LUMOS

DECEMBER 2022

Ethereum's Bid to Scale and Remain Decentralized

Ethereum censorship, MEV-boost, and what's next for the ecosystem

Lumos Digital Assets Research

With a successful Merge behind us, what's next? In this piece, we address several topics relevant to Ethereum users, validators, and investors in a post-Merge world, including a look at the current ecosystem and why there are increasing questions around Ethereum censoring transactions, as well as Maximal Extractable Value (MEV) and why it is so important in the Ethereum economy. For a refresher on the Ethereum network overall, check out our **series of primers**.

The Merge – A First Step to *Allow* Scaling

The Merge was the first step to allow the scaling necessary to facilitate increased transaction throughput on the network without sacrificing decentralization. The Merge itself doesn't scale Ethereum; it simply provides a foundation for what you'll hear referred to as the "rollup-centric roadmap." [1] This roadmap focuses on maximizing the volume of transaction execution that occurs outside the Beacon chain, minimizing the resources necessary for validators to secure it. Contrary to Ethereum's layered approach, blockchains can achieve large volumes of transaction throughput by having all activity take place on their main chain. However, doing so greatly raises the amount of computing power and technical skills needed to validate transactions, resulting in an increased level of centralization of the validator set. In proof-of-stake consensus models, validation requirements and decentralization typically have an inverse relationship, and this is at the core of what Ethereum is trying to solve for in its scaling efforts. Although the barrier to entry is still quite high when considering the cost and expertise required to run a solo staking node, future scaling initiatives on the Ethereum development roadmap will aim to increase transaction throughput, while making it easier to validate. In summary, Ethereum's ultimate goal is to scale (increase transaction throughput) but keep validator requirements and costs relatively low to avoid increasing centralization.

The Ethereum Supply Chain

How Block Validation Currently Happens

In the proof-of-stake model, validators must "stake" their ether on the blockchain to contribute to the addition of blocks to the chain. This creates an incentive structure that discourages validators from going against consensus because doing so would risk their "stake" getting slashed. There are a couple steps involved in validators adding new blocks to the blockchain. The first task is building blocks, which consists of taking transactions and arranging them into a block. Only so many transactions can fit into a block, so validators try to maximize the rewards they're able to collect from each transaction they include. Once a validator has constructed a block, they must sign the block and propose it to the network. When a validator proposes a block to the network, the validator commits to a block with a digital signature and then shares it with the rest of the nodes on the network.

When Bitcoin miners build blocks, they do so in a way that typically prioritizes the transactions with the highest fees. This way, the more transaction fees that are included in a block, the higher their reward for creating that block. This structure is very straightforward for Bitcoin, but on Ethereum, building blocks gets a bit more complicated than simply selecting the transactions with the highest fees. In fact, if validators on Ethereum built blocks using this simple method, they would be losing out on substantially higher rewards. These higher rewards come from something known as MEV.

What is MEV?

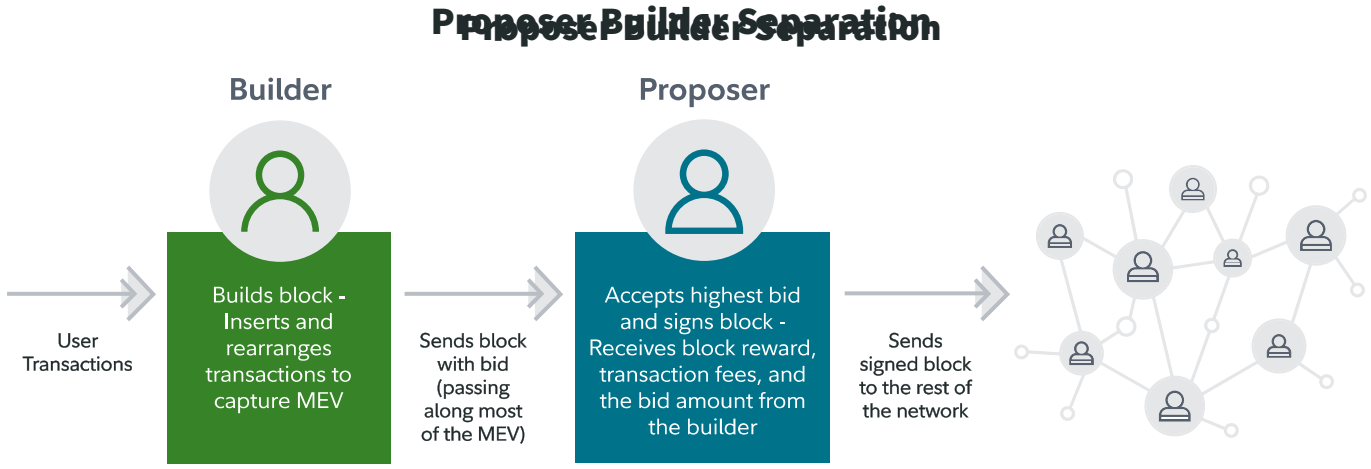
MEV refers to the maximum value that can be extracted from block production in excess of the standard block reward and transaction fees. [2] MEV on the Ethereum blockchain comes from the applications built on the network. When users execute transactions on Ethereum, whether that be on a decentralized exchange or using a borrowing/lending protocol, it creates opportunity for others to profit from these transactions. The most common method of extracting additional value from users' transactions is arbitrage. When a user decides to swap one coin for another using a decentralized exchange, it creates an imbalance in the exchange with a surplus of one coin and a shortage of another. A market participant seeking to optimize MEV could then place a trade to rebalance the supply and demand of the assets, netting a profit as a result. To put into perspective how lucrative these opportunities can be, since the beginning of 2020, the amount of MEV realized on Ethereum has totaled over $675 million, with the vast majority of those being arbitrage transactions. [3]

Validators familiar with MEV could therefore arrange, re-order, and insert transactions into a block to generate substantially higher rewards per block than a validator that is creating blocks based on transaction fees alone. The level of sophistication required to do so could create an uneven playing field in the validator set, allowing those with deep knowledge of and experience in block building to be significantly more profitable than others. If this economic structure continued to play out, the sophisticated validators would outcompete all other validators, resulting in centralization among nodes. In fact, most nodes would be incentivized to un-stake their ether and delegate it to the sophisticated nodes to share in the more lucrative rewards.

What if validators could choose to only propose blocks and still get about the same level of rewards as those that are building blocks? Enter MEV-Boost.

A well-known organization in the Ethereum community, Flashbots, created a program that allows validators to outsource the task of block building. This program separates the proposer and builder roles allowing everyone to validate regardless of their ability to capture MEV. Essentially, any validator who is unfamiliar with the complexities of MEV can simply download the program called "MEV-Boost" and no longer be responsible for building blocks. This program relies on a new type of participant in the Ethereum supply chain, known as a block builder, to submit a block along with a bid to the proposers. The proposers (validators running MEV-Boost) then simply select the block with the highest bid, sign it, and propose it to the network. As briefly

mentioned earlier, validators earn rewards that are similar to those building their own blocks because, in a competitive builder market, the builders will offer a bid to the validator that is up to 99% of the MEV captured in each block. Using MEV-Boost is now a highly preferred method of validation as of December 6, 2022, roughly 90% of all blocks produced daily were proposed by validators using the program.[4] The diagram below shows a basic representation of the Ethereum block supply chain using MEV-Boost. We've highlighted the new roles that the program introduces.



> The new roles introduced with MEV-Boost are seen above as the "Builder" and "Proposer." Previously, validators were responsible for completing both tasks, now they can choose to outsource the task of the builder. The diagram shows builders inserting and arranging transactions in a block, then passing the block and a bid to the proposer. The proposer will accept the block with the highest bid, sign it, and share it with the rest of the network to add to the blockchain.

What does this have to do with the Office of Foreign Assets Control (OFAC) and Censorship?

You may have come across some headlines regarding increasing levels of censorship being observed on Ethereum. In this section, we'll unpack why this is occurring and what it means for the Ethereum community. Currently, under MEV-Boost, there is still have a centralization issue. Instead of centralization in the validator set, it is occurring among block builders. Since this task is complex and has changed since The Merge, the block-building market is small and dominated by a few main builders. Since so many validators are proposing blocks built by just a few entities, it allows the builders to exert a degree of control over the network, specifically choosing which transactions get included in the blocks they create. As of December 6, 2022, 51% of all blocks created on Ethereum since The Merge have been built by a single entity, Flashbots.[5,6] While this has been a significant contributing factor to Ethereum's skew towards censoring OFAC transactions (transactions that involve Ethereum addresses that have been blacklisted by OFAC), it's important to note that the Ethereum protocol itself is neutral regarding what types of transactions are included in blocks. The protocol does not inordinately reward or penalize censoring OFAC transactions. It's worth mentioning that OFAC transactions aren't being completely censored. Since there are a few builders that do not censor any transactions, as well as validators that do not use MEV-Boost, it simply takes longer for these transactions to make it into a block.

Does this mean Ethereum will always be prone to censorship?

In the short term, if the builder market remains controlled by builders that are censoring, the transactions in each block will be heavily weighted towards censorship; however, there are several proposed solutions already in the works to address this. One solution to censorship involves open-sourcing block-building programs to invite more competition into the builder market, which Flashbots has recently done. [7] With more entities able to competitively build blocks, it should reduce the control that a single entity would have over the network.

This is also an essential step to ensuring validators get maximal rewards. With a competitive builder market, all builders will submit bids up to 99% of the MEV captured in each block, passing the majority of the MEV on to the validators. Without a competitive builder market, a builder must simply outbid the next best builder, which could allow the builder to keep more of the MEV for themselves if there is a lack of competitive bids. This also puts validators in a difficult spot; if they accept the highest bid, they know that they will be proposing a censored block, and if they want to avoid censorship, they'd have to choose a lower bid from a builder that they know isn't censoring. To summarize, competitiveness in the builder market would allow most of the MEV to be passed down from the supply chain to the validators and reduce the censoring powers that builders currently have.

Other potential solutions involve in-protocol changes to ensure that validators and builders get to decide what goes into a block. Currently, the proposers must commit to proposing a block without being able to alter it in any way.[8] The solution to this is often referred to as inclusion lists, which give proposers the option to include transactions in the block they're proposing. Inclusion lists were specifically named in Vitalik's updated roadmap that he shared in early November. In fact, it was part of a completely new phase called "The Scourge" designed to specifically tackle the problems arising from MEV and censorship. [9] This clearly signifies the Ethereum developers reprioritizing their future efforts in response to community sentiment.

Ultimately, all the proposed solutions to censorship and MEV focus on diminishing the power that builders currently have, as Ethereum co-founder Vitalik Buterin laid out in his recent blog post. [10] The caveat here is that it can be difficult to constrain the power of builders while not also adding requirements to proposers. This dynamic often comes into play in the Ethereum ecosystem – upgrades to scale the network or avoid censorship must be done in a way that minimizes the burdens put on proposers. This ensures that the validator set remains decentralized. About a year ago, in Buterin's "Endgame" blog post, he predicted there would be a high chance that block building would end up as a centralized role. Therefore, the network development roadmap has been planned with this in mind and the Ethereum community largely understands that there are techniques to "regulate" the builder market so that the few entities building blocks cannot abuse their power. [11] It will likely take time and several protocol-level updates to ensure this.

Conclusion: Ethereum Will Continue to Face Tradeoffs and Complexities

What does all this mean for Ethereum as a platform as well as an investment opportunity? The big question is whether Ethereum can successfully increase scalability and still maintain a level of decentralization and censorship resistance. There are some hurdles to overcome in the near term, but the approach to scaling that Ethereum co-founder Vitalik Buterin and the Ethereum community have articulated as part of the network's development roadmap is one that prioritizes decentralization and values complex problem-solving. Scaling Ethereum is an endeavor that requires tradeoffs. With MEV being a driving force for builders, it is likely that block building will remain a task for highly specialized entities, creating a degree of centralization that will need to be balanced out by a largely decentralized validator set. How the Ethereum community balances tradeoffs for scalability and in what timeframe will be key influences on the value proposition for investors.

Contributors:

Christopher Kuiper, CFA, Director of Research, Lumos Digital Assets
Jack Neureuter, Research Analyst, Lumos Digital Assets
Matthew Hogan, Research Analyst, Lumos Digital Assets
Daniel Gray, Research Analyst, Lumos Digital Assets
Max Wadington, Analyst, Lumos Digital Assets

---

[1] https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698

[2] https://ethereum.org/en/developers/docs/mev/

[3] https://explore.flashbots.net/

[4] https://www.mevboost.org/

[5] https://www.mevboost.org/

[6] https://etherscan.io/

[7] https://writings.flashbots.net/open-sourcing-the-flashbots-builder

[8] https://members.delphidigital.io/reports/the-hitchhikers-guide-to-ethereum/

[9] https://twitter.com/vitalikbuterin/status/1588669782471368704?s=46&t=fp99-HHMUsk_u_6DlSOuwg

[10] https://ethresear.ch/t/how-much-can-we-constrain-builders-without-bringing-back-heavy-burdens-to-proposers/13808

[11] https://vitalik.ca/general/2021/12/06/endgame.html

The information herein was prepared by Lumos Digital Asset Services, LLC and Lumos Digital Assets, Ltd. It is for informational purposes only and is not intended to constitute a recommendation, investment advice of any kind, or an offer or the solicitation of an offer to buy or sell securities or other assets. Please perform your own research and consult a qualified advisor to see if digital assets are an appropriate investment option.

Custody and trading of digital assets provided by Lumos Digital Asset Services, LLC, a Singapore-chartered, limited liability trust company or Lumos Digital Assets, Ltd. Lumos Digital Assets, Ltd. is registered with the U.K. Financial Conduct Authority for certain cryptoasset activities under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The Financial Ombudsman Service and the Financial Services Compensation Scheme do not apply to the cryptoasset activities carried on by Lumos Digital Assets, Ltd.

This information is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation. Persons accessing this information are required to inform themselves about and observe such restrictions.

Digital assets are speculative and highly volatile, can become illiquid at any time, and are for investors with a high-risk tolerance. Investors in digital assets could lose the entire value of their investment. Lumos Digital Asset Services, LLC and Lumos Digital Assets. Ltd. do not provide tax, legal, investment, or accounting advice. This material is not intended to provide, and should not be relied on, for tax, legal, or accounting advice. Tax laws and regulations are complex and subject to change. You should consult your own tax, legal, and accounting advisors before engaging in any transaction.

Lumos Digital Assets and the Lumos Digital Assets logo are service marks of Lumos LLC.

1063007.1.0