x42537d4E...e569d9e9D	0 ETH	0.00172121
0x8034ecc284...	Mint	19359986	1 min ago	0x4DD85925...7114c90E2	0x42537d4E...e569d9e9D	0 ETH	0.00172121
0x81ae33bf09b...	Mint	19359986	1 min ago	0xbea3BaE5...7325ba951	0x42537d4E...e569d9e9D	0 ETH	0.00172176
0x58cda24cf36...	Mint	19359986	1 min ago	0xbea3BaE5...7325ba951	0x42537d4E...e569d9e9D	0 ETH	0.00172176
0xfceed5a9360...	Mint	19359986	1 min ago	0xAd1Cc057...f019893fD	0x42537d4E...e569d9e9D	0 ETH	0.00172178
0x2e1dfc1171b...	Mint	19359986	1 min ago	0x408056C7...Fa26DB4f5	0x42537d4E...e569d9e9D	0 ETH	0.00172178
0xb5db541ec3...	Set Approval ...	19359986	1 min ago	ieatvegetables.eth	0x42537d4E...e569d9e9D	0 ETH	0.00283492
0xb44d5acfaae...	Set Approval ...	19359985	1 min ago	0x329479e0...a89123456	0x42537d4E...e569d9e9D	0 ETH	0.00310226

谢谢观看

<https://learnblockchain.cn/people/3877>

