This post was originally posted on 2021-12-11

Author: Robert Miller, @bert

[

1280×720 27.4 KB

](https://collective.flashbots.net/uploads/default/original/1X/cc940e333d40cf09fa9396e41a4dfabe3571f1b0.jpeg)

Central to the security of Ethereum is that every miner, and soon validator, can produce the most profitable block possible. Why is this? Why has Flashbots made it a goal to democratize access to the most profitable blocks? How are we doing so? This blog post answers these questions and more.

The changing role of miners and validators on Ethereum

In the last year the job of miners on Ethereum underwent its largest shift since Ethereum's inception. Previously miners optimized their blocks by ordering transactions they received by their gas price. There was little money to be made in investing in improving ordering by gas price. Instead miners focused on network-level optimizations, such as having a better view of the mempool or lowering the time it takes to receive new blocks.

Today miners employ much more complicated ordering schemes since the widespread adoption of techniques for extracting MEV, or maximal (formerly miner) extractable value

. MEV in this context is the value that can be captured by miners by ordering, inserting, or censoring transactions (for a formal definition of MEV see "On the Formalization of MEV"). For example, arbitraging the price difference between two assets on decentralized exchanges is a form of MEV. A miner maximizing their returns should optimize transactions in their blocks such that they capture as much MEV as possible, which juices their returns on top of the transaction fees they receive as well the block subsidy.

Arbitrage is one type of MEV alongside liquidations, sandwiches, and a long tail of more bespoke MEV strategies. The total size of the MEV market annually is nearing a billion dollars on Ethereum alone today. Indeed, individual MEV opportunities can be worth many, many times more than the block reward or transaction fees. For example, one arbitrage bot landed 2 arbitrage transactions each worth over $2m in a single day in October.

To ensure Ethereum's security it is essential that all miners can build blocks that capture these opportunities. If MEV extraction is not democratized then larger miners will be able to use their resources to optimize their MEV strategies more than other miners. With more advanced strategies larger miners will be able to generate more revenue from MEV than their peers. In turn these additional revenues can be used to grow larger, optimize more, and further cement their dominance in the network. As MEV extraction gets more complicated (e.g. cross-chain arbitrage) this dynamic is exacerbated because it will become more difficult to stay on the leading edge of MEV extraction.

To prevent the dynamic of economic centralization from MEV described above then all miners, and after the merge validators, must extract roughly the same amount of MEV relative to their share of the network. But extracting MEV is a daunting task. How can we democratize it?

Enter Flashbots Alpha

To democratize MEV Flashbots released its alpha: a marketplace for transaction ordering. Flashbots connects bot operators who find MEV, or "searchers," and miners who want to extract MEV. Searchers submit "bundles" of transactions that extract MEV and pay miners fees for including their bundles. Miners receive these bundles and include the bundles that are most valuable to them at the top of their blocks through an auction mechanism.

An example bundle from a searcher would be an arbitrage placed behind a large trade, where the miner is paid 90% of arbitrage profits by the searcher in the arbitrage transaction. For the majority of MEV strategies today searchers pay roughly 90 - 95% of profit to miners. Over time the auction structure and competition among searchers has led to most MEV being captured by miners while still supporting an ecosystem of searchers.

Miners that don't want to, or cannot, extract MEV on their own can tap into Flashbots' marketplace and have searchers extract MEV for them. All that is required is for miners to register with Flashbots, run mev-geth, the open source geth fork, and receive bundles. As a result of the market structure and ease of integration, Flashbots Alpha allows miners of any size to extract MEV and compete on producing the most profitable blocks.

The limits of Flashbots Alpha

Since release Flashbots bundles have quickly become a significant portion of a miners' overall income and have led to over $300m in profit for miners. At current rates the profit from Flashbots bundles alone is nearly a billion dollars. However, the impact of Flashbots Alpha has been constrained because the auction for block space that miners orchestrate is complex and not private.

First, searchers submit individual bundles and while many of these bundles are conflicting (e.g. they bid for the same opportunity) many bundles can be merged together without a problem. Figuring out the ordering and number of bundles that optimizes a miner's profits is a very difficult problem and is broadly referred to as "bundle merging."

To merge bundles together they first need to be simulated alone to understand which bundle should be placed first according to the gas price of those bundles. Then bundles must be simulated together one after another to understand if they conflict in some way. Lastly for each additional bundle that is being attempted to be merged an additional and parallel computing process needs to be created. For example, if a miner wants to merge a maximum number of 3 bundles together they will have 4 "workers": one creating a block without bundles, another creating a block with 1 bundle, a third with 2 bundles, and a fourth with 3 bundles. Then these four blocks are compared and the most profitable block is chosen.

If the details of the above are lost on you that's fine, just remember that bundle merging is a computationally complicated process. And sometimes there can be tens of thousands of bundles for a single block! Flashbots' MEV-Geth handles bundle merging for miners out of the box, but the computational complexity of merging places a cap on the number of bundles that can be included in a given block. The median miner will merge a maximum of 3 bundles per block, but many blocks have had more than 3 bundles that are profitable to include.

Moreover, Flashbots Alpha auctions off block space by optimizing for bundles with the highest gas price. Unfortunately this is not the same as optimizing for overall bundle profit. Consider the following two bundles:

- Bundle A: 100,000 gas with miner payment of 1 ETH and gas price of 10,000 GWEI
- Bundle B: 1,000,000 gas with miner payment of 9.9 ETH and gas price of 9,900 GWEI

Bundle A will win the Flashbots Auction because it has a higher gas price despite bundle B being more profitable overall for miners.

The reason this design decision was made is because optimizing bundles for gas price is computationally simpler than optimizing for overall profit. However this opens up a dimension for competition: if a miner has a proprietary solution that allows them to optimize bundles for overall profit they could extract more MEV than their peers in some cases. Similarly, being able to include more bundles per block would also lead to more MEV extraction.

Lastly, in Flashbots Alpha bundles are seen by both relays and miners. As a result searchers need to make a key trust assumption that relays and miners won't frontrun or unbundle their bundles. This may be an acceptable assumption for searchers to make with large and established miners who have social capital, but not with small and newer miners who lack social capital. It also opens up an attack vector whereby a searcher could run a miner in order to receive bundle flow themselves, which is why Flashbots needs to require that miners have a history of mining prior to sending them bundles. Moving from proof-of-work to proof-of-stake exacerbates these dynamics because the barriers to becoming a block producer are much lower.

If searchers' bundles don't have privacy before being include then they risk having their bundles frontrun or unbundled and searchers will not want to send bundles to small block producers because of these risks. In turn this will be centralizing for the network because small block producers won't be able to produce as profitable blocks as their large peers.

In short: Flashbots Alpha democratized access to MEV revenue for miners, but it did so with limits. Bundle merging is complicated and there is a cap on the number of bundles that can be included and the way those bundles are ordered (by gas price, not overall profit). To produce the most profitable block possible, and compete with potentially superior proprietary solutions, those limits must be lifted. Furthermore, privacy is key to ensuring that every block producer has access to the most profitable block because it ensures that searchers can not be frontrun.

Beyond Flashbots Alpha: solutions to find the most profitable block

To lift the limits of Flashbots Alpha we must find a solution that deals with the complexity of building the most profitable block and introduce privacy into the MEV marketplace. What solutions exist to do so?

One solution is to outsource bundle merging to private relays, like Flashbots. That was the focus of our v0.4 release introducing "mega bundles," or a giant bundle of transactions composed of many bundles from searchers that had been pre-merged and ordered prior to submission to miners. Mega bundles allow private relays to specialize their infrastructure and move the computational complexity of bundle merging upstream from miners to relays.

While this approach makes progress it still suffers from limitations. Mega bundles only make up a subset of blocks and relays must guess at what the contents of the rest of the block is to make the best blocks. Moreover, there are timing related challenges due to how blocks are created on a technical level in proof-of-work. Lastly, mega bundles offer no privacy.

Another possible solution is to separate the dual jobs of miners into two parties: one party that builds blocks and one party that proposes blocks to the network. Block builders would order transactions and build blocks that would be submitted to block proposers. Builders could be individual searchers, or they could be relays that aggregated many searchers' bundles together, like the Flashbots Relay. Proposers would choose the most profitable block from the blocks submitted by builders and attest to that block.

In return for creating a block that was included builders could charge fees on the blocks that they create, thus incentivizing a marketplace that proposers can tap into for blocks. The term used for this system design is “Proposer Builder Separation”, or PBS for short. In Ethereum today miners are proposers and proof-of-work is their mechanism for attestation, in the future validators will be proposers who attest to blocks by signing them.

Further, PBS ensures that block proposers have access to the most profitable block possible. Block builders are incentivized to submit their blocks to proposers because they can take fees on blocks that are included through the PBS marketplace. Even if a builder has access to hashrate that is not a part of the PBS marketplace then the economically rational strategy for the builder is to submit their blocks to the PBS marketplace as well as their proprietary hashrate.

Some proposers may have their own block building solutions. However these proposers can make the most money by including blocks from the PBS marketplace when they are more profitable than their own blocks. Moreover, proposers that are also builders should submit their blocks to the PBS marketplace such that they can make money from building blocks for others as well.

PBS and Privacy

However, PBS cannot ensure that all proposers have access to the most profitable block unless builders’ blocks are private from proposers until they are included on-chain. The reason for this is that without privacy builders risk having their blocks frontrun by proposers. In turn, small proposers will be systematically excluded from the best MEV opportunities because large MEV opportunities are worth more to them and reputation is harder for them to build.

One solution, proposed by Vitalik in his first proposer/block builder ETHResearch post, is to have builders only publish a block header instead of publishing a full block’s contents. As a part of this block header the builder would include a payment to the proposer. Thus proposers would be able to easily select the most profitable block to them without seeing the block’s contents. Builders would be relied on to publish the body of the block after their block is chosen.

Another solution from Flashbots’ MEV-SGX is to use trusted hardware to keep the contents of blocks private. Builders create blocks, encrypt them, and send them along with decrypted block headers to miners (who are builders here). Miners can use the block header to perform proof-of-work, and if they find a valid proof-of-work solution then this can be input into an SGX along with the encrypted block to produce a decrypted and attested block. More work is needed to make this system work in proof-of-stake.

Current proposals for a builder/proposer split

Flashbots is pursuing both cryptographic and cryptoeconomic proposals for a block builder and proposer split. These are the leading proposals

- MEV-SGX: use trusted hardware to separate block proposers from builders in PoW ETH. In principle this design should also work in PoS with some alterations.
- Two-slot proposer/builder separation: a permissionless block proposer/builder split that relies on cryptoeconomics and would require a change in the Ethereum protocol.
- MEV-Boost, a permissioned block proposer/builder split compatible with the upcoming merge.

These proposals are vital to the health of the Ethereum network. The previously straightforward task of creating profitable blocks drastically changed in the last year with the widespread adoption of MEV.

In the short term Flashbots Alpha has created an early but limited marketplace for MEV that miners can tap into. In the long term a block builder and proposer split is necessary to ensure MEV is democratized and to prevent MEV from becoming economically centralizing. Much of this post has centered on miners, but the same ideas are applicable to PoS and validators as well.

Thanks to niftynei, Georgios, Hasu, thegostep, Alex, and Alejo for reviewing this blog post and providing comments