Maximal Extractable Value

Slides from Dan Boneh and Chris Meisl (see this)

Decentralized Finance (DeFi)

- **Permissionless**: any financial instrument can be implemented and deployed with a few lines of Solidity code

(a centralized system could refuse to deploy a competing service)

- **Transparent**: Dapp code and Dapp state are public

  $\Longrightarrow$ Anyone can inspect and verify

- **Composable**: Dapps can call one another

  ERC-20 standard enables interoperability (6 functions)

Why DeFi? Failures of the existing financial system

- **Cross border inefficiency**:

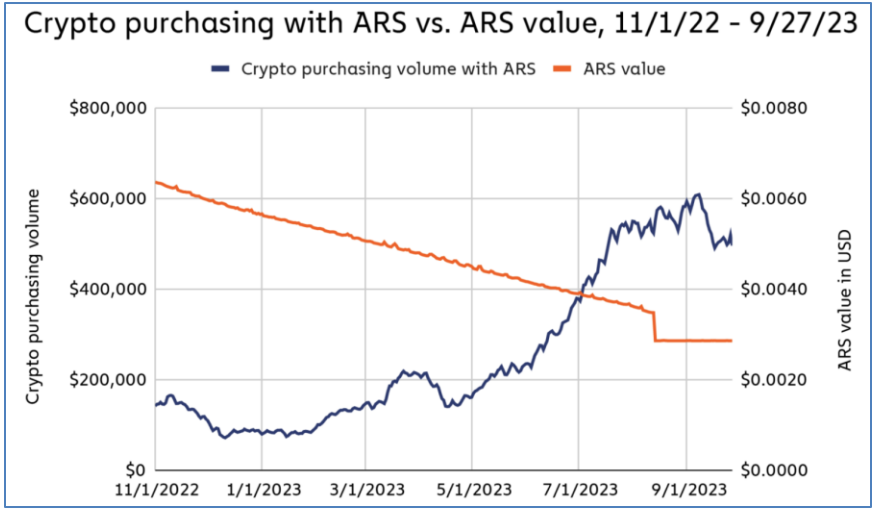
  send $10 to South America ⇒ 36% fees

- **The high cost of being poor in america:**

  In 2019, **5.4 percent** of US households were unbanked

- **Economies with an unstable fiat currency**

Why DeFi? Failures of the existing financial system



USDC/USDT daily purchasing volume in Argentina during inflation

"As crypto adoption has grown, lots of people [in Argentina] will now get their paycheck and immediately put it into USDT or USDC."

Alfonso Martel Seward, Lemon Cash

https://www.chainalysis.com/blog/latin-america-cryptocurrency-adoption/

Why DeFi? Failures of the existing financial system

- **On-chain exchanges (DEX)**

  Exchange UDC for DAI by calling a smart contract

- **On-chain lending protocols**

  Borrow and lend tokens to, for example, trade

- **TLDR**

  You can make (lose) a lot of money on chain

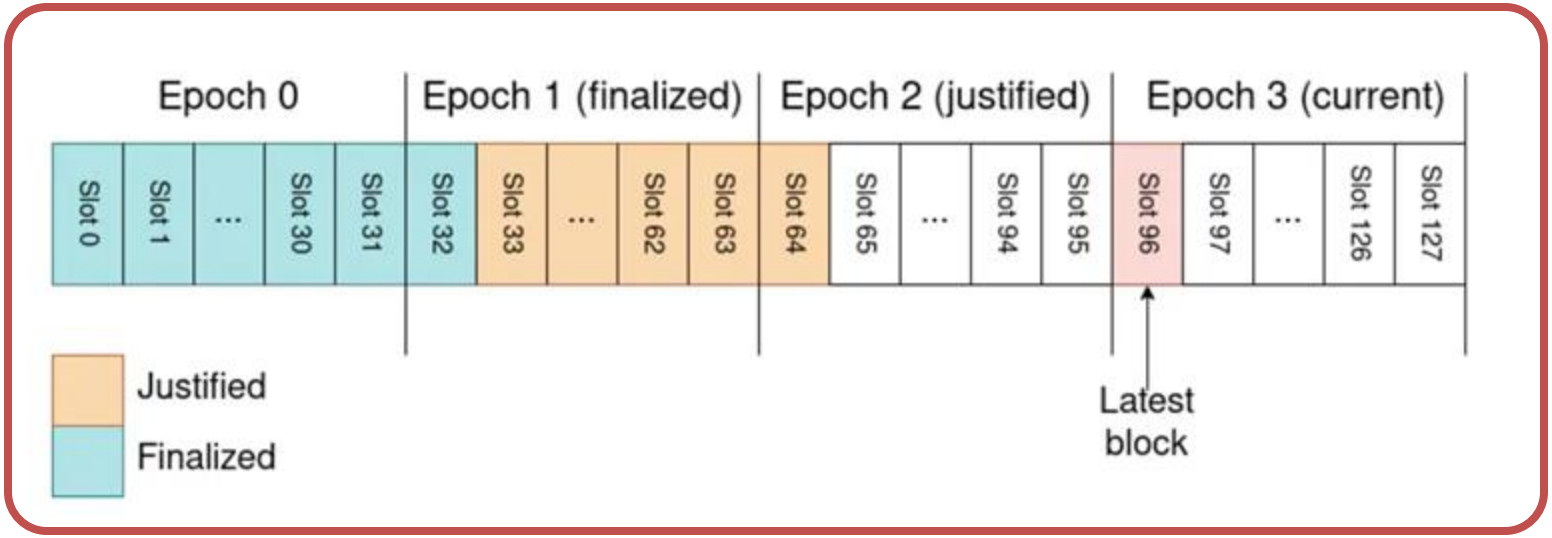
More next class

So what?

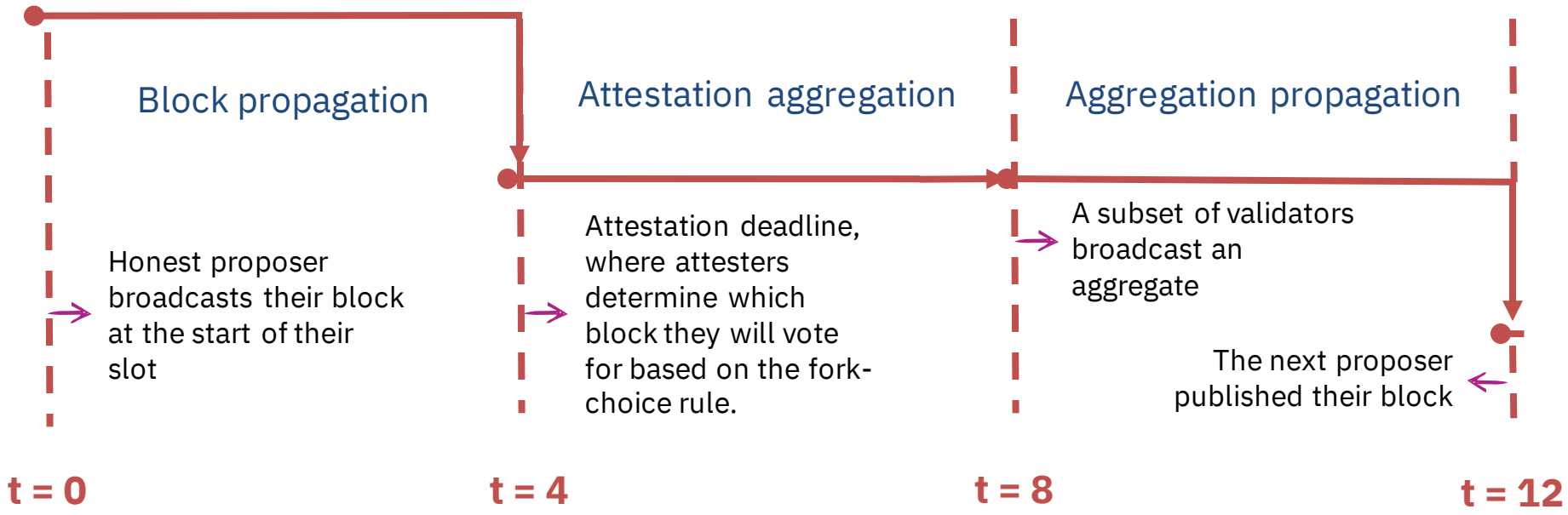
- Making money at the execution layer could impact what you do at the consensus layer

- How so?

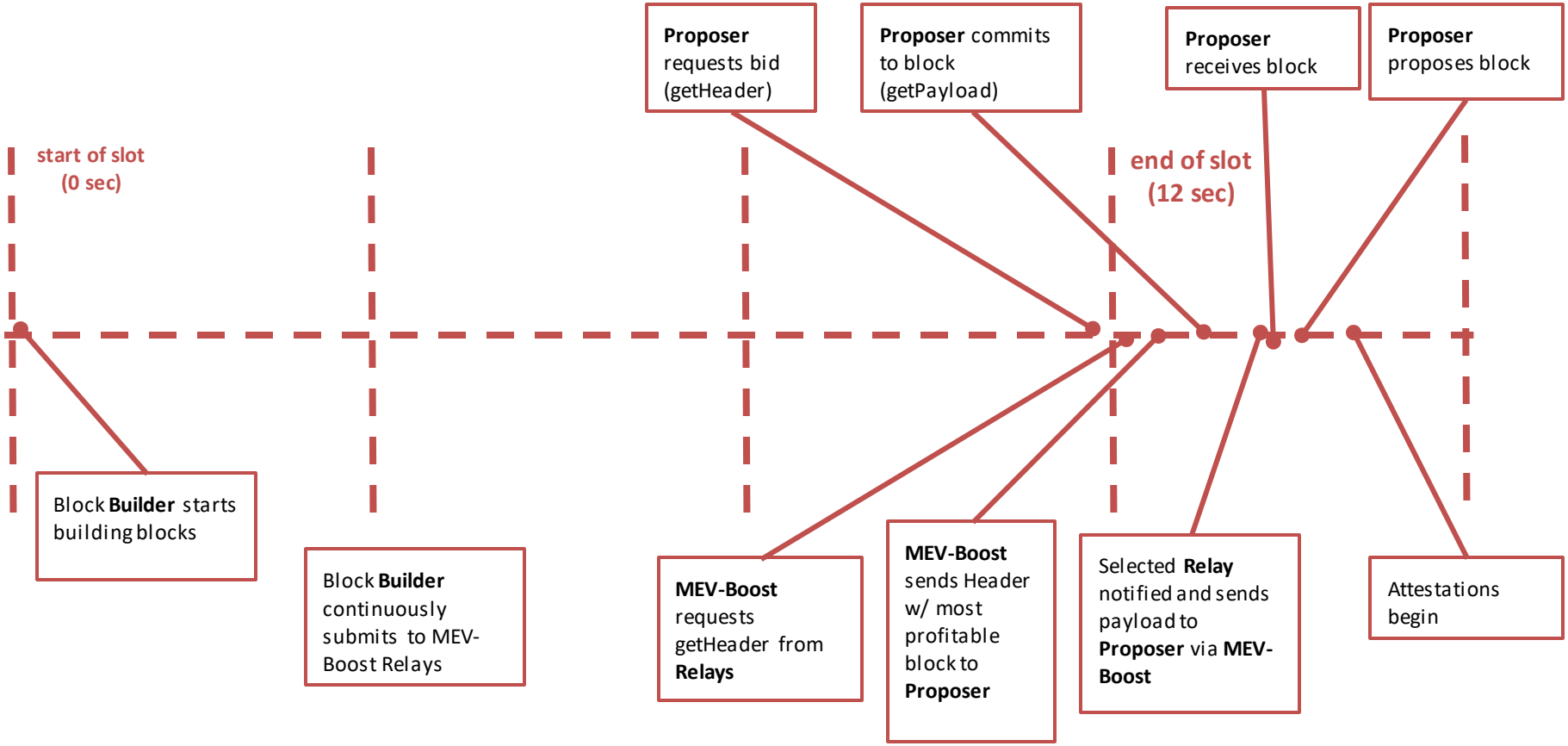
Recall what Ethereum slots look like



What happens within a slot?



What actually happens?



The MEV problem

Ethereum gives rise to a new type of business: **searchers**

- **Arbitrage:** Uniswap DAI/USDC exchange rate is 1.001
  whereas at Sushiswap the rate is 1.002

  ⇒ a searcher posts Tx to equalize the markets and profits

- **Liquidation**: suppose there is a liquidation opportunity on Aave

  ⇒ a searcher posts a liquidation Tx and profits

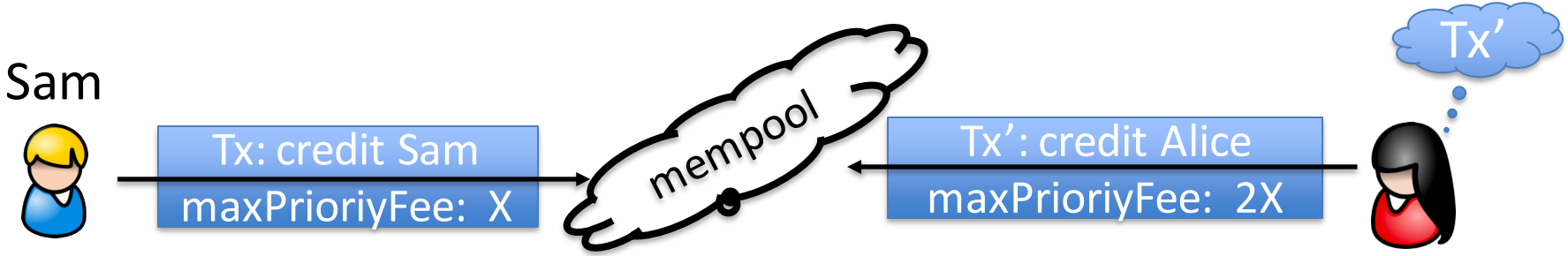
- Many other examples … often using a sequence of Tx (a bundle)

The MEV problem

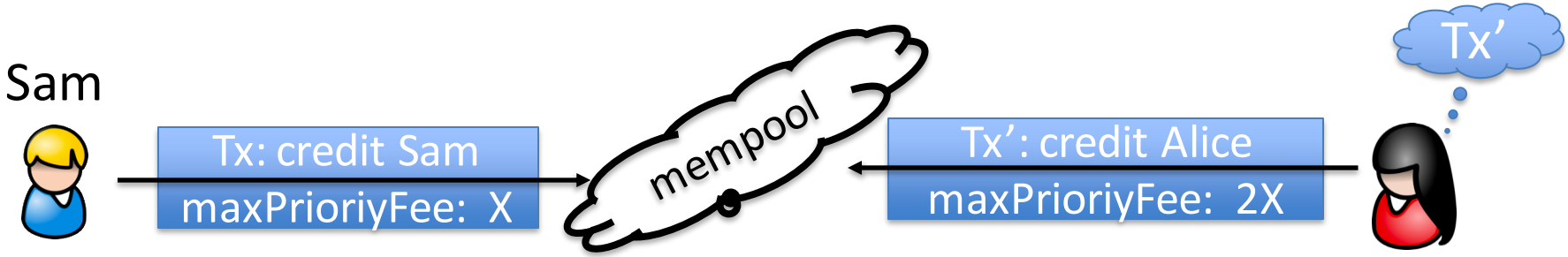
What happens when a searcher posts a Tx to the mempool?

- **Validator:** create a new Tx' with itself as beneficiary, and place it before Sam's Tx in the proposed block
- **Another searcher:** create a new Tx' with itself as beneficiary, and posts it with a higher *maxPrioriyFee*

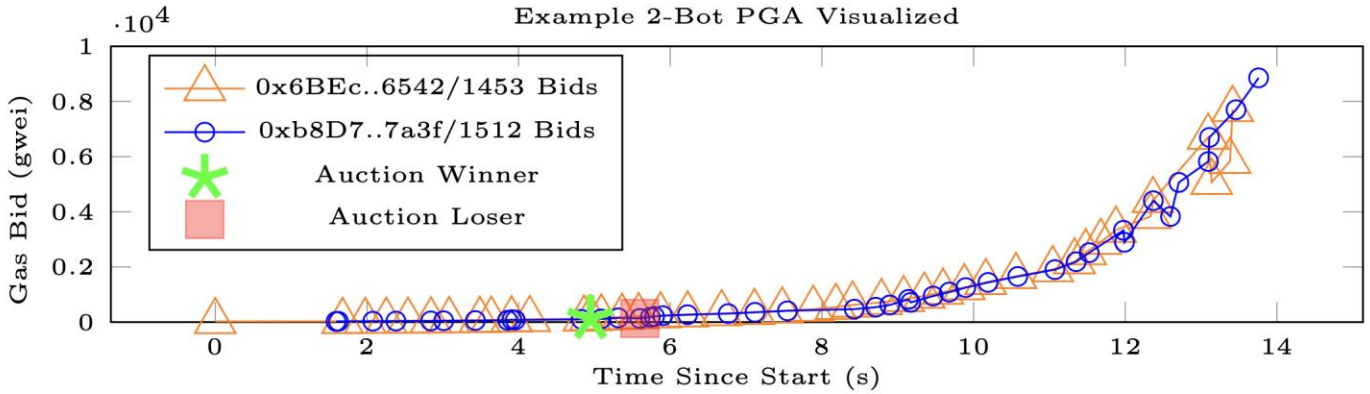
⇒ this action is now mostly automated by copy-paste bots



The MEV problem



The MEV problem



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).

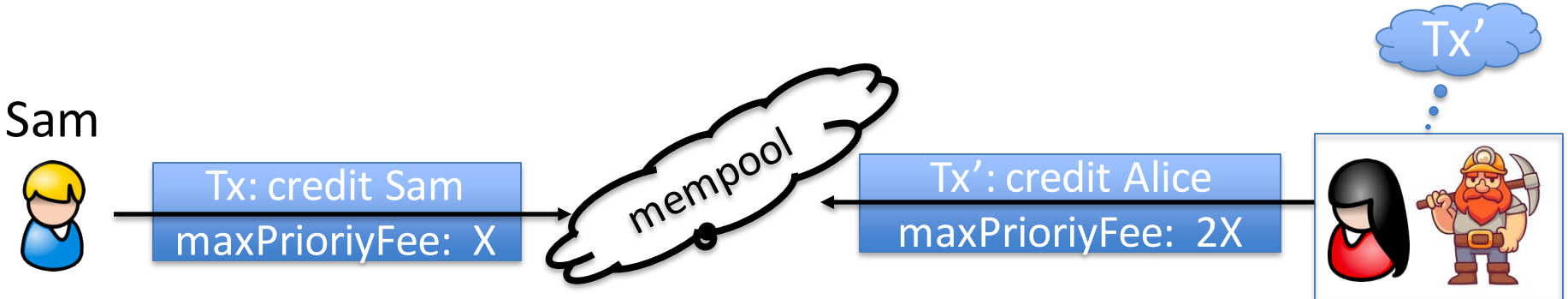
Flashboys 2.0

The result harms honest users

Price Gas Auctions (PGA): many searchers compete

- Repeatedly submit a Tx with higher and higher *maxPriorityFee* until a validator chooses one … happens within a few seconds

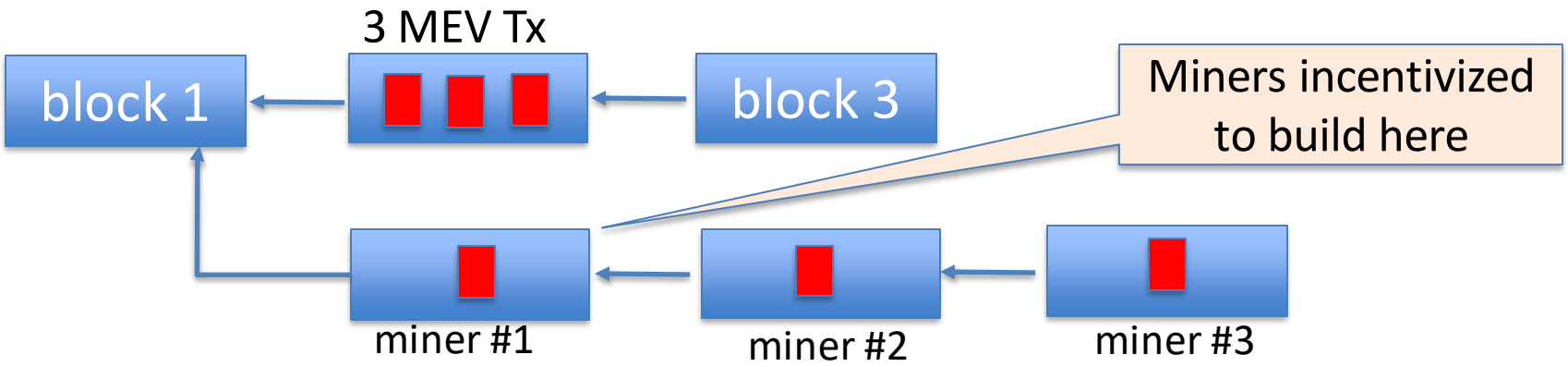
⇒ causes congestion (lots of Tx in mempool) and high gas fees



The result harms consensus

Undercutting attack on <u>longest-chain</u> consensus (not Ethereum)**:**

Rational miner: can cause a re-org by taking one MEV Tx for itself and leave two for other miners



The problem: MEV Tx generate extra revenue for miners, higher than block rewards

The result causes centralization

Validators can steal MEV Tx from searchers ⇒ **Private mempools**

Searchers only send Tx to a validator they trust

(have a business relation with)

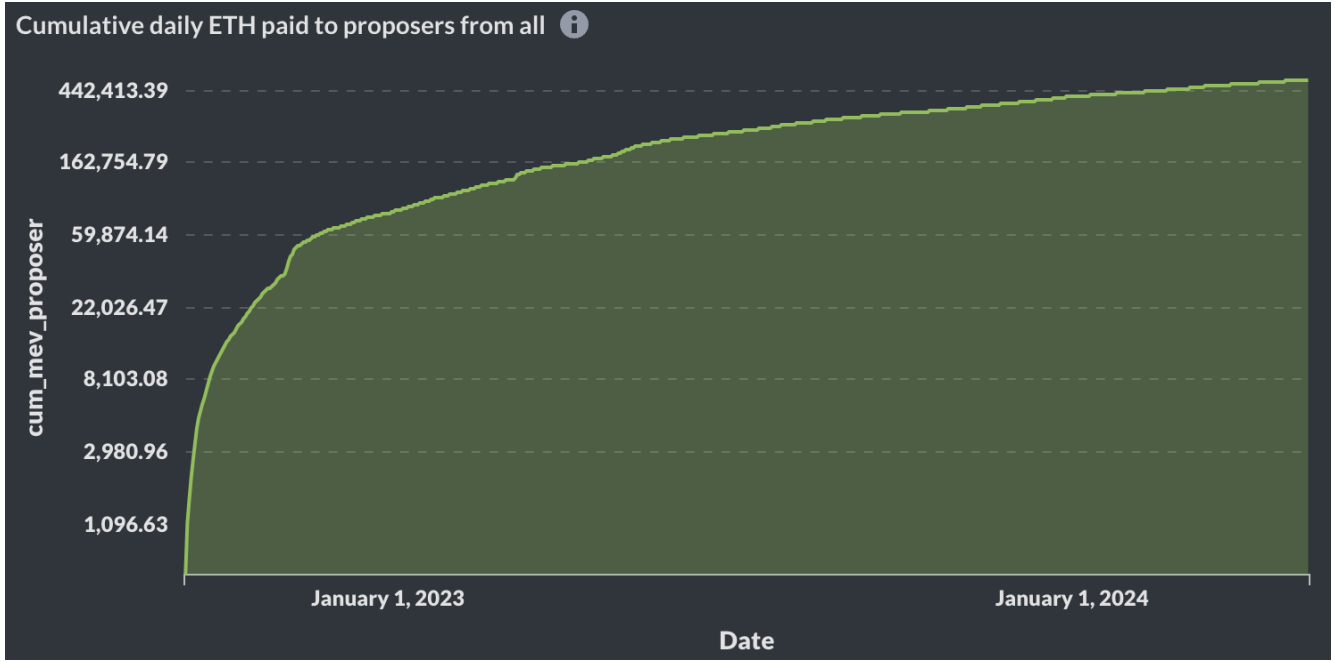
These validators do not propagate Tx to the network,

but put them in blocks themselves

In the long run: a few validators will handle the bulk of all Tx

How big are MEV rewards?

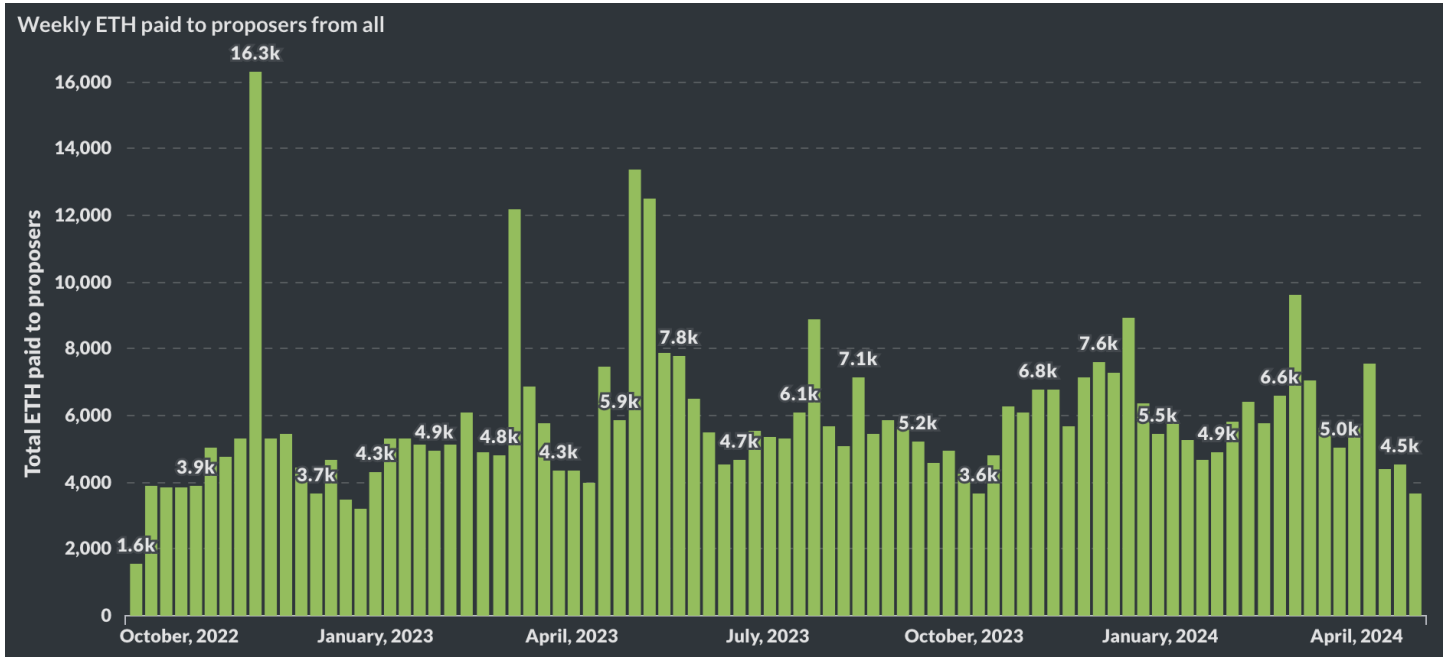
Cumulative MEV payments to validators since Nov. 2020:



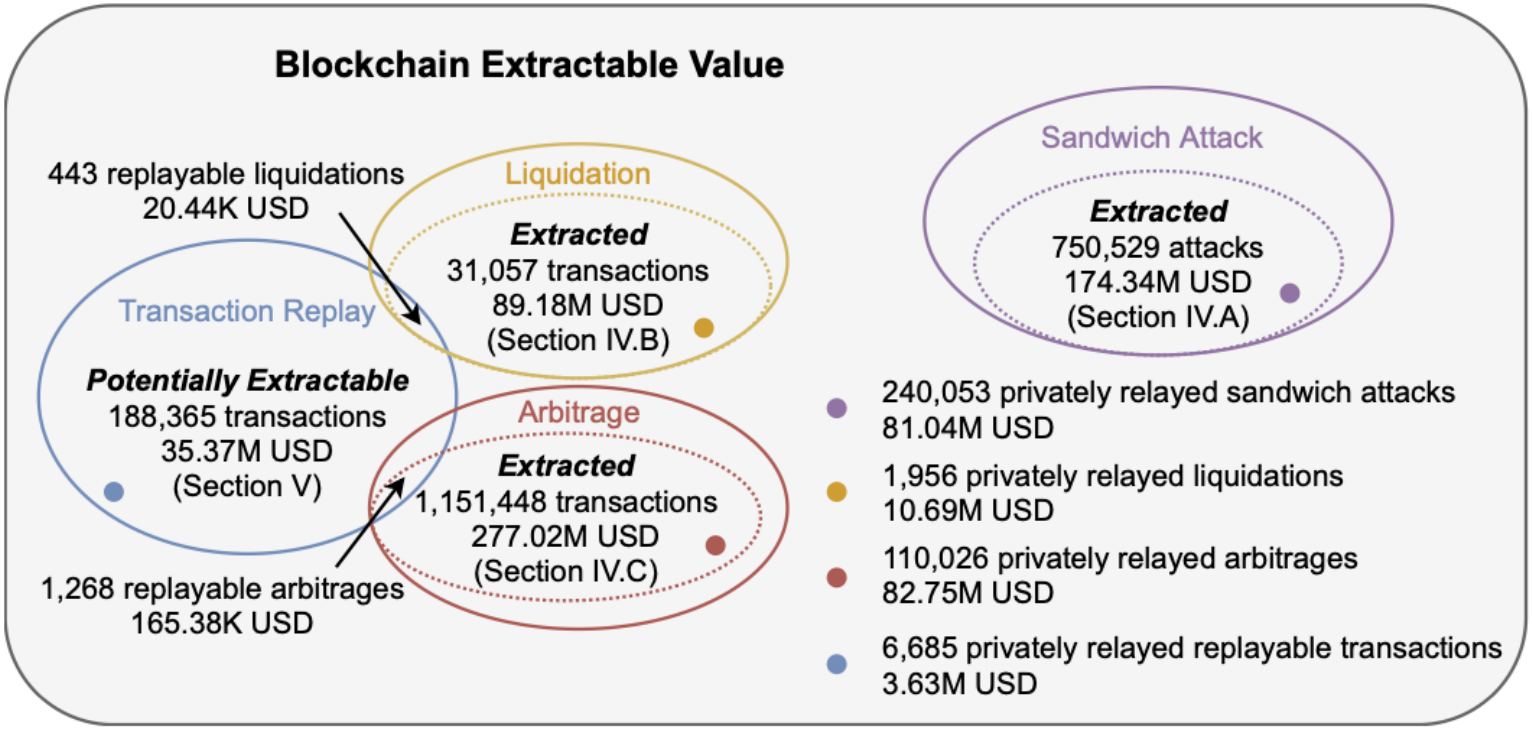
source: explore.flashbots.net

How big are MEV rewards?

Weekly MEV amount paid to validators (in ETH):

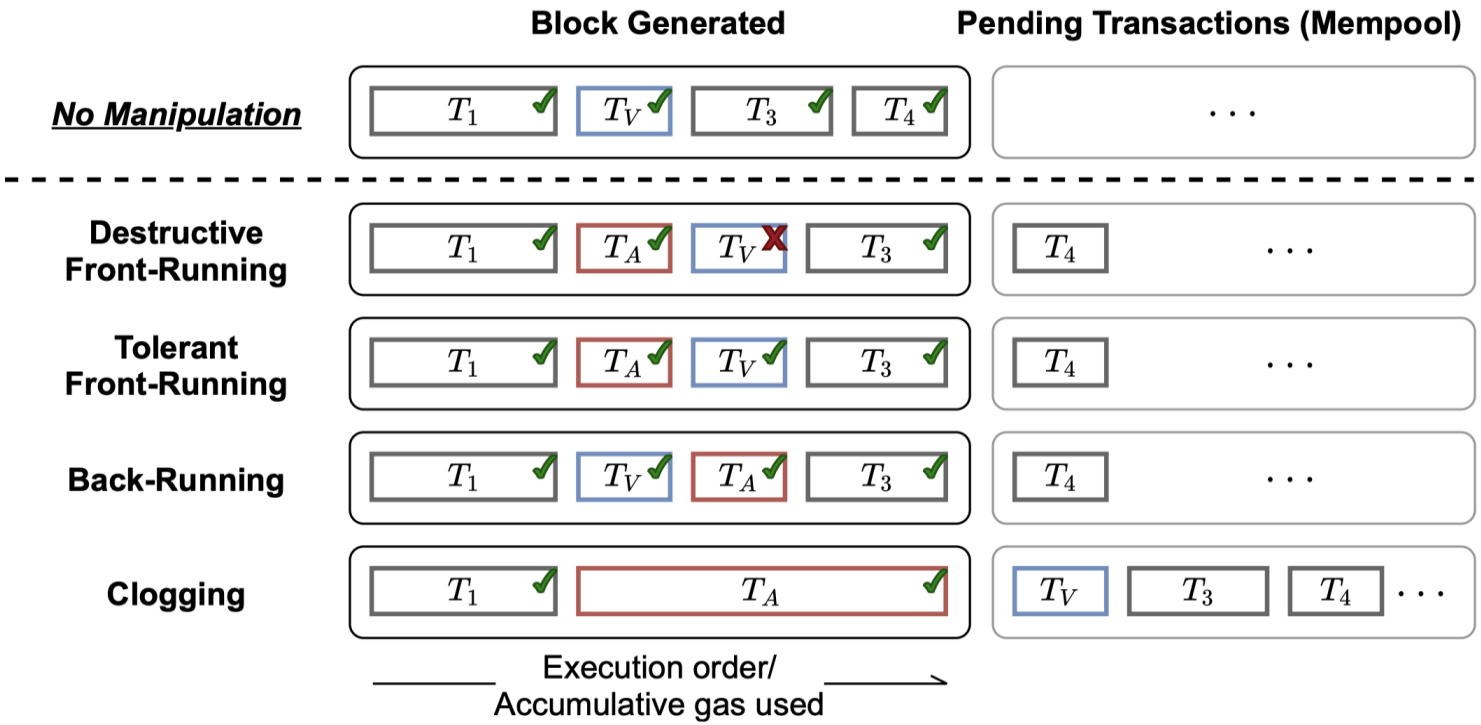


Where is this money coming from?



paper

Where is this money coming from?



What to do?

Two options

Option 1:

- Accept MEV is unavoidable; minimize its harm to the ecosystem

  $\Rightarrow$ Flashbots

Option 2:

- Try to prevent some MEV, by removing the block proposer's choice in ordering Tx in a block.

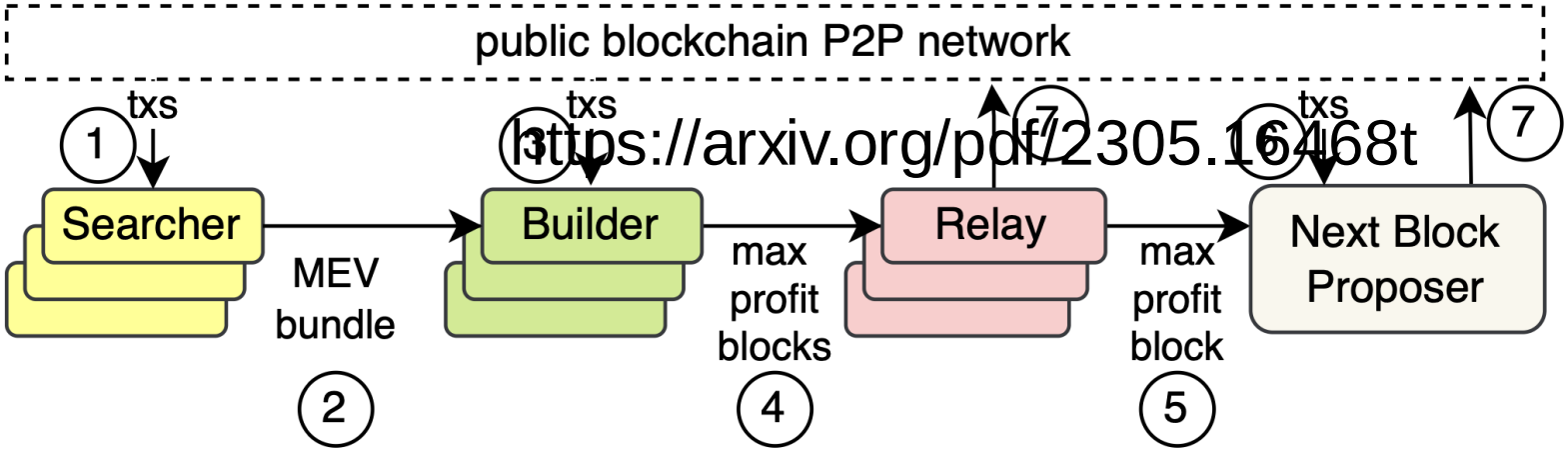
Option 1: Proposer Builder Separation (PBS)

Goals:

- Eliminate price gas auctions in the public mempool
  - Instead, create an off-chain market for searchers to compete on the position of their bundles in a block
- Prevent validator concentration: make it possible for every validator to earn MEV payments from searchers

Current PBS implementation: **MEV-boost**

The participants in PBS (as in MEV-boost)

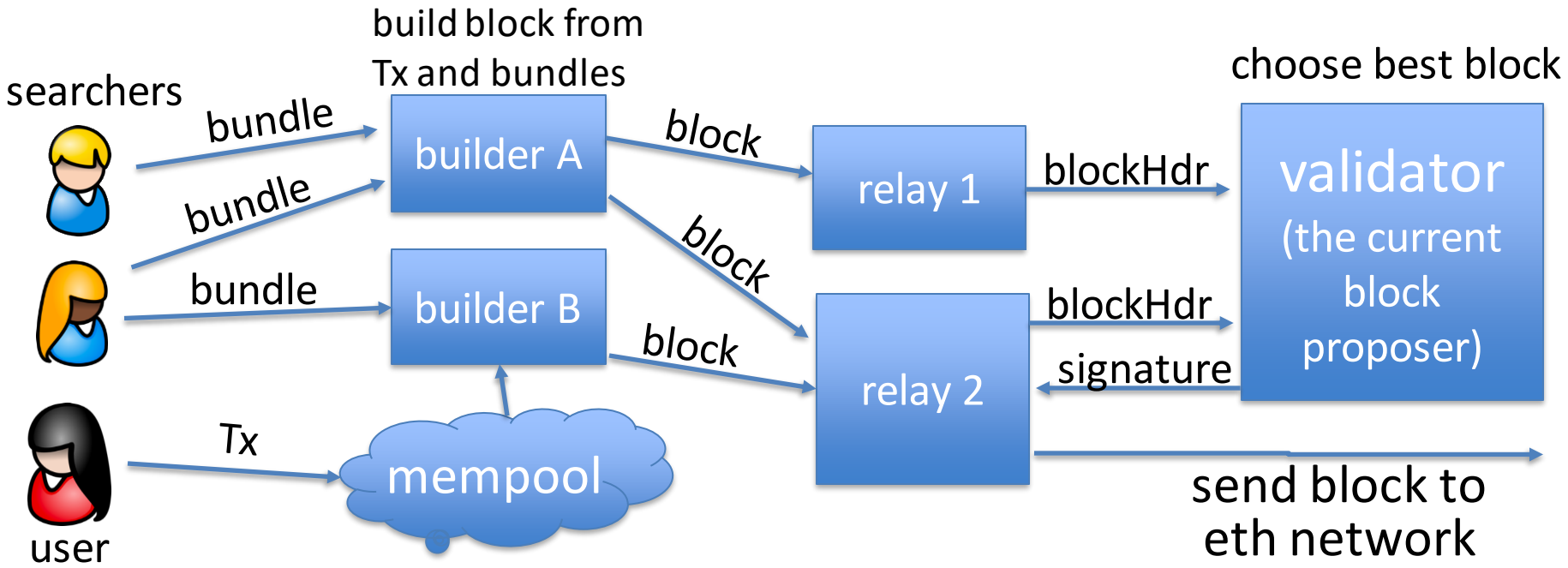


https://arxiv.org/pdf/2305.16468t

The participants in PBS (as in MEV-boost)

Users have Tx and searchers have bundles (sequence of Tx)

- searcher wants its bundle posted in a block unmodified



MEV-boost

Builder: collects bundles and Tx, builds a block (≈300 bundles/block)

- includes a MEV offer to validator (feeRecipient)

Relay: collects blocks, chooses block with max MEV offer

- sends block header (and MEV offer) to block proposer
- Can't expose Tx in block to proposer (proposer could steal Tx)

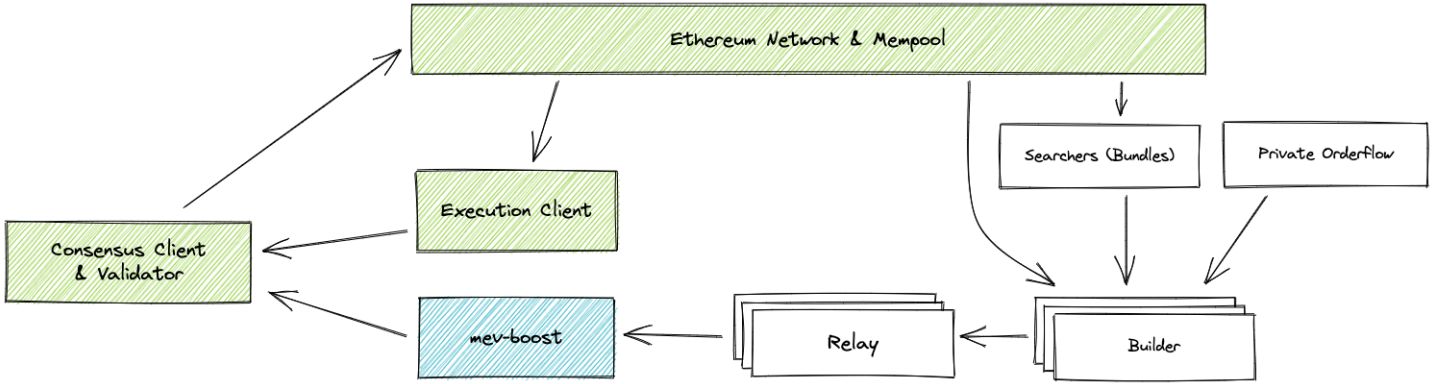
Proposer: chooses best offer and signs header with its staking key

⇒ Then Relay sends block to network, making it public

⇒ Now, proposer cannot steal MEV (why not?)

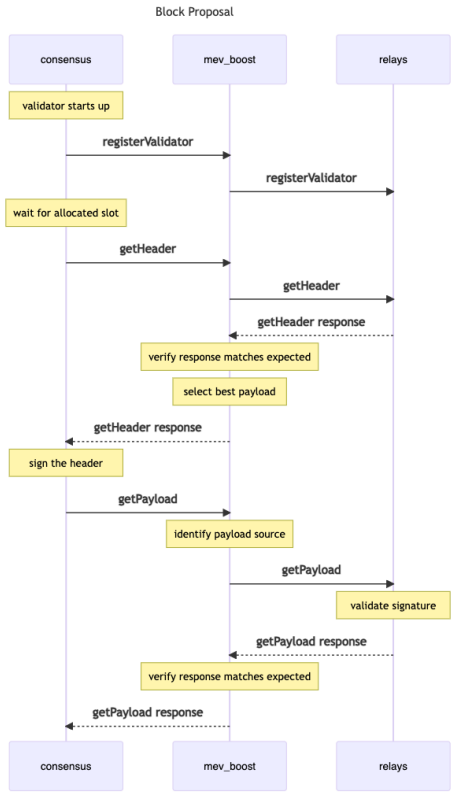
https://writings.flashbots.net/searching-post-merge

MEV-boost



from https://hackmd.io/@ralexstokes/SynPJN_pq

What actually happens in a slot



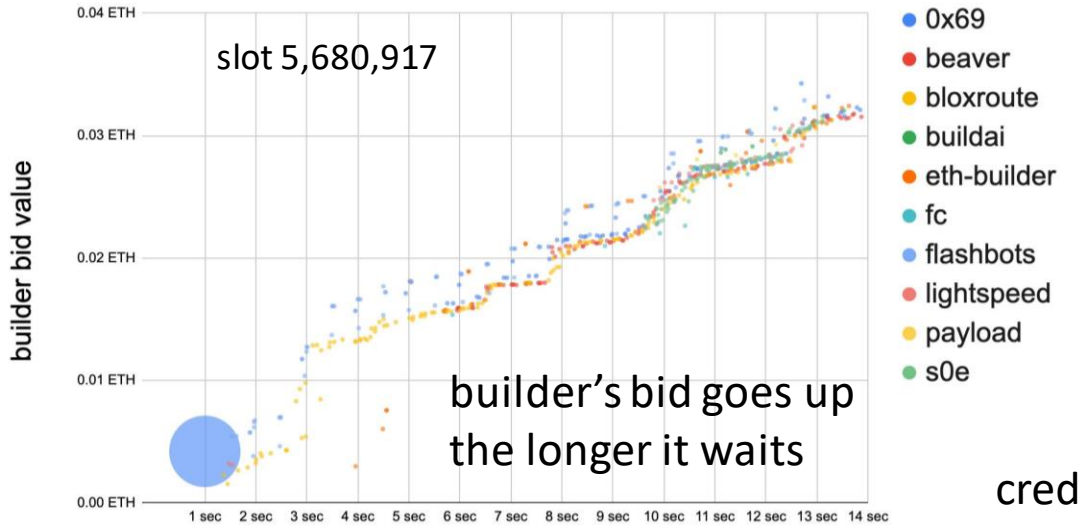

```
{
  "jsonrpc": "2.0",
  "id": 1,
  "method": "eth_sendBundle",
  "params": [
    {
      txs,               // Array[String], A list of signed transactions to execute in an atomic bundle
      blockNumber,       // String, a hex encoded block number for which this bundle is valid on
      minTimestamp,      // (Optional) Number, the minimum timestamp for which this bundle is valid, in seconds
since the unix epoch
      maxTimestamp,      // (Optional) Number, the maximum timestamp for which this bundle is valid, in seconds
since the unix epoch
      revertingTxHashes, // (Optional) Array[String], A list of tx hashes that are allowed to revert
    }
  ]
}
```

from https://hackmd.io/@ralexstokes/SynPJN_pq

Many block options per slot

A relay might receive 500 blocks per slot from builders

- Each builder might send 20 blocks to relay for one slot
- Why? The longer builder waits the more MEV opportunities …



credit: Justin Drake and Shea Ketsdever

Operating relays

Flashbots: Filters out OFAC sanctioned addresses,
aims to maximize validator payout
(so that many validators will work with it)

BloXroute: no censorship, aims to maximize validator payout

UltraSound: not for profit, non censoring

...

Flashbot relay

Recently Delivered Payloads

Epoch	Slot	Block number	Value (ETH ↓) ⇅	Num txs	Blobs	Block hash
218,508	6,992,273	17,806,773	584.0554235	96	0	0xb60c6e66c6ceca0940ccb8c467ba9292175d0e773a112380dd18f5288bc33ed1
252,066	8,066,117	18,871,827	566.3731393	12	0	0xe3c49d4ea801db5507096bb249e29f5a4f53c737193d262c6e97cc5984649ae1
231,547	7,409,519	18,220,525	560.1151699	166	0	0x76da6242ea64da78c0a907e3c5265e405e00499976de94c9cb01e2961786f146
188,720	6,039,070	16,867,031	523.6763927	228	0	0x06148e28cc7212b9e5157466ebe8cd0b5650a0e573a7e21f6105d41bc1cb6f2b
251,621	8,051,898	18,857,759	512.2719525	99	0	0x9cd57f2d1bf7228a510fbc96b16ffc3fd7712e8c474cce2323235c151c1784df
251,678	8,053,706	18,859,551	512.2558025	324	0	0xb3e051047b43c35d4fe8eeef30c7b7921eb0d740a411e2536731bb81890c5b40
251,607	8,051,424	18,857,291	512.0701828	17	0	0x0de0905cca4856228ac6b21dabb793d58c69d35b585ba68cac96c0c28dac1213
251,613	8,051,625	18,857,491	480.1064613	173	0	0xf4f740c71b16896e259466d5a4d1f36235ec146f0e47d931d75c6ad2e327f10e
252,637	8,084,398	18,889,912	440.6448043	203	0	0x722dbd4ad2fa5b277f5fc656dde42cde60420ec8316d0a77e8b5bd5dc57c7457

https://boost-relay.xx.net/

https://beaconcha.in/

Top relayers

7 Days 31 Days 180 Days

Network Participation: 90%

Name	Block Count	Unique Builders	Average Reward	Highest Reward	Overall Rewards	Uncensored	Unfiltered
ultra sound (Relay)	559968 (43.21%)	137	0.11487562 ETH	320.17215537 ETH (Slot 8,444,661)	64326.67348555 ETH	Yes	Yes
BloXroute [Max-Profit] (Relay)	461725 (35.63%)	75	0.11377005 ETH	279.03339775 ETH (Slot 8,233,166)	52530.47895752 ETH	No	Yes
Agnostic (Relay)	305304 (23.56%)	119	0.12129973 ETH	320.17215537 ETH (Slot 8,444,661)	37033.29574307 ETH	Yes	Yes
BloXroute [Regulated] (Relay)	298151 (23.01%)	62	0.12130134 ETH	512.29387683 ETH (Slot 8,052,043)	36166.11876615 ETH	No	Yes
Flashbots (Relay)	292457 (22.57%)	156	0.14205437 ETH	566.37313925 ETH (Slot 8,066,117)	41544.79735726 ETH	No	Yes
Aestus (Relay)	65008 (5.02%)	68	0.11764015 ETH	113.84092695 ETH (Slot 8,433,522)	7647.55147000 ETH	Yes	Yes
Titan (Relay)	11300 (0.87%)	8	0.07394124 ETH	56.03652616 ETH (Slot 8,814,671)	835.53602534 ETH	Yes	Yes
Manifold (Relay)	3505 (0.27%)	35	0.07972446 ETH	15.55568029 ETH (Slot 8,136,899)	279.43424791 ETH	Yes	Yes
Eden Network (Relay)	2309 (0.18%)	5	0.07197521 ETH	7.83227937 ETH (Slot 8,239,266)	166.19077304 ETH	No	???
Wenmerge (Relay)	8 (0.00%)	2	0.05396076 ETH	0.24519784 ETH (Slot 8,420,315)	0.43168608 ETH	Yes	Yes

Top builders

Builders:

Builders are the entities that are building the blocks distributed by the relays. Nothing prevents a single entity from using multiple Builder Public Keys, so some Builders may be opperated by the same entity.
Displayed below are active builders from the **last 14 days**

Builder	Seen Relays	Block Count	Latest Slot
0xb67eaa…8eab08	Aestus (Relay) ultra sound (Relay) Titan (Relay) BloXroute [Max-Profit] (Relay) Agnostic (Relay) Flashbots (Relay) BloXroute [Regulated] (Relay)	18014	9,023,735 (4 mins ago)
0xb26f96…48e681	BloXroute [Max-Profit] (Relay) Agnostic (Relay) Flashbots (Relay) ultra sound (Relay) Titan (Relay) BloXroute [Regulated] (Relay) Aestus (Relay)	15623	9,023,736 (3 mins ago)
0x83d349…1fb640	Agnostic (Relay) Flashbots (Relay) BloXroute [Max-Profit] (Relay) BloXroute [Regulated] (Relay) ultra sound (Relay)	15411	9,023,728 (5 mins ago)
0x978a35…3bd587	BloXroute [Max-Profit] (Relay) Agnostic (Relay) BloXroute [Regulated] (Relay) ultra sound (Relay) Flashbots (Relay)	11134	9,023,639 (23 mins ago)
0x95c8cc…81f742	Flashbots (Relay) BloXroute [Max-Profit] (Relay) Agnostic (Relay) Titan (Relay) BloXroute [Regulated] (Relay) ultra sound (Relay) Aestus (Relay)	10433	9,023,627 (25 mins ago)
0x8dde59…900521	BloXroute [Max-Profit] (Relay) ultra sound (Relay) Agnostic (Relay)	8826	9,023,682 (14 mins ago)
0xa21a2f…f4d2ee	BloXroute [Regulated] (Relay) Flashbots (Relay) BloXroute [Max-Profit] (Relay)	8813	9,023,739 (3 mins ago)
0xb211df…96df7c	Agnostic (Relay) BloXroute [Max-Profit] (Relay) ultra sound (Relay)	7998	9,023,729 (5 mins ago)
0x88e1d8…ccadc8	ultra sound (Relay) Agnostic (Relay) BloXroute [Max-Profit] (Relay)	7678	9,023,741 (2 mins ago)
0x93582c…3512a3	Flashbots (Relay) BloXroute [Max-Profit] (Relay) BloXroute [Regulated] (Relay)	5968	9,023,742 (2 mins ago)
0xae2ffc…110e7a	ultra sound (Relay)	4892	9,023,736 (3 mins ago)

https://explorer.rated.network/

Top builders

PBS LANDSCAPE

Builders

1d 7d 30d All time

VALUE OF BLOCKS BUILT	ACTIVE BUILDERS	TOP 3 BUILDERS SHARE	MOST VALUABLE BLOCK
460,675.6 ETH	183	57.47%	692 ETH

BREAKDOWN BY BUILDER	BLOCKS	MARKET SHARE	RELAY DISTRIBUTION	AVG TXS INCL.	EXCLUSIVE ORDER FLOW	MEDIAN BLOCK VALUE
Beaverbuild	1,009,765	27.28%		145		0.0572
Rsync	602,793	16.28%		148		0.0578
Flashbots	539,716	14.58%		145		0.0508
Builder 0×69	488,375	13.19%		142		0.0568
Titan Builder	474,695	12.82%		149		0.0474

So what?

Builder concentration: three builders build <u>57-95% of all blocks</u> !!

- Clear centralization in the builder market
- Enables censorship by builders

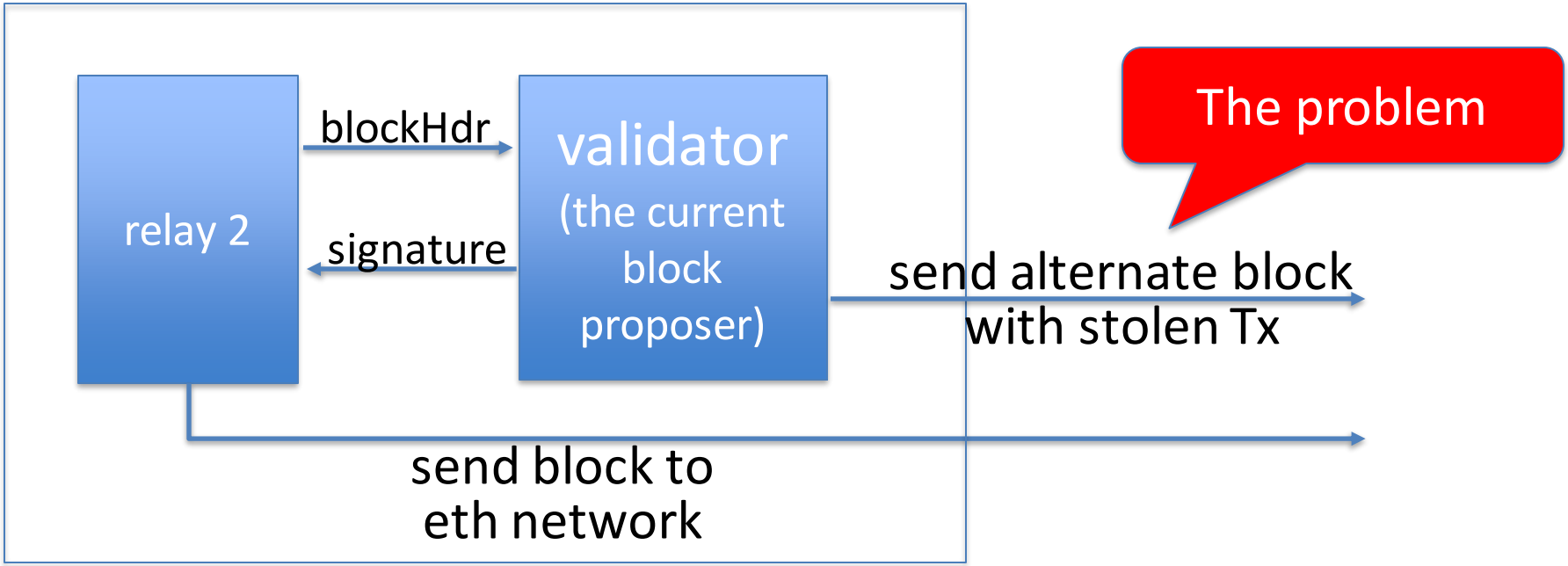
Proposers hold all the power (first price auction among builders)

$\Rightarrow$ Most MEV profits flow to block proposers

MEV-boost is not designed for cross-chain MEV

- For cross-chain arbitrage, no atomicity guarantee for bundle

What if the proposer is malicious?



Block proposer will be slashed (why?) ⇒ Lose 1 ETH

… but can gain much more in stolen MEV.

What if the proposer is malicious?

1: Honeypot transactions w/ unlimited slippage sent to mempool by a **malicious validator** to **bait**

2: MEV bots pounce to **sandwich** the honeypot transactions. To ensure maximum

3: When it came time to request a block from MEV-Boost, the malicious validator used **invalid values**

4: As a result, the MEV-Boost relay **submitted an invalid block** to the beacon chain, which does not

5: The malicious validator submitted a **revised block** that removed its honeypot transactions and

6: The malicious validator **drained $25 million** from the MEV bots it baited.

Show 10 entries

687a9414b0225092d4a8b859fe813

Address	Validator Key	Withdrawal Credential	Amount	Tx Hash	Time	Block	Validator State	Valid Signature
0x687A94…	0x960c2f…	0x0062…4fbf	32 ETH	0x9cf11f…	418 days 21 hrs ago	16836204	Slashed	✅

Showing 1 to 1 of 1 entries

see beaconcha.in