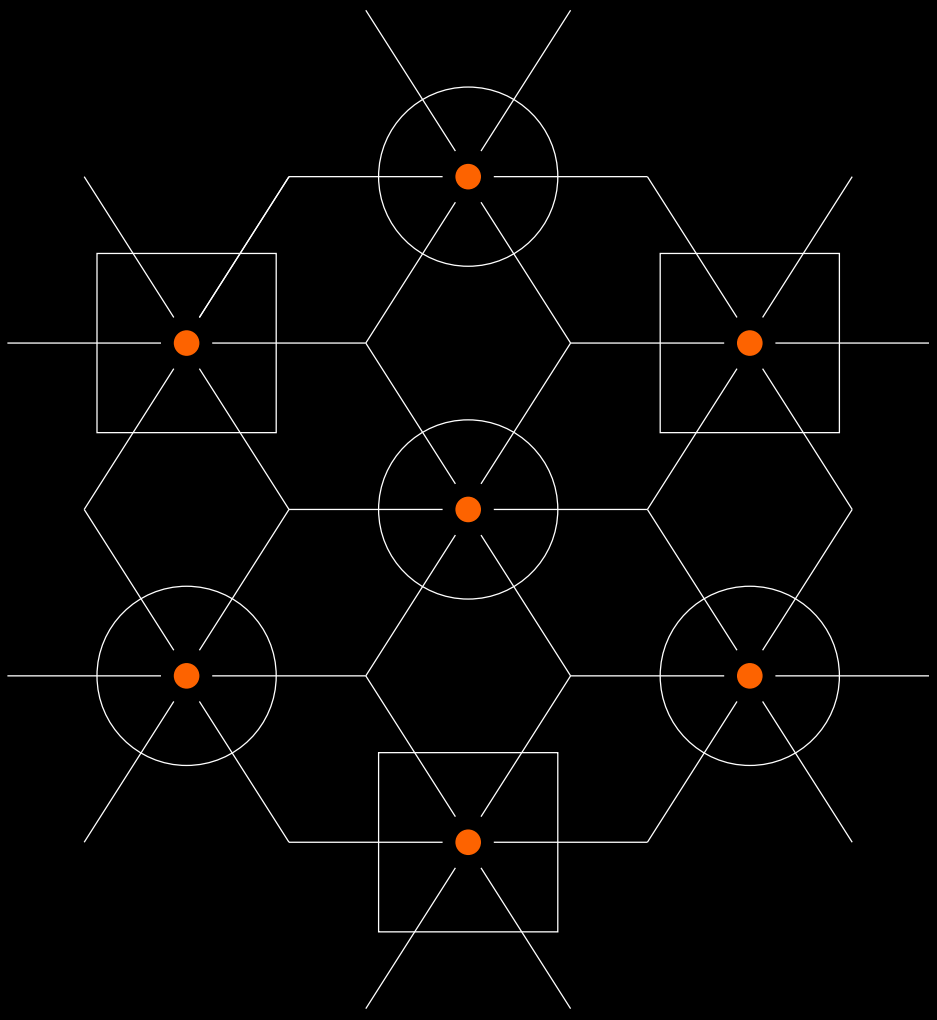
galaxy

Galaxy Digital Research

MEV: How Flashboys Became Flashbots

JANUARY 6, 2022



Author & Acknowledgements

Christine Kim
Galaxy Digital Research
email: christine.kim@galaxydigital.io
twitter: @christine_dkim

We would like to thank the following people for their support in researching and publishing this report: Alex Thorn, Francesca Don Angelo, Robert Bogucki, and Kelly Greer.

Special thanks to Robert Miller from Flashbots for his help in researching this report.

This report is a product of Galaxy Digital Research, a research organization within Galaxy Digital, the leading provider of financial services in the digital assets, cryptocurrency, and blockchain technology sector. Galaxy Digital Research provides top-tier market commentary, thematic views, tactical insights, and deep protocol research.

This report was written between November 1, 2021 and January 6, 2021.

View our publicly available research at www.galaxydigital.io/research. Contact us at research@galaxydigital.io.

Contents

Key Takeaways

- Miner or maximal extractable value (MEV) is the value extracted by miners or validators by utilizing their ability to order transactions within a block.
- MEV has grown more lucrative on Ethereum due to the rise of Decentralized Finance (DeFi) applications and become easier to earn due to the creation of Flashbots Auction, a dedicated marketplace for finding the most lucrative MEV opportunities.
- The three main types of MEV on Ethereum are arbitrage, liquidations, and sandwiching.
- There are three prongs to combatting the negative externalities of MEV. They include updates to Ethereum's consensus protocol, changes to decentralized application design, and education about MEV strategies executed on-chain.
- Miners and operators earned $730m in profit from MEV on Ethereum in 2021.
- At current rates, Ethereum miners alone are expected to earn more than $750m annually from MEV.

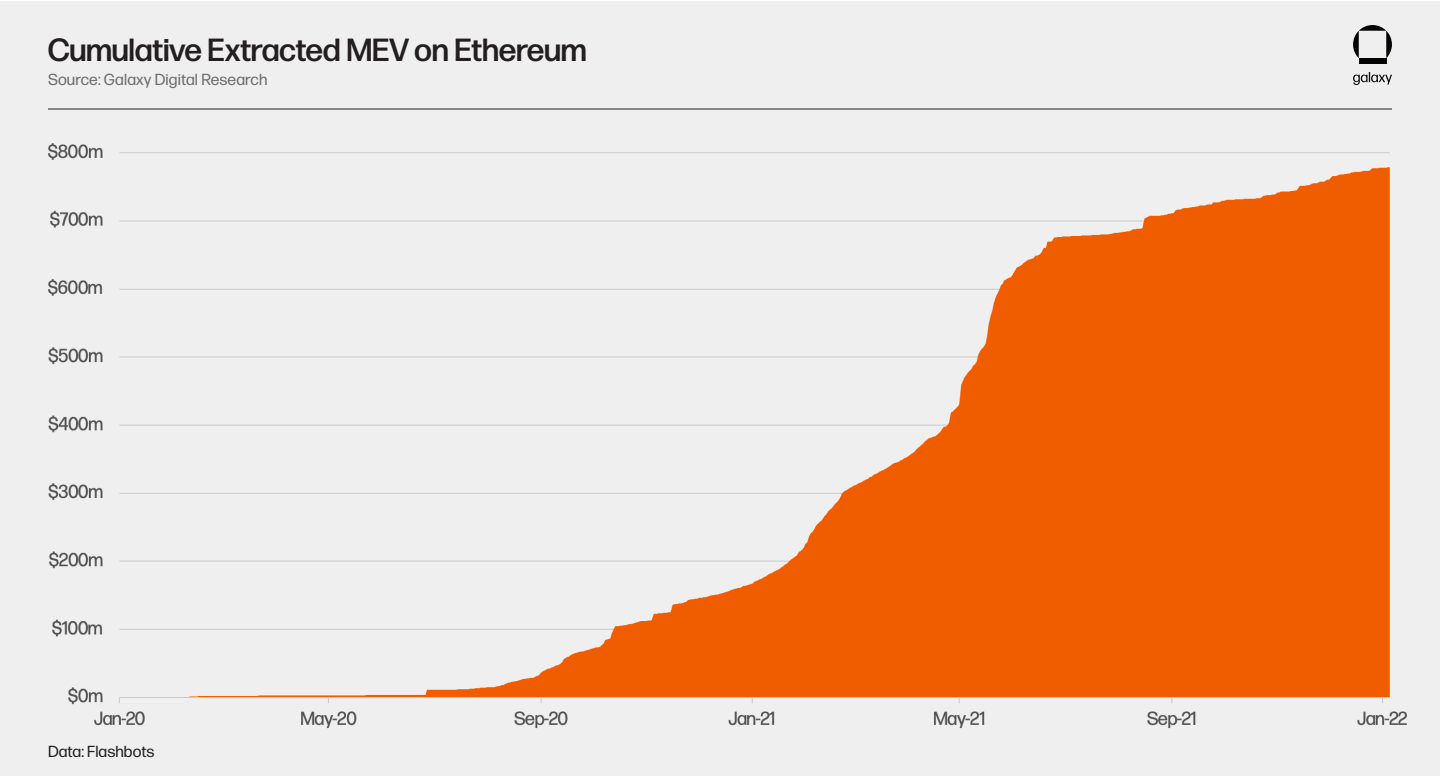
Introduction

The new era of finance is being built on Ethereum and despite all the ways in which Decentralized Finance (DeFi) differs from that of the traditional markets, the two industries struggle with the same persistent issue: frontrunning. This is the story of how the Flashboys of tomorrow, called Flashbots, are changing the game of frontrunning on Ethereum.

In traditional finance, frontrunning typically refers to trading a security based on publicly unavailable and material information about future purchases or sales of that security. While clear in writing, the extent to which frontrunning exists in practice in the markets today is highly disputed. For example, the infamous founder of the Investors Exchange (IEX), Brad Katsuyama, and the author of the book "Flashboys," Michael Lewis, are largely credited to have brought the practices of high-frequency traders into the public consciousness. High-frequency traders execute trades based off knowledge they know milliseconds before the rest of the market.

On Ethereum, similar types of behavior to arbitrage, run stops, and advantageous trading at high frequency are beginning to take root in the DeFi markets. As the transaction volumes of DeFi applications has grown, the value of trading more quickly than others has also increased. This new breed of high frequency trading allows savvy and technologically advanced participants in DeFi to arbitrage across decentralized exchanges (DEXs) and forcefully liquidate or draw down positions directly after a large swing in asset prices on trading and lending platforms, resulting in tidy profits. This new form of profit-taking is known as miner or maximal extractable value (MEV). **Between January 1, 2020 and December 31, 2021, more than $773m has been earned through MEV on Ethereum.**

Motivations for MEV are not unlike the opportunities that exist in traditional finance because certain players have privileged access to submitting and reordering trades in the markets. However, where these opportunities in traditional finance usually contribute to higher barriers to entry for market participants, MEV on Ethereum can contribute to greater levels of market participation, transparency, and efficiency. At its best, MEV helps make the DeFi markets more efficient by creating financial incentives to rectify price inconsistencies. At its worst, MEV can work to disrupt network consensus to the detriment of user trust in the Ethereum protocol and subject user trades to unforeseen slippage or attack.



To illuminate and democratize access to MEV, organizations such as Flashbots and the Ethereum Foundation are building tools to ensure the incentives for earning MEV are aligned with creating fair and open financial markets. Flashbots estimates that miners will earn more than $750 million in additional profit annually from MEV at current rates, the majority of which through pure arbitrage. The following chart illustrates how MEV ebbs and flows with DeFi activity.

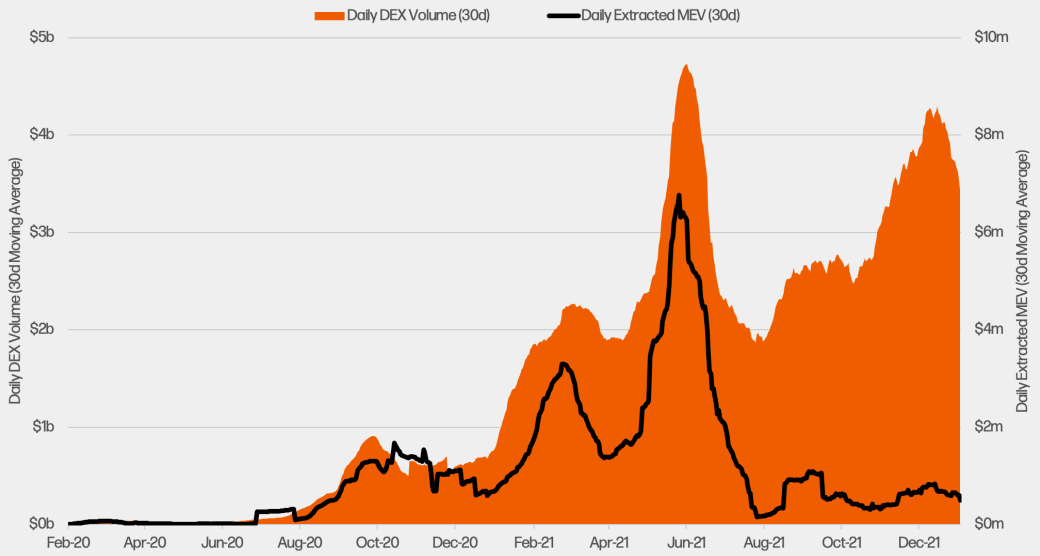
On a technical level, MEV is earned primarily by miners through their ability to reorder transactions within blocks and represents a third form of miner revenue beyond the block subsidy (new issuance) and transaction fees they earn in the normal course of mining. The ability to reorder transactions will be transferred from miners to validators once Ethereum retires its Proof-of-Work consensus protocol in favor of Proof-of-Stake, a change currently expected sometime in 2022.

Though MEV has been criticized as the pinnacle of rent-seeking behavior, deeper analysis reveals the issue is not so clear cut. Apart from some types of MEV being beneficial to market price discovery, MEV is also an inevitable byproduct of the safeguards that enable Ethereum to be permissionless and Turing-complete (able to execute code of boundless complexity). Much like how certain forms of frontrunning and information asymmetry persist in traditional finance, we argue MEV will continue to persist and evolve on Ethereum, as well as other smart contract blockchains. Therefore, the key to solving MEV is not about trying to eliminate all forms of this type of profit-making but rather to make space for these opportunities to flourish under transparent standards and norms.

Rather than being a force of good or evil, MEV is an unavoidable consequence of what Ethereum is designed to do. Attempts to mitigate MEV, much like regulation in the traditional financial markets, must be implemented with careful consideration of tradeoffs and possible third-order consequences that encourage dark market activity and private transactions pools.

Daily DEX Volume & Extracted MEV

Source: Galaxy Digital Research



Data: Dune Analytics, Flashbots

Note: A significant drop in MEV is seen from May 2021 onwards due to the release of Uniswap V3 and the migration of DEX activity from Uniswap V2 to V3. While data provider Flashbots does track MEV activity on Uniswap V2 and seven other DeFi protocols, it has yet to include activity from Uniswap V3, which is the top DEX by 24-hour trade volume.

Why MEV Exists and Will Persist

At is core, the ability of miners to express preference over transactions is needed to protect permissionless blockchains against spam transactions and denial of service attacks.

Rather than relying on the altruism of miners or centralized gatekeepers, many blockchains rely on self-interested actors motivated by transaction fees to filter out and avoid confirming junk transactions. Fees make it cost-prohibitive for a potential attacker to congest permissionless networks by overwhelming them with large volumes of transactions. Blockchains that haven't required transactors to attach fees, such as EOS, have found their chains filled with junk.

As such, the same incentives that enable public blockchains like Bitcoin and Ethereum to be permissionless also creates MEV. This is because the rationale that causes miners to express preference for transactions with higher fees over the ones with lower or nonexistent fees also drives them to exploit other opportunities that can potentially make them a higher profit. Other opportunities for lucrative payouts, which will be discussed in detail later in this report, are strong motivations compelling miners at times to ignore fee logic.

It is imperative that all opportunities for miner rewards on any public blockchain, be it through MEV, fees or block subsidies, are equally distributed. If a single miner has a clear advantage for earning rewards, there is the potential for that miner to become the dominant block producer of the network by capturing more revenue from their operations than others. Without democratizing opportunities to extract MEV, this type of profit-taking can end up becoming an economically centralizing force for wealth distribution and accumulation.

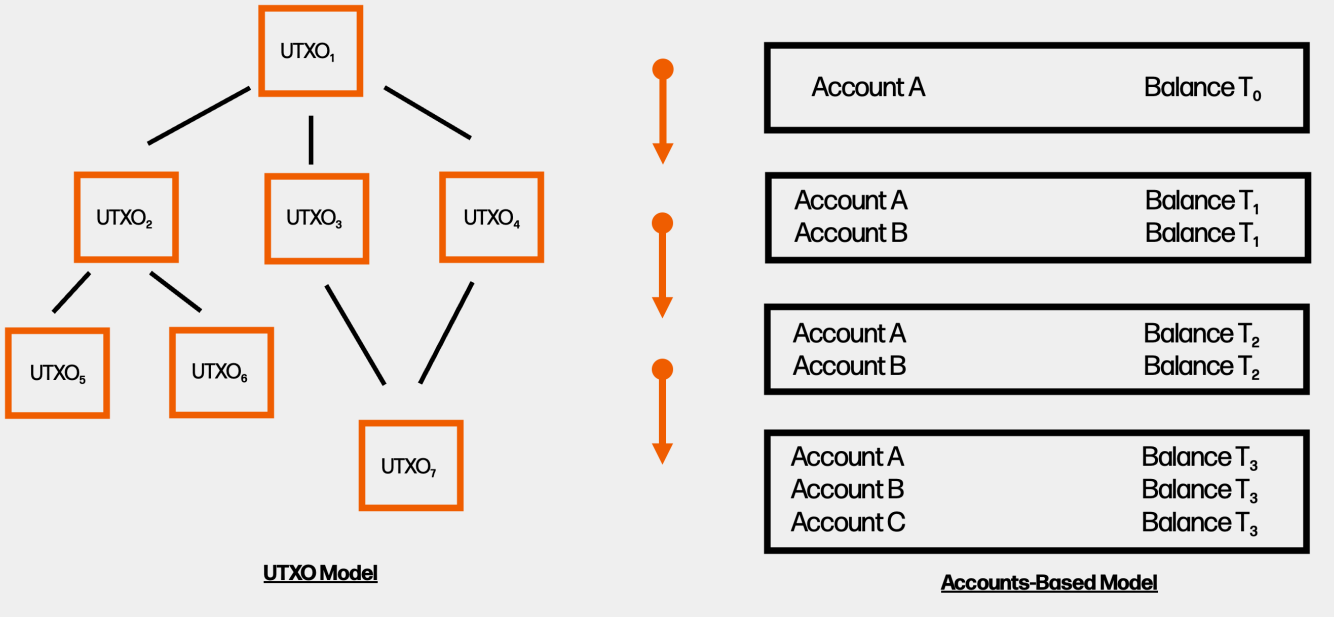
While MEV can exist on any public blockchain that relies on the self-interest of miners to gatekeep pending transactions, it is especially prolific on Ethereum due to its account-based model and transaction execution schema.

Accounts vs. UTXOs

Ethereum keeps track of the balances of users accounts in a comparable way to a traditional bank. There is a single balance that is credited and debited with every transaction. Other blockchains, most notably Bitcoin, operate using an unspent transaction output (UTXO) model which works in a similar manner to holdings paper bills. Every transaction creates "change" in the form of new UTXOs that a user holds in a Bitcoin address.

UTXO Vs. Account-Based Model

Source: Galaxy Digital Research



Compared to the UTXO model, an accounts-based model like Ethereum makes executing MEV transaction bundles easier for three main reasons:

- Transactions are sequential, meaning that changes to the balance of an account can only happen in the order transactions are included in a block. This is ideal for searchers who need to execute their transactions directly following or preceding another transaction. On Bitcoin, depending on the number of UTXOs held by an address, multiple transactions can be executed in parallel, which would theoretically make it harder for searchers to coordinate the execution of their transaction bundles.
- Complex transactions, meaning transactions that wait for an event to occur on-chain then redirects funds to another account or perhaps multiple after that, can be more easily coded due to the intuitive logic of an accounts-based model. Executing MEV opportunities by spending UTXOs before or after other transactions creates computational overhead because it requires tracking the balance of multiple new UTXOs as opposed to a single account balance. This is also one of the main reasons for why Ethereum has a sprawling DeFi ecosystem and Bitcoin does not. Ethereum's account model is designed to encourage the creation of decentralized applications and smart contracts while Bitcoin's UTXO model focusses strictly on facilitating peer-to-peer payments.
- Identifying patterns in spending behavior through transaction history is also easier with accounts than UTXOs. On Bitcoin, since new UTXOs are created each time a transaction is finalized on-chain, the norm is to generate a new address for every transfer of value. Indeed, most wallet software performs this service automatically for all users. Not until multiple UTXOs are spent in the same transaction can an observer assume that they belong to the same user, a heuristic upon which blockchain forensics companies rely to de-anonymize Bitcoin users. Even then, though, an observer cannot be certain that UTXOs belong to the same user, particularly with the emergence of privacy tactics like CoinJoin. On Ethereum, the account-based model encourages users to continue using the same account for consecutive transactions, which makes identifying patterns in spending for MEV easier.

For these reasons, it is easier from a design-perspective for miners to take advantage of MEV opportunities on Ethereum than Bitcoin. And while other chains that use an account-based model are also susceptible to MEV, we focus on Ethereum in this report because other smart contract blockchains such as Avalanche, Binance Smart Chain (BSC) or Solana have less DeFi activity than Ethereum today (and therefore fewer MEV opportunities). Attracting close to 70% of total value locked in DeFi, the issue of MEV is especially prolific on the world's first smart contract blockchain. In addition, data on MEV is comparably more transparent and accessible on Ethereum than on other blockchains such as Avalanche and BSC.

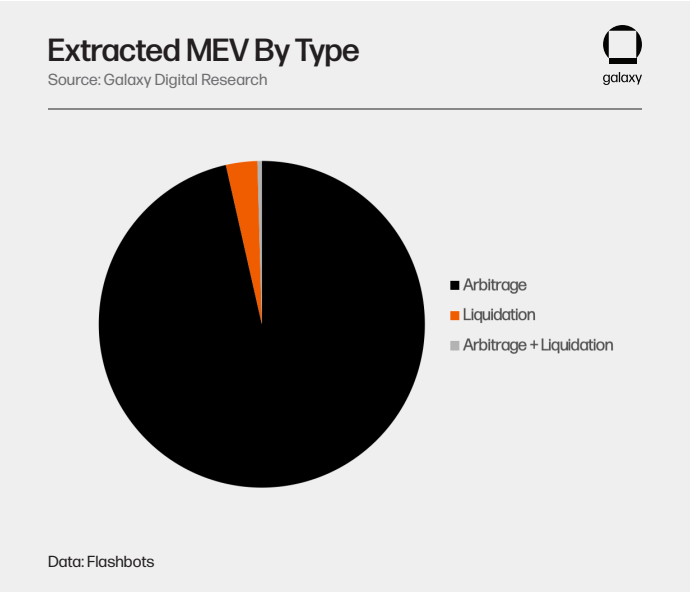
That said, even the users on more nascent blockchains than Ethereum are beginning to experience first-hand the negative fallout from MEV. In December 2021, BSC user "NullQubit" posted an issue on GitHub highlighting an example of transaction frontrunning behavior by validator MathWallet. (As background, a validator on BSC is the equivalent of a miner, meaning they are the ones to produce blocks.) Speaking to the issue, NullQubit wrote, "I don't believe that it's healthy for the network if validators do such things for profit. Validators are held to high standards and are supposed to be trustworthy."

In response, a software development team for BSC known as NodeReal responded assuring users that they were actively looking at MEV solutions. One of the solutions highlighted in their response was Direct Route, which is a private trading channel supporting private communication between traders and validators. Other chains, such as Avalanche have already implemented protocol-level solutions to varying degree of effectiveness. On Avalanche, the protocol restricts visibility into the pending pool of transactions, also called the mempool, to only validators that have staked 2,000 AVAX, which is roughly equivalent to $200,000. The motivation for doing this is to reduce the number of participants able to profit from MEV.

While reducing participation in MEV is desirable, there are negative consequences to only allowing validators to see the mempool. As the sole participants in the network able to take advantage of arbitrage opportunities, the public does not have visibility into how their transactions are processed on-chain. Validators that are frontrunning user transactions also have a financial incentive to keep their visibility into the mempool private rather than openly sharing this information. Second, the competition for MEV is limited to only the 1,000 or so active validators on the Avalanche network. Instead of anyone being able to participate and democratize the earnings from MEV, there is greater risk of MEV profit becoming centralized to only a few highly skilled and specialized validators.

In these ways, MEV persists to varying degrees of prevalence on all public blockchains, with each approaching the issue through different solutions. As interoperability protocols between chains becomes more advanced, research into cross-chain MEV strategies will become an increasingly important area of focus in the crypto industry.

Types of MEV on Ethereum



As a natural byproduct of the characteristics that make Ethereum well-suited for decentralized application (dapp) development, MEV can be exploited in a myriad of ways, not all of which negatively impact the network or end-users. The following are four common types of MEV seen on Ethereum as of December 2021. It is likely that, as the DeFi ecosystem and network evolves, these strategies for exploiting MEV will change in accordance with new innovations reinventing value-add and transaction flow in DeFi apps.

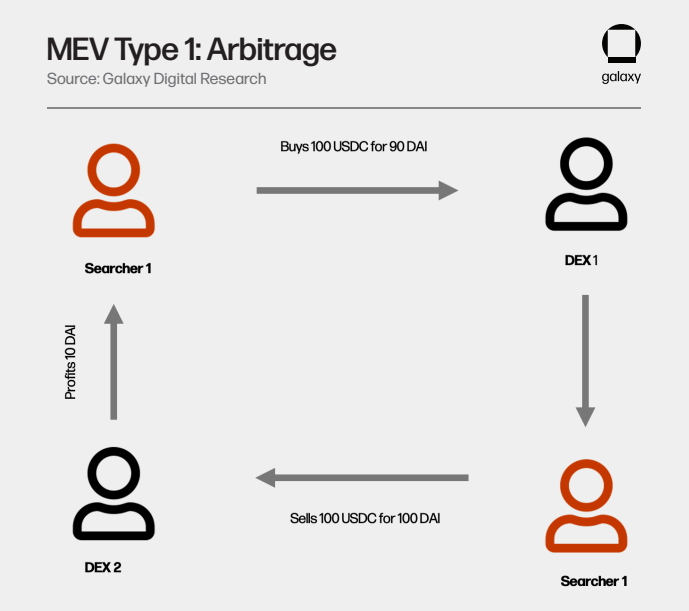
Arbitrage

The most common strategy for exploiting MEV on Ethereum is arbitrage trading.

When there is a price discrepancy for a listed asset on a DEX, miners can profit from bundling together two transactions: one to purchase the asset from the exchange with a lower price listing and a second to sell the asset on the exchange with a higher price listing. It is imperative that these two transactions occur immediately, before any other transactions occur that might change the underlying prices on the two exchanges. It is also imperative that the two transactions happen back-to-back to prevent any other transactions from changing the asset prices in the middle of the two-step trade.

Extracting profit from price discrepancies is only possible due to the inefficiencies of the DeFi ecosystem, which over time should begin to lessen as more participants and value start to flow into and out of these applications. This type of MEV ultimately has a positive impact on average users because it improves price discovery in DeFi markets. Tightening spreads between venues is beneficial for traders of all types.

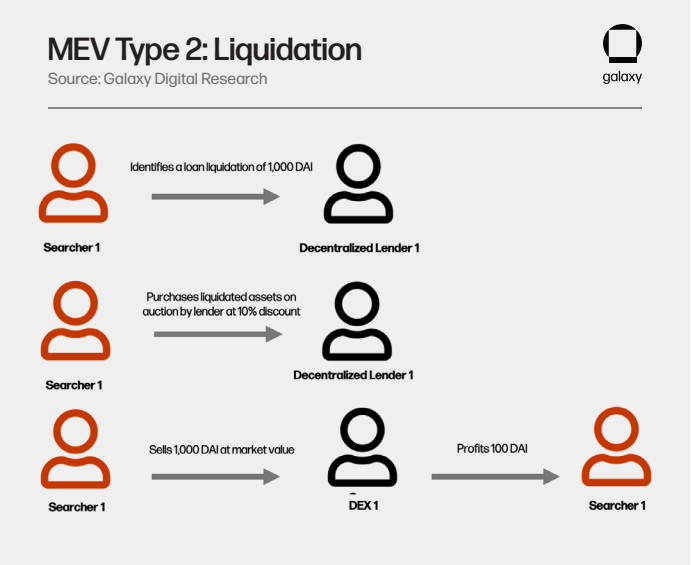
The following is a flow chart illustrating an example of an arbitrage opportunity. Specialized bots called "searchers" engineered to detect information asymmetries across various DeFi apps typically identify MEV opportunities first. Searchers work closely with miners to relay lucrative transaction bundles and have them executed in precise order on-chain. More details on searchers will be discussed in the next section of this report.



Liquidation

Another common strategy for earning MEV is liquidation. Decentralized lending applications generally have a minimum required collateral balance for all outstanding loans. Should the value of collateral for a loan drop below the minimum, the application will automatically sell locked collateral (and usually at a discount) to prevent the overall system from becoming insolvent.

Certain searchers specialized in tracking the collateral balance of large outstanding loans, waiting to buy an asset for a discounted price to resell it again at a higher price. This is akin to *stop running* in traditional finance which involves floor traders watching for visible highs and lows in the market to take advantage of stop loss orders designed to limit an investor's loss on their positions.



Like arbitrage, liquidation is seen as a net positive activity to the DeFi ecosystem of Ethereum. These bots are reliable buyers of defaulted loans that will quickly resell the assets at market value, which helps ensure that liquidity continues to move between applications and that prices of assets normalize across the ecosystem more quickly.

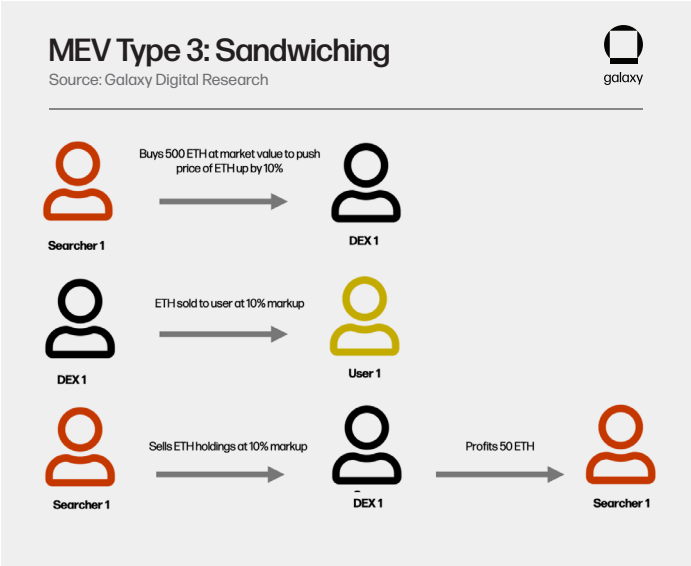
Sandwiching

Beyond arbitrage and liquidations, searchers can identify large purchases of a crypto asset and front run the purchase by buying up the asset before the trade is finalized on-chain. By purchasing the asset first, a searcher drives up the price of the asset for the original buyer and ensures that the execution of the buyer's trade is made at a slightly higher price than the one bid on.

With the sale complete, the searcher then sells the assets they have bought following the original buyer's purchase, returning the price of the asset back to normal but pocketing the difference between the asset's original price and artificially inflated one. As one of the most harmful types of MEV, sandwiching attacks have been executed more than 480,000 times and profited miners at least $190 million at the expense of users over the last 12 months.

Sandwiching creates artificial trade volume on DEXs for the sole purpose of tricking users into paying higher prices for their asset purchases. It is not unlike how high-frequency trading (HFT) works in traditional finance where high frequency traders front-run trades on exchanges by using colocation and advanced hardware. Supporters of HFT argue that the practice presents a positive outcome for traders by reducing price slippage that would otherwise be larger for retail traders without their involvement.

However, the same benefit cannot be said about sandwiching on Ethereum. The price slippage experienced by any DEX trader because of sandwiching is always greater due to MEV than without MEV. This is because searcher bots do not make miners any faster at executing trades on DEXs. Rather, searchers make miners more revenue by bribing them to delay specific trades so that they front run and back run those trades. Sandwiching is a net negative for end users that reduces the time a trade would have otherwise been executed and temporarily inflates the bid price at which an asset is purchased on a DEX.



Other

Poisoned Sandwiching

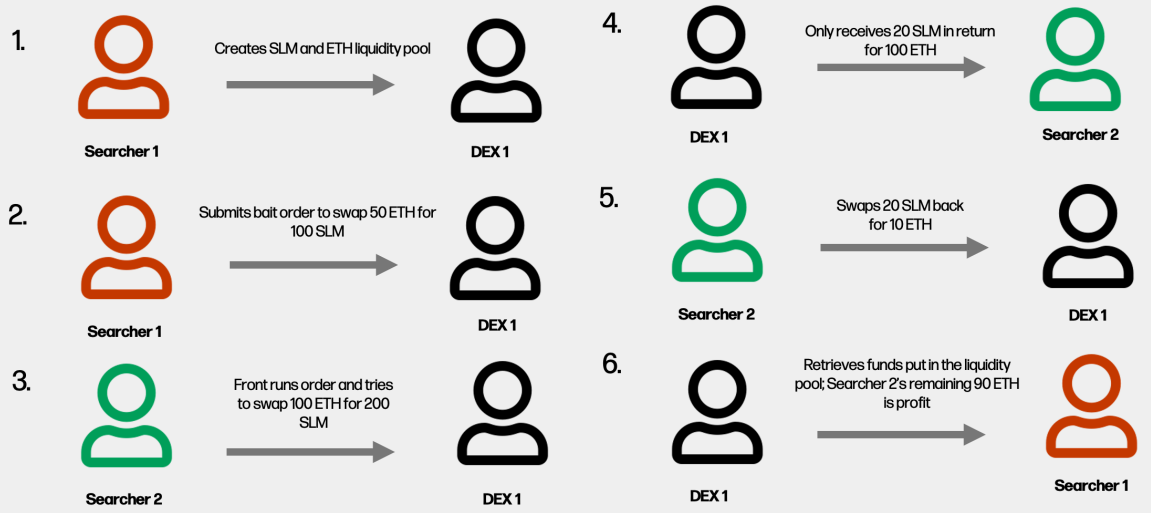
Several other types of MEV exist on Ethereum that build upon the basic premises of arbitrage, liquidation, and sandwiching. For example, "poisoned" sandwiching strategies take advantage of baiting searchers with large DEX trades only to precondition payout of any tokens bought to be 10% of the specified amount. To demonstrate this attack, known MEV searcher and LocalCoin Swap CTO Nathan Worsley created two ERC-20 tokens called "Salmonella" and "Listeria." Worsley pretended to make a large trade for these two tokens on Uniswap, which other searchers immediately bought up to artificially raise the price of the Salmonella and Listeria assets in a sandwiching attack.

Instead of receiving the full amount of Salmonella and Listeria tokens bought, the searchers only received 10% by the nature of Worsley's smart contract programming. As a result, these searchers were unable to sell their holdings at a profit. An estimated $250,000 worth of ETH was lost by searchers trying to buy up Salmonella and Listeria in March 2021. Though some searchers have learned to avoid this trap, variations of Worsley's token contracts can be re-executed on-chain to bait any unassuming searchers into paying large amounts of ETH for relatively little amounts of their desired token.

Unlike prior examples of MEV, this strategy is designed to take advantage of MEV participants, the searchers themselves. Poisoned sandwiching attacks highlights how MEV can be used to swindle the very individuals using MEV to swindle ordinary users.

MEV Type 4: Poisoned Sandwiching

Source: Galaxy Digital Research



Just-in-Time (JIT) liquidity attacks

Another interesting MEV strategy innovated from the basic premise of sandwiching attacks is Just-in-Time (JIT) liquidity attacks. This type of MEV can only be executed on Uniswap V3, which is the third and latest iteration of Ethereum's most popular DEX.

JIT liquidity attacks take advantage of concentrated liquidity pools on Uniswap V3 that allow liquidity providers (LPs) to allocate assets within a custom price range. Instead of uniformly distributing asset liquidity across the entire price interval, LPs can concentrate their capital by creating targeted depth over a specific price range, such as to a mid-price where the highest amount of trading activity happens, earning them more trading fees. Consequently, this makes traditional sandwich attacks harder to pull off on Uniswap V3 than V2 because deeper liquidity supporting the price of an asset over a specific range makes it harder for searchers to artificially inflate prices with a single large trade.

Given this reality, MEV searchers operating on Uniswap V3 provide and remove liquidity with the express aim of rebalancing their own asset portfolios into a more profitable make up. For example, say there is a user looking to swap 1,000 ETH for 4.5 million USDC. A searcher executing a JIT liquidity attack will fulfill that order and provide the liquidity for the user's trade first. In doing so, the searcher who gives JIT liquidity earns the trading fees on that trade as a stand-in liquidity provider.

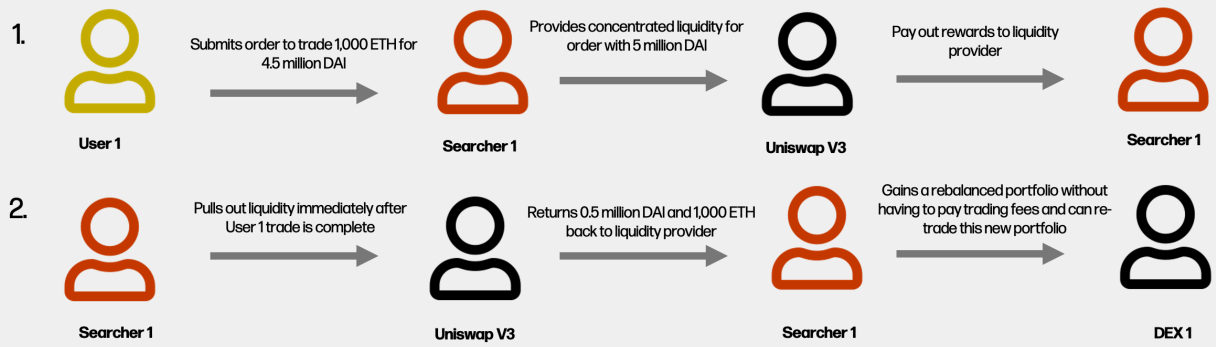
In addition, by removing the liquidity immediately after the user's trade is executed, the searcher also takes away a rebalanced portfolio of assets consisting of both USDC and ETH. Essentially, the searcher was able to gain ETH by servicing liquidity for a user's large trade out of USDC. Not only does this earn the searcher trading fees that would have normally gone to a passive LP on Uniswap, but the searcher also saves in paying for trading fees that the DEX would normally exact for swapping between two different assets. After a searcher removes their liquidity, they can trade their new portfolio of USDC and ETH for higher profits in another trading pool. According to Chainsight Analytics, searchers have earned over $1 million in saved trading fees alone from JIT liquidity attacks.

The aim of JIT liquidity, unlike sandwiching, is for getting a new asset that searchers are betting on to be more profitable. In other words, this MEV strategy requires searchers to actively manage a diversified asset portfolio and take risks associated with trading these assets non-atomically, meaning not over the span of a single block.

This type of MEV poses negative and positive consequences to network stakeholders. Though the activity is negative from the point of view of regular LPs that are not earning as many fees from traders, it is positive for the end user who get instantaneous liquidity for their individual trade at a price that is not artificially inflated.

MEV Type 5: JIT Liquidity Attacks

Source: Galaxy Digital Research



A Short History of MEV on Ethereum

Capturing MEV through the strategies explained above has been a theoretical concern for most of Ethereum's history. Anonymous hacker "Pmcgoohan" first identified the issue of miners engaging in profit-seeking transaction reordering back in 2014 before Ethereum launched. In their Reddit post, the hacker asked, "What is to stop front-running by a miner in any marketplace implementation by Ethereum?" The answer, as would be proved by the rise of DeFi, is quite simply: *nothing.*

In April 2019, researcher and software engineer Philip Daian released an academic paper presenting on-chain evidence for front-running behavior on DEXs and illustrated how MEV was a realistic, rather than theoretical, threat to network stability. Shortly following Daian's paper, several crypto research teams such as Paradigm also released case studies corroborating the existence and growth of MEV on Ethereum.

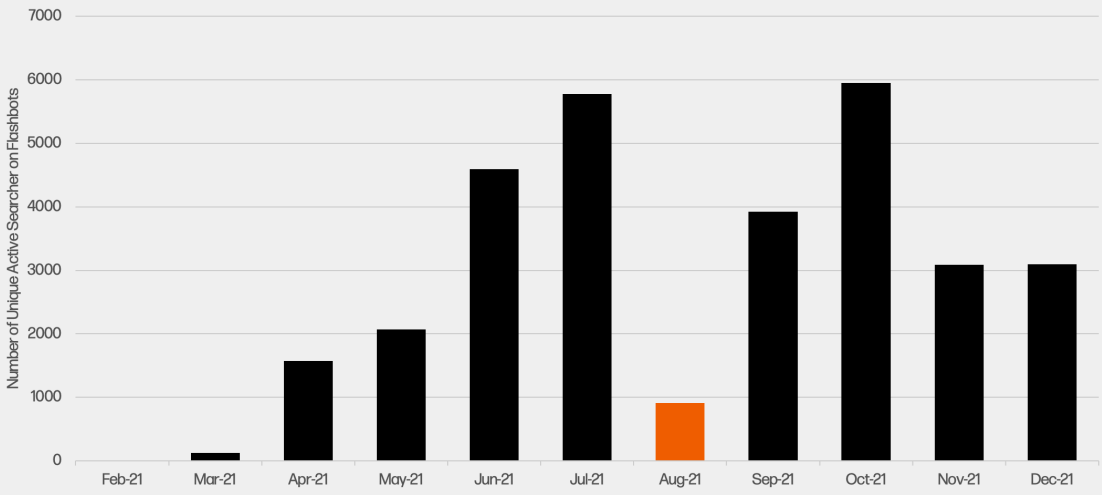
Daian and others found that the most advanced MEV attacks were being initiated not by miners but by bots, also called "searchers," specialized in identifying and exploiting information asymmetries in the DeFi markets. Due to fierce competition between searchers for MEV, miners are in a privileged position to select only the transaction bundles that offer the highest payout. Searchers can pay miners through high transaction fees for executing their bundles. The easier or simpler an MEV opportunity is, the higher the likelihood that miners will be able to earn the MEV themselves or select from several of the same bundles submitted by competing bots. This means the majority of MEV profits are usually earned by miners and in the form of bribes submitted by the most efficient searchers.

Until recently, the bidding process for MEV between searchers and miners happened primarily through private communication channels or Ethereum's pubic mempool. As background, the mempool is a waiting area for transactions that have been submitted but not yet confirmed on the blockchain. To avoid inundating the mempool with redundant transactions and to dissuade the use of private channels, Daian and a team of researchers, who together founded an MEV-focused think group known as Flashbots, launched an alternative and open communication channel called Flashbots Auction that moved the bidding process for MEV opportunities off-chain.

On Flashbots Auction, searchers submit bids for block space directly to miners, which miners then evaluate according to the bid amount. It is in the best interest of searchers to maximize their MEV payouts by minimizing gas costs for transaction execution. This allows searchers to make higher bids for block space without sacrificing their cut of the MEV returns.

Upgrade on Ethereum Causes Searcher Count to Drop

Source: Galaxy Digital Research



Data: Flashbots

The number of searchers on Flashbots has increased dramatically since the start of this year, though the count dropped temporarily in August when the Ethereum network underwent its London hard fork. The upgrade required searchers to update their bot software, and many did not do so until September likely because of the intensive changes to miner revenue and fee structure London contained.

The creation of Flashbots Auction in January 2021 is widely considered to have helped reduce average fees on Ethereum, though it is difficult to isolate that impact due to compounding effects from other network trends such as increased user activity for DeFi applications and non-fungible tokens (NFTs) in recent months. What is known for certain is that 75% of Ethereum miners, as measured by network hash rate, are now actively using Flashbots Auction to earn MEV.

Mitigating MEV

Flashbots Auction is one of several initiatives aimed at mitigating the negative externalities of MEV on Ethereum. Beyond reducing the number of high fee transactions, Flashbots Auction has helped to democratize MEV by making participation in this type of profit-taking easily accessible to both searchers and miners. The channel has also established norms and standards of behavior to protect searchers from being front-run by miners who try to execute their own transactions after seeing the ones submitted by searchers.

The solutions to MEV presented by Flashbots are by no means perfect. Flashbots Auction is managed by a centralized entity and as such, the transaction bundles submitted to the Flashbots Auction channel are not censorship-resistant. According to data from Flashbots, 50% of Ethereum blocks now include transactions from Flashbots Auction. As a percentage of total blockspace, less than 1.5% of blockspace on average is filled with Flashbots transaction bundles. While this value is minor today, if the use of Flashbots Auction for earning MEV grows, there is a danger for Flashbots as an organization to become the gatekeepers determining which searchers and miners get to participate in this type of profit-making and which don't.

Moreover, Flashbots has expanded its services to include front-running protection which encourages ordinary traders and users to submit their transactions to Flashbots Auction instead of the public mempool for enhanced safety against MEV. While this type of protection is greatly desired, the risk is that if 100% of users begin routing their transactions through Flashbots, the organization would be a central point of failure for the network and could effectively censor which transactions land on-chain.

Flashbots Tx Bundles as a % of Total Ethereum Blockspace

Source: Galaxy Digital Research

Data: Flashbots

Flashbots becoming the dominant private pool for transactions is an unlikely outcome seeing as the developers of Flashbots are actively working with Ethereum protocol developers to decentralize Flashbots Auction and transform it gradually into a permissionless protocol. In addition, there are services outside of the Auction that also offer traders and users MEV protection. Traders participating in DeFi have a vested interest in promoting a fair market structure, which is why sophisticated engineering of dapps to reduce or make MEV extraction harder is another force outside of Flashbots working to combat the most extractive types of MEV on Ethereum.

The newest liquidity pools in Uniswap V3 that make sandwiching attacks harder is a prime example of how changes to the code specifications of a DEX can serve to create new types of MEV that does not negatively impact traders while also dissuading the use of MEV strategies that do. Other DEXs such as 1inch and Archerswap are choosing to integrate their services with private transaction relays so that trades are not revealed to the public mempool until they are confirmed on-chain. This can be likened to the use of dark pools in traditional markets to avoid getting front run by high frequency traders.

Like Flashbots Auction, the use of alternative transaction relays has negative externalities of its own because these relays often do not have the same guarantees for transaction censorship-resistance as the Ethereum mempool. Yet, the existence of multiple relays for MEV protection does discourage transaction throughput from aggregating towards a single centralized gatekeeper. These private relays combined with changes to the design of DeFi dapps represent ongoing efforts to restore user trust in the resilience of the network's budding financial markets against MEV. These efforts are further bolstered by broader community consensus and engagement around the topic of MEV, which can manifest in a sort of self-policing force on a decentralized network.

In July 2021, MEV searcher Edgar Arout postulated specialized software for "time-bandit attacks," which is a type of MEV incentivizing block reorganizations on Ethereum. In a time-bandit attack, miners are incentivized to roll back the chain due to the MEV opportunity of doing so. Essentially, users could pay miners to conduct 51% attacks. Normally, miners are incentivized against attacking the network in this way since it would crash the value of their earnings in ETH. However, these incentives are arguably weaker with the impending transition away from proof-of-work mining to proof-of-stake validating.

While we have never seen time-bandit attacks conducted in the wild and they remain theoretical today, the potential for time-bandit attacks to become prolific on Ethereum sparked wide concern, with the community particularly suspicious of the mining pools most capable of taking advantage of these MEV opportunities. Ethermine, the largest mining pool by hashrate on Flashbots, chose to speak out against engaging in time-bandit attacks strictly out of principal, even though this type of MEV is theoretically possible and potentially profitable on Ethereum.

Relying on self-interested network stakeholders to think of the greater good is not a reliable solution for a public ecosystem of Ethereum's scale. However, a vigilant community can serve to identify and shame bad actors as a temporary stop gap for malicious MEV strategies until more permanent solutions can be implemented within dapps or the Ethereum protocol itself. Closely tied to initiatives combatting the most damaging types of MEV on network stability is Ethereum's upgrade to Proof-of-Stake (PoS).

MEV and Ethereum 2.0

Sometime next year, Ethereum is expected to upgrade to a PoS consensus model, which will remove the need for miners entirely from the network. Instead of being secured by the competitive computation of miners, Ethereum will be secured through validator node operators. These node operators are individuals and businesses who stake multiples of 32 ETH on the network and run specialized software for proposing blocks and attesting to valid blocks. In exchange for their efforts, validators collect newly minted issuance and transaction fees.

Validators will be the new entities collaborating with searcher bots to extract MEV once Ethereum transitions to PoS. Under the new consensus model, reorganizing the chain through a time bandit attack will become practically impossible due to the new fork choice rules which govern how the network determines canonical blocks and finalizes them. This change to Ethereum's fork choice rules will remove a major negative outcome of MEV – that miners could be paid to reorganize the chain, which would cause significant network instability.

However, while validators could not reorganize the chain to undo past blocks, under the current specifications for Ethereum 2.0 it is within the realm of possibility that validators could delay future block proposals to optimize for a lucrative MEV opportunity, which presents new complications. To mitigate the feasibility for reorganizations of future blocks, a new weighting dynamic for the votes of validators called "proposer boosting" is in the process of being formally added to the specifications of Ethereum's upgrade to PoS. The proposer boosting proposal is aimed at securing the network from any type of adversary, not just MEV-hungry validators, from pulling off future-looking block reorgs.

Apart from these types of upcoming design tweaks aimed at improving network security are efforts to improve the scalability of Ethereum over the long-term while also mitigating the negative edge cases of MEV. Layer 2 rollups are a technology quickly becoming the dominant scaling solution for the network. Rollups batch multiple transactions and only submit the bare minimum amount of information, called a proof, to the public mempool of Ethereum. This not only reduces the weight of transactions to allow for more transactions in a block but can also work to obfuscate opportunities for MEV from searchers and miners.

The downside is that Ethereum has not yet built up the necessary infrastructure for supporting the technology. Executing rollups is not always cost-effective for users wanting to deploy complex smart contracts and the interoperability between Layer 2's has yet to be fully fleshed out. Furthermore, rollups often rely on a centralized sequencer for processing transactions on a Layer 2 and submitting proofs of the transactions on the Ethereum base layer.

As the infrastructure for rollups is advanced and standardized across Ethereum, the technology is likely to have far-reaching impacts on MEV, especially when it comes to the implementation of PBS, Proposer Block Builder Separation. PBS is an untrusted and permissionless version of what the Flashbots team is currently working on for the network's upgrade to proof-of-stake.

Flashbots 2.0

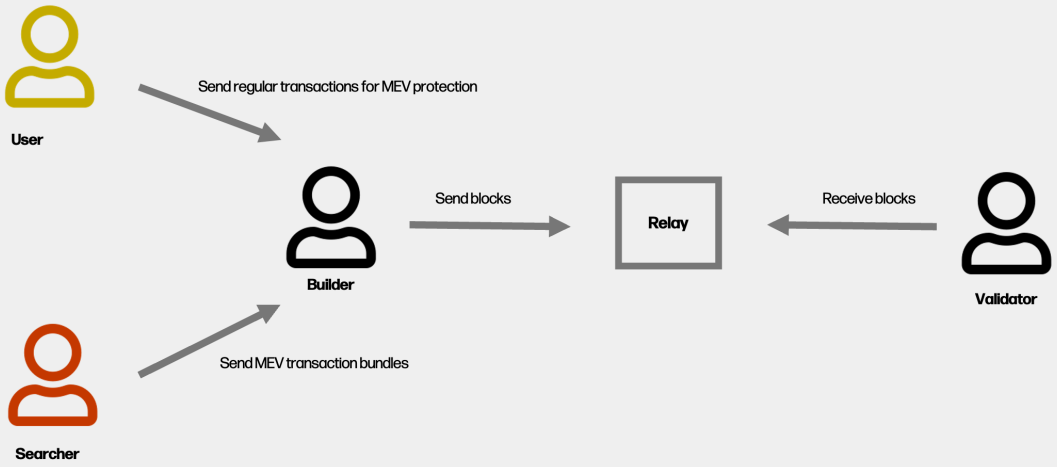
The creators of Flashbots Auction are working on new designs for their MEV communication channel that are adapted for validators. The upgrade for Flashbots Auction called "MEV Boost" introduces a neutral third party to build blocks from searchers and relay them to the block producers, which in a PoS consensus model are the validators. MEV Boost does not require changes to the Ethereum protocol and instead relies on trusted relays to protect users and searchers from frontrunning behavior. Over the long-term, Ethereum protocol developers are working towards implementing an untrusted set-up of MEV Boost called "Proposer/Block Builder Separation."

Under MEV Boost, block builders receive a fee to build the most lucrative blocks for validators and manage the complexities of running between validators and searchers. This creates a new area of specialization that participants in MEV can earn rewards from. While there are clear gains from being a searcher and identifying lucrative MEV opportunities, as well as being a validator and executing these strategies on-chain, users who focus exclusively on transaction bundle ordering and block gas optimization can also stand to earn a piece of the MEV pie.

Additionally, the benefit of delegating transaction ordering to block builders is to further obfuscate the content of blocks from validators and reduce the ability for validators to front run searchers by replicating their transaction bundles. This helps to democratize MEV and ensure that the gains from this type of behavior are not centralized over the long-term to validators alone. Finally, having a neutral third-party to the relationship between searchers and block producers is anticipated to improve the trust relationship between these two parties and encourage more complex, and perhaps net-positive MEV types to be innovated over the long-run.

In these ways, protocol developers from the Ethereum Foundation and the creators behind Flashbots Auction are redesigning elements of how MEV is earned today to provide long-term security for Ethereum's consensus model.

MEV Boost Architecture
Source: Galaxy Digital Research



The Future of Finance on Ethereum

Due to the wide-ranging impacts of MEV on Ethereum, the solutions for managing this type of profit-taking are not only varied but riddled with tradeoffs. For example, while Flashbots Auctions has democratized participation in MEV and moved the burden of MEV transaction activity off-chain, it has also accelerated the adoption of this type of profit-taking and routed the majority of this activity to a centralized communication channel.

As for MEV protection channels such as CowSwap, though billions of dollars in trade volume are now protected against sandwiching and other malicious MEV attacks, it also means there is reduced visibility not only for searchers but also the general public into DeFi market liquidity and activity. In addition, by circumventing the public mempool, MEV protected DEXs add a layer of complexity and technological risk to the DeFi ecosystem by introducing alternative protocols for transaction settlement.

As such, managing MEV on Ethereum and other smart contract blockchains comes down to optimizing between these various tradeoffs to reach a sustainable equilibrium where MEV and DeFi can co-exist. Over time, as on-chain expertise grows, we expect that DeFi markets will become more efficient, reducing MEV arbitrage and liquidation opportunities. However, the most value extractive MEV opportunities, such as sandwiching, will not reduce simply because market participants become more aware of them.

Finding ways to effectively mitigate negative MEV is essential for the long-term health of Ethereum-based economic systems and to prevent trust from gradually eroding in the fairness of the DeFi ecosystem. It is also important that the solutions that are being increasingly relied on for protecting users against MEV attacks trend towards decentralized systems as opposed to centralized gatekeepers. The ideal is that over time a combination of newly engineered dapps, on-chain and off-chain communication channels, as well as protocol-level upgrades will support a robust Goldilocks economy on Ethereum that is permissionless and transparent with minimal negative MEV impacting users.

As a still nascent ecosystem that has been in operation for less than a decade, the rules and norms governing the budding Ethereum DeFi markets are still largely in the process of being fleshed out. Efforts to optimize MEV solutions for maximizing

decentralization and user trust in DeFi are analogus to efforts seeking to create fair and open financial markets in the U.S. The tradeoffs discussed in this report for addressing MEV are not unlike the ones that the traditional finance industry have had to grapple with for the past century. However, this time around with DeFi and blockchain technology, the aim is to build a financial system that incorporates the core ethos of crypto predicated on values of openness, transparency and trustlessness.

Conclusion

Opportunities for MEV have significantly grown in number over the past year as the value locked in DeFi has also increased. Some types of MEV in DeFi such as sandwiching create profits at the expense of traders, while others such as arbitrage are widely seen as positive forces in DeFi creating market efficiency and deeper liquidity for traders. The most common types of MEV seen on Ethereum are arbitrage, liquidations, and sandwiching, though new types of MEV are being created by searchers taking advantage of the forefront of DeFi innovations.

MEV is an innovation that takes advantage of the fact that Ethereum miners (and soon validators) have the discretion to order transactions within blocks they produce. This discretion has an important purpose: it helps guard the network against spam. But this important power (transaction ordering) has given rise to an industry not unlike the high-frequency traders in traditional finance. Both MEV and HFT rely on identifying opportunities for profit by executing transactions in a specific order, usually ahead of the transactions of another market participant. Both can create negative outcomes, either directly or via externalities, for market participants and can erode the trust of traders in the market, encouraging the use of private means of communication to execute trades.

Unlike the traditional markets, there are no centralized regulatory bodies to oversee and enforce rules around MEV on Ethereum. As a decentralized and permissionless system, the only laws governing MEV on Ethereum are the ones explicitly codified in the network's consensus mechanism. This places a greater burden on protocol developers, dapp users, and the wider Ethereum community to promote code changes and enforce norms around the types of MEV that should and should not be tolerated on-chain.

Efforts to combat MEV are riddled with tradeoffs. A prime example of this is the creation of Flashbots Auction, which created unprecedented transparency around the types and volumes of MEV earned on-chain but also made it significantly easier for miners to rely on MEV for additional profits. In addition, by moving the bulk of the bidding wars for MEV profit by searchers off-chain, Flashbots has helped reduce congestion in the Ethereum mempool but also created a centralized gatekeeper for which the majority of Ethereum miners now rely on for earning MEV.

There are upgrades to Flashbots that are expected to improve these various tradeoffs and make Flashbots Auction a more trustless system but none of these upgrades create a network void of transaction ordering manipulation. In a future where both MEV and DeFi must flourish together, the question remains whether trust and resilience in Ethereum's dapp ecosystem will remain unscathed over the long run.

Legal Disclosure

For all inquiries, please email contact@galaxydigital.io.

galaxy

contact@galaxydigital.io

galaxy.com