COINMETRICS

WHAT IS MEV ANYWAY?

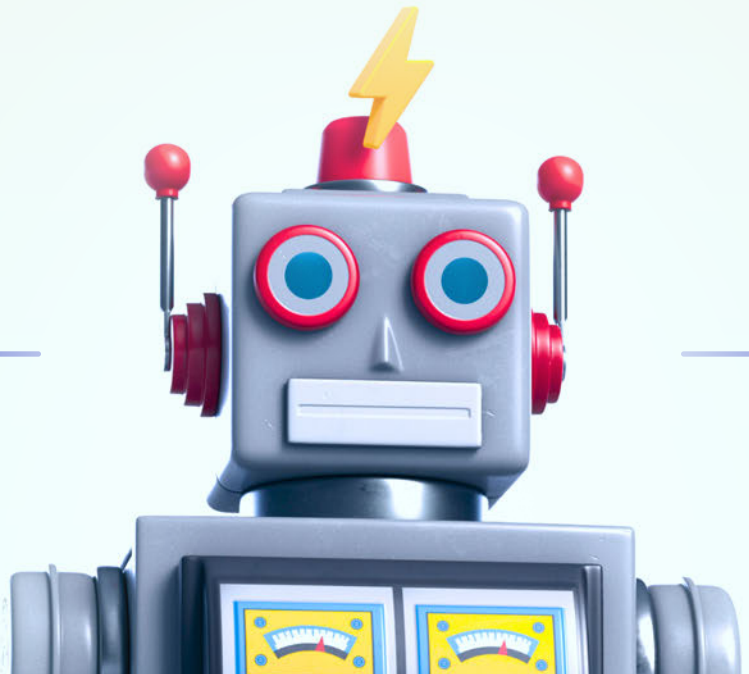
AN INTRODUCTION TO THE EXISTENTIAL THREAT FACING ALL BLOCKCHAINS

By Alex R. Mead Ph.D.

WHAT IS MEV ANYWAY?

AN INTRODUCTION TO THE EXISTENTIAL THREAT FACING ALL BLOCKCHAINS

This research paper aims to provide a summary overview of maximal extractable value (MEV), also known as miner extractable value, and its potential impact on the Ethereum blockchain and stateful blockchains as a whole. The concept of MEV has sparked a significant amount of interest and concern in the blockchain community, and this paper aims to shed light on what it is and why it matters. We will begin by examining the fundamental principles of MEV, followed by an overview of its prevalence in the Ethereum ecosystem. Through the examination of real-world examples, we will delve deeper into the mechanics of MEV and its potential consequences.



MAXIMAL EXTRACTABLE VALUE (MEV)

MEV is *the process of extracting additional value beyond tips and block rewards a validator (or miner) can extract by reordering, blocking, or including additional transactions within the blocks they produce.* This broad definition intentionally covers a wide range of behaviors, and while most MEV actions are relatively low in value, some can be very large. For example, this block worth 430 Ether ($515k USD day of trade), or this block worth over 200 Ether ($234k USD day of trade), which both occurred over a few day stretch in November 2022.

To begin to explain MEV, you need to understand how transactions are submitted to and processed by blockchains. The primary focus of this paper is the Ethereum blockchain; however, the principles discussed apply to other blockchains as well. MEV can occur on both Proof-of-Work and Proof-of-Stake consensus blockchains, independently of their consensus mechanism.

Ethereum Nodes and the Mempool

When a user of Ethereum engages with the network, it is always in the form of transactions that are submitted to a node in the network. This typically happens using browser-based frontends, such as Uniswap or Aave, but can also be undertaken programmatically using tools like web3.py. Regardless of how the transactions are made, the lifecycle always follows a well-defined series of steps.

To begin, the transaction data structure itself is formed with various fields, including the "to" address, "from" address,[1] the "value" of ether to be sent, as well as the "gas price," and others. This transaction is then "signed" using encryption and sent to a node on the Ethereum network. Once at a node, the transaction will wait to be processed in a public mempool with all the other transactions waiting to "use" Ethereum. Sending a transaction is similar to sending a postcard in the mail, with a "to" and "from" address and the content completely visible to anyone handling it. Further, a fee is paid to the postman in the form of a stamp.

An important note on the mempool is that each mempool's contents are specific to its node. Each mempool contains a slightly different set of transactions as they are broadcast through the system.

[1] Technically the "from" address is derived from the signature part.

This is because transactions are originally sent to just one node, and then that node broadcasts the transaction to other nodes. These delays can be understood by modeling the Ethereum node network as a partially connected mesh network using a flooding routing algorithm.

This broadcasting of the transactions continues until a given transaction is included in every mempool (i.e., one per node) on the network. With new transactions being broadcasted continuously, transactions will eventually be received by all nodes around the world; however, not exactly at the same time. It usually takes anywhere from 100 ms to 500 ms for a transaction to effectively be present in all mempools across the Ethereum Network. For an insight into this network delay, see zeromev.org. They run three geo-distributed nodes and estimate average network delay for the transactions within a block; that figure is then displayed when examining a block in the top right corner of the page.

Ordering of Transactions Within Blocks

The next question is: how are the transactions picked from the mempool and bundled into blocks with limited "space" for transactions? This notion of transaction selection and ordering is critical to MEV, so let's look at this a little closer.

If two transactions arrive at nearly the same time, both using about the same amount of gas, the user willing to pay more *per unit of gas* will be processed by the Ethereum Virtual Machine (EVM) first. Meaning users communicate their desire to be processed by the EVM through the price they are willing to pay for gas. This is similar to a classic first-price auction; in Ethereum, this process happens in groups of transactions every 12 seconds.

Hence, in theory, the highest bidding transactions[2], where bid = gas_price * gas_used, are collected from the mempool every 12 seconds, processed and included in the next Ethereum block. As such, a transaction can be included quickly by paying a higher gas fee, or with a lower gas fee, can be "stuck" in the mempool for longer periods until gas prices reduce to make their bid competitive. Current Ethereum system wide parameters permit a maximum 30 million gas units to be used each block, hence Ethereum block space is a scarce resource and necessitates the transaction gas auction to determine what transactions are included.

[2] To learn more about gas on Ethereum, check out our Coin Metrics Report on the topic.

This batched ordering of transactions based on a user's willingness to pay more is generally referred to as the *fair-ordering*[3] of transactions. When you step back and examine the system, it makes sense—most Ethereum users would agree this is intuitively a pretty fair way of doing things. However, the plot thickens when one realizes the transaction submission to Ethereum is a bit more complicated. For example, by moving a transaction's position within a block its value can change significantly because the state of the blockchain is dependent on block location. More details will be provided below, specifically private mempools and proprietary orderflow.

Dangers of the Mempool (The Dark Forest)

One critical feature of Ethereum and the mempool to consider is that the mempool and the current state of the blockchain is visible to anyone with access to a node. A second feature to consider is that the transactions are sitting in the mempool, for all to see, for potentially several seconds to minutes. This is a dangerous situation, and often referred to as The Dark Forest.[4] It is dangerous for anyone with profitable transactions as deeply skilled players, typically in the form of bots, are watching the mempool and taking action to profit at the expense of unsuspecting user transactions. This is where the *ordering, inclusion, and exclusions of transactions* from the definition of MEV above come into play. Next, we will go into some details of how this happens on-chain.

A Brief Summary of how MEV Works

Now, putting it all together, we will briefly explain an MEV example. MEV begins when a user submits a transaction to the public mempool, which will be profitable for them to execute. However, due to the public nature of the mempool a bot sees the transaction and copies it with the payment address changed to its own. After confirming the transaction is profitable via EVM emulation locally, the bot submits the copied transaction with a higher gas price. The validator will then likely put the bot transactions ahead in the ordering of transactions in the block, because it will receive more in gas fees. This allows the bot's transactions to beat the original user to execution and "extracts" the value

[3] Some MEV researchers refer to the time of arrival of transactions in the mempool as the "fair-ordering." That is, a first-in-first-out (FIFO) mempool construction. zeromev.org is one such group.

[4] "The Dark Forest" is an informal name for the mempool playing off the name of the book by Liu Cixin and was originally put forth by the now classic paper, "Ethereum is a Dark Forest," by Dan Robinson and Georgios Konstantopoulos of Paradigm Research. In the article, Robinson describes a situation where he tries to recover a user's $12,000 worth of tokens left on the proverbial Ethereum sidewalk — without alerting any opportunistic bots to the booty. Despite some clever mempool obfuscation, a bot sweeps up the funds before he can rescue them.

for both the validator (in higher gas fees) and the bot itself. This is the simplest example, or pattern, of how MEV works, and is known as a "generalized frontrun." Other examples—including decentralized exchange (DEX) arbitrage and sandwich trades—are covered next.

MEV Patterns and Transaction Semantics

Ordering, *inclusion*, and *exclusion* of transactions is a very broad definition, but in practice, several "patterns" of this behavior exist and are generally known as MEV. Below we will cover several known types of MEV in more detail. Further down, on-chain examples for some of these patterns are also presented.

It is crucial to know, all MEV discussions and measurements will always capture a lower bound estimate of the MEV of a given block or transaction. While several typical patterns exist and are well known for MEV, there is always the possibility that advanced users are taking actions not well understood and they go undetected by the Ethereum community, however, they are still MEV. It should also be noted for clarity, not all transactions can be exploited via MEV. For example, a simple ether transfer with no smart contracts involved cannot be exploited.

Generalized Frontrunning

As mentioned above, this pattern of MEV involves an unsuspecting user submitting a profitable transaction to the mempool. A bot watching the mempool copies that transaction, replacing the payment address with their own. After confirming the transaction is profitable, the bot submits it to the mempool with a higher gas fee. This higher fee incentivizes the validator to pick the bot transaction first, meaning the original user transaction is "frontrun," and results in an error when their transaction is executed as the "value" is already gone.

Frontrunning is perhaps the simplest type of MEV and is the topic of the—now classic—Ethereum is a Dark Forest paper. However, getting "frontrun" is still a very real possibility, and even a certainty, for transactions submitted to the public mempool. In reality, the presence of generalized frontrunning bots is so common that not only will your transaction be frontrun, but likely several bots will compete with each other to frontrun you. Keep in mind, this is only applicable to certain transaction types, generally those involving DeFi of some type. For example, a regular ether transfer between accounts cannot be "frontrun."

This results in a gas bidding war, called a gas priority auction (GPA), for proper position inclusion in the block and has driven a whole "cottage industry" of reducing gas fees included by frontrunning. This process, called gas golfing, is based on the premise that if a bot can do the same transaction as another bot for less gas, they can bid a higher price per gas and still be profitable with a given frontrun.

As discussed below, the MEV landscape has changed dramatically in the last few years. It should be noted that in the present Flashbots-led MEV system discussed later, GPAs are not as prevalent. This is because the mempools have become private for MEV so there is less direct head-to-head bot bidding. Further, at present, the MEV system comes with guaranteed execution as a feature, so if a transaction fails, the user doesn't pay a fee. A common argument in favor of today's MEV Relays is that they make block space cheaper, on average, because there are fewer failed transactions included on-chain arising from GPAs.

DEX Arbitrage

Simple in its construction, a DEX arbitrage begins with the condition on-chain of a single token being available on two separate decentralized exchanges (DEX), for example Uniswap and Curve, at a different price. Seeing this difference, a bot buys at the lower price and sells at the higher price, all within a single transaction. This trade is thus "risk-free" because of the atomic nature of transactions in a single block. Meaning, if the transaction doesn't go through, both purchase and sale fail, not just the purchase.

This atomic, risk-free, money guarantee has created a large number of DEX Arbitrage bots. These bots make the reality of running a profitable DEX Arbitrage very competitive and akin to the original Flashboys days, analogous to traditional markets with high frequency trading. However, as opposed to frontrunning, many would point to DEX Arbitrage as a benevolent form of MEV because arbitrage transactions are facilitating the price discovery process for assets in the crypto marketplace.

Sandwich Trading

Sandwiched MEV trading is one of the most malicious forms and involves price manipulation specific to decentralized exchanges (DEX) on blockchains. It consists of a bot identifying a large trade request on a DEX in the public mempool. Due to DEX mechanics, this trade will move the price of the assets—that is, if the trade is large enough as compared to the trading pair reserves. Bots target mainly trades of significant volume likely to drain local market liquidity and move those prices. Bots may then "sandwich" this original trade transaction with both a frontrun and backrun transaction.

The first bot transaction buys a large amount of the asset the original trade was intended to acquire. This transaction is specially designed to move the price of the asset just enough that the original order will still be executed. As expected, the original transaction then goes through at the DEX, driving the cost of the asset up even further. Finally, the bot's backrun transaction then sells the originally purchased asset from the frontrun at that higher price.

As can be seen, an MEV sandwich extracts value from an unsuspecting user and transfers it to the bot through the second asset sale and the participating validator through gas fees. One should note, however, that sandwich attacks do carry some risk, as the second transaction may not go through, causing the bot to be stuck with the original DEX transaction. This risk is largely mitigated with modern MEV systems; however, it still exists for sandwich trading.

Liquidations

Liquidations are the blockchain equivalent of a margin call in traditional finance and come into play for lending protocols like Aave or MakerDAO. In general, on-chain loan protocols allow users to "borrow" tokens up to a protocol-defined ratio of some deposited collateral.

As market conditions change, the loan-to-collateral ratio changes; however, the margin requirement ratio of the loan does not. If the loan-to-collateral ratio drops below the protocol's requirements, the loan is revoked (i.e., is liquidated), and a fee is charged to the loan owner. This liquidation for on-chain loan protocols is initiated by some third party, the address of which receives some of that user fee, and thus creates an opportunity for MEV.

Knowing all the loans are publicly available on-chain, MEV bots scour outstanding loans for users who failed to meet the required loan-to-collateral ratio. With the loan user identified, they design a margin call transaction to liquidate the loan and collect part of the user fee as a reward from the protocol. This mechanism ensures the loaning users receive their collateral back and non-performing loans are terminated.

While many argue liquidations are a healthy part of the decentralized finance world, clearing "bad debt," they can quickly turn malicious. For example, a bot can manipulate the price of a token to force a liquidation that would not have occurred if their price manipulation had not occurred. Further, blocking a user transaction trying to put more capital into the collateral of a loan can also happen. This forces the user into liquidation, even though they may have tried to avoid this if only their transaction was processed.

Other MEV Patterns

As mentioned above, the discussed MEV patterns are a subset of all possible MEV opportunities. Others include *NFT sniping* and *cross-chain* MEV through bridges. But the number of MEV opportunities continues to grow as on-chain experimenting continues. It is very likely MEV patterns are being executed which are not well understood beyond the searcher performing them.

There also exist "counter measures" to MEV such as the ENS Domain system two step registration process. First a user pre-registers, then reveals their domain using two separate transactions specifically to avoid frontrunning. Another complication, called a salmonella attack, is a predatory contract designed to take advantage of MEV bots. All in all, the expressions MEV can take are manifold and are continuing to be developed.

"Helpful" versus "Malicious" MEV

There is an ongoing, charged debate about MEV's role within blockchains. Opinions range from a fair part of a market's price discovery mechanism to MEV is outright exploitation. The truth is more complicated, as there are clear examples like frontrunning or sandwiches that just cost users. Still, there is also price discovery arbitrage which helps keep DEX pricing aligned throughout the ecosystem.

With this in mind, knowing the opinions of who and what you're reading and learning about can be helpful when it comes to MEV. Flashbots is a very large player in MEV as you'll learn below and represents a balanced pro-MEV position. You can learn a lot on their webpage, freely available online. In contrast, ZeroMEV.org is a voice that is *against* MEV in nearly all forms. They also have good resources on their webpage to learn more.

As the market dynamics of MEV and its interaction with the overall stateful blockchain based systems evolves, more and more will be learned about MEV. One thing for certain is clear, MEV is not "all good" or "all bad," but rather an interesting emergent phenomenon in the exciting space of blockchain.

SEARCHERS, BLOCK BUILDERS, RELAYS, AND VALIDATORS

The maximal extractable value (MEV) we have described above is all too real on Ethereum today. It is alive and well, making the public mempool totally unsafe for many types of transactions. In fact, a complete industry of *private mempools* (sometimes called "dark pools") has now emerged in parallel to the protocol-level Ethereum. This development has been brought forth primarily by a group called Flashbots and their flagship product MEV-Boost. While a lot has happened in Ethereum since the original Flashbots paper, entitled "Flashboys 2.0" back in 2019, and there are other players now in MEV, they will be our primary focus as they still dominate the landscape.

In the sections below, we will review the system components of how MEV plays out on Ethereum today. While presumably other architectures for MEV could exist, and perhaps even do exist, the architecture described below is the largest player and that is where we will dedicate our attention. In this market, there are 4 important components: Searchers, Block Builders, Relays, and Validators. We will now discuss how they fit together. See **Figure 1** below for a graphical representation of how it all fits together.

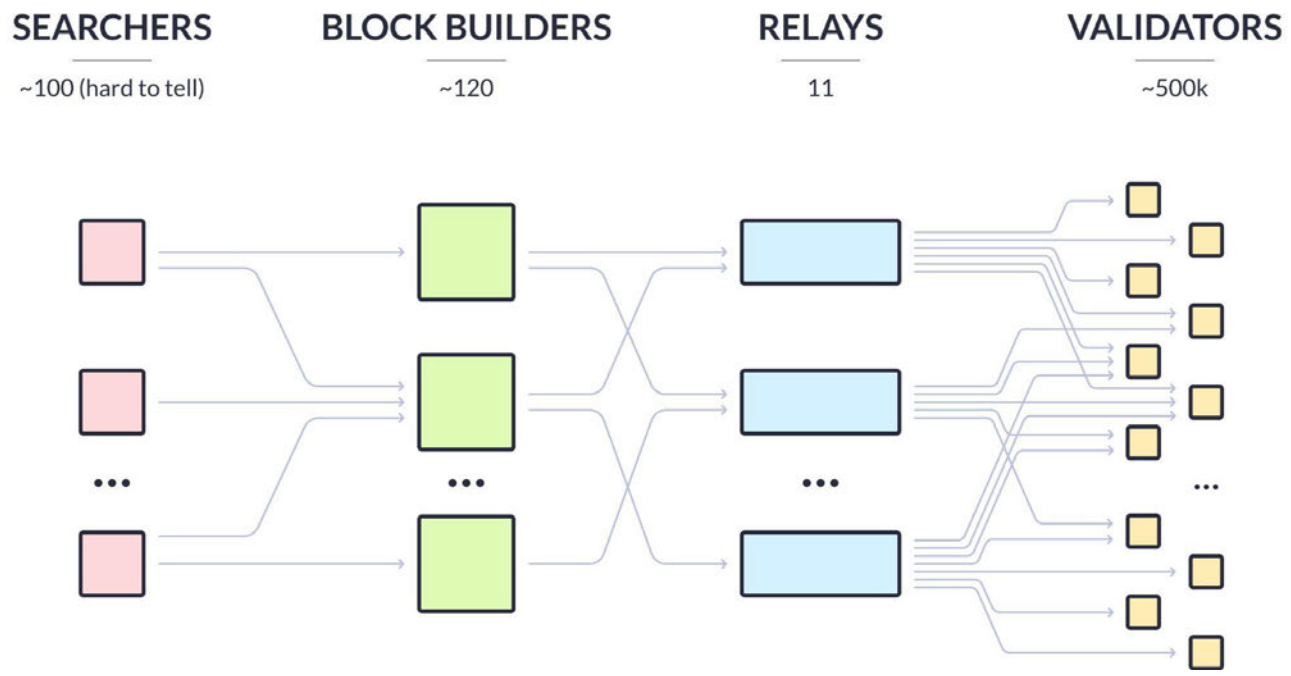


Figure 1: *The extra-protocol MEV system not in Ethereum. Note: validators can also connect directly to builders.*

Searchers

We begin the discussion with searchers, who are advanced users of Ethereum, typically taking the form of bots[5]. These bots continuously monitor the blockchain, the mempool, and several other information sources to find profitable MEV opportunities, see **Figure 2**. These opportunities may take the form of decentralized exchanged (DEX) arbitrage, frontrunning transactions in the mempool, or any one of several other known and possibly unknown MEV strategies. MEV strategy, as discussed above, is an area of intense R&D by searchers and MEV researchers alike in a race to find the most profitable opportunities.

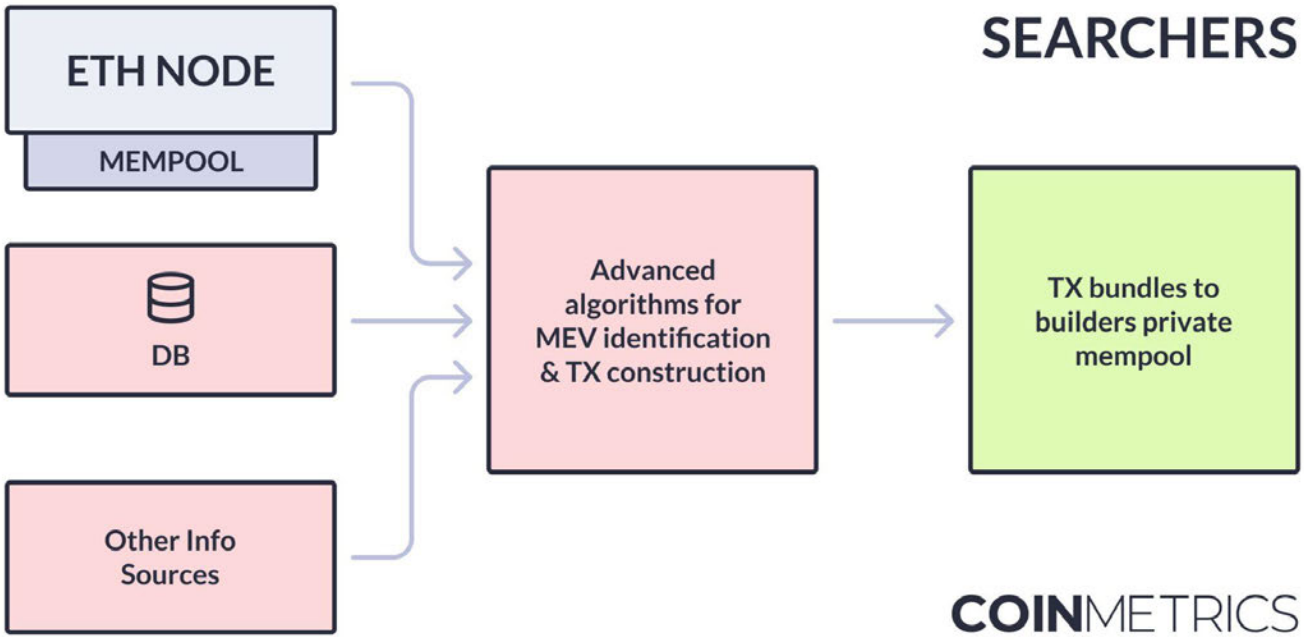


Figure 2: *Conceptual representation of Searchers within the Ethereum MEV system.*

[5] A "bot" is simply a computer program executing an algorithm 24/7/365 designed to run very fast with 100% uptime. Technically, any non-public transactions are "searchers" in Flashbot language, so they may not be a bot, but just a regular user who is aware of MEV and wants "protection" using Flashbots RPC.

Once a profitable strategy is found, the searcher then constructs one or more transactions and bundles them together in the order they would like them to be executed within a block. Notice, these bundles may have discovered transactions from the public mempool, which the searcher is utilizing beyond their own transactions—an example would be a sandwich attack.

This bundle of transactions is then delivered to a block builder for the next step. It should be noted that the searcher–block builder relationship is a trusted one, as the block builder could simply steal the searcher's transactions bundle. Searchers "pay" for their transactions either through the standard gas price mechanism or by transferring funds to the coinbase address, giving the searcher's transaction failure protection by executing a zero gas transaction. There can also be exclusive order flow agreements between searchers and block builders, with payments happening off-chain.

Block Builders

Using proprietary algorithms,[6] block builders attempt to maximize gas fees and MEV profits by arranging transactions taken from both the searchers they have relationships with, as well as the public mempool, see **Figure 3**. The "fair ordering" of transactions is a rather simple sorting of the mempool and execution of the maximum number of transactions that will fit in the block. However, fitting searcher submitted bundles of transactions can be quite complicated as payments can come in coinbase transfers and possible off-chain payments, not only gas fees. As with searching, block building is an area of intense research.

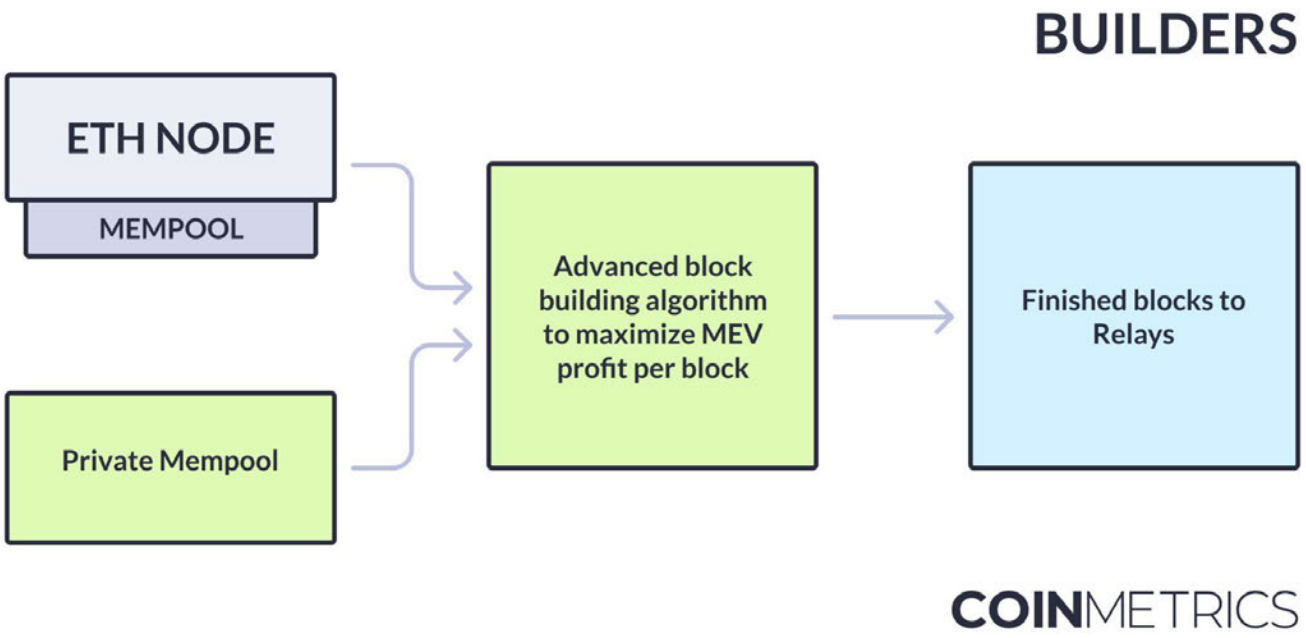


Figure 3: *Conceptual representation of a block builder in the Ethereum MEV system.*

[6] Flashbots has recently open sourced their block builder.

Once built, the builder will transfer the block payload to one or more relays. Relays can also see the block content, so this is again a trusted relationship between builder and relay. It's important to mention the requirement for timeliness in block building. After Ethereum's move to Proof-of-Stake via The Merge, there are only 12 seconds between slots, and broadcasting of the proposed block happening at 6 seconds, the builders must work quickly to ensure there is enough time before the current slot expires.

Block builders are specialized participants in the MEV system and compete with each other to get the business of searchers. They then in turn also compete with other builders to bid for the current slot by appealing to validator payments as well. This separation of concerns allows more specialization, and in theory better overall system performance—the best bundle-constructor may not be the best block-builder, and vice-versa.

Relays, Validators

Relays have trusted relationships with block builders, and semi-trusted relationships with as many validators as possible. They act as an escrow between block builders and the proposing validator for a given slot, see **Figure 4**. Thus, having more validators in their network makes a relay more likely to bid for a slot. Each relay takes completed block payloads as input, then shares the block header with the validator chosen to propose the given slot on the mainnet chain, assuming they have a relationship with said validator. Not all validators have these relationships—either because they simply didn't initialize it with a given relay or they don't participate in MEV for ethical reasons.

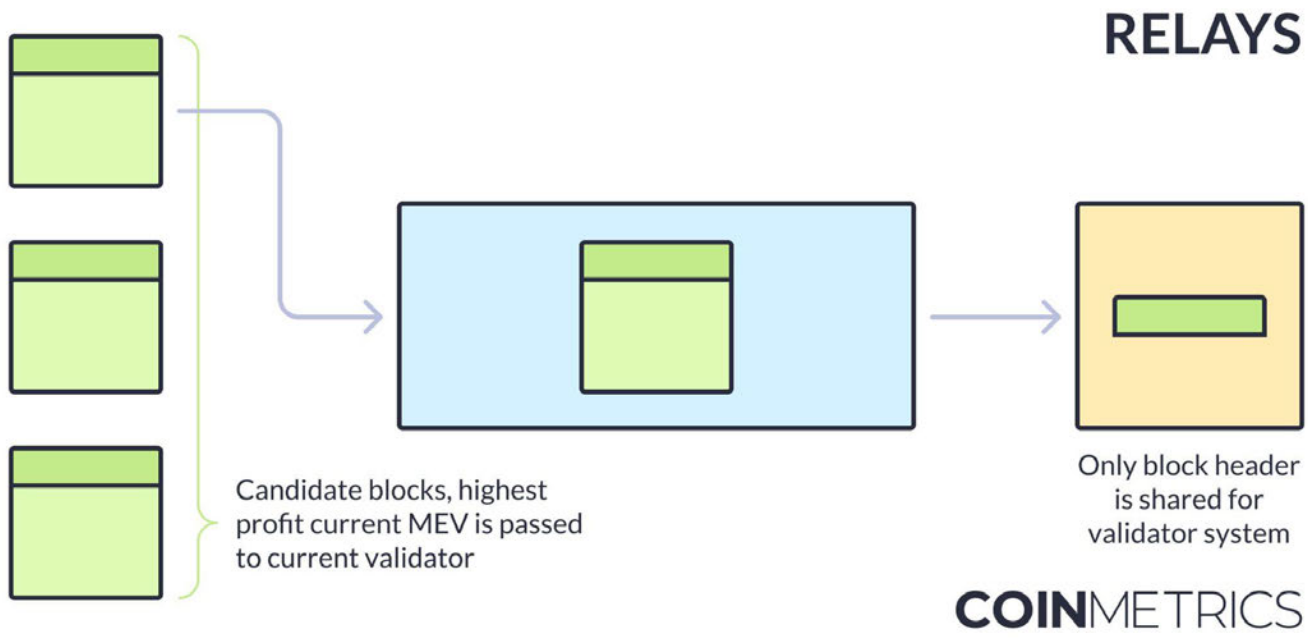


Figure 4: *Conceptual representation of a relay in the Ethereum MEV system.*

Only the header of the block is shown to the proposing validator; otherwise, the validator could steal the block transactions for themselves. Further, the proposer only validates the header once they have seen their payout amount, see **Figure 5**. Hence, proposers can communicate with multiple relays and pick only the highest paying blocks.

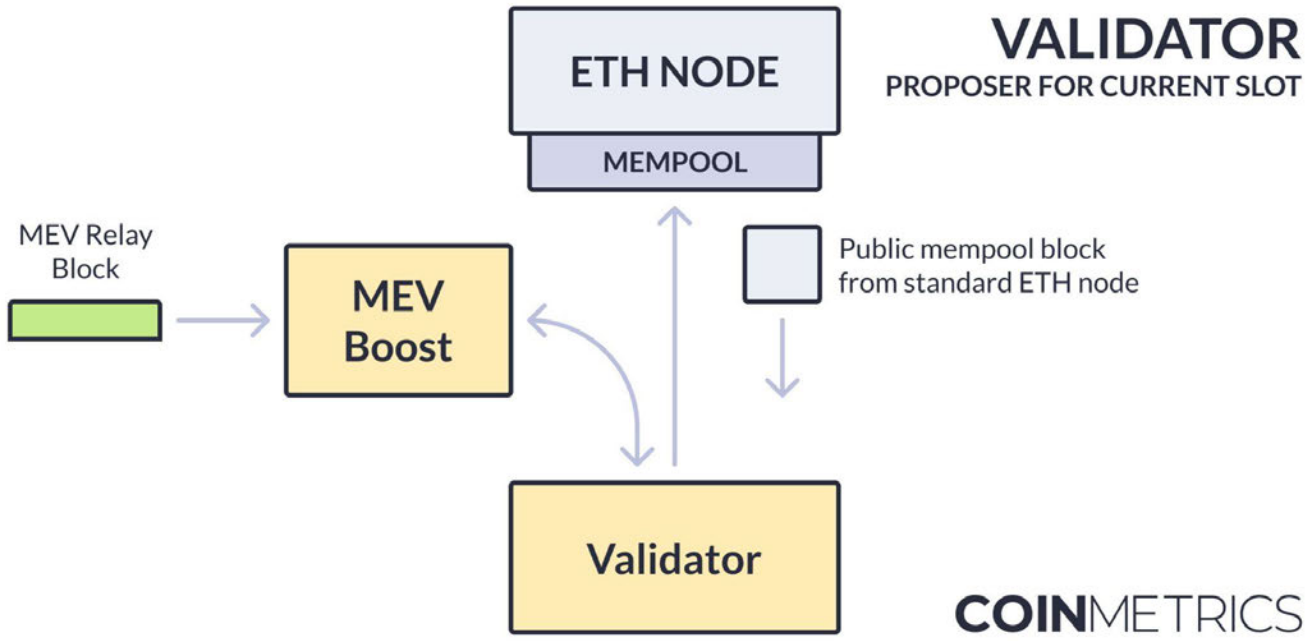


Figure 5: *Conceptual representation of a Proposer in the Ethereum MEV system.*

The proposing validators can also build their own "fair ordering" blocks, called *Vanilla* block building, from their local mempool. Thus, if no MEV opportunities exist from their relays, proposers can use their own blocks. If the proposer selects the relay-proposed block, they sign the header and send it back to the relay. With this signed header, the entire block is broadcast to the whole network by the relay on behalf of the proposer.

The trust relationship between relays and proposers is one of the key concepts of proposer-builder-seperation (PBS) and is a large part of keeping trust minimized across the network.

Today on Ethereum there are 11 known relays, with Flashbots still being the dominant force by far as of this writing, delivering more than 70% of MEV blocks since the Merge. The others include BloXroute-Ethical, BloXroute-MaxProfit, BloXroute-Regulated, Blocknative, Eden, Manifold, Relayoor, Gnosis, Aestus, and Ultrasound-Money. They all support similar API's for both block builders as well as validators, making interoperability straightforward.

QUANTIFYING MEV ON ETHEREUM

With a background in how MEV works on Ethereum outlined and explained above, we will now dive into a more quantitative characterization of how MEV is playing out on Ethereum. As blockchains never sleep and continuously grow, we'll limit our analysis from the the first block after the Merge on September 15, 2022 (block_number=15 537 394) through the end of the 2022 calendar year (UTC) on December 31, 2022 (block_number=16 309 684).

Relays and Block Production

To begin, let's look at some summary statistics of the relays and block production. How many of the blocks on the mainnet chain are coming through the MEV-Searcher-Builder-Relay-Validator pipelines? The number of blocks on the main chain in our analysis is simply: 16 309 684 - 15 537 393 = 772 291 blocks. **Table 1** shows a further breakdown of those blocks by the relays that produced them. The source of this data is a publicly available API supported by all Relays as of the time of this writing. Its specification can be found here and is where each relay "takes credit" for the blocks on the main chain they produce. Note that, while Flashbots is dominant, not all relays have been operational for the entire analysis window.

Table 1: *Breakdown of block production delivered by each relay over the analysis period.*

Relay Name	Block Count
Flashbots	403 646
BloXroute-max	75 607
Blocknative	25 176
Eden	16 327
BloXroute-ofac	13 347
BloXroute-ethical	9 555
Manifold	5 869
Gnosis	4 943
Relayooor	2 376
Ultrasound-money	1 967
Aestus	27
Non-MEV | Unknown relay	213 451
Total Blocks:	**772 291**

Putting these numbers into a pie chart, see **Figure 6**, it's clear Flashbots is the dominant force for block building. However, it must be noted the MEV landscape is ever evolving, and adding a temporal component to the analysis will prove insightful.

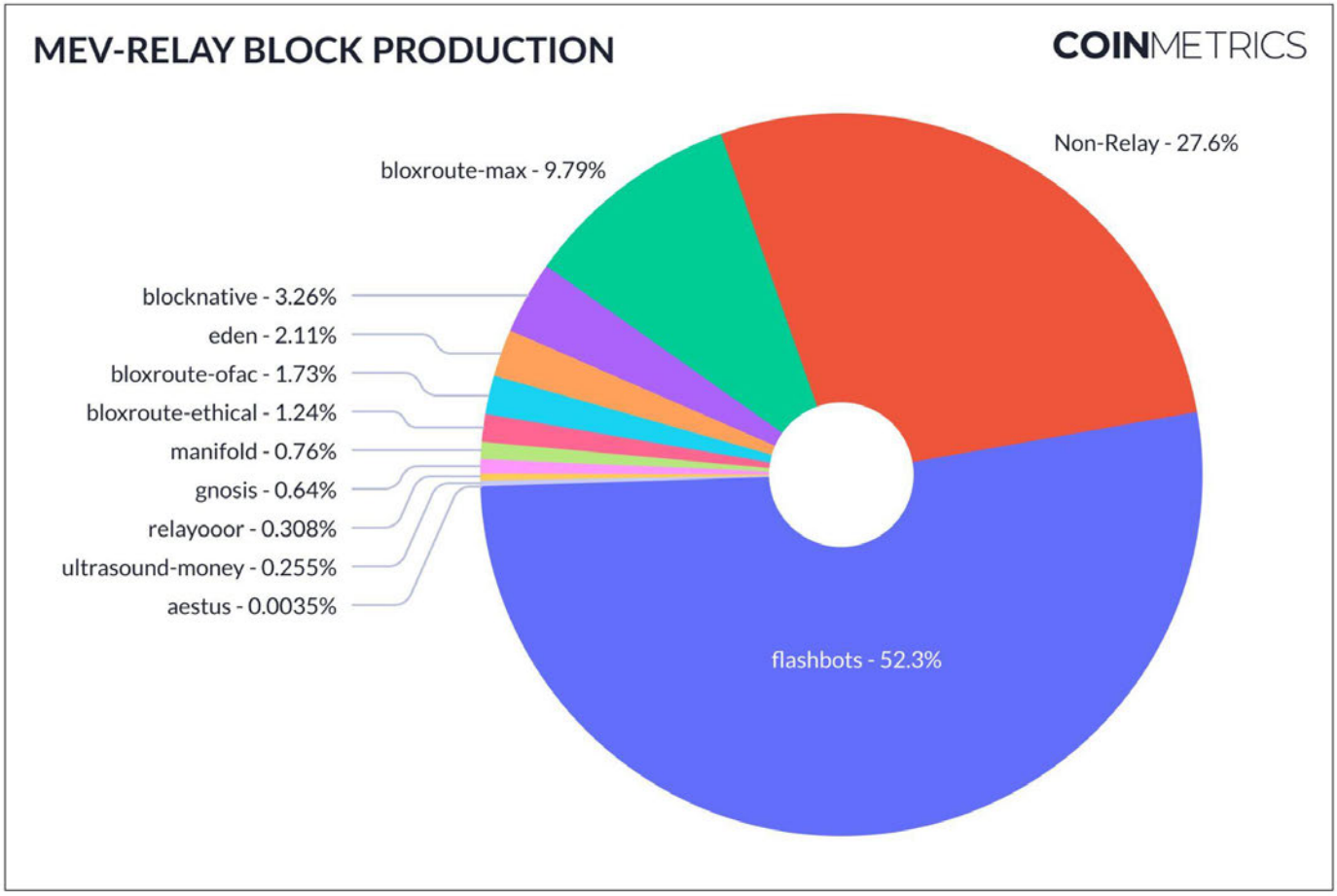


Figure 6: *Pie chart showing the total relay proportions of block construction over the analysis period, the Merge through the end of 2022.*

Inspired by [mevboost.pics](), a day-by-day aggregation of each relay's block production, as well as non-MEV blocks can be seen in **Figure 7**. Here one can see since the Merge a gradual shift from the majority of non-MEV blocks, to over 90% of all blocks being MEV Relay originating by the end of 2022.

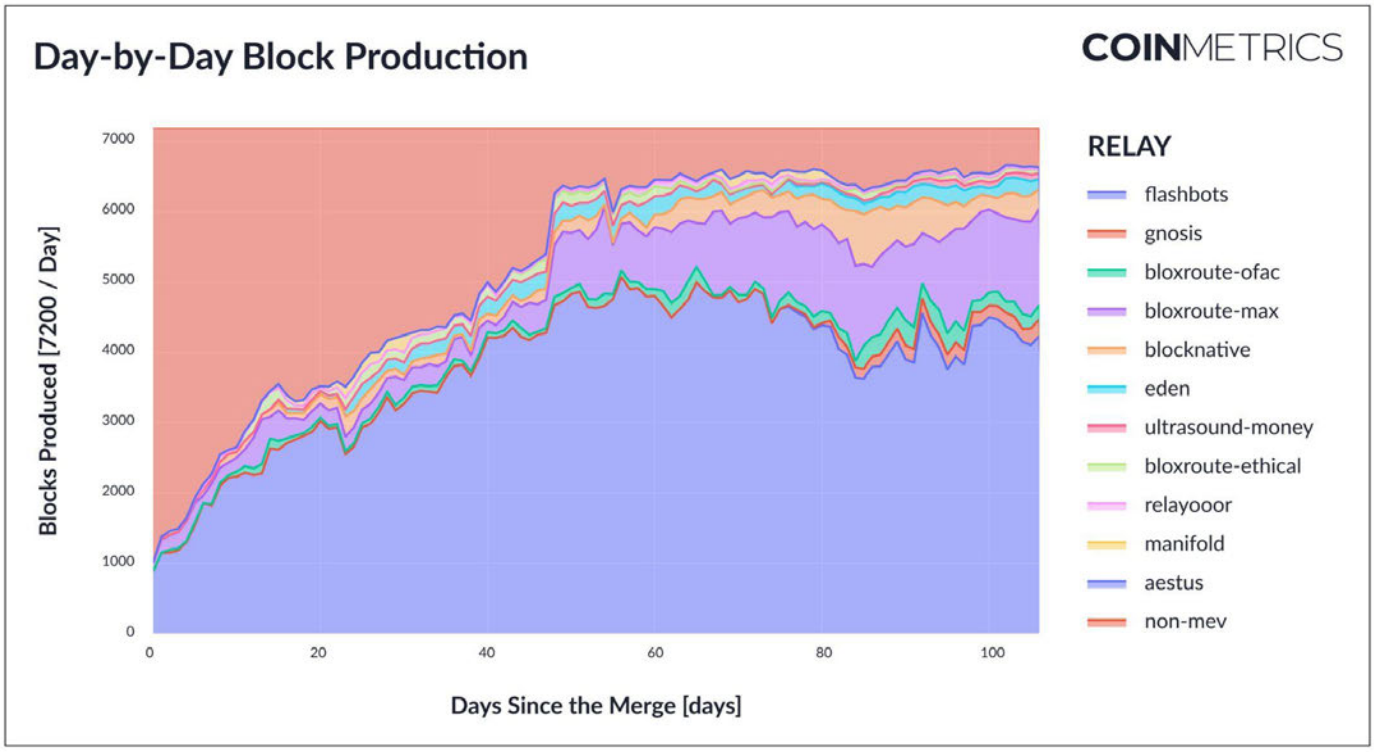


Figure 7: *Relative block production on chain from each relay, includes non-mev blocks. Technically speaking, days in this analysis are not aligned with calendar days, but used for conceptual analysis purposes only.*

While the total block counts produced by the MEV Relay system are important to consider, the more interesting statistic is the *additional value* this system brings. To explore MEV profits, **Figure 8** below presents a box plot of the daily MEV profits since The Merge. Here, we can see that for the overwhelming majority of blocks, the profits are less than 0.1 Ether (~$150, at time of writing)[7]. Further, notice how the average value per block is decreasing with each day. An apparent trend line down from day one of just under 0.1 Ether, to the end of the year with an average profit of about 0.05 Ether. This downward trend in MEV profits is an interesting observation. Perhaps this trend is reflective of the increased competition within the MEV space, the current "crypto winter," or maybe there are simply less MEV opportunities to be exploited on-chain.

[7] For computational ease, float64 data types are used to process "values." Meaning small rounding errors are present, however, these are insignificant for this analysis, on the order of a few wei.

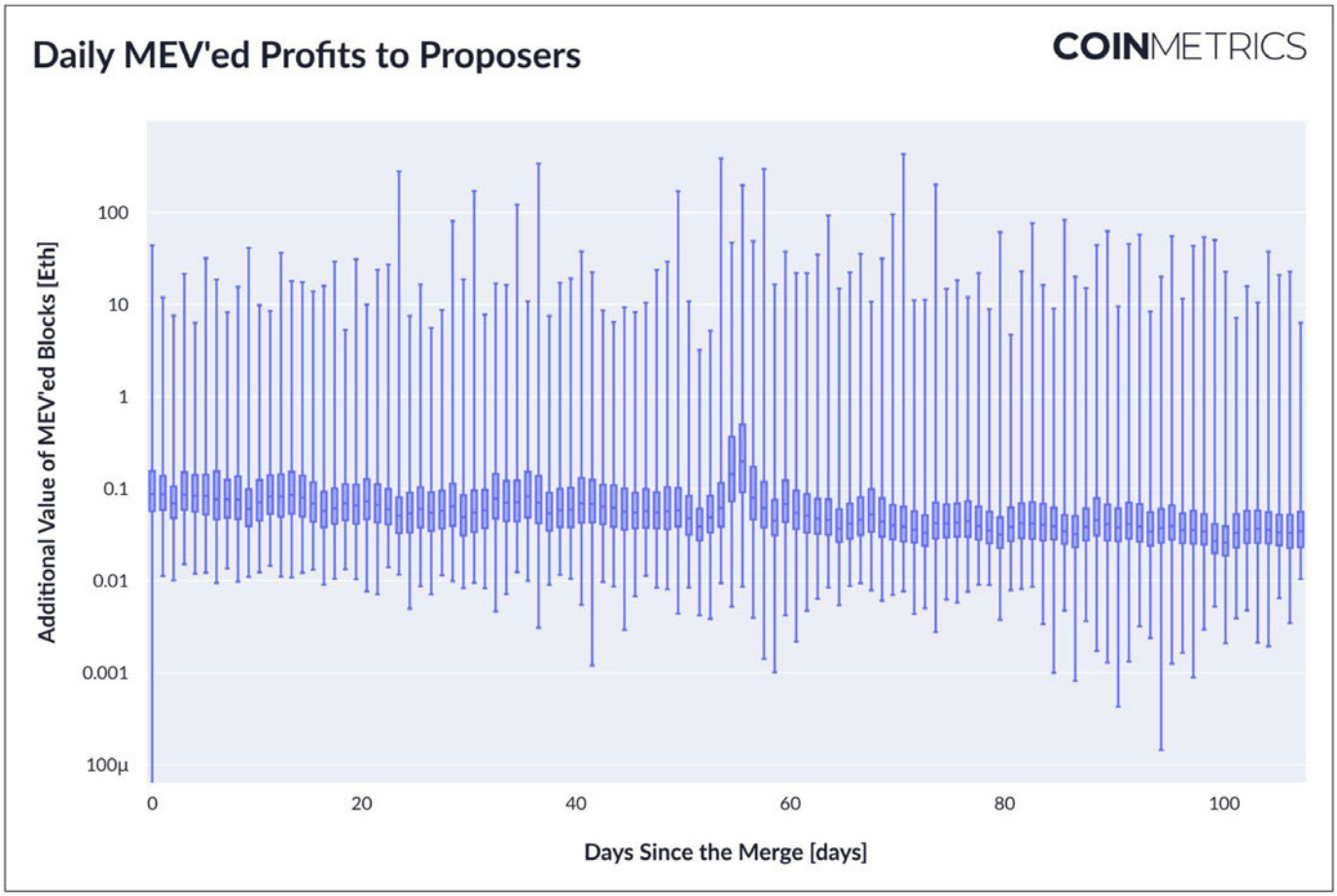


Figure 8: *Box plot of MEV profit for blocks produced per day, all MEV relays are grouped together here. Note the logarithmic vertical axes as some blocks are in fact worth hundreds of Ether, but most are worth less than 0.1 Ether.*

Regardless of the trend down in average MEV profits, it should be noted the logarithmic scale of **Figure 8** and the truly significant MEV profits some blocks command. For example, the maximum profit block since the merge is block_number=16 048 189 with nearly 430 ETH, or ~$515K USD.

Moving beyond relays we now take a look at block builders themselves and make some summary statements about their behavior.

Block Builders

To begin our look into block builders, we again present summary statistics of the various entities involved. For the block interval of analysis here, there are 121 individual block builders (as identified via the "builder_pubkey" field in the API) across all relays. It should be noted, some of these are the same organization running separate block builders (e. g. Flashbots). The block builder production resulting in on-chain blocks follows a strong power law distribution as seen in **Figure 9**, with the top 20 builders landing over 90% of the MEV blocks on chain. For those concerned about centralization risks in the Ethereum ecosystem, this is a significant fact and warrants pause and consideration.

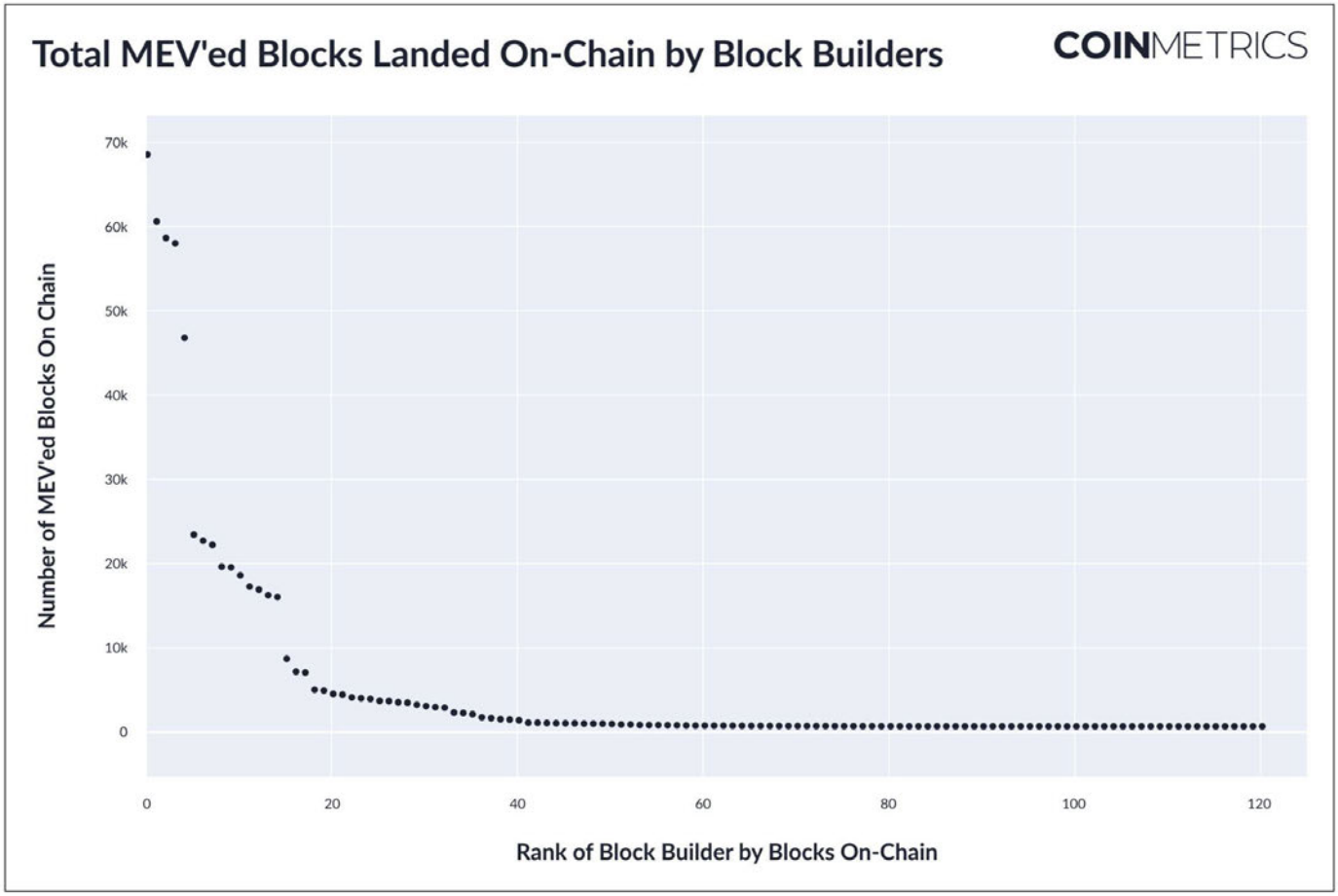


Figure 9: *Rank ordering of Block Builders by MEV'ed blocks they land on-chain.*

Further, the block profit for the top 20 builders are presented in Box Plot form in **Figure 10**. Notice, there does not appear to be an obvious trend between the number of blocks produced by a block builder and the MEV value that builder provides on average with its block. However, one should notice some block builders have much higher "maximum" profits than others as the vertical axis is again logarithmic in scale. This may have to do with the searcher's contribution, as searchers can have partnerships with multiple block builders.

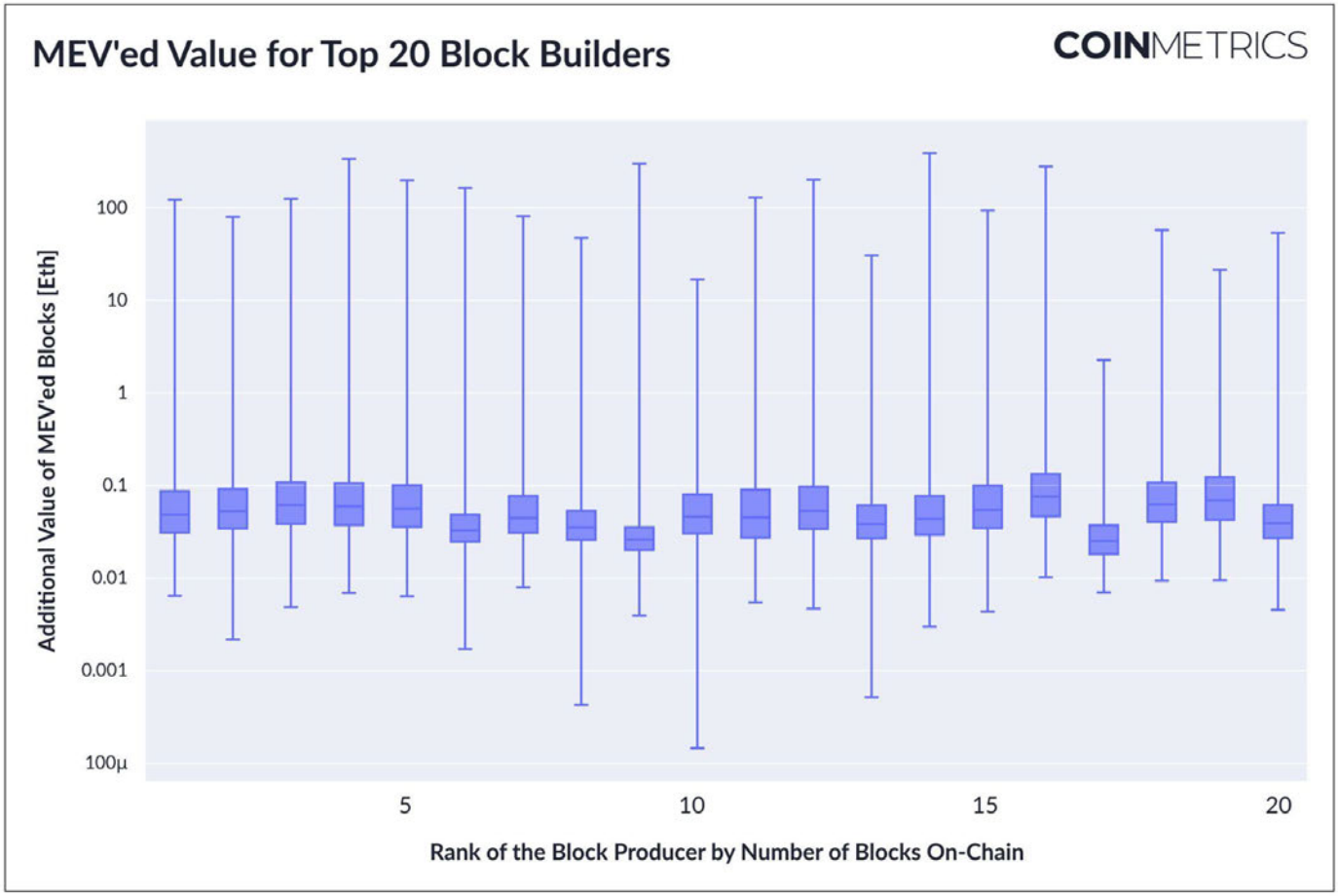


Figure 10: *Box Plots of the top 20 block builders by block count representing the MEV value their respective blocks provide.*

As such, if a group of searchers' transactions significantly drives the profits, and this group uses multiple builders, this could explain the relative indifference in profit between builders. Because the true alpha generation is coming from searchers and they can use multiple builders, adding noise to the signal of where MEV profits originate. This is purely speculation, as builders certainly also contribute value.

Specifically looking now at the single top block producer by number of blocks, we examine the

changing nature of the MEV value of their blocks with respect to time since the Merge. As can be seen in **Figure 11**, as time moves on the average value each block brings is in fact decreasing. Again, this could be the result of a more competitive MEV space, the "crypto winter," or perhaps fewer MEV opportunities available.

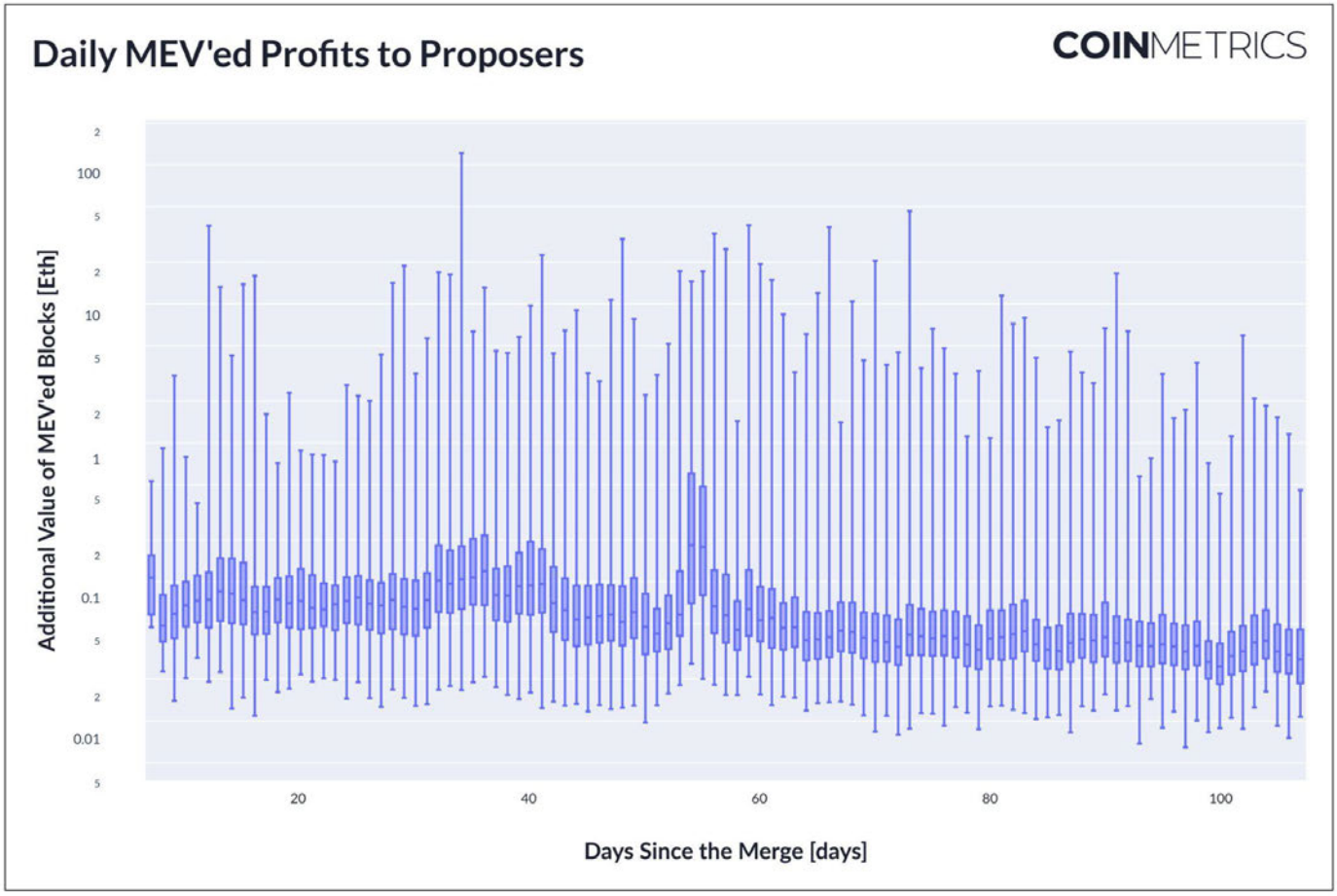


Figure 11: *A Box Plot of MEV value for the top block builder (0xb194..3027) by number of blocks landed on chain, day-by-day analysis.*

Next, let's take a look at how block builders and relays interact with each other. That is, do block builders always use the same relay? The answer to this question is no, and can be seen in **Table 2** below. Notice how the Flashbots relay is very dominant, as expected from before, however, few of the top 20 block builders use it exclusively. And this makes sense, as the builders want to spread their chances of getting into a relay with the next validator in its collection of validators. Hence, using only one relay is less advantageous than using multiple relays with overlapping validator sets.

Table 2: *Total blocks delivered by the top 20 block builders by number of blocks to each respective relay.*

builder	flashbots	bloxroute-max	blocknative	eden	bloxroute-ofac	bloxroute-ethical	manifold	gnosis	relayooor	ultrasound-money	aestus	total
0xb194..3027	66596	0	0	0	0	0	0	940	0	351	0	67887
0x96a5..fc27	25977	27749	0	0	4740	0	0	1084	0	379	0	59929
0xa1de..27fc	57528	0	0	0	0	0	0	329	0	111	0	57968
0x81ba..80f9	56789	0	0	0	0	0	0	418	0	127	0	57334
0x81be..994f	45599	0	0	0	0	0	0	388	0	126	0	46113
0x9000..8246	0	0	22759	0	0	0	0	0	0	0	0	22759
0xa1da..14e9	22031	0	0	0	0	0	0	0	0	0	0	22031
0x976e..6013	4217	17332	0	0	0	0	0	0	0	0	0	21549
0x8eb7..8ad0	16921	0	12	23	0	0	1988	0	0	0	0	18944
0x94aa..7c67	10144	8731	0	0	0	0	0	0	0	0	0	18875
0xa971..cf9d	16652	0	0	0	0	0	0	912	0	359	0	17923
0xa4fb..6772	15991	0	0	0	0	0	0	158	374	66	0	16589
0x8b8e..5fba	1998	14248	0	0	0	0	0	0	0	0	0	16246
0x80c7..d3d5	13580	0	0	0	1991	0	0	0	0	0	0	15571
0xb8fc..e899	15345	0	0	0	0	0	0	0	0	0	0	15345
0x8e39..0a8b	0	0	0	8029	0	0	0	0	0	0	0	8029
0x8ea1..a525	6227	0	0	0	0	0	172	0	0	97	0	6496
0xa5ee..bef5	0	0	0	6391	0	0	0	0	0	0	0	6391
0x8bcd..9501	3975	374	0	0	0	0	0	0	0	0	0	4349
0xaec4..c347	1070	2589	0	0	479	0	0	79	0	32	0	4249
Total	**380640**	**71023**	**22771**	**14443**	**7210**	**0**	**2160**	**4308**	**374**	**1648**	**0**	**504577**

Again, going beyond simply the number of blocks sent to each relay and considering the profits of the blocks sent though each relay is also of importance. Examining **Table 3**, this information is presented. As expected, the overall profits from MEV are dominated again by the Flashbots relay. Another interesting statistic, however, is that the most profitable block builder is not the most prolific in terms of number of blocks, as can be seen in the far right totals column.

Table 3: *Total block value in Ether sent by the top 20 block builders to each relay.*

builder	flashbots	bloxroute-max	blocknative	eden	bloxroute-ofac	bloxroute-ethical	manifold	gnosis	relayooor	ultrasound-money	aestus	total
0xb194..3027	7839.84	0	0	0	0	0	0	65.22	0	21.04	0	7926.1
0x96a5..fc27	3459.32	3583.01	0	0	652.1	0	0	92.11	0	36.91	0	7823.45
0xa1de..27fc	7693.51	0	0	0	0	0	0	21.48	0	5.8	0	7720.79
0x81ba..80f9	7894.09	0	0	0	0	0	0	31.98	0	7.92	0	7933.99
0x81be..994f	5968.11	0	0	0	0	0	0	31.5	0	9.98	0	6009.59
0x9000..8246	0	0	1890.59	0	0	0	0	0	0	0	0	1890.59
0xa1da..14e9	3502.03	0	0	0	0	0	0	0	0	0	0	3502.03
0x976e..6013	614.77	1082.5	0	0	0	0	0	0	0	0	0	1697.27
0x8eb7..8ad0	1245.57	0	2.21	4.1	0	0	77.87	0	0	0	0	1329.75
0x94aa..7c67	1105.77	736.03	0	0	0	0	0	0	0	0	0	1841.8
0xa971..cf9d	3387.37	0	0	0	0	0	0	47.81	0	18.4	0	3453.58
0xa4fb..6772	2845.67	0	0	0	0	0	0	17.97	35.5	7.88	0	2907.02
0x8b8e..5fba	102.03	1059.46	0	0	0	0	0	0	0	0	0	1161.49
0x80c7..d3d5	1810.63	0	0	0	214.37	0	0	0	0	0	0	2025
0xb8fc..e899	2484.31	0	0	0	0	0	0	0	0	0	0	2484.31
0x8e39..0a8b	0	0	0	1946.64	0	0	0	0	0	0	0	1946.64
0x8ea1..a525	228.93	0	0	0	0	0	6.24	0	0	3.45	0	238.62
0xa5ee..bef5	0	0	0	965.54	0	0	0	0	0	0	0	965.54
0x8bcd..9501	624.05	40.53	0	0	0	0	0	0	0	0	0	664.58
0xaec4..c347	148.42	284.2	0	0	45.18	0	0	12.9	0	10.53	0	501.23
Total	**50954.42**	**6785.73**	**1892.8**	**2916.28**	**911.65**	**0**	**84.11**	**320.97**	**35.5**	**121.91**	**0**	**64023.37**

Much more could be said about MEV and in fact Coin Metrics will be publishing more reports in the near future to further quantify this phenomenon. For now, this introductory report hopes to present enough data on MEV to peak the interest of the reader and to communicate that MEV is a significant trend on Ethereum and is already playing a large part in on-chain activity.

With the high level statistics quantified above, we now take a closer look at a few well known patterns of MEV and examine specific examples of MEV transaction sequences.

EXAMPLES OF MEV FROM ON-CHAIN

For blockchain based systems, all the data is stored “on-chain” and can be viewed by anyone. This is also true for many of the components within MEV on Ethereum. Below, examples will be presented of actual MEV Patterns being executed on chain.

Sandwich Attack

To examine a sandwich attack, we will take a look at Ethereum block: 16133912, which is low in absolute MEV profit, however, is typical of these attacks. Going to zeroMEV.org, we can clearly see this block was produced by the Flashbots Relay and further it consists of a complicated bundle structure of both public and private mempool transactions. This information is also available in API form from Flashbots. This additional API beyond the relay information is rich in content and worth further exploration.

Specifically, bundle 3 is the sandwich attack we will examine. It consists of three separate transactions: the frontrun (0x2ed..eb6b), the sandwich (0x50ca..4fd3), and the backrun (0x0e2c..37d0). The sandwich occurred against the UNION Protocol Governance Token (UNN) on a Uniswap V2 pool. The actual attack played out like this: first Wrapped Ether (WETH) was traded for UNN to drive up the price - the frontrun. Next, the victim traded WETH for Tether (USDT), and then traded that USDT for UNN at the higher price - the sandwich. Finally, the originally purchased UNN was traded back from WETH, however, due to the market action just described, at a higher price than it was purchased.

The sandwich attack ended up costing the user $23.86 and netting the searcher $21.61 given Ether prices on the day of the attack. This mismatch of loss-to-gain is common in sandwich attacks. While this was not particularly profitable for the searcher, it none-the-less is an example of a completely risk free profit. Seeing there is a clear winner and loser, sandwiches are often referred to as toxic MEV.

Frontrunning Pattern Example

For an example of frontrunning, we're going to look back in the chain to Ethereum block: 10281528. Here, we see the classic frontrun example presented by Scott Bigelow (@epheph) of the Ethereum Foundation. This example is chosen because the transactions are simple in nature and the contracts involved are straightforward to understand. Further, Mr. Bigelow has released a corresponding YouTube video explaining in very helpful detail what is happening.

In summary, a smart contract is deployed to mainnet containing a special withdrawal function. This withdrawal function will return 0.035 Ether to anyone who knows the "secret" key, which they will submit when calling the contract function via a transaction. Mr. Bigelow submits such a transaction and waits for his Ether. However, because that secret key is in the payload of a public mempool transaction, a front-running bot copies the secret key and submits their own transaction, executing the withdrawal function call before the rightful owner. The bot then received the 0.035 Ether and the rightful owner who knew the secret key was out of luck.

While this is a contrived example of frontrunning, it is shared here because the execution is quite simple and further the accompanying resources are very helpful to build intuition around MEV. Finally, this trivial example of 0.035 Ether goes to illustrate that the mempool is in fact a very dangerous place. No matter how small the amounts involved, public mempool transactions have the possibility of being frontrun.

CONCLUDING REMARKS

MEV is a fact of modern day blockchain technology and is not going anywhere soon. It is an exciting time as new and diversified solutions, each with pros and cons, are being experimented on in real time. A major force to keep an eye on is the recently announced Single Unifying Auction for Value Expression or SUAVE, proposed by Flashbots.

Regardless of how MEV develops in the future, it behooves any user of blockchains to familiarize themselves with this phenomena and take the corrective action needed to protect themselves. It truly is a Dark Forest out there.

ACKNOWLEDGMENTS

A special thank you to Toni Wahrstätter (@nero_eth) of Vienna University of Economics and Business for his careful review and helpful comments.

WHAT IS MEV ANYWAY?

AN INTRODUCTION TO THE EXISTENTIAL THREAT FACING ALL BLOCKCHAINS

By Alex R. Mead Ph.D.

COINMETRICS

To view more from Coin Metrics Research go to coinmetrics.io/pubs or subscribe to State of the Network