# Why you should care about Maximal Extractable Value (MEV)

by Quintus Kilbourn & Alex Obadia (Flashbots)

# Talk Structure

1. what is mev
2. a selection of open problems

before we start..

# background: ethereum & its mempool

Is there a whiteboard I can use? :D

*disclaimer: this is an abstraction of what happens in reality*

# thought experiment

suppose there exists a price imbalance between two exchanges built on Ethereum that is created at block N-1.

after all nodes see block N-1, many actors will act to submit an arb ‘action’ at block N. yet, this opportunity is time-bounded and capacity constrained, there will likely be only one winning arbitrager.

how is the winner decided ❓

# whoever constructs the block! 👷

them and them only decide who wins, as well as deciding none of the participants win but they do by prioritizing their own action.

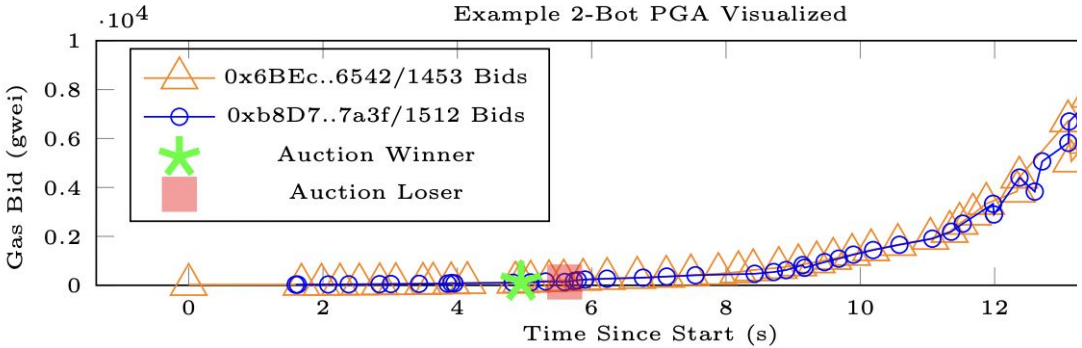
# an early definition - from flashboys 2.0

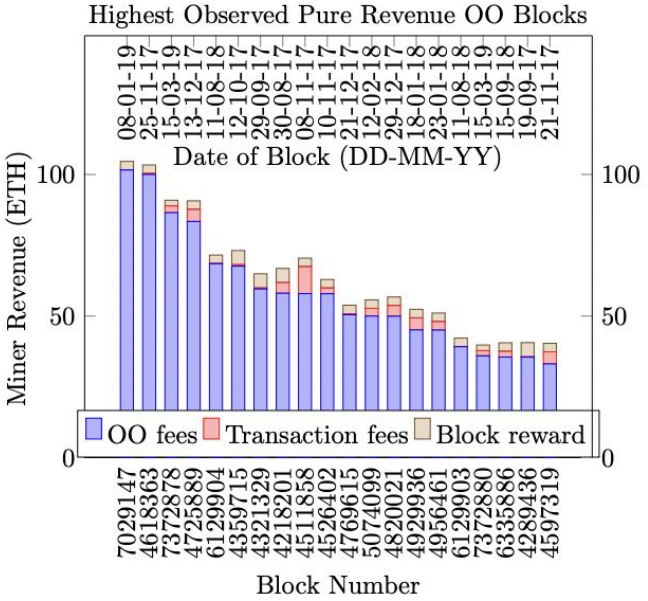
in the past, this entity was the miner ⛏. hence the initial term to describe MEV called 'miner extractable value'. we can generalize ‘ordering fees’ to a broader concept that led to the (initial) definition for MEV:

*Maximal (ex-Miner) Extractable Value is the **total value** that can be extracted from the re-ordering, insertion or censorship of transactions within a given timeframe, which may include multiple blocks worth of transactions.*

# mev, the ecosystem

# before flashbots




| Seconds Elapsed | Quantity @ Price Bid | Ethereum Transaction Origin (Public Key Hash) | Nonce | Transaction Hash |
|---|---|---|---|---|
| 0.000 | 192085 @ 25.10 | 0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542 | 1453 | 0xd32653ca9694a6d1299335f3c04f74cc159bee48c1d32d3a421db08c638ffc78 |
| 1.593 | 231520 @ 25.00 | 0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f | 1512 | 0xb901e6dc2c229fd9105448fcc23eaebdedb476c21b6c6e7ddf8d2df4e838d2c7 |
| 1.624 | 231520 @ 28.75 | 0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f | 1512 | 0x9f592504eb71a7452b7a395a7f5ecd34eaa5d090da1162e74221562af54c8f67 |
| 1.679 | 227534 @ 28.81 | 0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542 | 1453 | 0x83e2a6774654a9540c3fad8837afcc88b4c932ab2374819254f887305c3a4b22 |
| ... | ... | ... | ... | ... |
| 4.949 | 227534 @ 134.02 | 0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542 | 1453 | 0xc889bd13594f75e4dd824f04f0c2ad03896cb7ec6518df02455e9560367bb9c4 |
| 5.599 | 231520 @ 133.76 | 0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f | 1512 | 0xaa86d782328c0c9c422e3f2a3170ff41ae21a27ad395c48db76b0080898f85db |
| ... | ... | ... | ... | ... |
| 13.383 | 227534 @ 5834.77 | 0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542 | 1453 | 0xb0dc97140394c5f65332ebc459d5e66f89099dbb4d335c866b32280270102858 |
| 13.416 | 227534 @ 7716.48 | 0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542 | 1453 | 0x1825be6951577e72a1dafc8de564ce1ccfe5d284173e11e77b2e7f6b1b44571c |
| 13.462 | 231520 @ 7701.08 | 0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f | 1512 | 0xa9823358c99149f0e6343c604c35988468d01d02868437d8251b3cee282dc92b |
| m13.759 | 231520 @ 8856.24 | 0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f | 1512 | 0x366c30a534b5f3d8a6d251f97d401997624d1fe8d3af07ede4d19105dc970942 |

Fig. 2. One example PGA that was observed over the Ethereum peer-to-peer network, resulting from the profit opportunity in Figure 1. The top graph shows the gas bids of two observed bots over time, while the bottom table details the first and last two bids placed by each bot and the two mined bids (center).

# the risk

**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.**

https://arxiv.org/pdf/1904.05234.pdf

# other risks

- state bloat & increased network load
- Increased fees
- Unilateral miner-searcher deals & vertical integration

# enter flashbots

**Frontrunning the MEV crisis**

> *Enter Flashbots*

Flashbots is a research and development organization formed to mitigate the negative externalities and existential risks posed by MEV to smart-contract blockchains. We propose a permissionless, transparent, and fair ecosystem for MEV extraction to preserve the ideals of Ethereum.

Our approach to mitigating the MEV crisis can be broken down into three parts: *Illuminate the Dark Forest*, *Democratize Extraction,* and *Distribute Benefits*. We believe each part is necessary for Flashbots to succeed.

https://medium.com/flashbots/frontrunning-the-mev-crisis-40629a613752

# we

- Democratize:
  - released open source miner software (mev-geth) that created a first price sealed-bid auction between traders & miners. This in turn avoided miners cutting unilateral deals with traders/vertical integration, and isolated this activity to its own lane.
  - Not perfect but twas a first step

- Illuminate:
  - released public dashboards on MEV that quantified it
  - organized lots of events
  - started publishing research on the topic

# industry growth

mev-geth adoption:

January 2021 - 3-4% hashrate

Feb 2021 - 12% hashrate

March 2021 - 58% hashrate

April 2021 - 84% hashrate

https://explore.flashbots.net, data from mev-inspect-py :)

# mev the academic field

Multi-disciplinary field mixing:

- game theory
- security research
- mechanism design
- consensus protocol research
- markets microstructure research

anecdotally, DevCon talks

# so why care?

- Not only is the topic interesting and the industry around it growing extremely rapidely, but also there is so much greenfield research to do.
- the field has many characteristics of a nascent field
    - engineering is driving theory
    - taxonomy is unclear and muddied, no standardization
    - formalizations only starting to exist

- This is a high impact, high leverage burgeoning field, where researchers can have an extremely meaningful influence. in general crypto is a petri dish on steroids for large scale economic experiments.

- ultimately, we believe MEV is fundamental to permissionless systems. Making sure it doesn't destroy them and learning how to harness it will get us closer to unlocking the real potential of this technology -- what trustless scalable economic coordination can provide.

# how do we get there?

maybe this is where you come in? :D

# Open Problems From A User’s Perspective


Searchers watching a
user trade on an AMM

# Open Problems From A User’s Perspective

- Order Flow Auctions

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user
  - Complicated for users

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user
  - Complicated for users
  - General order types

# Open Problems From A User’s Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user
  - Complicated for users
  - General order types
- Privacy

# Open Problems From A User's Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user
  - Complicated for users
  - General order types
- Privacy
  - Preserve properties of underlying system (Ethereum)

# Open Problems From A User's Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user
  - Complicated for users
  - General order types
- Privacy
  - Preserve properties of underlying system (Ethereum)
  - Allow for MEV harnessing

# Open Problems From A User's Perspective

- Order Flow Auctions
  - Decentralised
  - General order types
  - Built on existing system
- Changing Execution Incentives
  - Align incentives of searcher and user
  - Complicated for users
  - General order types
- Privacy
  - Preserve properties of underlying system (Ethereum)
  - Allow for MEV harnessing
- Applications

Reach out!
alex@flashbots.net

# Clockwork Finance: A New Definition

$$\mathrm{EV}(P, \mathcal{B}, s) = \max_{(B_1,\ldots,B_k)\in\mathcal{B}} \left\{ \sum_{a\in A_P} \begin{array}{l} \mathsf{balance}_k(a)[0] \\ -\mathsf{balance}_0(a)[0] \end{array} \right\}.$$

$$k\text{-}\mathrm{MEV}(P, s) = \mathrm{EV}(P, \mathsf{validBlocks}_k(P, s), s).$$

**MEV**: the amount a miner can increase their balance across a series of blocks