MEV Driven Centralization in Ethereum: Part 1

Simon Brown

Follow

--

2

Listen

Share

With the merge looking likely to happen within the next couple of months, I thought it would be interesting to write a post that speculates how MEV will affect Ethereum's landscape after the merge. Being this close to the merge gives me the opportunity to publish a two part "before-and-after" series of posts that compare my idea about what might happen to what does actually happen in real life, which for me, is an interesting experiment.

Overall, the objective of this post is to imagine certain scenarios that may or may not emerge, and to compare those scenarios to the ones that do actually emerge post-merge.

This post assumes you have at least a basic understanding of Ethereum's roadmap and specifically the move to proof-of-stake, as well as a grasp of the fundamentals of MEV.

Obligatory disclaimer: the opinions in this post are entirely my own, not representative of the views of my employer, colleagues or any other organization I'm associated with.

PoW to PoS

Back in 2017, when PoS was still being thought about in one of the many iterations towards "eth 2.0", Vitalik ostensibly had doubts about the degree that PoS would affect decentralization:

"all in all, the centralization balance is an empirical question for which the answer is unclear until the system is actually running for a substantial period of time".

To be fair, Vitalik has subsequently stated in other posts that he sees PoS as being more decentralized than PoW. From my perspective though, to what extent it may improve decentralization is still uncertain.

But decentralization was never the only motivating factor toward the move to PoS, there were other benefits that made it a logical choice, including being able to reduce the ETH issuance that is required to incentivize participation, because the network uses less power than PoW, meaning a lower cost to participants. It also means the network uses less energy overall, which is good for the planet.

But if the move to PoS never had a clear improvement over the level of centralisation in PoW Ethereum, well at least it couldn't make it any worse. Or could it?

Enter MEV . . .

The Flashboys 2.0 paper by Daian et al. was published in 2019, and I was lucky enough to attend a talk by Phil Daian in which he presented this paper. He warned that there was a possibility that explicit re-ordering and targeted insertion of transactions in blocks could create game theoretic incentives that could "leak down" to affect the security at the base consensus layer.

Just to put things in context, MEV does not account for a huge amount of revenue, it's a relatively small amount (according to the Flashbots' MEV Explorer anyway). Currently the amount of MEV captured from blocks is a relatively low percentage of the overall profit from the amount in transaction fees and block reward, (I put it at an average of 1.63% for the past 18 months, please correct if added up wrong).

However, with the block reward being reduced substantially with PoS, the amount of MEV becomes much bigger relative to the block reward, and this is what makes a difference.

That means that validators will want to get MEV. If they don't, well then that's money left on the table. Furthermore, it's reasonable to assume that staking pools will want to ensure that their customers know that they are receiving the best possible return on their staked ETH. That means, block rewards, transaction fees, and MEV.

Economies of scale

MEV skews the economic design of PoS Ethereum, because large staking pools will enjoy economies of scale that smaller staking pools will find difficult to compete with. Intuitively, this makes sense, because the higher the percentage of the network's validator set a staking pool has, then the more often that staking pool will have one of it's validators nominated as

proposer, and thus the more MEV that staking pool will capture, earning more capital that it can convert into more validators, and so on. For more of a deep dive into the economies of scale of MEV in PoS Ethereum, see Alex Obadia's excellent research on the subject.

But what if block building was totally separated? What if constructing the block was undertaken by another entity, separate and independent to the proposer / validator? What if these separate block builders could bid against each other to have their block proposed? Under this scenario, the validator that was nominated as proposer for a given slot needs to only accept the block from the builder that was offering the highest amount of value to the proposer. This would mean that every proposer that was nominated by the network would be able to capture the most amount of MEV possible, irrespective of how sophisticated an MEV searcher they were, leveling the playing field between validators. Also, competition between block builders bidding against each other would mean that more MEV would go to validators, smoothing out the variance in revenue that MEV caused.

Enter PBS . . .

This is exactly what Proposer-Builder-Separation aims for, to separate the construction of a block and the validation of a block into separate concerns.

Quickly it was discovered that PBS has other benefits in terms of scalability, and is one of the core requirements for danksharding, but originally it was intended to deal with the centralizing effect that MEV could have on the validator set, as described in the earlier paragraph.

PBS works by outsourcing the block building concerns to a dedicated block builder, while allowing the validators to concentrate on proposing the blocks to the network and providing attestations. This helps scalability because it means that validators have less of a heavy lift (they no longer need to expend computational effort on building blocks — or extracting MEV).

With PBS, block builders provide block headers, with a fee that will be paid to the proposer. The proposer doesn't see the block body until they commit to selecting one of the blocks being provided. Naturally they will select the block that pays them the highest fee.

In-protocol PBS is going to take some time, and the exact mechanism by which in-protocol PBS will be implemented is still under discussion, (see here, here, and here). For the time being, PBS will be implemented via mev-boost, which allows for 'relayers' to act as escrow, facilitating an open sealed-bid auction between block builders and proposer / validators.

See this ethresear.ch post for original specifications.

Validator Centralisation

What PBS / mev-boost does is smooth out the variance of validator revenue to a degree, by giving solo stakers the same chance getting as much MEV for the blocks they propose as a large staking pool, but it doesn't really fix MEV driven validator centralisation. At the end of the day, If you have 10x more validating power than the next staking pool, then you will have 10x more opportunities to earn MEV. That's more profit that you can re-invest into more validators, to have yet more opportunities for capturing MEV, and so on…

Block Builder Centralization

In order to be competitive and out-bid other block builders in the mev-boost auction, and hence have their blocks chosen by proposers, block builders will need to be able to extract more value from the transactions in the block, than the value derived from simply selecting the transactions with the highest gas fees. This means that block builders will need to rely on MEV searchers to provide the highest value transaction bundles, so that the blocks they produce will be chosen by the proposer.

From the searcher's point of view, they must choose which block builder to send their bundles to. It is reasonable to expect that a searcher will make this decision by determining which block builder is the most likely to have their blocks chosen by the proposer.

The block builder that will most likely have their blocks chosen by the proposer:

1. is the block builder that consistently presents the highest value blocks to the proposer,
2. which is the block builder that consistently has the highest number of transaction bundles to choose from,
3. which is the block builder that most searchers submit their bundles to.

It is relatively trivial for searchers to ascertain which block builders are winning bids, even in real-time.

This simple network effect creates a virtuous cycle that can plausibly lead to the emergence of a single block builder. While a single monopolistic block builder does not present any obvious threat to the network, (as they can't adversely affect the liveness or safety of the system), it does raise a number of concerns.

If we assume that there will be only a handful of dominant block builders in the space, (or even just one), then what potential implications does this have?

Let’s assume there are only a handful of dominant block builders. They must extract as much MEV as possible in order to remain competitive. That means they need to explore all avenues to to extract MEV, including:

- Censorship-as-a-Service — accept payments to censor specific transactions for x number of blocks.
- Preferential treatment — slow down withdrawals from competitor exchanges / rollups / bridges, for a fee.
- Bundling all transactions to a particular AMM trading pair into one block, in order to amplify the price impact — causing transactions with tight slippage tolerance to fail on-chain.
- Potentially offering reorgs-as-a-service in order to maximize MEV.

Even without the above mentioned tactics, there are still inter-block MEV strategies that I have no doubt will emerge.

Is this all just FUD?

I want to point out that this is all speculation at this point, and block builders may never resort to such strategies to remain competitive. Personally I don’t think that these strategies will be employed by block builders. I think block builders will take a long term view and put the health of the ecosystem above short term competitive advantage and will find a way to make it work. Nobody knows for sure, but I’m taking as guidance the fact that currently only 3 or 4 mining pools share over half the hashrate on the network (and so I presume they generate half the blocks on average). Currently the operators of these mining pools don’t engage in the sort of practices I’ve outlined above.

That being said, the other difference between block construction pre and post merge, is that currently the “other” 50% of the hashrate is very diverse, whereas if we end up 5 or 6 block builders, it may well be the case that those are the only block builders we have. If that scenario arises, it would make it much easier for regulators to target them, which is worth thinking about as we figure out how to enshrine PBS at the protocol level over the next couple of years.