The Key Neutrality of Baselayer Markets

A Response to Questions Posed in SEC Commissioner Hester Peirce's "There Must Be Some Way Out of Here"

By Alex Grieve, Rodrigo Seira

PDF Version [here]

Summary

SEC Commissioner Hester Peirce recently released 48 questions on which the SEC Crypto Task Force has sought clarity. Paradigm seeks to provide helpful context on MEV – a native, economically rational feature of Ethereum's decentralized architecture that supports efficient blockspace allocation and market stability.

While certain mechanics of MEV can create negative externalities, we seek to demonstrate that

the market is already addressing these challenges through technical innovation. We also examine why MEV activity on its own does not satisfy the legal elements of securities fraud, insider trading, or best execution violations under U.S. law.

Paradigm argues that any regulatory intervention would risk disrupting a still-maturing but self-correcting market structure, and we encourage the Commission to take a tech-neutral, flexible approach that preserves decentralization and fosters innovation.

I. Introduction

We thank Commissioner Peirce and the Crypto Task Force for posing important questions regarding how the Commission and its registrants should think about MEV and any potential regulatory response.[1]

In this paper we will first provide background on MEV, describe its rapid and continuing evolution, and disambiguate between the different types of MEV that currently exist. We will then show how the development of MEV infrastructure generally has had a net positive impact on crypto markets and its participants. While certain types of MEV in their current implementation can create negative externalities, we argue that ongoing technological development will address these externalities and ultimately achieve the Commission's policy goals better than regulatory impositions could. Therefore, the Commission should defer to this continued technological development and avoid relying on overly-prescriptive guidance or rulemakings that would stymie such development or undermine its benefits.

In the second part of this paper, we will address certain criticisms that have been levied against current forms of MEV, including claims that it amounts to market manipulation, insider trading, or that MEV is inconsistent with the principles of best execution. We will show that, even if MEV were to take place in transactions subject to the securities laws, it would not meet the legal stands of market manipulation or insider trading. In fact, MEV can be consistent with the principles of best execution.

While MEV is a phenomenon across all of crypto, Ethereum has one of the most-studied and developed MEV ecosystems, so we will focus this paper on

[1] Peirce, Hester, *There Must Be Some Way Out of Here*, February 21, 2025, available here: https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125.

- Question 17 ("Trading"): Does execution in offchain order books or on blockchain networks pose complexities for broker-dealers in satisfying any applicable best execution obligations? Does onchain execution pose complexities for broker-dealers in satisfying their best execution obligations, given onchain complexities such as transaction ordering and block construction? Should any rules, guidelines, or disclosures be modified to address broker-dealer execution reasonably available under the circumstances in offchain and onchain trading environments?
- Question 20 ("Trading"): How should Commission registrants assess Maximal Extractable Value ("MEV") when they consider building or transacting in these environments? How best should Commission registrants delineate between the different types of MEV occurring onchain? In what ways is the market addressing the MEV in which MEV extractors order or re-order transactions to engage in front running, back running, or so-called "sandwich attacks"?

Ethereum as a case study for understanding MEV and its relevant regulatory considerations.

II. What is "MEV"?

A. Origin and Evolution of the Term "MEV"

The concept of "MEV" was first identified in the context of Ethereum's proof-of-work (PoW) network as "Miner Extractable Value." Researchers in 2019 coined this term to describe the profit that a miner could make by optimally ordering, including, or censoring transactions in a block.[2] In essence, miners could capture extra value (beyond the standard block reward and fees) by including certain trades in a profitable sequence, or excluding and inserting transactions to capitalize on price discrepancies. Following Ethereum's transition from proof-of-work to proof-of-stake (PoS) in the 2022 "Merge," the terminology shifted to "Maximal Extractable Value."[3] The acronym remains MEV, but now emphasizes that the MEV phenomenon extends beyond miners to other "base layer" actors (be it a miner, validator, or sequencer on layer-2 chains).

B. Ethereum's PoS Block Production Supply Chain

Ethereum's block production supply chain has evolved and matured over many years, now involving separation among different specialized actors:

- **Searchers:** Independent, specialized actors who scan the blockchain as well as transaction pools or "waiting rooms" called "mempools" for MEV opportunities. Searchers typically run bots that look for arbitrage opportunities, liquidations, and other profit scenarios. When they detect an opportunity, they formulate a sequence of transactions (sometimes including user transactions plus their own transactions) to capitalize on it. This sequence is packaged as a "bundle" and submitted to block builders, with a fee (or "tip") attached to incentivize inclusion.[4] Searchers typically do *not* produce blocks or have protocol-level authority; rather, they compete to influence ordering by offering profit to those who do have that authority.

- **Block Builders:** Entities in the post-Merge Ethereum that specialize in constructing entire blocks. Instead of validators individually picking transactions, most validators outsource this task to builders. Builders aggregate transactions from the public mempool and bundles from private searchers to assemble an optimal block – i.e. the block that yields the highest fees or MEV profit. They take into account gas fees and any extra tip from searcher bundles, creating a proposed block that maximizes payoff. Builders then bid this block to the validator (proposer) by offering a portion of the profit (e.g. a direct payment to the

[2] Daian et al., *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, April 10, 2019, available here: https://arxiv.org/pdf/1904.05234.pdf

[3] See, Salas, Alejo, Quantifying Realized Extractable Value, March 19, 2021, available here: https://hackmd.io/@flashbots/quantifying-REV

[4] See, e.g., Varunx, Ethereum Block Building: The Hidden Economy Behind Every Transaction, March 24, 2025, available here: https://hackernoon.com/ethereum-block-building-the-hidden-economy-behind-every-transaction

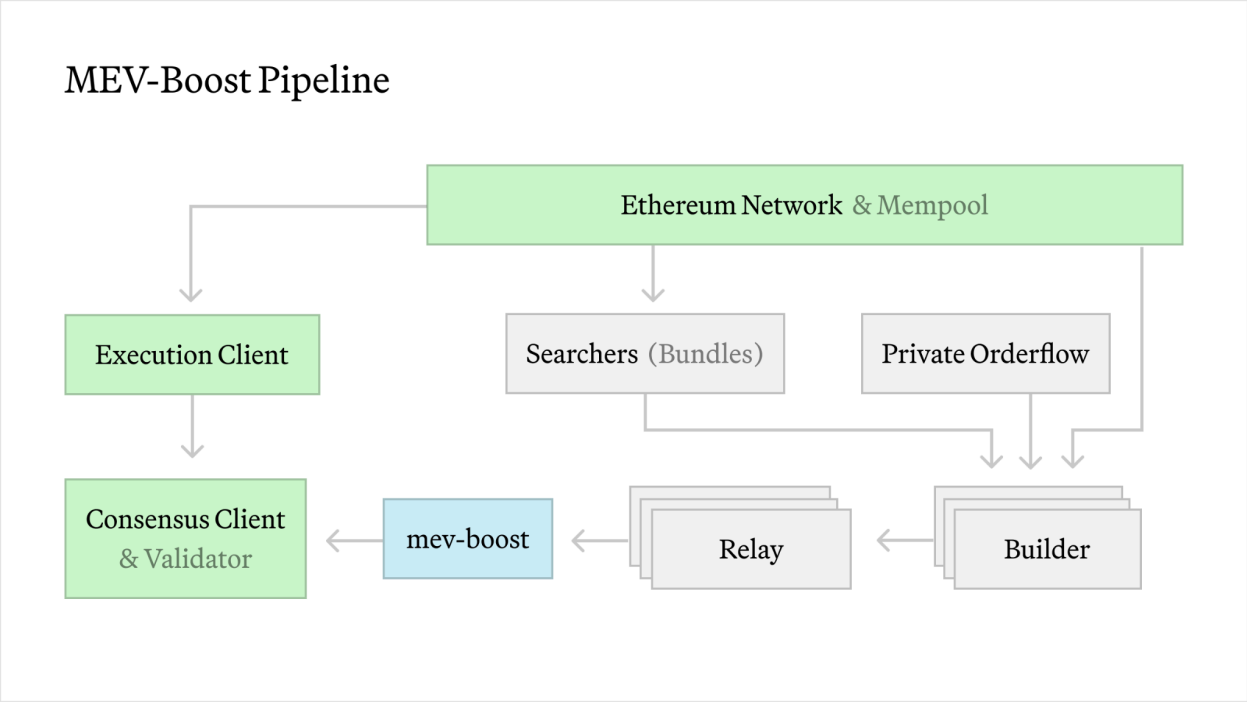
validator). In practice, multiple builders compete for each block, each submitting an execution payload and a bid (in ETH) to the proposer. This competition is essentially an auction for the right to build the block.

- **Block Proposers (Validators):** In PoS Ethereum, validators take turns proposing blocks (each 12-second slot has a randomly chosen proposer). Under the "proposer-builder separation" ("PBS") model, a proposer no longer needs to determine the block's contents; instead the proposer's role is to choose the best block from builders. "Best" typically means the block that pays the highest fee to the proposer (while still being valid). The proposer receives bids (via a relay system) from various builders and will almost always select the block containing the most value (since that maximizes the proposer's own reward and increases the resilience of the network). The proposer then signs this block and it gets finalized in the blockchain.

  The division of labor in PBS emerged as a solution to earlier problems where validators had to choose between establishing sophisticated operations or lower block rewards. This choice placed the neutrality of validators, the centralization of stake, and the barrier to entry to home stakers at odds, causing harm to the economic security of the network. Now searchers compete to find MEV, builders compete to package MEV into blocks, and validators select the highest-paying result. This separation *democratizes* access to MEV revenue and streamlines block production. Even though PBS was not "enshrined" in the first version of the Merge, it is implemented in practice through off-chain coordination (e.g. the MEV-Boost system).[5][6]

  In the MEV-Boost pipeline (the de-facto PBS mechanism since the Merge), the steps are as follows:

[5] See Flashbots, MEV-Boost, available here: https://docs.flashbots.net/flashbots-mev-boost/introduction
[6] Flashbots, an Ethereum research group, is a Paradigm portfolio company.



1. **Bundles & Transactions:** Users and searchers submit transactions. This can happen through the public mempool or through private channels. Searchers often send their bundled transactions directly to builders rather than exposing them publicly.

2. **Block Assembly:** Competing block builders take the available transactions and bundles to construct a candidate block (an execution payload) optimizing for profit. The builder will set its own address as the coinbase (to collect block rewards, priority fees, and MEV profits) and typically include a special transaction paying the proposer's fee (the bid for that block) at the end of the block.

3. **Block Auction via Relays:** The builders transmit a block header (without revealing the full contents) and bid to the network of relays (e.g. Flashbots relay) which facilitate the auction. The relays check that the bids are real (e.g. the offered payment to the proposer is as stated) and forward these block proposals to the validator's MEV-Boost software. MEV-Boost then selects the most valuable block header (the one with the highest proposer payment) and passes it to the validator.

4. **Proposal and Sealing:** The validator (proposer) signs the chosen block header, effectively sealing that block for the given slot. The signed block is returned to the relay, which then releases the full block (with all transactions) to the network. At this point, the block is official on the blockchain, and the proposer collects the bid, while the builder and any included searchers collect the remaining MEV profits.

   This whole process takes place within a fraction of a second before each block is published on the Ethereum blockchain. It's a parallel, low-latency auction for blockspace that repeats every block. To an outside observer, Ethereum blocks just appear one after another with sets of transactions. But within each

12-second slot there is intense competition among block builders. Builders simulate potential blocks using sophisticated algorithms to identify the most profitable block sequence. These simulations are sent to relays and the simulations continue up to and through the close of the auction, ensuring that all potential transactions and bundles submitted within a block time are considered for inclusion. From the validator's perspective, these bids arrive nearly simultaneously, and the validator picks the highest bid in the real-time auction.

The short interval before block inclusion is a battleground of speed and strategy – but it's an *open battleground*. Anyone with the technical savvy can participate as a searcher. The outcome (the block order) is ultimately constrained by who bid the most or found the most efficient combo of transactions. This system is beneficial for the whole ecosystem since it leads to the most efficient allocation of blockspace.

C. Transaction Ordering: Auctions vs First-Come-First-Served

A crucial difference between transaction ordering in Ethereum as compared to the traditional financial markets with which the Commission is more familiar is how the priority of transactions is determined. In traditional financial markets (like stock exchanges), orders are usually executed in the exact sequence they are received ("first-in-time" priority), or by strict price-time priority rules. An equity trade cannot usually cut in front of a prior trade unless, perhaps, it offers a better price – and even then, certain fairness rules apply.

In distributed systems, such as the Ethereum network, each node in the network maintains its own list of pending transactions (each node maintains its own mempool, there is not one canonical mempool). Therefore it is technically infeasible to establish a first-in-time priority on Ethereum. If Alice and Bob send transactions to the Ethereum network separated by one second, nodes in different parts of the world will log those transactions at different times depending on their geographic and latency relationship to Alice and Bob's locations.

Establishing a first-in-time ordering policy for Ethereum would break the inherent value of using a distributed system. A first-in-time ordering policy would necessitate a single canonical node to establish time-based ordering. This would lead to all systems in Ethereum co-locating infrastructure to that node, breaking the decentralization of the network and creating a single centralized infrastructure network.[7]

Block builders are therefore not *re*ordering transactions. In fact, the protocol *incentivizes* miners/validators to pick the highest-fee transactions first (that's how users compete for inclusion). By outsourcing the block production role to block builders, the validator network is made more resilient and the validator set more decentralized.

[7] See, Daian, Phil, Decentralized Crypto Needs You to Be a Geographical Decentralization Maxi, March 2023, available here: https://collective.flashbots.net/t/decentralized-crypto-needs-you-to-be-a-geographical-decentralization-maxi/1385

As the Bank for International Settlements noted, in traditional markets orders are sequenced by time by a central intermediary, but in a blockchain, block production is a competitive process – who gets to make the block is random or stake-based, and that winner can include transactions in whatever order yields the best reward.[8] This, a functional market for block building, is what allows for block ordering without any central authority.

Crucially, nothing in this process violates the protocol's rules or consensus. All transactions still have to be valid and pay the required fees; no one is stealing funds or forging transactions. MEV extraction is permissionless – a form of competition enabled by the network's transparency and the fact that multiple transactions are in flight at once. One might say *MEV is a side-effect of Ethereum's decentralization*: no single clock or gatekeeper orders transactions, so economic incentives fill that gap. This is why MEV does not inherently amount to an exploit or manipulation, but rather a form of latency arbitrage native to blockchains.

D. MEV's Role in Efficient Blockspace Allocation and Mitigating Congestion and Fee Volatility

One way to view MEV is as a mechanism for price discovery and allocation of scarce blockspace. Each Ethereum block has limited space for transactions. When demand is high and each slot in a block is contested, there must be a way to decide who gets in and who waits.

Prior to the current MEV-auction infrastructure, users spammed (i.e. submitted a massive number of transactions in a short timeframe) high-fee transactions to the public mempool. That led to inefficient outcomes – massive congestion, lots of failed or canceled transactions, and volatile gas prices.[9] For instance, during the "DeFi Summer" of 2020, gas prices would skyrocket due to bots constantly outbidding each other to be first in line for lucrative trades, often reaching hundreds of Gwei and causing regular users' transactions to stall. This made transaction inclusion very unpredictable – a user might set a fee they thought was high, only to see the target gas price double in seconds as two arbitrage bots battled.

With the introduction of off-chain MEV auctions, much of this competition moved off the network. Instead of bidding up the *public* gas price in the mempool, searchers started bidding through private auctions and directly to builders. The result was a notable drop in spam and more stable fees for users. A Flashbots report highlighted that these private orderflow auctions eliminated many failed transactions and artificially inflated fees, leading to a smoother user experience.[10] Essentially, MEV infrastructure turned a chaotic, implicit competition into an explicit, organized market.

---

[8] Raphael Auer, Jon Frost and Jose Maria Vidal Pastor, Miners as intermediaries: extractable value and market manipulation in crypto and DeFi, June 16, 2022, available here: https://www.bis.org/publ/bisbull58.pdf

[9] See, Chris Maree, Unbundling MEV Supply Chain Part 1: History and Evolution, March 7, 2024, available here: https://blog.hack.vc/unbundling-mev-supplychain-part-1-history-and-evolution/

[10] https://docs.flashbots.net/flashbots-auction/overview

By extracting MEV, block producers are creating an efficient market for blockspace where every bit of block capacity finds the highest bidder.[11] Under-provisioned blockspace (where demand far exceeds supply) inherently causes high fees; MEV doesn't eliminate that, but it ensures that whoever values the space most gets it. From the network perspective, by removing spam and wasted transactions, more of each block is filled with useful transactions. In periods of high DeFi activity, this prevents situations where a valuable liquidation or arbitrage is missed (which could have knock-on effects like unbalanced prices or insolvent loans). Moreover, MEV revenue (the payments from searchers to proposers) gets distributed to validators, which strengthens the incentive to participate in securing the network.

III. Types of MEV

There are many different types of activities that can be categorized as MEV. Most of the actions make the ecosystem more robust and prices more accurate, benefiting market participants. While certain types of MEV in their current implementation create negative externalities, we highlight various technological advances which we believe will mitigate these externalities.

A. Arbitrage, or Loss-vs-Rebalancing

Unlike US securities exchanges like the New York Stock Exchange, where liquidity is effectively orphaned on-exchange, and trading happens predominantly during trading hours on weekdays – crypto markets are global, and trade 24/7, with liquidity spread across innumerable centralized and decentralized venues. Further, the decentralized exchanges that power most of this activity generally do not use Central Limit Order Books the way a traditional securities exchange would – instead, Automated Market Makers, or AMMs, enable users to swap between pools of assets based off each pool's mathematical relation to the other (e.g. when a user wants to swap $15 of USDC for ETH, the user deposits USDC in the smart contract comprising the USDC pool, and then is able to withdraw an amount of ETH from the corresponding ETH pool based on the relative balances held by the AMM). Anyone can contribute their own assets to these pools. In other words, "trading" on AMMs is really just rebalancing of asset pools, governed by self-executing code, without any intermediaries or direct counterparties.

Given their decentralized design, and emphasis on incentives to drive distributed network coordination, crypto markets rely on market makers and arbitrageurs to resolve dislocations between asset prices on centralized and decentralized trading venues, buying on one venue and selling on another, to capture the spread. In doing so, there is effectively a "global best bid and offer" on crypto

[11] For example, suppose there's an arbitrage opportunity that will net $1,000 profit. A searcher is willing to pay, say, $900 in fees for it (keeping $100 profit). If that arbitrage transaction fits in the block, it will outbid other transactions for gas space, but it also creates value by arbitraging markets (potentially bringing prices back in line across exchanges). The block builder who includes it gets $900 that blockspace wouldn't have otherwise yielded. If the builder didn't include it (say out of a notion of fairness to time ordering), the opportunity might go to waste – or be picked up in a later block by someone else. Either way, not including it would mean the block earned less in fees.

assets as a result of raw economics and market forces. This arbitrage can be between centralized and decentralized exchanges (CEX-DEX), between two or more decentralized exchanges (DEX-DEX) or even between two or more pools in the same decentralized exchange. The value that market makers are willing to pay block producers to include their transactions in blocks swiftly enough to capture these spreads is one of the most common forms of MEV. CEX-DEX arbitrage remains the most valuable source of MEV for blockbuilding on Ethereum by a significant margin.[12] When a searcher arbitrages a price difference between decentralized exchanges, they are forcing the prices to realign, which benefits everyone trading after them (the markets sync up closer to fair value).

While some arbitrage-based MEV is inevitable and useful for the functioning of these markets, researchers and market participants agree that it would be valuable to reduce the costs imposed by it. This is an active area of research.

B. Liquidations

Decentralized lending protocols such as Compound and Aave enable users to lend and borrow digital assets through autonomous smart contracts, eliminating the need for traditional financial intermediaries. Lenders contribute assets like ETH or stablecoins into liquidity pools and, in return, receive receipt tokens that represent their liquidity pool positions (which they can then later return, and "burn", to retrieve their pooled assets). Borrowers, by contrast, must provide collateral (some other digital asset valued at greater than the value of their loan) to secure loans. Should the value of their collateral fall below a specified threshold, the position becomes subject to liquidation—a foundational safeguard designed to preserve the solvency of the protocol and protect depositors from loss.

MEV is critical in enabling timely and efficient liquidations. When a borrower's position becomes undercollateralized—typically due to price volatility or accrued interest—external actors, often automated bots, are incentivized to repay the outstanding debt in exchange for a portion of the collateral at a discount. MEV strategies allow these participants to compete for liquidation opportunities by bidding for transaction priority within blocks. This competitive process ensures that distressed positions are resolved within seconds of becoming at-risk, thereby preventing the accrual of bad debt and maintaining the protocol's financial integrity. MEV in this context plays a constructive and stabilizing role, leveraging market incentives to uphold the health, transparency, and resilience of decentralized financial infrastructure.

C. Transaction MEV

On the other end of the spectrum is the form of MEV described in the canonical Ethereum is a Dark Forest by Dan Robinson and Georgios Konstantopoulos.[13] Searchers scan the public mempool (as discussed earlier, effectively the transaction "waiting room", where transactions queue up for inclusion in blocks)

[12] https://libmev.com/

[13] Robinson, Dan and Georgios Konstantopolous, *Ethereum is a Dark Forest*, Paradigm blog (8.28.2020), available here: https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest

for MEV opportunities. For example, a buy order on a DEX in a low-liquidity pool presents an opportunity for a "sandwich attack"; whereby a transaction to buy that asset *before* the targeted transaction (the "frontrun") and a transaction to immediately sell that asset *after* the targeted transaction (the "backrun"), paying sufficient priority fee to ensure that their transactions are prioritized appropriately to execute their desired intent. As a result, the searcher can capture some of the value from the price dislocation caused by the trading strategy at the expense of the trader. And then there is "backrunning", a third type of transaction MEV: backrunning involves inserting a transaction behind a large order that has moved the price substantially (typically on an AMM), profiting by moving the price back in line with a global equilibrium.

Frontrunning and sandwiches can implicate execution below the quoted price for traders and enable sophisticated actors to profit from the transparent nature of the network to extract value.[14] Conversely, backrunning can be used as a mechanism for users to re-capture value that might otherwise be leaked to other MEV actors. As discussed above, given that transactions submitted to the mempool lack an explicit order until they are arranged in a block and proposed, this is using economic forces to influence the *ordering* of transactions, rather than *re*-ordering transactions. And, critically, where a problem exists, the market provides a solution – or, in this case, many solutions.[15] As with all things, competition breeds better outcomes for users.

- **Protective Tools:** Two of the most popular MEV protection tools are Flashbots Protect and MEV Blocker. These tools optimize the transaction experience for DEX users by protecting their pre-trade information and providing gas refunds and MEV rebates. DEXs, frontends, wallets, and individual users can set their RPCs to submit transactions through these tools. Tools such as Flashbots Protect share a public end point for searchers that reveals only enough information for arbitrage opportunities, increasing execution predictability for users, but not enough information for sandwich bots to frontrun the transaction. Ultimately, these tools are designed to make MEV searchers compete to return as much value as possible to the user. The result?Up to 90% of the arbitrage opportunity is shared back to the user following inclusion.

- **Direct Validator/Builder Submissions:** Some sophisticated users or protocols form direct links to block builders or validators. For example, a trader executing a multi-million dollar transaction might coordinate with a builder to include it in the next block for a predetermined fee, ensuring it is not front-run. This can be done via the MEV-Boost relay network or even by running one's own builder. The Builder API that Ethereum clients support (via MEV-Boost) allows anyone to submit a payload for consideration. While regular users don't usually submit entire blocks, some are experimenting with user-driven block building (especially on L2s with proposer ordering rules). The net effect is a richer landscape of

[14] All transactions take place within the range of a user's market order, also known as their set "slippage". All sandwiches are in the range of slippage set by users. A transaction would not land onchain if it were to execute outside the user-set slippage of their market order.
[15] Interestingly, many Layer 2 networks lack mempools, and thus do not have prevalent sandwich activity.

orderflow auctions – not just one public auction (the mempool) but many private ones.

- **MEV Dashboards and Monitoring:** Transparency has improved with tools that let anyone observe MEV activity in real time. For instance, Sorella Labs provides a real-time MEV dashboard that classifies each Ethereum block's extracted MEV.[16] Their backend, called Brontes, analyzes blocks to detect common MEV strategies (arbitrages, sandwich attacks, liquidations, etc.) and streams this info live.[17] A user or researcher can look at such a dashboard to see, for example, which builder won the latest block, how much MEV was in it, and what types of strategies were executed. Other platforms and community dashboards (on Dune Analytics, etc.) track metrics like the percentage of blocks sourced from Flashbots, the total MEV extracted per day, and how many transactions bypassed the public mempool. All these give legal and technical observers insight into the MEV market as it unfolds.

- **Decentralizing Builders:** While MEV-Boost market structure has successfully alleviated network congestion issues and centralizing forces on the validators set, over time certain blockbuilders have begun to win a disproportionate number of block inclusion auctions. The market has responded to this trend and introduced a technological innovation to addresses growing concerns of centralization. Flashbots, together with Beaverbuild (a large blockbuilder) and Nethermind (an Ethereum research and engineering organization and supporter of the Nethermind Ethereum node implementation), recently developed BuilderNet, a decentralized network of blockbuilders.[18] BuilderNet leverages advances in Trusted Execution Environments (TEEs) – encrypted enclaves where execution occurs, but is cryptographically verifiable by third parties – and introduces a multioperator system where multiple parties can operate the same blockbuilder by running instances of that open source builder in a TEE, which apps and users can then route their transactions to. Thus, there is joint simultaneous operation of a single blockbuilder. Ultimately, the objective is to have an efficient and fully decentralized blockbuilding landscape.

These developments indicate a maturing ecosystem where MEV is competitive but also cooperative: users, searchers, builders, and validators are finding arrangements that share value and reduce harm. In effect, this ecosystem provides balance and improved outcomes despite or even because of the existence of many competing traders and differing trading strategies. It is a microcosm of how decentralization makes things both stronger and better. This steady, constructive evolution in block production market structure is the very reason that flexibility in approach is required for these technical solutions to continue to develop.

[16] Sorella Labs is a Paradigm portfolio company.
[17] See, Sorella Labs Dashboard, available here: https://sorellalabs.xyz/dashboard
[18] See, "Introducing Buildernet," available here: https://buildernet.org/blog/introducing-buildernet

IV. Legal Analysis

Some of the policy discussions about MEV have compared certain MEV strategies to behaviors that could be unlawful in traditional securities markets, such as front-running client orders. Below, we examine why MEV on Ethereum does not amount to securities fraud or insider trading under U.S. federal securities laws. We also evaluate MEV in light of U.S. best execution obligations.

A. MEV and Securities Fraud

The Bank for International Settlements (the "**BIS**"), the International Organization of Securities Commissions ("**IOSCO**"), the International Monetary Fund (the "**IMF**") and the Financial Stability Board (the "**FSB**") have all broadly analogized MEV extraction to *market manipulation or abuse* in conventional markets.[19] For example, a BIS bulletin observed that Ethereum validators "open[] the door to front-running and other forms of market manipulation," noting that in most jurisdictions such front-running is illegal.[20] However, as discussed in this section, these analyses are fundamentally flawed because they fail to account for the critical differences between traditional finance and crypto markets, including the different systems for determining transaction priority. When analyzing specific claims, it's clear that MEV does not meet the required elements of securities fraud or insider trading.

1. Applicable statutes, rules and elements of a claim

Section 10(b) of the Securities Exchange Act[21] and SEC Rule 10b-5[22] broadly prohibit the use of "any manipulative or deceptive device or contrivance" in connection with the purchase or sale of securities. To successfully find that a defendant is liable for fraud in violation of Rule 10b-5, a plaintiff must plead and prove:

1. The defendant engaged in a **manipulative** or **deceptive** act.[23] To state a claim that a defendant engaged in market manipulation under Rule 10b-5, the plaintiff must show that the activity was intended to deceive investors about how other market participants value a security.[24]

[19] Tom Momberg & Angela Angelovska-Wilson, Regulating the Unseen: Limiting the Potential for Negative Externalities from MEV Realization, October 22, 2024, available here: https://dlxlaw.com/leaderships_blog/regulating-the-unseen-limiting-the-potential-for-negative-externalities-from-mev-realization/

[20] Raphael Auer, Jon Frost and Jose Maria Vidal Pastor, Miners as intermediaries: extractable value and market manipulation in crypto and DeFi, June 16, 2022, available here: https://www.bis.org/publ/bisbull58.pdf

[21] 15 U.S.C. § 78j(b).

[22] 17 C.F.R. § 240.10b-5.

[23] , 485 U.S. 224, 232 (1988) (quoting
, 426 U.S. 438, 449 (1976)).

[24] Prohibited activities include illegitimate, sham, or inherently deceptive conduct where a defendant aims to create a false appearance of market activity, such as:

- Disseminating false or misleading financial statements about the company's profits or losses (see, for example, Pub. Pension Fund Grp. v. KV Pharm. Co., 679 F.3d 972, 986 (8th Cir. 2012)).

2. **Scienter**, which is defendant's knowledge that an act or conduct is wrongful and the defendant's intent to act despite this knowledge.[25] In market manipulation cases, scienter is often the only factor that distinguishes legitimate trading activity from improper manipulation.

3. **Reliance** by the investors on the manipulative or deceptive act when making investment decisions.[26]

4. **Economic loss** suffered by investors.[27]

Insider trading is one type of "device, scheme, or artifice to defraud" enforced under Section 10(b) and SEC Rule 10b-5. The law emerged from the principle that violating the relationship of trust and confidence that exists "between the shareholders of a corporation and those insiders who have obtained confidential information by reason of their position with that corporation" amounts to fraud.[28] Insider trading violations may also involve securities trading by individuals who misappropriate material nonpublic information.[29]

In the context of an insider trading claim under Section 10(b) of the Exchange Act and Rule 10b-5, a plaintiff must plead and prove:

1. A breach of a **fiduciary duty** or other relationship of trust and confidence. As discussed above, the two broad theories that define the types of duty that, when breached, can lead to insider trading violations are: (A) the *classical theory* of insider trading, which states that liability arises for corporate officers or insiders who owe a fiduciary duty to the company and its shareholders;[30] and (B) the *misappropriation theory* which rests on a duty of trust and confidence that the person making the trade owes to the source of the confidential information.[31]

2. The use or possession of **material, nonpublic information** in connection with the purchase or sale of securities.

- Ponzi schemes, which typically provide quick payments to investors in a nonexistent enterprise from money supplied by later investors (see, for example, In re J.P. Jeanneret Assoc., Inc., 769 F. Supp. 2d 340, 347 (S.D.N.Y. 2011)).
- Creating and distributing research reports that include false or misleading information about a company (see, for example, In re Galena Biopharma, Inc. Sec. Litig., 117 F. Supp. 3d 1145, 1198-99 (D. Or. 2015)).

[25] See, *Aaron v. SEC*, 446 U.S. 680 (1980); *Ernst & Ernst v. Hochfelder*, 425 U.S. 185 (1976).
[26] See, e.g., *In re Garrett Motion Inc. Sec. Litig.*, 2022 WL 976269, at *17 (S.D.N.Y. Mar. 2022).
[27] See, e.g., *Fezzani v. Bear, Stearns & Co. Inc.*, 716 F.3d 18, 22-23 (2d Cir. 2013).
[28] *United States v. O'Hagan*, 521 U.S. 642, 651-52 (1997)
[29] Insider trading claims most commonly are based on alleged violations of Section 10(b) of Exchange Act, 15 U.S.C. § 78j(b), and its implementing regulation, Rule 10b-5, 17 C.F.R. § 240.10b-5. However, these types of claims also can be pursued under other Exchange Act provisions as well as other statutes, including: Rule 14e-3 under the Exchange Act, 17 C.F.R. § 240.14e-3a, Section 20(a) of the Exchange Act, 15 U.S.C. § 78t(a). Federal prosecutors have brought insider trading claims under criminal statutes prohibiting mail, wire, and securities fraud. (see 18 U.S.C. §§ 1341, 1343, 1348.
[30] *Chiarella v. United States*, 445 U.S. 222, 228-29 (1980).
[31] *United States v. O'Hagan*, 521 U.S. 642, 652 (1997)

3. **Scienter**.

4. A **personal benefit**, for cases where corporate insiders (tippers) pass or "tip" material nonpublic information to outsiders (tippees) who trade based on that information.

In addition, Section 9 of the Exchange Act[32] provides a more targeted prohibition against specific manipulative trading practices. These deceptive schemes are designed to create a false impression of market activity and ultimately influence the price of a security. Classic examples include pump and dump schemes,[33] matched trades,[34] or wash sales.[35]

To establish a Section 9 violation, the plaintiff must plead and prove:

1. **Manipulative** activity.

2. **Scienter**.

3. Purposeful **inducement**, meaning that the manipulative activity was conducted specifically to induce others to buy or sell the security.

4. **Reliance**.

5. **Effect on the price**, meaning that the manipulative affected the price at which the plaintiff bought or sold the security.[36]

2. Analysis

Suppose, for the sake of argument, we assume that the MEV transactions in question involve the trading of securities and satisfy the requisite jurisdictional means. Notwithstanding, we argue that the MEV activity we describe above would not violate Section 10(b) of the Exchange Act, Rule 10b-5 or Section 9 of the Exchange Act.

---

[32] 15 U.S.C. § 78i.

[33] These schemes involve artificially inflating the price of a security through artificial trading activity of buying the security while disseminating false or misleading statements or promotional campaigns to the public. This manipulative activity creates a false impression of market activity which allows the manipulator to then sell the security at the inflated price to unsuspecting investors. See, e.g., SEC v. Stubos, 634 F. Supp. 3d 174, 202-03 (S.D.N.Y. 2022).

[34] Matched trades involve placing pre-arranged buy and sell orders for a security of substantially the same size, time, price in the same security on a national securities exchange. The coordinated trading activity is designed to artificially inflate or depress the stock price. See, e.g., SEC v. Fiore, 416 F. Supp. 3d 306, 316 (S.D.N.Y. 2019).

[35] Wash sales involve an investor simultaneously buying and selling the same security with no change in beneficial ownership. This trading activity is designed to create the illusion of trading activity stock. It can also be used to generate artificial losses for tax purposes, allowing the investor to claim deductions they otherwise would not be entitled to take. See, e.g., SEC v. Masri, 523 F. Supp. 2d 361, 366-67 (S.D.N.Y. 2007).

[36] See, e.g., Dekalb Cnty. Pension Fund v. Transocean Ltd., 817 F.3d 393, 403 (2d Cir. 2016); AnchorBank, FSB v. Hoefer, 649 F.3d 610, 616-17 (7th Cir. 2011).

a) MEV does not involve the scienter required for claims under Section 10(b), Rule 10b-5 or Section 9

As described above, any claim under Section 10(b) of the Exchange Act, Rule 10b-5 or Section 9 of the Exchange Act would require a showing that the relevant MEV participant employed manipulative or deceptive acts and did so with scienter. However, the MEV activity we describe above does not meet this standard. Consider for example a searcher that implements a "sandwich attack." This searcher operates using public information in the mempool, exploiting transparency and speed to "frontrun" a market moving transaction, and profit with a "backrun". However, the searcher is not intentionally creating a false impression of market activity.[37] To identify conduct that is "unrelated to the natural forces of supply and demand,"[38] courts assess whether the subject transactions convey "a false pricing signal to the market."[39] Here, the searcher is not deceiving others with falsities (including the trader that got sandwiched) or creating the appearance of a false trading activity like spoofing or wash trading: they are submitting real economic transactions.

Or consider a blockbuilder that is assembling transactions from the public mempool and private searcher bundles for maximum profit. As discussed above, blockchain transaction ordering does not operate under the same assumptions as traditional markets, and behavior that is manipulative in a first-in-time, order-protected market is not so in Ethereum. Unlike on an exchange with time-priority rules, Ethereum has no inherent rule promising that earlier-submitted transactions execute first. The protocol explicitly allows a blockbuilder to prioritize transactions that pay a larger tip over transactions that were submitted first to the mempool. In that sense, what looks like manipulation (jumping the queue) might be considered a built-in feature of the system's design (a fee auction for blockspace).[40]

b) MEV does not involve a breach of fiduciary duty or misappropriation of material nonpublic information required for an insider trading claim

Nor does MEV activity inherently meet the standard of insider trading since it does not involve a duty under either the classical or misappropriation theory, nor any nonpublic information. MEV actors do not have any explicit fiduciary duty to network users broadcasting transactions. MEV actors like searchers or blockbuilders are also not in a position to take advantage of agency relationships

---

[37] See, e.g., *ATSI Communications, Inc. v. The Shaar Fund, Ltd.*, 493 F.3d 87 (2d Cir. 2007); *Pagel, Inc. v. SEC*, 803 F.2d 942 (8th Cir. 1986); *Markowski v. SEC*, 274 F.3d 525 (D.C. Cir. 2001).

[38] *Mobil Corp. v. Marathon Oil, Corp.*, 669 F.2d 366, 274 (6th Cir. 1981).

[39] *ATSI Communications, Inc. v. The Shaar Fund, Ltd.*, 493 F.3d 87 (2d Cir. 2007)

[40] It's important to distinguish the actions of MEV actors such as searchers or block builders from the alleged actions of the defendants in United States v. PERAIRE-BUENO, 1:24-cr-00293, where the defendants were changed with conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering. According to the indictment, the defendants exploited a vulnerability in the MEV-Boost software allowing them to access and alter pending private transactions. In contrast, searchers or block builders are operating according to the understood protocol rules.

or information asymmetries such that a court would impose an implicit fiduciary duty.

MEV actors such as searchers or blockbuilders are also not misappropriating any confidential information that violates a duty of trust. In fact, Ethereum's public mempool means that pending transaction information is openly available to anyone monitoring the network. If a searcher bot sees a user's Uniswap trade in the mempool and decides to execute a sandwich, the information (the trade size, asset, etc.) was publicly visible. It's not "insider" information in the legal sense; there is no breach of confidence, because the trader voluntarily broadcast the transaction to a public network. Absent a duty of confidentiality, merely possessing information (even if it gives a trading edge) is not illegal. As the Supreme Court made clear in *Dirks* and *United States v. O'Hagan*, insider trading liability hinges on misappropriating information or breaching a fiduciary-like duty.[41] In short, the typical MEV scenario – exploiting publicly available mempool data – does not fall under the classical definition of insider trading, because the information used (pending orders) is not nonpublic. It's akin to high-frequency traders in equities who glean cues from public order flow; that might raise fairness concerns, but it isn't insider trading since they didn't steal or improperly obtain the information.

B. MEV and Best Execution

1. Applicable statutes, rules and elements of a claim

The duty of best execution is a foundational principle under federal securities law that reflects the broader investor protection goals of the U.S. securities laws. The obligation is derived from a combination of Financial Industry Regulatory Authority (FINRA) rules, SEC oversight and longstanding common law fiduciary duties. At its core, the best execution requirement mandates that broker-dealers use reasonable diligence to ensure that customer orders are executed under the most favorable terms reasonably available, considering price, speed, and other relevant factors at the time of execution.

The primary rule governing best execution in the U.S. is FINRA Rule 5310, which explicitly requires broker-dealers to seek the best market for a customer's order and to execute that order so the resulting price is as favorable as possible under prevailing market conditions.[42] This rule outlines several factors broker-dealers

[41] Dirks v. SEC, 463 U.S. 646 (1983); United States v. O'Hagan, 521 U.S. 642 (1997).

[42] "(a)(1) In any transaction for or with a customer or a customer of another broker-dealer, a member and persons associated with a member shall use reasonable diligence to ascertain the best market for the subject security and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions. Among the factors that will be considered in determining whether a member has used "reasonable diligence" are:

(A) the character of the market for the security (e.g., price, volatility, relative liquidity, and pressure on available communications);
(B) the size and type of transaction;
(C) the number of markets checked;
(D) accessibility of the quotation; and
(E) the terms and conditions of the order which result in the transaction, as communicated to the member and persons associated with the member."

must consider, including the character of the market, order size, and the number of markets checked. Importantly, best execution does not require always obtaining the lowest price, but rather making a diligent effort to evaluate and access the most advantageous execution based on a range of criteria. Broker-dealers are also expected to regularly review their execution quality and order routing practices to ensure continued compliance.

In addition to FINRA rules, SEC regulations such as Regulation NMS (National Market System) reinforce best execution principles. Rule 611,[43] the Order Protection Rule, prevents "trade-throughs" by requiring that trades be executed at the best displayed price across all national exchanges. Further, SEC Rule 606[44] imposes public disclosure requirements on broker-dealers regarding their order routing practices and any receipt of payment for order flow (PFOF), a practice that can create potential conflicts of interest. Broker-dealers must ensure that such conflicts do not compromise their duty to seek best execution for their customers.

Finally, a broker-dealer's obligation to obtain best execution of a customer's order in any security is based, in part, on the common law agency duty of loyalty, which obligates an agent to act exclusively in the customer's best interest. That's why behavior like a broker trading ahead of a client ("front-running") or secretly adding a markup is forbidden: it deprives the client of the best price available.

2. Analysis

In the current DeFi landscape, users often transact without any intermediary owing them a fiduciary or best execution duty. For example, a searcher that "frontruns" a large transaction in the public mempool does not owe the party that broadcasted that transaction a best execution duty. While regulators, including the SEC, have previously hinted that certain DeFi front-ends and wallets could be deemed to be broker-dealers (and thus be subject to a best execution duty), courts have so far held that noncustodial products do not meet the definition of broker-dealers.[45] In other words, best execution is a concept tied to intermediaries who owe duties to investors; decentralized and noncustodial infrastructure is not subject to best execution duty.

However, an SEC registered broker-dealer that facilitates customer trades in tokenized securities via a DEX on Ethereum would still owe a duty of best execution. Therefore, it would need to assess the execution quality on the DEX, including the likelihood of slippage and risk that its transactions may be "sandwiched" by a searcher. For instance, if a retail broker-dealer allowed a client's order to be systematically sandwiched on an exchange when alternatives existed, regulators may find a failure of best execution. The best execution duty

---

[43] 17 CFR § 242.611.
[44] 17 CFR § 242.606.
[45] SEC v. Coinbase, No. 1:23-cv-04738 (SDNY) at 82-83 ("The SEC does not allege that Coinbase performs any key trading functions on behalf of its users . . . Coinbase has no control over a user's crypto-assets or transactions via Wallet . . . while Wallet helps users discover pricing on decentralized exchanges, providing pricing comparisons does not rise to the level of routing or making investment recommendations.").

compels intermediaries to consider factors like price improvement and market impact; knowingly sending orders into a public mempool where it's likely to be sandwiched by an MEV bot could violate that duty if better options are reasonably available.

However, there is nothing inherent in the block production supply chain or MEV that would prevent the broker from meeting its obligations. For example, the broker might use MEV mitigation techniques, including splitting orders, using a private mempool, or seeking out trading venues that utilize forms of MEV protection – whether that is a venue with native protection, such as CoW Swap, or other DeFi frontends that have embedded solutions like Flashbots Protect.

In other words, a regulated broker can't simply ignore MEV, but the dynamic nature of market structure and trading technology continues to shape the scope of this obligation, requiring firms to adapt their practices accordingly.

V. Conclusion

The market continues to provide solutions for each successive issue around efficiency or execution, and regulators should thus be judicious in how they choose to address MEV and the blockbuilding supply chain.

For one, the Commission could consider opt-in disclosure guidelines for DeFi frontends (user interfaces that are webhosted by development companies, rather than the self-executing protocols themselves) that wish to attract the trading activity of Commission registrants, describing what technical approaches or third-party software that venue uses to mitigate MEV. In so doing, registrants can make informed decisions that will best suit their best execution duties to their clients.

Additionally, to encourage that these networks continue to trend towards decentralization, the Commission may consider whether guidance should be issued around whether entities registered with the Commission as exchanges (whether currently, or under some future market structure legislative framework) are also allowed to operate blockbuilders on Layer 1 networks, to avoid centralizing forces and any potential conflicts of interest.

Ultimately, these baselayer markets are still quite nascent, with significant research and risk capital invested in making them increasingly more efficient. While the Commission has a duty to protect investors and consumers, its duty to promote capital formation and foster innovation must take precedence here, and any guidance the Commission might choose to issue should take a "first, do no harm" approach, and trend towards flexible principles, rather than ossifying requirements. Continued neutrality of the baselayer is imperative for the further development of these decentralized protocols, and egalitarian access by their users.

—---

Acknowledgments

Thank you to Reid Yager, Dan Robinson, Katie Biber, Justin Slaughter, and Gina Moon for review and feedback.