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

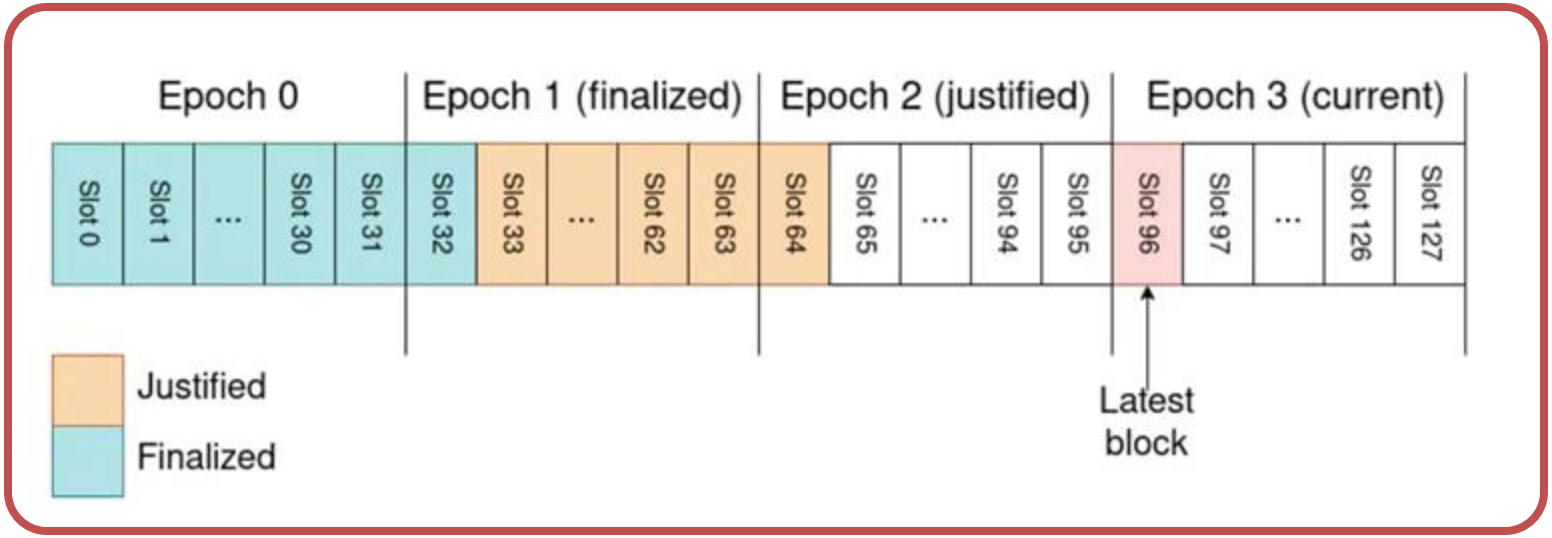
  ERC-20 standard enables interoperability (6-7 functions)

Implications of DeFi on security

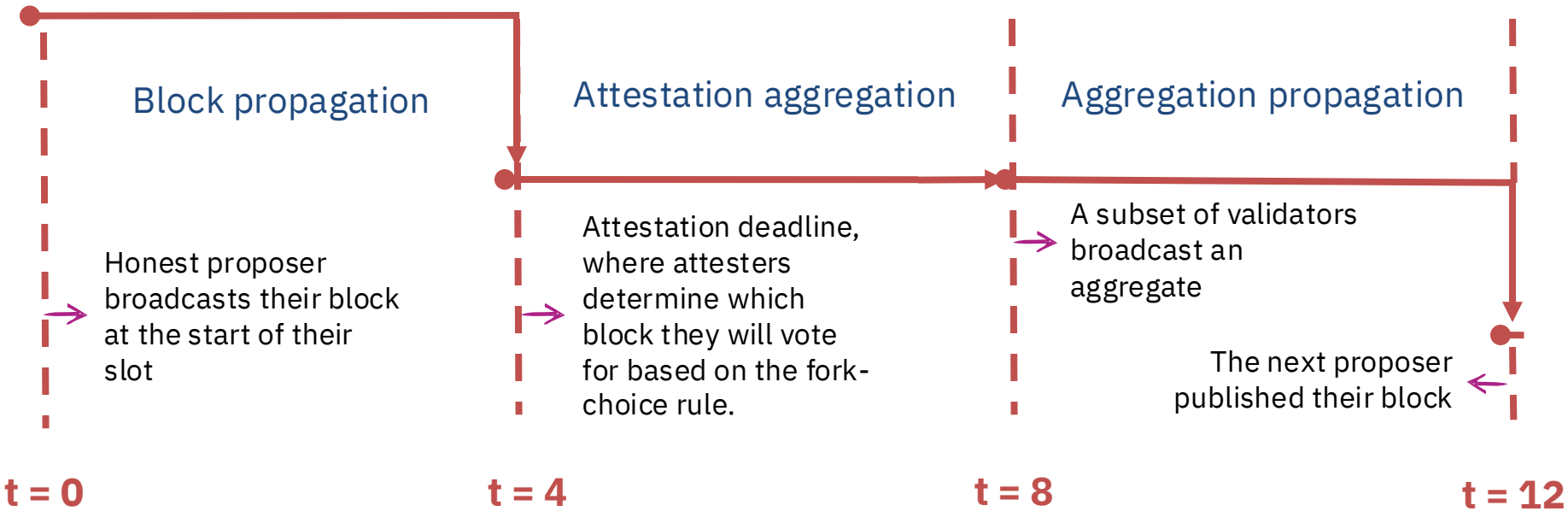
- Making money at the execution layer could impact what you do at the consensus layer

- How so?

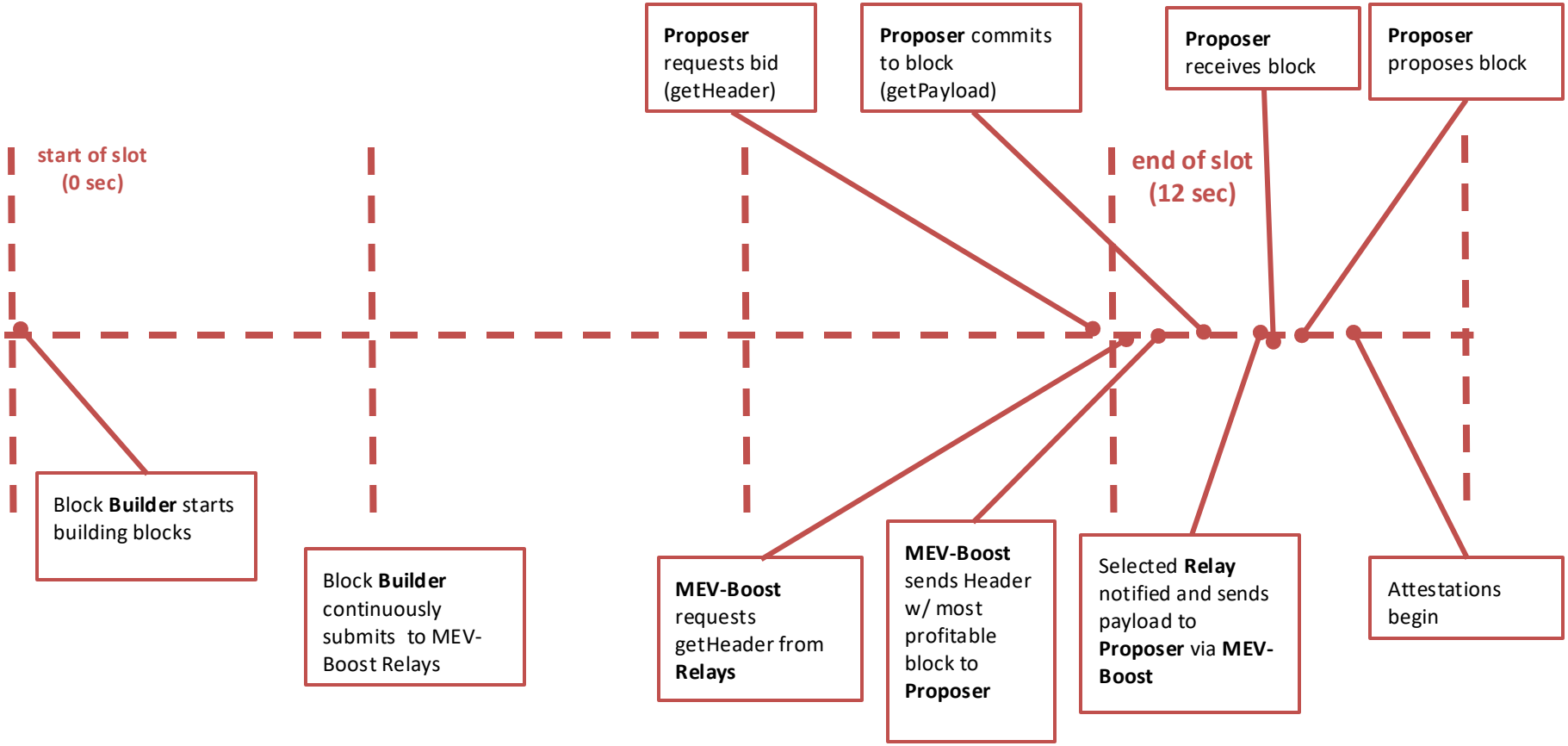
Recall what Ethereum slots look like



What happens within a slot?



What actually happens?



The MEV problem

Ethereum gave 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

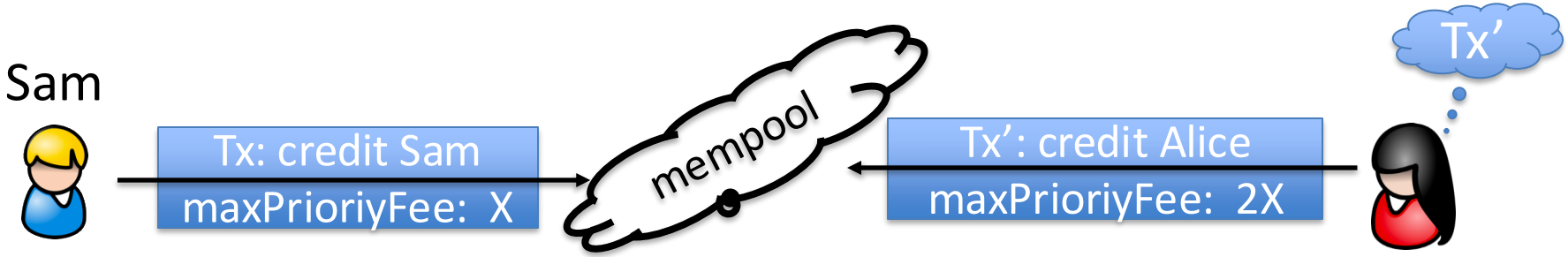
- Many other examples … often using a sequence of Tx (a bundle)

The MEV problem

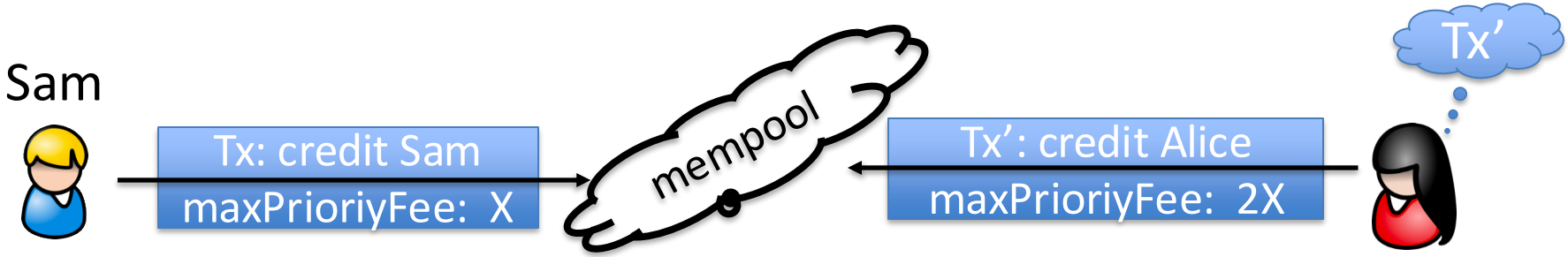
What happens when a searcher posts a Tx to the mempool?

- **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*

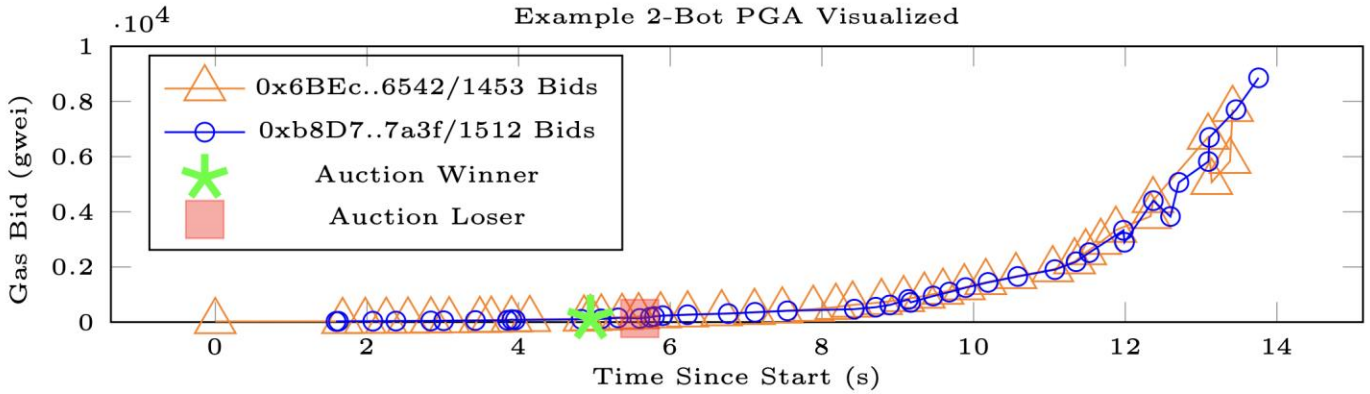
⇒ this action is now mostly automated by copy-paste bots



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).

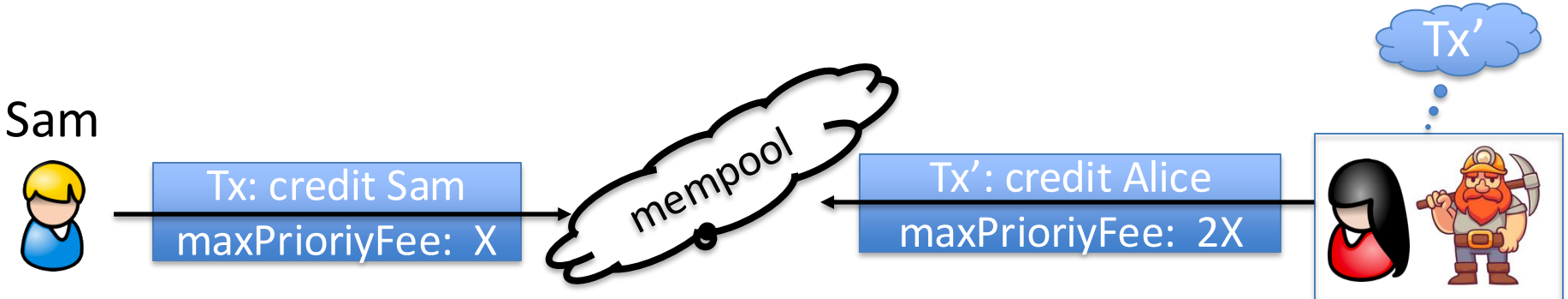
Flashboys 2.0

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

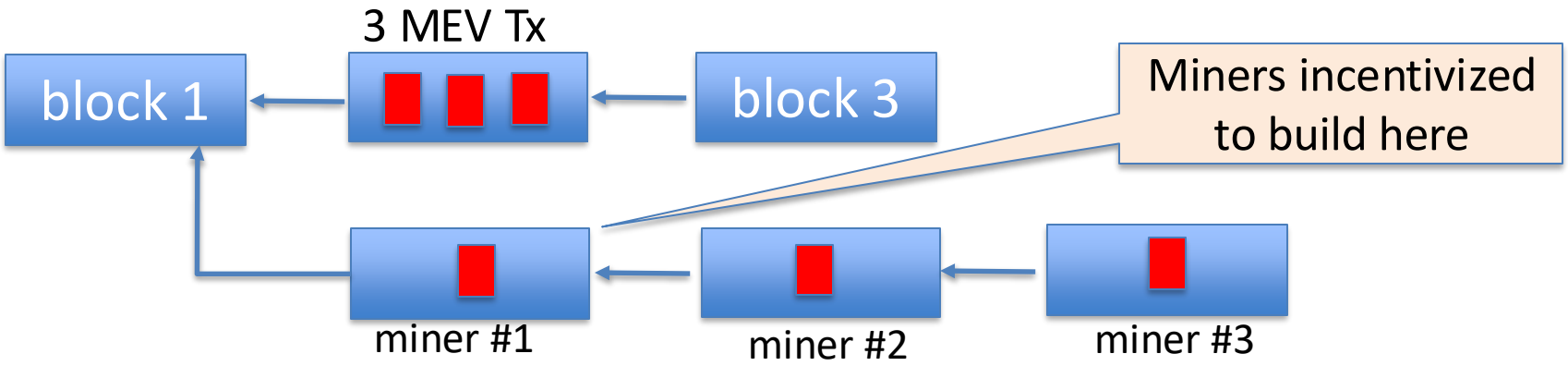
⇒ causes congestion (lots of Tx in mempool) and high gas fees



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)

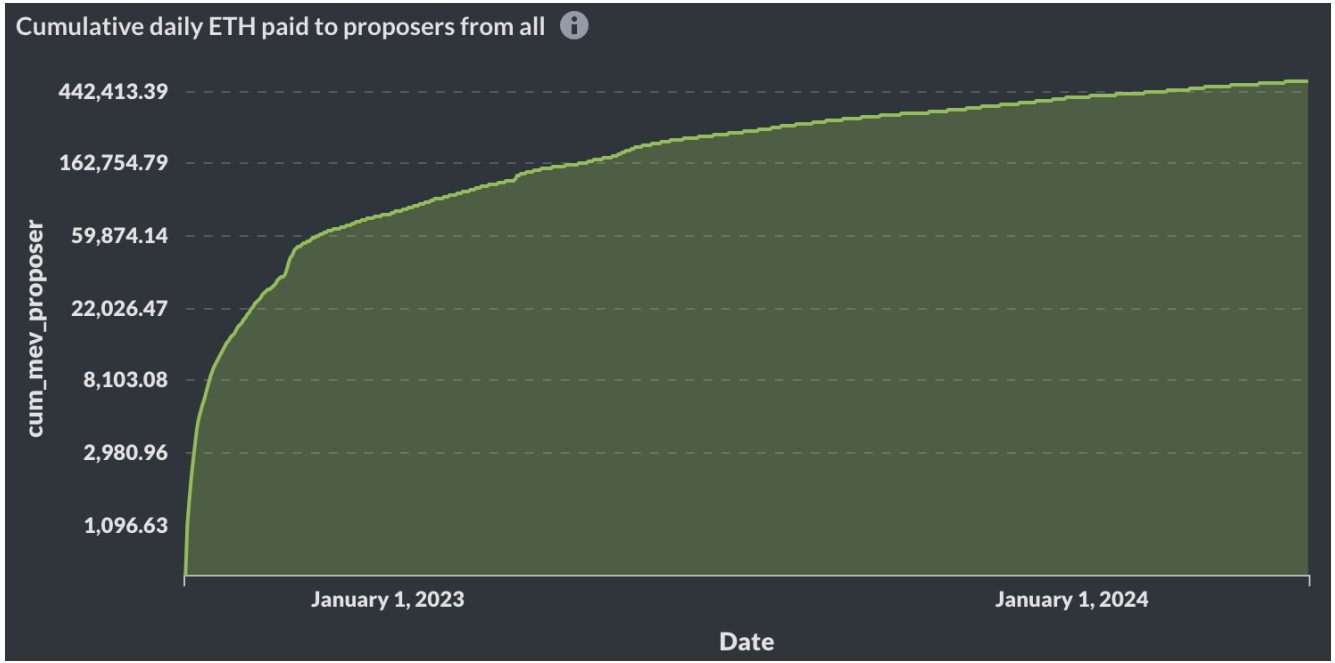
These validators do not propagate Tx to the network,

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?

Latest Blocks | Top Blocks

Slot	Proposer	Relays	Block Reward	Block Extra Data
11,060,728	1562032	Flashbots (Relay)	2144.01166801 ETH	Gambit Labs (https://gmbit.co)
10,977,050	277858	BloXroute [Max-Profit] (Relay) BloXroute [Regulated] (Relay) Titan (Relay)	1243.34455623 ETH	
6,039,069	131545	Agnostic (Relay)	691.96319226 ETH	Illuminate Dmocratize Dstribute
6,181,978	232931	Agnostic (Relay)	689.01747383 ETH	beaverbuild.org
6,992,273	428198	Agnostic (Relay) Flashbots (Relay) ultra sound (Relay)	584.05542354 ETH	payload.de
8,066,117	450543	Flashbots (Relay)	566.37313925 ETH	I can haz block?
7,409,519	303167	Flashbots (Relay)	560.11516990 ETH	Gambit Labs (https://gmbit.co)
6,039,070	75568	Agnostic (Relay) Flashbots (Relay)	523.67639274 ETH	by @builder69
9,594,066	614082	Titan (Relay)	512.30677704 ETH	25
8,052,043	652288	BloXroute [Regulated] (Relay)	512.29387683 ETH	@penguinbuild.org

How big are MEV rewards?

MEV-Boost Analytics

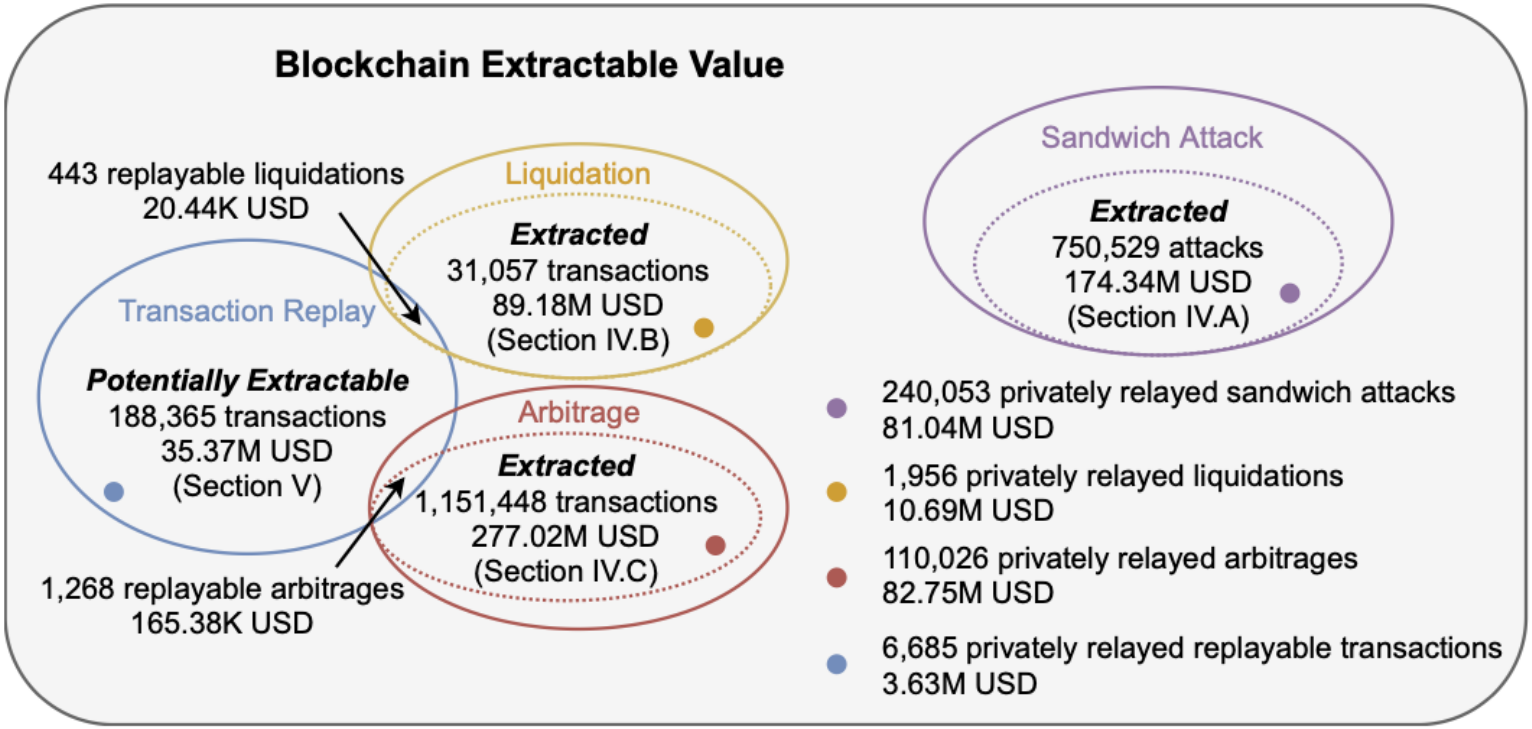
Updated at slot 11753650 (5 minutes ago)

Overview · **Builder Profitability**

7d · 24h · 12h · 1h

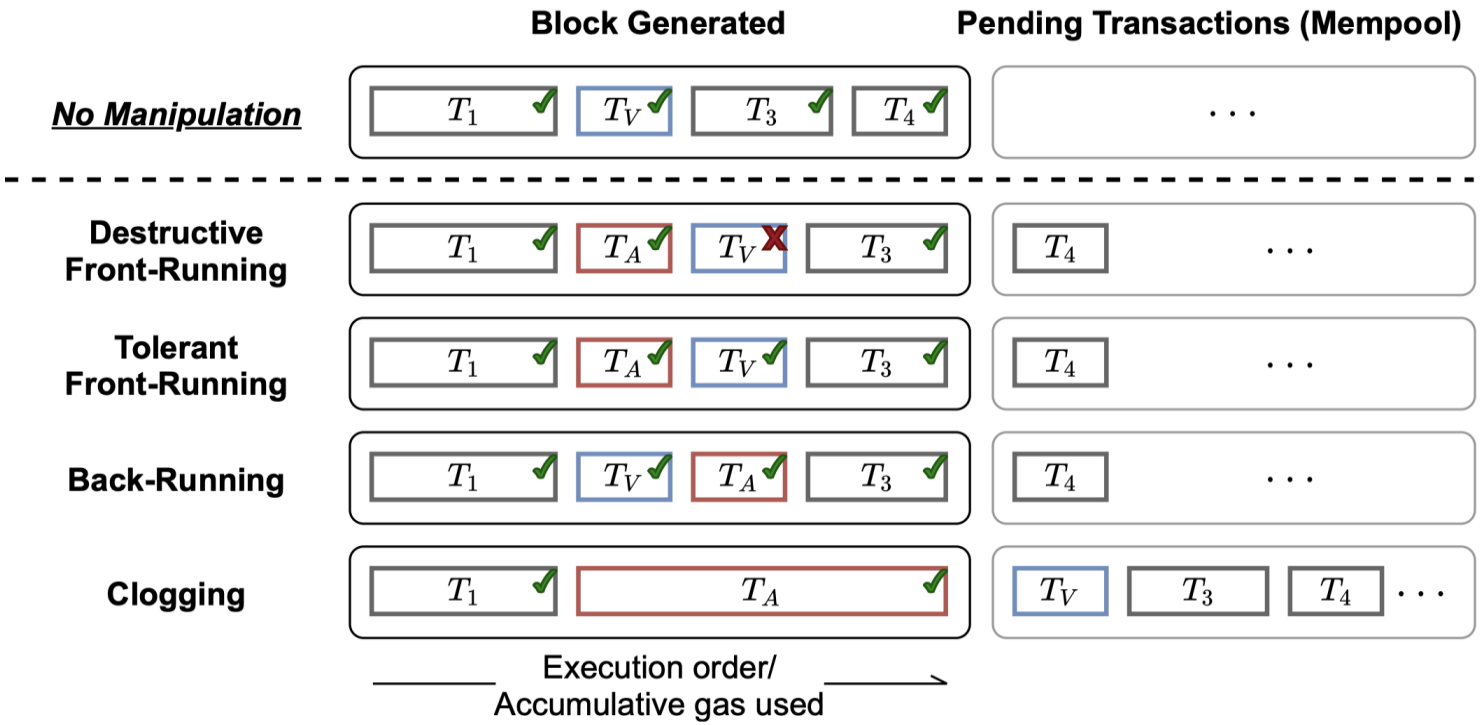
Builder extra_data	Blocks	Blocks with profit	Blocks with subsidy	Overall profit (ETH)	Subsidies (ETH)
Titan (titanbuilder.xyz)	20,375	19,246	1,129	346.8814	0.8747
beaverbuild.org	14,037	11,678	2,359	177.5177	1.7000
BuilderNet	5,471	2,856	2,615	37.9597	4.0857
rsync-builder.xyz	3,043	1,034	1,986	31.9761	10.8935
bobTheBuilder.xyz	141	141	0	20.1466	0.0000
	22	21	1	2.5707	0.0016
BuildAI (https://buildai.net)	23	21	2	1.0830	0.0002

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, BuilderNet

Option 2:

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

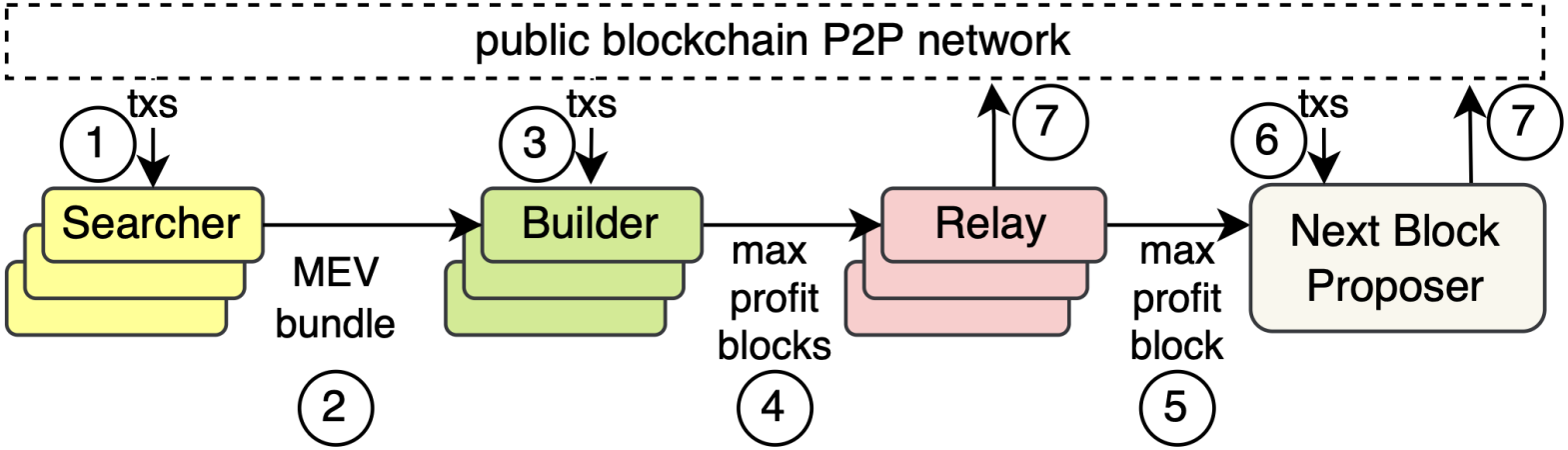
Option 1: Proposer Builder Separation (PBS)

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)

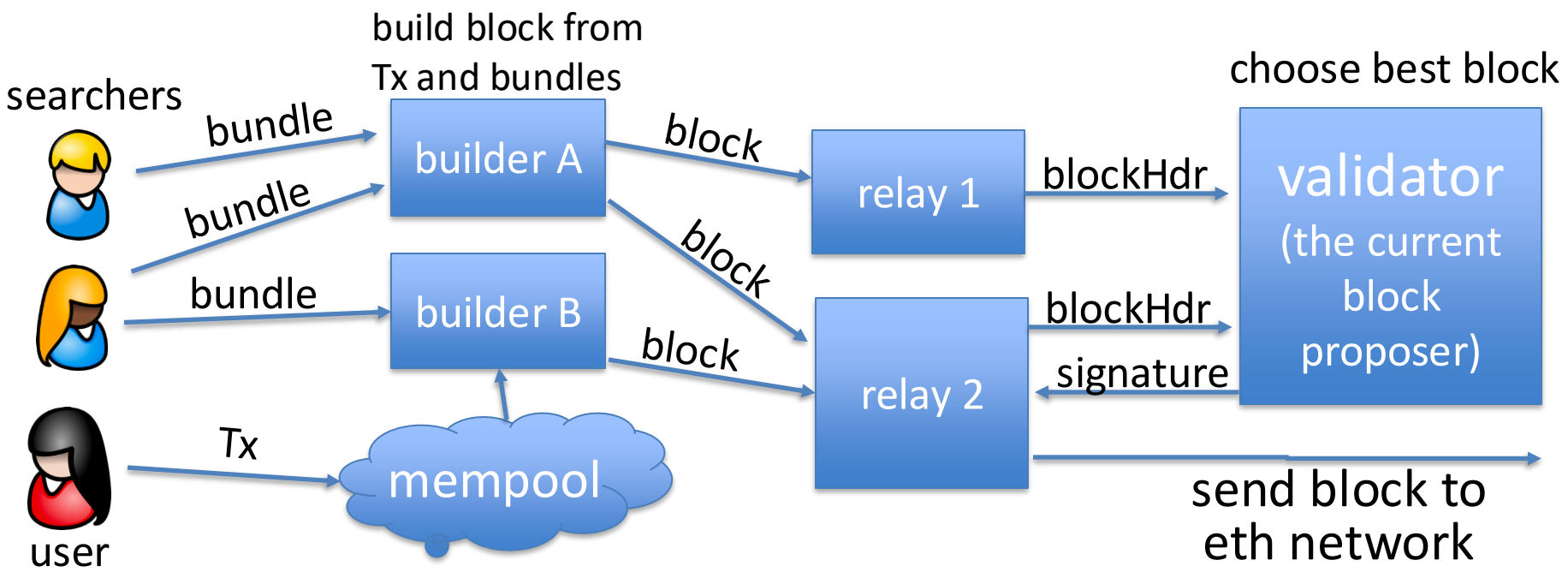


Time to Bribe

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)

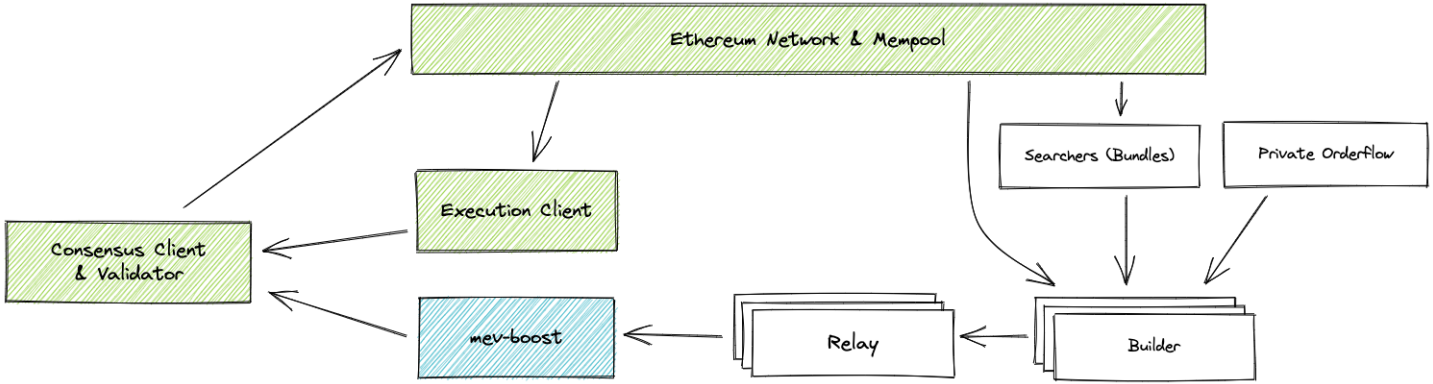
Proposer: chooses best offer and signs header with its staking key

⇒ Then Relay sends block to network, making it public

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

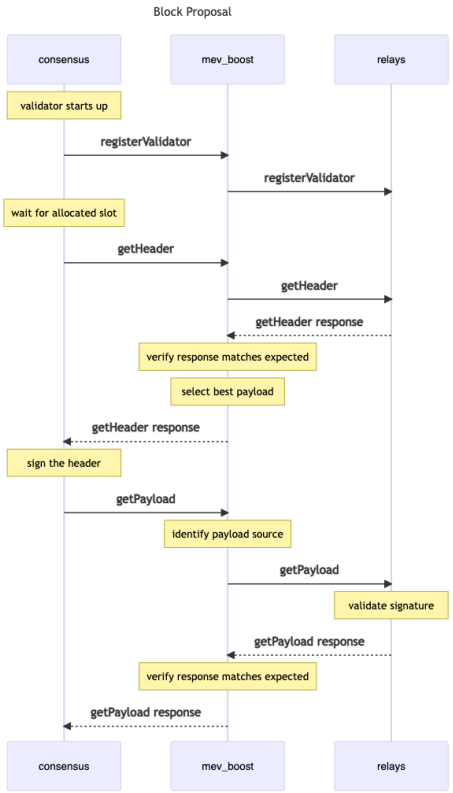
https://writings.flashbots.net/searching-post-merge

MEV-boost



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

What actually happens in a slot



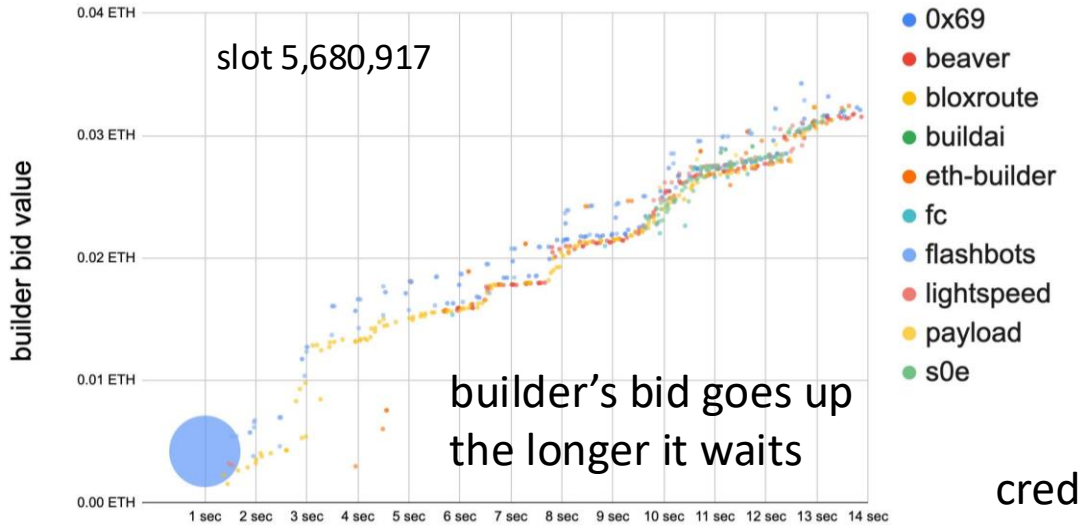

```
{
  "jsonrpc": "2.0",
  "id": 1,
  "method": "eth_sendBundle",
  "params": [
    {
      txs,               // Array[String], A list of signed transactions to execute in an atomic bundle
      blockNumber,       // String, a hex encoded block number for which this bundle is valid on
      minTimestamp,      // (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

...

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)	771570 (59.53%)	131	0.07355341 ETH	280.12114539 ETH (Slot 10,907,119)	56751.61060244 ETH	Yes	Yes
BloXroute [Max-Profit] (Relay)	637948 (49.22%)	68	0.07496127 ETH	1243.34455623 ETH (Slot 10,977,050)	47821.39640934 ETH	No	Yes
BloXroute [Regulated] (Relay)	538112 (41.52%)	69	0.07551597 ETH	1243.34455623 ETH (Slot 10,977,050)	40636.05133364 ETH	No	Yes
Titan (Relay)	256284 (19.77%)	81	0.08920678 ETH	1243.34455623 ETH (Slot 10,977,050)	22862.27268369 ETH	Yes	Yes
Flashbots (Relay)	103690 (8.00%)	112	0.11181069 ETH	2144.01166801 ETH (Slot 11,060,728)	11593.65128769 ETH	No	Yes
Agnostic (Relay)	91676 (7.07%)	90	0.11791272 ETH	170.68440865 ETH (Slot 10,976,876)	10809.76651939 ETH	Yes	Yes
Aestus (Relay)	37977 (2.93%)	57	0.08282054 ETH	160.01327199 ETH (Slot 10,626,020)	3145.27598773 ETH	Yes	Yes
Eden Network (Relay)	17609 (1.36%)	62	0.08104995 ETH	90.13824778 ETH (Slot 11,432,069)	1427.20861226 ETH	No	???
Manifold (Relay)	286 (0.02%)	8	0.05034166 ETH	1.74608215 ETH (Slot 10,482,936)	14.39771675 ETH	Yes	Yes

Top builders

Latest Blocks | Top Blocks

Slot	Proposer	Relays	Block Reward	Block Extra Data	Proposer Fee Recipient	Builder
11,753,735	1767662	Titan (Relay)	0.02095425 ETH	Titan (titanbuilder.xyz)	0x9361F2...4881d1	0xa9d0a0...2fdaef
11,753,734	1505900	BloXroute [Max-Profit] (Relay)	0.03370540 ETH	Titan (titanbuilder.xyz)	0x388C81...B19297	0xb4a435...1caa5d
11,753,733	1921502	Flashbots (Relay)	0.01935222 ETH	Titan (titanbuilder.xyz)	0x68B143...907b8A	0x95c8cc...81f742
11,753,732	206476	ultra sound (Relay)	0.02013654 ETH	beaverbuild.org	0x388C81...B19297	0x99dbe3...40da96
11,753,731	1912088	BloXroute [Max-Profit] (Relay)	0.04726965 ETH	Titan (titanbuilder.xyz)	0x0AD1B3...129385	0xb26f96...48e681
11,753,730	718480	ultra sound (Relay)	0.02844904 ETH	Titan (titanbuilder.xyz)	0xd4E96e...7605b7	0xb67eaa...8eab08
11,753,729	1790564	BloXroute [Max-Profit] (Relay) BloXroute [Regulated] (Relay)	0.01730279 ETH	beaverbuild.org	0xAF11d5...5E3ca7	0xa412c4...3b9504
11,753,726	1090764	ultra sound (Relay)	0.02762697 ETH	Titan (titanbuilder.xyz)	0x7dA0aE...859dF8	0xb47963...2d5144
11,753,725	1060312	ultra sound (Relay)	0.03389839 ETH	beaverbuild.org	0x388C81...B19297	0xb211df...96df7c
11,753,724	1681941	BloXroute [Max-Profit] (Relay)	0.04032179 ETH	Titan (titanbuilder.xyz)	0x73f7b1...51dd58	0x95c8cc...81f742
11,753,724	1681941	BloXroute [Regulated] (Relay)	0.04032179 ETH		0x73f7b1...51dd58	0xb67eaa...8eab08

Top builders (in % of blocks)

MEV-Boost Analytics

Updated at slot 11753775 (6 minutes ago)

Overview · Builder Profitability

7d · 24h · 12h · 1h

Relay	Payloads	Percent
relay.ultrasound.money	23,608	40.27 %
bloxroute.max-profit.blxrbdn.com	14,775	25.20 %
bloxroute.regulated.blxrbdn.com	9,738	16.61 %
titanrelay.xyz	5,408	9.22 %
boost-relay.flashbots.net	2,573	4.39 %
relay.edennetwork.io	1,074	1.83 %

Builder (extra_data)	Blocks	Percent
Titan (titanbuilder.xyz)	20,384	44.10 %
beaverbuild.org	14,035	30.37 %
BuilderNet	5,466	11.83 %
BuilderNet (Beaver)	2,977	6.44 %
BuilderNet (Nethermind)	1,277	2.76 %
BuilderNet (Flashbots)	1,212	2.62 %

So what?

Builder concentration: two builders build majority of blocks

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

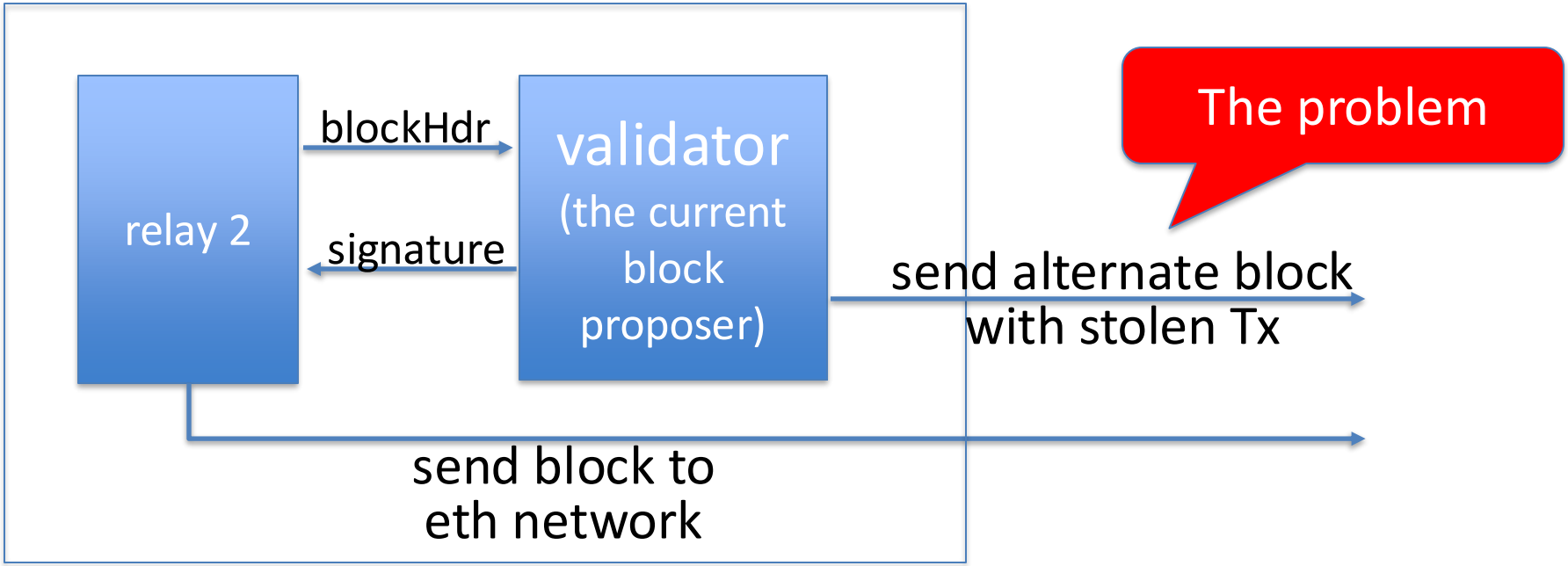
Proposers hold all the power (first price auction among builders)

$\Rightarrow$ 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

The SUAVE Multiparty Computation

Goals:

- Tx should be private (encrypted) until signed by block proposer

  ... but should be available to all block builders to build blocks

Seems contradictory! crypto to the rescue:

⇒ requires a ~~massive MPC or~~ secure HW enclaves

The SUAVE Multiparty Computation