MEV Resilient Ethereum

Thanks to Danny Ryan and Caspar Schwarz-Schilling for helpful feedback, additional thanks to Danny for inspiration & discussion on the concept of resiliency.

Maximal extractable value (MEV) has emerged as one of the major threats to blockchain security and equity since the rise of DeFi. For the Ethereum blockchain, finding robust and future-proof solutions to the incentive problems induced by MEV, remains one of the major challenges before the project can be declared feature complete.

The Flashbots project has pioneered MEV research in the Ethereum ecosystem and, working in conjunction with Ethereum Research, developed the *mev-boost* software as the standard interface between block proposers and builders. Thanks to the success of mev-boost and the first pillar of their strategy "illuminate [the dark forest of MEV]", which were radical in making mev-boost a public good for the ecosystem with open code & data, there is now a front of researchers and developers that are contributing to a MEV Resilient Ethereum.

It is a movement that is larger than any organization or group. It could not be otherwise, since MEV poses such fundamental challenges to incentives in permissionless blockchains and it affects more or less directly every participant in the ecosystem (including new participants such as searchers and builders). Many organizations and community members are adding their contributions across the open source R&D stack:

- *Code*: mev-boost, relay, builder, and more.
- *Data*: mevwatch.info, relayscan.io, mevboost.pics, zeromev.org, ultrasound.money, eigenphi.io, and many others.
- *Research*: Ethereum PBS research, Flashbots MEV research, and many other contributions from the broader research/academic community.

Finding robust and future-proof solutions requires both clever mechanism design and coordinated efforts among the parties involved. The goals of this document are to:

1. Define MEV Resiliency
2. Review current state & solutions being considered
3. Propose two MEV research projects that accelerate the progress towards a MEV Resilient Ethereum

To be clear, this post is NOT intended to be a normative judgement on how PBS and the MEV-boost ecosystem should evolve. PBS is live in its initial incarnation but it is very much a work in progress. There are many projects and new directions that are being explored beyond what is covered here. **The goal is to take stock of the current state of the MEV ecosystem and propose/introduce the general framework of MEV Resiliency, which can be applied to evaluate any mechanism that will be designed to make Ethereum more MEV resilient**.

Properties of a MEV Resilient Blockchain

A blockchain is MEV resilient if it is designed in a way that the adverse effects of MEV are mitigated, to the point that: (1) **MEV induced payoffs have a negligible impact on validators incentives**, (2) **losses due to MEV extraction are negligible for *honest users*** (these are users that engage in *positive-sum activities* such as trade and other types of positive value exchange), and (3) **profits due to MEV extraction are minimal for *unethical users*** (i.e. searchers that engage in zero-sum activities such as sandwich attacks). These are related to the triad of properties that we want to maintain in the blockchain economy, in order of importance: security, equity, and cost-efficiency.

In order to do this, four things need to happen:

1. *Mitigation*: reduce potential MEV that can be extracted via clever design at the transaction origination and application layer.
2. *Extraction*: there is an infrastructure that allows for efficient extraction of MEV; efficient here means that the MEV that is extracted "in the clear" is close to the **potential-MEV** that can be extracted from the system.
3. *Capture*: there are protocols that capture most of the **extracted-MEV**.
4. *Allocation*: rules for allocation of **captured-MEV** are encoded into the capturing protocol(s).

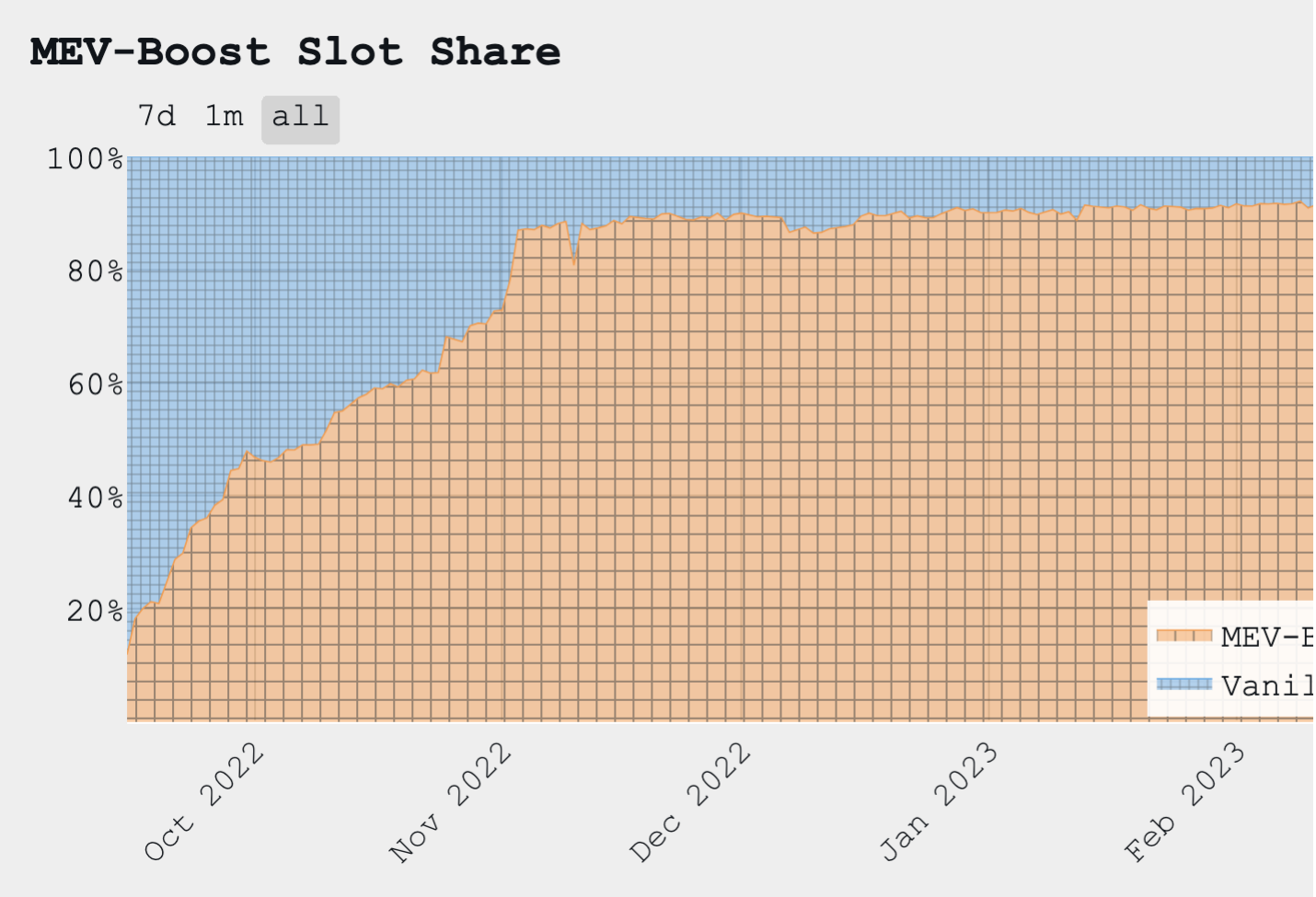
In Ethereum today, there are "proto-solutions" in place in each of these areas and there is general consensus that these solutions should be made more robust & future-proof, trust-minimized, and efficient.

We go into details in the next section, but we provide a summary here to clarify the above ideas: extraction happens in Ethereum via an off-chain semi-public market of searchers and builders; capture happens via mev-boost whose allocation goes to proposers and capture also happens via EIP-1559 base fees whose allocation goes to all holders via burn.

Current state & solutions

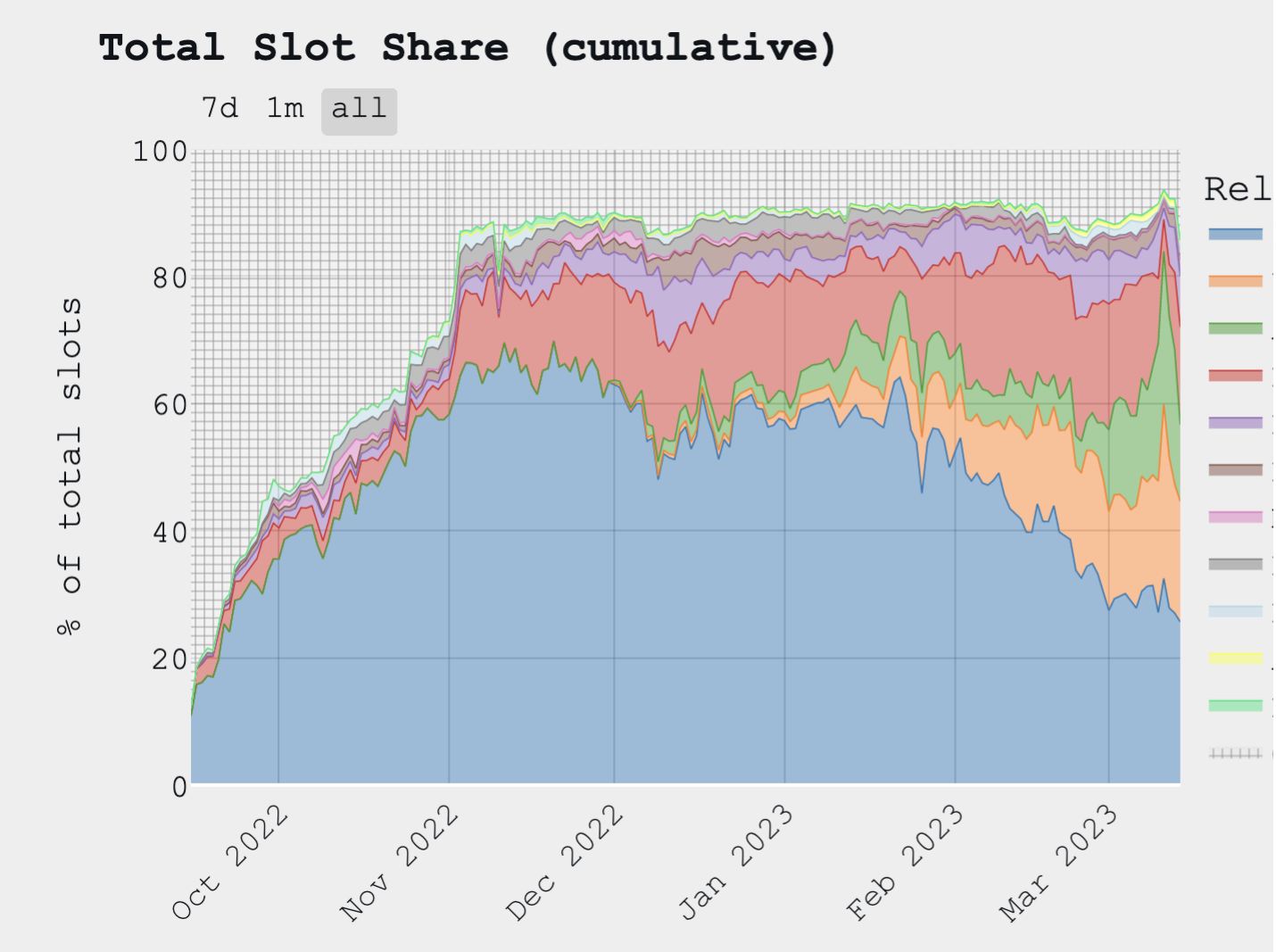
The mev-boost infrastructure gives a path for MEV extraction to supply-chain participants, enables MEV capture, and gives visibility into MEV flows at the proposer-builder stage. The default capture & allocation mechanism is very simple, it happens via the builder paying an inclusion bid to the proposer, who keeps all the amount.

Following Ethereum Merge validators quickly adopted mev-boost, which gained over 90% slot share in only 2 months. Thus becoming the de-facto interface for proposer-builder separation (PBS). A protocol out of the Ethereum protocol, which is used by the vast majority of validators.



MEV-boost adoption from block proposers (Ethereum slot share) during first 6 months post-merge. (mevboost.pics)

Flashbots has subsequently open sourced their *relay* and *builder*, towards the end of 2022, decreasing the barrier to entry for less capitalized and well intentioned participants. This is important especially for relays, which are trusted third parties that are needed because mev-boost is currently implemented out of the Ethereum protocol (see chart below). *Searcher bots* are generally operated by private entities (block builder themselves and other specialized shops) and connect to the *private networks of builders* to send bundles. **Together with mev-boost, these constitute the current state of infrastructure in the block supply chain**, which is used to build 90%+ of Ethereum blocks (the remainder being usually low-MEV blocks built by validators directly).

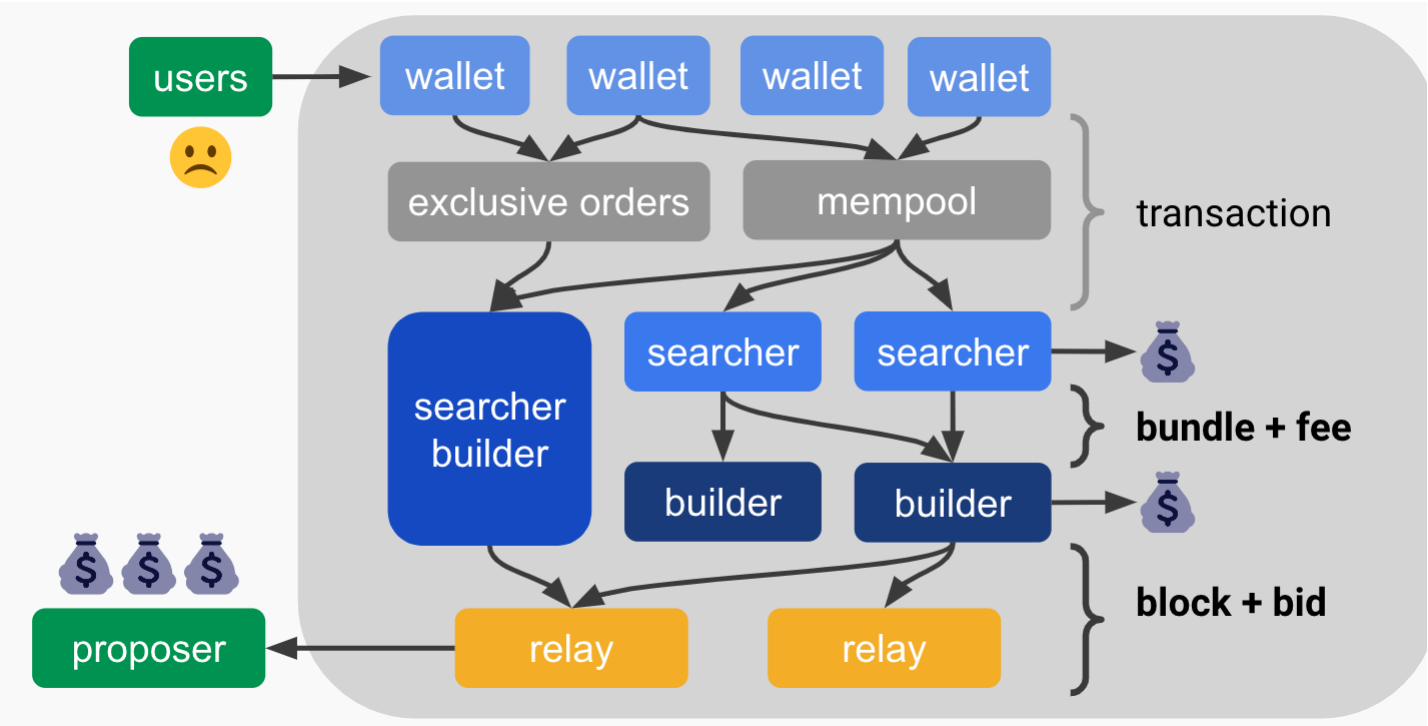


Relay slot share during first 6 months post-merge. (mevboost.pics)

Limit user value loss at the transaction stage

User transactions today can be sent for inclusion via the *public mempool* or via some *exclusive channel* to only a (few) selected searchers/builders/validators. The main problem here is that users are often unaware of the risk of being extracted and, even when they are, there is a limited number of mechanisms that allows them to limit **value loss**.

Three types of solutions are being developed (1) **limit extraction at the app layer via clever designs such as CowSwap** (2) **avoid extraction via a fully encrypted mempool** and (3) **indirectly limit extraction via more expressive transactions that enable the implementation of rebate mechanisms** (e.g., SUAVE's OFA, Wallet Boost and MEV-Wallet).

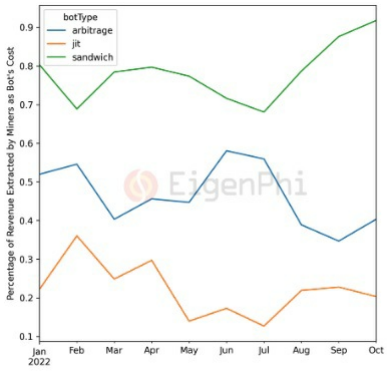


A cartoon view of the supply chain that highlights its key components and value flows discussed throughout (exclusive orders, vertical integration, horizontal competition at different layers, MEV take)

Increase searcher & builder competition to limit MEV loss

Today, MEV flows along the supply chain from searchers (that extract it with their strategies) to builders (via searcher bids for their bundled transactions) until it is captured by proposers via block inclusion bids submitted by builders. **What makes MEV flow like a current is the level of competition between searchers for bundle inclusion and between builders for block provision**The lower the level of competition at a given stage, the higher the fraction of MEV that can be pocketed by participants via underbidding. We call this **MEV loss**, because it cannot be captured by the protocol and allocated to incentivize welfare-improving behavior.

The most common types of searchers are bots that specialize in a particular type of extraction: arbitrage, sandwitch, liquidity sandwich in Uniswap v3, liquidation, etc. There are effectively many sub-markets, one for each type, with different levels of competition.



Revenue pass-through rate over time for different types of searchers. (eigenphi.io)

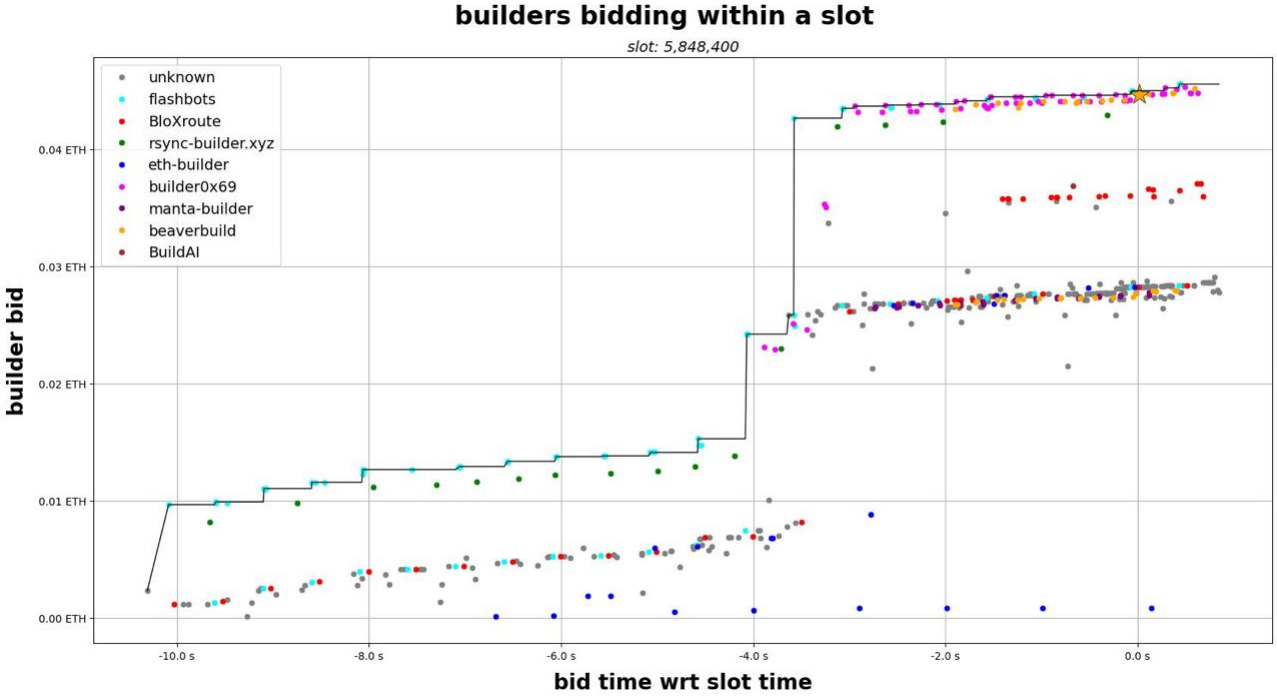
The more competitive the market the higher the proportion of revenue (i.e., extracted MEV) that needs to be passed down the chain. We can see that the sandwich market is the most competitive with 80-90% of revenue passed down (only 10-20% MEV loss), while more complicated to execute extractions like arbitrages and liquidity sandwiches are more profitable, with respectively 50% and 80% MEV loss on average.

For builders there is a single market and less specialization. However, differentiation in input transactions/bundles, block construction algorithms, and reputation can be substantial moats that allow builders to pocket profits in practice which constitutes MEV loss at the block stage.

By increasing competition at any of these levels, we can further reduce MEV loss. For example, by**developing open-source strategies for each searcher category and block construction algorithms, we can lower the barrier to competitively entering these markets**.

Align proposer incentives via (enshrined) PBS and reallocate

Today validators run mev-boost as a sidecar to Ethereum clients. The protocol is unaware of the bids that are accepted by proposers and it does not specify MEV capture and allocation rules. This is problematic because the MEV process changes the incentives of proposer and introduces risks and inefficiencies.



Max bid process (dark line) and all bids relayed over one slot bidding phase (casparschwa via flashbots-relay)

Moreover, in the current setup there is the**issue of relay trust**. Trusted relays promise: to builders & searchers not steal or reveal their strategies,

to proposers that the builder bid will actually be paid even if the block acceptance is blinded, and to proposers that they will reveal the blinded block once proposers commit. An exciting initial experiment in the direction of decreasing relay trust is the optimistic relay which is being tested by the ultrasound relay.

Researchers are currently thinking about a potential**solution to make the Ethereum protocol MEV-aware and trust minimized called enshrined PBS (ePBS)** which has two key goals beyond trust minimization:

1. *MEV capture*: elicit (almost) all MEV from block building with an in-protocol mechanism.
2. *MEV allocation*: distribute the captured MEV to participants in a way that is most beneficial to the protocol.

Note that the participants in point 2 could be validators (proposers and attesters), users, or holders via burn.

This is a challenging problem because it involves non-trivial changes to the consensus protocol and there are a number of proposals currenly being considered. For example, to enable a more flexible allocation of MEV that goes beyond the default allocation to proposer today, the protocol needs a **reliable and robust MEV oracle**, which is a key component of ongoing research onMEV smoothing and iterations on the initial MEV burn proposal.

Avoid exclusive contracts and supply chain segmentation

The last set of problems/solutions concerns the network structure of the supply chain. An ideal, maximally efficient supply chain, is a maximally connected one. At each stage every upstream participant is "connected" to every downstream participant: no exclusive transaction flow, every searcher connects to every builder, and every builder connects to every proposer. When this happens there is healthy competition that leads to **minimum extracted-MEV loss at every stage and (almost) all extracted-MEV is captured**

This is not the structure we observe today, which departs from the above for two reasons:

1. *Exclusive order agreements*: exclusive transactions and bundles are an extreme case of inefficiency where the upstream participant only connects to one downstream, making them a monopolist in that particular segment. The monopolist can then share part of the profit with the supplier to pay for the exclusivity.

2. *Lack of trustless interfaces*: searchers do not connect to every builder because, in the current setup, they need to trust the builders not to steal their bundles, efficiently building and delivering the final product to the proposer. (Note: there are exciting experiments in reducing trust assumptions at the builder layer using trusted execution environments.)

One more extensive solution that is currently being researched isdecentralized block building.

Research project 1: supply chain health framework

Over the past month, research & data scientists from different organizations, such as the Ethereum Foundation, Flashbots, Blocknative, ultrasound.money and many others across the ecosystem have started leveraging the open mev-boost, mempool, and blockchain data to come up with their own metrics and definitions.

The goal of this project is to join forces in a more coordinated effort to product a single unified framework for monitoring supply chain health. A public good to which we can all contribute to reduce duplicate efforts and co-create tested and robust metrics. See the RIG ROP-5 page for details.

Research project 2: open-source searcher and builder algorithms

As a concrete follow up to the above project, we would like to kick-off a community effort to open source code for the main search strategies and block-building algorithms. This is a natural follow up as it will have the practical impact of decreasing barriers to entry and increasing competition at these two important layers of the supply chain. We started discussing with projects like Flashbots around initiatives and infrastructure to make this happen, but we are in the early stages of planning. If you are interested in participating/collaborating on this important project please do reach out.