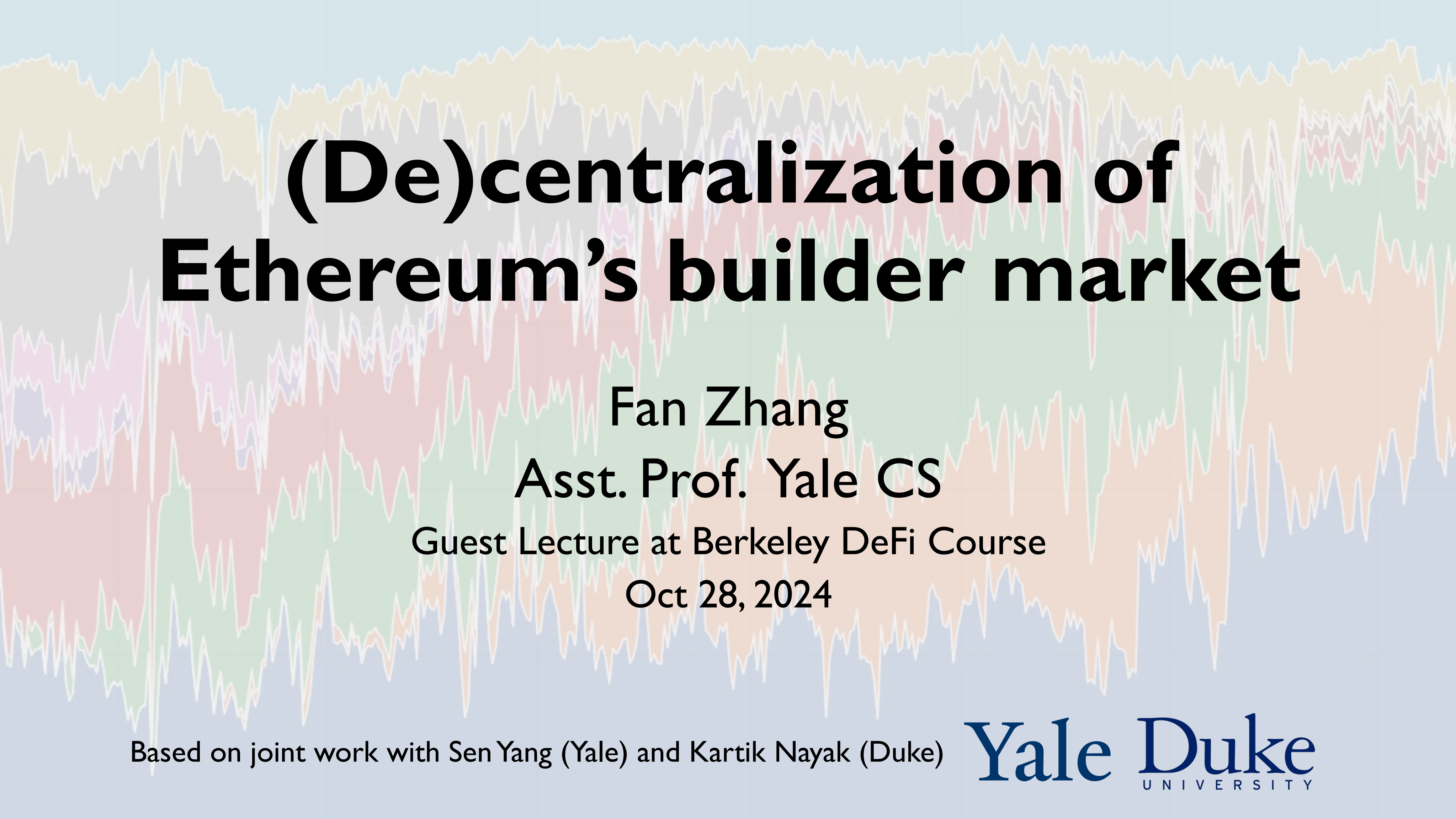


(De)centralization of Ethereum's builder market

Fan Zhang

Asst. Prof. Yale CS

Guest Lecture at Berkeley DeFi Course

Oct 28, 2024

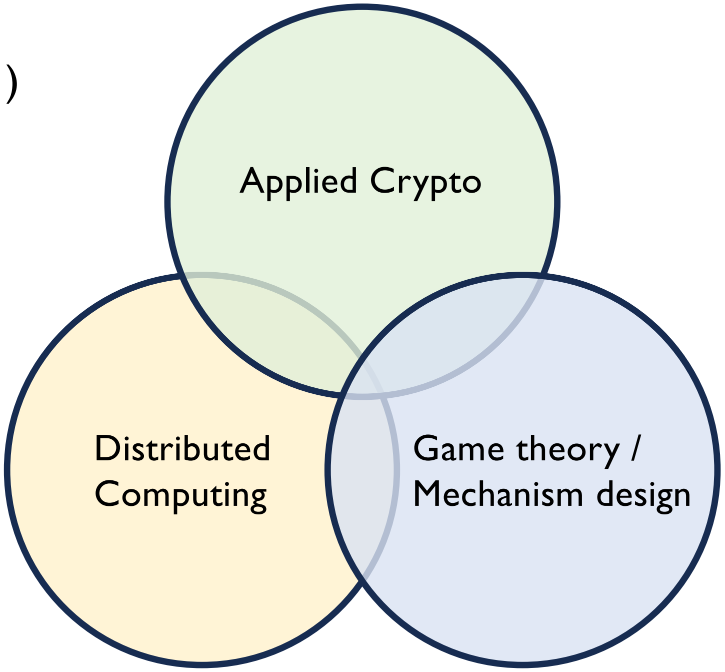
Based on joint work with Sen Yang (Yale) and Kartik Nayak (Duke)

Decentralized Systems Group @ Yale CS

https://www.fanzhang.me/

We work on security and privacy problems in distributed and decentralized systems.

- **Interoperability**
  - b/t web3 systems (CCS'22)
  - b/t web2 and web3 (aka zkTLS) (CCS'16, CCS'21, SP'21)
  - b/t web2 systems (EuroSP'23)
- **Strategic behaviors and mechanism design**
  - Maximal Extractable Values (MEV) (CCS'24)
  - Bribery attacks (NDSS'23)
- **Distributed consensus**
  - Resource efficiency (UseSec'17,'24)
  - Order fairness (CRYPTO'20)
  - TEEs (EuroS&P'19)
- **Anonymity**
  - Anonymous broadcast (PETS'25)
  - Secret single-leader election (SSLE)



MEV: Values gained from ordering manipulation

```
Alice: sell @ $90
Adv  :  buy @ $90
Bob  :  buy @ $100
Adv  : sell @ $100
```

Frontrunning attack

Bob	-10
Adv	**+10**

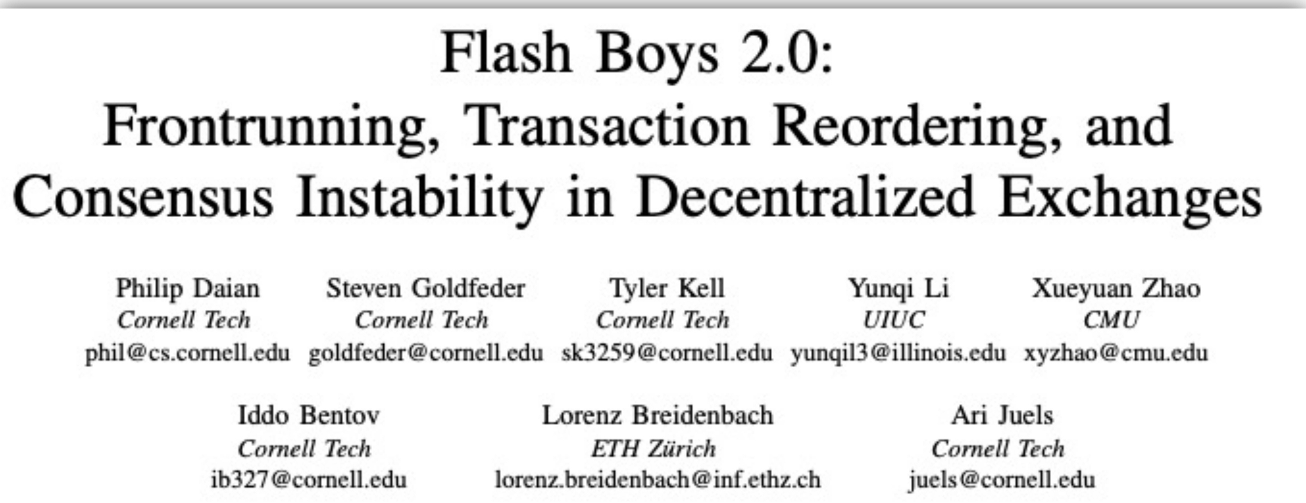
Adv “extracted” $10 by ordering txns cleverly

- Who can do this?
- In TradFi, HFT firms gain timing advantage through co-location, low-latency networks, etc

Blockchain is supposedly much better, but not really: miners/validators *dictate* transaction ordering!

MEV

- **Miner/Maximal Extractable Value** (MEV) refers to the profits gained from manipulating the ordering of transactions
  - First studied in Daian et al ('19)



Flash Boys 2.0:
Frontrunning, Transaction Reordering, and
Consensus Instability in Decentralized Exchanges

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

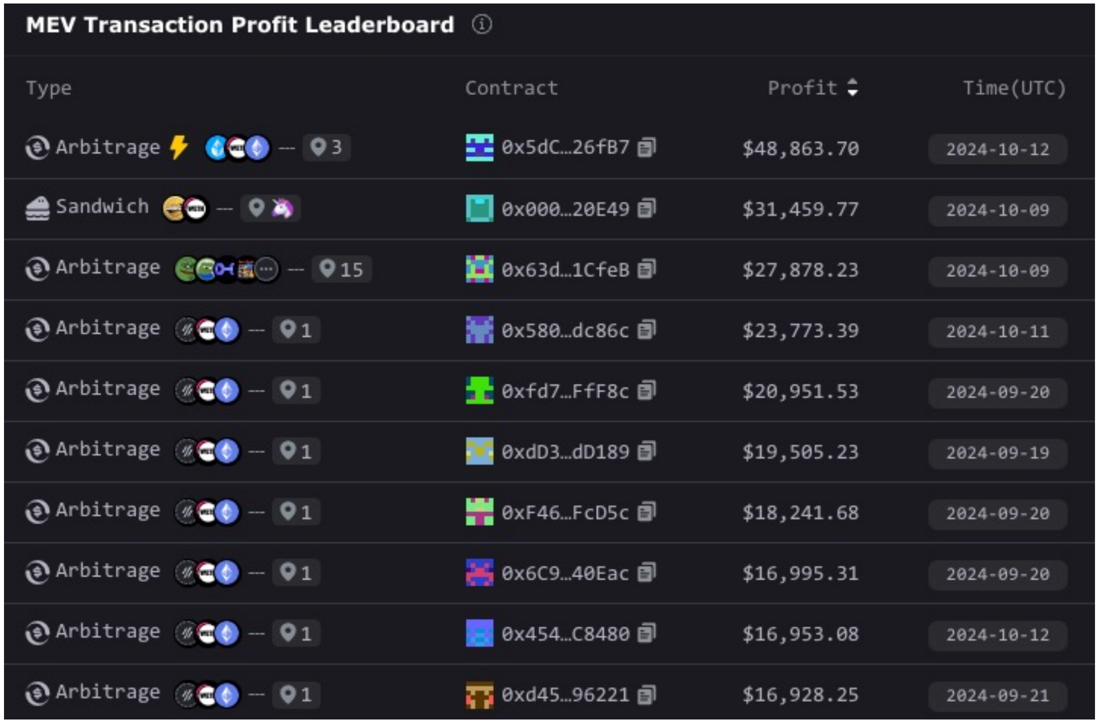
Xueyuan Zhao
CMU
xyzhao@cmu.edu

Iddo Bentov
Cornell Tech
ib327@cornell.edu

Lorenz Breidenbach
ETH Zürich
lorenz.breidenbach@inf.ethz.ch

Ari Juels
Cornell Tech
juels@cornell.edu

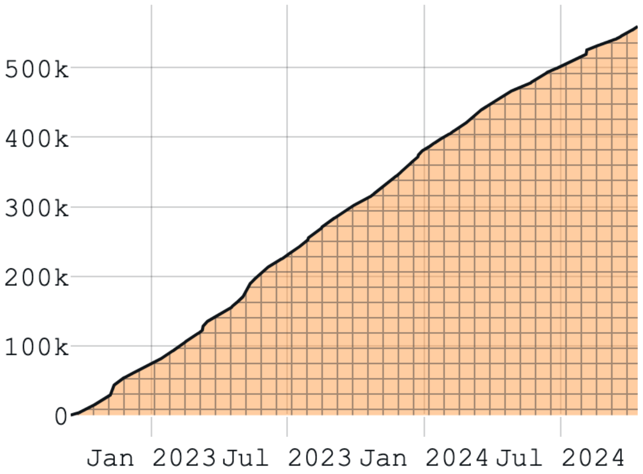
We are talking about a lot of money



MEV Transaction Profit Leaderboard ⓘ

Type	Contract	Profit	Time(UTC)
Arbitrage ⚡ — 3	0x5dC…26fB7	$48,863.70	2024-10-12
Sandwich —	0x000…20E49	$31,459.77	2024-10-09
Arbitrage — 15	0x63d…1CfeB	$27,878.23	2024-10-09
Arbitrage — 1	0x580…dc86c	$23,773.39	2024-10-11
Arbitrage — 1	0xfd7…FfF8c	$20,951.53	2024-09-20
Arbitrage — 1	0xdD3…dD189	$19,505.23	2024-09-19
Arbitrage — 1	0xF46…FcD5c	$18,241.68	2024-09-20
Arbitrage — 1	0x6C9…40Eac	$16,995.31	2024-09-20
Arbitrage — 1	0x454…C8480	$16,953.08	2024-10-12
Arbitrage — 1	0xd45…96221	$16,928.25	2024-09-21

Total MEV distributed through MEV-Boost (in ETH)

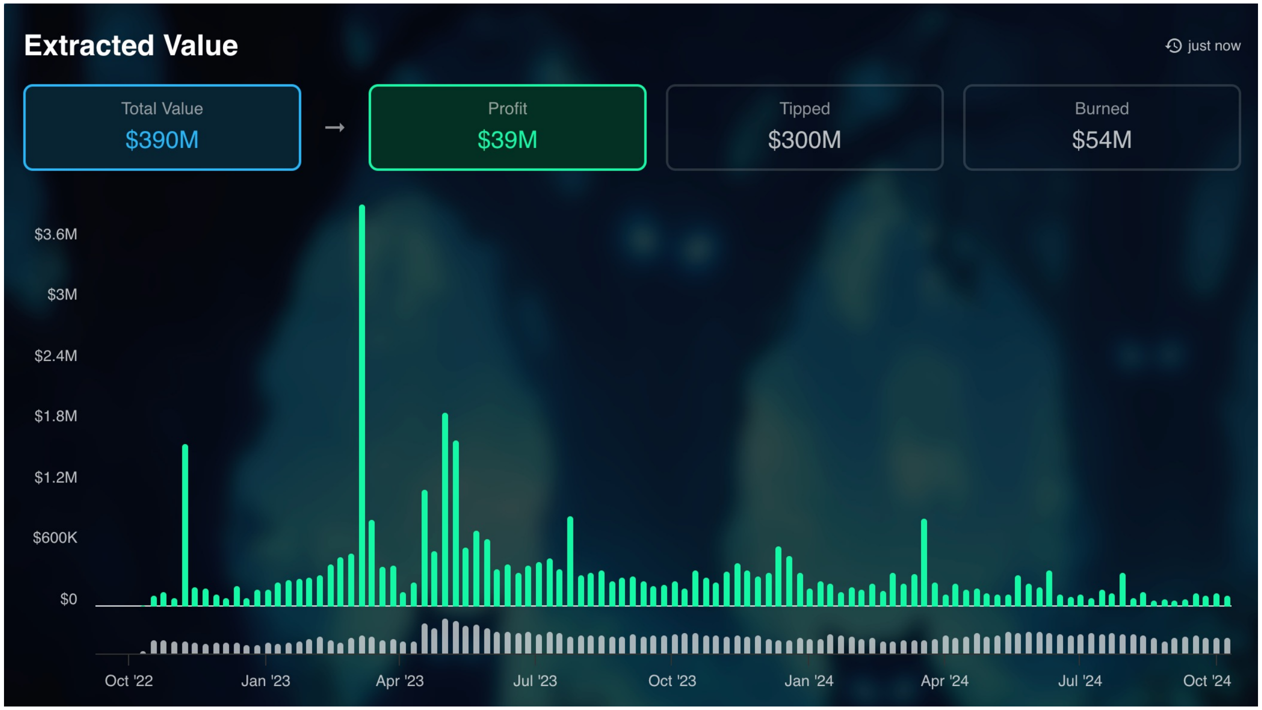


Over **550K ETH (~$1.3B)** has been extracted on Ethereum!

Why should we care?

1. User loss

Some MEV extraction directly causes users to lose money.



For example, the total revenue of **sandwich attacks** is ***$390M*** since the Merge.

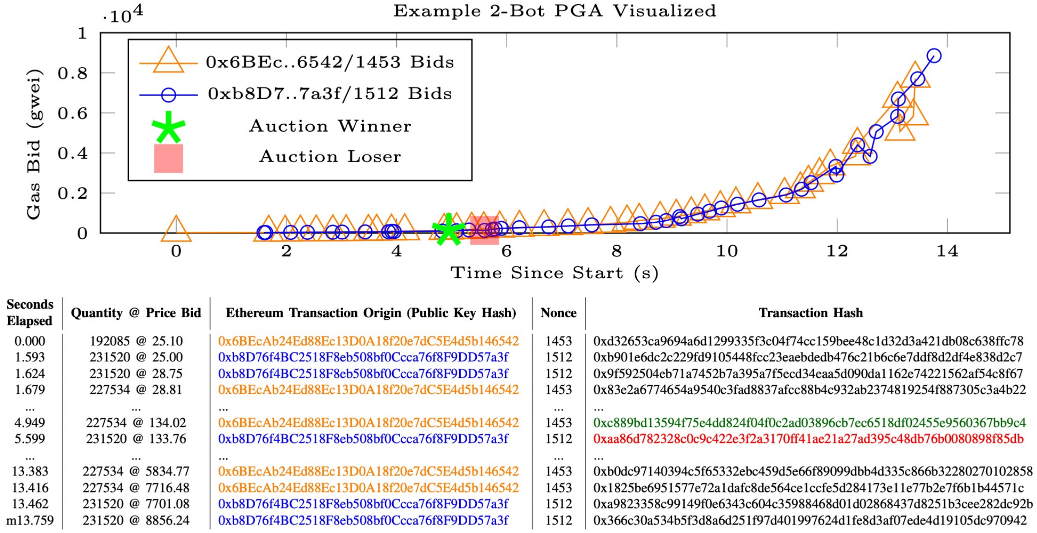
-- This is at the expense of the victims.

Data source: libmev.com

2. Inefficiency

Inefficiency due to the lack of coordination:

- For example, MEV searchers compete for MEV opportunity in on-chain bidding wars, which can cause network congestion.
- The example from Flash Boy 2.0 paper.

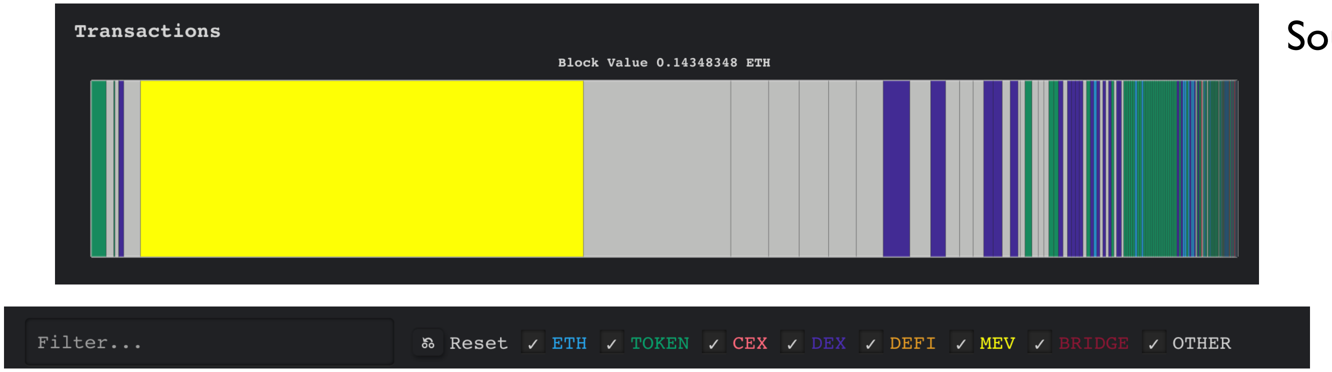


Seconds Elapsed	Quantity @ Price Bid	Ethereum Transaction Origin (Public Key Hash)	Nonce	Transaction Hash
0.000	192085 @ 25.10	0x6BEcAb24Ed88Ec13D0A18f20e7dC5E4d5b146542	1453	0xd32653ca9694a6d1299335f3c04f74cc159bee48c1d32d3a421db08c638ffc78
1.593	231520 @ 25.00	0xb8D76f4BC2518F8eb508bf0Ccca76f8F9DD57a3f	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).

3. Consensus instability

- MEV extraction already dominates block rewards in Ethereum today.
  - For example, one MEV transaction contributes 1/3 of block profit in a recent block (20964474).

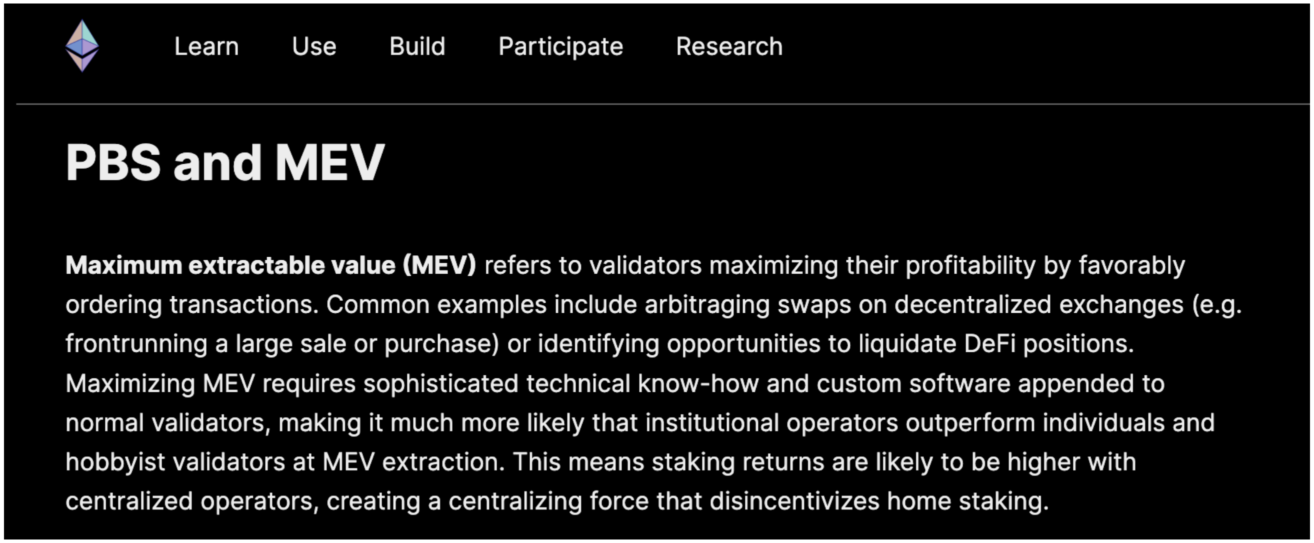


Source: payload.de

  - Miners may deviate from honest mining and fork out high-fee blocks to attract other miners to build on the fork (**time-bandit attacks**).

4. MEV is a centralizing force

- MEV extraction requires resources.
- In Ethereum PoS, big validators (e.g., backed by trading firms) will outcompete small validators (e.g., home stakers)



PBS and MEV

Maximum extractable value (MEV) refers to validators maximizing their profitability by favorably ordering transactions. Common examples include arbitraging swaps on decentralized exchanges (e.g. frontrunning a large sale or purchase) or identifying opportunities to liquidate DeFi positions. Maximizing MEV requires sophisticated technical know-how and custom software appended to normal validators, making it much more likely that institutional operators outperform individuals and hobbyist validators at MEV extraction. This means staking returns are likely to be higher with centralized operators, creating a centralizing force that disincentivizes home staking.

Validators will be centralized as smaller ones are driven out of the market!

Source: Ethereum

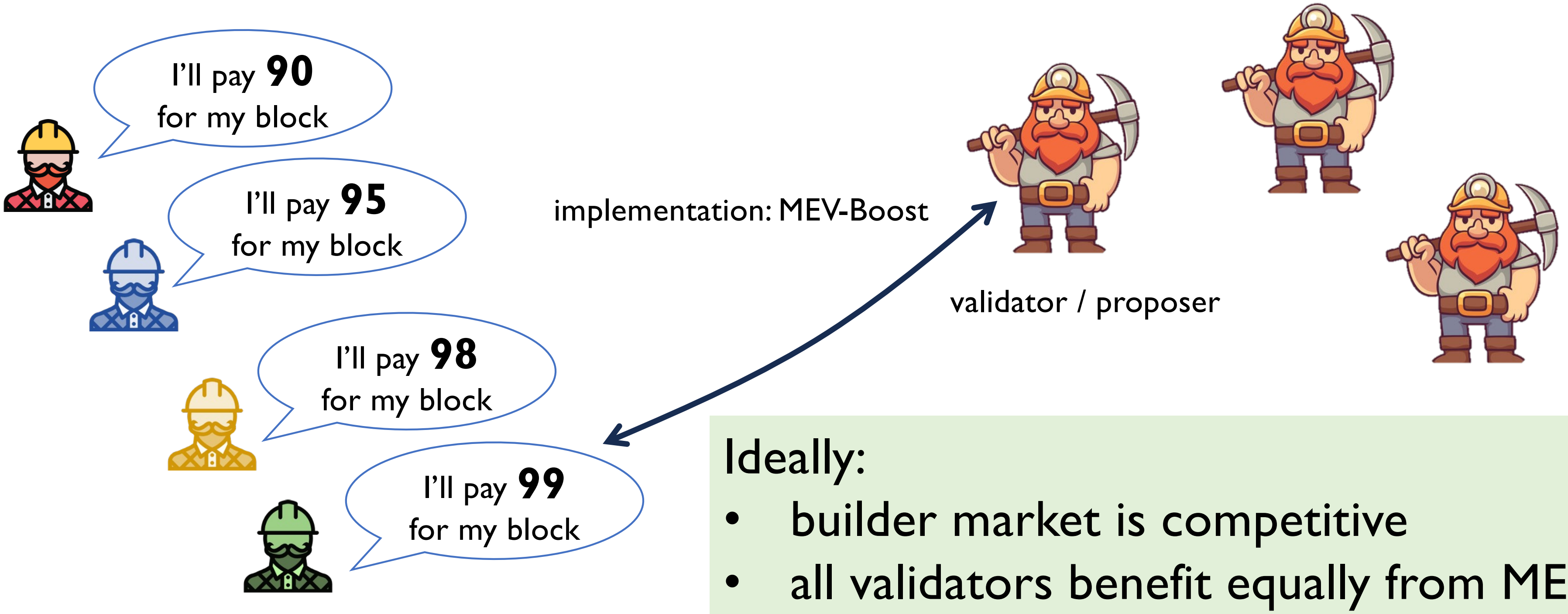
Proposed solutions

- First-come-first-served ordering (e.g., Aequitas (CRYPTO'20))
  - Relies on honesty assumptions (i.e., not working in rational model)
  - Can lead to latency war
- Blind ordering (e.g., Shutter Network)
  - Relies on honesty assumptions (we showed a fix in AnimaguSwap (CCS'24))
- MEV auctions: auction off the rights to extract MEV, and re-distribute MEV "in some good ways"
  - Ethereum's solution: Proposer-builder separation (PBS)

For more, see, e.g., SoK: MEV Countermeasures: Theory and Practice (Yang et al, 2022)

PBS and builder market

- Idea: allow outsourcing of block building (i.e., MEV extraction) to builder market.

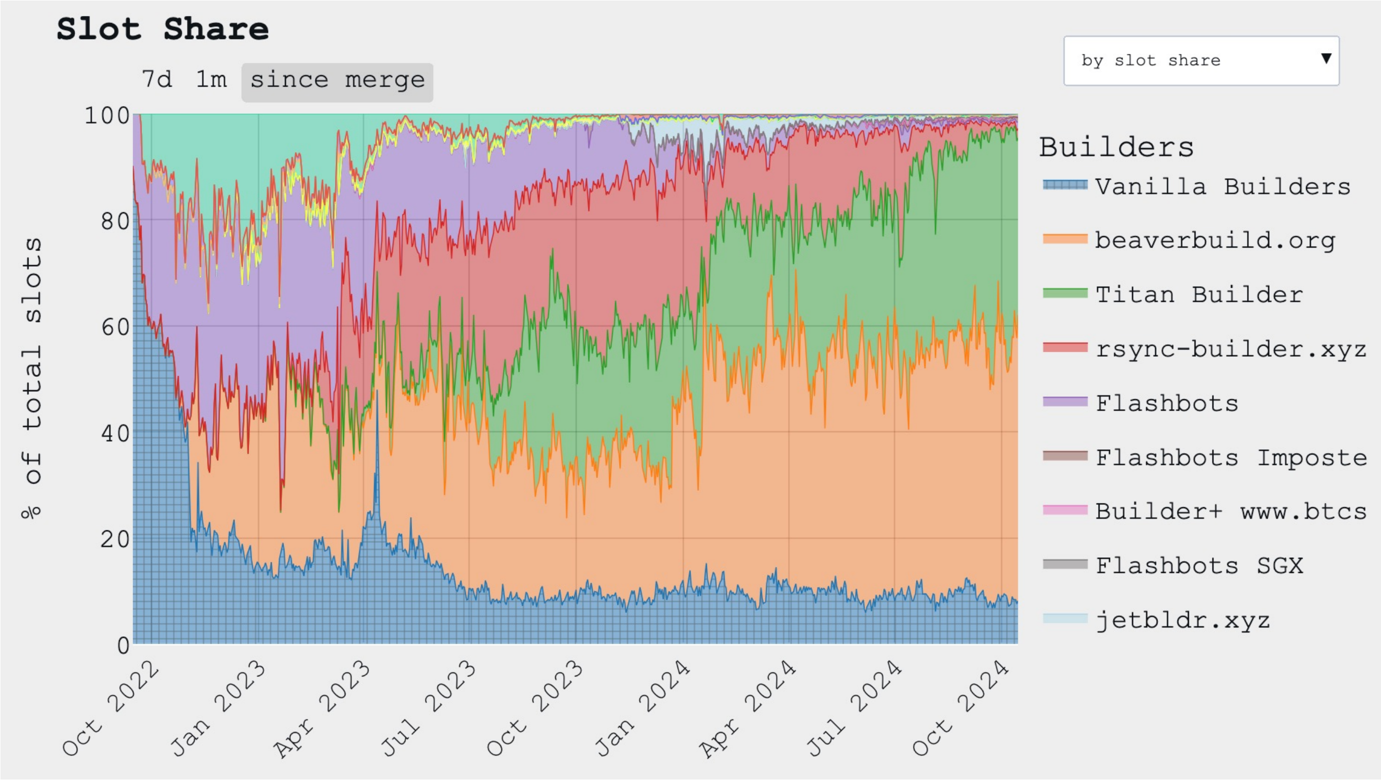

I'll pay **90** for my block
I'll pay **95** for my block
I'll pay **98** for my block
I'll pay **99** for my block
implementation: MEV-Boost
validator / proposer

New player: Builders

Ideally:

- builder market is competitive
- all validators benefit equally from MEV

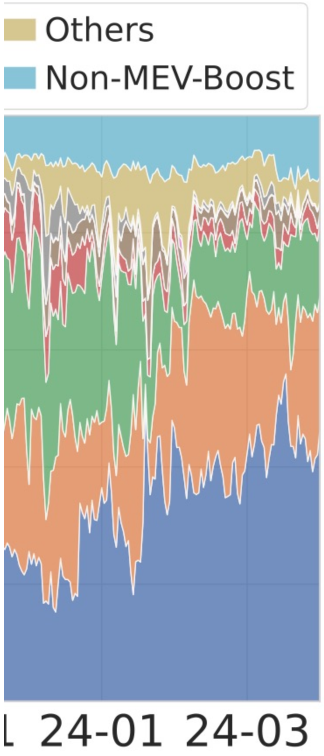
Market share of Ethereum's builders market



<u>Top-two</u> builders build ~87% blocks as of Oct 2024.

https://mevboost.pics/

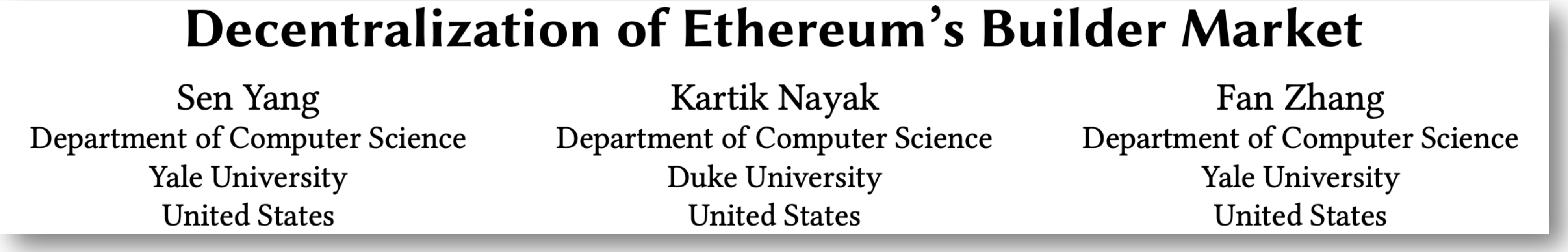
Is centralized block building okay?



- Popular opinion is "*yes, it's okay.*"
  - "centralized block production is fine as long as [validators are decentralized]" --- ethereum.org
- We want to provide a different view:
  - Concern: proposers would incur a ***profit loss*** in a centralized builder market.
  - Proposer loss has ***undesired consequences***.

Implications of proposer loss

- #1: Instability of PBS
  - Proposers might be incentivized to extract MEV themselves.
  - Big validators have competitive advantages or small ones, leading to validator centralization.
- #2: inaccurate MEV oracles
  - Auctions are used to measure MEV (MEV oracles) (e.g., MEV burn).
  - proposer loss ⟹ inaccurate MEV oracles
- Our work: quantify the loss, understand its causes, and explore mitigation.



Decentralization of Ethereum's Builder Market

Sen Yang
Department of Computer Science
Yale University
United States

Kartik Nayak
Department of Computer Science
Duke University
United States

Fan Zhang
Department of Computer Science
Yale University
United States

Modeling MEV Auctions

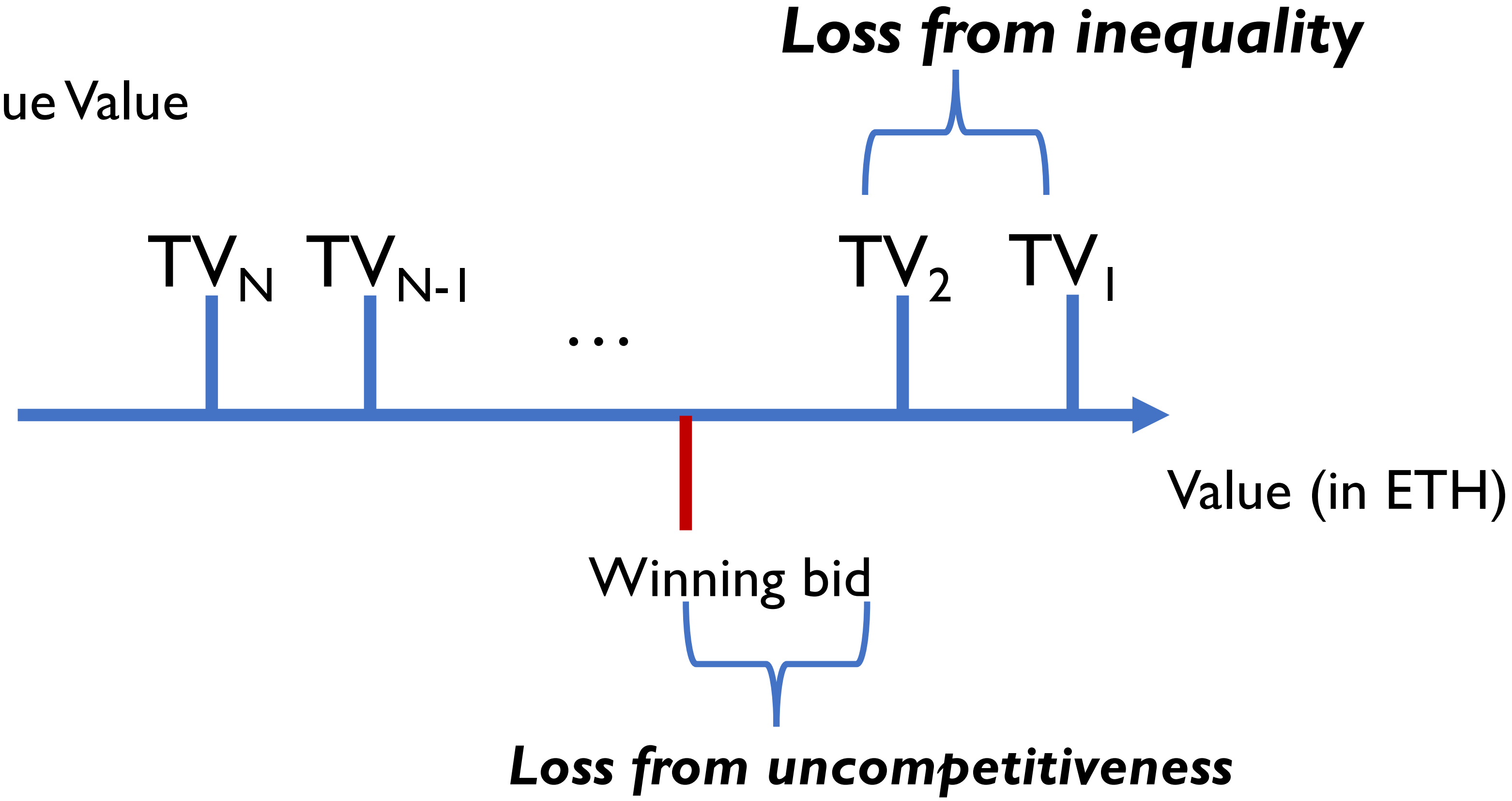
- In each instance, builders submit bids in the form of (B, BV)
  - B: a block
  - BV: amount to pay if bid is accepted
- Open bid, akin to an English auction
- Builder's **<u>true valuation (TV)</u> underlying a bid B :=** balance increase after executing B
  - i.e., TV(B) is the sum of values from txns in B
- When auction concludes, B with the highest BV wins.
  - Block B is added to the blockchain
  - Builder of B gets TV
  - Builder pays the proposer BV
- Builder's profit = TV – BV

Potential reasons for proposer loss

- **1) Does the mechanism incentivize competition?**
  - Reasons for yes: MEV boost auction is akin to an English auction
  - Reasons for no: Fixed deadline may not allow full competition. Builders may collude.
- **2) Do builders have similar block-building capacity (BBC)?**
  - Alice extracts 100 ETH, Bob extracts 10 ETH, Charlie extracts 9.5 ETH. Assuming competitive auctions, auction revenue is $10 + \epsilon$ (far from 100)
  - i.e., Proposer can get up to 90 ETH more if they build blocks.
- They lead to two types of loss: 1) **Loss from uncompetitiveness**, and 2) **loss from inequality**

Proposer loss definition

TV = True Value

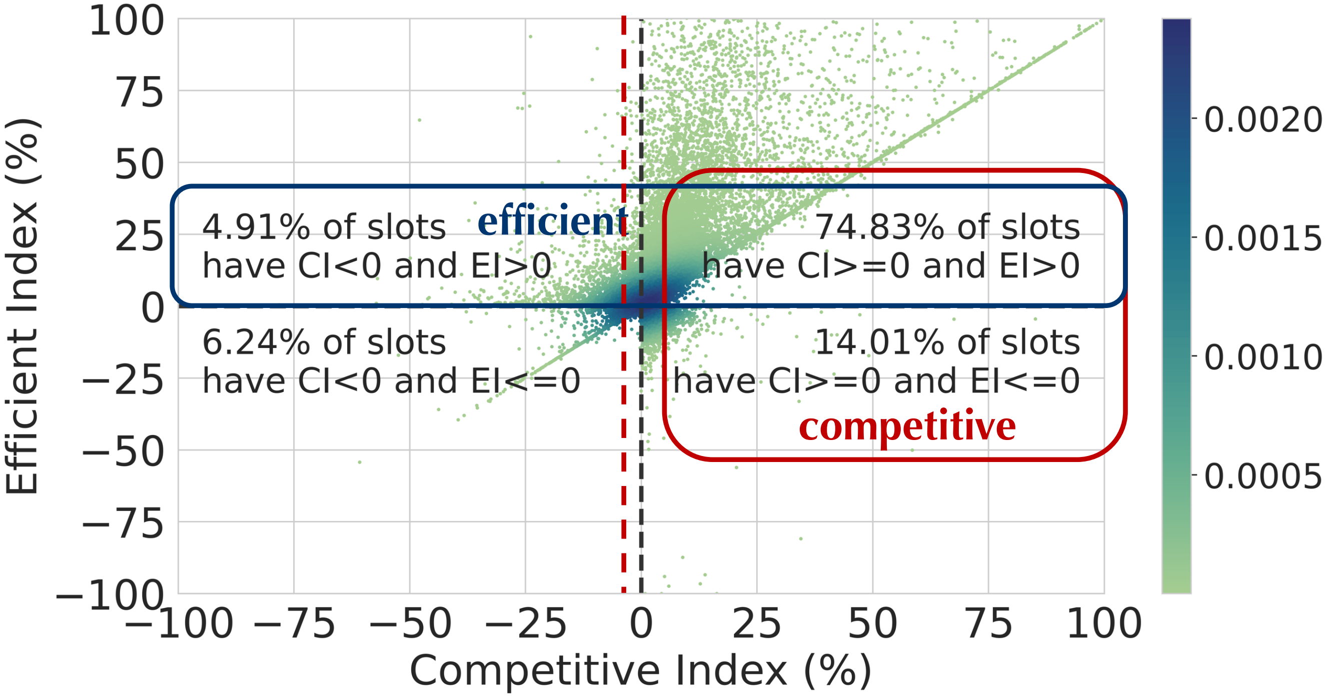


Quantification of proposer losses

- Practical challenge: auction data is not recorded on-chain
  - Blockchain only records the winning bids. We need losing bids too.
- We started to archive auction bids since 2022
  - 5 billion partial bids (block hash, bid) since Sep 2022 to March 2024 (collected by querying relays)
  - full bids (partial bids + txns) from ultra sound relay (200 GB / day)
- cross validation against public datasets & related papers

Result: competitiveness of past MEV auctions

- **Competitive := winning bid > second highest true value**
- **Efficient := winner has the highest TV**

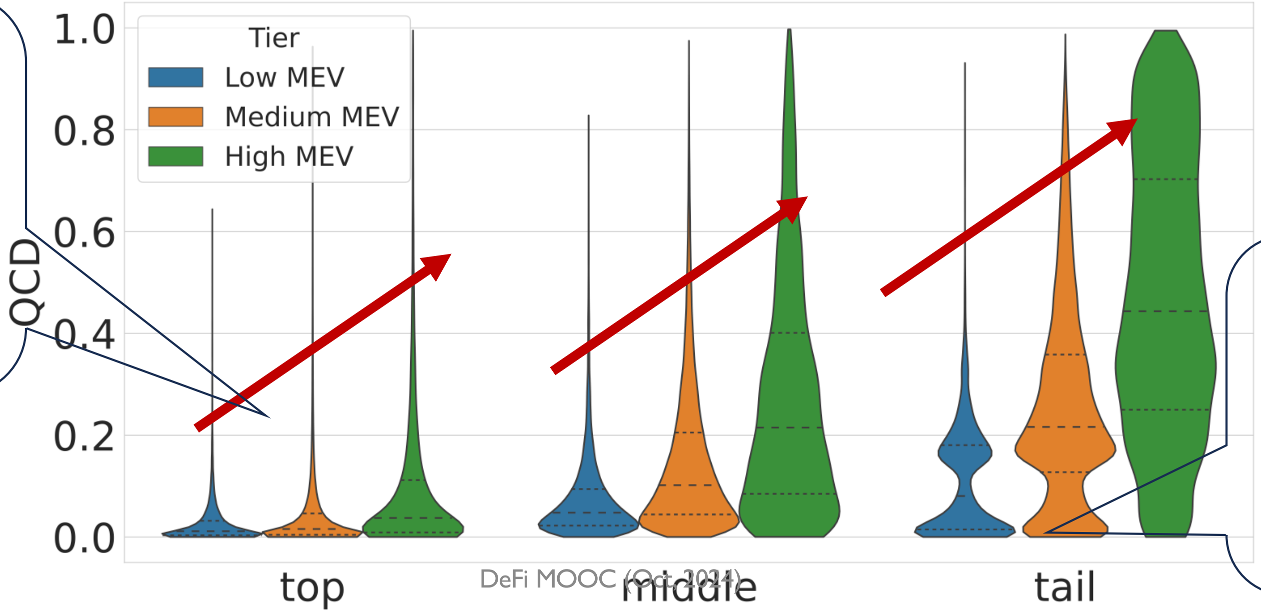


- Examined auctions from April 9-15, May 1-7, June 1-7, July 1-7, and August 1-7, 2023
- Competitive: 89%
- Efficient: 80%
- Both: 75%

Result: Inequality of block-building capacity

- **Builder's true valuable** represents its **block-building capability**
- We use Quartile coefficient of dispersion (QCD) to measure the disparity of true values (**the higher the worse**)

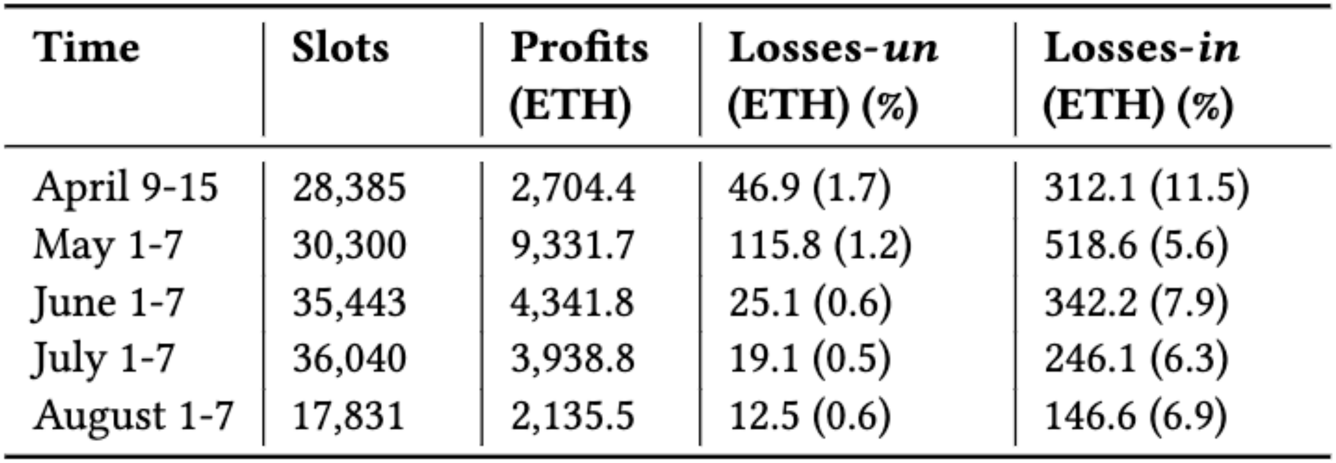
- Top builders have similar capability in low MEV slots.
- Inequality worsens as the MEV of a slot increases.



Inequality worsens as we go down the list of builder groups.

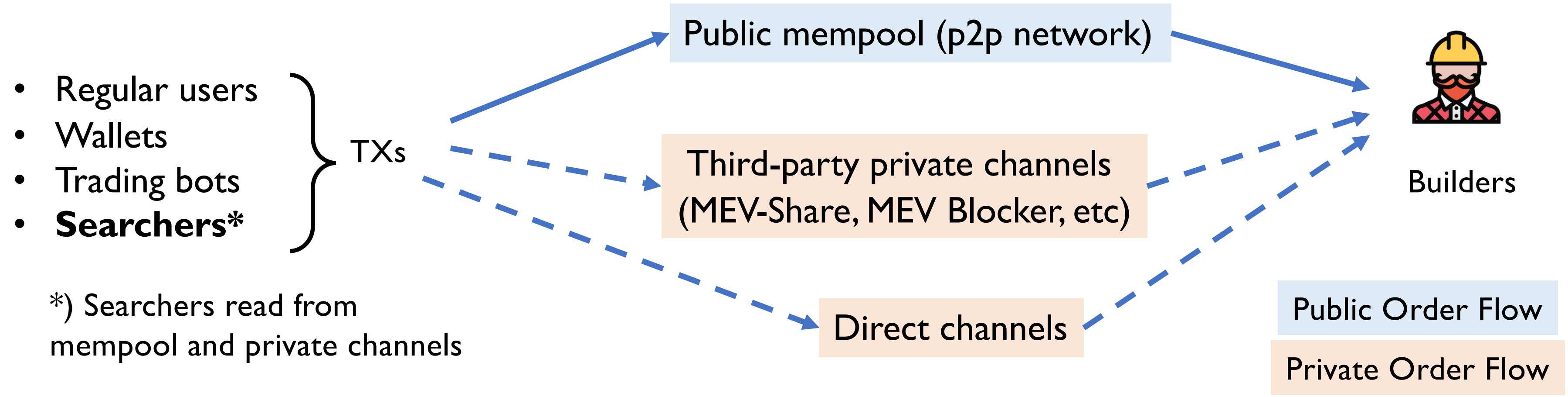
Result: proposer loss in past auctions

- Between April – August 2013:
- Loss from uncompetitiveness is moderate (~1%)
- Loss from inequality (of BBC) is more significant (6-12%)



Time	Slots	Profits (ETH)	Losses-*un* (ETH) (%)	Losses-*in* (ETH) (%)
April 9-15	28,385	2,704.4	46.9 (1.7)	312.1 (11.5)
May 1-7	30,300	9,331.7	115.8 (1.2)	518.6 (5.6)
June 1-7	35,443	4,341.8	25.1 (0.6)	342.2 (7.9)
July 1-7	36,040	3,938.8	19.1 (0.5)	246.1 (6.3)
August 1-7	17,831	2,135.5	12.5 (0.6)	146.6 (6.9)

What accounts for builder’s inequality?



- Regular users
- Wallets
- Trading bots
- **Searchers***

TXs

Public mempool (p2p network)

Third-party private channels (MEV-Share, MEV Blocker, etc)

Direct channels

Builders

Public Order Flow

Private Order Flow

*) Searchers read from mempool and private channels

- A stream of TXs is called an <u>order flow (OF)</u>
- Public OF (primarily the mempool) is accessible by all builders.
- Private OFs, well, are private.
- Which is more important?

More than 80% of MEV is from private OFs

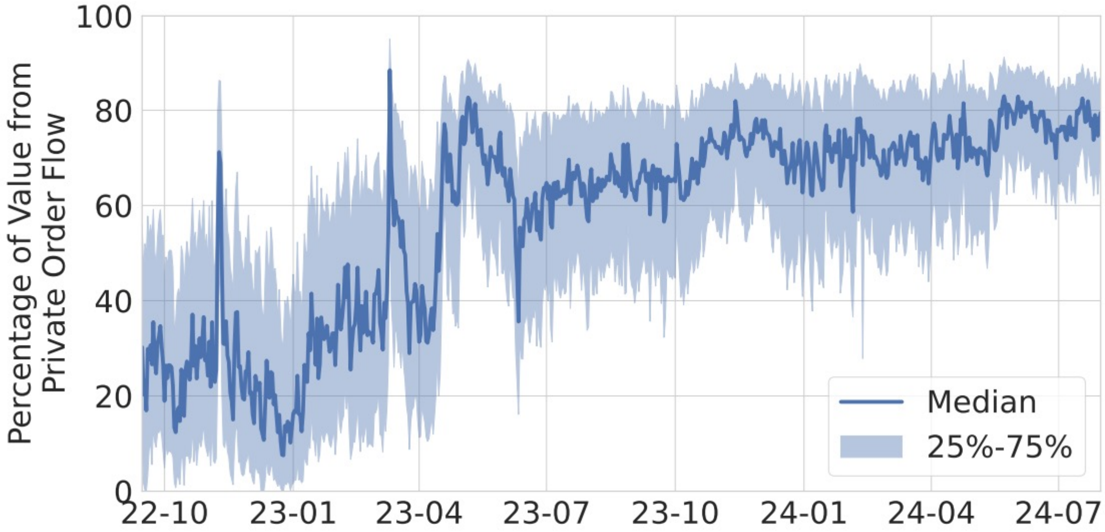


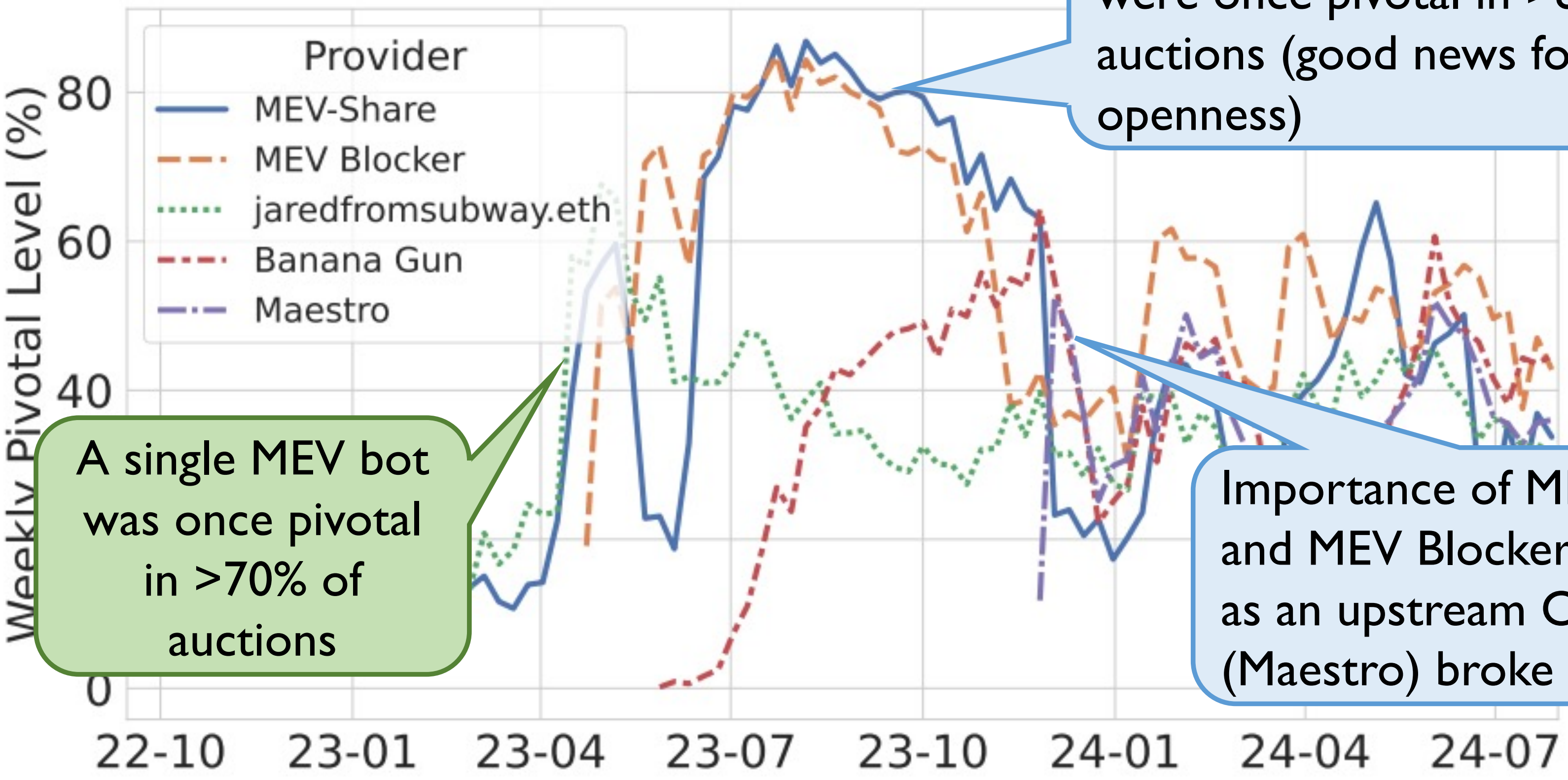
Figure 7: Fraction of builder income from private order flows.

- To win auctions, builders *need* private OFs.
- Where do they get private OFs?
- How equal/inequal are builders' abilities to access good private OFs?

Identifying pivotal private OFs using data

- We define an order flow OF to be ***pivotal*** for an auction if the winner would have lost without txns from OF.
  - I.e., pivotal OFs are necessary to win
- Next slide: We identified five OFs were pivotal in >50% auctions over a period longer than two weeks (i.e., they had sustained impact)
  - If a builder cannot access any of these OFs, it will lose the majority of the auctions!

Identify pivotal order flows using data

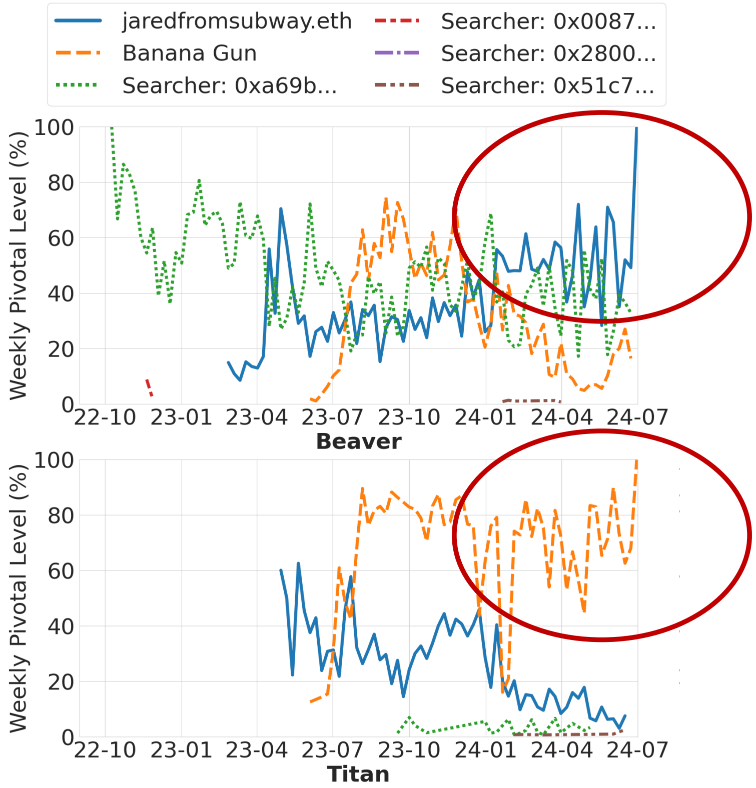


MEV-Share and MEV Blocker were once pivotal in >80% of auctions (good news for openness)

A single MEV bot was once pivotal in >70% of auctions

Importance of MEV-Share and MEV Blocker declined as an upstream OF (Maestro) broke away.

Builder-specific pivotal level



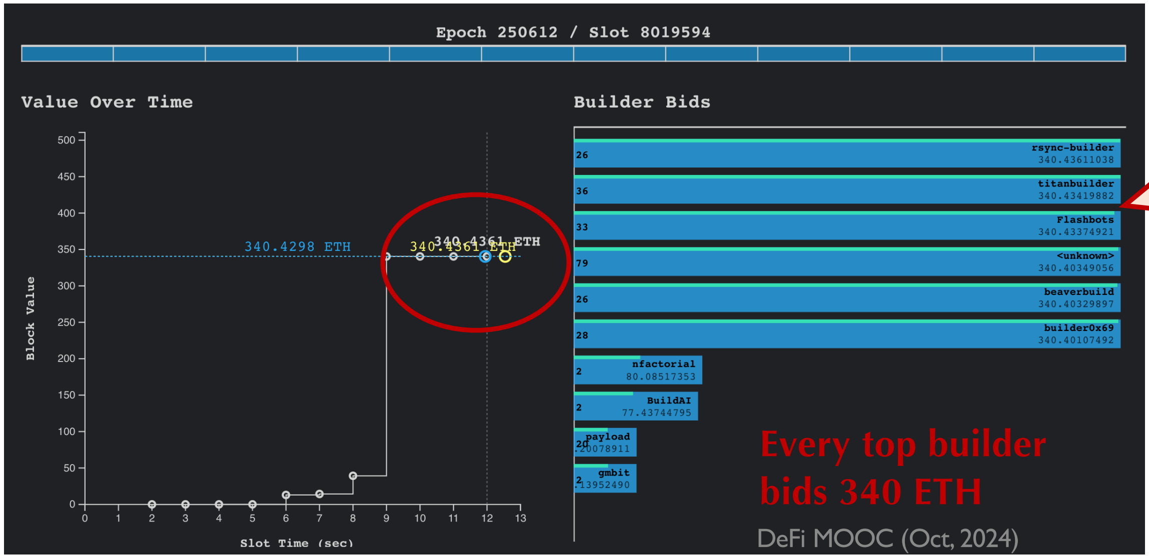
- Pivotal level for top-2 builders
  (focusing on the blocks those bid value > 1ETH)
- Strong signal for *exclusive OFs* between Banana Gun <> Titan, jaredfromsubway <> Beaver.
- Exclusivity can cause inequality.

How integration affects auctions?

- All three top builders [> 90% market share collectively] have exclusive OF providers.
  - Revealed unknown integration between Banana Gun (a telegram bot) and Titan, jaredfromsubway (a sandwich searcher) and Beaver.
- Main concerns: i) it prevents competition; ii) there is ***strong incentive*** to form integration.

Example: Incentive for integration

- For example, in slot 8019594, about 340 ETH came from Banana Gun (OF), and all 340 ETH was captured by the proposer.

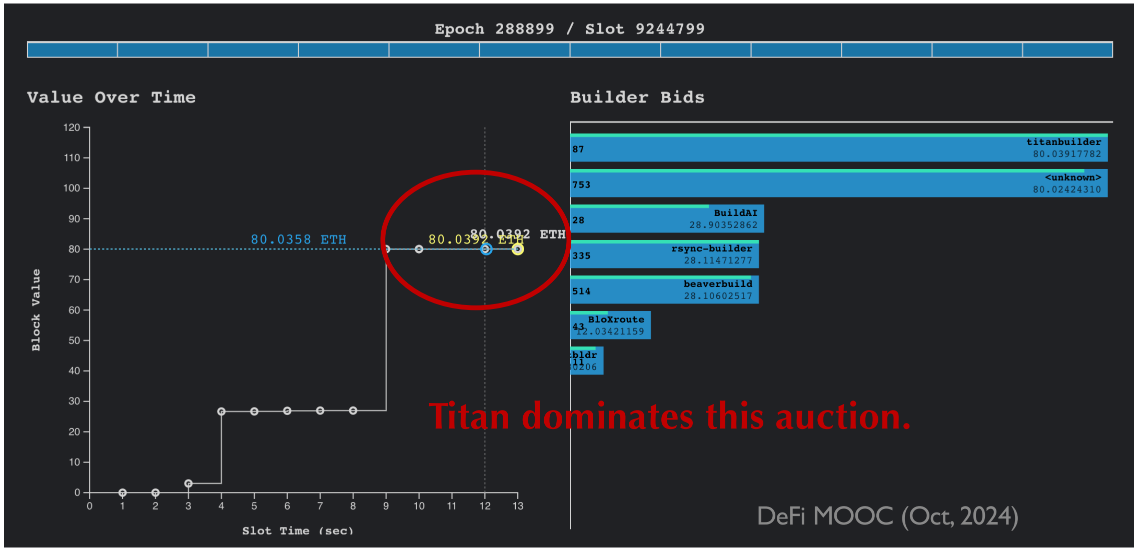


Every top builder bids 340 ETH

Multiple builders bid 340 ETH.

Example: Incentive for integration

- With integration, more **MEV "escapes" the protocol**
- E.g., Top 3 builders (all with integrated OFs) made $5.5M in the first of week of June 2024!



Titan dominates this auction.

In slot 9244799, 208 ETH came from Banana Gun, and only Titan received it. Titan paid 80 ETH to the proposer.

128 ETH can be shared between Banana Gun and Titan!

Status Quo

Where we are today:

- Two builders build >87% blocks in Ethereum
- Last week: PBS distributed ~1000 ETH to Titan, ~500 ETH to Beaverbuild [1]; All proposers together received ~4000 ETH [2]
- Losses mainly stem from exclusive OFs

How did we get here:

- Builders compete on two dimensions simultaneously: *MEV-carrying txns* and *extraction algorithms*.
- Builders cut closed-door deals to get *exclusive access* to the former.
- Without the former, the latter doesn't matter.

[1]: https://www.relayscan.io/builder-profit
[2] https://mevboost.pics

Paths forward?

Can new builders join to increase competition?

- Unlikely. There is strong incentive for existing OFs to not work with new builders.
- Also trust barriers

Is PBS stable in the long term?

- A proposer with large stake should think about exiting from PBS.
- Doesn't seem hard to do: much of builder's job is to simply *collect* transactions.
- E.g., BTCS recently started a builder (We don't know why.)
- Other changes might affect PBS too, such as app-level MEV redistribution.

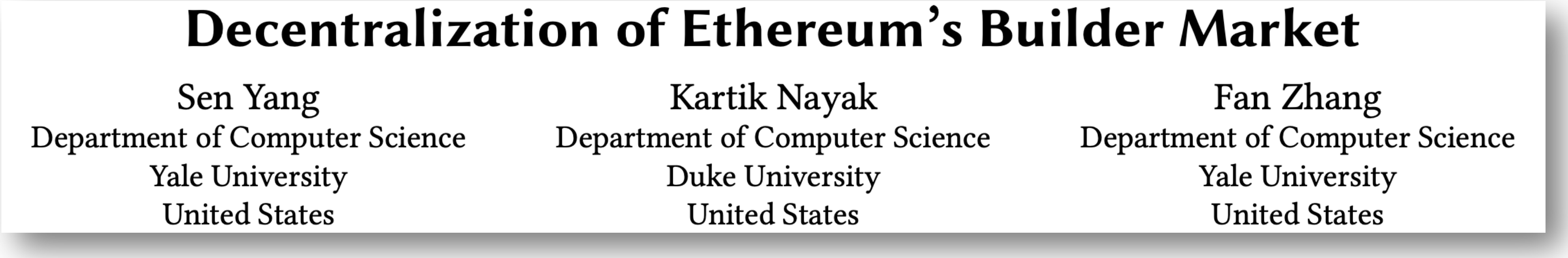
Not obvious how to avoid builder centralization.

Other problems caused by a centralized builder market

- Censorship by builders
  - A malicious builder may refuse censor transactions to exit from CDP for higher gain in liquidation
- Builder frontrunning
  - Builders see all transactions
  - If you don’t like Titan or Beaverbuild, you need to wait ~8x longer
- Builder boycotts
  - If builders doesn’t like certain protocols (e.g., those reducing their profits), they can block them.

Open challenges

- How to mitigate the negative impacts of integration?
  - Execution Auctions, PROF, etc, do not directly address this problem.
- How should MEV be allocated between users, searchers, builders, proposers?
- Immediate problems like builder censorship resistance



Decentralization of Ethereum's Builder Market

Sen Yang
Department of Computer Science
Yale University
United States

Kartik Nayak
Department of Computer Science
Duke University
United States

Fan Zhang
Department of Computer Science
Yale University
United States

Blog post: https://decentralizedthoughts.github.io/2024-05-07-decentralization-ethereum/

Paper: https://arxiv.org/pdf/2405.01329

X: 0xfanzhang