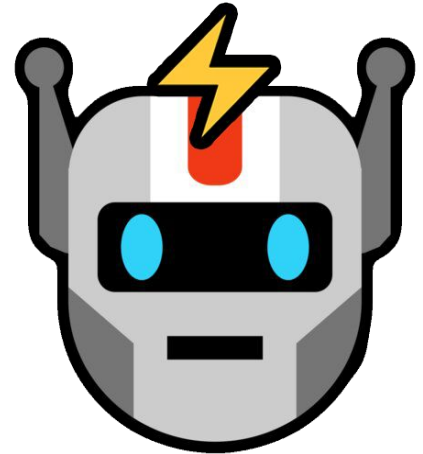


MEV across crypto in 2021

Robert Miller

MEV.day, Amsterdam



MEV activities at 30,000 feet



I want to talk about three broad categories of MEV activities today

- Extraction: efforts to capture MEV across crypto
- Externalities: negative effects from MEV extraction
- Mitigation: efforts taken to reduce negative externalities

We'll begin by looking at some numbers

MEV by the numbers: ETH L1



mev-explore: \$475.41m

community 🥪 profit estimate: \$379.92m

NFT MEV: ~\$75m?

Maker liquidations: ~\$25m?

Other long tail (liquidity sniping, etc): ~\$50m?

Total: ~\$900m - \$1bn

Not included: non-atomic arb, e.g. CEX <> DEX arbs

MEV by the numbers: other L1 chains



Polygon: **\$43.3m**

BSC: **\$55.79m**

Avalanche: **\$18.84m**

Solana: **\$8.31m**

Total: ~\$126m

Sources

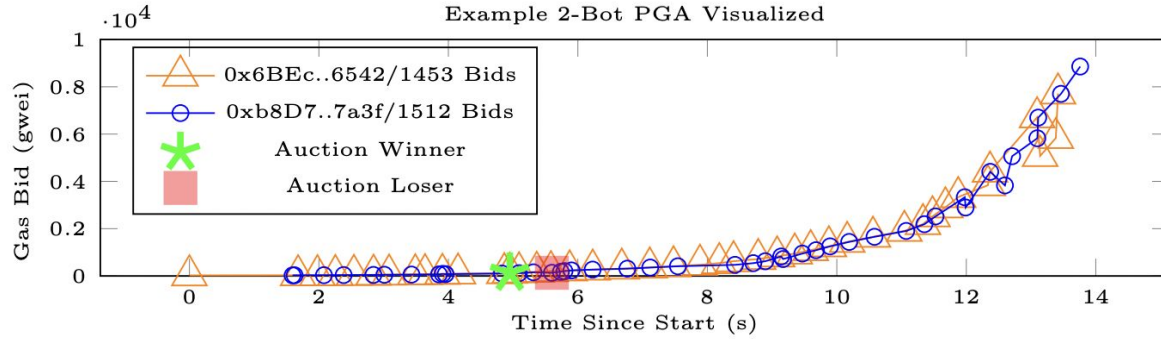
Polygon: Marlin Protocol, Explore, Jan 1st - Dec 31st 2021

BSC: Eigenphi, June 1st - Dec 31st 2021

Avalanche: Will Sheehan, August 1st - Dec 31st 2021

Solana: 0xMisaka, August 1st - Dec 31st 2021

Extraction strategy: Priority Gas Auctions



- An iterative game where bots competitively bid up transaction fees in an effort to receive priority in a block
- Bots competing on having the best networking, latency, and view of the mempool

Externality: wasted blockspace



@bertcmiller ⚡🤖
@bertcmiller

In a block earlier there was a \$70k arb won by a Flashbots user. Losing PGA bots sent over 20 useless transactions & one paid 17ETH in fees!

Ultimately none of these 20+ useless txs would have landed on chain if all these bots used Flashbots
etherscan.io/txs?block=1227...

2:14 PM · Apr 20, 2021 · Twitter Web App

| From | Transaction Type | Time | Age | Hash | Gas Used | Gas Price | Value | Fee |
|--------------------------|------------------|----------|-------------------|--------------------------|----------|--------------------------|------------|-------------|
| 0x0441b9eafabcc4db1c... | Delegate | 12277790 | 2 hrs 45 mins ago | 0xe47c990171cfe8cb8... | → | 0x860bd2dba9cd475a61... | 0 Ether | 0.59786663 |
| 0xb9196d9afbf052b38f... | Transfer | 12277790 | 2 hrs 45 mins ago | 0x69181a03fd84d1e267... | SELF | 0x69181a03fd84d1e267... | 0 Ether | 0.0187817 |
| 0x826226f2f4608a4739... | 0x5433ee39 | 12277790 | 2 hrs 45 mins ago | 0x00000000bdf114f55a8... | → | 0x00000000000005117d... | 0 Ether | 0.10251143 |
| 0x01b999e6291caed89... | 0x5433ee39 | 12277790 | 2 hrs 45 mins ago | 0x0000000759c3cd89... | → | 0x00000000000005117d... | 0 Ether | 0.10251143 |
| 0x5d9bb75013e00794cf... | 0x102241f1 | 12277790 | 2 hrs 45 mins ago | 0x41ed16c0982099bf5d... | → | 0x00000000000007f150b... | 0 Ether | 0.04811905 |
| 0x82fc67e381901c0c9cf... | 0x855a6b4f | 12277790 | 2 hrs 45 mins ago | 0x33b28888803e1bc1d... | → | 0x7ee8ab2a8d890c000a... | 0 Ether | 0.03455502 |
| 0x2203758072b9095e73... | 0x5433ee39 | 12277790 | 2 hrs 45 mins ago | 0x000000003370b0e6... | → | 0x00000000000005117d... | 0 Ether | 0.12431401 |
| 0x755d4aabf2b1bb29a1... | 0x855a6b4f | 12277790 | 2 hrs 45 mins ago | 0x614750e0d05f031a3ee... | → | 0x7ee8ab2a8d890c000a... | 0 Ether | 0.03564708 |
| 0x83517cd72f4d6b29c0... | 0x855a6b4f | 12277790 | 2 hrs 45 mins ago | 0x362adc1e2e437b0ea0... | → | 0x7ee8ab2a8d890c000a... | 0 Ether | 0.03454429 |
| 0x76e3e0496549fb54... | 0x5433ee39 | 12277790 | 2 hrs 45 mins ago | 0x000000003a5154bc2a... | → | 0x00000000000005117d... | 0 Ether | 0.12429256 |
| 0x487ee16bdcd9ac58cc... | 0x1038ab0 | 12277790 | 2 hrs 45 mins ago | 0x0336e78e4d09b86a8... | → | 0x00000000000007f150b... | 0 Ether | 0.03605251 |
| 0xd3eab89399a0361d2c... | 0x1022ab0 | 12277790 | 2 hrs 45 mins ago | 0x2029f47eb80ecc2e4... | → | 0x00000000000007f150b... | 0 Ether | 0.11846131 |
| 0x05d4b9c4... | | 12277790 | 2 hrs 45 mins ago | 0xf146b0bdf89b704d09a... | → | 0x628642fe0ab20dccc... | 0 Ether | 0.15109182 |
| 0xf9313b54... | | 12277790 | 2 hrs 45 mins ago | 0xee698b39655285d400... | → | 0x53be2d32b2bb522db6... | 0 Ether | 0.6539241 |
| 0x05a496c4bfee141079... | 0x103485 | 12277790 | 2 hrs 45 mins ago | 0x029f388ac4d5c8bf490... | → | 0x00000000000007f150b... | 0 Ether | 0.03804663 |
| 0x74011fc155e00388acc... | 0x8694cd3 | 12277790 | 2 hrs 45 mins ago | 0x94d8522c80bb261c14... | → | 0xb958a8f59ac6145851... | 0 Ether | 0.631575 |
| 0x814664c0a8b20f86a3... | 0x68c25b | 12277790 | 2 hrs 45 mins ago | 0x680175608d2efacc73... | → | 0x3d71d79c224999e608... | 0 Ether | 0.08355394 |
| 0x165bd94b1cc05eacfd6... | Transfer | 12277790 | 2 hrs 45 mins ago | 0x8d056d457a52c4daf7... | → | 0x2ad7d7faebcc97f3e2... | 0.54 Ether | 0.021231 |
| 0x587e6f6addcaeda5e8... | 0x5433ee39 | 12277790 | 2 hrs 45 mins ago | 0x0000000c9916569fd... | → | 0x00000000000005117d... | 0 Ether | 0.11445743 |
| 0x9363dcb6bb156ef7d3b... | 0x1022ab0 | 12277790 | 2 hrs 45 mins ago | 0x23e28b5adbf08319b... | → | 0x00000000000007f150b... | 0 Ether | 0.14080515 |
| 0xdd5405c28e31c024ae... | Transfer | 12277790 | 2 hrs 45 mins ago | 0x00e43c0bfa23033102... | SELF | 0x00e43c0bfa23033102... | 0 Ether | 0.02691123 |
| 0x2e19311899516e96f1... | 0x5433ee39 | 12277790 | 2 hrs 45 mins ago | 0x0000000b2de13965f... | → | 0x00000000000005117d... | 0 Ether | 0.20619804 |
| 0x6350c0a82635d9913... | 0x1022ab0 | 12277790 | 2 hrs 45 mins ago | 0x21f179df331cd85833... | → | 0x00000000000007f150b... | 0 Ether | 0.1407024 |
| 0x0606c380a526f0daae... | 0xd13966a2 | 12277790 | 2 hrs 45 mins ago | 0xedefdf37f23e326f2b... | → | 0x00000000000005117d... | 0 Ether | 17.59644808 |
| 0x655999fada0e846a4... | 0x103485 | 12277790 | 2 hrs 45 mins ago | 0x003d5f6030b8c1a4d2... | → | 0x00000000000007f150b... | 0 Ether | 1.18251704 |
| 0x535a37bc5c348a0a73... | | 12277790 | 2 hrs 45 mins ago | 0x3e4d248fb892e7ac2a... | → | | 0 Ether | 0 |

20+ transactions from bots whose transactions have failed

1 tx from a Flashbots bot operator capturing a ~\$70k arb

Mitigation: MEV-Geth



Flashbots: Frontrunning the MEV crisis

Economics ■ mev

MEV-Geth: A proof of concept

We have designed and implemented a proof of concept for permissionless MEV extraction called MEV-Geth. It is a sealed-bid block space auction mechanism for communicating transaction order preference. While our proof of concept has incomplete trust guarantees, we believe it's a significant improvement over the status quo. The adoption of MEV-Geth should relieve a lot of the network and chain congestion caused by frontrunning and backrunning bots.

| Guarantee | PGA | Dark-txPool | MEV-Geth |
|----------------------|-----|-------------|----------|
| Permissionless | ✓ | ✗ | ✓ |
| Efficient | ✗ | ✗ | ✓ |
| Pre-trade privacy | ✗ | ✓ | ✓ |
| Failed trade privacy | ✗ | ✗ | ✓ |
| Complete privacy | ✗ | ✗ | ✗ |
| Finality | ✗ | ✗ | ✗ |

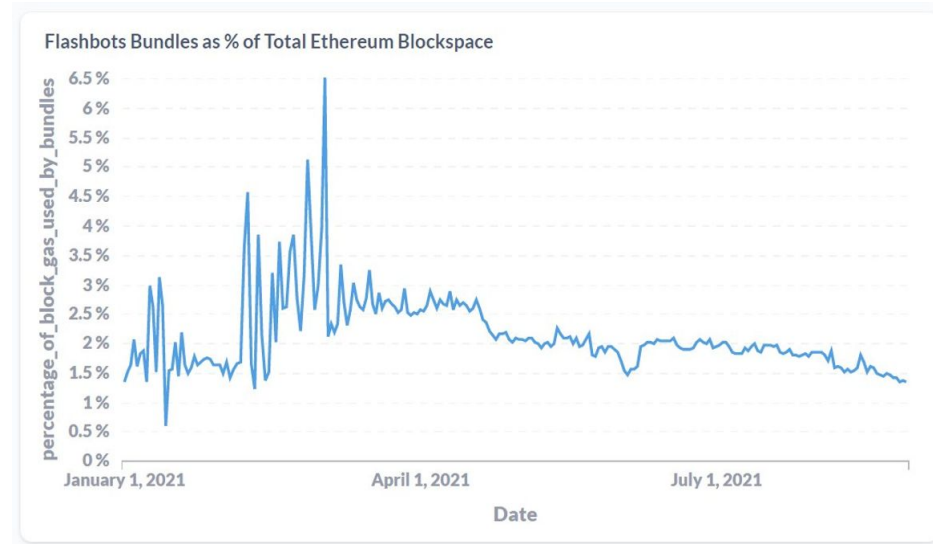
Mitigated

- Wasted blockspace from failed MEV transactions
- Centralization risk that unequal MEV extraction posed

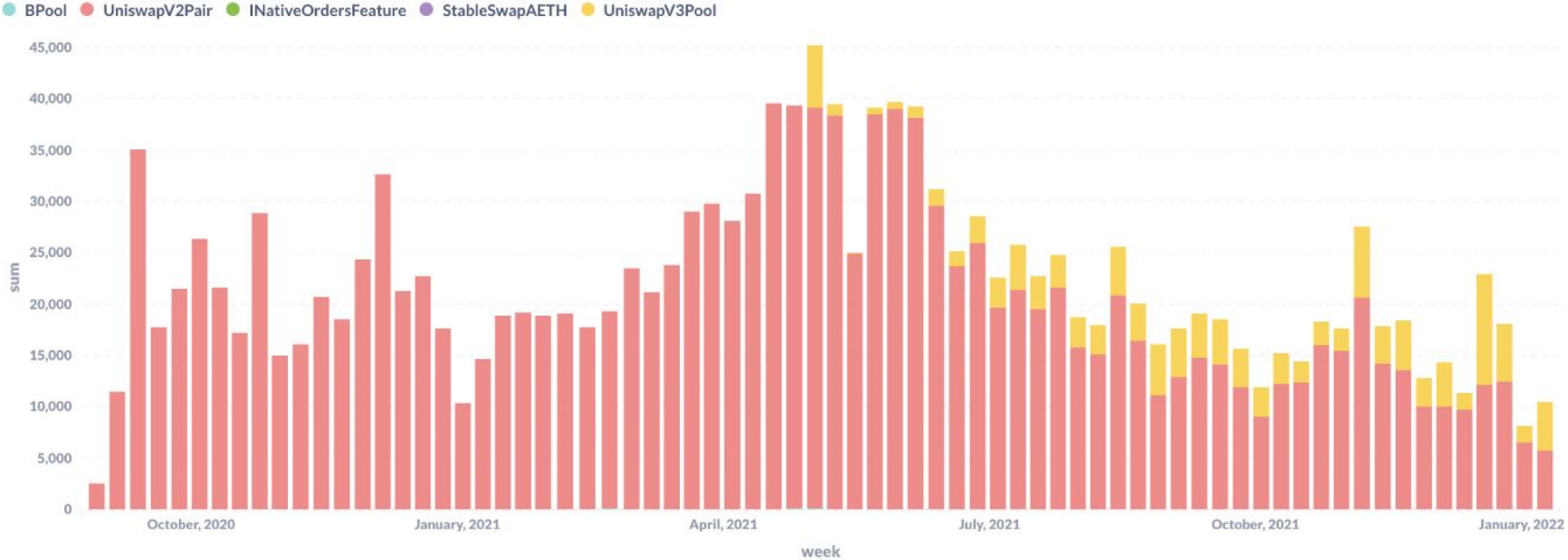
Extraction strategy: Flashbots Auction



- The Flashbots Auction optimizes for gas price to decide which txs get included
- Searchers are incentivized to make their MEV extraction as efficient as possible
- The majority of MEV for common strategies gets paid to miners
- Searchers are also incentivized to find novel forms of alpha where there is less competition



Externalities: sandwiches on Ethereum



Mitigation: Flashbots Protect



The screenshot shows the MetaMask 'Networks' interface. At the top, there's a header with the MetaMask logo, 'Ethereum Mainnet', and a globe icon. Below that is a title bar with '< Networks' and a close button. A yellow warning box states: 'A malicious network provider can lie about the state of the blockchain and record your network activity. Only add custom networks you trust.' The form fields are: 'Network Name' (Flashbots RPC), 'New RPC URL' (https://rpc.flashbots.net), 'Chain ID' (1), 'Currency Symbol (optional)' (ETH), and 'Block Explorer URL (optional)' (https://etherscan.io). At the bottom are 'Cancel' and 'Save' buttons. Red arrows with numbers 3 and 4 point to the 'New RPC URL' and 'Save' buttons respectively.

| Mitigated |
|--|
| - Frontrunning risk to users from sending their trades in the public mempool |
| - No gas cost from failed transactions |

Add <https://rpc.flashbots.net> to your MetaMask to use Flashbots Protect!

Extraction strategy: on-chain search spam



- For a chain with first-come-first-serve ordering and fast block times, if blockspace is cheap enough then **searchers will look for MEV *on-chain***
- e.g. some Solana bots will flood the network with transactions that look for arbs on-chain, hoping that they land behind a transaction that generated one, and reverting if not

| | |
|---------------------|--|
| Timestamp | about 5 hours ago 🕒 March 23, 2022 08:21:48 AM +UTC |
| Result | 🟢 Success Finalized (MAX confirmations) |
| Fee | 0.000005 SOL |
| Main Actions | <p>Interact with program YoLozH...KPCxPo</p> <ul style="list-style-type: none">🔄 Transfer from 6hyuGq...urbK4W to 4ofEvM...KfQ1U for 70 USDC🔄 Transfer from 4ofEvM...KfQ1U to 6hyuGq...urbK4W for 5,620,026.91 CASH🔄 Transfer from 4ofEvM...KfQ1U to 4a8uew...J2UPWH for 0 CASH <p>Interact with program YoLozH...KPCxPo</p> <ul style="list-style-type: none">🔄 Transfer from 6hyuGq...urbK4W to 4YG45t...25ShpQ for 5,620,026.91 CASH🔄 Transfer from 4YG45t...25ShpQ to 4YG45t...25ShpQ for 2,219.86 SUNNY🔄 Transfer from 4YG45t...25ShpQ to 6hyuGq...urbK4W for 4,610,847.32 SUNNY <p>Interact with program YoLozH...KPCxPo</p> <ul style="list-style-type: none">🔄 Transfer from 6hyuGq...urbK4W to 7NP8DT...aD8rrp for 4,610,847.32 SUNNY🔄 Transfer from 7NP8DT...aD8rrp to 6hyuGq...urbK4W for 15,802.82 USDC |
| Previous Block Hash | HCvTVuYi93w3BPhtAPLmSMcFvUDJxEzuTFWu3ewTYFMN |

Externalities: MEV leading to downtime for users



ceteris

@ceterispar1bus



tldr of what i understand is, solana limits the amount of compute in tx's, this was fine half a year ago, but now for more complex defi stuff the amount of compute on network is skyrocketing, liquidation bots causing issues. compute fee based model will be needed.

...ect of the issues:
...eraged position on DeFi where he borrows USDC against SOL collateral. If SOL price drops 20% his position would be li
...s 20%
...s eligible for liquidation. But DeFi doesn't work like regular banking, there's no automated backend processing stuff
...a liquidator and can "trigger" the liquidation of Bob's position, since it has now become eligible for liquidation
...y doing so the liquidator gets a bounty (reward)
...s large market movements lots of DeFi positions become eligible for liquidation, just like Bob's
...racing to collect bounties by being the first to liquidate positions
...submit the transaction dozens or hundreds of times to the network in order to ensure their attempt succeeds
...n't sufficiently removing duplicate transactions before processing and verifying them, which is a compute intense proces
...network is stuck trying to sift through all the "spam" from the liquidation bots
...mented in the new release 1.8.14 fix a lot of this, this is being tested on mainnet now with 8% of stake, as it is confirmed
...led out
...an incredible and exponential explosion of DeFi usage in recent months which didn't exist six months ago or a year ago,
...much much more "expensive" to compute so the amount of "compute" the network is doing has increase massively. Ear
...und deduplication weren't a problem as the compute load was lower but now this has become a bottle neck.
...makes significant inroads in fixing this, but right now all we can do is be patient and trust that everyone capable is work



Solana Status @SolanaStatus · Jan 22

Mainnet Beta Validators: Please upgrade to github.com/solana-labs/so...

1:08 PM · Jan 22, 2022 · Twitter Web App

Extraction strategy: network propagation spam!



- There is randomness in which transactions are propagated to Polygon and Solana validators
- If you want to ensure your transaction gets to a validator in time, you are incentivized to spam the validator with transactions!

Reduce competitive spam by having sentries always send full transactions to validators #292

Closed ajb wants to merge 1 commit into `maticnetwork:master` from `ajb:ajb/fix-spam`

Conversation 14 · Commits 1 · Checks 0 · Files changed 2

ajb commented on Jan 10 · edited

Competitive spam is a huge problem on Polygon. There are many blocks where over 90% of the transactions are from arbitrageurs trying to get a "backrun", where they land immediately after a target transaction, by sending a transaction with the same exact gas price.

This is not a new thing. Geth has dealt with this before, which is why they implemented [ethereum/go-ethereum#21358](#). In addition, there have been similar issues opened for BSC [bnb-chain/bsc#269](#), and here in the Polygon repo: [#209](#) (cc @ferranbt @moneyoriented)

This has also been highlighted on Twitter by threads such as this one: <https://twitter.com/bertcmiller/status/1412579402345586696> from @bertcmiller

However, Polygon actually implements the geth PR already! So why does this continue to happen, only on Polygon much worse than other chains?

<https://github.com/maticnetwork/bor/pull/292>

Externalities: spam!



@bertcmiller ⚡🤖
@bertcmiller

Low fees + low latency + PGAs = spam

A token sniper on BSC is spamming HARD to get where they want in blocks. This block they used ~1000 txs and the majority of the block to get the tokens they wanted!



bscscan.com
Binance Transactions Information | BscScan
Transactions that have been validated and confirmed on the Binance Blockchain. The list consists of transactions from ...

1:38 PM · Nov 26, 2021 · Twitter Web App

||| View Tweet analytics

14 Retweets 4 Quote Tweets 115 Likes



Carnation (👉, 💰)
@Oxcarnation

On aurora dexes, we are starting to observe accounts spamming hundreds of txns worth a tenth of a penny.

Taking a slightly closer look it's MEV bots doing triangular arbs

On a gas-less chain, the proliferation of these bots will lead to network congestion

| Value |
|----------|
| 0.002518 |
| 0.002518 |
| 0.002521 |
| 0.0126 |
| 0.01259 |
| 0.01259 |
| 0.02523 |
| 0.002524 |

11:24 PM · Apr 8, 2022 · Twitter Web App

10 Retweets 8 Quote Tweets 171 Likes



@bertcmiller ⚡🤖
@bertcmiller

MEV negative externalities

This Polygon bot has been active since June 29th & has sent ~2m transactions, failing *almost* all the time

These failures cost close to nothing but bloat the state, while the few successes pay for the failures many times over

```
Transaction Hash: 04c331b68853875cc2219fd53e8a7937c382428e1a62041951ed19847e8773
Status: Success
Block: 16581504 (159 Block Confirmations)
Time: @ 40 mins ago (Jul-07-2021 12:23:00 AM +UTC)
From: 0x87acc52d99e1c574f4a3b39f115235860c02546
To: 0x0786db079793421127342053a42b755f9a21
Action: Swap 9.267937356568663841 @ YIELD For 1,802.181339 @ USDC On QuickSwap
Transferred:
- From 0x0786db079793421127342053a42b755f9a21 For 1,567.49396868490958002 @ Wrapped Mat...
- From 0x0550d0c827447... To 0x0a89c06e2875... For 9.267937356568663841 @ PolyYield Tok... (YIELD)
- From 0x0a89c06e2875... To 0x87a796a0e905... For 1,802.181339 (1,802.18) @ USD Coin (P... (USDC)
- From 0x87a796a0e905... To 0x0786db079793421127342053a42b755f9a21 For 1,563.109330917555115723 @ Wrapped Mat... (WETH)
```

9:09 PM · Jul 6, 2021 · Twitter Web App

- Wastes blockspace and raises cost for regular users
- Adds a ton of load to the p2p layer
- Bloats state over time

Externalities: spam bringing networks down



Composability Toly,  

@aeyakovenko



Replying to [@gilledcheese](#)

Bots during a raydium ido are flooding the network at 300k txs per second. The queues that forwards txs to block producers grew in size to a point that caused excessive forking. The fix to prioritize messages in this queue was already in the works but wasn't out yet.

11:10 AM · Sep 14, 2021 · Twitter Web App

Mitigation: fee markets, block producer optimizations

Extraction strategy: maximize stake weight, fast gossip



Pre-snowman++! Not anymore!

- Maximizing your % of stake to hear about unconfirmed blocks ASAP
- Gossip blocks with MEV extraction ASAP, even with full nodes
- Result: **lots of competing blocks**

<https://www.youtube.com/watch?v=1NmVORC2R-A>

Snowman (before Snowman++)

- Distribution: Sample $K=20$ validating nodes by weight with replacement
 - Technically, sample K nanoAVAX (equivalent of Ethereum's wei) without replacement. Due to $O(10^{**21})$ odds of a repeated sampling, one can reasonably ignore this technicality
- Messages: C-Chain blocks, not transactions, were gossiped
- Strategy: Maximize staked AVAX to hear about unconfirmed blocks ASAP
- Strategy: Gossip blocks containing MEV-extracting transactions ASAP
 - Any node, including non-validators, could propose a block
 - This led to contention issues, as competing searchers would publish dozens of blocks at the same height.
- Note that all transactions had a gas price of 225 gwei. So there were no gas-price-priority games

Interplay Between Protocol Design and MEV Strategies on Avalanche - Ward Bradt

Externalities: MEV leading to networking load



@bertcmiller



@bertcmiller



A nice demonstration of why protocols need to design in an MEV aware way from day 1

There was an edge in having many non-validating nodes on Avalanche, so MEV bots launched 1000s of them "dragging the whole network down" with increased load/latencies [twitter.com/convexdegen/st...](https://twitter.com/convexdegen/status/1461111111)

This Tweet was deleted by the Tweet author. [Learn more](#)

12:02 PM · Nov 23, 2021 · Twitter Web App

Mitigation: Snowman++



Optimization 1: Snowman++ (Reducing MEV & Contention)

In Avalanche, any node can produce a block at any time as long as that block contains some non-zero number of fee-paying transactions. After producing a valid block, it is up to the consensus engine, known as Snowman, to finalize one of the many potentially conflicting blocks at any given height. Regardless of the magnitude of the contention, Snowman eventually clears through all conflicts and accepts 1 block at each height (rejecting all others). As a general principle, however, the lower the contention, the faster the time to finality (less resources spent resolving conflicts).

Extraction strategy: latency optimization



- First-come-first-serve chains with moderate and up fees (e.g. rollups) incentivize searchers to try to have the lowest latency possible
- Latency games I've seen:
 - An underground full node guide being passed around discord when there was no public guide for a rollup
 - Searchers launching 1000s of AWS servers to find the one that is closest to a sequencer
 - An oracle team also running a liquidation bot



ARBITRUM



Externality: block producer centralization



- The faster your block time the harder it is to optimize for MEV extraction in that time
- Searchers are incentivized to colocate with validators (or become one), these kinds of deals are hard to make transparent or democratize
- **Intuition:** chains where latency optimization is the dominant strategy trend towards block producer centralization over time
- Besides, do we really want to reproduce HFT style latency wars in crypto again?


Mitigations on the horizon



MEV Resistance

Osmosis's upcoming roadmap includes the tackling of maximum extractable value (MEV), one of the largest challenges seen in decentralized transactions. Since all trades are facilitated through the blockchain – meaning they're available on the public ledger – miners are able to rearrange transactions within their block to their own benefit. Miners would have an advantage over ordinary users in situations where it is important to get a transaction approved first, such as for front-running trades or acquiring a prized NFT. This type of MEV behavior disadvantages DEX users in favor of those with privileged access to the blockchain.

MEV originated as a privacy issue only to evolve into a financial one. According to MEV Explore, over \$600 million has been extracted away by miners since January 2020 on Ethereum alone.

 Jito Labs

**Building
Solana
MEV
Infrastructure**

Flashbots

[Home](#) / [Announcements](#)

Creating a Highly Scalable and MEV-Resistant DeFi Ecosystem Using Arbitrum and Fair Sequencing Services

December 9, 2021 • Chainlink

The [smart contract](#) economy has created a large ecosystem of decentralized applications in only a few years time, supporting unique markets like [decentralized finance](#) (DeFi), [Non-Fungible Tokens](#) (NFTs), [play-to-earn gaming](#), and many more. However, if the smart contract economy is to onboard the next billion users and become the dominant system of contractual agreements, it will need to both scale its transaction processing capabilities and maintain high levels of trust by minimizing the harmful effects of [Miner-Extractable Value](#) (MEV). In this post, we will explore Chainlink's recommended solution for scaling smart contracts on Ethereum, Arbitrum, and how Arbitrum and Chainlink are together exploring solutions to create fairer smart contracts by eliminating MEV on Arbitrum.

APR 4, 2022 • 5 MIN READ • ROLLING SHUTTER

Rolling Shutter: MEV protection built into Layer 2

Summary



In 2021 across crypto we saw:

- The rise of a professionalized class of MEV extractors
- As a lower bound over a billion dollars in MEV captured
- Protocol design being stress tested under adversarial conditions
- Networks buckling and even failing under stress from MEV searchers
- MEV mitigations were implemented, more are being pursued in 2022

Thanks for listening :)

@bertcmiller on Twitter / Telegram

botcmiller#4207 on Discord