DRK Lab Web3青年学者计划

MEV黑暗森林：量化区块链可提取价值

Kaihua Qin

Phd Student@Imperial College London
Co-founder@d23e.ch

区块链可提取价值

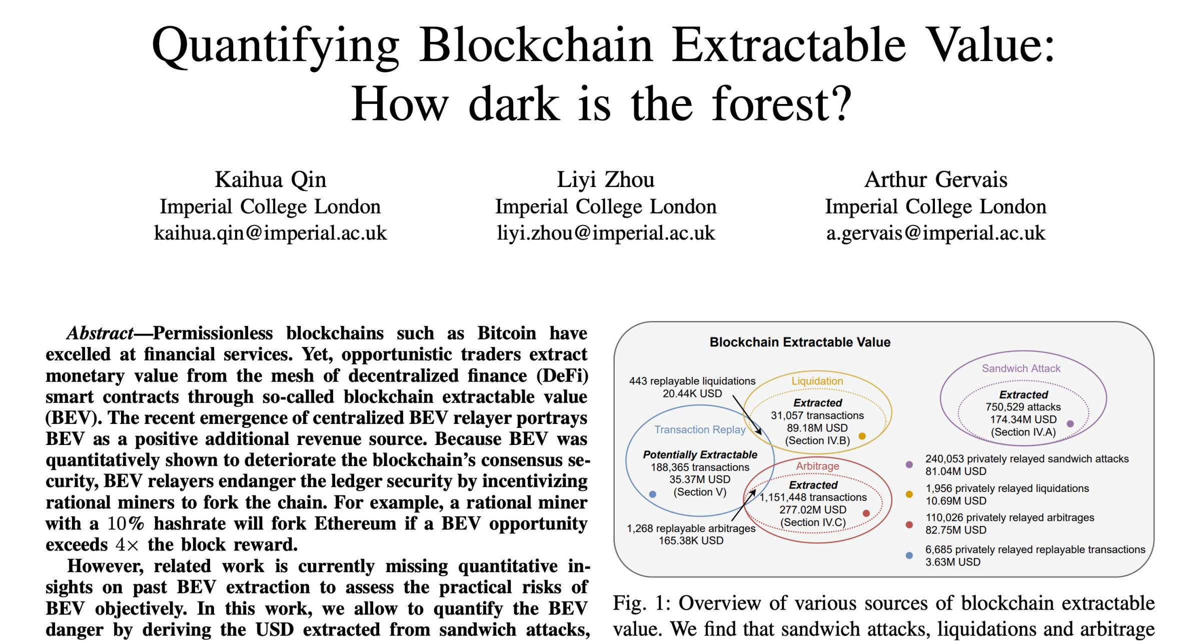
Miner/Maximal Extractable Value (MEV)

Blockchain Extractable Value (BEV)

昨天

今天

明天



Quantifying Blockchain Extractable Value: How dark is the forest?

Kaihua Qin
Imperial College London
kaihua.qin@imperial.ac.uk

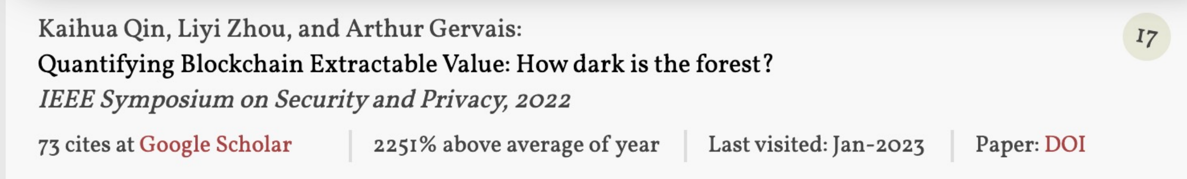
Liyi Zhou
Imperial College London
liyi.zhou@imperial.ac.uk

Arthur Gervais
Imperial College London
a.gervais@imperial.ac.uk

***Abstract*—Permissionless blockchains such as Bitcoin have excelled at financial services. Yet, opportunistic traders extract monetary value from the mesh of decentralized finance (DeFi) smart contracts through so-called blockchain extractable value (BEV). The recent emergence of centralized BEV relayer portrays BEV as a positive additional revenue source. Because BEV was quantitatively shown to deteriorate the blockchain's consensus security, BEV relayers endanger the ledger security by incentivizing rational miners to fork the chain. For example, a rational miner with a 10% hashrate will fork Ethereum if a BEV opportunity exceeds 4× the block reward.**

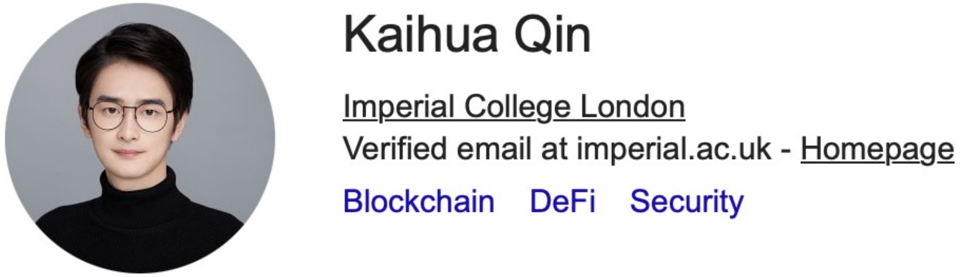
However, related work is currently missing quantitative insights on past BEV extraction to assess the practical risks of BEV objectively. In this work, we allow to quantify the BEV danger by deriving the USD extracted from sandwich attacks,

Fig. 1: Overview of various sources of blockchain extractable value. We find that sandwich attacks, liquidations and arbitrage



Kaihua Qin, Liyi Zhou, and Arthur Gervais:
Quantifying Blockchain Extractable Value: How dark is the forest?
IEEE Symposium on Security and Privacy, 2022

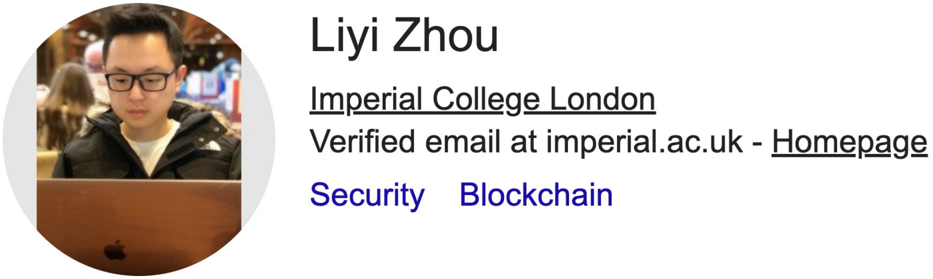
73 cites at Google Scholar | 2251% above average of year | Last visited: Jan-2023 | Paper: DOI



Kaihua Qin

Imperial College London
Verified email at imperial.ac.uk - Homepage

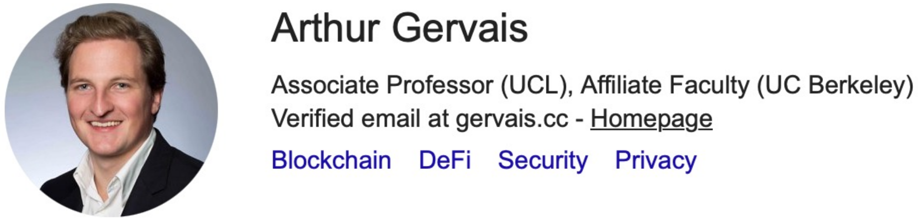
Blockchain DeFi Security



Liyi Zhou

Imperial College London
Verified email at imperial.ac.uk - Homepage

Security Blockchain



Arthur Gervais

Associate Professor (UCL), Affiliate Faculty (UC Berkeley)
Verified email at gervais.cc - Homepage

Blockchain DeFi Security Privacy

MEV

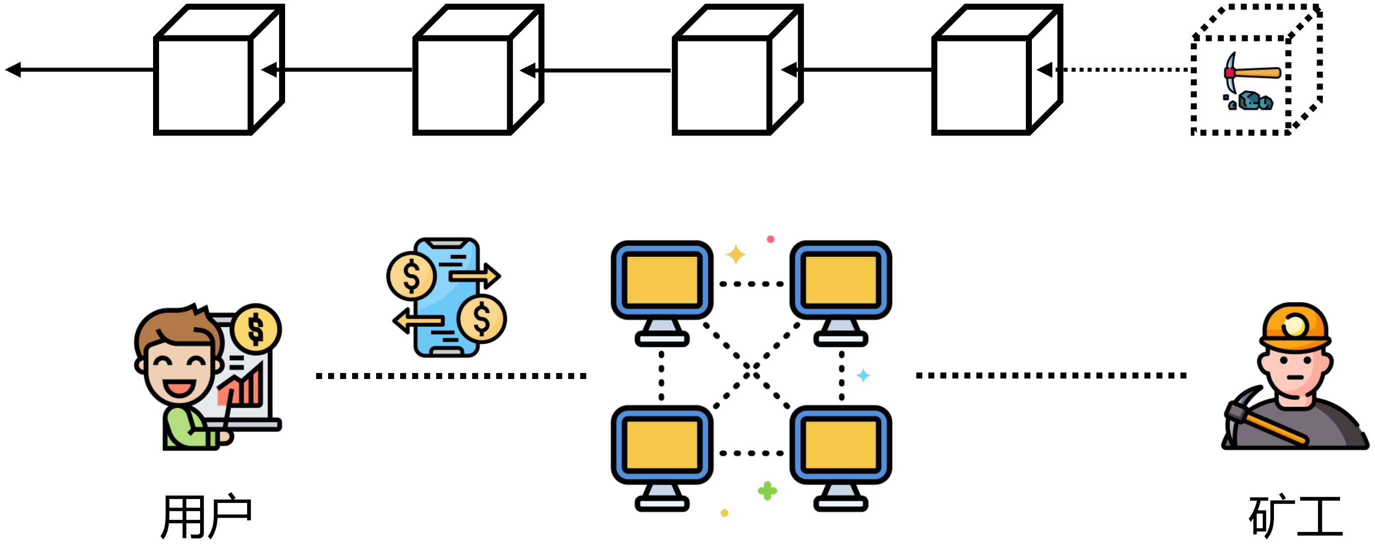
昨天

- Proof-of-work
- Peer-to-peer network
- Front-running as a service

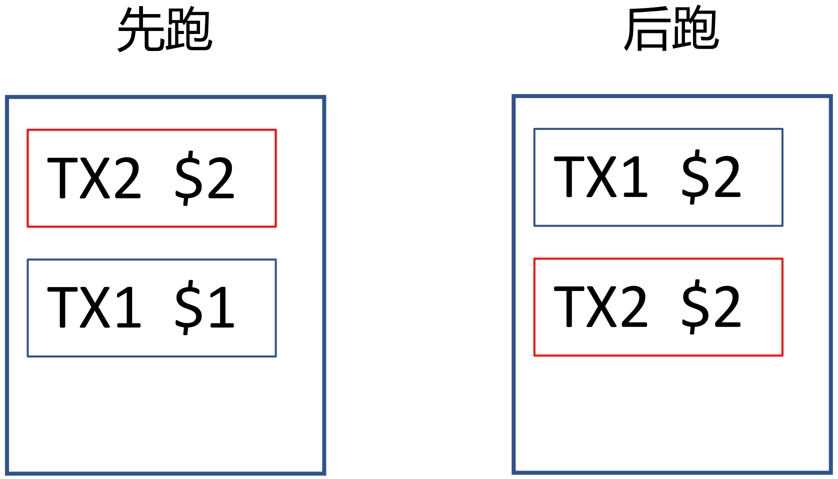
今天

明天

系统模型



交易执行顺序



先跑

TX2 $2

TX1 $1

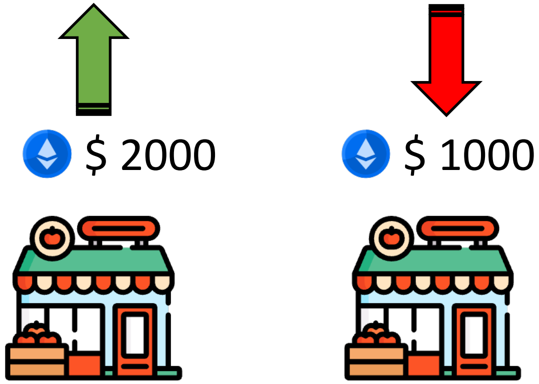
后跑

TX1 $2

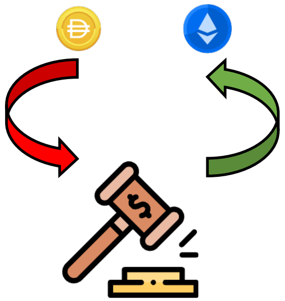
TX2 $2

MEV主要来源

套利

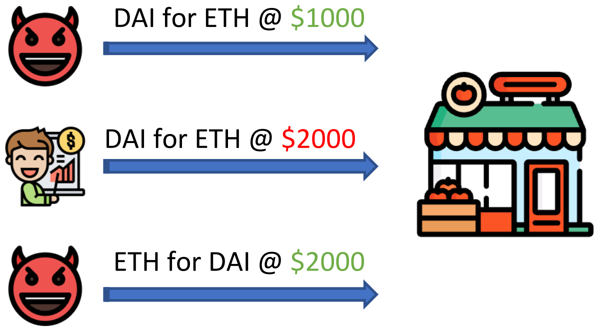


清算



Qin, Kaihua, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. "An empirical study of defi liquidations: Incentives, risks, and instabilities." In Proceedings of the 21st ACM Internet Measurement Conference, pp. 336-350. 2021.

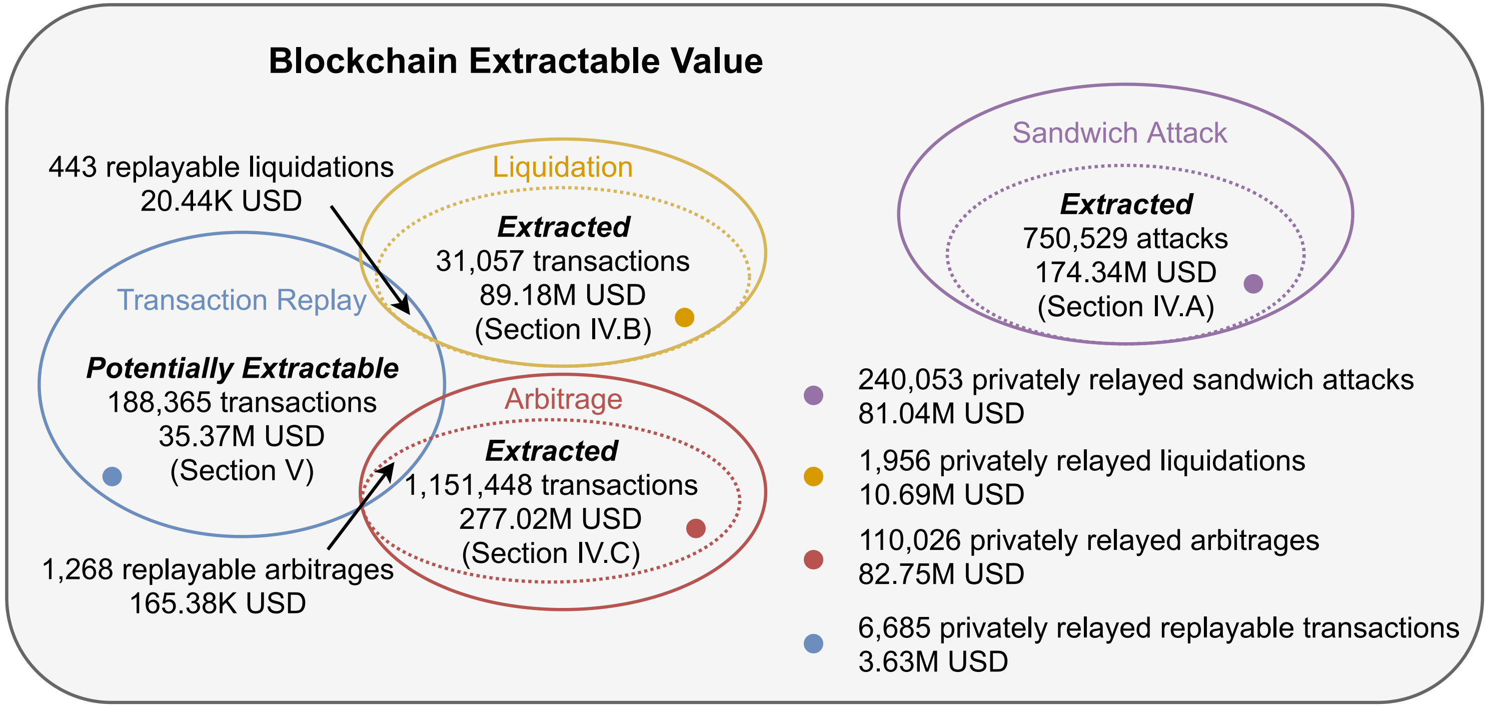
三明治攻击



Zhou, Liyi, Kaihua Qin, Christof Ferreira Torres, Duc V. Le, and Arthur Gervais. "High-frequency trading on decentralized on-chain exchanges." In 2021 IEEE Symposium on Security and Privacy (SP), pp. 428-445. IEEE, 2021.

量化MEV

- 2018年12月1日至2021年8月5日（32个月）
- 540.54M USD



Blockchain Extractable Value

443 replayable liquidations
20.44K USD

Liquidation

Extracted
31,057 transactions
89.18M USD
(Section IV.B)

Sandwich Attack

Extracted
750,529 attacks
174.34M USD
(Section IV.A)

Transaction Replay

Potentially Extractable
188,365 transactions
35.37M USD
(Section V)

Arbitrage

Extracted
1,151,448 transactions
277.02M USD
(Section IV.C)

1,268 replayable arbitrages
165.38K USD

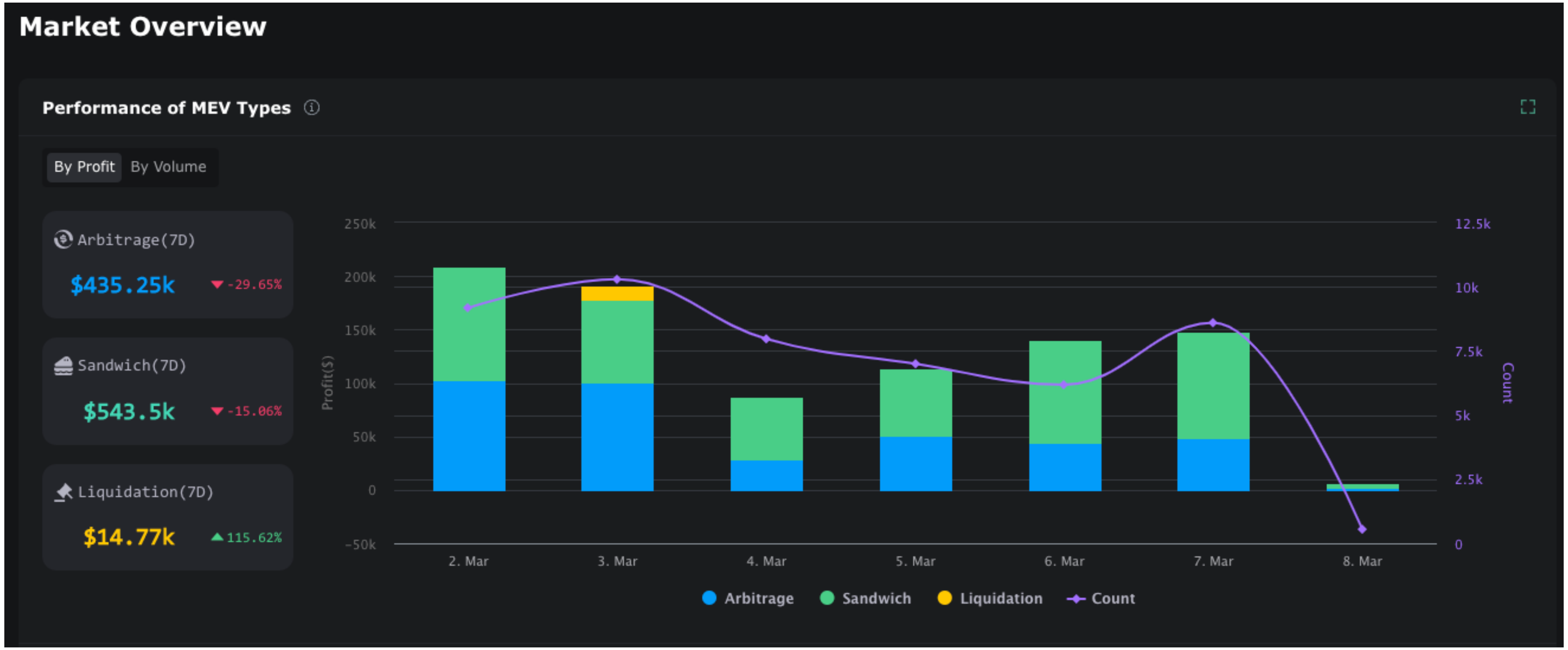
● 240,053 privately relayed sandwich attacks
81.04M USD

● 1,956 privately relayed liquidations
10.69M USD

● 110,026 privately relayed arbitrages
82.75M USD

● 6,685 privately relayed replayable transactions
3.63M USD

量化MEV



Market Overview

Performance of MEV Types

By Profit By Volume

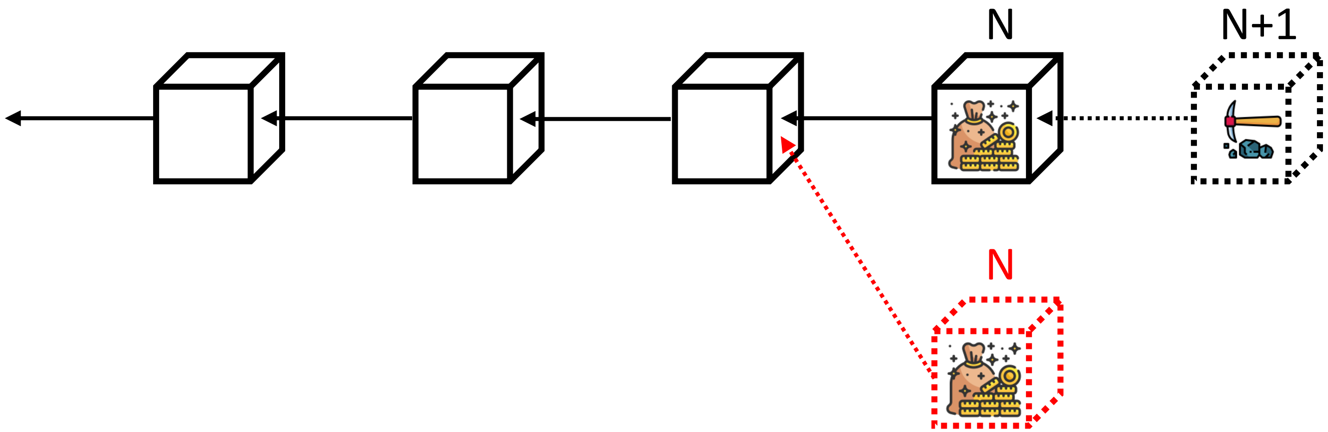
Arbitrage(7D)
$435.25k ▼-29.65%

Sandwich(7D)
$543.5k ▼-15.06%

Liquidation(7D)
$14.77k ▲115.62%

https://eigenphi.io/

共识层安全

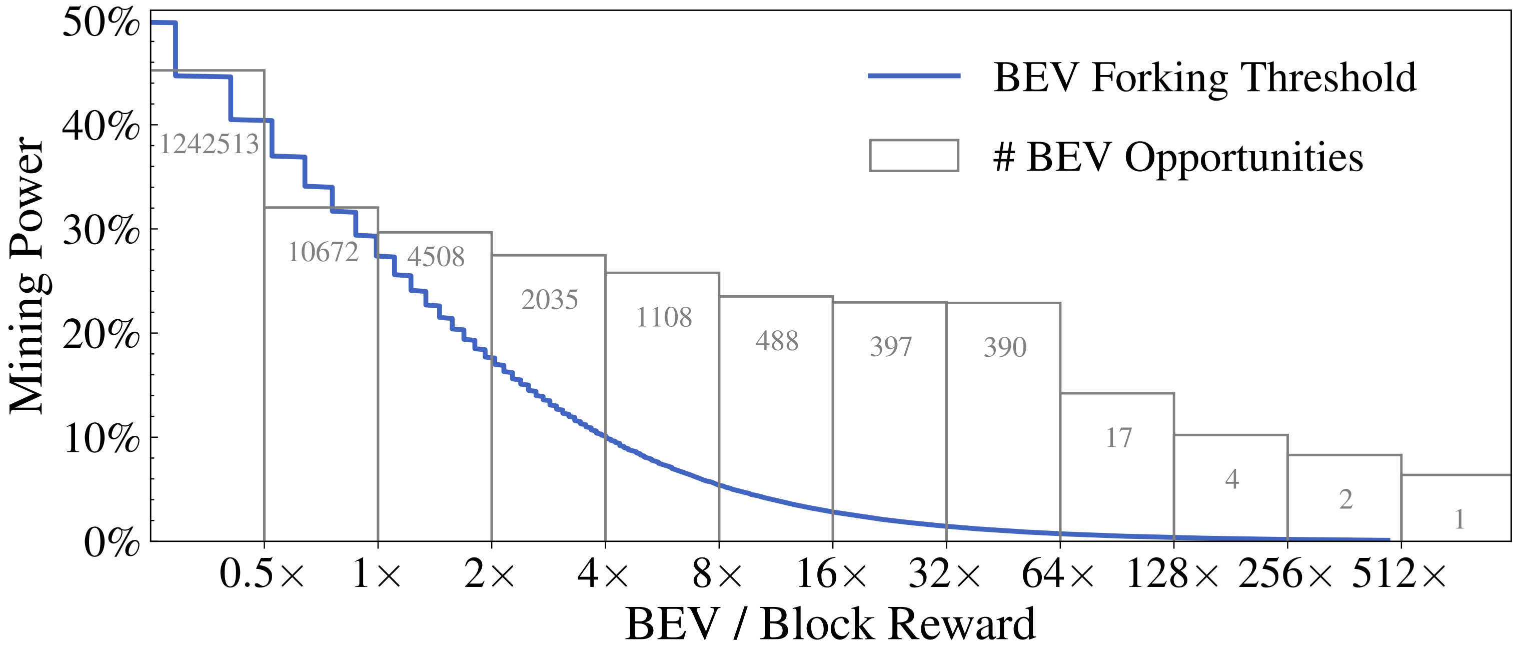


共识层安全

MEV/Block Reward > 4x

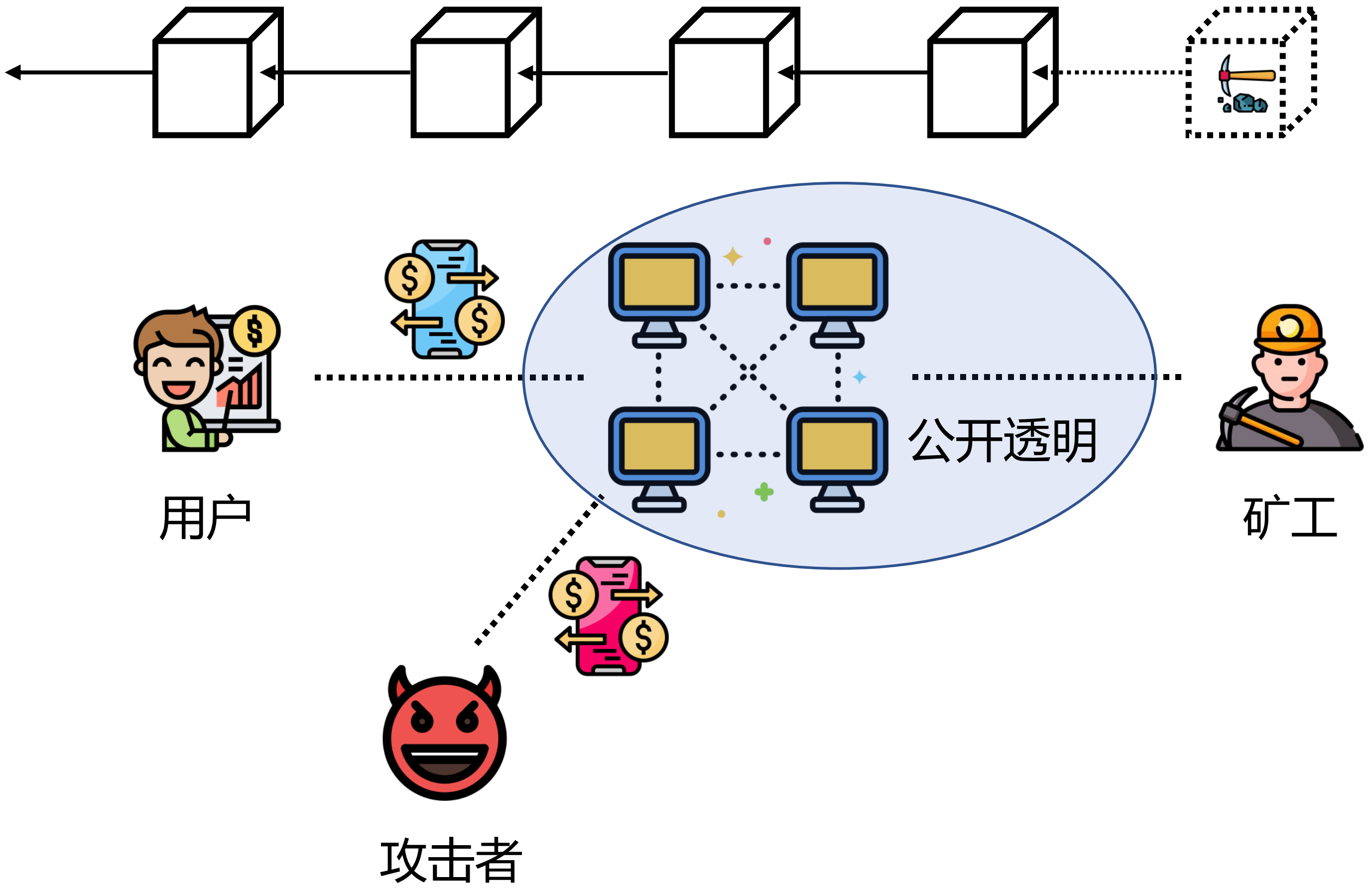
⇩

10%矿工恶意分叉



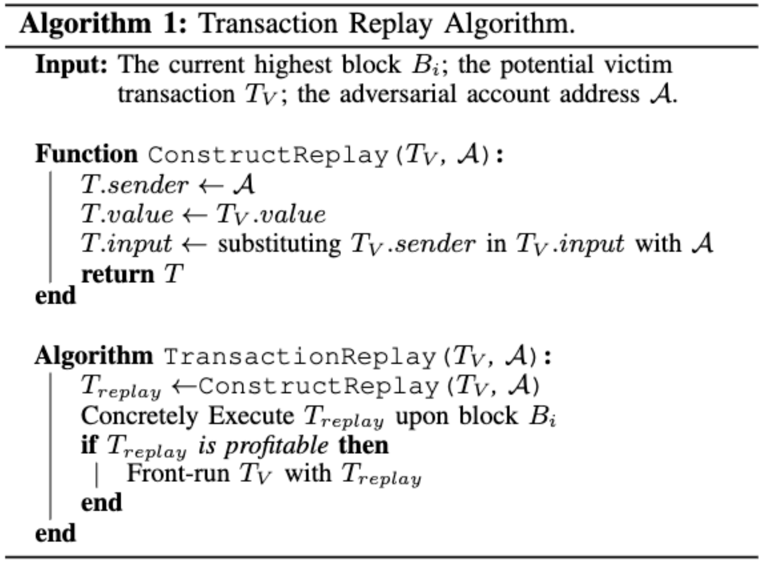
模仿攻击

~~Replay~~ Imitation Attack



模仿攻击

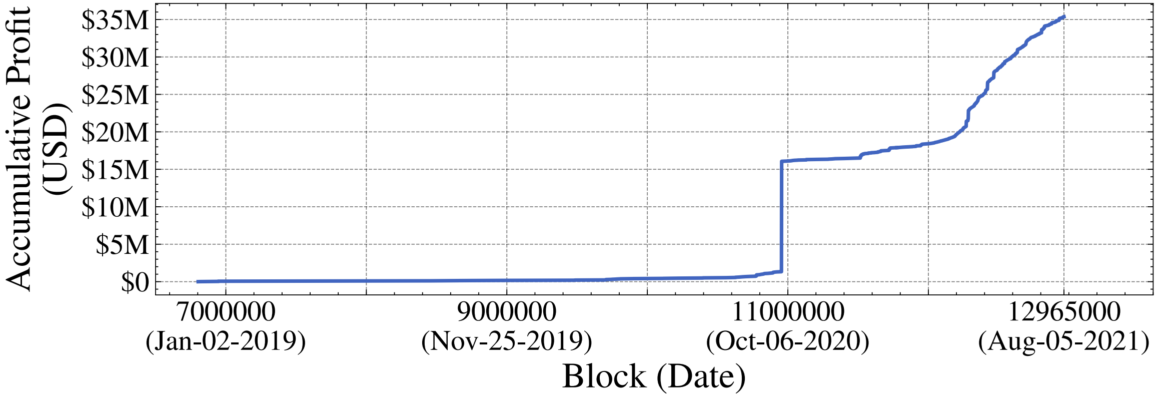
- 2018年12月1日至2021年8月5日（32个月）
- 35.37M USD

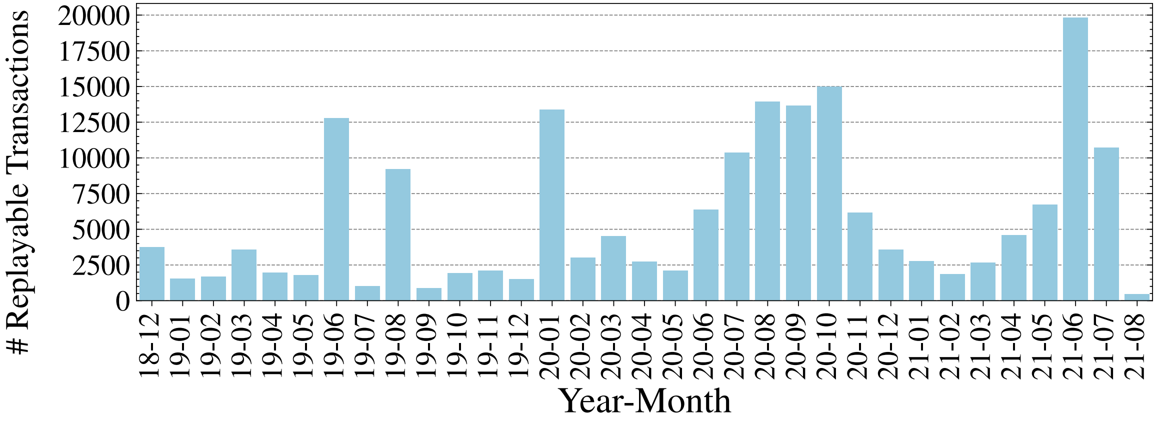


Algorithm 1: Transaction Replay Algorithm.

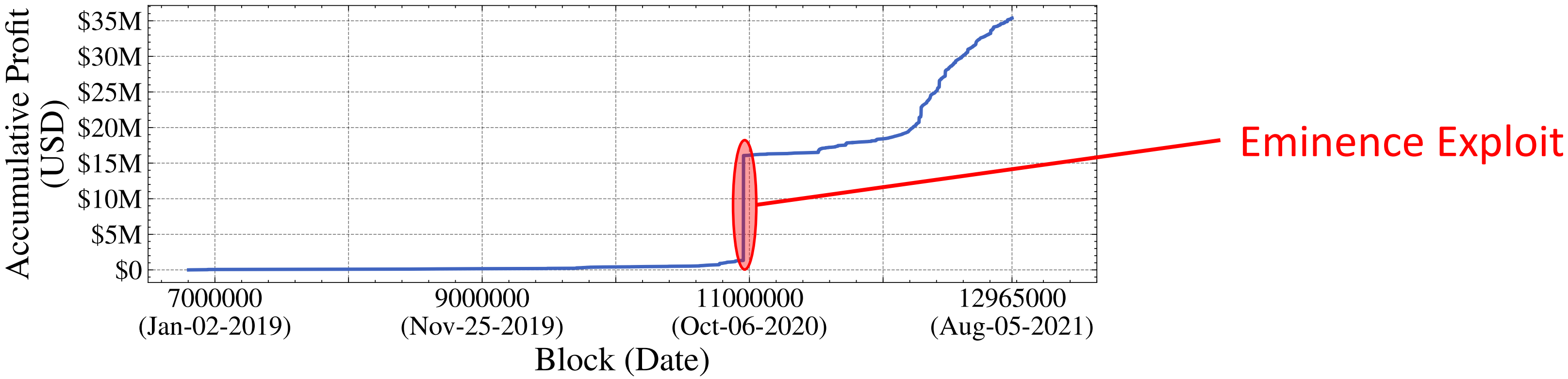
Input: The current highest block B_i; the potential victim transaction T_V; the adversarial account address $\mathcal{A}$.

```
Function ConstructReplay($T_V$, $\mathcal{A}$):
    $T.sender \leftarrow \mathcal{A}$
    $T.value \leftarrow T_V.value$
    $T.input \leftarrow$ substituting $T_V.sender$ in $T_V.input$ with $\mathcal{A}$
    return $T$
end

Algorithm TransactionReplay($T_V$, $\mathcal{A}$):
    $T_{replay} \leftarrow$ConstructReplay($T_V$, $\mathcal{A}$)
    Concretely Execute $T_{replay}$ upon block $B_i$
    if $T_{replay}$ is profitable then
        Front-run $T_V$ with $T_{replay}$
    end
end
```

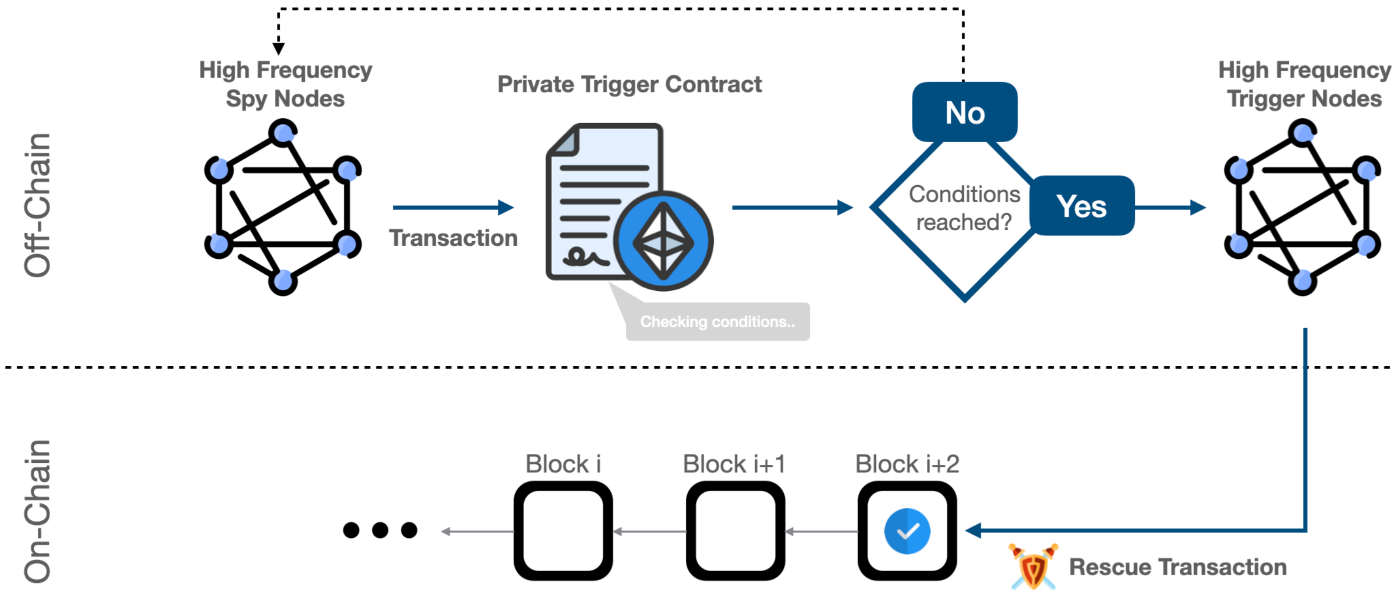




防御手段?


Accumulative Profit
(USD)
$35M
$30M
$25M
$20M
$15M
$10M
$5M
$0
7000000
(Jan-02-2019)
9000000
(Nov-25-2019)
11000000
(Oct-06-2020)
12965000
(Aug-05-2021)
Block (Date)
Eminence Exploit

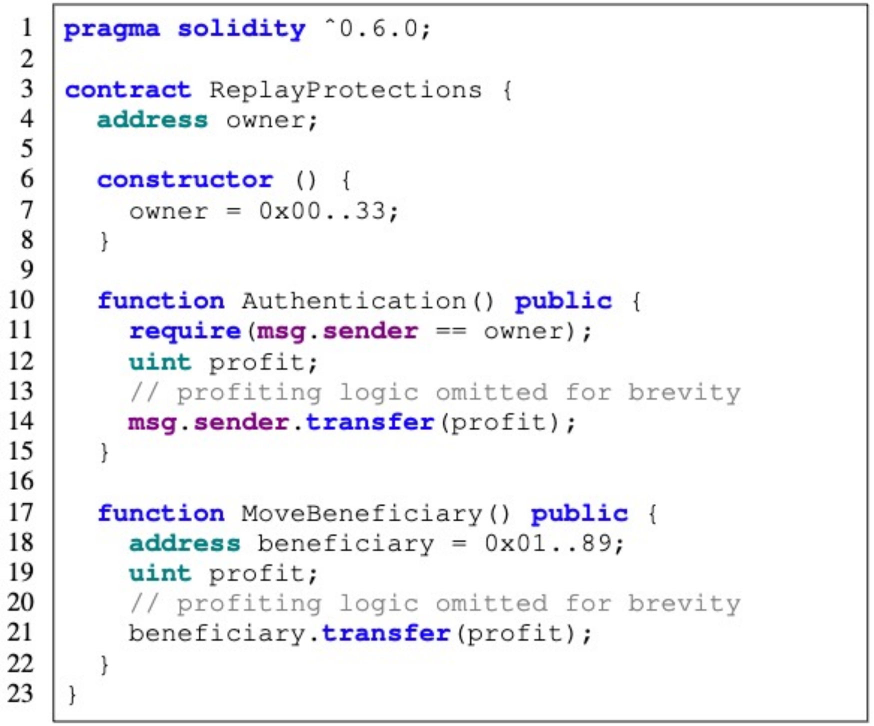
D23E –
新一代的即时防御系统



抵抗模仿攻击

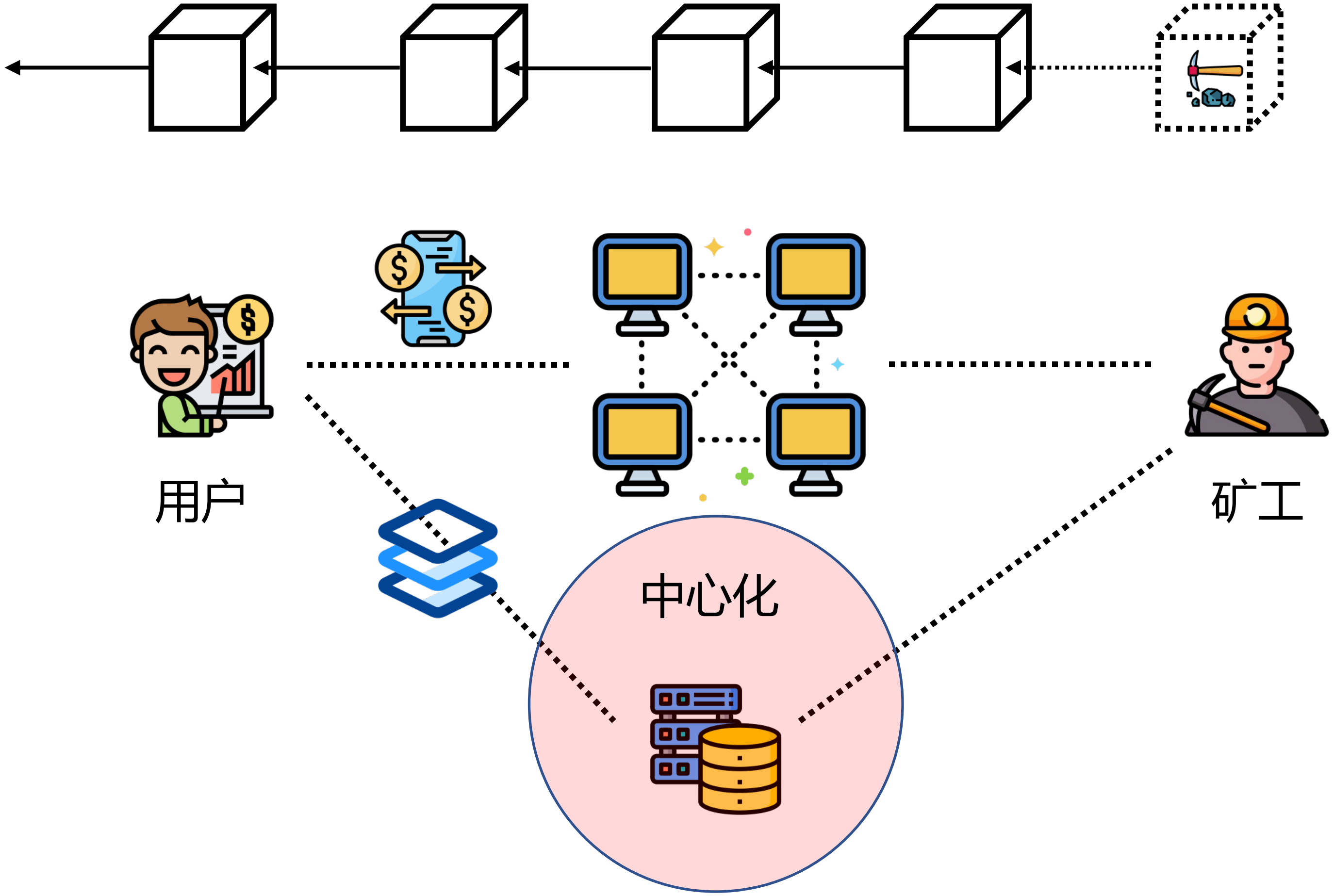
- 身份验证
- 混淆受益者

- 公平排序技术
- 可信硬件



```
pragma solidity ^0.6.0;

contract ReplayProtections {
  address owner;

  constructor () {
    owner = 0x00..33;
  }

  function Authentication() public {
    require(msg.sender == owner);
    uint profit;
    // profiting logic omitted for brevity
    msg.sender.transfer(profit);
  }

  function MoveBeneficiary() public {
    address beneficiary = 0x01..89;
    uint profit;
    // profiting logic omitted for brevity
    beneficiary.transfer(profit);
  }
}
```

Front-running as a service (FaaS)



Front-running as a service (FaaS)

- 无风险
- 基于信任
- 抗审查?
- 首价密封投标拍卖 (First price sealed bid auction)

$$b_i^{\mathrm{PA}}(\mathcal{O}, \mathcal{S}_i) = \frac{n-1}{n}\mathcal{R}_i(\mathcal{O})$$

$$\mathbb{E}\left[\max_i b_i^{\mathrm{PA}}(\mathcal{O}, \mathcal{S}_i)\right] = \frac{n-1}{n+1}\mathcal{R}_{\max}$$

区块链可提取价值

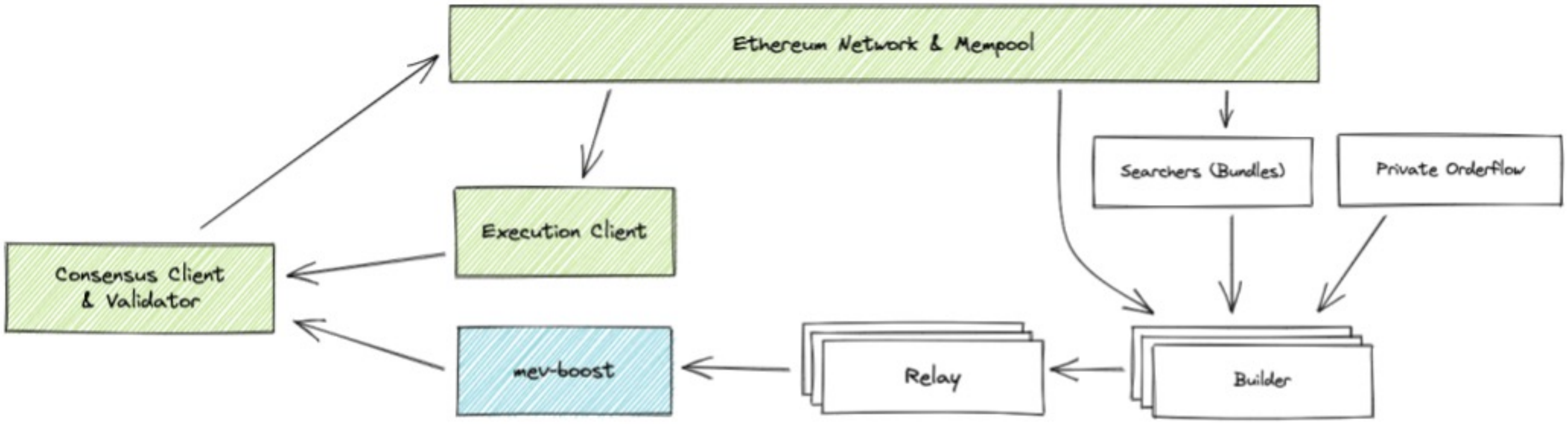
昨天

今天

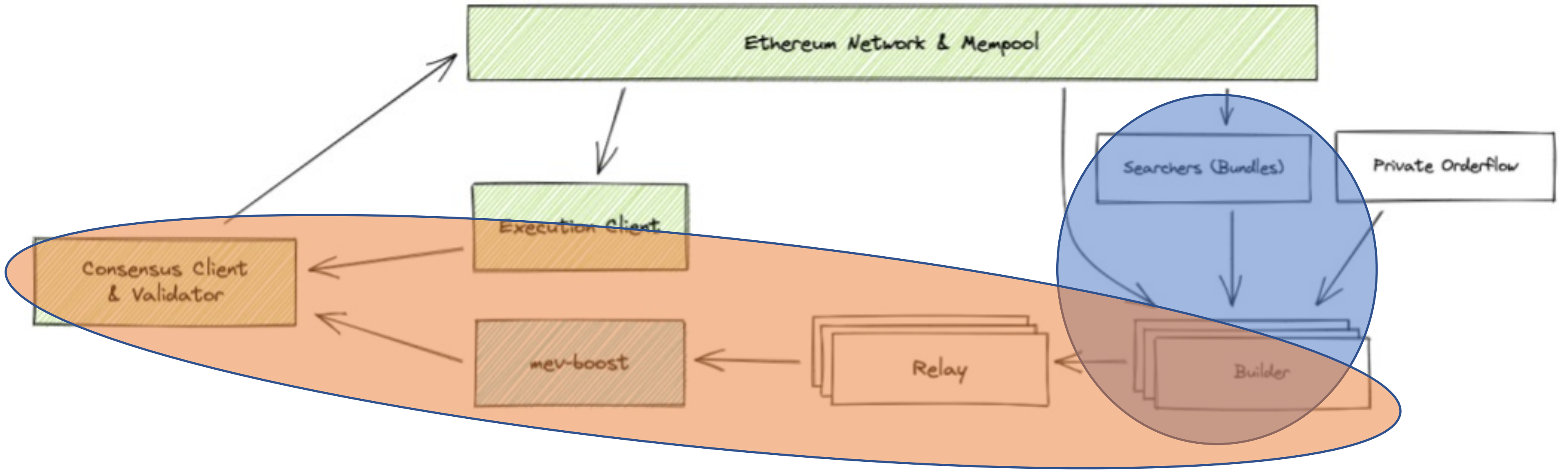
- Proof-of-stake (PoS)
- Proposer/builder separation (PBS)

明天

Proposer/builder separation (PBS)



Proposer/builder separation (PBS)



Proposer/builder separation (PBS)

$$\mathbb{E}\left[\max_i b_i^{\mathrm{PA}}(\mathcal{O}, \mathcal{S}_i)\right] = \frac{n-1}{n+1}\mathcal{R}_{\max}$$?

区块链可提取价值

昨天

今天

明天

与MEV共存

- MEV-aware design

Zhou, Liyi, Kaihua Qin, and Arthur Gervais. "A2mm: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges." *arXiv preprint arXiv:2106.07371* (2021).

Qin, Kaihua, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. " Mitigating Decentralized Finance Liquidations with Reversible Call Options." In Financial Cryptography and Data Security, 2023.

- Encrypted mempool/Fair sequencing

- Cross-domain

THANK YOU
FOR YOUR ATTENTION