MEV Blocker OFA

MEV Blocker's Transaction Flow can be broken down into 6 major steps. In the picture below you can find a general overview of the flow of a transaction.

User submits the transactions

This is the first step, where the user creates the transaction:

1. If you are a normal user in which you have 100% control of all settings, you must first have installed the custom MEV Blocker RPC in your wallet. Learn more about how to do it here
2. If you are a wallet that sends the transaction on behalf of the user, then your code must have integrated the custom MEV Blocker RPC. Learn more about how to do it here

3. If you are a dApp that sends the transaction on behalf of the user - for example, because you use intents like CoW Swap - then your code must have integrated the custom MEV Blocker RPC. Learn more about how to do it here

4. Otherwise, you can prompt your users to protect themselves by adding MEV Blocker using this simple JavaScript

5. If the highest paying bundle no longer simulates correctly on the top of the block (e.g. because the submitted transaction route is no longer available), a lower paying bid can still be included so that the user gets the highest possible reward without a delayed execution (it's also possible that a user gets multiple refunds in a single block).

MEV Blocker system mixes users' real transactions with AI-generated fake transactions

The third step is unique to MEV Blocker; no other RPC providers do this. In this step, the MEV Blocker system generates fake transactions to disguise from searchers the truthfulness of the transactions in such a way that they cannot try to probabilistically exploit the transactions. This step is used as an additional protection mechanism for the user, and it is used to keep the searchers onboarding fully trustless and decentralized. Additionally, depending on the type of transaction, more of the transaction details may be hidden.

1. In the case of swap transactions, MEV Blocker removes some sensitive information (such as slippage tolerance) from the transaction so that it's not possible to effectively sandwich.
2. If the transaction is unlikely to receive a backrun but is vulnerable to sandwiching, MEV Blocker doesn't share it with the searchers at all.

In order for searchers to be able to create the rebate that is forwarded to the user, they first need to create the bundle that captures the value. For this to happen, they need to know the information containing the user's transaction, or else, they wouldn't be able to do it. But, by having access to all the information, it also means that in theory they could probabilistically extract value without following the MEV Blocker OFA rules. In order to avoid this, MEV Blocker hides transactions by mixing them with fake transactions that will never land on-chain. This way, the searcher has to create the bundle based on all transactions, whether they are real or fake, if they want to capture the opportunity they found.

Forwarding the transactions to MEV Blocker connected searchers

The MEV Blocker system shares the transactions with all the searchers connected to the websocket. Once they receive order flow, searchers proceed to crunch their numbers and give their bundles back to MEV Blocker. The searcher that provides the bundle that gives the most value back to the user is declared the winner, not which searcher pays the highest fee to the validator. As long as searchers return in time for builders to still include it in the next block, they can have a chance to have their BID selected.

Forwarding the searcher's bundle for Builders to include them in the next block

In this step, the MEV Blocker system proceeds to gather all the bundles created by the searchers, discarding those containing the fake transactions the system created, and attach the remaining part of the user transaction - the signature - to the bundle so that block builders can create the block with them.

In order to have their bundles forwarded and executed by builders, searchers bid an arbitrary amount denominated in ETH (most likely searchers will have an internal valuation of the backrun bundle profit to be larger than their bid or else wont bid for the opportunity) for the right to backrun a specific transaction. After the builder has selected a searcher bundle bid, they are obligated to refund 90% of the value of that bid to the user, and use the remaining 10% of the value to pay the validator/proposer.

Block builders propagate their block to the proposer

This step is where the actual auction takes place. MEV Blocker forwards all the bundles to all major builders, who then proceed with selecting the different bundles based on the extra value they bring to the validator. As the higher the value for the validator in a block, the more likely the validator is going to select one particular block builder over another.

- If the highest paying bundle no longer simulates correctly on the top of the block (e.g. because the submitted transaction route is no longer available), a lower paying bid can still be included so that the user gets the highest possible reward without a delayed execution (it's also possible that a user gets multiple refunds in a single block).

Transaction inclusion on-chain

Once the block builders have received the transactions and decided which bundles to include in their block, the entire block is passed on via relays to the proposers (validators) who then select the highest paying block.

Once they have selected their "winning" block, the proposer proposes the block, and all the transactions in that block get executed on-chain.

Edit this page Previous MEV Blocker Endpoints Next How can MEV Blocker OFA give you 90% refund?