One Block - One Batch

Application Design
Choices reducing MEV

Anna George
CoW Protocol
Agenda

1. Status Quo: (De)Centralization of PoS
2. Utopian future for Ethereum
3. Application Design Choices
4. CoW Protocol
Status Quo: (De)Centralization of PoS
How Decentralized is PoS?
● Validators within at least one epoch are known, allows for multi block and cross chain MEV extractions

● Response: Proposer-Builder-Separation (PBS)
PBS may greatly improve validator decentralization, but it risks leaving builders very centralized:

- One builder may well produce >60% or even >95% of all blocks
- Private Order Flow increases centralization risk
MEV in PoW vs PoS

MEV before & after the Merge
Comparing last and first 145,000 Blocks

![Chart showing MEV in PoW vs PoS before and after the Merge](chart.png)
MEV in PoW vs PoS

Sandwich

USD

<table>
<thead>
<tr>
<th>day</th>
<th>0.00</th>
<th>50,000.00</th>
<th>100,000.00</th>
<th>150,000.00</th>
<th>200,000.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ZEROMEV
MEV-Boost Centralization

Transparency dashboard

Percentage of blocks proposed by Flashbots MEV-Boost Relay vs. other by day

Flashbots MEV-Boost Relay | Other

% of blocks proposed

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

September 18, 2022 | September 25, 2022 | October 2, 2022

49%
Percentage of Validators
MEV-Boost Relay Centralization

>40% of all blocks on Ethereum today are censoring tx from accounts that interacted with Tornado Cash.
25% of all Ethereum blocks are crafted by two builders.

On top of that: Private order flow as additional centralization risk!
Dystopian Future Scenario

A single block builder craft >80% Ethereum blocks.
Utopian Future for Ethereum
The Utopian Future for Ethereum

“My goal is insulating the Ethereum base layer from centralizing tendencies.”
– Vitalik

- Healthy base layer shielded from political pressure and centralizing forces
- Risks absorbed by layer2s and applications
“The best mitigation for MEV is not to sell the MEV to someone who can extract it, it’s to create applications that don’t expose as much MEV.”

Stephane Gosselin, Founder @ Flashbots
Application Design Choices
What is the root of MEV?
The Root of MEV: one asset, many prices

Sequential Execution in 1 block

1. Buy-Order
2. Buy-Order
3. Buy-Order
4. Sell-Order
The Root of MEV: Inefficient & Unfair Pricing

ETH-USD Price occurrences

Dune Analytics

example block: 15673043

Sequential Trade Execution:

Prices in a block spread over a spectrum → MEV Opportunities

price spread of 1.05%
https://dune.com/queries/1382032
Batch Auctions on Blockchains

**Additional price improvement 930$**
[https://dune.com/queries/1382324](https://dune.com/queries/1382324)

**Batch auctions:**
One Price per Batch $\rightarrow$ no MEV

Example block: 15673043

[ETU-USD Price occurrence chart]

**Dune Analytics**
Minimizing MEV: Batch Auctions

Miners Frontrunning

Miners can see all the contract code they run (obviously), and the order in which transactions run is up to individual miners.

What is to stop front running by a miner in any market place implementation by ethereum?

For example, in an ethereum decentralized stock exchange, I could run a miner (or rather many miners) processing exchange transactions. When a large buy order comes in, I could delay it on all my miners, put a buy order in myself on all my miners simultaneously, and then process the original transaction. I would get the best price, and could possibly even sell to the originator for an immediate profit.

You wouldn't need anything close to 50% of mining power, because you aren't breaking any network rules. It would probably be profitable even if it only worked a fraction of the time, as in a low transaction fee environment, you could afford many misses for a few hits.

This is true for many of the proposed killer apps on ethereum, including peer-to-peer betting, stock markets, derivatives, auction markets etc.

It seems like a big problem to me, and one fundamental to the way ethereum operates.

Any ideas on this?

vbuterin - 8 yr. ago

Just some guy

One idea is process orders in batches rather than sequentially. Specifically, let orders accumulate for a few blocks, and then come up with a list of all orders that have appeared during that time sorted by price, and then match them one by one. If "a few" is something like 5, then there are going to be enough different miners that every order will almost always get in.
CoW Protocol
Batch Auctions in CoW Protocol

Sign message

Off-chain Order Book

CoW Batch Builders

Mempool

MEV Boost

Proposer
Batch Auctions in CoW Protocol

Sign message
Off-chain Order Book
CoW Batch Builders

Focus: Most value for user
Focus: Most value extraction
Objective Function

The key goal of a solver is to find solutions that maximize the utility of the users. However, in the objective, we also add a fee component for the service provided, and subtract costs that the transaction execution on the blockchain is expected to incur. Hence, our objective reads

$$\text{maximize } (\text{total utility}) + (\text{total fees paid}) - (\text{total execution cost}).$$
CoW Batch Builder

Staking & Slashing:

CoW Batch Builders (“Solvers”) stake tokens to participate in the competition.

In case of malicious behaviour gets slashed.

When winning the competition they get rewarded by the protocol.
$2300 of added surplus from batching:
- $800 Reduced LP fees
- $1500 Reduced price impact

Execution price: 48.2 USDC for FOLD
Protecting from MEV
One Block - One Batch

CoW Protocol

Batching and finding best paths per order

Submit Batch to Block Builder

12 seconds
Fight MEV at the application layer!

Github @cowprotocol
Open positions cow.fi/careers
Twitter @CoWSwap