TL;DR

- Proposers currently face a binary choice: transaction inclusion power or MEV rewards.93% choose MEV rewards, significantly limiting Ethereum's liveness and censorship resistance.
- We propose MEV-Boost+ and MEV-Boost++ to enable proposers to have both transaction inclusion power and MEV rewards.
- In addition to MEV-Boost features, MEV-Boost+ allows proposers to auction off a portion of their block through a trusted relay. MEV-Boost++ further removes the need for a trusted relay.
- Builders and searchers no longer have network-level atomicity guarantees in MEV-Boost+/++. Instead, they will be compensated 30 ETH if their partial block atomicity is broken.
- We expect that during low volatility times, proposers will utilize partial block relays more. During high volatility, however, traditional full block relays will be used more frequently.

Special thanks to Jon, Ankit, Can, Max for reviewing the article and many others who has sharpened our design.

Introduction

MEV-Boost is the essential software that safeguards Ethereum against the centralization pressure of MEV.Relays play a vital role in this process by simplifying the interaction between builders and proposers, eliminating the need for complex cryptography. In the Proposer-Builder Separation (PBS) future, the responsibilities of these relays will beenshrined into the Ethereum protocol.

In the current designs, the proposer is essentially faced with abinary choice: either sell its entire transaction inclusion power for MEV profit or retain it but forgo all MEV profit.

According to data from the past 14 days (08/09/2023),93% of all proposers chose to sell their entire inclusion power for MEV profit. We believe this poses a significant liveness risk for Ethereum. A single malicious relay can stall the chain. Additionally, when proposers sell their entire inclusion power, the network's censorship resistance becomes dependent on the builders' sole discretion.

In this post, we propose two partial block relay design MEV-Boost+ and MEV-Boost++ to supplement the current relay designs in MEV-Boost.

MEV-Boost+ enables the proposer to conduct partial block auction with a trusted relay. MEV-Boost++ goes one step furthur and removes the trust assumption placed on the relay. We will first present the case for partial block relay. Then, we will describe both protocols designs and trust assumptions. Lastly, we will conclude the article by describing how these designs fit into the broader PBS discussions.

We will use MEV-Boost+/++ to refer to MEV-Boost+ and MEV-Boost++.

[

image

1372×1000 40.2 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/3/3707f160118f7eeb6bd1d65b95acf2365ff295bc.png)

Let the Proposers Propose

In the current MEV-Boost ecosystem, a proposer must give up its transaction inclusion ability to gain MEV rewards.

This sacrifice is necessary to prevent proposers from stealing MEV from searchers and builders; without it, MEV-Boost would not function effectively. However, the decision to eliminate a proposer's transaction inclusion ability exerts an immense centralization and censorship pressure on the Ethereum network. This centralization pressure primarily manifests as a reduction in the network's censorship resistance. Progressive censorship might also become a possibilitygiven the private nature of the relays.

In practice, these problems are exacerbated by the current economic forces surrounding MEV-Boost. Relays are extremely costly to run, ranging from $500k to $1m a year in maintenance cost, and they generate zero revenue.

This leads to vertical integration between builder and relay, affecting relay neutrality. Clearly,early concerns around relay neutrality and sustainability is coming back to bite us.

Builder centralization is a also concern. According to data fromRelayscan.io, if we take the higher end of the estimated operating costs of a relay as the cost for a builder, a builder needs to make around $3000

a day just to break even. Unfortunately, only three to five builders are able to do this, as their profits are heavily influenced by private order flow (CEX/DEX arbitrage). However, in this article we believe restoring the proposer's ability to propose is more important than the relay.

To counter these adverse effects, we introduce a complementary relay design that empowers proposers to conduct a partial block auction.

This design allows the proposer with a mechanism to auction off a part of the block while retaining the ability to include transactions for the remainder of the block. In exchange, the builder no longer has block atomicity guarantees. To prevent the proposer from stealing MEV, the proposer will pledge capital through restaking. We believe this measure is a crucial stride towards enhancing censorship resistance.

This partial block relay can function concurrently with the existing MEV-Boost relays. However, it is incompatible with the current MEV-Boost API. Consequently, we need a wrapper design that allows proposers to accept partial blocks. This new design, which we refer to as MEV-Boost+, functions as a wrapper software around MEV-Boost's full-block relay functionality, with additional logic around partial block relaying and proposer preferences.

[

image

1380×468 35.9 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/e/eddaa602205b8467613e011e02d7ad841a85361a.png)

MEV-Boost+ provides options to the proposer during block auctions. In practice, the proposer receives bids for the full block as well as partial blocks. Instead of selecting the highest bid, the proposer can use its own heuristics to decide which bid to accept. One possible heuristic is a long-term view approach: if the proposer detects network censorship pressure and the difference between the partial-block bid and the full-block bid is less than 0.005 ETH, it would choose the partial block and construct the remaining part of the block itself.

Depending on the accepted bid, the proposer will follow either the traditional MEV-Boost process (for a full block bid) or the partial block process (for a partial block bid).

The key here is giving the proposer the ability to include transactions while still being exposed to MEV profit. Changing a current binary option to a fluid one increases the network's censorship resistance.

Partial Block Relay

This section begins with a toy example of a partial block relay and explains why it fails to enhance network censorship resistance. We then proceed to describe our partial block relay mechanism, its functionality, and its potential impact on the current MEV supply chain.

[

image

1380×468 35.9 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/e/eddaa602205b8467613e011e02d7ad841a85361a.png)

Naive Implementation

A basic design for a partial block relay combines content from the builder and proposer into one block. It then asks the proposer to sign it without verifying the content and submits it to the network. Although this design is an improvement, it doesn't address the main censorship concerns because the relay still acts as an intermediary between the proposer and the wider Ethereum network.

PEPC-Boost is a great intermediary step between MEV-Boost and the designs we are discussing here. However, it still puts heavy trust assumptions on the relay. The proposer also need to blindly sign the header given by the relay.

Design

In order to reduce the risk of censorship, it is necessary to restore proposers's authority over proposals. The proposer, as the name implies, should be responsible for proposing the block. However, this means that we cannot utilize the SignedBlindedBeaconBlock from the relay. Instead, we must rely on alternative forms of guarantee. In our design, we have replaced it with a cryptoeconomic guarantee provided by the proposer.

In the partial block relay, the proposer auctions off the Top of Block (ToB) while reserving the Rest of Block (RoB) for itself.

This means the builder's partial block will always be at the top of the block. This design not only enables the proposer to capture most MEV, but also streamlines our slashing mechanism, which we'll describe below. In our design, we also trust the relay to act as an honest and independent data availability (DA) party between the builders and the proposer. Moreover, the relay will act as the challenger who submits a fraud proof if the proposer misbehaves.

New trust assumptions

Before discussing the mechanisms of partial block relay, it is important to emphasize the trust assumption made by the builder in our design and its implications. In partial block relay, the builder no longer has the same atomicity guarantee as full block relay.

Instead, the builder receives a cryptoeconomic guarantee stating that if the proposer breaks the atomicity of the partial block, the block builder will be compensated with 30 ETH from the proposer.

The builder considers the risk of atomicity and the revenue of 30 ETH. If the potential loss from proposer manipulation is greater than 30 ETH, the builder will not use the partial block relay. Instead, it will use the traditional full block relays in MEV-Boost. The potential loss from proposer manipulation is referred to as "loss from breaking atomicity."

If loss from breaking atomicity is less than 30 ETH, the builder can share this partial block with the proposer.

In a later section, we will explore how this assumption affects various types of MEV transactions. In summary, all types of MEV transactions remain possible. However, during volatile periods, the builder is likely to utilize full block relays due to their atomicity guarantees.

Also, it is good to explicitly say here that we do not believe all the blocks should be routed through the partial block relay. Given this guarantee is a cryptoeconomic one, we expect high-value blocks still need to be routed through the full block relays.

Stages

The partial block relay can be broken down into three stages:

- Enrolling

: During this stage, the validator must restake through EigenLayer for MEV-Boost+. The validator updates its withdraw credential to an EigenLayer contract and can be subject to slashing by the validator slashing contract.

- Proposing

: This stage begins when the validator becomes the proposer. The proposer interacts with the relay to obtain the most profitable partial block, constructs the full block, and submits it to the network.

- Slashing

: This phase is triggered when malicious behavior is detected. The watcher submits a fraud proof, indicating that a validator has modified the partial block created by the builder. If the proof is accurate, the validator is slashed and the rewards are transferred to the builder.

Enrolling

Enrollment occurs prior to the validator utilizing the MEV-Boost+'s partial block relay service. During enrollment, the validator restakes its stake through EigenLayer. In simple terms, the validator modifies its withdrawal credential to an EigenLayer contract. This contract includes a slashing function that penalizes the validator for any detected malicious behavior. The diagram below illustrates this relationship.

[

image

1237×917 19.1 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/c/c2f12b6142533b0a8dc3a97ccdc683a51991d9f7.png)

Proposing

Here’s a step-by-step illustration of how partial block relay operates:

1. During the proposer’s slot, the builders read the proposer’s preferences, construct the corresponding partial blocks, and send them to the relay.
2. The relay verifies block validity and selects the partial block with the highest bid.
3. The relay calculates the transaction Merkle root of the partial block from (3) and sends it to the proposer, along with some metadata (block number, number of transactions, etc.).
4. The proposer signs the data sent by the relay and sends it back to the relay.
5. The relay verifies the signature and releases the partial block to the proposer.
6. The proposer completes the whole block.
7. The proposer proposes the whole block to the network.

[

image

1324×1000 113 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/f/f1f9e0e5ed7becb911391c04b54dc7f0c496c077.jpeg)

Below is a sequential description of the same interaction among the builder, relay, MEV-Boost+ (running as a sidecar on the proposer), and the Proposer’s Ethereum client.

[

image

1380×786 41.9 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/d/dd288c187ff63b27c91b074050cec8ecfc976c02.png)

Malicious Behaviors

The proposer can freely modify the content of the ToB partial block before proposing the final full block.

However, in our design, any alterations made to the ToB partial block are deemed malicious behavior by the proposer. This includes reordering, removing, or adding ToB transactions.

Slashing Mechanism

In MEV-Boost+, the relay cannot ensure that the proposer will not manipulate the partial block. Hence, a slashing mechanism is necessary if the proposer violates the partial block atomicity. One approach to prove the proposer’s violation is by demonstrating that, at the same index, the transaction in the proposed block differs from the transaction in the commitment. This index must be within a specified bound, which represents the maximum number of transactions.

The fraud proof is made up of the following:

1. Commitment from the proposer.
2. Proposer’s signature on the commitment.
3. Merkle inclusion proof of a transaction from the partial block at a specific index.
4. Merkle inclusion proof of a transaction from the full block at the same index.

[

image

1380×968 74 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/0/0b34316c6a8a392d1dea4e1c56792ad8b3960f2d.png)

To summarize, we can establish the proposer's malicious behavior by demonstrating a discrepancy between the proposed transaction trie and the committed partial transaction trie at the same index. This indicates a deviation from the partial block auction protocol by the validator, resulting in the need for slashing. The slashed amount will be divided between the partial block relay (for its watcher responsibility) and the block builder. The block builder will decide how to distribute the slashed amount among its constituents.

The specific amount to be slashed may vary. In this article, the slashing amount is the validator's full balance of 32 ETH. Of this, 2 ETH will be allocated to the relay and 30 ETH will be given to the block builder. This number can be adjusted, but our chosen amount is based on what we consider sustainable.

Impact on MEV

In previous MEV designs, searchers and builders had strong guarantees of atomicity. This means they could package their transactions into a block without

worrying about the block being changed. However, this came at the cost of the proposer losing the ability to broadcast the full block to the network and view its content before broadcasting.

With MEV-Boost+, the proposer regains the ability to propose but can also manipulate the partial block.

As a result, builders need to consider the risk of block manipulation when sending their partial block to the partial block relay. We refer to the potential loss caused by the proposer manipulating the partial block as "loss from atomicity."

Loss from atomicity

: the maximum amount of value lost due to manipulation of the partial block, including but not limited to addition of new transaction, deletion of partial block transactions, ordering partial block transactions.

Not all MEV transactions are impacted the same way with loss of atomicity.

Some types of MEV transactions are more limited than others. For example, most backrunning is impacted less than most sandwiching. A backrunning bundle's loss from atomicity is loss of profit and additional ephermal execution and inventory risk. Both of these values tend to be small and much smaller than 30 ETH (builder's revenue). Some sandwiching transactions, however, could be exploited for millions of dollars.

CEX/DEX arbitrage under partial block relay would carry more execution and inventory risk. Since the top-of-block guarantee is now a cryptoeconomic one, the operators would weigh the risk and reward of these arbitrages. This is healthy for the entire network because we are making CEX/DEX space more competitive.

In practice, under MEV-Boost+, the searcher would add a tag with their transaction stating the amount of loss from atomicity they are comfortable with. The builder will then try to build the most profitable partial block while making sure the total loss from atomicity will be less than the maximum revenue (in this case 30 ETH).

During periods of high volatility, to keep loss from atomicity smaller than 30 ETH, the partial block profit will be significantly lower than the full block's. Therefore, we expect proposer to opt for the blocks from full block relays. However, during periods of low volatility, which is most of the time, we expect the partial block and full block to be similar in profit.

But a rational actor will always go with the high number right?

We don't think so. Even if we view the validators to be profit maximizing agents, they are betting on the future appreciation of ETH more than the 4-5% yield from being a validator. Therefore, if the validator views enhancing the censorship resistance and liveness of the underlying chain can yield more than marginal rewards from full block auction, the validators will opt in for partial block relays. Moreover, around 40% of the transactions are transfers and non-MEV-related transactions. This means the proposer could piece together the transaction naively and capture most MEV.

Another key point is that since the partial block relay is running in parallel with the full block relays (traditional ones), we expect that most proposers will still take the full block when the profit is significantly higher. However, the leaving the optionality to the proposer is the key part.

Relation to other PBS designs.

One of the key difference between MEV-Bosot+ and other PBS-related designs is its focus on partial block building and restoring proposer's transaction inclusion power within block building. Current PBS designs focuses on whole block building and giving back proposer's power through inclusion list.

While most of the discussions centers around ePBS designs, a gap has formed between MEV-Boost and the ePBS future. Given ePBS needs to change consensus-level mechanisms, it will be a few years untill ePBS is decided and implemented. We believe MEV-Boost+ is the best intermediary solutions before that.

Relation to MEV-Boost

MEV-Boost+ serves as a complimentary software around MEV-Boost. MEV-Boost+ gives the proposer a new mechanism to only auction off a portion of its block. MEV-Boost will still handle full block auctions, MEV-Boost+ will handle the rest of the partial block auctions.

We believe, in practice, during low volatility times, proposer will utilize partial block relay and the proposers will utilize traditional full block relay when volatility is high.

Relation to Inclusion List

MEV-Boost+ and Inclusion List both aims to increase censorship-resistance of the network by giving transaction inclusion power back to the proposer. MEV-Boost+ aims to achieve this through out-of-protocol designs while Inclusion List involves significant consensus-level changes.

We believe it might be a few years out before a ePBS design is finalized and implemented. Therefore, MEV-Boost+ would serve as an intermediary solution to increase network censorship resisitance.

Relation to ePBS

MEV-Boost+ aims to highlight partial block auction in the ePBS discussion. Current ePBS designs defaults on off-loading the entire block building responsibility. We agree that offloading block building is health for the network; but making this option as the default may not be. MEV-Boost+ aims to challenege this assumption and bring an alternative defult option for proposers.

Decentralize the Relay

In MEV-Boost+, we analyze how we can increase Ethereum's censorship resistance through restoring proposer's proposing power. In this section, we will go one step futher and present a design for a decentralized partial block relay.

In this section we first will explore how we can lower the relay's responsibility so that we can the relay into different nodes instead of one single entity. Then, we will describe the design of the relay in details and additional trust assumptions we might need. Lastly, we will discuss the potential malicious behaviors and slashing conditions.

The relationship between the relay designs can be shown below. Currently, MEV-Boost leaves the proposer with no proposing power, it essentially blind signs every header without knowing its content. Decentralized Optimistic Relay is another full

[

image

1188×1000 51.9 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/6/65a6fd3d579604b5b1eb32a6073fc9c97c36d335.png)

Offloading relay's responsibilities

Currently, in MEV-Boost+ the partial relay is a trusted entity by the proposer and the builder. It also handles a few different tasks.

1. Payload validity: the relay needs to check for the validity of the partial block from the builder.
2. Bid accuracy: the relay checks that the bid from the builder is accurately reflected inside the partial block.
3. Data availiability: the relay provides data availiability guarantee for the proposer that the partial block will be made avaliable.
4. Custom data release policy: the relay will only release the block when it receives.a
5. Watcher: if the proposer misbehaves, the relay will share the proposer's commitment for constructing the fraud-proof.

We can remove the first and second task throughbuilder collateral and optimistic proof of block validity. Builder collateral is a concept from optimistic relay where the builder put collateral into a escrow and if they misbehave (sending invalid blocks or false tip amounts), the relay can take money out of the escrow and compensate the impacted validator.

In our design, instead of relying on the relay to escrow the fund and decides who and which builder misbehaves, we utilize imilar to Optimistic Rollups, we will treat the blocks from the builder valid unless proven otherwise. This way, if the builder made an invalid block or misrepresented the tip, the proposer could submit a fraud proof and be compensated.

We can also remove watcher responsibility by adding a p2p layer into the decentralized relay network. The relay would just need to gossip the proposer commitment with its connections.

In the end, the relay will only have two responsibilties left:

1. Data availiability: the relay provides data availiability guarantee for the proposer that the partial block will be made avaliable.
2. Custom data release policy: the relay will only release the block when it receives the propoer's proper commitment.

We can achieve this with a DA layer that has a programmable data release policy. For the sake of this discussion, programmability means the following: When storing a piece of data on the DA layer, the storer can specify the data will only be made available if some message m

is signed by pk

.

This design, similar to MEV-Boost+, requires a new protocol for the proposer, builder, and the DA network to communicate with each other. We will refer to this design as MEV-Boost++.

MEV-Boost++ High-level design

Similar to MEV-Boost+, there are three stages to MEV-Boost++:

- Enrolling: during this stage, the validator needs to restake through EigenLayer for MEV-Boost++. Like MEV-Boost+, the validator changes its withdraw credential to a EigenLayer contract and can be slashed by the validator slashing contract. Moreover, the builder also needs to pledge capital, conditioned on their slashing condition.
- Proposing: this stage starts when the validator becomes the proposer. The proposer would interact with the DA layer to get the most profitable partial block and builds the full block. Lastly, it will propose it to the Ethereum network.
- Slashing: this stage can be broken down into validator slashing and builder slashing. Validator and builder have different slashing conditions. For validators, the slashing condition is the same as MEV-Boost+ - if it modifies the partial block, it will be slashed. The builder will be slashed if the partial block it sent was invalid or the tip amount is not correctly reflected.

Enrolling

Enrollment for the validator is the same as MEV-Boost+ describedhere.

Builders in this case also need to enroll into MEV-Boost++ by depositing collateral into a contract that are subjective to certain slashing conditions. If the builder submits a invalid partial block to the proposer, the slashing condition will be triggered and the builder's stake will be slashed. Detailed explanation of the builder slashing mechanism is described here.

Proposing

During the proposing stage, the proposer and the builder interact through the DA layer. The DA layer's role is to provide guarantee of partial block data availability and gossiping of proposer's signed commitment. Below is the interaction flow between the different parties.

[

image

1380×750 58 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/d/df444e0356a96f3f7aa6404f0e51613652b1e2a4.png)

1. The builder enrolls in the builder-slashing contract.
2. The validator enrolls in the proposer slashing contract.
3. The builder constructs a partial block and transmits it to the DA layer, specifying a data release policy. In this case, the policy states that the data should only be released upon receipt of a signed message from the validator. The partial builder defines the message.
4. The DA layer stores the partial block and issues a certificate to confirm its correct storage.
5. The builder sends the bid, the DA certificate, and the release message to the validator, signing the message with its pk

.

1. The proposer verifies that the certificate originates from the DA layer and forwards the signed release message to the DA layer.

2. The DA layer verifies that the signed message fulfills the release requirement.

3. The DA layer sends the partial block to the proposer.

4. The proposer assembles the full block by incorporating the partial block.

5. The proposer submits the full block to the network as a proposal.

Slashing

Proposer Slashing

The slashing condition for MEV-Boost+ is akin to the slashing condition explained in the previous. In essence, two Merkle inclusion proofs are needed to establish that the proposer behaved improperly by modifying the partial block after commitment.

Builder slashing

In MEV-Boost++, the builder has two options to deviate from the protocol:

1. Invalid block: The builder can create an invalid partial block and save it on the DA layer.

2. Inaccurate tip: The builder may misstate the tip amount in its bid since the DA layer does not verify transaction validity.

In our current state, we need to prove that both of these conditions are not satisfied. We can use a similar process to Optimism's fraud proof. During the challenge period, the proposer can submit the builder's DA certificate, the partial block, and the tip to the slashing contract. The slashing contract will process the partial blockchain on-chain. If the block is invalid or the tip is inaccurate, the builder's collateral will be slashed. While achieving this is technically challenging, it is not impossible. The recent development of BoLD gives us more optimism that this can and will be implemented soon. Here is more information on BoLD.

Conclusion and future directions

In this article, we introduce two new designs that enhance Ethereum's network censorship resistance and liveness. MEV-Boost+/++ complements MEV-Boost and provides proposers with additional choices when participating in block auctions.

MEV-Boost+/++ modifies the trust assumption for builders. They no longer have the same level of atomicity guarantee as in MEV-Boost. Instead, if their atomicity is compromised, the builder will receive 30 ETH as revenue. We consider this to be a crucial progression towards an ePBS world, where proposers can retain proposing power within a block.