COTW: The Battle of the Bots and Maximal Extractable Value

Pending transactions on Ethereum and other blockchains await inclusion in a block in what's known as the mempool. The ability to know future transactions in advance, however, has led to a behind-the-scenes battle of the bots seeking to identify, front run, and snipe transactions from users and each other. We discuss maximal extractable value in this week's Chart of the Week.

The Mempool Dark Forest: When transacting on Ethereum, a user will broadcast his or her transaction to the network, with the transaction including a base fee and a priority tip, collectively known as gas, to compensate the miner for the computation required to process the transaction. As transactions are not immediately added to the blockchain, the transaction is then placed in a pending transaction queue known at the txpool or mempool, where nodes run a series of transaction validity tests before a miner picks it up for inclusion in a block. Importantly, miners may choose both the transactions they want to include in their proposed block as well as the transaction order, and typically select transactions from the mempool with the highest gas price and order them by gas spend. While the mempool acts as an important waiting area and source of information on pending transactions, knowing future transactions in advance can also be used malevolently, for example, by bots looking to front run pending trades. In fact, so prevalent are these bots scouring the mempool for profitable opportunities, battling each other to be the first to discover a trade, snipe each others' transactions, and engage in gas fee bidding wars, that Paradigm's Dan Robinson famously christened the mempool The Dark Forest after the sci-fi book which features an environment where detection means certain death at the hands of advanced predators.

Maximal Extractable Value (MEV): Coined in a 2019 seminal study titled Flash Boys 2.0 by Philip Daian and others, MEV is a measure of profit that a miner or validator can extract from block production beyond the block reward and gas fees by including, excluding, and changing the order of transactions in a block. While miners are in prime position to identify and capitalize on such transactions, as they control which transactions are included and in what order, the majority of MEV is extracted by independent third parties called searchers that use sophisticated trading strategies to capture MEV. Miners who see such MEV-extracting transactions may then copy the searcher's transaction to profit

from the transaction themselves, or other searchers will notice and copy the MEV-extracting transaction and a gas price bidding war will ensue, leading to the miner capturing the majority of the MEV via a higher gas fee. Searchers therefore not only compete on identifying opportunities, speed, transaction obfuscation, ect, but also on programming transactions to use as little gas as possible, allowing them to pay a higher gas price than competitors while still maintaining the profitability of the transaction.

MEV Examples: In practice, searchers identify and execute MEV extraction through what's known as an engine or bot, code that automates transactions based on an algorithm of user-defined parameters. Bots may look for specific types of transactions in the mempool, such as a trade on a decentralized exchange, or may be generalized bots that scour the mempool for any transaction that can be profitably front run before copying the code, replacing addresses with its own, and submitting the transaction with a higher gas price. In addition to front running, bots also employ backrunning, where a transaction is broadcast with a slightly lower gas price than an existing pending transaction so that it gets mined immediately after in the same block. This may occur, for example, when executing a loan liquidation after a price oracle update showing the loan has breached the minimum collateralization ratio. MEV transactions run the gamut, but common examples include:

- Decentralized Exchange Arbitrage: As liquidity in crypto is fragmented, searchers can monitor various venues to arbitrage price differences. For example, if two venues are showing a different price for the same asset, one may buy the asset at the lower priced venue and sell it at the higher priced venue in one atomic transaction.

- Sandwich Trades: Sandwich trades are where a searcher looks through the mempool for large trades on a decentralized exchange and then wraps the trade with its own buy and sell order, profiting as the DEX buy order moves the price in the searcher's direction after the searcher has bought the asset but prior to sale. Illustrating just how prevalent and advanced the bot wars have become, there are even sandwich attacks on sandwich attacks, as well as sandwich attacks on DEX liquidity providers that deploy significant liquidity immediately before a transaction only to remove it immediately after, capturing the transaction fee but avoiding impermanent loss.

- Liquidations: Borrow lend protocols allow users to take out overcollateralized loans against deposited cryptocurrency. Due to fluctuations in the value of the collateral, however, the collateralization ratio may fall below a pre-arranged minimum threshold, allowing the loan to be liquidated. Most borrow lend protocols allow outside third parties to perform the liquidation, who then earn a portion of the liquidation fee. Liquidators will thus search through blockchain data to discover and be the first to liquidate such loans.

Implications of MEV: While certain types of MEV trades are beneficial - for example, arbitraging prices between DEXs to ensure users pay the same global market price or liquidating riskier loans to ensure lenders are paid back - MEV has a number of negative externalities, including:

- Transaction Execution: MEV creates worse execution for traders, who, when front run, buy at elevated prices and face greater slippage than what otherwise would have been the case.

- Gas Prices: MEV causes elevated gas prices for normal users, as searchers occupy block space and bid up gas prices to increase the probability of being included in the next block.

- Blockchain Properties: MEV also hurts the neutrality, transparency, and permissionlessness of the blockchain, as it encourages permissioned, centralized communication infrastructure between searchers and miners.

- Network Stability: MEV makes the Ethereum blockchain less stable as miners are incentivized to re-mine blocks to capture high MEV transactions for themselves. For example, if a miner mines a block containing a $10m MEV opportunity, another miner is incentivized to re-mine this block to capture the $10m MEV opportunity for themself rather than build upon it, a situation known as a time-bandit attack and which may happen whenever the profit from re-mining outweighs the base block reward.

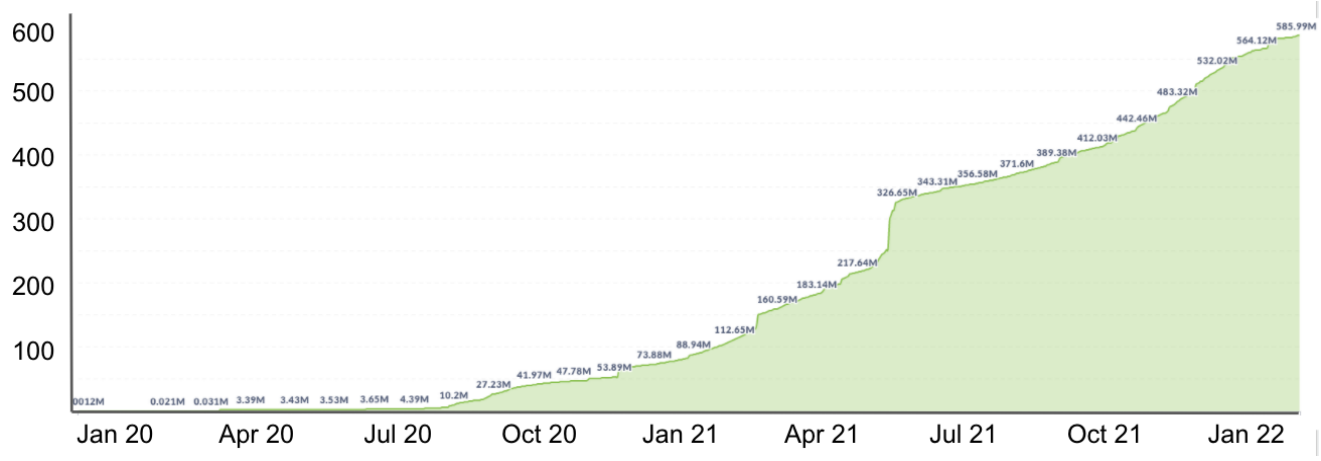
Democratizing MEV Access with Flashbots: There are many companies and projects working on mitigating the negative externalities of MEV via various strategies and methods, though perhaps the most well known is Flashbots. Flashbots is a research and development organization seeking to illuminate, democratize, and redistribute MEV by serving as a neutral, public, open source infrastructure for permissionless MEV extraction. Rather than the current system where users broadcast transactions with a gas price to the public mempool causing gas price bidding wars, unnecessary network load, artificial blockspace scarcity, and less user control, Flashbots introduces an open-sourced, democratic, and neutral private communication channel between miners and searchers called Flashbots Auction. Flashbots Auction allows users to privately communicate their bid and granular transaction order preference using a first-price sealed-bid auction, creating an efficient venue for price discovery on the value of a MEV opportunity. The system works by Flashbots searchers creating bundles, which are ordered lists of transactions prioritizing the searcher's transactions followed by the most profitable transactions (for the miners) from the public mempool. Bundles are then sent to a specialized server called a relayer, which forwards the bundles to Flashbot miners running mev-geth, a patch on top of the go-ethereum client, and who have a private mempool that only Flashbots miners can see. Miners then evaluate bundles examining the sealed bids and place the most profitable bundles at the top of the block before comparing the Flashbots block with a traditional block and mining the more profitable one. Flashbots miners are compensated by Flashbots searchers with ETH, and the entire system prevents gas wars and failed transactions, eliminates front running, allows for several transactions to be executed atomically, and brings in additional revenue for miners. Lastly, Flashbots also offers a suite of tools for increasing MEV transparency as well as an open research effort studying important MEV-related research questions. While some have applauded Flashbots for lowering gas fees, reducing bot war-driven on-chain congestion, and improving network stability, others have criticized it for essentially auctioning off the right to front run users, likening it to theft. Over 50% of Ethereum blocks contain a Flashbots bundle, per the Flashbots MEV explorer, and nearly $600m of cumulative MEV has been extracted since January 2020, as shown in **Exhibit 1.** Note that this measure only captures extracted MEV rather than available MEV, and does not cover sandwich attacks, making this more representative of a lower bound.

The Future of MEV: MEV is a highly complex topic and significant research efforts have been underway for some time. One line of study involves fairness algorithms, which attempt to use cryptographic methods such as time-locked commitments to transaction ordering or pending transaction state to enforce time-based fairness guarantees. Another line of research involves protocol design, aiming to fundamentally order transactions fairly to begin with, as well as encrypting transactions until after they've been ordered. Other research focuses on the potentially network

destabilizing effects of re-orgs, with partial answers including separating the act of inclusion and ordering for miners, moving to strong finality guarantees, and slashing PoS validators who attempt to re-org. There is yet another line of thought that MEV will not be eliminated entirely, so it's better to allow it via an open, transparent, and efficient system. Lastly, mitigation brings about tradeoffs that need to be thoughtfully considered, such as with time lock encryption adding latency and fair sequencing servicing adding security assumptions.

Going forward, the opportunity to capture MEV may grow as DeFi activity grows, all else equal, and as more miners attempt to capture MEV themselves, given that they may execute more complex strategies compared to searchers mainly relegated to gas price auction-related MEV. Moreover, searchers are likely to move to alternative layer ones with less MEV competition, and cross-chain MEV and multi-block MEV are likely to increase. There is hope, however. Ethereum's upgrade to proof-of-stake will make short-term re-orgs extremely difficult, as block production will be bifurcated into proposer and attester roles. And while some researchers have suggested there may be more MEV on ETH 2.0, the presence of MEV can actually enhance security as it attracts more validators. Scaling solutions can help too, with different strategies being taken on such as MEV auctions with Optimism and fair ordering with Arbitrum. And new protocol design can mitigate MEV, such as with Uniswap V3's concentrated liquidity that reduces the price impact of a trade and thus MEV, Eden Network's transaction ordering network tokenizing blockspace, Injective Protocol's verifiable delay function, and KeeperDAO's guild of MEV-searching keepers incentivizing coordination over competition. So while MEV is likely to always be present in some form, Ethereum appears to be on its way to mitigate where possible, and democratize when not.

Exhibit 1: Cumulative MEV Extracted Since Jan 1, 2020, $m



Source: Flashbots, GSR

Author: Brian Rudick, Senior Strategist

Sources

- Cornell Tech: Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges
- Ethereum Foundation: MINER EXTRACTABLE VALUE (MEV)
- Paradigm: Ethereum is a Dark Forest
- Paradigm: MEV and Me
- Flashbots: Frontfunning the MEV Crisis
- ETHGlobal: Flashbots: Finding & Capturing MEV 101
- ETHGlobal: The State and Future of MEV
- ETHGlobal: Is MEV a Problem to be Solved or a Reality to be Lived With
- Stanford: A Note on Bundle Profit Maximization
- Coindesk: Miners, Front-Running-as-a-Service Is Theft
- Coindesk: Miners, Front-Running-as-a-Service Is Theft

About GSR

GSR is a global leader in digital asset trading, market making, OTC derivatives, and investments. We operate in a culture of excellence and leverage our first-rate reputation, deep relationships and proprietary trading technology to move swiftly and capitalize on market opportunities.

GSR's experienced team brings together decades of institutional trading expertise, while our industry-leading proprietary technology stack anchors everything we do.

Our main service areas are: market making; proprietary and algorithmic trading; client execution; structured products; risk management solutions; and portfolio investments.

For more information or if we can help with anything, please see gsr.io or contact us at gsr@gsr.io.

Required Disclosures

This material is a product of the GSR Sales and Trading Department. It is not a product of a Research Department, not a research report, and not subject to all of the independence and disclosure standards applicable to research reports prepared pursuant to FINRA or CFTC research rules. This material is not independent of the Firm's proprietary interests, which may conflict with your interests. The Firm trades instruments discussed in this material for its own account. The author may have consulted with the Firm's traders and other personnel, who may have already traded based on the views expressed in this material, may trade contrary to the views expressed in this material, and may have positions in other instruments discussed herein. This material is intended only for institutional investors. Solely for purposes of the CFTC's rules and to the extent this material discusses derivatives, this material is a solicitation for entering into a derivatives transaction and should not be considered to be a derivatives research report.

This material is provided solely for informational purposes, is intended for your use only and does not constitute an offer or commitment, a solicitation of an offer or comment (except as noted for CFTC purposes), or any advice or recommendation, to enter into or conclude any transaction (whether on the indicative terms shown or otherwise), or to provide investment services in any state or country where such an offer or solicitation or provision would be illegal.

Information is based on sources considered to be reliable, but not guaranteed to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of the date of publication, and are subject to change without notice. Trading and investing in digital assets involves significant risks including price volatility and illiquidity and may not be suitable for all investors. GSR will not be liable whatsoever for any direct or consequential loss arising from the use of this Information. Copyright of this Information belongs to GSR. Neither this Information nor any copy thereof may be taken or rented or redistributed, directly or indirectly, without prior written permission of GSR. Not a solicitation to U.S. Entities or individuals for securities in any form. If you are such an entity, you must close this page.