FLASH BOYS 2.0

Nathan Hettige, Michael Cowan, Zhien Zhang

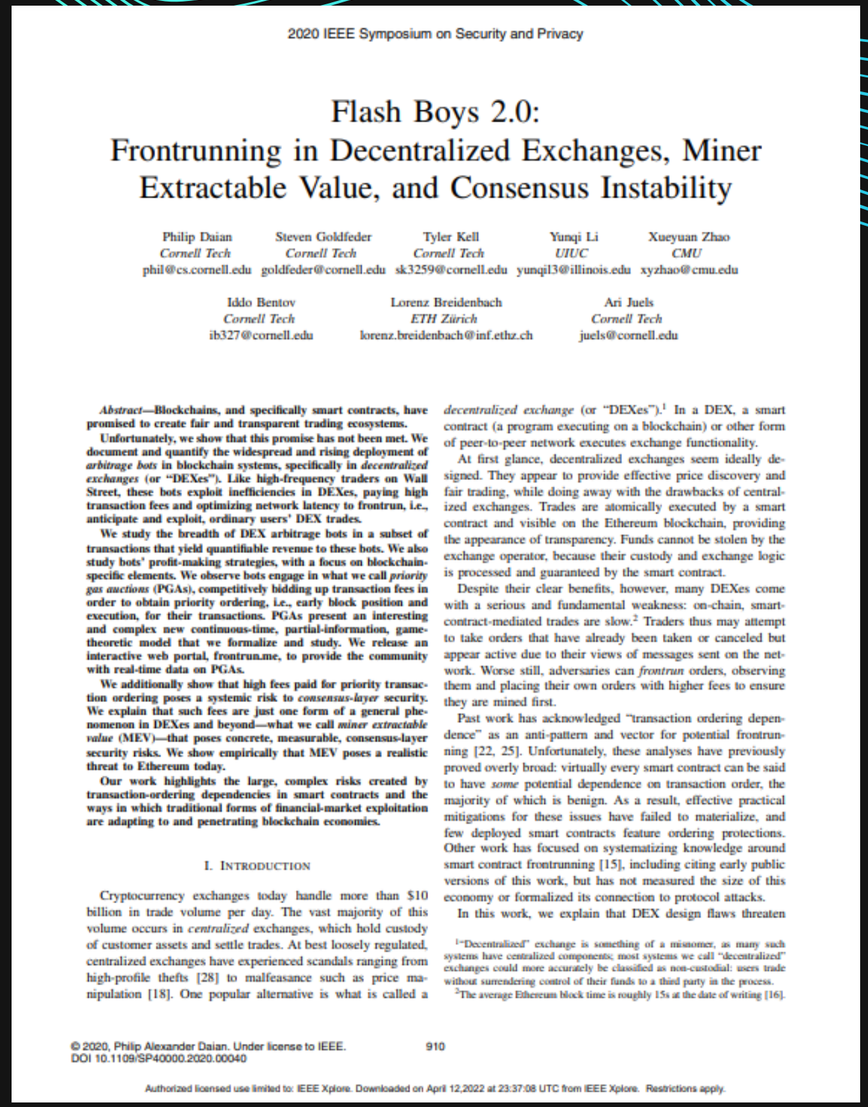
COMS4507

CONTENTS

Flash Boys 2.0: Frontrunning in Decentralised Exchanges, Miner Extractable Value, and Consensus Instability

By Daian, Philip ; Goldfeder, Steven ; Kell, Tyler ; Li, Yunqi ; Zhao, Xueyuan ; Bentov, Iddo ; Breidenbach, Lorenz ; Juels, Ari

2020 IEEE Symposium on Security and Privacy (SP), 2020-05, p.910-927



2020 IEEE Symposium on Security and Privacy

Flash Boys 2.0:
Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability

Philip Daian, *Cornell Tech*, phil@cs.cornell.edu
Steven Goldfeder, *Cornell Tech*, goldfeder@cornell.edu
Tyler Kell, *Cornell Tech*, sk3259@cornell.edu
Yunqi Li, *UIUC*, yunqil3@illinois.edu
Xueyuan Zhao, *CMU*, xyzhao@cmu.edu
Iddo Bentov, *Cornell Tech*, ib327@cornell.edu
Lorenz Breidenbach, *ETH Zürich*, lorenz.breidenbach@inf.ethz.ch
Ari Juels, *Cornell Tech*, juels@cornell.edu

***Abstract*—Blockchains, and specifically smart contracts, have promised to create fair and transparent trading ecosystems.**

Unfortunately, we show that this promise has not been met. We document and quantify the widespread and rising deployment of *arbitrage bots* in blockchain systems, specifically in *decentralized exchanges* (or "DEXes"). Like high-frequency traders on Wall Street, these bots exploit inefficiencies in DEXes, paying high transaction fees and optimizing network latency to frontrun, i.e., anticipate and exploit, ordinary users' DEX trades.

We study the breadth of DEX arbitrage bots in a subset of transactions that yield quantifiable revenue to these bots. We also study bots' profit-making strategies, with a focus on blockchain-specific elements. We observe bots engage in what we call *priority gas auctions* (PGAs), competitively bidding up transaction fees in order to obtain priority ordering, i.e., early block position and execution, for their transactions. PGAs present an interesting and complex new continuous-time, partial-information, game-theoretic model that we formalize and study. We release an interactive web portal, frontrun.me, to provide the community with real-time data on PGAs.

We additionally show that high fees paid for priority transaction ordering poses a systemic risk to *consensus-layer* security. We explain that such fees are just one form of a general phenomenon in DEXes and beyond—what we call *miner extractable value* (MEV)—that poses concrete, measurable, consensus-layer security risks. We show empirically that MEV poses a realistic threat to Ethereum today.

Our work highlights the large, complex risks created by transaction-ordering dependencies in smart contracts and the ways in which traditional forms of financial-market exploitation are adapting to and penetrating blockchain economies.

I. Introduction

Cryptocurrency exchanges today handle more than $10 billion in trade volume per day. The vast majority of this volume occurs in *centralized* exchanges, which hold custody of customer assets and settle trades. At best loosely regulated, centralized exchanges have experienced scandals ranging from high-profile thefts [28] to malfeasance such as price manipulation [18]. One popular alternative is what is called a *decentralized exchange* (or "DEXes").[1] In a DEX, a smart contract (a program executing on a blockchain) or other form of peer-to-peer network executes exchange functionality.

At first glance, decentralized exchanges seem ideally designed. They appear to provide effective price discovery and fair trading, while doing away with the drawbacks of centralized exchanges. Trades are atomically executed by a smart contract and visible on the Ethereum blockchain, providing the appearance of transparency. Funds cannot be stolen by the exchange operator, because their custody and exchange logic is processed and guaranteed by the smart contract.

Despite their clear benefits, however, many DEXes come with a serious and fundamental weakness: on-chain, smart-contract-mediated trades are slow.[2] Traders thus may attempt to take orders that have already been taken or canceled but appear active due to their views of messages sent on the network. Worse still, adversaries can *frontrun* orders, observing them and placing their own orders with higher fees to ensure they are mined first.

Past work has acknowledged "transaction ordering dependence" as an anti-pattern and vector for potential frontrunning [22, 25]. Unfortunately, these analyses have previously proved overly broad: virtually every smart contract can be said to have *some* potential dependence on transaction order, the majority of which is benign. As a result, effective practical mitigations for these issues have failed to materialize, and few deployed smart contracts feature ordering protections. Other work has focused on systematizing knowledge around smart contract frontrunning [15], including citing early public versions of this work, but has not measured the size of this economy or formalized its connection to protocol attacks.

In this work, we explain that DEX design flaws threaten

[1]"Decentralized" exchange is something of a misnomer, as many such systems have centralized components; most systems we call "decentralized" exchanges could more accurately be classified as non-custodial: users trade without surrendering control of their funds to a third party in the process.

[2]The average Ethereum block time is roughly 15s at the date of writing [16].

DOI 10.1109/SP40000.2020.00040

Frontrunning

"Frontrunning is generally the exploit of information asymmetries created by power dynamics within a financial structure"

Due to no single party playing the role of broker in decentralised systems, this information asymmetry usually arises due to the underlying infrastructure

Decentralised Exchange (DEX)

Community Focus

Community driven, open source platforms

Leverage Smart Contracts

Trades are automatic and transparent

Not Foolproof

Can still be exploited by targeting the underlying infrastructure

Bot Arbitrage

Gossip Protocol

Some nodes receive knowledge of transactions prior to others

Batch Processing

Blocks containing multiple transactions

Book Order

Continuous Limit VS Automated Market Maker

Prevalence

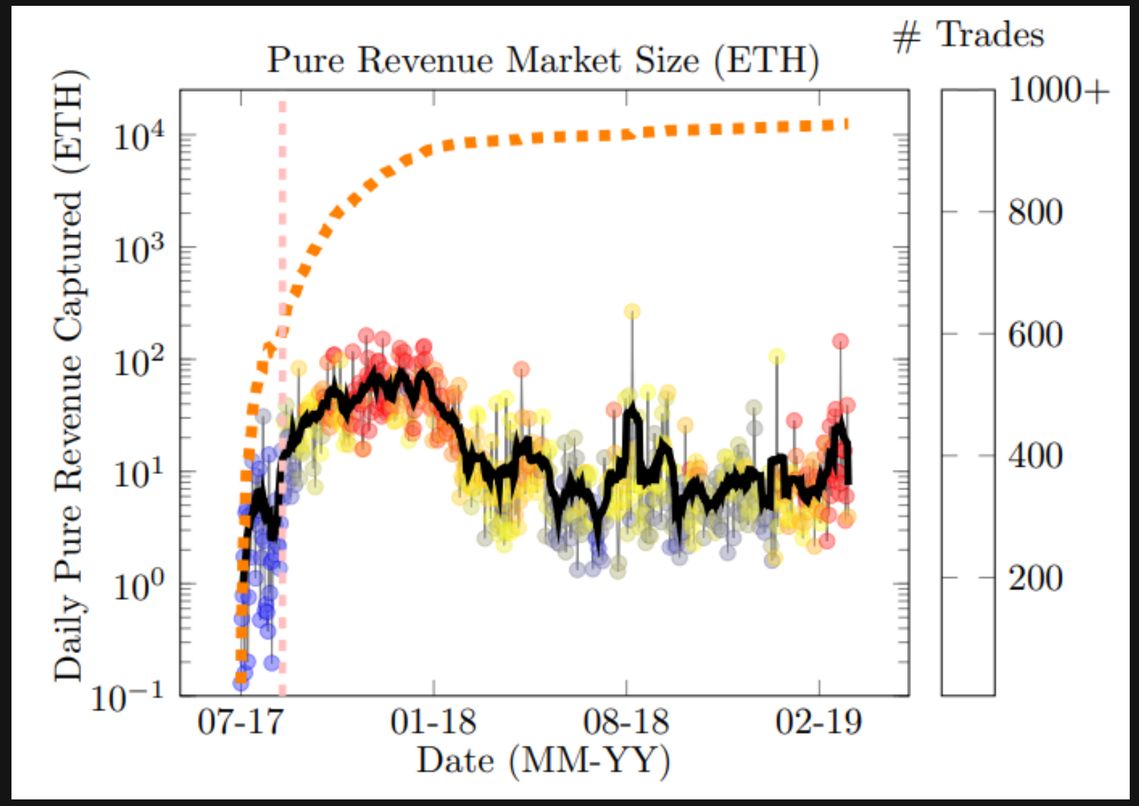


Figure of Prevalence Sourced From [1]

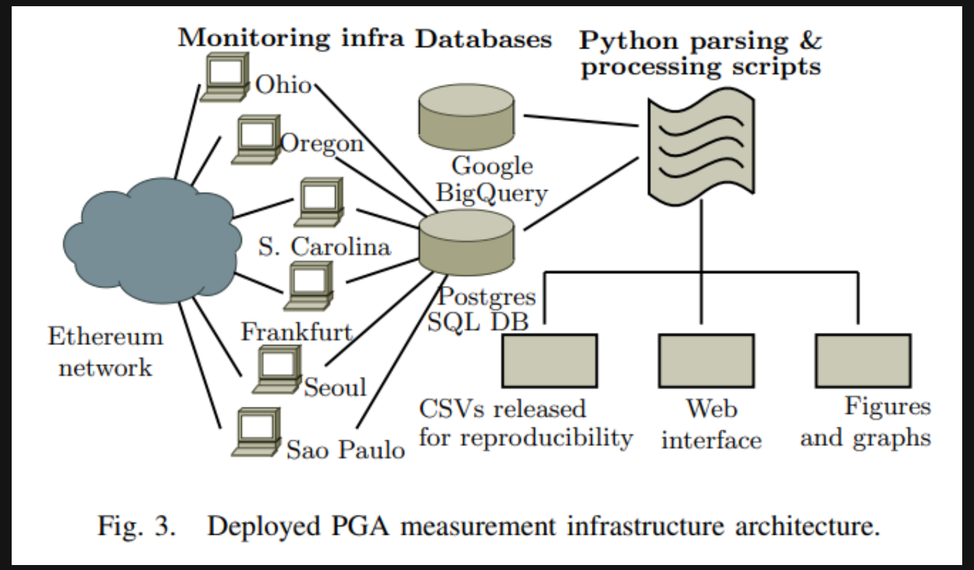
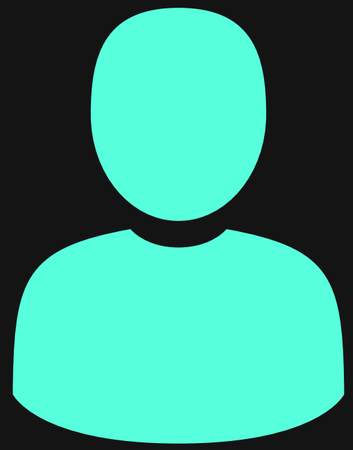


Fig. 3. Deployed PGA measurement infrastructure architecture.

Figure of Test Rig Sourced From [1]

Pure Revenue Opportunity



User

1. Use 5 Ether to buy 100 Free Coin

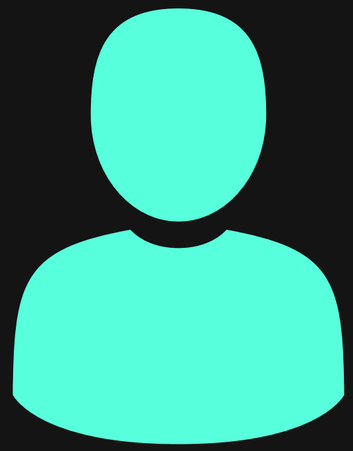
20 FREE/ETH

2. Use 100 Free Coin to buy 10 Ether

10 FREE/ETH

TokenStore
on
Ethereum

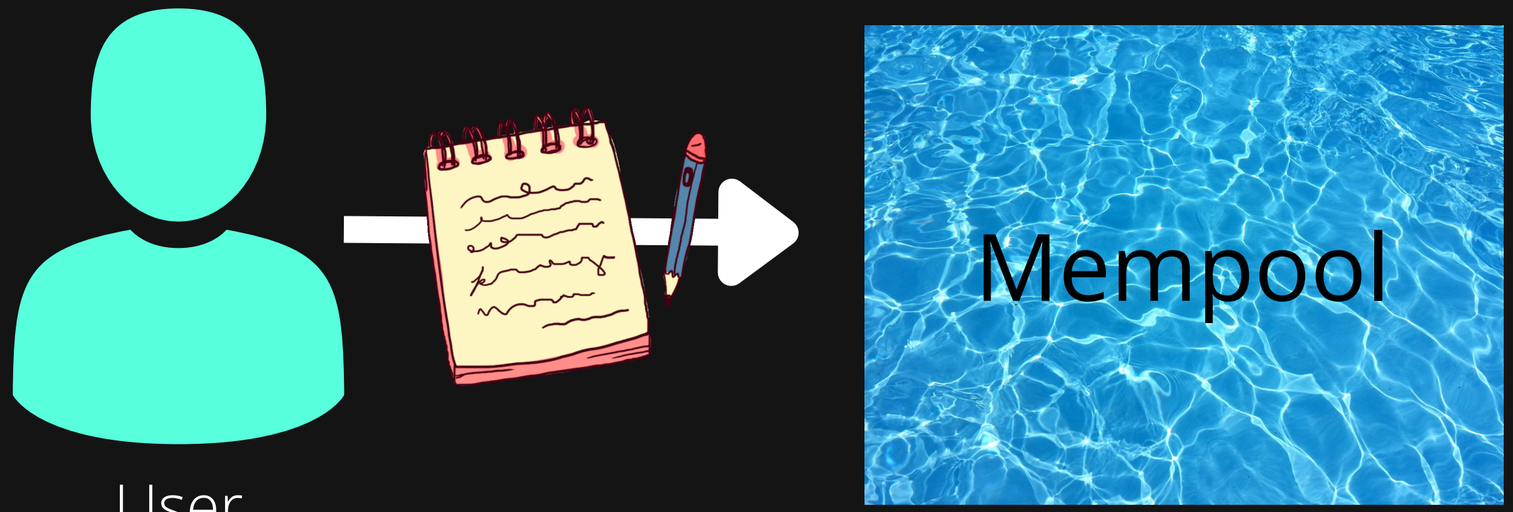
Pure Revenue Opportunity



User

	ETH	FREE
BEFORE	5	0
AFTER 1st	0	100
AFTER 2nd	10	0

Pure Revenue Opportunity



Pure Revenue Opportunity

Priority Gas Auctions (PGAs)

Bots noticed a pure revenue opportunity will try to secure the transaction by having it processed by a miner as soon as possible.

This is achieved by biding up gas fees of the transaction to attract miners.

This process is called Priority Gas Auction.

Bot Strategies to Win in a PGA

Latency Wars

Try to reduce the bidding latency

Blind Raising

Increase the bid amount by a fixed portion regardless of other bots' behaviour

Counterbidding

Make the next bid depending on the last bid made by the competitors

Cooperation

Stop competing with higher gas fees and split the profit among competitors

Why is cooperation possible?

The possible profit will decrease as the number of bids increases, because bids are non-decreasing.

Therefore, it is more profitable for competitors to coordinate and split the profit.

In a PGA with two users, the maximum profit can be achieved by each user bidding the minimum increase every time, and split the profit after one of them wins.

Cooperation in PGAs

Nash equilibrium in coorperative strategies

A cooperative equilibrium has been observed, which is consistent with the results of the existing literatures on game theory.

12.5% is the minimum alllowed raise

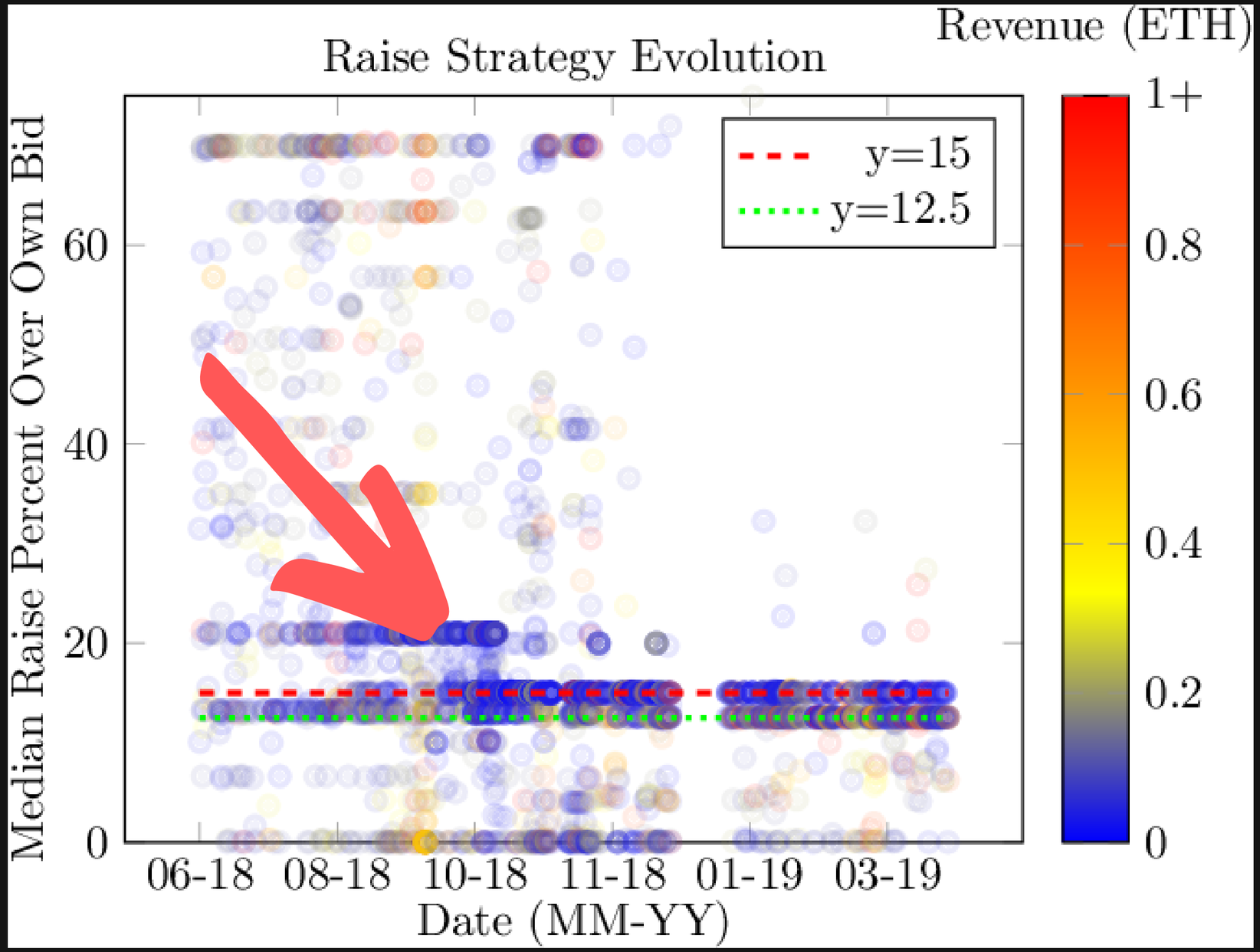


Figure 10 in [1]

Cooperation in PGAs

Nash equilibrium in coorperative strategies

A cooperative equilibrium has been observed, which is consistent with the results of the existing literatures on game theory.

Many PGAs are not profitable

Which is another motivation for the bots to cooperate to maintain the profitability of PGAs.

- The majority of the winners do not profit from PGAs.
- It is still likely for some winners to make a considerable profit.
- Given the low cost in participation, bots are still motivated to engage in PGAs.

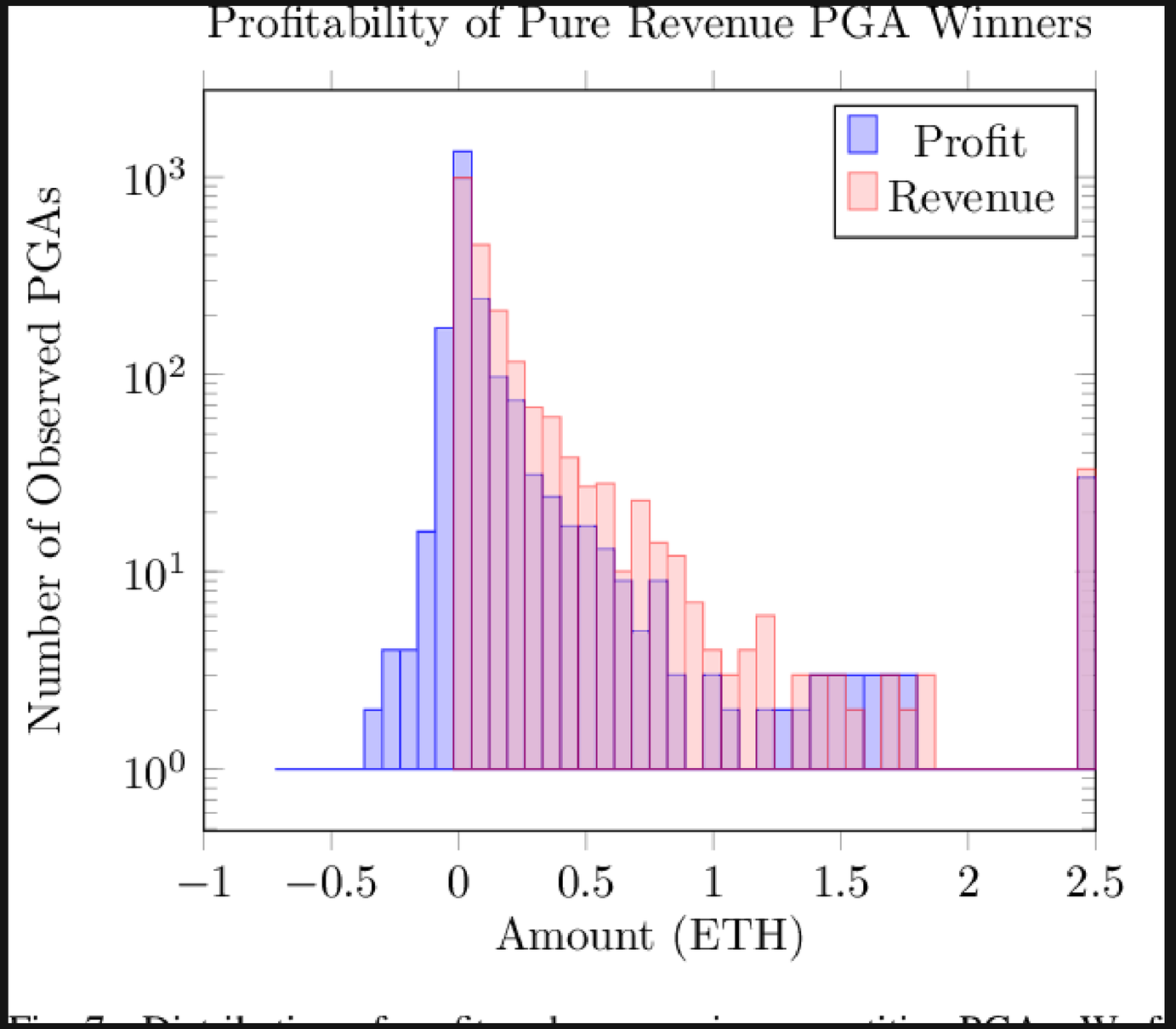


Figure 6 in [1]

Cooperation in PGAs

Nash equilibrium in coorperative strategies

A cooperative equilibrium has been observed, which is consistent with the results of the existing literatures on game theory.

Many PGAs are not profitable

Which is another motivation for the bots to cooperate to maintain the profitability of PGAs.

Cooperation can be developed on-chain without explicit negotiation

Though perfect coopation has not been observed, but arbitrage bots have the inherent motivation to form cooporations.

Security flaws and potential attacks

Intuitve solutions to solve problems

PRIORITY GAS AUCTIONS (PGA'S)

Problem: The network is slow and there may be a huge queue waiting to run their transactions

Solution: Introduce a gas price (GWEI) to incentivise miners to priortise your transaction

DECENTRALISD EXCHANGES (DEX'S)

Problem: Centralised exchanges rely on a third party to match orders.

Solution: Replace the exchange operator with a smart contract and trade between any two tokens at any time.

RESULTING BEHAVIOUR:

Predatory market behaviour that poses a risk to consensus layer security.

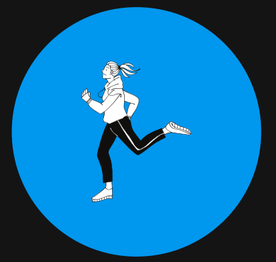
Miner Extractable Value (MEV)

The maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding and chain the order of transactions

-

https://ethereum.org/en/developers/docs/mev/

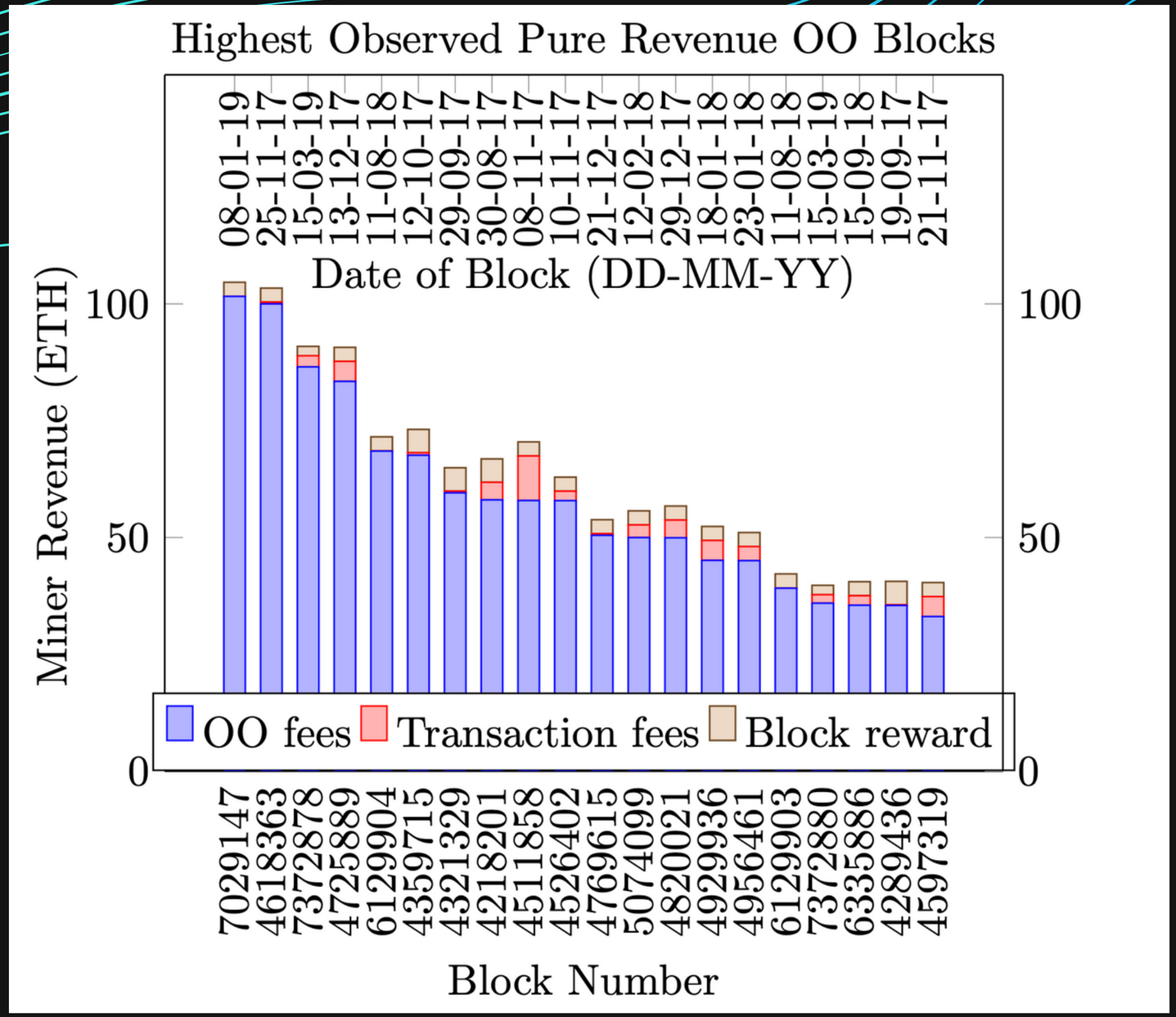
Order Optimisation



Front running

Sandwich Trading

Rewrite Transactions



Blocks with the highest pure revenue OO fees observed on Ethereum till 2019.

In theses blocks, OO fees dominate both block rewards and transaction fees by many magnitudes.

Figure 11 from [1], Blocks with the highest OO fees on Ethereum

The good and the bad of MEV

GOOD

PRIORITY TRANSACTIONS

DEX ABITRAGE ENSURES ACCURATE PRICES FOR USERS

BORROWING AND LENDING PROTOCOLS

DECENTRALISED FINANCE

BAD

WORSE USER EXPERIENCE

BAD EXECUTION OF TRADE

NETWORK CONGESTION

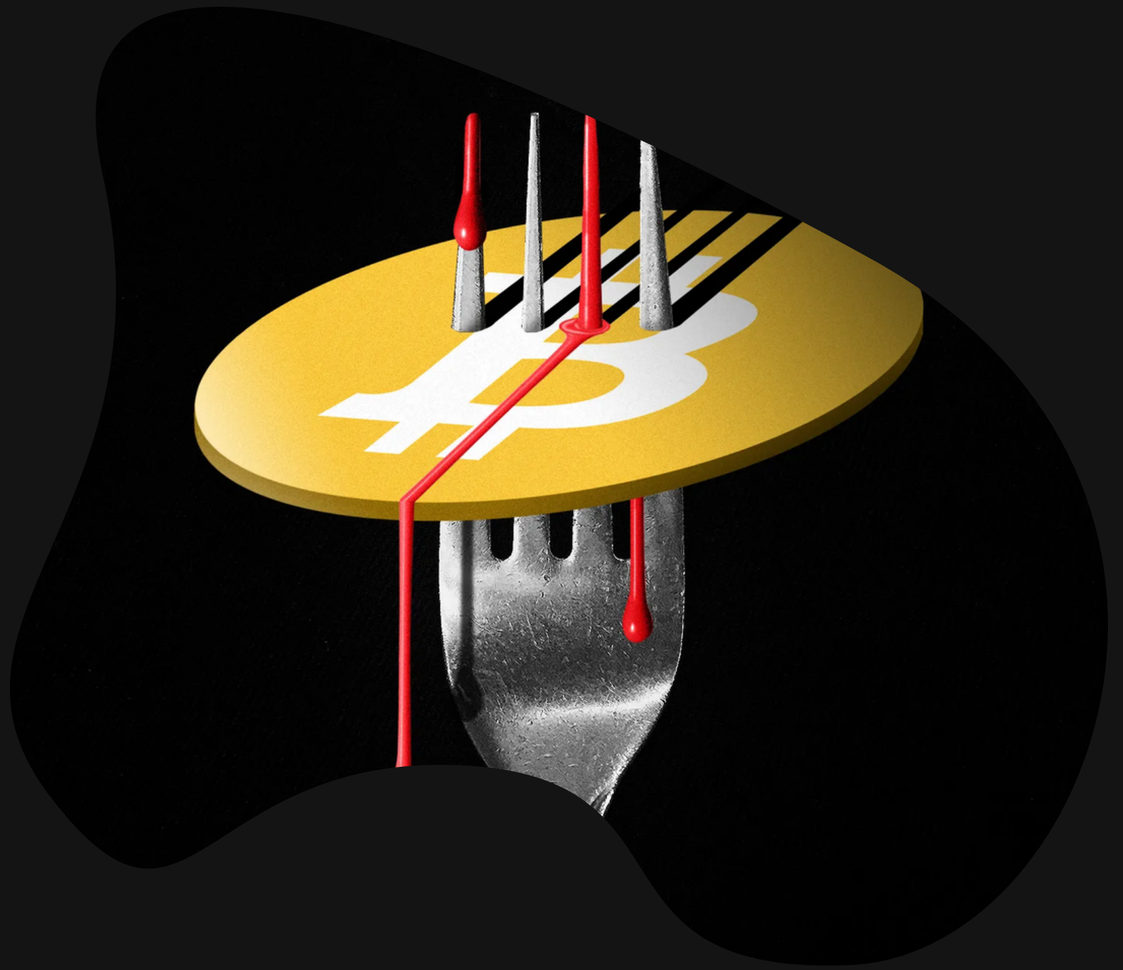
INCREASED GAS PRICES

SUBSIDIZE FORKING ATTACKS

RISK TO CONSENSUS LAYER

Threat to consensus layer:

Significant MEV in a block can subsidize forking attacks.



Undercutting attack

Forking attacks

CONCEPT:

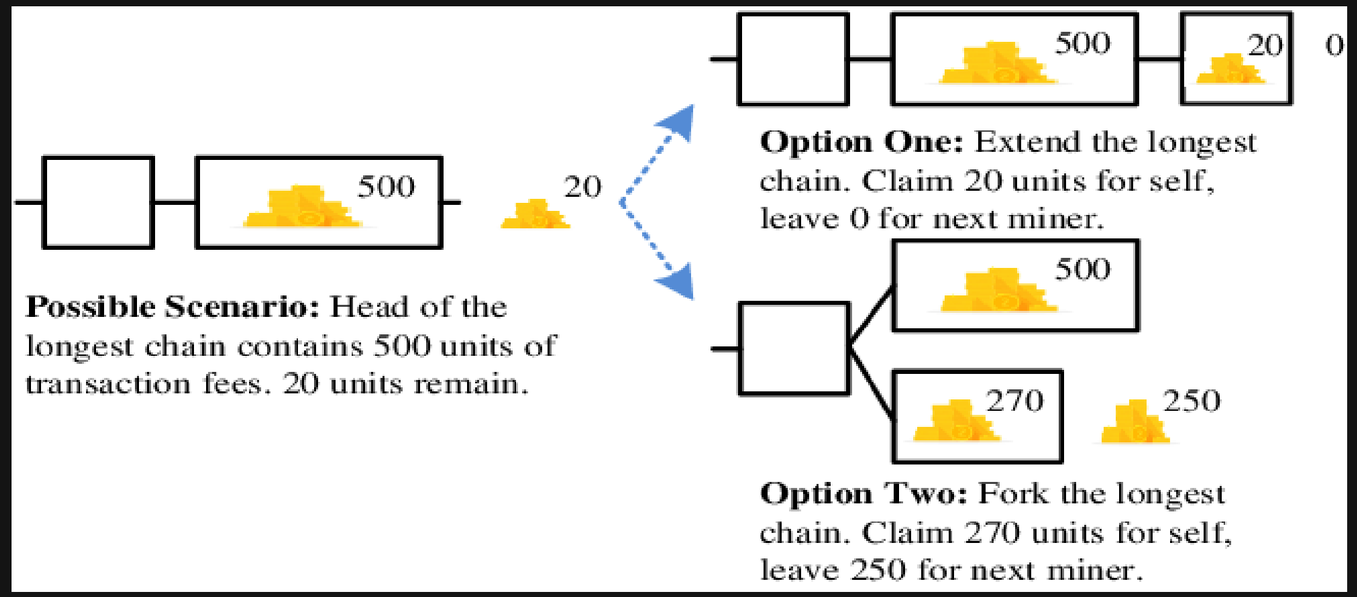
"Ignore" the mined block with good MEV in your chain and remine it yourself.

Leave out some transactions with enticing MEV from your block, leaving it for other miners to mine it into the next block.

This will add confirmations to your block and ideally orphan the "ignored" block.

RESULT:

Claim the MEV of that block as yours



Liu, Ziyao & Nguyen, Cong & Wang, Wenbo & Niyato, Dusit & Wang, Ping & Liang, Ying-Chang & Kim, Dong In. (2019). A Survey on Applications of Game Theory in Blockchain.

Time-Bandit attack

Forking attacks

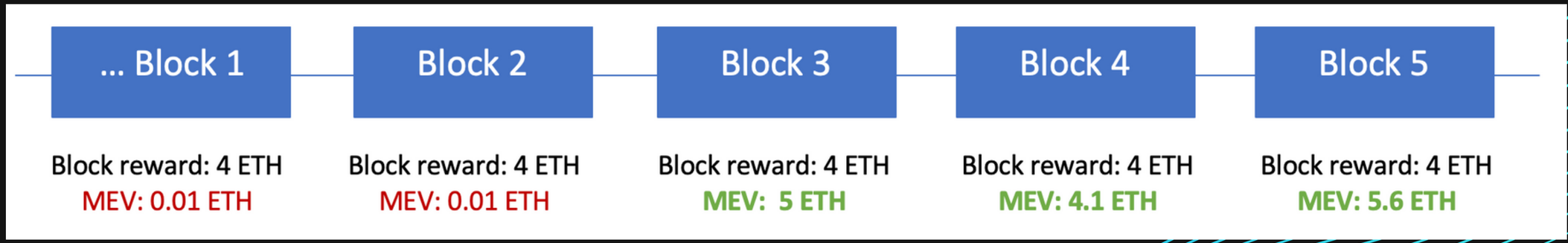
CONCEPT:

Select a set of blocks from the current height in which stealable value exceeds the block rewards.

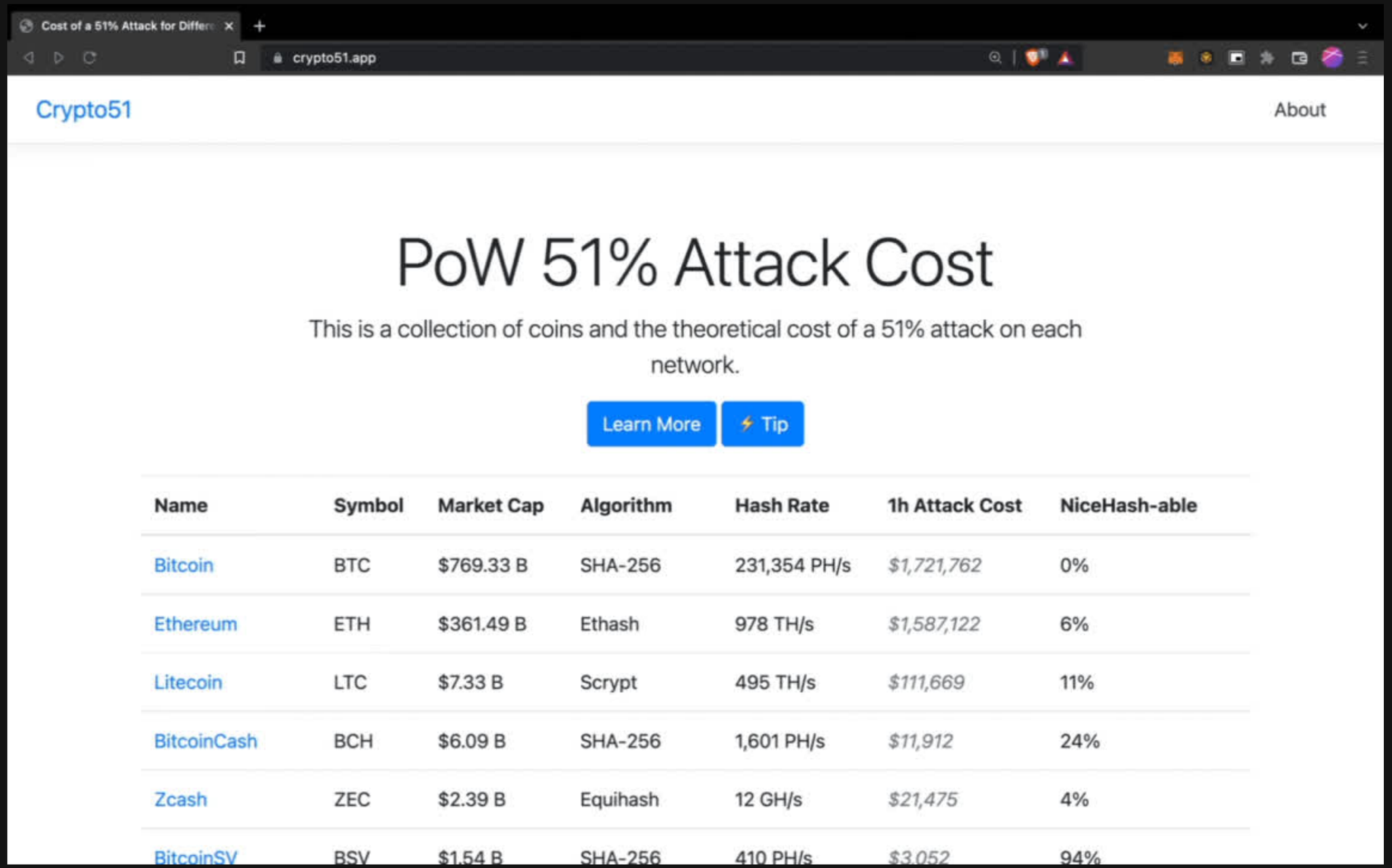
Provision mining resources to perform a 51% attack that mines a fork up to or past the current height.

RESULT:

Claim the MEV of the chosen past and future blocks. Bonus: Rewrite any abitrage transactions to profit into your account as well.



Time-Bandit attack



IN A NUTSHELL...

DEX ARBITRAGE

leads to

FRONTRUNINNG

leads to

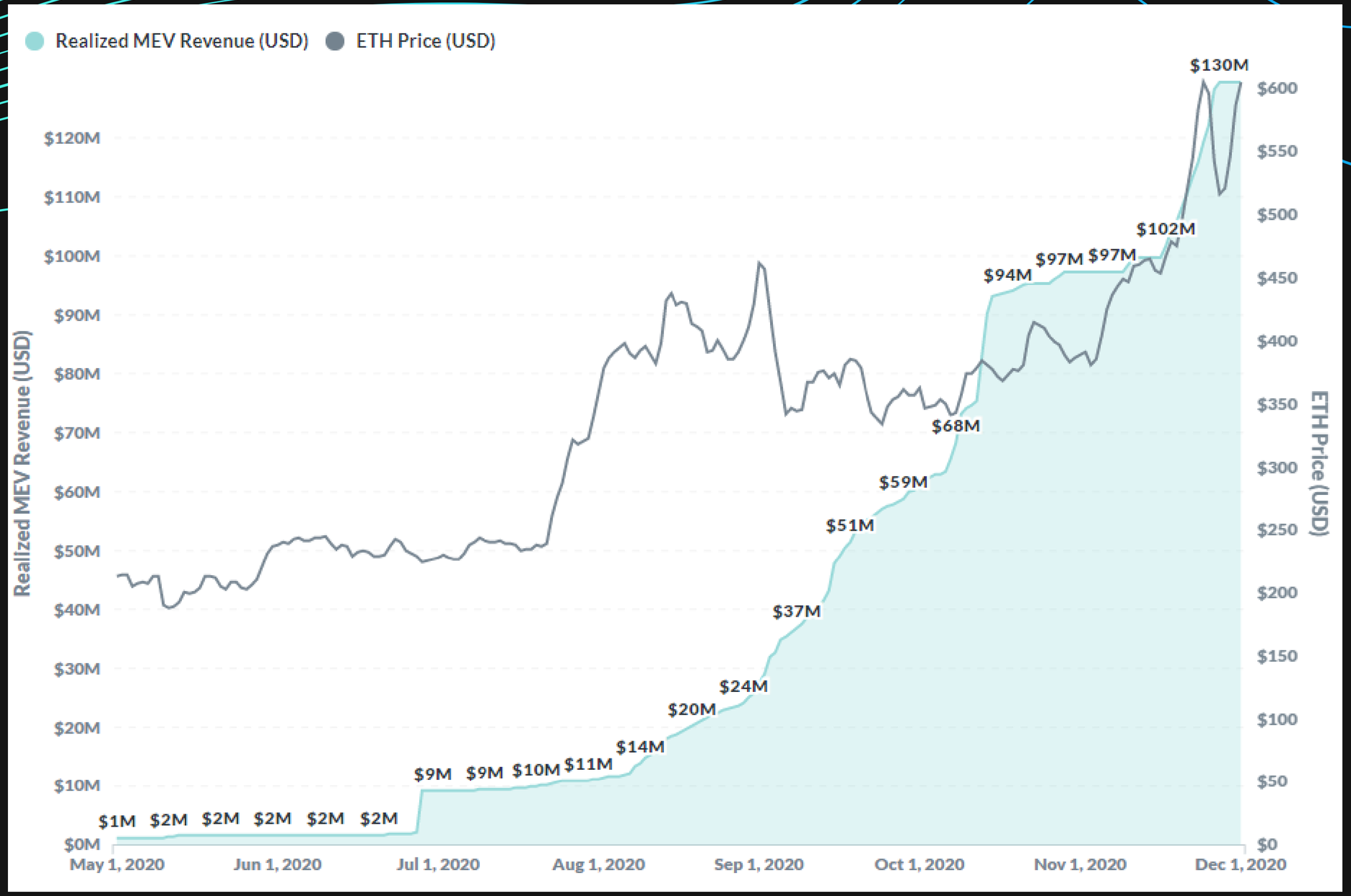
PRIORITY GAS AUCTIONS

which generates

MINER EXTRACTABLE VALUE

which if greater than the block reward can promote

CONSENSUS INSTABILITY

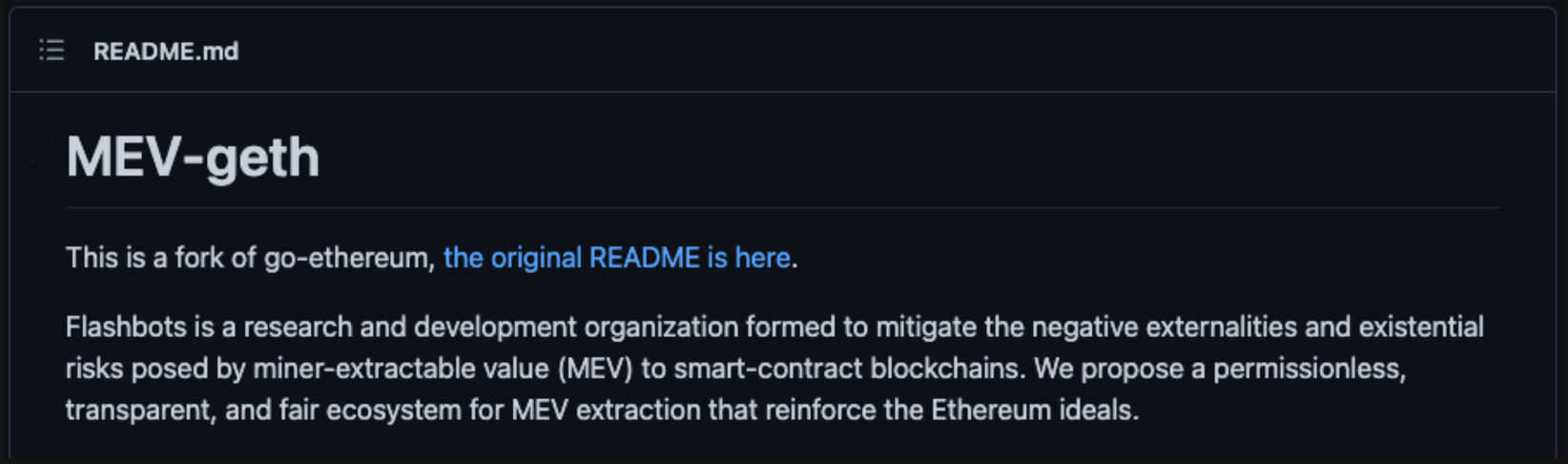


Noyes, C., 2021. MEV and ME. [online] Paradigm Research. Available at: <https://research.paradigm.xyz/MEV>

FLASHBOTS MEV RELAY

Flashbots

A fork of go-ethereum client to allow MEV searchers to directly send their transactions to miners



github.com/flashbots/mev-geth

Other research and developments

MITIGATE MEV

- Design dApps to minimise MEV
  - Network cannot enforce this
- Offer additional security incentives to offset MEV

MAKE FORKING ATTACKS MORE DIFFICULT

- Sepearate the right to include and order blocks to different miners
- Stronger finality garuntees
- Proof-of-stake
- However this just makes forking attacks more difficult

FURTHER READING

- Chainlinks Fair Sequencing Sevice
- Committee driven MEV smoothing

Reference

[1] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L. and Juels, A., 2019. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. arXiv preprint arXiv:1904.05234.

[2] Noyes, C. (2021). MEV and ME. Retrieved 11 May 2022, from https://research.paradigm.xyz/MEV

[3] Liu, Ziyao & Nguyen, Cong & Wang, Wenbo & Niyato, Dusit & Wang, Ping & Liang, Ying-Chang & Kim, Dong In. (2019). A Survey on Applications of Game Theory in Blockchain.

Q & A