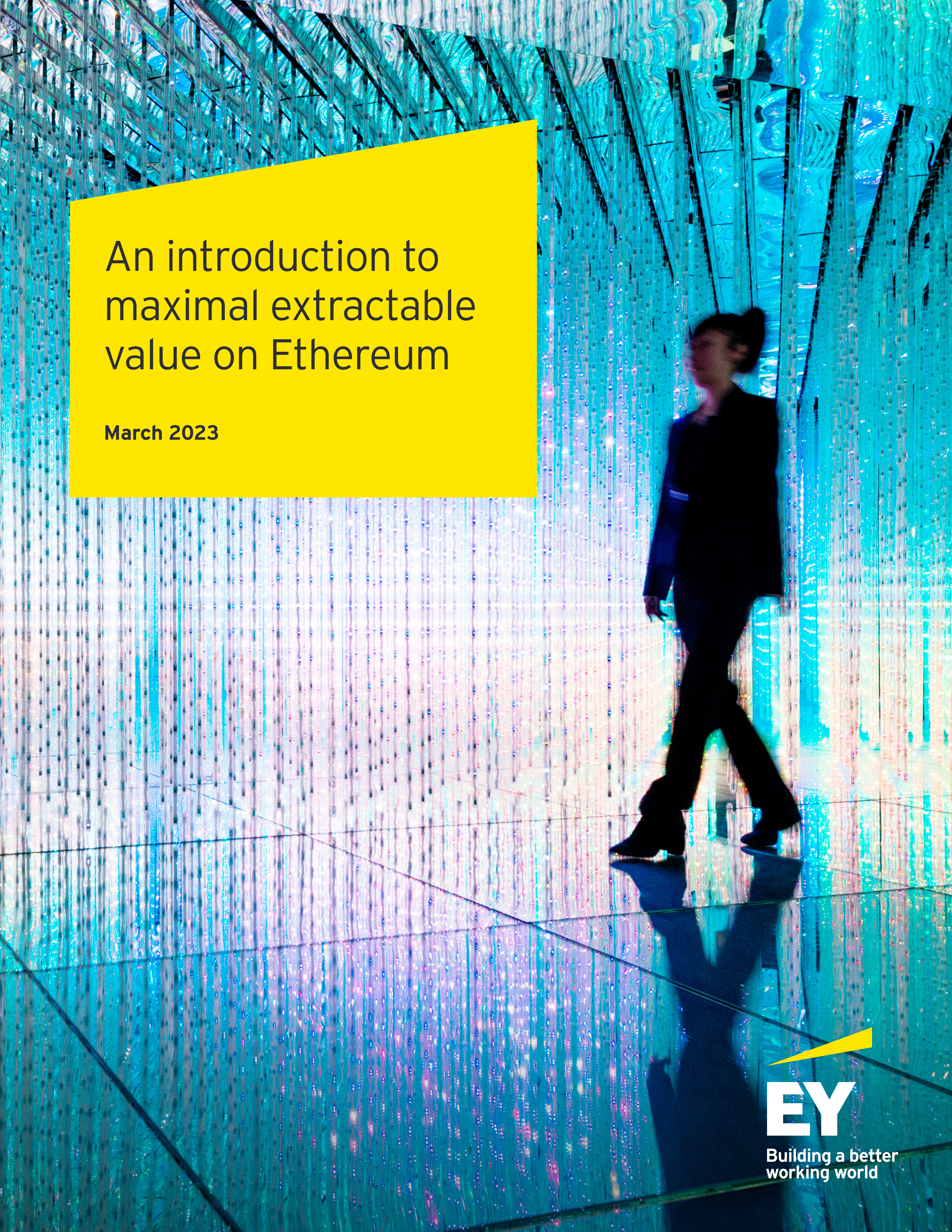


An introduction to maximal extractable value on Ethereum

March 2023

In brief

- Maximal extractable value (MEV) is a complex, systemic problem for public blockchains, particularly for smart contract blockchains with significant transaction volume, such as Ethereum.
- In the absence of centralized intermediaries, MEV is value that is extractable by market participants, usually miners or staking validators, but also by others, which becomes available through the block production process of a blockchain.
- MEV, if left unchecked, can present systemic consensus-layer vulnerabilities that may result in existential risk for any given blockchain and its users.
- There are potential solutions to MEV, but depending on their implementation, they may have various externalities or trade-offs.
- All participants of a given blockchain – from institutional users to retail users, from developers to investors – should be aware of the risks posed by MEV on their selected blockchain, the opportunities being captured by certain participants, and the planned mitigants or solutions.

MEV arises as a function of the overlapping preferences of market participants who transact on a blockchain. MEV is a complex systemic challenge for blockchains with various potential solutions, implementation paths, and externalities.[1] Ethereum, and more specifically the public mempool (the set of pending, unconfirmed transactions), has been described as the "dark forest," a reference to science fiction by Chinese writer Cixin Liu, meaning "an environment in which detection means certain death at the hands of advanced predators. In this environment, publicly identifying someone else's location is as good as directly destroying them." In this paper, we attempt to illuminate the dark forest by answering the question, what is MEV?

There is no way to eliminate MEV entirely. Once users send their transaction to be included in a block, economically incentivized, independent actors in the MEV supply chain look for ways to extract value by reordering, inserting, censoring or front running any arbitrary transaction. According to Flashbots, the preeminent research and development organization working on mitigating the negative impacts of Ethereum MEV, 99% of MEV extraction today on Ethereum is arbitrage activities. Only the most sophisticated actors capture this value.

In the first half of the paper, we define who the MEV participants are, how they capture value, and the serendipitous emergence of Flashbots. Then we will explain the MEV supply chain in terms of how it functioned on proof of work Ethereum and how it functions post-merge, on proof of stake Ethereum.

In the second half, we examine what types of mitigation and redistribution strategies at the application and consensus layers are being developed by the top researchers in this domain. Finally, we address the existential threat of cross-domain MEV and postulate a conclusion about the MEV end game, ultimately placing users in the privileged position that has been historically occupied by miners.[2]

In summary, we believe awareness and understanding of this topic is critical for any market participant looking to build blockchain-based solutions or transact on public blockchains. Ultimately, composable blockchains that prioritize mitigating the negative externalities of MEV will reduce existential risk for their own chains; contribute to broader cross-domain MEV protection; and provide anti-fragile, censorship-resistant public blockchains that mass adoption can more safely take place on.

Preface

Before the invention of specie (hard money), merchants dealt with the problem of finding a coincidence of wants. For example, a shoemaker would need to find a baker willing to swap loaves of bread for shoes if they desired bread. A universal medium of exchange, specie and later fiat currency, solved this problem as goods could be denominated in a unit of account that acted as a store of value (backed by hard money) and medium of exchange. Shoemakers no longer needed to worry how many loaves of bread one pair of shoes could buy. Instead, they could sell shoes for $1 and then in turn buy $1 worth of bread. This helped the baker avoid slippage and created more liquidity for buyers and sellers.

From this point on, capital markets scaled across the world. As capital markets became the modern system we know today, arbitragers were born. These market participants operate within the confines of global value transfer structures to extract value based on the inefficiencies of other market participants' transactions.

While the cryptocurrency market has made significant progress solving the coincidence of wants problem, the overall market structure is still rapidly evolving and has not scaled to comparable levels of maturity as traditional capital markets. On-chain trading is a fundamentally new way of exchanging value and, as such, new types of arbitragers were born. These market participants operate within the confines of various blockchains and extract value referred to as MEV.

Of the various smart contract blockchains, Ethereum has the most advanced on-chain market structure. As a result, we will dive into Ethereum's block production process to define the participants, discuss their overlapping preferences, and consider their motivations forming a Schelling point (a solution people tend to choose by default in the absence of communication) around MEV.

This article does not analyze or discuss the market structure and activities related to centralized exchanges or custodians. Instead, it explores MEV as it exists on Ethereum today, its future appearances, and mitigation schemes. While we will attempt to simplify where possible, we expect the reader to be challenged, and a certain level of knowledge of on-chain trading is a suggested precursor.

Introduction

What is MEV? MEV originally meant miner extractable value. The term has since evolved to mean maximal extractable value. MEV is the value that can be captured on chain in a game that is played among miners, searchers, block builders, wallets and users. The opportunity to extract value arises from ordering, censoring, and/or inserting transactions in front of or behind user transactions that can be seen in the public memory pool before being executed.[3] Historically, mining pools have sat in the privileged position of being able to select which transactions are or are not included in a block.[4]

MEV provides an opportunity for any on-chain actors to extract value. Though the competition is fierce, access is permissionless. Flashbots estimates that more than $720m of value was captured by MEV activities on Ethereum in 2021.[5] It is important to note that MEV opportunities are not distributed uniformly within blocks. They are unpredictable and can be highly lucrative as a result.

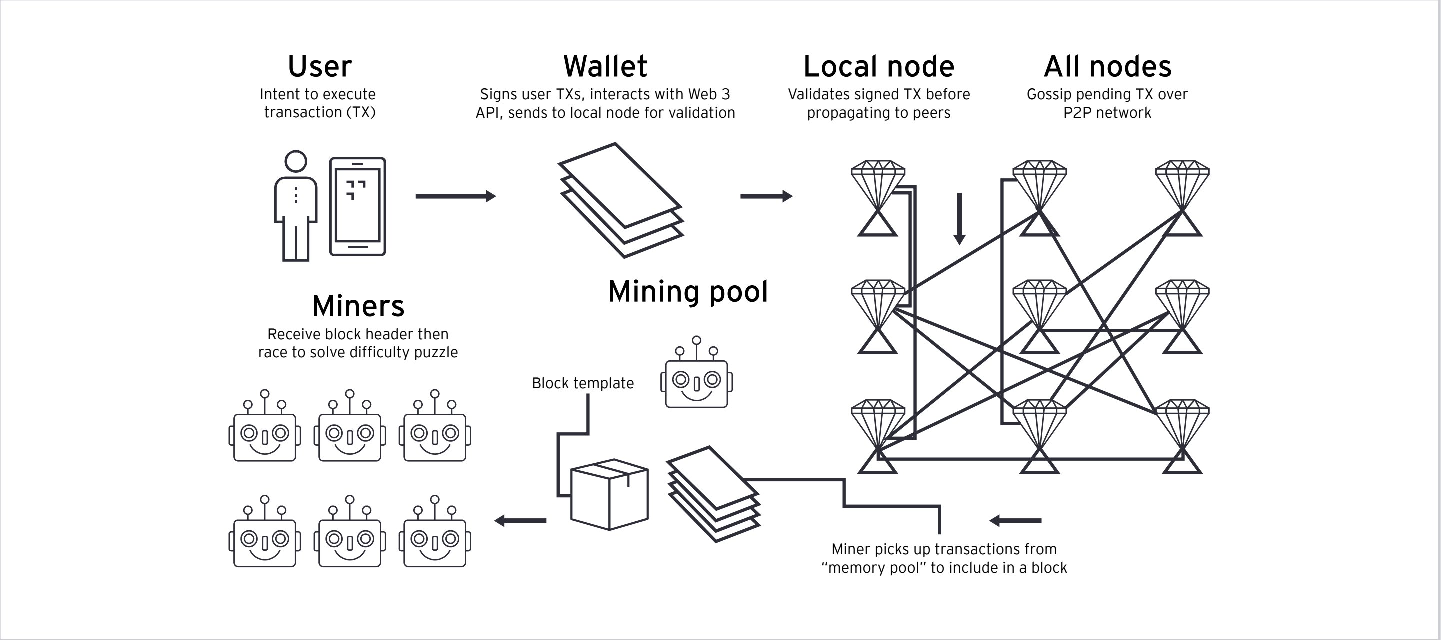
Understanding MEV is integral to understanding the block production process in both proof of work and proof of stake networks. The dynamics of the block space market directly impact the transaction fees users pay and the order in which their transactions are processed.

MEV is a neutral force. However, MEV can be captured maliciously or in an inegalitarian manner. Thus, leaders in the space are thinking hard about how to mitigate malignant forms of MEV, but also how to democratize access for all users, while making block production as economically efficient and decentralized as possible.[6]
We will attempt to explain MEV from the perspective of Ethereum by examining:

- Types of MEV
- Players of the game
- The block production supply chain
- The evolution of MEV and the role of Flashbots (priority gas auctions (PGAs) vs. bundles)
- Long-term solutions (cryptography, sequencing)
- End game and conclusion

There are several recent developments in the MEV space, both for Ethereum and non-Ethereum blockchains, that we don't explicitly discuss in this paper but have summarized below. These developments are the natural progression from what you will read in this paper and are topics we may decide to provide our perspective on in the future, as they evolve. After you have mastered the ideas discussed in this paper, you will want to be up to date on these emerging topics, if you wish to stay close to the rapidly evolving MEV solutions:

- The concept of builders in the MEV lifecycle is discussed in great detail in the paper below. It is widely acknowledged that market participants will seek to specialize as builders, which would exert a centralizing tendency on the protocol and threaten censorship-resistance and the overall resilience of the network. Therefore, the concept of a Distributed Builder[7] is an open research problem with various researchers proposing solutions.
- A related topic is the concept of crLists (also known as Inclusion or Forward Inclusion Lists).[8] This potential functionality seeks to limit the centralization of block builders. For example, when a proposer provides an inclusion list, which is a list of transactions that they demand must be included in the block, unless the builder can fill a block completely, they must be included.
- Since the Merge and Tornado Cash[9] sanctions, there has been much discussion on MEV and OFAC sanctions compliance on Ethereum.[10] MEV-Boost, the Flashbots software discussed in detail in the paper below, has a new Min bid[11] feature that allows validators to maximize Ethereum's censorship resistance by building low-MEV blocks locally while still outsourcing the building of high-MEV blocks. Using this feature carries an opportunity cost—the price of resilience.
- SUAVE[12] is Flashbots' recently announced project which aims to decentralize the block building process. SUAVE is an independent network that can act as a plug-and-play mempool and decentralized block builder for any blockchain. Although SUAVE is a new blockchain, it is not a general-purpose smart contract platform that rivals Ethereum or any other participating chain.
- The topic of order flow auctions[13] has gotten more traction. This is a mechanism where any Searcher/Builder can bid for user order flow. For example, a wallet could provide an auction service to all searchers/builders where they expose a stream of unsigned transactions to be bid on.
- MEV Capturing AMM[14] is an idea propagating that calls for new automated market maker (AMM) to shift the transaction ordering power, at least partly, to AMM designers and liquidity providers. These constructions would allow AMMs to capture part of the MEV that is currently only harvested by block-builders and proposers.


User
Intent to execute transaction (TX)
Wallet
Signs user TXs, interacts with Web 3 API, sends to local node for validation
Local node
Validates signed TX before propagating to peers
All nodes
Gossip pending TX over P2P network
Miners
Receive block header then race to solve difficulty puzzle
Mining pool
Block template
Miner picks up transactions from "memory pool" to include in a block

- Solana[15] and Cosmos[16] ecosystems have been rapidly maturing in the MEV space with products and ideas such as Jito on Solana, The Scheduler on Cosmos, and the Fair Ordering Protocol on Osmosis. While Ethereum core devs and Flashbots have taken the primary lead on MEV research to date, we expect Cosmos and Solana teams to innovate in interesting ways.

0.1 The dark forest

Welcome to the dark forest, where any and all weaknesses will be exploited. In 2020, Dan Robinson from Paradigm wrote a post titled "The Dark Forest" in which he outlined a collaborative rescue attempt of $12,000 user funds stuck in a Uniswap contract. The user mistakenly sent funds to a Uniswap LP token contract. At this point anyone could call the burn function on the Uniswap contract and capture the $12,000. Fearful of generalized front-running bots, the rescue team crafted an obfuscation strategy.

Generalized front runners, also called bots, would see transactions appear in the public mempool and replicate those transactions themselves and bid a higher gas price than a user to be included in a block first, which would cause the user's transaction to revert on chain; the transaction would fail while still paying the gas fee.

The obfuscation strategy required the rescue transaction to be split in two parts so that a general front runner would not be able to decipher the intent of the first sent transaction. The team's local node had fallen out of sync, so they decided to use Infura. The first transaction failed, perhaps due to load balancing issues of Infura Nodes.

As the clock was ticking to call the burn function and rescue user funds, the team decided to ditch the obfuscation strategy. After a nerve-racking moment of waiting for confirmation, their transaction reverted. The team investigated the block and found a generalized front-running bot had stolen their rescue transaction and claimed the user funds from the Uniswap contract.

There are always eyes on the Ethereum Mempool looking for opportunities to extract value. The mempool sets the stage for an adversarial game, MEV, played by rational economic actors. At first this game, identified by the Flashbots research collective (see section 4), was played only in the general mempool in the form of PGAs, which are an all-pay auction where participants bid against each other to have competing transactions included in a block. Later Flashbots moved the game out of the public mempool to an off-chain auction where searchers bid to have bundles included in block templates. After the merge, two layers of auctions exist. Builders bid to have proposers choose their execution block while searchers still compete to be included in builders' blocks.

0.2 Lifecycle of an Ethereum proof of work transaction

We will briefly explain the lifecycle of an Ethereum proof of work transaction by reviewing how user transactions were submitted, propagated, ordered, and ultimately mined, thereby included in a proof of work block. The concepts introduced here will help the reader build an intuition about the MEV supply chain that will be introduced in section 3. Later in section 5, we will examine Mev-Boost, a middleware that plugs into proof of stake Ethereum's architecture. The reader will gain a better sense for post-merge block production there.

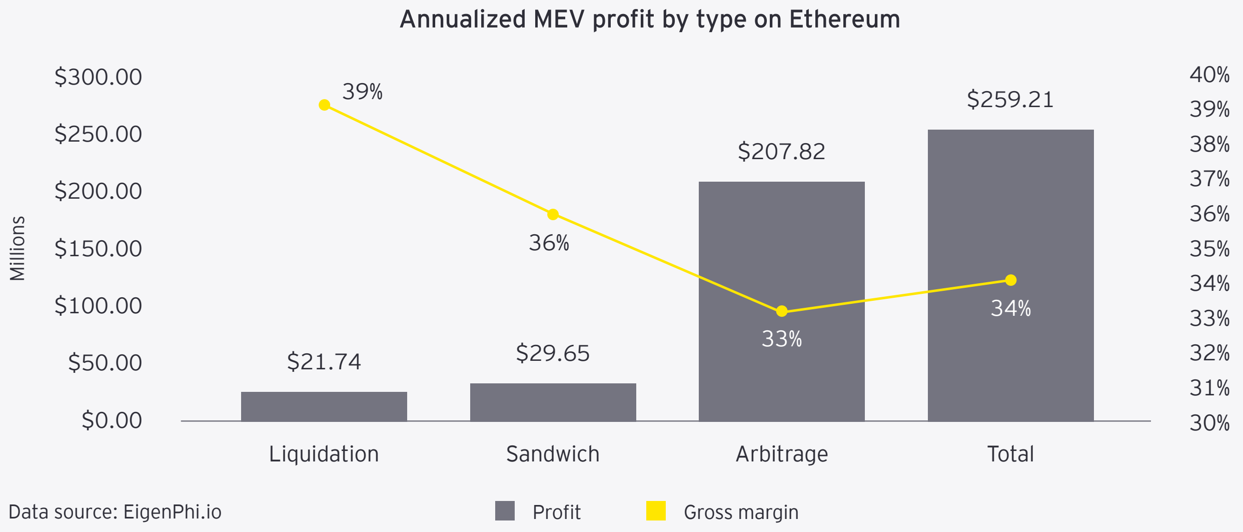
- User who had an intent to transact logged into their Web3 mobile or browser wallet, which is used to connect to decentralized application's front end.
- Wallet signed the user's transaction (TX), interacting with the Web3 application programming interface, then sent the user TX to a local node. Some wallets rely on a node service provider like Infura.
- The local node received the signed TX and validated its correctness before propagating to peer nodes.
- Full nodes gossiped the pending TX and stored it in their general memory or "mempool."
- Mining pools picked up TXs from the mempool and ordered those by a greedy algorithm that sequences TXs based on fees. The limit per block is 30m gas. Target block size is 15m.
- The mining pools created a block template and forwarded the headers to miners who competed to solve the difficulty puzzle, eventually giving the winning block weight in the fork choice rule.
- Once a valid block was mined, the miner informs the network and the block is broadcasted to and propagated by the full nodes, which check that all of the block's transactions are valid; full nodes can reject invalid blocks that do not follow consensus rules.

There were four distinct economic actors in our example; the user, the wallet, the builder (mining pool) and the miners. Here, each party had its own incentives. Users who prefer to get their transactions included in a block paid a gas fee. Wallets who wished to acquire more users provided the lowest latency. Mining pools were incentivized to include transactions paying the highest fees. Miners were incentivized to compete for the Coinbase reward received for mining a valid block.

Miners sat in a privileged position because they had the exclusive ability to order or censor user transactions while inserting their own transactions to capture extractable value. Take for example a user who had an intent to swap Ethereum for Token X on a decentralized exchange. This user's transaction leaked value because they accepted a non-zero slippage on their trade. A miner could have front ran the user by placing an order to copy the user's buy order, which gave the miner a better fill. The miner could have then placed an order behind the user transaction to sell Token X and could have captured the back run opportunity that was created. This is known as a sandwich, which can be included in a block and executed atomically at the discretion of the mining pool. This is just one example of how a miner could extract value created by a user. We will review the general categories of MEV in section 1.

1. Types of MEV

There are four general types of MEV: arbitrage, liquidations, sandwich (front/back run), and long-tail.[17]



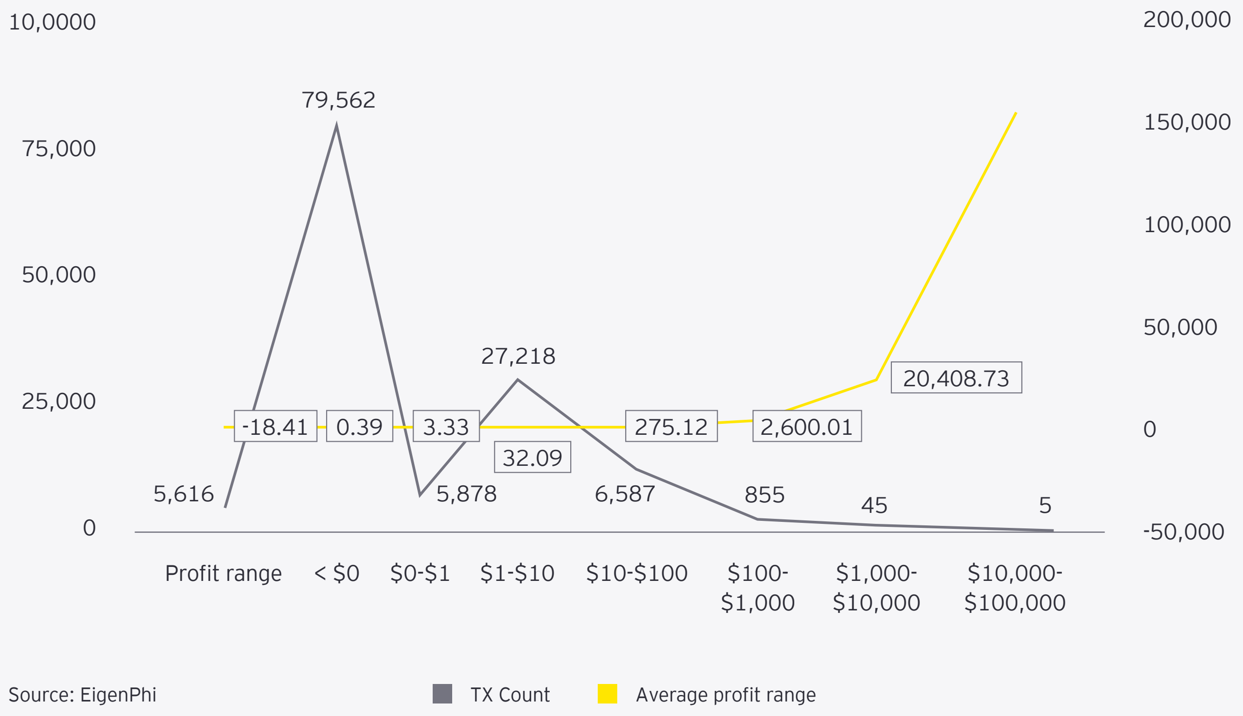
Data source: EigenPhi.io

(1.1) Arbitrage

Arbitrage opportunities account for 99% of all MEV captured.[18] Arbitrage plays an important role on-chain as decentralized exchanges (DEXs) rely on arbitragers to keep prices of their AMMs in line with competing AMMs and off-chain oracle prices.

A common arbitrage opportunity occurs when AMMs that contain the same token pairs, e.g., Ethereum-DAI, across different DEXs are imbalanced (divergent value), allowing for a buy or sell order that can bring prices of both AMMs back in line. Another example would be off-chain to on-chain arbitrage from a centralized exchange to a DEX. This article does not touch on or speculate on this type of arbitrage.

Arbitrage profit distribution vs. transaction (30D)



Source: EigenPhi

(1.2) Liquidations

Liquidations occur when a debt position on-chain becomes undercollateralized. Users who seek liquidity for their on-chain assets can post them as collateral to take out a loan. When the loan falls below a specified loan to value ratio the debt position enters liquidation. Protocols like MakerDAO will auction off the collateral to be liquidated to repay the loan and remove the debt from the system.

Top 10 MEV TXs of all time	Summary of miner payment	Summary of gas used (gwei)	Summary of $gross profit
Arbitrage	**$84,511.82**	**783,001**	**$4,789,881.26**
June 16, 2022, 11:57 PM	$84,294.51	539,041	$2,848,770.92
October 14, 2021, 3:21 PM	$217.32	243,960	$1,941,110.34
Liquidation	**$39,555.58**	**5,338,682**	**$16,345,268.83**
November 26, 2020, 9:13 AM	$4032.15	1,297,423	$4,383,348.37
February 23, 2021, 9:17 AM	$10,519.03	556,359	$3,264,587.08
February 23, 2021, 9:14 AM	$8,089.28	585,789	$1,952,805.68
November 26, 2020, 9:06 AM	$252.27	698,616	$1,791,674.77
February 23, 2021, 9:15 AM	$15,755.83	609,329	$1,784,883.97
February 19, 2021, 10:12 AM	$385.28	890,742	$1,714,368.40
November 26, 2020, 9:03 AM	$512.76	700,424	$1,453,600.56
Grand total	**$124,067.40**	**6,121,683**	**$21,135,150.09**

Source: Flashbots MEV Dashboard v0.1

Liquidators (keepers) receive a fee for their services in addition to the discount on the collateral they purchase for their services. Because liquidations can be quite profitable there is much competition among searchers to capture this form of MEV. As the charts above suggest, liquidations can be extremely lucrative and represent some of the best MEV opportunities for searchers able to capture them.

(1.3) Sandwiches

Sandwich attacks are probably the most well-known form of MEV as they are user-facing. A sandwich attack occurs when a user sends a swap transaction to the general memory pool with a non-zero slippage. An MEV bot, deployed by a searcher, will front run the user by placing a transaction in front of the user's transaction to get a better fill while then filling the user at their max slippage tolerance by moving the price before their trade is executed. The bot will then place a transaction behind the user known as back running to capture the profit of the price being bid up. The user winds up paying a higher price for their swap via slippage and their assets are now worth less post-sandwich than they would have been with no front run/back run. Users can mitigate sandwiches by using Flashbots protect, RFQ orders, Batch auctions, or other direct to miner relay services (Ethermine, Blockroute). There are other novel sandwich-type attacks like just in time (JIT) liquidity, which benefits traders looking for deeper liquidity on Uniswap V3 but the MEV capture comes at the cost of the liquidity provider. The bot will see an order in the mempool, create a transaction to front run, add liquidity ahead of the trade to capture the LP fee, and then remove the liquidity after the swap is complete. JIT liquidity accounts for less than 0.1% of Uniswap V3 trades currently.[19] Sandwich attacks are commonly cited as an example of how MEV is always bad for users. Based on the explanation above, one can see how a sandwich would be negative for an individual user, i.e., the user is getting the worst possible price he or she will tolerate. However, researchers are looking into how on an overall basis sandwiching can be a positive as it makes users avoid bad routes and smooths congestion.[20]

(1.4) Long-tail MEV

Long-tail MEV (LTMEV) activities denote uncommon or infrequent types of MEV not mentioned above. Long-tail MEV can be the most profitable. It is captured by interacting with lesser-known protocols, employing event-based strategies or exploiting design mechanisms. For example, an MEV bot could front run a fraud prover by posting a fraud proof to the network and then claim the reward for successfully proving fraud. This was done during the attempted Rainbow Bridge exploit.[21]

(1.5) Generalized front running

Generalized front running is sometimes considered a "malicious" form of MEV. A generalized front-runner bot will search the mempool for profitable transactions, then copy the transaction and replace the sender address with their own, then increase their bid (gas price) to price + x to be included in a block first front running the original searcher. In a sense, this could be considered MEV stealing. Searchers use private relays to lessen this impact. However, if a searcher uses a particular strategy repeatedly even through a private relay the transaction will still land on chain and become known to observers who can write front-running algorithms for specific instances.

NFT front running is an emergent form of front running that can exploit users attempting to mint an exclusive NFT. A searcher can exploit the rules of the mint by being first in line repeatedly by paying higher transaction fees and inserting their own mint transactions in a block before anyone else. Depending on the logic of the mint contract the searcher can even mint out an entire collection with one transaction.[22]

2. Players of the game

(2.1) Users

Users are the individuals transacting on the network both at the institutional and retail levels. Sophisticated users can enjoy front-running (no one can place an order ahead of user transactions having seen it in advance) free execution by using services like Flashbots Protect for sending transactions. In addition, users can receive front-running protection when trading by using services like COW swap or Archer Swap. The user's order flow creates MEV opportunities. By default, users often send their transactions to the public memory pool.

(2.2) Wallets

Wallets are the medium with which users interact on chain. Wallets can give users the ability to send transactions over a private relay that will send their transactions to a private memory pool to be included in a block. In the future it is expected that wallets will receive payment for order flow from searchers and in turn provide better order execution and/or gas refunds to users.

(2.3) Searchers

Searchers scour the public memory pool for arbitrage opportunities. Searchers will look for an opportunity to insert a transaction or transactions of their own to capture value from changes in the global state. The searcher will then create a "bundle" of transactions that they send using a private relay either via a service like Flashbots, Blockroute, Ethermine, et al. In some cases, searchers directly send transactions to block producers. Searchers will be selective who they send transactions to in order to shield long-tail opportunities from attention or to customize their ordering preferences.[23]

Typically, searchers specialize in one form of MEV over another. As arbitrage opportunities have become crowded, profitable searchers have shifted their focus to long-tail opportunities. Though many searchers operate independently, there are MEV collectives like Project Blanc where Searchers work together to capture MEV while taking a large slice of the opportunities.[24]

Searchers are experts at optimizing for gas savings, the game known as gas golfing. Some will shuffle through contract addresses to get one with as many leading zeros as possible.[25] The EVM gas fee schedule charges less for 0 bytes in a transaction's input data. Skilled searchers can optimize their contracts for more gas efficiencies by writing their contracts in the lower-level assembly language, Yul, which gets them closer to the Ethereum Virtual Machine (EVM) Byte Code (non-human readable opposite of source code).

In the past, searchers were known to use self-destructs or gas tokens[26] to pay for transactions.[27] The tokens could have been purchased when gas prices were cheaper. Searchers leave no stones unturned in looking for ways to optimize for gas savings, allowing them to bid more during auctions.

(2.4) Builders

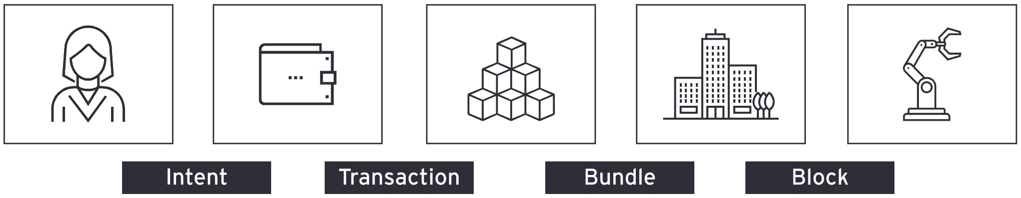
The role of the builder was played by the mining pool who selected the transactions that are were put into the block. The builder then forwarded the hash of the block header to the miners, who competed to mine the golden nonce,[28] which has a value lower than the target. When mining pools or builders received bundles of transactions from searchers via a private relay like Flashbots they participated in an auction by selecting the bundles with the highest profitability. Builders simulated blocks in parallel that determined how profitable a block with n amount bundles would be.

The builder was incentivized to include the searcher's bundle at the top of the block based on a fee they received from the searcher via gas paid for execution of the bundle or directly through the block's coinbase transfer (reward for mining a block). A miner using Flashbots must have also reserved space for transactions in the public mempool.

(2.5) Miners

Miners played the role of block proposer. Miners received a block template from builders (mining pools/MEV-Geth workers) and attested to it via a hashing algorithm, which gave the block economic weight allowing mining participants to come to consensus.[29] Miners captured a priority fee paid by users as well as the coinbase reward for mining a block. Therefore, the higher a transaction fee is relative to other transactions in the mempool, the more likely a transaction would be included in a block.

3. Block production supply chain



User	Wallet	Searcher	Builder	Miner
‣ Alice wants the best execution possible. ‣ Her incentive is to avoid the public memory pool.	‣ The wallet provider wants to provide Alice easy access to on-chain APIs. ‣ Wallet provider is incentivized to have a default API to ensure Alice's transaction is broadcast over P2P network and makes it to the public memory pool to be included in a block.	‣ Searchers scour the public memory pool for arbitrage opportunities. ‣ The searchers send a "bundle" of transactions using a private relay to be included in a block. ‣ Searchers are incentivized to bid the highest amount of their profit margin for their bundles to be included in the next block.	‣ Builders are mining pools who select the transactions that are put into a block. ‣ The builder is incentivized to include the searcher's bundle at the top of the next block based on a fee they receive from the searcher. ‣ A builder will reserve space for transactions in the public memory pool as well.	‣ Miner receives block header from builder and races to mine the correct nonce attesting to it via hashing algorithm. ‣ Miners are incentivized to mine the block with the most economic value.

For mining pools, block production became an increasingly complex process. Priority gas auctions increased competition and demand for blockspace and transaction inclusion. Thus, private relationships between mining pools and searchers/trading firms began to emerge.[30] This could have led to a highly centralized block production cartel.

Instead, Flashbots created MEV-Geth, a bespoke Ethereum client implementation, that provided a trusted MEV-relay for searchers to send transaction bundles to mining pools and provided mining pools software that simulated searcher bundles and mega bundles vs. vanilla Geth blocks (using the greedy algorithm) to ensure profit was maximized.[31]

There was a high trust agreement between searchers and miners with Flashbots acting as an intermediary.[32] The searchers agreed not to spam miners with unprofitable bundles while the miners agreed not to unbundle searchers' transactions. In a way, this relationship secured the block production market by ensuring the most economic value was extracted. Hence, Flashbots saw dominant adoption among miners with over 90%.[33]

4. Flashbots and the evolution of MEV-Geth

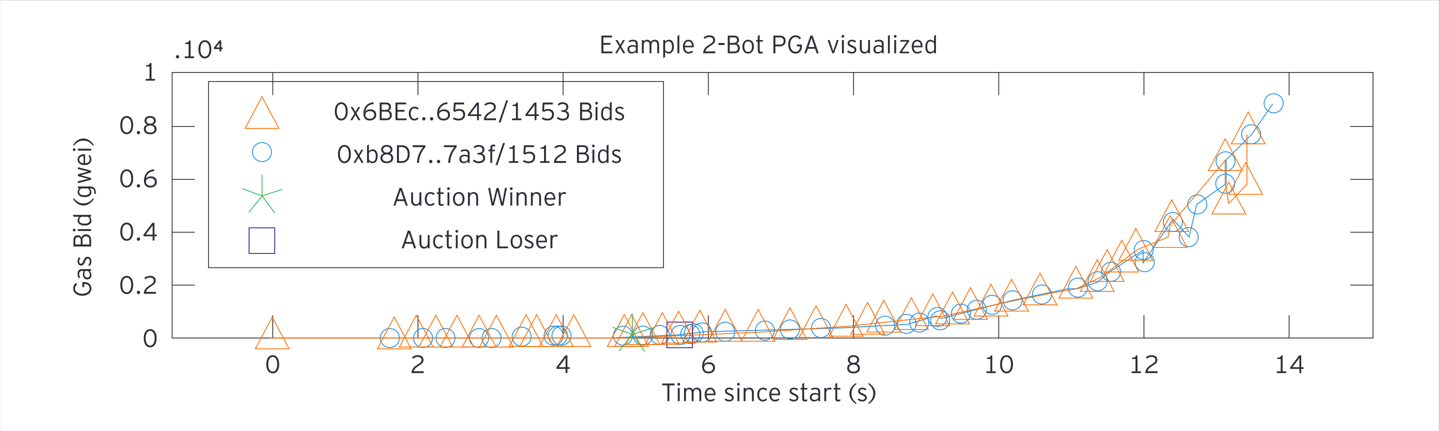
Flashbots is a research and development organization working on mitigating the negative externalities of current MEV extraction techniques and avoiding the existential risks MEV could cause to state-rich blockchains like Ethereum. Its primary focus is to enable a permissionless, transparent and fair ecosystem for MEV extraction. It falls under three goals:

1. Democratize access to MEV
2. Bring transparency and awareness to MEV activity
3. Redistribute MEV revenue

Flashbots currently oversees MEV-Geth, MEV-Inspect, MEV-dashboard v0.1, and MEV-Boost. In response to community feedback following the Merge and the recent OFAC sanctioning of Tornado Cash, Flashbots open-sourced its relayer and builder to ensure a healthy ecosystem of competitive MEV.

4.1 Priority Gas Auctions (PGAs)

Priority Gas Auctions is a term, coined in the Flashboys 2.0 paper, that describes the hyper-competitive game that MEV Bots (front runners and arbitragers) played to get their transactions included in a block first. MEV bots would spam multiple orders (same account and nonce) with higher gas prices until their profit margins were eliminated. A bot could cancel their order by replacing their bid with a transaction paying 21,000 gas, the cheapest Ethereum transaction, costing them a small fee compared with their MEV opportunity. Effectively arbitrage bots were bidding against each other in the form of a hybrid English/All-pay auction the miner arbitrated. The miner was incentivized to order competing transactions based on the highest bids (fees).



PGAs had negative impacts such as:[34]

- Unnecessary peer-to-peer (P2P) networking load
- Inefficient miner and searcher coordination
- Failed bids reverted on chain -> artificial blockspace demand -> disequilibrium
- Searchers not able to express granular preferences

These negative externalities were borne by average Ethereum users who now had less assurance on transaction inclusion guarantees and faced consistently volatile gas prices. Enter MEV-Geth.

(4.2) MEV-Geth

Until the Merge, Flashbots provided a pivotal service in the block production supply chain which moved the PGA game away from the public mempool and made MEV capture more efficient. To achieve this, the Flashbots team built MEV-Geth (Maximal Extractable Value – Go Ethereum), which was Flashbots' bespoke implementation of Geth, providing a way for mining pools to delegate the task of finding and ordering transactions to searchers.[35] Geth was and still is by far the most used execution client implantation of Ethereum. These searchers would compete among each other to find the most profitable transaction ordering and bid for their inclusion in the next block using a standardized template called a transaction bundle.

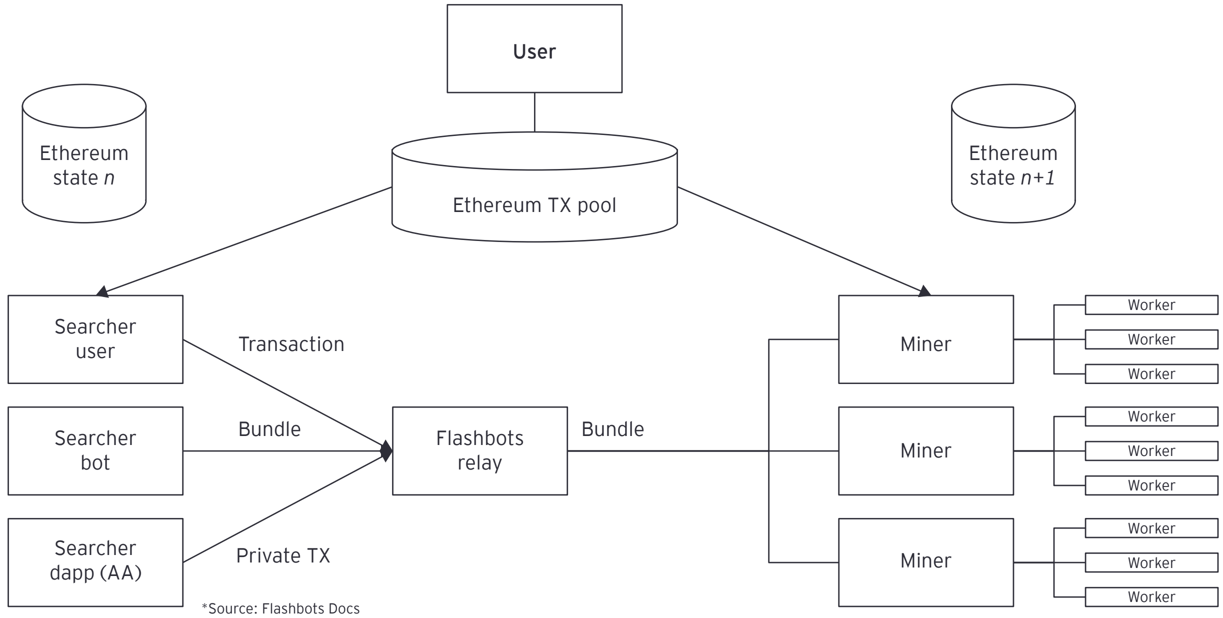
These bundles were evaluated in a sealed-bid auction, Flashbots Auction, hosted by mining pools. The goal of these auctions were to produce a block template that holds the information about transaction order required to begin mining. The highest bundle bid was included at the top of the block. Bundles could not have ordinary transactions from the general mempool inserted between them. They had to follow sequentially in a block.

The searcher bundles allowed for granularity and expressivity. A searcher could specify parameters like a particular block height or transaction execution order which, if not met, would revert off-chain. This was a major improvement from PGAs where reverted transactions had searchers pay unnecessary fees with questionable inclusion guarantees. A searcher bundle could consist of one or multiple transactions. There was no upward limit for how many transactions could be included in a bundle, but was limited by Ethereum's gas limit (30m).

Searchers could send their bundle to a relay who specialized in merging bundles or forming mega bundles. Miners specified a whitelist of relays they were willing to accept merged bundles from. Mega bundles were implemented in Alpha v(0.4) release of MEV-Geth. Mega bundles had to be executed at the top of a block with transactions executed in the provided bundle ordering. Miners picked up mega bundles if they were more profitable than the best-known block so far. This led to significantly increased profitability, approximately +50%.[36]

The searcher bundles were simulated by workers in parallel who compared multiple block constructions to find the most profitable template. The header of the block template, once selected and packed with transactions, was forwarded to miners to mine for the golden nonce.[37, 38]

MEV-Geth



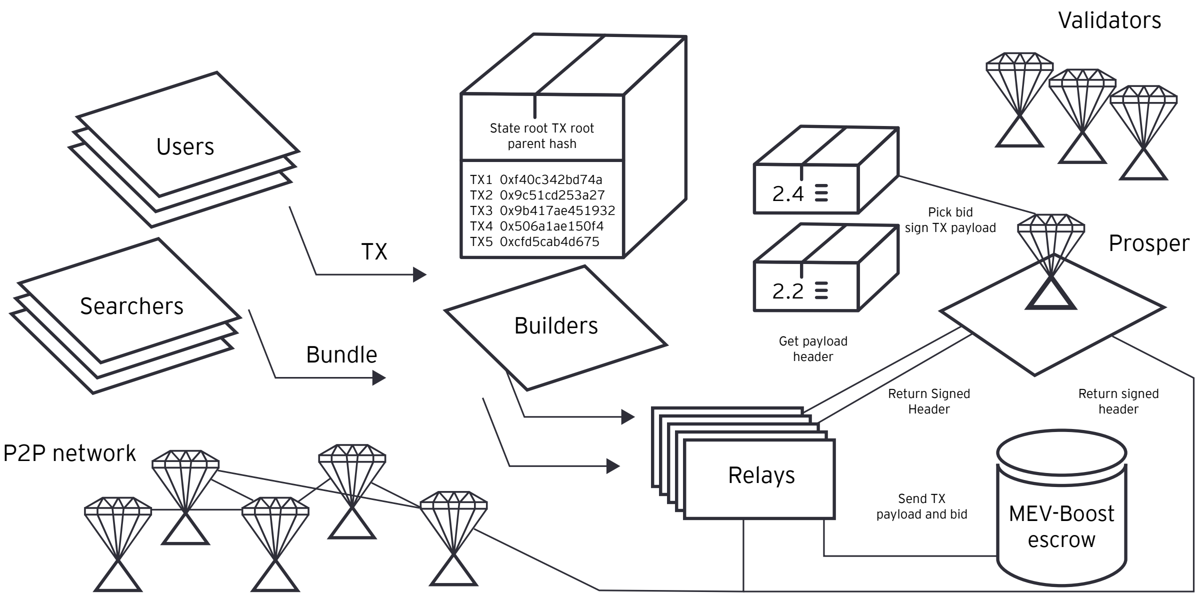
*Source: Flashbots Docs

MEV-Geth is more than software, however. By creating a trusted MEV-relay intermediatory, Flashbots gave a strong guarantee to searchers that their transaction bundles would not be unbundled down the supply chain, which could have allowed MEV stealing. Flashbots also guaranteed mining pools that the searcher's bundles would contain high-value transactions. In the past it would have been possible for a searcher to distributed denial-of-service (DDOS) attack a miner by sending bundles filled with low-value transactions costing more to execute than the value extractable. Indeed, searchers had to build trust relationships with individual mining pools to ensure their MEV would not be stolen.

5. MEV-Boost

MEV-Boost is an implementation of proposer-builder separation (PBS) built by Flashbots for proof of stake Ethereum. It is sidecar (middleware) software that is client-agnostic and sits between the execution and consensus clients, unlike MEV-Geth. The sidecar handles the relay, escrow, profit switching logic for selecting the most profitable payload, and provides a fallback mechanism to a local execution client like Geth if relays get disconnected.[39] Multiple relay services will exist however, which builders will likely route through. A significant benefit of division of labor is role specialization and optimization, which increases the profitability and efficiency of the block production supply chain.

MEV-Boost



Sources: Gosselin, MEV-Boost Merge Ready Flashbots Architecture, Mev-Boost Github

- Validators can but are not expected to produce blocks. Instead, builders will sequence transactions in blocks, including bundles received from searchers, as well as transactions from the general memory pool.
- The builder then forwards block header with a payment (bid) to the proposer, and a commitment to all the transactions to relays, who then communicate with the proposer of the current slot.
- The relay is specialized in denial-of-service protection and networking. The relay validates and routes execution payloads from builders to proposers.
- In between, the escrow, who is trusted by the relay for data availability and privacy, receives the full execution payload from relays.
- The proposer, who is incentivized to choose the payload with the highest bid, then signs the execution payload (stripped of contents) with the highest fee.
- The proposer then returns the header to the relay and escrow to be propagated over the P2P network.

In this way builders sit in the privileged position as they can sequence transactions, insert transactions, censor transactions and merge searcher bundles.

Trade-offs with this design:

- **Information leakage leading to centralization –** large builders will likely also run relays and validators, which could create a centralized block production design
- **Relay proposes bad payload –** inaccurate payload, inaccurate value, missing data
- **Sealed bid vs. open auctions –** if open, missed slots as builders wait for lowest possible bid
- **Out of protocol bribes –** builders could collude to make artificially low bids and share the MEV with validators out of protocol
- **Transaction censorship –** in protocol proposer builder separation will have censorship resistance lists

A core benchmark on the Ethereum roadmap post-merge is the implementation of block proposer and builder separation with censorship resistance lists. PBS not only enshrines the above described MEV-Boost type of architecture into the protocol level and removes the notion of trusted intermediaries, but also will help Ethereum unlock scalability for roll-ups as PBS is required for danksharding.[40]

As we reviewed the block production supply chain above, we should be reminded that separating out the roles of the supply chain can incentivize specialization through division of labor. These incentives will reinforce a decentralized block production process.

Therefore, to prevent the consolidation of validator power and ensure that at-home validators who propose blocks have equal access to MEV opportunities, Ethereum is working toward implementing PBS. The builders would provide block headers for the proposer to choose from including commitment to the block body, payment for the proposer, and a signature from the builder. The proposer will choose the block with the highest fee. This is like the current MEV-Boost implementation outlined above.

In PBS, users will send transactions directly to builders or via a searcher entity. However, there will still be a need for a public mempool to ensure that transactions not processed by builders are guaranteed to be included, as they cannot be censored. The guarantee can be enforced by an attestation game between the proposer of the current block who publishes a CrList (a list of transactions that the proposer sees that must be included) at the same time as their beacon block and the builder of the next block.[41] This list is published to the P2P network. Assuming minimal latency, the builder of the next block must prove to the following proposer that the CrList contains no valid transactions post the current block or the current block is full at 30m gas.

The PBS scheme removes complexity from proposers and enshrines the democratization of MEV at the protocol layer. Until PBS is implemented, Flashbots MEV-Boost will facilitate the separation between builders and proposers.

In theory, PBS has a near identical construction with MEV-Boost. A core difference, however, is how the relay and escrow are performed in-protocol. Therefore, the trust relationship between the builder and the block proposer is guaranteed by Ethereum. Currently, the Ethereum Foundation is researching two varieties of PBS: 2 Slot and 1 Slot. The above diagram showcases the flow of what a 2 slot PBS mechanism could look like.

- **Execution header published;** contains execution block hash, bid, and signature from builder
- **Beacon block deadline;** beacon block must include the winning execution header
- **Beacon block attestations;** only one committee
- **Intermediate block deadline;** the winning builder publishes intermediate block, contains execution block body and visible beacon block attestations
- **Intermediate block attestations;** remaining N-1 committees attest to the intermediate block
- **Signature aggregation of intermediate block attestations (BLS)**
- **Next execution header published**

In this 2 Slot PBS[42] scenario, each slot would span about eight seconds. Effectively there would be two rounds of attestations for the same beacon chain block, one with only the header of the execution block and another round with the block's full body. If the beacon block is missing by the deadline, the next slot will switch from an intermediate block to a beacon block.[43]

(6.1) Single Secret Leader Election (SSLE)

In SSLE, in the context of the beacon chain, a group of validators aim to randomly choose exactly one validator from the group, with the restriction that the identity of the proposer will be known exclusively by the chosen proposer. The specific implementation details are not set in stone.

Vitalik Buterin recently proposed a shuffle protocol relying on a size-2-bind-and-swap primitive that proves two output commitments are re-encryptions of two given inputs without revealing which is a re-encryption of which.[44] The shuffle protocol would use a large amount of these bind-and-swaps to shuffle commitments. Eventually a commitment is picked to be a proposer. The proposer would need to reveal their identity to claim their proposal opportunity. However, the proposer remains unknown until the block is published.[45]

Currently, block proposers are known in advance of their slot. This opens validators to DDOS attacks due to an exposed IP address, which could directly impact at-home staker's ability to capture MEV.[46] An attacker may be incentivized to perform this attack if they propose a block in the next slot. By DDOS attacking the proposer of the current slot s1, proposer for s1 would miss their slot. The attacker then would have two slots worth of MEV to extract.

(6.2) Verifiable delay functions (VDFs)

A VDF is a commit reveal scheme for randomness that introduces time delays. For example, the beacon chain has 32 slots per epoch. Randomness r is generated at the 32nd slot for future epochs. During the epoch, the proposer is invited to reveal a secret they have committed to. Hashed secrets are what generates randomness r. With VDFs the value of r is only revealed well after the slot is finalized.[47] Without VDFs, if a proposer of slot 32 decided not to reveal their secret to bias randomness they could in theory position themselves to propose blocks at specific heights to take advantage of a specific NFT mint or token launch. The Ethereum Foundation is on something called NOVA folding protocol to enable this.

(6.3) Single Slot Finality

Ethereum has shifted from proof of work to proof of stake and hence its sybil resistance mechanism and block production consensus has changed. While Ghost LMD provides dynamic availability like the proof of work GHOST Consensus (Nakamoto family) it also provides provable finality with Casper FFG. This means blocks can be finalized after 2 epochs, 64 slots. However, even with a heaviest chain fork choice rule there is still the possibility of multiblock re-orgs.[48] As a result, Ethereum researchers are investigating how to implement Single Slot Finality for the beacon chain making Ethereum blocks final in each slot. This would eliminate multi-block MEV-related re-orgs entirely.

The limiting factor is BLS signature aggregation. Hundreds of thousands of signatures will need to be aggregated for each slot. BLS signatures allow for signature aggregation. Today signature aggregation is done on P2P subnets. Each committee has signatures aggregated into its own subnet. There are 16 randomly assigned privileged aggregators who make aggregates and commit them to the main subnet.[49] The proposer then takes the aggregate from each committee and aggregates those together to make a single combined aggregate. This scheme imposes a high load on subcommittee validators. Current EF research is focused on this problem, with a time to market of two years or more.

(6.4) MEV smoothing

Smoothing MEV means reducing the variance in the MEV that is captured by each validator, with the goal of getting the distribution of rewards for each validator to be as close as possible to uniform: a staker would then get a share of rewards proportional to their stake, just like with issuance.[50]

A committee-based approach could be optimal on Ethereum as there is a reliance on hundreds of thousands of validators participating in consensus. In this scenario the validators proposing a block would receive an equal distribution of MEV as any validator who is attesting to the validity of the block as well as the proposer. The block proposer in this scenario would not receive all the MEV from the block, but instead share with committee members who made attestations. This approach assumes an implementation of proposer builder separation.

7. Long-term solutions at the execution layer

As Ethereum scales to accommodate users, developers and applications, MEV is shifting from Ethereum's layer 1 enshrined execution environment to layer 2. Layer 2 is a broad term. In Ethereum, layer 2 generally refers to roll-ups, both optimistic and zero knowledge, as well as Validiums, optimistic chains, and new hybrid constructions allowing the user to choose full on-chain security or only settlement like Voltions or Celestiums.

All these layer 2 constructions typically have a more centralized block production scheme than Ethereum's, often using a single sequencer. The leader selection process of the roll-up and defined protocol rules will dictate how MEV is extracted on roll-ups. Optimism is focused on MEV auctions while Arbitrum is focused on fair sequencing. In addition, services like Chainlink and Shutter plan to offer additional threshold encryption schemes, which could combine with the above to help eliminate generalized front-running activity.

(7.1) Fair sequencing and threshold encryption

Fair sequencing refers to predetermined methods of sequencing transactions. The intuition here is that specifying protocol rules for ordering transactions is fair because it helps prevent information leakage, which can be used to extract MEV.

Arbitrum, an Ethereum Optimistic roll-up, currently processes transactions in this method.[51] Recall on a roll-up a user sends transactions to a sequencer who sequences the transactions, collects batches, and posts the roll-up block data to Ethereum in the form of call data. If sequencer is honest then transactions are processed first come, first served. The sequencer's output fully determines the state of the roll-up.[52]

The advantage to a first-come, first-served ordering for Arbitrum is that users receive fast transaction pre-confirmations and do not need to worry about being front run if they trust the sequencer. Once the sequencer sends batch of roll-up data to the layer 1 contract it is final unless fraud is proven through an interactive fraud proof game.

If builders or, in the case of roll-ups, sequencers cannot re-order or insert their own transactions, searchers who optimize for speed become the privileged entities as they become incentivized to co-locate in data centers where the sequencer resides, like high frequency trading. In this way MEV can still be extracted by top of block arbitrage, back-running, optimistic sandwiches, and special arbitrage to identify a few examples.

Fair sequencing can come in several flavors like first-come, first-served ordering, which can be coupled with commit-reveal protocols, the same with delayed recovery, and threshold encryption.[53] The common feature of these cryptographic techniques is to hide the transaction data itself, waiting until the order at the consensus layer has been established, and to reveal the transaction data later for processing. This preserves the causal order among the transactions that are executed by the blockchain.

A threshold scheme requires a threshold committee to generate encryption and decryption keys. The following actions are taken by the committee:

1. Commit – send commitment of private information
2. Sequence – sequence orders
3. Reveal – commit revealed once ordering is final

Committees could be specialized entities like keepers, roll-up sequencers in a permissionless environment or a Decentralized Oracle Network. For example, Chainlink is actively building out a fair sequencing implementation, Fair Sequencing Services (FSS). In addition, Osmosis, an app-chain DEX in the Cosmos ecosystem, is also developing a Threshold encryption scheme.[54]

One of the drawbacks of this approach is that significant communication overhead is added to the network. MEV can also leak to the settlement layer with first-come, first-served ordering as censorship is incentivized. Also, not all transaction metadata can be encrypted as some metadata information must remain transparent for transactions to be executed, including gas price, gas limit, and account signatures. This allows for the aforementioned information leakage which could be used for optimistic front running.

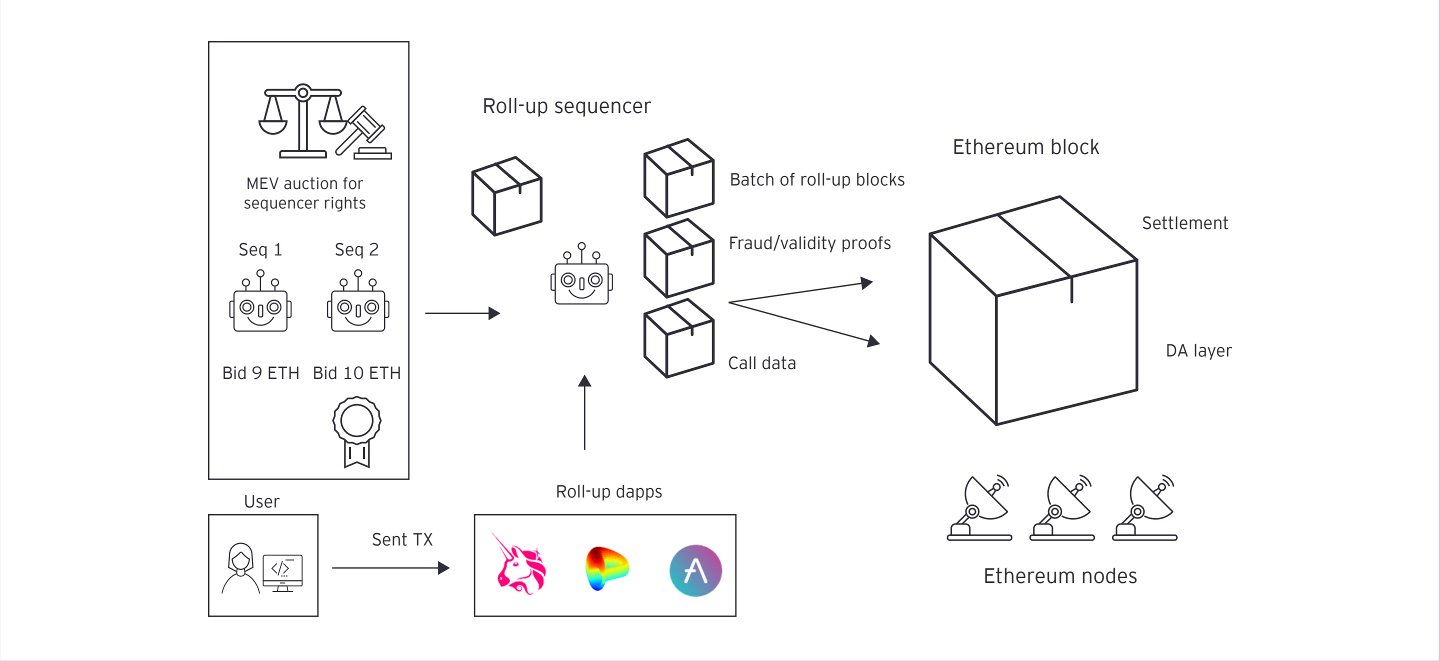
Even so, fair sequencing and threshold encryption is a powerful combination that if implemented appropriately could improve some of these trade-offs.

(7.2) MEV auctions (roll-up sequencer)

Today, Optimism, which is an Optimistic roll-up that settles on Ethereum, relies on a centralized sequencer controlled by the Optimism Foundation. In the future Optimism plans on selling the right to participate in its decentralized sequencer network. In effect potential sequencers will be bidding to produce blocks. Optimism DAO will auction off the right to reorder transactions within an N-block window to the highest bidder. This MEV Auction (MEVA) grants the winner of the auction the rights to reorder submitted transactions and insert their own, if they do not delay any specific transaction by more than N blocks. This should help quantify the value of MEV of a given block, as a potential sequencer would only bid up to a threshold of their total projected profit margin.[55]

The MEVA could be done well in advance of specific block slots to enable a time-based MEV smoothing of sorts where the bidder of the auction would not be able to bid on a granular per block basis. Here the DAO would lock in sequencer revenue. While they may miss out on fluctuations and long-tail opportunities that would prove more profitable for the sequencer in this scenario, the DAO could lock in revenue in doing so, as well as mitigate collusion around slot-based bidding.

The value captured by the OP DAO in the form of the fees collected will be used to retroactively fund public goods. The idea is to have MEV subsidize the growth of Optimism through retroactive public good funding. There are moral and ethical questions around this approach that governance will contend with. Also, it remains to be seen if this Robin Hood type of strategy will motivate users to transact on Optimism over other roll-ups knowing that their MEV is funding public goods.



Conveniently MEVAs are composable with fair sequencing and threshold encryption schemes. The Sequencer in this case would bid up the right to back-run users and win arbitrage opportunities at the top of every block.

Trade-offs to this approach include significantly increasing latency for many transactions. A dishonest Sequencer could censor transactions if protocol rules are not specified, which could include requiring the Sequencer to post a bond and face slashing conditions for censoring user transactions. A Sequencer could re-sell their winning bid and order transactions based on an off-chain bribe.

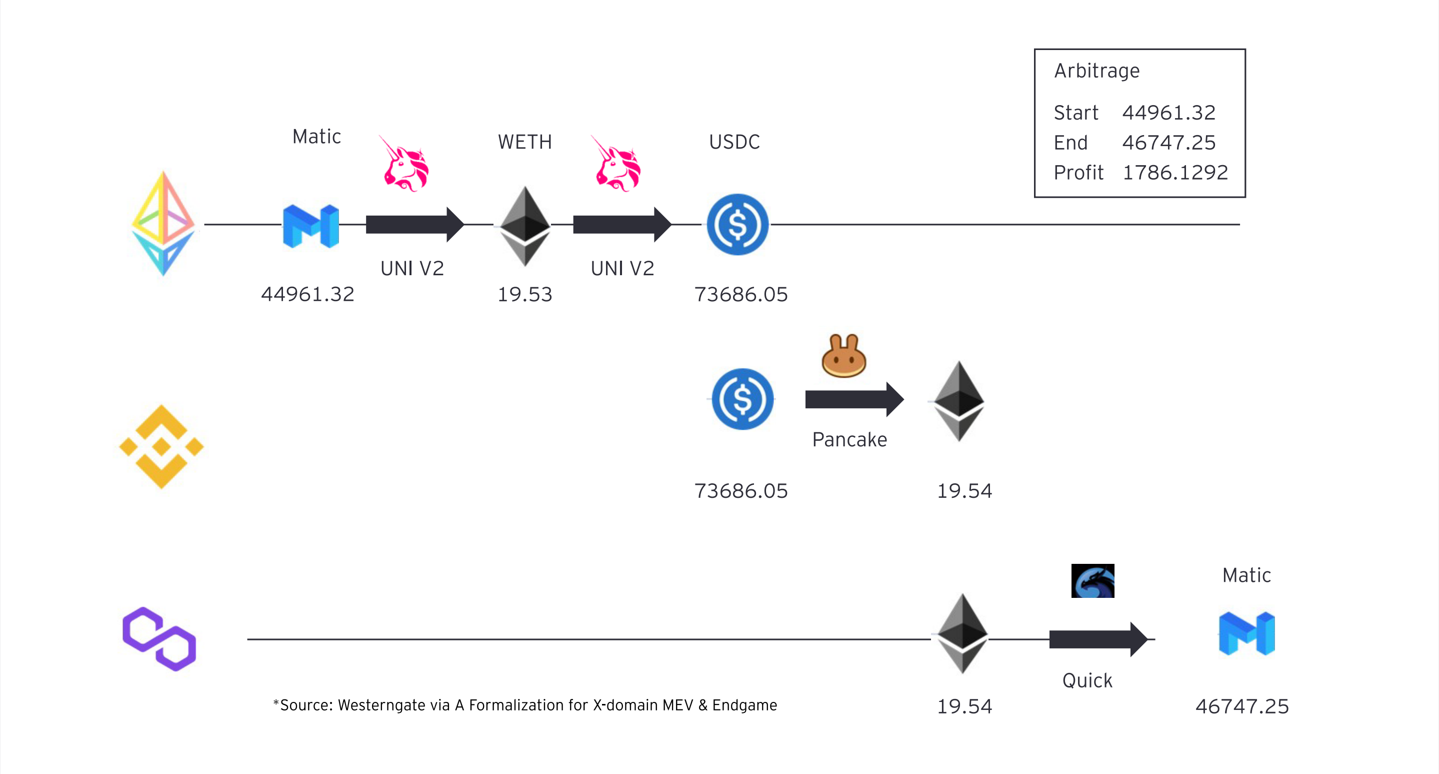
(7.3) Batch auctions

Batch auctions have been a popular research topic as a solution to mitigate pricing inconsistencies in high frequency trading. In a batch auction, orders are placed and collected off-chain, not executed immediately. The orders are then aggregated and settled into batches matching users by finding a coincidence of wants directly or through ring trades. Currently, on Ethereum, Cowswap has the most popular batch auction implementation.[56]

Cowswap's batch auctions work as follows. A user signs a transaction off-chain, which routes their orders to a "solver." A solver is anyone who submits a solution for a batch (order settlement). Solvers compete to find the best order execution by using the user's liquidity to match orders directly by finding a coincidence of wants and/or by using multiple user orders to create rings, which help facilitate the order matching. For example, when multiple traders hold an asset that the others want, their orders are matched and settled directly between these users without the need for an external market maker or liquidity provider. After the process is complete there will be a remainder balance that needs to get posted on chain for execution. The remainder of unfilled orders are routed through a DEX aggregator to complete the transaction.[57]

Hence, batch auctions combine off-chain interactions with on-chain interactions in the same transaction. This allows all traders in a "batch" to receive the same price on their orders while maintaining protection from generalized front-running and sandwich attacks.

8. End game



*Source: Westerngate via A Formalization for X-domain MEV & Endgame

Cross-domain MEV is an existential risk to the decentralization of blockchains. Cross-domain MEV is the value captured from arbitrage transactions executed in a specified order across multiple domains (blockchains L1/L2).[58]

Sophisticated operators across multiple domains are positioned to take advantage of opportunities that are not available to all market participants. For instance, in the above example by Westerngate, the flow of transactions starting with 44961 Matic on Ethereum ends on Polygon with 46747 Matic.[59] Larger players can execute cross-chain arbitrage sequentially in this way, having an advantage with networking latency vs. regular users. Execution is still a risk in this scenario as it relies on message passing and multiple contract interactions.

However, more importantly, a large operator could validate on multiple chains and maintain a large inventory of tokens at any given time allowing for cross-chain atomic arbitrage. This is especially troubling if these cross-chain operators are consensus validators who due to their sophistication will earn more rewards than their peers and eventually dominate the MEV market as their stake weight in proof of stake validation increases. It could be trivial for a large player to censor transactions and find new ways to extract rent from users. There would likely also be collusion or collaboration among the behemoth cross-chain actors. This type of scenario would diminish blockchain decentralization and would enshrine a rent seeking oligopoly that can exploit users via sole domination of the block production supply chain.

However, as Vitalik noted in his "End game" article, block producers are likely to succumb to the MEV forces and wind up centralized either as one roll-up dominates, or multiple roll-ups dominate, but have the same set of block producers. In this case, the decentralization of the base layer Ethereum is what will ensure the integrity of the protocol. With danksharding enabling data availability sampling, Verkle Tries enabling statelessness, and distributed validator technology enabling smaller staking pools, the power to attest to valid blocks and reject invalidate blocks as a light validating node will ultimately keep the network decentralized by increasing user participation in the consensus process.

(8.2) Payment for order flow

In traditional financial markets, payment for order flow is common. However, it is a new phenomenon in the space of blockchains.

In this scenario, searchers/builders would pay to receive order flow from wallets or applications. For example, a searcher/builder may specialize in arbitrage and as a result be able to guarantee specific profit margins on their operations. This would allow them to bid some portion of their profit margin for transaction order flow of wallets.[60]

- The wallet benefits by securing users "gasless" or minimal slippage swaps while the searcher benefits from reliable order flow.
- As searchers receive order flow, they are incentivized to provide builders with the best bundles to maximize their profit (Flashbots auctions).
- The builder may decide to merge with the searcher or secure specific relationships securing specific wallet order flow directly.
- The builder will bid up to their minimum profit margin to the proposer for their block to be selected and signed by the proposer then released and appended to the canonical chain.

If payment for order flow is implemented in an open and decentralized way, everyone up and down the supply chain can benefit. The division of labor will help users negotiate the terms of the game, placing them in the privileged position to extract value. Users are in the ultimate position to choose where transaction order flow goes. Wallets and dapps will have an important role in building MEV-aware systems. In this world, power is placed back in the user's hands.

9. Conclusion

Indeed, as cryptography progresses along with software development and reduction in resource requirements, MEV mitigation at the protocol level is likely. There will be a progression of implementing consensus changes like SSLE, VDFs, Single slot finality and zero knowledge Ethereum Virtual Machine. Changes that require social consensus like PBS will need strong support.

The most promising solution at the consensus level is committee-based MEV smoothing. In this scheme committee members would receive MEV distributions equally based on per epoch attestations. Currently each validator attests at least once per epoch. Their MEV reward would be tied to this attestation, perhaps releasing MEV rewards linearly after each finalized checkpoint (two epochs of 2/3 majority consensus). This would incentivize more stakers to run validators or participate in smaller staking pools because committee attestations, the work every validator contributes to consensus, are equal. No longer would a solo staker proposing a handful of blocks per year be at a disadvantage to large staking pools who smooth their rewards internally. As a positive externality this could reinforce a better staking distribution in the long-term setting Ethereum up to take advantage of stateless clients, post-Verkle Tries.

MEV smoothing could also force the community to have more conversations around what types of MEV are acceptable. In a PBS world, the proposer will be incentivized to accept the maximum bid from a builder. In an MEV smoothing world, the proposer does not have that incentive as they are accepting the bid for all participating validators. This could lead to discussion around whether blocks should contain sandwich attacks or other types of user-extracting MEV. Should builder bids, representing the MEV extracted, be burned? A clear benefit is the formation of social consensus around MEV.

MEV will exist in some form. Acknowledging MEV now while the market is still evolving at the infrastructure and application layers is critical. Existential risks like a centralized block production supply chain lurk but can be avoided by raising awareness of cross-domain MEV and testing mitigation strategies in production. Ethereum roll-ups will provide a robust testing ground. The question becomes what tradeoffs are you willing to make and how fast can you execute?

We believe awareness and understanding of this topic is critical for any market participant looking to build blockchain-based solutions or transact on public blockchains. Ultimately, composable blockchains that prioritize mitigating the negative externalities of MEV will reduce existential risk for their own chains, contribute to broader cross-domain MEV protection, and provide anti-fragile, censorship resistant public blockchains that mass adoption can more safely take place on.

References

1 “Why Is Ethereum Trying to Maximize Value From Users? Two Sides Debate - Ep. 388,” Unchained Podcast, YouTube website, www.youtube.com/watch?v=AhnaiZNv3O4, 23 August 2022.

2 “#29: Interview with a Searcher – with MEV Senpai and Hasu + transcript,” Uncommon Core website, uncommoncore.co/29-interview-with-a-searcher-with-mev-senpai-and-hasu, 19 July 2021.

3 “MEV..wat do next? – Phil Daian (Flashbots),” www.youtube.com/watch?v=vhxIjEnhutw, 20 May 2022.

4 “#29: Interview with a Searcher – with MEV Senpai and Hasu + transcript,” Uncommon Core website, uncommoncore.co/29-interview-with-a-searcher-with-mev-senpai-and-hasu, 19 July 2021.

5 “MEV in 2021: A Year In Review,” www.youtube.com/watch?v=V_wICeVWMgk, 13 January 2022.

6 Every node has a view of transactions in memory waiting to be included in a block memory pool.

7 “Distributed block building,” Github website, github.com/flashbots/mev-boost/issues/139, 7 June 2022.

8 “How much can we constrain builders without bringing back heavy burdens to proposers?” Eth research website, ethresear.ch/t/how-much-can-we-constrain-builders-without-bringing-back-heavy-burdens-to-proposers/13808, 1 October 2022.

9 “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” U.S. Treasury website, home.treasury.gov/news/press-releases/jy0916, 8 August 2022.

10 “Jimmy Ragosa Twitter thread,” Twitter website, twitter.com/JimmyRagosa/status/1597967678672891904?s=20&t=e1fi8kTRrRfue6T2EcJrUQ, 30 November 2022.

11 “The Cost of Resilience,” Flashbots website, writings.flashbots.net/the-cost-of-resilience, 21 November 2022.

12 “The Future of MEV is SUAVE,” Flashbots website, writings.flashbots.net/the-future-of-mev-is-suave, 22 November 2022.

13 “Auctions,” Rook website, docs.rook.fi/reference/rook-protocol/auctions.

14 “MEV capturing AMM, Eth research website, ethresear.ch/t/mev-capturing-amm-mcamm/13336, 10 August 2022.

15 “MEV on Solana Twitter thread,” Twitter website, twitter.com/0xmisaka/status/1506318206281170964?s=20&t=EVYARBvq3ivebZoI6rHEDw, 22 March 2022.

16 “Interchain Scheduler Design Update,” Informal Systems website, informal.systems/2022/10/24/interchain-scheduler-design-update, 24 October 2022.

17 “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges,” arXiv website, arxiv.org/abs/1904.05234, 10 April 2019.

18 “MEV-Explore,” Flashbots website, explore.flashbots.net.

19 “Daniel Robinson - Uniswap v3, or How I Learned To Stop Worrying And Love Concentrated Liquidity,” www.youtube.com/watch?v=mBVgnufwZpA, 20 July 2022.

20 “alpha-v0.5,” Flashbots Docs website, docs.flashbots.net/flashbots-auction/releases/alpha-v0.5, 15 February 2022.

21 “Rainbow Bridge attack,” Alex Shevchenko Twitter thread, twitter.com/alexauroradev/status/1520810591803293696, 1 May 2022.

22 “alpha-v0.5,” Flashbots Docs website, docs.flashbots.net/flashbots-auction/releases/alpha-v0.5, 15 February 2022.

23 “#29: Interview with a Searcher – with MEV Senpai and Hasu + transcript,” Uncommon Core website, uncommoncore.co/29-interview-with-a-searcher-with-mev-senpai-and-hasu, 19 July 2021.

24 “Episode 216: A Dip into the Mempool & MEV with Project Blanc,” Zero Knowledge website, zeroknowledge.fm/216-2, 2 February 2022.

25 “Hitchhikers Guide to the EVM,” Medium website, medium.com/geekculture/hitchhikers-guide-to-the-evm-56a3d90212ac, 24 August 2021.

26 GasToken works by taking advantage of the storage refund in Ethereum. Ethereum provides a refund when

a storage element is deleted. This refund can pay for up to half of the gas used by a contract transaction (only batched sends to contracts, however, can benefit from GasToken). See gastoken.io.

27 "#29: Interview with a Searcher – with MEV Senpai and Hasu + transcript," Uncommon Core website, uncommoncore.co/29-interview-with-a-searcher-with-mev-senpai-and-hasu, 19 July 2021.

28 "MEV in 2021: A Year In Review," www.youtube.com/watch?v=V_wICeVWMgk, 13 January 2022.

29 "The threat of MEV centralization: an anatomy of the transaction supply chain - Hasu (Flashbots)," YouTube website, www.youtube.com/watch?v=GmBqoBr6yI4, 22 May 2022.

30 Flashbots, MEV-geth spec v(0.6) current, v0.6 (current) | Flashbots Docs, https://docs.flashbots.net/flashbots-auction/miners/mev-geth-spec/v06

31 "Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers," Berkeley website, people.eecs.berkeley.edu/~ksk/files/MEV_CFMM.pdf, July 2022.

32 "#29: Interview with a Searcher – with MEV Senpai and Hasu + transcript," Uncommon Core website, uncommoncore.co/29-interview-with-a-searcher-with-mev-senpai-and-hasu, 19 July 2021.

33 "MEV in 2021: A Year In Review," www.youtube.com/watch?v=V_wICeVWMgk, 13 January 2022.

34 "FAQ," Flashbots Docs website, docs.flashbots.net/flashbots-auction/searchers/faq, 2022.

35 MEV-Geth is a bespoke Ethereum client implementation that provides a trusted MEV-relay for searchers to send transaction bundles to mining pools and provides mining pools software that simulates searcher bundles and mega bundles vs. vanilla GETH blocks (using the trivial algorithm) to ensure profit is maximized.

36 "alpha-v0.5," Flashbots Docs website, docs.flashbots.net/flashbots-auction/releases/alpha-v0.5, 15 February 2022.

37 "#29: Interview with a Searcher – with MEV Senpai and Hasu + transcript," Uncommon Core website, uncommoncore.co/29-interview-with-a-searcher-with-mev-senpai-and-hasu, 19 July 2021.

38 "MEV in 2021: A Year In Review," www.youtube.com/watch?v=V_wICeVWMgk, 13 January 2022.

39 "MEV-Boost: Merge ready Flashbots Architecture," Ethresearch website, ethresear.ch/t/mev-boost-merge-ready-flashbots-architecture/11177/25, November 2021.

40 Proposers (validators) will not be required to download all roll-up transaction data (shard blobs), only a portion of the data using a technique called data availability sampling where the data is made redundant using erasure coding and KZG commitments (validity proofs) to prove the encoding has been done correctly. Only builders will be required to download all the shard data. The specification is still under development.

42 "Two-slot proposer/builder separation," Ethresearch website, ethresear.ch/t/two-slot-proposer-builder-separation/10980, October 2021.

43 "Proposer/block builder separation-friendly fee market designs," Ethresearch website, ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725, June 2021.

44 "Simplified SSLE," Ethresearch website, ethresear.ch/t/simplified-ssle/12315, 4 April 2022.

45 "Single Secret Leader Election," International Association for Cryptologic Research website, eprint.iacr.org/2020/025.pdf.

46 "Ethereum Reorgs After The Merge," Paradigm website, www.paradigm.xyz/2021/07/ethereum-reorgs-after-the-merge, 20 July 2021.

47 "Justin Drake - MEV & Cryptography (Flashbots Research Talks)," YouTube website, www.youtube.com/watch?v=jLHf6yw7b5Y, 2 May 2022.

48 "Ethereum Reorgs After The Merge," Paradigm website, www.paradigm.xyz/2021/07/ethereum-reorgs-after-the-merge, 20 July 2021.

49 "Paths toward single-slot finality," Ethereum website, notes.ethereum.org/@vbuterin/single_slot_finality.

50 "Committee-driven MEV smoothing," Ethresearch website, ethresear.ch/t/committee-driven-mev-smoothing/10408, August 2021.

51 The Arbitrum Sequencer is fully centralized; fair sequencing will be put to the test once decentralized

sequencing commences.

[52] "L2 sequencing and MEV - Ed Felten (Arbitrum)," YouTube website, 22 May 2022.

[53] "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks," Chainlink website, research.chain.link/whitepaper-v2.pdf?_ga=2.3986163.2116901074.1657698405-1599499160.1652118244, 15 April 2021.

[54] "MEV Protection Built Into L2s Using Threshold Encryption," Shutter MEV Day 2022, docs.google.com/presentation/d/1_8ztpdNVDrUq-ZeFrIc87Z7ZjdeJoUaJh0rM0k8OX7M/edit#slide=id.g124a42c540e_0_54.

[55] "MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Value," Ethresearch website, https://ethresear.ch/t/mev-auction-auctioning-transaction-ordering-rights-as-a-solution-to-miner-extractable-value/6788, January 2020.

[56] "CoW Swap," CoW Protocol website, docs.cow.fi/front-end/cowswap.

[57] Ibid.

[58] "Unity is Strength: A Formalization of Cross-Domain Maximal Extractable Value," arXiv website, arxiv.org/abs/2112.01472, 2 December 2021.

[59] Ibid.

[60] "The threat of MEV centralization: an anatomy of the transaction supply chain - Hasu (Flashbots)," YouTube website, www.youtube.com/watch?v=GmBqoBr6yI4, 22 May 2022.

Authors

Greg Damalas
Senior Manager
Capital Markets
Ernst & Young LLP
gregory.damalas@ey.com

Patrick Ambrus
Contract Crypto Researcher
Ernst & Young LLP

Other key contacts

Steve Beattie
Financial Services
Crypto Risk Leader
Ernst & Young LLP
steven.beattie@ey.com

Paul MacIntosh
Financial Services
Crypto Leader
Ernst & Young LLP
paul.macintosh@ey.com

Daniel Scrafford
Financial Services
Crypto Leader
Ernst & Young LLP
daniel.scrafford@ey.com

Rebecca Carvatt
Financial Services
Crypto Banking & Capital
Markets Leader
Ernst & Young LLP
rebecca.carvatt@ey.com

Paul Brody
Principal
Global Blockchain Leader
Ernst & Young LLP
paul.brody@ey.com

Chen Zur
US Blockchain Practice
Leader
Ernst & Young LLP
chen.zur@ey.com

David Byrd
Blockchain Strategy Leader
for Assurance
Ernst & Young LLP
david.byrd@ey.com

Arwin Holmes
Global Blockchain CTO
Ernst & Young LLP
arwin.holmes@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

US SCORE no. 18928-231US

2210-4104748 BDFSO
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com