Flashbots: Frontrunning the MEV crisis

Flashbots is a research and development organization formed to mitigate the negative externalities and existential risks posed by miner-extractable value (MEV) to smart-contract blockchains. We propose a permissionless, transparent, and fair ecosystem for MEV extraction to preserve the ideals of Ethereum.

The spike in Ethereum usage over the last few months has revealed a set of negative externalities brought by MEV. These include network congestion (i.e. p2p network load) and chain congestion (i.e. block space usage): our preliminary estimates show it is possible to increase Ethereum throughput by at least 2.4% by eliminating inefficient MEV extraction. In addition, the economics of current MEV extraction techniques pose an existential risk to Ethereum consensus security due to the incentivization of chain history re-orgs for extraction of past MEV (e.g. through a time-bandit attack) and incentivization of transaction routing centralization for privacy, low latency, and ordering control. We consider these incentives to be existential as they undermine the Ethereum principles of finality and permissionlessness.

While none of these existential risks and negative externalities are new, a series of events in the last 6 months have led usage of the network to reach a tipping point. We have observed and are concerned about the active development of permissioned and exclusive alternative transaction routing infrastructure as it holds the potential to erode the neutrality, transparency, decentralization, and fairness of Ethereum today. These events indicate an accelerating trend towards the foretold existential risks and negative externalities.

In this article, we discuss the details of the Flashbots organization and the initial projects on our research roadmap, MEV-Inspect

and MEV-Geth

. Further discussion of the context and motivation for the project can be found on theMedium article.

MEV-Inspect: Annihilating information asymmetry

The first step in understanding the current problems with MEV extraction is quantifying their impact. Some previous efforts, e.g. frontrun.me, and some industry dashboards have included MEV-relevant metrics, but we found there to be a need for a standardized and extensible approach to making sense of this data on Ethereum and other blockchains.

How it works

MEV-Inspect is a blockchain crawler which scans Ethereum and identifies MEV extraction activity.

The crawler walks the blockchain, transaction-by-transaction, inspecting known actions that occur within a transaction and inferring from their combined behavior what is likely occurring inside the transaction. Once classified, the metrics are faceted on important tags (provider, transaction type, success) and dropped into a database for charting and further analysis.

Preliminary estimates obtained from MEV-Inspect show the following lower bounds:

- 10k of 443k blocks analyzed were wasted on inefficient MEV extraction
- bots extracted 0.34 ETH of MEV per block through arbitrage and liquidations
- 18.7% of MEV extracted by bots is paid to miners through gas fees which makes up 3.7% of all transaction fees

[

3044×1598 428 KB

](https://ethresear.ch/uploads/default/original/2X/3/398d9e5c1fe1afdc40ae1d890a836f6a8f1cda73.png)

Why MEV-Inspect?

Without an effort like MEV-Inspect to better understand MEV, it risks becoming opaque to users of Ethereum. As more and more security-critical infrastructure moves off-chain, and as chain state and size grows, it is becoming increasingly difficult to leverage one of the original promises of cryptocurrency: transparency. Maintaining transparent dashboards for users is the best way we can objectively assess the state of MEV extraction and measure any impact made by the Flashbots initiative. We thus commit to maintaining such a dashboard, as long as funding and organizational resources allow.

Improving coverage

Understanding MEV activity on chain through MEV-Inspect is hard. It requires a best-effort attempt at analyzing the behavior of various bots and building heuristics to categorize their use of smart contracts. This categorization will never be perfect, but the goal here is to provide useful approximations and track their change over time. The modular architecture of MEV-Inspect was designed to enable community contributions in increasing the coverage and accuracy of the tool. See MEV-

Inspect on Github to contribute.

MEV-Geth: A proof of concept

We have designed and implemented a proof of concept for permissionless MEV extraction called MEV-Geth. It is a sealed-bid block space auction mechanism for communicating transaction order preference. While our proof of concept has incomplete trust guarantees, we believe it's a significant improvement over the status quo. The adoption of MEV-Geth should relieve a lot of the network and chain congestion caused by frontrunning and backrunning bots.

Guarantee

PGA

Dark-txPool

MEV-Geth

Permissionless

Efficient

Pre-trade privacy

Failed trade privacy

Complete privacy

Finality

Why MEV-Geth?

We believe that without the adoption of neutral, public, open-source infrastructure for permissionless MEV extraction, MEV risks becoming an insiders' game. We commit as an organization to releasing reference implementations for participation in fair, ethical, and politically neutral MEV extraction. By doing so, we hope to prevent the properties of Ethereum from being eroded by trust-based dark pools or proprietary channels which are key points of security weakness. We thus release MEV-Geth with the dual goal of creating an ecosystem for MEV extraction that preserves Ethereum properties, as well as starting conversations with the community around our research and development roadmap.

Design goals

- Permissionless

A permissionless design implies there are no trusted intermediary which can censor transactions.

- Efficient

An efficient design implies MEV extraction is performed without causing unnecessary network or chain congestion.

- Pre-trade privacy

Pre-trade privacy implies transactions only become publicly known after they have been included in a block. Note, this type of privacy does not exclude privileged actors such as transaction aggregators / gateways / miners.

- Failed trade privacy

Failed trade privacy implies losing bids are never included in a block, thus never exposed to the public. Failed trade privacy is tightly coupled to extraction efficiency.

- Complete privacy

Complete privacy implies there are no privileged actors such as transaction aggregators / gateways / miners who can observe incoming transactions.

- Finality

Finality implies it is infeasible for MEV extraction to be reversed once included in a block. This would protect against time-bandit chain re-org attacks.

The MEV-Geth proof of concept relies on the fact that searchers can withhold bids from certain miners in order to disincentivize bad behavior like stealing a profitable strategy. We expect a complete privacy design to necessitate some sort of private computation solution like SGX, ZKP, or MPC to withhold the transaction content from miners until it is mined in a

block. One of the core objective of the Flashbots organization is to incentivize and produce research in this direction.

The MEV-Geth proof of concept does not provide any finality guarantees. We expect the solution to this problem to require post-trade execution privacy through private chain state or strong economic infeasibility. The design of a system with strong finality is the second core objective of the MEV-Geth research effort.

How it works

MEV-Geth introduces the concepts of “searchers”, “transaction bundles”, and “block template” to Ethereum. Effectively, MEV-Geth provides a way for miners to delegate the task of finding and ordering transactions to third parties called “searchers”. These searchers compete with each other to find the most profitable ordering and bid for its inclusion in the next block using a standardized template called a “transaction bundle”. These bundles are evaluated in a sealed-bid auction hosted by miners to produce a “block template” which holds the information about transaction order required to begin mining

[

2042×674 61.9 KB

](https://ethresear.ch/uploads/default/original/2X/d/d12cb0041e4dd5e6f9570176ae05678db7b73afc.png)

The MEV-Geth proof of concept is compatible with any regular Ethereum client. The Flashbots core devs are maintaining a reference implementation for the go-ethereum client.

How to use as a searcher

A searcher’s job is to monitor the Ethereum state and transaction pool for MEV opportunities and produce transaction bundles that extract that MEV. Anyone can become a searcher. In fact, the bundles produced by searchers don’t need to extract MEV at all, but we expect the most valuable bundles will. An MEV-Geth bundle is a standard message template composed of an array of valid ethereum transactions, a blockheight, and an optional timestamp range over which the bundle is valid.

{ "signedTransactions": ['...'], // RLP encoded signed transaction array "blocknumber": "0x386526", // hex string "minTimestamp": 12345, // optional uint64 "maxTimestamp": 12345 // optional uint64 }

The signedTransactions

can be any valid ethereum transactions. Care must be taken to place transaction nonces in correct order.

The blocknumber

defines the block height at which the bundle is to be included. A bundle will only be evaluated for the provided blockheight and immediately evicted if not selected.

The minTimestamp

and maxTimestamp

are optional conditions to further restrict bundle validity within a time range.

MEV-Geth miners select the most profitable bundle per unit of gas used and place it at the beginning of the list of transactions of the block template at a given blockheight. Miners determine the value of a bundle based on the following equation. Note, the change in block.coinbase balance represents a direct transfer of ETH through a smart contract.

\frac {\Delta balance(block.coinbase) + \sum_{tx=0}^n gasPrice_{tx} * gasUsed_{tx}} {\sum_{tx=0}^n gasUsed_{tx}}

To submit a bundle, the searcher sends the bundle directly to the miner using the rpc method eth_sendBundle

. Since MEV-Geth requires direct communication between searchers and miners, a searcher can configure the list of miners where they want to send their bundle.

How to use as a miner

Miners can start mining MEV blocks by running MEV-Geth or by implementing their own fork that matches the specification.

In order to start receiving bundles from searchers, miners will need to publish a [public https endpoint that exposes the eth_sendBundle

RPC](https://github.com/flashbots/mev-relay-js).

MEV-Geth is maintained by the Flashbots core dev team and the source code can be found on Github.

Moving beyond proof of concept

We provide the MEV-Geth proof of concept as a first milestone on the path to mitigating the negative externalities caused by MEV. We hope to discuss with the community the merits of adopting MEV-Geth in its current form. Our preliminary research indicates it could free at least 2.4% of the current chain congestion by eliminating the use of frontrunning and backrunning and significantly increase mining rewards on Ethereum. That being said, we believe a sustainable solution to MEV existential risks requires complete privacy and finality, which the proof of concept does not address. We hope to engage community feedback throughout the development of this complete version of MEV-Geth.

Flashbots: The organization

Flashbots arose out of the MEV Pi-rate Ship, a neutral, chain-agnostic, interdisciplinary research collective that supports MEV-related theoretical and empirical research.

Research and development are tightly-coupled dual engines that propel Flashbots in a phased approach:

- Our research efforts are long-term oriented. They spec out and update our roadmap, define our organization's phases and identify key milestones associated with each of them;
- Our development efforts are milestone-oriented. They are organized as product-focused teams that ship core infrastructure and ecosystem tools, while collecting data and producing other artifacts that feed back into research.

Our research process entails open, transparent and iterative collective creation, which taking inspiration from both academic and applied research, and is modeled upon Ethereum Improvement Proposal (EIP) process. Research contributions are incentivized through an MEV Research Fellowship program.

Public Commitments

As an open research organization, we commit today and in the future, to:

- Preserving the core values of Ethereum in what we create, i.e. openness, permisionlessness, decentralization, against the coming MEV crisis.
- Making our research and core Flashbots infrastructure code open source for any community member to contribute to and benefit from.
- Creating sustainable alignment across key actors of the ecosystem by taking into account the needs of users, miners, developers, node operators, public infrastructure operators and developers, contract/dapp devs, and ecosystem researchers.
- Contributing to open-ended ethical research questions in the MEV space, 100% in the public domain.

Research Objectives

Our goal to mitigate the MEV crisis can be broken down in three parts: Illuminate, Democratize and Distribute. For each part, we've outlined questions we'd like to answer:

Illuminate the Dark Forest

- How can we objectively measure the negative externalities of MEV extraction and impact of Flashbots technologies?
- How can we quantify user harm caused by MEV extraction and provide tooling for builders to reduce their dApp's surface for MEV extraction?
- How can we introduce more transparency in the MEV space for the community to formulate social norms with respect to MEV extraction?

Democratize Extraction

- How can we avoid market mechanics that lead to power centralization?
- How can we create a system that enables efficient MEV extraction in a permissionless manner?
- How can we provide equal opportunity for accessing opportunities provided by MEV?

Distribute Benefits

- How can we create sustainable incentive alignment between miners, traders, DeFi developers, etc.?

- How can we generate virtuous cycles through channeling some of the profits into funding public goods such as Ethereum client development?
- How can we minimize the negative externalities of MEV extraction and maximize positive externalities?

Research Roadmap - Phase I

We've split our research roadmap into different phases that will build onto the results and questions uncovered in the previous phases. We intend for Phase I to consist of two papers:

Paper 1: Flashbots Architecture

Summary: A description of the architecture and design trade-offs of the infrastructure we are building

- How can we build a "good" auction mechanism for communicating transaction order preference to miners?
- What does a formal mathematical definition of a "good" auction mechanism look like? How can we leverage existing auction literature to create a mempool auction theory?
- How would such a mechanism differ across PoW/PoS/Leaderless and in rollups with tx ordering auctions?

Paper 2: Flashbots Ethics

Summary: A discussion on ethical questions related to MEV and the infrastructure we are building.

- Should we build a "good" auction mechanism for communicating transaction order preference?
- How do we minimize possible consensus harms and user harms of priority bribe incentives?
- Should we allow for any MEV on the system? Should we bound the MEV? What social norms are desirable?
- What kind of transparency should we allow in the system with regard to MEV Extraction?
- How does MEV interact with legal system? How do these systems interact with industry self-regulation?

Call for Feedback & Contributions

- Contribute to MEV-Research

We invite you to review ourMEV-Research GitHub repo to learn about our MEV Fellowship program. Start contributing through opening or answering a Github issue, and/or writing a Flashbots Research Proposal (FRP), and join our discussion on our MEV-Research discord community.

- Try our proof of concept

If you are a miner or a mining pool, we invite you to review our code and try running MEV-Geth. If you are a DeFi trader or run bots, we invite you to test out Flashbots and start sending bundles. Join our Flashbots discord community or contact us at info@flashbots.net

- Subscribe to MEV Ship Calendar

You can follow the latest updates and events by subscribing to ourMEV Ship Calendar: join us on our semi-monthly community call "MEV Ship Treasure Map Roast", semi-weekly core dev call, weekly research workshop, and the upcoming unconference: MEV.wtf

Flashbots is stewarded by Scott Bigelow, Phil Daian, Stephane Gosselin, Alex Obadia, and Tina Zhen. We exist thanks to the continued support of members of the MEV Pi-Rate Ship and Paradigm.

Special thanks to Andrei Anisimov, Ivan Bogatyy, Vaibhav Chellani, Brock Elmore, Georgios Konstantopoulos, Jason Paryani, Alejo Salles, samczsun, and Austin Williams for their contributions on MEV-Geth and MEV-Inspect, and Sunny Aggarwal, Surya Bakshi, Phillippe Castonguay, Tarun Chitra, Dan Elitzer, Lev Livnev, Charlie Noyes, Dev Ojha, Dan Robinson, Mark Tyneway, and Micah Zoltu for their feedback on MEV-Research.