Overview

Flashbots Auction is a permissionless, transparent, and fair ecosystem for efficient MEV extraction and frontrunning protection which preserves the ideals of Ethereum. Flashbots Auction provides a private communication channel between Ethereum users and validators for efficiently communicating preferred transaction order within a block.

Flashbots Auction started with mev-geth , a patch on top of the go-ethereum client, along with the mev-relay , a transaction bundle relayer.

In PoS Ethereum, the Flashbots Auction is built on mev-boost , an implementation of proposer-builder separation for Ethereum.

Why Flashbots Auction?

Throughout the second half of 2020 and beginning of 2021, a spike in Ethereum usage 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) caused by inefficient communication between PGA bot operators and (PoW) miners for transaction order preference. These negative externalities create a deadweight loss which is shouldered by regular Ethereum users though high gas price volatility and artificially scarce blockspace.

The extraction of MEV introduces an existential threat to Ethereum's consensus security. This is primarily due to the potential for chain history re-org to extract past MEV, known as time-bandit attacks , and the centralization of transaction routing for the benefits of privacy, low latency, and control over transaction order. These factors critically undermine Ethereum's foundational principles of finality and permissionlessness, posing a serious risk to its very existence.

We've noted with deep concern about the rise of exclusive transaction routing infrastructures that could undermine Ethereum's neutrality, transparency, decentralization, and fairness. As a response, Flashbots Auction is built as an open-sourced, democratic, and credibly neutral alternative, designed to counter these existential threats and risks.

Timeline

- July 2020: Formation of MEV-Ship Research Collective.
- November 2020: Formation of Flashbots Research Organization and proposal of Flashbots Auction architecture
- .
- January 2021: Flashbots Auction Alpha (v0.1) made available for miners and searchers to adopt.
- May 2021: Flashbots Auction Alpha (v0.2) made available for miners and searchers to adopt.
- August 2021: Flashbots Auction Alpha (v0.3) made available for miners and searchers to adopt.
- September 2021: Flashbots Auction Alpha (v0.4) made available for miners and searchers to adopt.
- February 2022: Flashbots Auction Alpha (v0.5) made available for miners and searchers to adopt.
- February, 2022: Flashbots Auction Alpha (v0.6) made available for miners and searchers to adopt.

How does it work?

Flashbots Auction provides a private transaction pool and a sealed bid blockspace auction mechanism. This enables block proposers (validators; previously "miners" in PoW) to trustlessly outsource the task of finding the optimal block construction.

In the standard Ethereum transaction pool, users broadcast transactions to the public peer-to-peer network, specifying a gas price that represents their willingness to pay for each unit of computation on the Ethereum chain. Block builders receive these transactions, sort them by gas price, and employ a greedy algorithm to construct a block that aims to maximize the value derived from transaction fees. This mechanism is a hybrid of an English auction and an all-pay auction , where bids for blockspace are made openly, the highest bidder secures the opportunity, and all participants bear a cost.

Here are the key issues with this mechanism:

1. The open nature of the regular transaction pool leads to bidding wars for blockspace. This results in unnecessary network load and gas price volatility. It also puts less sophisticated network participants at a disadvantage, as they may lack access to advanced bidding strategies.
2. The all-pay nature of the auction results in failed bids reverting on-chain, unnecessarily consuming blockspace. This leads bidders to underprice their bids due to the risk of execution failure, creating artificial blockspace scarcity and reducing validator (previously "miner") revenues.
3. The dependency on gasPrice restricts bidders from expressing detailed ordering preferences, as they are limited to bidding for the top position in the block. This limitation encourages alternative strategies such as spamming to increase the chances of winning, thereby exacerbating the deadweight loss.

Instead, the Flashbots Auction infrastructure uses a first-price sealed-bid auction which allows users to privately communicate their bid and granular transaction order preference without paying for failed bids. This mechanism maximizes validator payoffs, while providing an efficient venue for price discovery on the value of a given MEV opportunity. Crucially,

this mechanism eliminates frontrunning vulnerabilities.

Roadmap

The Flashbots team is taking an iterative approach to decentralizing the Flashbots Auction architecture. As mentioned in our initialethresearch post , there remain some key research questions to be answered.

The ultimate design goals include:

- Pre-trade privacy
- : Transactions are only made public after their inclusion in a block, excluding intermediaries such as relays and block builders. This means that the details of a transaction are not visible to the network until the transaction has been successfully included in a block.
- Failed trade privacy
- : Losing bids are never included in a block, thus they remain unknown to the public.
- Efficiency
- : MEV extraction is conducted without causing unnecessary network or chain congestion.
- Bundle merging
- : Multiple incoming bundles can be merged without conflict.
- Finality protection
- : Once propagated to the network, it becomes impractical to modify Flashbots blocks containing Flashbots bundles. This protects against time-bandit chain re-org attacks.
- Complete Privacy
- : This extends the concept of pre-trade privacy to all intermediaries involved in the transaction process. Not only are transactions hidden from the network until their inclusion in a block, but also intermediaries such as relays and validators are unable to view the content of transactions until they are included in the blockchain. This ensures that no party has an unfair advantage by being able to view transaction details before they are publicly available.
- Permissionless
- : This system does not rely on trusted intermediaries, thus eliminating the possibility of transaction censorship.

Stage PGA DarkPool ⚡ v0.1 ⚡ v0.2 ⚡ v0.3 ⚡ v0.4 ⚡ v1.0 Pre-trade privacy ✗ ✓ ✓ ✓ ✓ ✓ ✓ Failed trade privacy ✗ ✗ ✓ ✓ ✓ ✓ ✓ Efficiency ✗ ✗ ✓ ✓ ✓ ✓ ✓ Bundle merging ✗ ✗ ✗ ✓ ✓ ✓ ✓ Finality protection ✗ ✗ ✗ ✗ ✗ ✗ ✓ Complete privacy ✗ ✗ ✗ ✗ ✗ ✗ ✓ Permissionless ✓ ✗ ✗ ✗ ✗ ✗ ✓

Technical Architecture

The Flashbots Auction architecture proposes a network with three distinct parties who specialize in performing a subset of the work required for sustaining this communication channel.

Flashbots Auction introduces a neweth_sendBundle RPC which standardizes the message format in the communication channel. This message is called a "Flashbots Bundle".

The bundle comprises an array of arbitrary signed Ethereum transactions, accompanied by metadata that specifies the conditions under which these transactions should be included.

{ "jsonrpc": "2.0", "id": 1, "method": "eth_sendBundle", "params": [{ txs, // Array[String], A list of signed transactions to execute in an atomic bundle blockNumber, // String, a hex encoded block number for which this bundle is valid on minTimestamp, // (Optional) Number, the minimum timestamp for which this bundle is valid, in seconds since the unix epoch maxTimestamp, // (Optional) Number, the maximum timestamp for which this bundle is valid, in seconds since the unix epoch revertingTxHashes, // (Optional) Array[String], A list of tx hashes that are allowed to revert }] }

Searchers

Searchers are Ethereum users who opt for the Flashbots private transaction pool over the standard p2p transaction pool. These users keep track of the chain's state and submit bundles to block builders.

Searchers typically fall into one of the following categories:

1. Ethereum bot operators seeking swift and risk-free access to blockspace, such as arbitrage and liquidation bots.
2. Ethereum users seeking protection from frontrunning for their transactions, such as Uniswap traders.
3. Ethereum Dapps that require advanced features like account abstraction or gasless transactions.

Searchers create bundles with information from various sources and send them to a block builder. Searchers submit bundles directly to block builders, bypassing the p2p network. This approach ensuresPre-trade privacy as the transactions remain unseen by the rest of the network until they are included in a block. Searchers express their inclusion bids through Ethereum transactions, either as a gas price or as a direct ETH transfer to the coinbase address. Opting for direct payments over gas price allows users to condition their payments on the success of their transaction, thereby eliminating the need to pay for unsuccessful bids.

See thesearcher quick-start guide to learn how to get started.

Block Builders

Block builders, often referred to as "builders", are specialized entities that receive transactions from users and searchers. Their primary role is to construct the most profitable block from these transactions. Once a block is built, it is transmitted to validators via an mev-boost relay. For a more detailed understanding of relays, refer to theRelays section. It's important to note that searchers can send bundles to multiple builders.

Block builders construct blocks by integrating bundles from searchers and transactions from the mempool, which are submitted by regular users. ⚠ Not all builders can be trusted ⚠

Builders have full view of incoming transactions, which gives them the power to frontrun, censor, etc. When choosing a builder, there are a few criteria to look for:

- Do they uphold fair and unbiased execution principles?* A reputable builder will refrain from front-running, sandwiching, or censoring bundles, and will avoid exploiting privileged data access.
- Are they connected to a reliable relay (or relays)?* Remember that relays also have visibility of raw transactions, which could potentially enable front-running, censorship, and other manipulative practices.
- Are their relays linked to a sufficient number of validators?* The more validators a relay is connected to, the more slots are typically available for builders linked to that relay. If you're aiming for a specific block/slot, it's crucial to send your transactions to a builder that is connected to the validator tasked with proposing a block in that slot. More validators equate to improved inclusion rates.
-
    - Note: Any validator canutilize mev-boost to establish connections with the Flashbots relay and other relays
-
    - .
-
    - It's also beneficial to consider the collective stake of the validators connected to a relay. Generally, if more than one block is proposed to the network (which is unusual but possible), the block with the highest collective stake attesting to it will be included. This scenario is further elaborated in theEthereum docs
-
    - .

Keep in mind that block builders can specialize in certain areas. Some may be more compatible with your strategy than others. While all builders are incentivized to include your bundles in their blocks due to competition, some may prioritize specific strategies over others, regardless of potential profits. Additionally, certain bundles may be censored by builders due to local regulations or corporate strategies. Given these variables, it's advisable to experiment with several reputable builders to determine which ones best suit your needs.

Learn more about thetrust assumptions of the Flashbots Auction.

Relays

Relays play a pivotal role as illustrated in the preceding architecture diagram. Their main responsibility is to securely store blocks received from builders and subsequently make them accessible to validators.

The relay selects the most profitable block from the builders it is connected to and holds it in escrow for the validator. In the mev-boost system, validators select the most profitable block from a variety of relays. Each relay maintains the privacy of a block's contents until the validator commits to proposing it for inclusion in the network.

Specifically, relays do the following:

- Receive new blocks from builders
- Send the header of the most profitable block to a validator upon request* The validator secures their commitment to propose the full block by signing this header
- Send the full block to the validator after receiving the block header signed by the validator
- Execute all of these tasks swiftly and reliably to ensure validators meet proposal deadlines

For a deeper explanation of mev-boost and relays, Check out @thegostep'sethresear.ch post .

For more information about how bundles are sent post-merge, seethis forum post .

Learn more about thetrust assumptions of the Flashbots Auction.

Validators

In Proof of Stake (PoS) Ethereum, validators, also known as "proposers", have the crucial role of proposing new blocks to the network and appending these blocks to the blockchain. For a comprehensive understanding of validators, refer to theEthereum documentation .

Validator uses mev-boost to choose the most profitable block to propose from multiple relays. By incorporating MEV-generating transactions into their blocks, builders can increase the profitability of these blocks. Validators, in turn, can enhance their earnings by selecting these more profitable blocks via mev-boost. For a deeper understanding of mev-boost, visitboost.flashbots.net .

Learn more about thetrust assumptions of the Flashbots Auction.

Trust Assumptions

The current iteration of Flashbots Auction has certain technical constraints that prevent it from operating in a completely trustless manner. Specifically, the network has yet to achieve complete privacy and permissionlessness, both of which are crucial for full decentralization.

Looking ahead, theFlashbots Auction roadmap is designed to replace these trust-based elements with cryptographic and cryptoeconomic guarantees that ensure total privacy. We encourage privacy researchers and other interested parties to review our proposed architecture and contribute to the development of a more robust and decentralized system. Edit this page Last updatedonJan 30, 2024 Previous Sending Tx and Bundles Next Quick Start