I. Introduction: MEV And The Base Layer

Blockchain networks[1] are generally designed in an attempt to preserve the neutrality of the base layer actors. This principle of "**base layer neutrality**" is as fundamental to blockchain networks as neutrality is to the internet more broadly. This principle asserts that a blockchain network's foundational layer and the actors involved—responsible for ordering database transactions and publicly recording them in data blocks—must operate without prejudice to maintain network integrity and functionality.

The actors that comprise a blockchain network's base layer (as "**base layer actors**") execute functions akin to those performed by IT infrastructure or network providers in their role of allocating public goods necessary for communications, data transfer, and data storage. Base layer actors include, for example, miners in proof-of-work ("**PoW**") systems,[2] validators in proof-of-stake ("**PoS**") systems,[3] and operators of authorized nodes in proof-of-authority ("**PoA**") systems.[4] While these are only three examples that underlie an even more diverse array of blockchain networks and associated actors, they underscore the role of base layer actors in achieving consensus.

These blockchain networks function not just as technology, but as major economic ecosystems. Economic security forms the bedrock of blockchain networks, underpinning their resilience, integrity, and decentralization. In most blockchain networks, block rewards and gas fees[5] serve as the primary economic incentives for base layer actors to support the underlying network's

---

[1] A "blockchain network" is a decentralized database maintained across a network of nodes (*i.e.*, computers), which, through a specific consensus mechanism (*see, e.g.*, *infra* note 2, 3, 4), collectively update the database. When referring to blockchain networks, this paper is referring primarily to internet-based blockchain networks that are open and 'permissionless.' Unlike permissioned networks, which have transaction ordering rules limiting third-party MEV opportunities, permissionless networks support general computing activities, most often including but not limited to financial transactions.

[2] In PoW systems, miners secure the blockchain network by solving complex computational puzzles, incentivized by block rewards and transaction or 'gas' fees. This process, while energy-intensive, ensures network integrity through computational expenditure.

[3] PoS systems are secured by participants who are either validators themselves or who delegate their digital assets to validators, which ultimately stake native digital assets as collateral to help establish trust in the network's base layer. This mechanism aligns validators' economic incentives with the network's long-term health, where any malicious actions would jeopardize their stake.

[4] PoA systems rely on a limited number of authorized nodes to securely propose and validate each block on the network, where trust is widely placed in the nodes because they are operated by vetted actors.

[5] "Block rewards" are incentives allocated to base layer actors for their role in securing and operating a blockchain network, typically consisting of newly minted or unlocked digital assets and possibly transaction fees. The structure of block rewards varies across blockchain networks, depending on the consensus mechanism in place. "Gas fees" are payments made by users to cover the computational costs of executing and validating transactions on a blockchain network. These fees fluctuate based on network demand and transaction complexity, serving to deter spam and compensate base layer actors for their computational efforts. Both mechanisms are crucial for the functioning and security of blockchain networks, influencing the behavior and economic strategies of base layer actors.

aims in scalability, decentralization, and security.[6] The base layer actors record messages on a blockchain network by coming to an agreement (*i.e.*, "**consensus**") on updates to the network's state (each state update, a "**block**"), and are thus trusted with maintaining economic security by securely and efficiently recording "**messages**"[7] on the network.

Blockspace is a core commodity on blockchain networks as each block has limited capacity and users' messages must be ordered within each block. While each blockchain's technical design dictates the size of each block, blockchains are generally agnostic with respect to how messages are ordered within blocks.

"**MEV**" (sometimes referred to as "miner extractable value" or "maximal extractable value") refers to the maximum value that can possibly be realized from a given block[8] as a result of the most optimal and efficient contents and order of messages within that block. By this definition, MEV is generated by the users of a blockchain network based on where, when, and how they transact and submit messages to the network.

The amount of MEV realized in a given block is a function of both (i) the messages that are included in a given block; and (ii) the way that the included messages are ordered in the block. In this way, MEV serves as a measure of a blockchain network's efficiency in handling and prioritizing messages within the limited space of a block, especially as volumes may fluctuate. Not all database transactions can be processed immediately or in the order they are submitted, so MEV ought to be conceptualized more broadly as a tool to understand how transaction priority affects a network's efficiency, and therefore overall health, security and resiliency.

If base layer actors must prioritize the economic security of the network, then they will naturally do so by engaging in maximal value-optimizing strategies. If base layer actors do not maximize MEV realization, then other potentially adversarial actors will execute profit-seeking strategies. The resulting imbalances among base layer actors could risk the economic security and resilience of networks, including the potential for consensus attacks, geographic concentration, and other consolidations of power that could lead to arbitrary or inappropriate rejection or prioritization of certain database transactions.

For these reasons, interested parties must understand that while MEV can and often does affect transaction ordering, it does not necessarily equate to what some call "frontrunning" or any

---

[6] Scalability, decentralization, and security comprise the blockchain network trilemma, referring to the challenges that developers face in creating blockchain-based systems. Decentralization demands the use of consensus to verify transactions, as opposed to a centralized body in traditional financial markets. Scalability enables the blockchain to provide an ecosystem for growth and wide-spread adoption without constraints. Security prevents hackers from attacking the source code that makes up the underlying blockchain. These three principles make up the foundation of blockchain network development.

[7] "Messages" are commands or instructions transmitted on the blockchain. Messages may contain transaction instructions.

[8] "Blocks" contain datasets which consist of timestamps and encrypted details concerning recent database transactions, which require validation by the network prior to being incorporated into a blockchain.

other form of “targeted trading.”[9] They can be carried out by otherwise neutral base layer actors to ensure the market for blockspace remains efficient and the underlying blockchain remains healthy and secure.

By framing the discussion against the backdrop of how the base layer actually works, we can shed light on the rational behaviors of the actors within various blockchain-based environments (even when they engage in activities that might introduce challenges or potentially negative externalities). The base layer actors and other participants that might attempt to realize various MEV opportunities typically operate rationally within the parameters of underlying market systems, navigating opportunities and constraints presented by the architecture of a given blockchain network or protocol.

The evolution of MEV strategies reflects the ongoing maturation of blockchain technology and the digital ecosystems this technology supports. As these strategies become more sophisticated, they not only test the resilience and adaptability of existing legal frameworks but also highlight the need for a nuanced understanding of blockchain economics. This paper, therefore, advances a dual narrative: one that explores developments in MEV as a critical component of blockchain innovation, and another that considers the implications of these developments.

Thus, this paper seeks to explain how block construction on public blockchains works, as well as the various incentives that motivate behavior in the market for blockspace. Much of the discussion advanced in this paper is rooted in the principle of economic allocation of scarce resources, offering a perspective that situates MEV-related activities within a broader dialogue about market dynamics and the economic rationale driving the actions of participants in various blockchain networks.

After providing this background, we also advance the following MEV fair market principles, explained in more detail below:

- Allow open blockchain communities to flourish by innovating solutions themselves.
- Advance Network Neutrality
- Encourage Broad Participation
- Ensure Transparency and Accountability
- No manipulation of blocks once proposed
- Respect Privacy and Data Security
- Promote End User Awareness and Education
- Drive Toward Long-Term Network Stability and Market-Efficient Outcomes

[9] For a description of what this paper refers to as “targeted trading” activities, *see infra* note 12.

In following some of the considerations discussed in this paper, blockchain network and application developers ought to be able to harness the benefits of a decentralized execution environment and adopt strategies that both curb the potential for disruptive behaviors and at the same time strengthen economic security.

II. Understanding MEV

As mentioned above, each block has limited capacity and users' messages must be ordered within each block. This fact in and of itself creates MEV opportunities.

Each blockchain network's participants will have to identify the tools, systems, and decisions for how to address MEV. While some forms of MEV have different downstream implications than others, it is likely that MEV cannot be removed at this stage of maturity, and the prohibition of certain types of MEV can harm a system's overall resilience towards mitigating negative externalities.

There are three fundamental characteristics of blockchain networks that suggest why it might be impossible to ever completely remove MEV from from public blockchains:[10]

1. **Transcriptability**: Blockchain networks must be auditable. This typically occurs by creating transcripts, or proof arguments, that can be validated by others. This opens the door to MEV, as there will always be users that prefer one version of events to another, and create economic incentives to encourage that version being recorded.

2. **Interoperability**: The interaction between different blockchain networks creates MEV opportunities. As information flows across networks, financial incentives emerge to find efficiencies created through onchain actions across networks.

3. **Diverse trust models**: The existence of various fairness protocols and trust assumptions within and across blockchain networks also creates MEV opportunities in addressing differences in trust models for profit.

Base layer actors are economically incentivized to propose blocks for consensus that maximize MEV realization (*i.e.*, optimal maximization of profitability). Although this can lead to overall increased costs for users, developers of protocols underlying most blockchain networks have found ways to balance this profitability motive with network health and security.

---

[10] *See* Phil Daian, *IC3 Initiative for Cryptocurrencies and Contracts: MEV Wat Do*, YOUTUBE.COM (Aug. 9, 2021), https://www.youtube.com/watch?v=9tRLaCE_s9w (explaining that MEV is fundamental to (a) transcriptability, whereby systems need to be auditable to decentralize trust, (b) interoperability, whereby different systems must be able to communicate to ensure data is in sync, and (c) diverse trust models, whereby users rely on no single fairness protocol but consider relevant incentives in choosing among different protocols, each of which is integral to decentralized systems and necessary to create economic incentives in the form of MEV).

For example, MEV opportunities arising directly from base layer actors' ability to prioritize or de-prioritize transactions in an effort to optimize profits is foundational to a blockchain network's economic security and inherent in its *transcriptability*. These kinds of MEV opportunities are typically harnessed to incentivize base layer actors to continuously manage the building, proposal, and confirmation of blocks in a way that fosters an ongoing competitive and decentralized base layer environment.

Sometimes, depending on the systems and incentive structures in place to support a blockchain network, these strategies can lead to potentially disruptive practices this paper refers to as "**targeted trading**."[11] These strategies can expose the network's end users to negative externalities. Nevertheless, targeted trading strategies can largely be limited (if not eliminated) based on the structures of the protocols and MEV-related incentives underlying a blockchain network's consensus and supporting systems.

Targeted trading practices—or, for that matter, any other form of MEV realization that could potentially be considered disruptive to a blockchain network or its users—are not necessarily problematic based on their form. Rather, these forms of MEV realization could be disruptive depending on their effect and the unique purposes and attributes of the given network or system. Other potentially adversarial or disruptive tactics that might be performed by or among base layer actors, like censorship,[12] reorganizations,[13] or multi-slot attacks,[14] are generally considered only theoretically, although restricted technically, based on the development and design decisions that go into a blockchain network's underlying protocols or supporting systems.

Of course, many methods for realizing MEV opportunities are not available exclusively to base layer actors. They may be used by other blockchain network participants[15] to support market efficiency and network security, scalability, and decentralization in additional ways. For example, "**arbitrage**" strategies are crucial to price discovery, convergence, and efficiency in the digital asset markets that blockchain networks make possible. This allows traders to take profits

---

[11] As used in this paper, the term "targeted trading" refers to the practice of leveraging available information about the order of transactions or the contents of unordered transactions to request a competing transaction that benefits from a price differential if ordered first. While this form of targeted trading can often be conflated with the practice of "frontrunning" in traditional financial markets, targeted trading on blockchain networks encompasses broader strategies to take advantage of transaction ordering for profit. "Targeted trading" includes where a transaction is placed ahead of a known future transaction to capitalize on the ensuing price movement, as well as "sandwich attacks," where a trader places transactions both before and after a target transaction to profit from the price impact caused by the target transaction. Although the effects of "backrunning" are not necessarily inherently negative, this method of MEV realization can also potentially be described as targeted trading, where transaction requests might be submitted by a participant immediately after a known profitable trade to capitalize on the initial transaction's market impact.

[12] "Censorship" involves the act of block builders to selectively ignore or delay certain transactions to prioritize others that may yield higher profits, effectively manipulating market outcomes.

[13] A "reorganization" is an adversarial MEV realization strategy that entails altering the blockchain's transaction history to benefit from transactions that are not initially favorable, challenging network integrity.

[14] A "multi-slot attack" exploits vulnerabilities in the timing and ordering of transactions across multiple blocks, allowing attackers to affect outcomes over a broader range of actions for financial gain.

[15] This includes traders on centralized and decentralized exchanges, operators of DeFi lending platforms, and providers of order book liquidity.

based on price differentials among various assets and across different centralized or decentralized exchanges (respectively, "**CEXs**" or "**DEXs**"). The availability of arbitrage opportunities are inherent in the *interoperability* of blockchain networks and therefore will likely continue to grow more complex as networks become increasingly interconnected.

Many other forms of MEV often play crucial roles in the functionality and efficiency of the systems built on top of blockchain networks, such as in decentralized finance ("**DeFi**") or decentralized applications ("**dApps**"). For example, on DeFi lending platforms, the process of loan collateral liquidation requires gas expenditure, a cost effectively borne by traders running self-executing lines of programming (known as "**bots**"). These bots—incentivized by a share of the liquidated collateral as a form of MEV—engage in liquidations and make "**oracle**"[16] updates, effectively ensuring the system remains operable even during spikes in gas costs.[17]

Providers of order book liquidity on DEXs similarly benefit from the realization of MEV where market participants might extend additional rewards to incentivize the liquidity provider to offer up available assets, fostering a more fluid and efficient trading environment. This dynamic also extends to other blockchain-based contracts, such as in connection with games, collectibles, or meme protocols, where MEV enables users to fund gas fees for actions like minting new items or participating in complex game states, thereby enhancing user engagement and platform vitality.

III. A Historical Review Of MEV on Ethereum

Following the initial observations of MEV and the subsequent research into how to address economic security implications, protocol researchers and industry participants have coalesced around strategies and tools to address MEV's impact. In this section, we primarily focus on the evolution of MEV on Ethereum, reviewing the historical decisions and outcomes for MEV mitigation.

Early PoW Ethereum

MEV was formally introduced as a concept related to network security in 2019 by security researchers Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels.[18] The phenomena identified in the paper suggested that as

---

[16] "Oracles" are external data feeds that provide smart contracts with real-time information from outside of a blockchain network. They help play a role in MEV realization, especially liquidation on DeFi lending platforms, by enabling smart contracts to execute trades based on predefined conditions influenced by external market data.

[17] If trading bots were not able to realize this MEV, these lending platforms might either falter under operational inefficiencies or resort to the use of permissioned actors to manage liquidation processes, undermining the foundational principle of decentralization.

[18] Philip Daian et al., *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, Cornell University: Arxiv: Cryptography and Security: Computer Science and Game Theory (Apr. 10, 2019), https://arxiv.org/abs/1904.05234.

application activity on public blockchains grows, economic security assumptions for consensus can be impacted by additional value-optimizing strategies.

Following the discovery of MEV phenomena on early Ethereum, which operated on PoW consensus,[19] this group of researchers sought out ways to relieve some of the effects the MEV realization game had in leading to greater centralization of mining power among miners.[20] The objective was to advance a permissionless and transparent structure that can channel and harness MEV opportunities in a way that alleviates network congestion and protects base layer neutrality and decentralization.[21] This mechanism, known as "**mev-geth**,"[22] allowed miners to trustlessly[23] outsource the tasks of maximizing profits and optimizing the block construction process to separate specialized actors called "**searchers**."[24]

---

[19] The public mempool on PoW Ethereum had often aptly been described as a 'dark forest,' where searchers (as predators) lurk in the shadows waiting to exploit every possible profit-maximizing opportunity generated by novice end users (as unsuspecting victims). Many precursory forms of MEV shield protocols—as described under Section II.B (*User protection interests on Ethereum*)—had been deployed on early Ethereum to reduce users' exposure to potentially disruptive forms of MEV realization and provide them with options for priority message ordering, including using early protected mempool tools offered by organizations like Archer DAO, *assoc. with* Archmev Ltd. (https://www.archerdao.io/), as well as Flashbots, Ltd. (https://www.flashbots.net/) and the former KeeperDAO that is now known as Rook, assoc. with Rook Labs Ltd. (https://rook.fi/en/). Other early solutions to shield users from potentially disruptive forms of MEV realization included Gas Token, *a service of* the Initiative for CryptoCurrencies & Contracts (https://gastoken.io/). Gas Token enabled users to tokenize gas and leverage it for transactions when gas prices were high. This strategy not only enabled users to hedge against gas price volatility but also subtly influenced transaction prioritization by incentivizing miners to select transactions utilizing GasToken due to potentially higher earnings. This would reduce the use of harmful MEV strategies by adjusting miners' economic incentives, leading also to a more efficient network during peak times.

[20] *See* Alex Obadia, *Flashbots: Frontrunning the MEV Crisis*, MEDIUM: NEWS: MEV (Nov. 23, 2020), https://medium.com/flashbots/frontrunning-the-mev-crisis-40629a613752.

[21] Decentralization refers to the transfer of trust in markets from centralized institutions and intermediaries to a dispersed network of neutral actors.

[22] Mev-geth is an Ethereum node implementation that is a fork of Ethereum's "geth" client created by Flashbots, Ltd. (https://www.flashbots.net/) to specifically limit the successful use of certain targeted trading strategies that could be disruptive to users.

[23] A transaction is considered trustless because the miner does not place faith in any single person or intermediary. Instead of placing trust in a single entity, the miner allows the network to function as intended and execute transactions through its underlying protocols.

[24] In PoW Ethereum, searchers were able to naturally engage in some potentially disruptive MEV realization strategies, analyzing information about the requested operations contained in user messages from the network's public 'mempool', where those messages await inclusion within a block, to be able to offer optimal block constructions to miners. A "mempool," short for 'memory pool,' is a digital holding area within each node of a blockchain network where all pending messages anticipate confirmation and inclusion within a validated block. Each node that is part of a blockchain network maintains its own mempool, independently verifying and storing unconfirmed transactions broadcast (or "gossiped") from other nodes in the network. This distributed system allows transactions to be processed in a secure and transparent manner, with mempools playing a critical role in managing the flow of transactions and potentially affecting transaction speed, fees, and overall network efficiency. Public mempools naturally occur on any permissionless and decentralized blockchain network, not just Ethereum. On the Bitcoin network, for example, the mempool serves as a temporary staging area for transactions where those transactions are stored after a user submits a proposed transaction to transfer bitcoin from one address to another. On the Bitcoin network, miners select transactions for block formation, typically prioritizing those with higher fees. This demonstrates the market-driven nature of transaction processing in blockchain, where users can choose to pay higher fees for faster confirmation.

In September 2022, Ethereum upgraded from its original PoW mechanism to proof-of-stake in an event known as the merge.[25] Upgrading a blockchain network is a technically challenging process, requiring multiple open-source stages of review and audits to ensure all contemplated changes to the protocol are technically sound and will not disrupt network security or functionality. Ethereum's successful transition to a PoS consensus was the culmination of multiple years of research and development.

After this transition from a PoW system to a PoS system, validators replaced miners as the actors responsible for proposing new blocks for verification on the network. While Ethereum's PoS system was designed to allow any validator[26] to earn the same rewards, the competitive nature of the block building process in pursuit of available MEV opportunities threatened the neutrality of the network's base layer.

At economies of scale, making validators responsible for MEV optimization would inevitably lead to more sophisticated actors being able to dedicate more time and resources to block building and therefore the ability to earn more fees. This trend would serve as an unavoidable centralizing force on validators that would, instead of operating as neutral base layer actors, consolidate under the control of only a few entities specialized for the purpose of optimizing MEV realization.

To mitigate these concerns, protocol and community researchers proposed separating the duties of validators into two roles: block proposers and block producers. Validators would be responsible for only the service to the network of proposing blocks to the chain and the role of block production would be delegated to new base layer participants. This concept is known as Proposer-Builder Separation (PBS):

> "Instead of the block proposer trying to produce a revenue-maximizing block by themselves, they rely on a market where outside actors that we call block-builders produce bundles consisting of complete block contents and a fee for the proposer, and the proposer chooses the bundle with the highest fee. The proposer's choice is reduced to picking the highest-fee bundle [...]"[27]

---

[25] The Merge refers to the original Ethereum Mainnet merging with a separate proof-of-stake blockchain called the Beacon Chain, now existing as one chain. *See* Ethereum Foundation, *The Merge*, ETHEREUM.ORG: NEWS (Mar. 13, 2024), https://ethereum.org/en/roadmap/merge/.

[26] Validators are node operators that stake digital assets, as collateral, to the blockchain with the intent to secure the network. Validator nodes can be operated by individuals who individually possess the requisite number of native digital assets needed to operate a validator node, by institutional staking-as-a-service providers who stake on behalf of individuals, or by staking protocols that programmatically stake on behalf of network participants. *See* Proof of Stake Alliance, *U.S. Federal Securities and Commodity Law Analysis of Liquid Staking Receipt Tokens*, at 3, 6, 13, PROOFOFSTAKEALLIANCE.ORG (Feb. 2023), https://www.proofofstakealliance.org/s/US-Federal-Securities-and-Commodity-Law-Analysis-of-Liquid-Staking-Receipt-Tokens-Willkie-Draft-0214.pdf.

[27] Vitalik Buterin, *Proposer/block builder separation-friendly fee market designs,* ETHEREUM RESEARCH: BLOG: ECONOMICS (June 4, 2021), https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725/1 (explaining the implementation of PBS on Ethereum).

Although Ethereum protocol researchers and community teams still retain the ultimate goal of enshrining PBS as part of the network's underlying protocols (a concept known as 'enshrined' PBS or "**ePBS**"), it will take a substantial amount of time to identify technically feasible designs. In the interim, reflections on the success of mev-geth in PoW Ethereum demonstrated the feasibility for an out-of-protocol solution to alleviate some centralizing pressures caused by MEV. An out-of-protocol substantiation[28] of PBS (often called "**MEV-Boost**"), was introduced to replace mev-geth following Ethereum's PoS transition. This interim solution for observing PBS on PoS Ethereum has reshaped the landscape for MEV realization while maintaining an essential balance between base layer security and economic incentives inherent in open and permissionless blockchain-based systems.

PBS on PoS Ethereum

MEV-Boost introduced two new participants to the base layer: block builder and relay.[29] The block builder is a specialized actor that is responsible for the ordering of transactions. The relay is a specialized actor that provides a service between the block builder and validator. For every block that is added to the chain, a single proposer (validator) is chosen. This proposer has a 12 second window (known as a "**slot**") to propose their block. Missing your proposal window results in economic penalties for the validator.[30]

During these 12 seconds, known as a slot, block builders gather all pending transactions from both public sources (the public mempool) and private sources such as protected mempools or transactions sent directly to the block builder. The block builder simulates the optimal order of transactions and broadcasts updated bids to the relay. The relay then chooses the most profitable bid from the set of block builders, which are all competing for the right to build the block. The proposing validators' consensus client then propagates the most profitable block received from MEV-Boost to the Ethereum network for attestation and block inclusion.

Block builders provide a critical service for Ethereum users by creating a market for transaction prioritization. As the market structure for MEV has developed, tools and services that provide users with more expressivity over their operations and to protect them from negative externalities have been developed in large part because of this market.

---

[28] The success of mev-geth under Ethereum's former PoW consensus demonstrated the feasibility of out-of-protocol solutions in relieving some of the centralizing pressures influenced by miners' natural inclination to optimize for MEV realization.

[29] Independent groups or organizations voluntarily maintaining relays to support Ethereum include Blocknative Corp. (https://www.blocknative.com/), BloXroute Labs, Inc. (https://bloxroute.com/), Goe Network Ltd. a.k.a. Eden Network (https://edennetwork.io/), Flashbots, Ltd. (https://www.flashbots.net/), and Manifold Finance, Inc. (https://kb.manifoldfinance.com/).

[30] Penalties, referred to as "slashing," are used to ensure consensus and deter misbehavior throughout the consensus process. Slashing occurs when a validator dishonestly proposes a block, either by proposing or signing two different blocks for the same time slot, changing block history, or double voting on a single block. *See* Matthieu Saint Olive & Simran Jagdev, *Understanding Slashing in Ethereum Staking: Its Importance and Consequences*, CONSENSYS: NEWS: STAKING (Feb. 7, 2024), https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences.

Relays provide a beneficial service to the Ethereum network as public goods infrastructure. They are trusted by the block builders to not alter the contents of blocks, and by the block proposers to provide a valid block header and to publish the full beacon block. However, relays operate as a choke point for censorship where the contents of blocks are screened by some relays for elements such as sanctioned wallet addresses.

While MEV-Boost remains an imperfect system, it has stabilized the PoS Ethereum network and protected the neutrality of validators and created a robust market for transaction inclusion and prioritization that has contributed to a more efficient network. Protocol and community researchers continue to investigate pathways to deprecating MEV-Boost in favor of in-protocol ePBS structures. These designs, and additional improvements such as execution tickets, inclusion lists, and more, are the result of years of academic research into network security for distributed systems.

MEV market structure is constantly evolving and the prospect of new research and development necessitates a deep understanding of the dynamics of MEV to allow the market and economic security of Ethereum develop without enshrining inefficient or suboptimal market structures.

IV. MEV IN PRACTICE

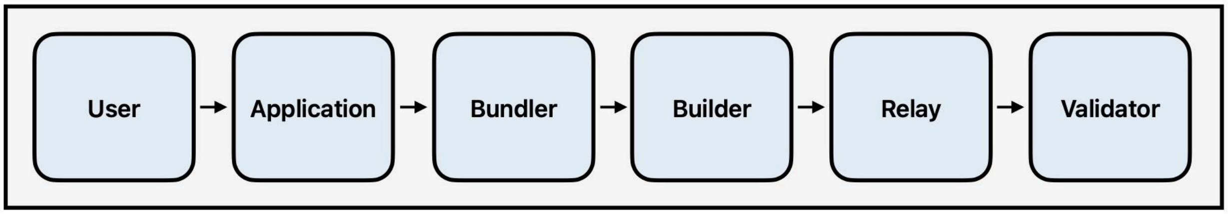
At its core, MEV emerges from the execution of user-submitted operations. These operations—whether buying, selling, transferring, or swapping digital assets or sending an onchain message, taking an action in an onchain game, or writing information to the network—inject a potential for value realization. Users can express priority using gas or by leveraging available information to have their operations executed with beneficial timing; either way, prioritization is ranked based on the potential fee for processing the operation.

A user operation is typically submitted through an application that provides a front-end interface to the user. The user broadcasts their message and their intent using the application to the public mempool or another channel, like a protected mempool.[31] At this stage, the pending message awaits inclusion in a block. Before block inclusion, however, another set of specialized actors (known as "**bundlers**") provide block builders with sets of pending operations known as bundles that are optimally ordered depending on inclusion priority and profit-maximizing strategies.

Block builders receive these bundles and update their optimal block. Relays select the highest value block from the corresponding block builder and from there a block is included onchain by a validator. This system provides an efficient process for users to express their inclusion priority and for actors in the operation supply chain to execute operations. (*see Exhibit 1* for a step-by-step overview of this block building lifecycle on Ethereum).

[31] *See infra* note 33.

Exhibit 1: Overview of the Ethereum block building lifecycle, simplified



During this process, it is critical that applications provide information to users about their onchain actions. Aspects such as gas, slippage tolerance, operation venue, and submission method all factor into how an operation will be included onchain and potential impact to the operation as it is processed. The process of including an operation onchain based on priority fee or profit-maximizing strategies does not change an outcome for a user. Rather, an application quotes a user a potential outcome and it is the responsibility of application developers to ensure that the operation is executed in the quoted manner, or communicate to the user the implications for their onchain operation based on their fee, slippage, or the manner in which their operation is submitted for inclusion.

By assuming message inclusion and ordering optimization responsibilities, bundlers, block builders, and relays enable a competitive market for blockspace in a way that improves network efficiency, allowing validators to focus exclusively on their primary role in maintaining the economic security of the network.

A. *Types of MEV*

The term MEV has expanded to include a range of activities, strategies, and concepts and the definition of MEV relating to consensus security does not cover the breadth of these onchain actions. To shed additional light on these actions, we consider MEV actions as efficiency-maximizing or value-maximizing.

Efficiency-maximizing actions include arbitrage, liquidations, oracle updates, and other actions. Atomic arbitrage refers to the ability of a trader to rebalance across one or more decentralized exchanges (DEXs) in a single block. Statistical arbitrage refers to arbitrage between a centralized exchange (CEX) and DEX where the trader is leveraging continuous CEX updates while a DEX updates with each state change (block) on Ethereum.

Arbitrage provides a necessary and important function for liquidity on DEXs. DEXs utilize MEV to incentivize liquidity providers, fostering a more fluid and efficient trading environment–a function in traditional financial markets typically executed by centralized institutions with proprietary agreements with trading venues. Inclusion and priority are critical to arbitrage strategies and MEV creates an efficient mechanism for their execution.

Liquidations and oracle updates refer to specialized roles on decentralized lending platforms for processing undercollateralized positions. The process of loan collateral liquidation necessitates gas expenditure—a cost effectively borne by trading bots. These bots, incentivized through a share of the liquidated collateral, embody MEV in action, ensuring the system's operability even during spikes in gas prices. If they did not utilize MEV, these platforms might either falter under operational inefficiencies or resort to the use of permissioned actors for liquidation processes, undermining a foundational principle of decentralized lending markets.

In each of these scenarios, there is potential value in one or more operations in a block where the specific placement of the operations will result in some value realization. In many cases, transaction ordering is providing a service to the chain to increase efficiency and expressivity of users, ultimately improving execution. However, some MEV occurs because of the principle of economic security where actors are incentivized to execute maximally value-seeking strategies. These are known as value-maximizing MEV actions.

Value-maximizing actions leverage publicly available information about user operations to place additional operations before or after an operation, known as trading ahead. In many cases, this can cause the execution quoted by an application to change and may be the result of improper slippage tolerance or transacting in DEX pools with low liquidity.

In a system that categorically does not permit some forms of value-maximizing actions, users are restricted in their methods for transaction prioritization. In these systems, users that want to prioritize their transaction ahead of others would only have access to setting high gas fees or other strategies such as spamming operations to increase rates of inclusion which would congest the network and raise gas fees to all users. Therefore systems that can provide users with protection from these types of value-maximizing actions all-the-while providing some users with the ability to leverage their information for improved inclusion are more robust than systems that do not.

At the core of MEV in practice is understanding how information about user operations are carried through the system. The public mempool of Ethereum provides a detailed view of pending operations. It is from this information that efficiency-maximizing or value-maximizing strategies can be realized. Providing users and applications with tools and systems to control their information through the process of including an operation in a block yields more control over how MEV impacts execution.

B. User protection interests on Ethereum

As the understanding of MEV on Ethereum has matured, two new classes of systems have been developed to move operation execution closer to providing optimal execution for users. First, the creation of protected mempools[32] have allowed applications to submit user operations in a manner where the information of operations are not disclosed. Secondly, in combination with protected mempools, orderflow auctions[33] have introduced a mechanism for users to express

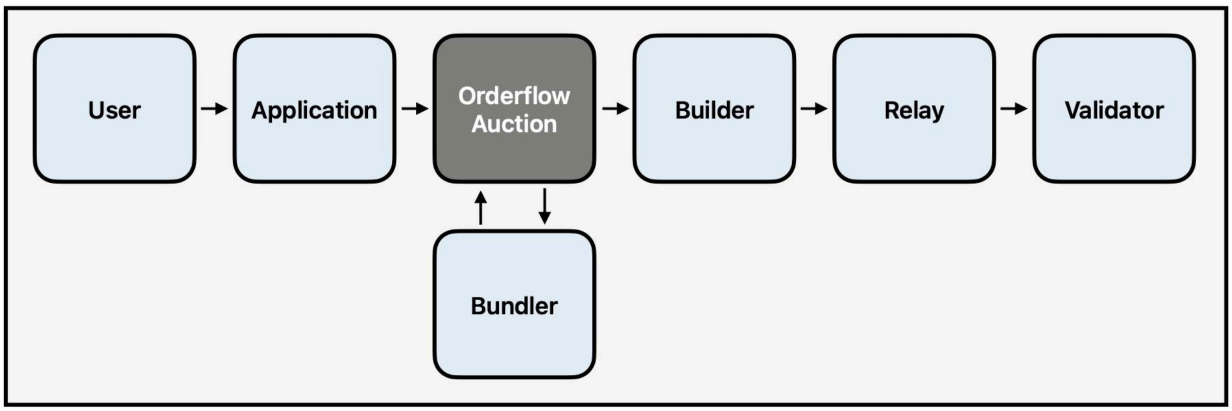
[32] "Protected mempools" are exclusive memory pools containing messages accessible only to contributing bundlers and block builders. They allow participating applications to submit user messages in a manner that hides information about underlying requested operations from the public mempool until each message is ready for inclusion in a validator's proposed block. By routing user messages through a protected mempool, application developers can provide their users with a reliable layer of privacy and consumer protection.

[33] Orderflow auctions process transactions in batches and implement predetermined rules that mitigate advantages that certain MEV actors possess. *See* Angela Lu, *Illuminating Ethereum's Order Flow Landscape,* FLASHBOTS WRITINGS: NEWS (Jan. 16, 2024), https://writings.flashbots.net/illuminate-the-order-flow (explaining the role of order flow

how they would like their operations executed and bundlers to bid for the right to execute them. These systems have drastically reduced the amount of value-maximizing MEV on Ethereum.[34]

The orderflow auction process works by aggregating user intents into a market where block builders can assess the value of including specific messages based on the fees users are willing to pay and the builders' ability to meet those intents. This creates a more dynamic and user-centric approach to message inclusion within each block on Ethereum, moving beyond the simple fee-based prioritization methods that conventionally dominated Ethereum's previous systems for block space allocation (*see Exhibit* 2 for an overview of an orderflow auction's place within the Ethereum block building lifecycle). The auction process also introduces a layer of strategic decision-making for block builders, who must balance the profitability of including certain messages against the complexity of fulfilling diverse user intents.

Exhibit 2: Overview of the Ethereum block building lifecycle, with orderflow auction



Application developers, instead of leaking information of pending operations, now have the ability to submit operations with pre-execution privacy, providing a necessary layer of consumer protection for users. By developing a market for information, application developers can now build systems where users have near full control over their information and execution quality, while providing a pathway for users to benefit from part of the value created through a cut of the payment associated with order flow auction being rebated to users, aligning incentives and enabling cheaper transaction fees. While many of these systems today are operated by third-parties, researchers and developers are exploring using trusted execution environments

auctions on Ethereum). In combination with protected mempools, "orderflow auctions" provide users with an improved capacity to express how they would like their operations to be executed (known as an "intent"), driven by bundlers bidding for the right to include them in their message bundles based on user intents. A user's 'intent' can range from seeking the fastest possible execution, targeting a specific execution cost, or even specifying a desire to avoid certain MEV realization strategies that might affect the outcome of the user's underlying requested operations. By expressing an intent, a user can effectively communicate their priorities and constraints to bundlers and block builders.

[34] Protected mempool services and orderflow auction services are offered by a variety of organizations, primarily including but not limited to all the same organizations maintaining MEV-Boost relays: Blocknative Corp. (https://www.blocknative.com/), BloXroute Labs, Inc. (https://bloxroute.com/), Goe Network Ltd. a.k.a. Eden Network (https://edennetwork.io/), Flashbots, Ltd. (https://www.flashbots.net/), and Manifold Finance, Inc. (https://kb.manifoldfinance.com/). *See supra* note 30.

(TEEs) and other privacy technologies such as fully-homomorphic encryption (FHE) and zero-knowledge proofs (zk proofs) to remove themselves as trusted intermediaries, further advancing onchain activity to a maximally decentralized state.[35]

Lastly, a robust market for operation execution is critical for the efforts of white hat (ethical security hacker) operations that seek to protect users and applications from hacks and exploitations. White hat operators leverage prioritization systems to prevent hackers from executing exploits and hacks by monitoring onchain activity and taking actions such as submitting exploitation operations ahead of hackers and then returning the funds to the responsible parties.[36]

Understanding these forms and sources of MEV is crucial for many, but especially for blockchain developers. It allows for the development of strategies that mitigate the potential negative externalities of MEV while harnessing its potential to contribute positively to network security and market efficiency. This dynamic also extends to other blockchain-based contracts, such as in connection with games, collectibles, and more, where MEV enables users to fund gas fees for actions like minting new items or participating in complex game states, thereby enhancing user engagement and platform vitality.

C. MEV Developments on Other Blockchain Networks

MEV can evolve or assume different forms and result in a variety of implications for different blockchain networks. From more common forms of consensus on the most widely used and highly capitalized layer-1 ("**L1**")[37] blockchain networks to the different message ordering approaches of layer-2 ("**L2**")[38] networks, approaches to MEV and base layer economic security can vary widely, and largely depend on the maturity of the network.

MEV Variations

Proof of Stake (PoS)

Although there are many different iterations, PoS systems underlie the most widely used and highly capitalized blockchain networks. The dynamics of PoS blockchains expand the availability of MEV opportunities.

---

[35] Although many of these systems are today operated by third-parties, Ethereum researchers and developers continue to explore alternatives for managing block space markets in a decentralized fashion. Vitalik Buterin, *Multi dimensional EIP 1559,* Ethereum Research: Blog: Economics (Jan. 5, 2022), https://ethresear.ch/t/multidimensional-eip-1559/11651.

[36] *See* Security Alliance, *Whitehat Safe Harbor*, GitHub: Blog (Feb. 14, 2024), https://github.com/security-alliance/safe-harbor (providing a framework for white hat actors to act in the best interest of blockchain networks).

[37] L1 blockchain networks provide a base layer of infrastructure and consensus that serve as the foundation of blockchain technologies.

[38] L2 networks are built on top of L1 networks to enhance L1 network scalability, and they typically depend on the L1 network's consensus protocols for security.

Polygon

Other modified forms of PoS systems handle MEV and the block building and proposal process in different ways. The community behind Polygon,[39] for example, applied an adapted form of PoS's basic principles to suit the network's specific aims and technical requirements, namely in pursuit of improved network scalability and interoperability.

The Polygon network's unique PoS-based architecture and commitment to user-friendly MEV solutions set it apart from most other blockchains. Unlike Ethereum, the absence of a private bundle relayer to Polygon validators significantly reduces the prevalence of targeted trading strategies[40] and private order flows.[41] This openness ensures all pending messages become public in Polygon's mempool, leveling the playing field for all network participants.

As part of the solutions in place to support Polygon, members of the network's developer community deployed FastLane,[42] a software protocol that aims to balance between generating MEV revenue for validators and protecting users from the targeted trading strategies.[43] Solutions like SUAVE[44] and Atlas[45] refine the network's approach to MEV. SUAVE is an infrastructure network comprised of TEEs (trusted execution environments) that facilitates private interactions among dapps, users, and solvers creates a competitive marketplace meant to prioritize user benefits.[46] Atlas is a smart contract platform that facilitates trustless interactions among dApps, users and solvers, attempts to export Fastlane's benefits to other EVM chains.[47] Polygon's interchain functionality (enabled by its unique "commit-chain" structure) is designed to achieve scale by operating alongside the Ethereum mainnet, but it introduces additional layers where MEV can be extracted, not only in the block building lifecycle within Polygon itself but also in the cross-chain interactions between Polygon and Ethereum. Working together, SUAVE and Atlas provide all relevant cross-chain participants with a collaborative means to address MEV mitigation.

---

[39] Polygon network, *assoc. with* Polygon Labs UI Ltd. (https://polygon.technology/).

[40] The Polygon community set out to ensure the network offers users with additional protection against potentially disruptive forms of MEV realization with a blended solution consisting of both infrastructure and smart contracts that makes the environment among validators less adversarial compared to Ethereum. Polygon's avoidance of private relays further democratizes the block building process by ensuring all pending messages are visible and contestable by the network participants and community.

[41] Scraping Bits (podcast), *Reopening The Mempool: Disrupting Monopolized Private MEV Orderflow*, Spotify (Jan. 15, 2024), https://open.spotify.com/episode/6npHE7qHPUlhceUtvyvysV (explaining that private order flow is non existent because everything is public).

[42] FastLane, *a service of* FastLane Labs, Inc. (https://www.fastlane.xyz/).

[43] *See* Alex Watts, *Polygon FastLane White Paper*, FastLane Labs (May 2022) https://www.fastlane.xyz/pfl_white_paper_1_5.pdf (providing detailed information in connection with the implementation of Polygon FastLane).

[44] SUAVE, *a service of* Flashbots (https://www.flashbots.net/).

[45] Atlas, *a service of* FastLane Labs (https://www.fastlane.xyz/).

[46] *See* Flashbots, *The Future of MEV is SUAVE*, Flashbots.net: Writings (Nov. 22, 2022), https://writings.flashbots.net/the-future-of-mev-is-suave.

[47] *See* Alex Watts et al., *Atlas White Paper*, FastLane Labs (Feb. 2, 2024), https://www.fastlane.xyz/Atlas_Whitepaper.pdf.

Additionally, Polygon's use of account abstraction and 'intents' networks like the Banana SDK[48] emphasizes user protection and efficient execution quality. By allowing users to sign transactions without directly paying gas fees, and by ensuring transactions are publicly contestable, Polygon fosters a competitive environment that broadly benefits users and discourages monopolistic practices among base layer actors.

Solana

The Solana network's consensus mechanism involves the round-robin election of a validator (termed a "**leader**") every 4 sequential blocks to receive the responsibility to build and propose those 4 blocks in that cycle. Unlike Ethereum, Solana does not have a public mempool. Operations are forwarded directly to the leader (and the next two leaders). There is no in-protocol mechanism for global ordering of operations, the leader is only able to order operations locally, as they are forwarded. This means that there is both no mechanism for inclusion priority and that operations are not included first-come-first-serve.

This has significant implications for inclusion and prioritization as users and applications have to resort to certain strategies to increase chances for specific execution. The most common strategies are latency games–building the fastest connection to the leading validator to ensure your operation reaches the validator first. This has implications for network resiliency and centralization risks as applications and infrastructure providers are incentivized to co-locate their infrastructure with the largest validators to have the fastest possible latency between operation and inclusion. The second primary strategy is spamming–sending hundreds of operations every millisecond to maximize chances of inclusion. This leads to network congestion and blocks that are filled with failed operations.

This is especially relevant to MEV, as efficiency-maximizing strategies need precise inclusion in a block. Some validators may run algorithms locally to execute MEV strategies but this does not solve the need for an open market for inclusion priority. To close this gap, infrastructure provider Jito Labs designed a protocol for validators (Jito-Solana) that allows them to participate in an auction for block space similar to the mev-geth and MEV-Boost protocols on Ethereum.

Jito-Solana established an efficient mechanism for inclusion priority and significantly reduced the amount of failed transactions consuming Solana block space. While Jito-Solana does slow the Solana consensus client slightly due to pausing the continuous block production in order to collect, order, and propose blocks from the auction, it has improved the overall efficiency of the network and will decrease the delay over time.

As detailed above, there are multiple types of MEV, including some forms that can negatively impact operation execution. As Solana is a newer network, the range of infrastructure on Solana

[48] Banana SDK, *a service of* Rize Labs (https://www.bananawallet.xyz/).

is less mature than the Ethereum ecosystem. Therefore, innovations such as protected mempools and order flow auctions are not yet available. As activity on Solana continues to increase, Jito Labs observed the Jito-Solana protocol being used to execute an increasing amount of profit-maximizing strategies. In order to provide users with an optimal experience, Jito Labs announced in March 2024 a decision to suspend the Jito-Solana mempool until a sustainable mechanism for user-protection could be introduced.

This change required searchers to adopt new strategies for MEV capture but positive MEV such as arbitrage is still available while strategies with negative externalities are generally prevented. However, this signaled a significant understanding by both Jito Labs and the larger Solana ecosystem of the value of MEV and the opportunity to build trustless, efficiency-maximizing systems for inclusion prioritization, all-the-while providing users with execution guarantees.

Other PoS Variations

Other PoS blockchains—such as Algorand, Avalanche, Cardano, Cosmos, Polkadot, and Tezos networks—can have potentially dramatically different MEV implementations depending on how base layer incentives are structured, the means by which and speed with which consensus is achieved, and other factors. However, they all have at least a few attributes in common. On each of these blockchain networks, security and integrity are in some way maintained by validators and tokenholders who stake native tokens. The MEV infrastructure on these networks is less well-understood due to their more recent launches. Therefore, developers in these ecosystems are more focused on creating and improving this fundamental infrastructure, while balancing the natural MEV opportunities to mitigate potentially negative externalities.[49]

Proof of Work (PoW)

The PoW model for consensus, pioneered by Bitcoin, is distinct from its PoS counterparts. Bitcoin, as the progenitor of blockchain technology, significantly contrasts with the complex smart contract ecosystems found in networks like Ethereum. Bitcoin's scripting language is deliberately designed to be limited, prioritizing security and simplicity over versatility. This design choice inherently narrows the scope for MEV opportunities, particularly those that might otherwise be associated with smart contract interactions and targeted trading strategies prevalent in PoS systems.

On Bitcoin, the primary incentive for miners revolves around block rewards and transaction fees. This incentive structure fosters a competitive environment for block space, especially during periods of high network congestion. Miners are motivated to select transactions offering higher fees, creating a natural market dynamic for block space allocation. The simplicity of

---

[49] *See* Skip Protocol, *Announcing MEV Satellite: The First Cosmos Ecosystem MEV Dashboard*, MEDIUM: NEWS: MEV (Sep. 12, 2022), https://medium.com/@skip_protocol/announcing-mev-satellite-the-first-cosmos-ecosystem-mev-dashboard-9c1445e29e22 (detailing a solution to safely harness MEV on Cosmos).

Bitcoin's model, however, limits the complexity and variety of MEV opportunities compared to those available on PoS chains.

Bitcoin's community has worked to developed solutions like CoinJoin[50] and the Lightning Network[51] to further limit and refine MEV opportunities and enhance user privacy and network scalability, respectively. CoinJoin allows multiple users to combine their transactions into a single, larger transaction, making it more challenging to determine the origin and destination of funds. This aggregation can obscure potential MEV opportunities by complicating the analysis of transaction flows. Separately, the Lightning Network is a layer-2 protocol built on top of Bitcoin that facilitates instant, low-cost transactions by enabling off-chain payment channels. This solution is not only meant to address Bitcoin's inherent scalability limitations and transaction fee costs but also help reduce MEV generation on Bitcoin overall by moving a significant volume of transactions away from the main, L1, network to minimize their visibility and the predictability of transaction flows.

Across likely all PoW networks, the base layer process of block building and the competitive nature of mining introduce unique MEV considerations. The system's reliance on computational power for block validation, coupled with the direct financial incentives of block rewards and transaction fees, creates a straightforward yet highly competitive landscape for MEV realization. Unlike PoS systems, where validators might have long-term vested interests in the network's health due to staked assets, PoW miners are primarily motivated by immediate returns, which is likely the primary driver of their strategies for message selection and block construction.

V. Key Economic Considerations

At the core of understanding MEV lies a fundamental economic inquiry: How are scarce resources (specifically, block space and transaction ordering) allocated within blockchain network-based market environments? This question does not solely pertain to blockchain networks but also mimics classical economic dilemmas where optimizing the allocation of limited resources is paramount. Thus this concept is not merely a common element of the design inherent in permissionless blockchain networks but an economic function inherent in almost any open market for assets, goods, or services in finite supply.[52]

This paper proposes a simplified economic model grounded in game theory that conceptualizes blockchain networks and ecosystems as sustaining competitive markets where various actors

[50] CoinJoin, *a service of* Wasabi Wallet (https://wasabiwallet.io/) and JoinMarket (https://joinmarket.net/).

[51] Lightning Network, *assoc. with* Lighting Labs, Inc. (https://lightning.engineering/).

[52] For an interesting examination of the challenges of ordering a highly popular service in the face of finite supply, *see* Defunctland, "Disney's FastPass: A Complicated History", available at https://youtu.be/9yjZpBq1XBE?si=4TXB0lN_cryxd3pP (tracing the challenges faced by The Walt Disney Company to allocate ride availability in their theme parks in a manner that is both perceived as "fair" by customers while maximizing revenue for the company).

(*i.e.*, users, miners or validators, searchers or solvers, etc.) interact under conditions of scarcity and often strategic behavior and information asymmetry.

Essentially, every blockchain network-based market or market scenario can be viewed as a *game* where participants compete for the allocation of scarce resources (block space and transaction priority). Each participant has different objectives, like profit maximization (for traders and arbitrageurs) or reward maximization (for miners and validators). Below are four baseline considerations for each MEV *game* scenario analyzed in this paper:

1. *Strategies & Rewards*: Participants choose *game* strategies based on their information set, which includes knowledge of pending database transactions, gas prices, and potential MEV opportunities. The reward for each participant depends on the strategy mix of all players, reflecting the interdependent nature of their decisions.

2. *Information Asymmetry*: Viewing each scenario as a *game* highlights the role played by potential information asymmetries, where certain participants have more or better information about transaction ordering, leading to potential MEV extraction.

3. *Externalities*: Potentially "negative"[53] externalities—such as increased transaction fees or network congestion—are often caused by the existence of information asymmetries, and they can be modeled as costs that could potentially be imposed on participants or, of primary consideration, non-participating users.

4. *Theoretical Equilibrium*: If possible to identify, the equilibrium of any particular *game* can provide insights into how MEV can be distributed across participants and the conditions under which certain MEV realization strategies might become dominant. This analysis helps identify potential inefficiencies and externalities arising from MEV activities.

Considerations in early Ethereum environments

In the early days of Ethereum, the public mempool was a common area where all database transactions awaited confirmation by miners, which assumed the role of block builders to order transactions and build and finalize blocks. This setup created a fertile ground ripe for MEV-related opportunities where miners could observe pending database transactions and act on them before they were confirmed. In any given public mempool scenario, the following set of conditions can be assumed based on the four baseline *game* considerations:

1. *Strategies & Rewards*

    - Miners can choose which transactions to include in a block based on transaction fees, and traders and searchers can observe the public mempool for opportunities to

[53] Regular users bear the burden of increased gas prices and reduced block space.

submit transactions with higher gas fees to "jump the queue" and exploit profitable opportunities before others do.

2. *Information Asymmetry*

    - Miners have control over transaction ordering, and all other participants and non-participating users have the technical capability to monitor and react to the mempool in real-time but not the ultimate ordering of database transactions.

    - This created an information asymmetry between miners and all others involved, allowing miners to, for example, insert transactions ahead of others or manipulate the order of transactions within a block to their advantage if they saw a profitable opportunity.

    - In block space auctions,[54] miners could exploit the system by artificially congesting the network to drive up gas prices or by preferring transactions that offer them the highest rewards, potentially at the expense of network efficiency and fairness.

3. *Externalities*

    - Notwithstanding the potential direct effects of frontrunning on a user's transaction, the activities of traders and searchers[55] in the public mempool (and the ordering activities of miners) can potentially lead to negative externalities, such as increased gas prices and network congestion.

    - These externalities disproportionately affect regular users who are not participating in MEV extraction but suffer from its consequences, such as delayed transaction confirmations and higher transaction costs.

    - The users may find themselves outbid in a block space auction or unaware of the strategic bidding war happening in the background.

4. *Theoretical Equilibrium*

    - In this scenario, equilibrium would theoretically be achieved when all profitable frontrunning opportunities are exploited, and the gas prices reflect the competition for block space.

[54] On early PoW Ethereum, the gas market essentially functioned as an auction for block space, where users could submit bids (*i.e.* offered gas prices) for their transactions to be included in miners' next block.

[55] While the transaction information in the public mempool was publicly available and therefore not marked by more traditional notions of information asymmetry between users and traders or searchers, this scenario often disadvantaged non-knowledgeable, retail end users of Ethereum. Traders and bots have visibility into pending transactions and can use this information to their advantage, while less sophisticated users may not be aware of these activities or know of ways to limit their generation of potential for MEV opportunities for traders or searchers on the network. This asymmetry potentially enables the realization of MEV at the expense of the most vulnerable of users.

- This equilibrium highlights the efficiency in MEV extraction but underscores the inequity and increased costs for regular users.

As discussed earlier,[56] concerns related to MEV and transaction privacy on early Ethereum led to the development of several strategies to protect transactions from being observed and exploited by others before they were mined into a block. Various dApp developers and digital asset exchanges implemented mechanisms to reduce the risk of potentially harmful forms of MEV realization. These could include batching transactions, using relayers, or creating smart contracts designed to obscure transaction details until execution.

Applying the four *game* considerations—strategies and rewards, information asymmetry, externalities, and theoretical equilibrium—provides a robust framework to assess the presence of a fundamental market failure within any given scenario. Through this lens, it becomes evident that despite the complexities and challenges posed by MEV, early Ethereum for example never experienced a fundamental market failure. The Ethereum community's adaptive responses and rapid innovation underscore its resilience and capacity for self-regulation.[57]

Moving forward, various MEV-related protocols and projects on early Ethereum ultimately helped lay the groundwork for thinking about how to protect transactions from potentially predatory practices. Many of the early efforts to address the potential for harmful effects from MEV realization on early Ethereum[58] evolved over time as a result of the community's efforts to separate the role of validators (previously miners) as block builders from the role of 'block proposers' with the launch of PoS Ethereum.[59]

Ethereum's transition to PoS reshaped its economic underpinnings, especially in how validators and solvers interact within this evolved ecosystem. In this landscape, the separation of roles into block proposers and block builders has redefined economic interactions on Ethereum, creating a more structured and competitive marketplace for block space and message order.

Considerations in current environments

In reevaluating how MEV manifests on Ethereum following the move to PoS, and, in contrast with the public mempool *game* scenario,[60] the following set of conditions can be assumed based again on this paper's four baseline *game* considerations:

1. *Strategies & Rewards*

---

[56] *See* Section II.B (*User protection interests on Ethereum*).

[57] For examples of these responses, *see* Section II.A and Section II.B.

[58] *See* Section III.A (*Early PoW Ethereum*).

[59] *See* Section III.A (*PBS on PoS Ethereum*).

[60] *See* Section III (*Considerations in early Ethereum environments*).

- Ethereum's switch to PoS fundamentally altered the strategic landscape, where validators are incentivized to select the most economically advantageous blocks, often those crafted by solvers identifying lucrative MEV opportunities.

- MEV-boost block relays have become pivotal in the new Ethereum environment, creating block space markets that account for all if not nearly all blocks proposed by validators, providing marketplaces for solvers to propose MEV-optimized blocks to validators while also observing basic principles.

- Most validators connect to upwards of three different relays,[61] seeking to compare and propose the block among them containing the most fees or financial incentive; although block builders' observation of baseline principles does not limit this overall inflation on end user costs, it does generally reshape the reward matrix for network participants and help to weed out potentially harmful forms of MEV realization.

2. *Information Asymmetry*

- Solvers, utilizing priority transaction networks and many MEV-boost block relays, often leverage not just public mempool data but protected mempool data and sophisticated tools to uncover various MEV realization opportunities.

- On early Ethereum, miners were motivated to potentially manipulate the order of transactions both to build and propose profitable blocks and to potentially profit by trading based on the informational asymmetry created by miners' knowledge of the transaction order; in contrast, validators on Ethereum are now generally motivated—still to propose the most profitable block, but—only to focus on proposing profitable blocks, validating blocks, and securing the network.[62]

- By providing a transparent view into the mempool's state, many tools help to mitigate some of the information asymmetry that historically characterized Ethereum, contributing to a more equitable environment for all participants.

- With the form of PBS currently observed with Ethereum PoS, the presence of an information asymmetry still exists between block builders and validators (previously miners), but where solvers are now more likely to possess information (such as from membership to protected mempools) for which validators no longer have a concern and without which validators remain profitable in acting only as block proposers.

[61] *See* Blocknative, *The Pros and Cons of Connecting your Validator to Multiple MEV-Boost Relays*, BLOCKNATIVE: BLOG: VALIDATORS (Jan. 17, 2023), https://www.blocknative.com/blog/ethereum-relay-diversity-for-validators (detailing the distribution of validators connected to three or more unique relays)..

[62] Gas prices drive the incentive structure that propels base layer actor behavior. The implementation of PBS on Ethereum has both enhanced security of the blockchain network but also maintains an incentive structure that diminishes the likelihood that base layer actors would act in violation of PBS principles. *See* Section II A. (*PBS on PoS Ethereum*).

- Ultimately, validators on Ethereum must rely on block builders (with the help of bundlers) to present the most profitable blocks without having direct insight into the construction of those blocks; this form of PBS is intended in part to address the information asymmetry that persisted on early PoW Ethereum, making this notion generally superfluous in any more modern Ethereum MEV-related *game* scenario.

3. *Externalities*

- A less knowledgeable user, when interacting directly with Ethereum or any DEX or DeFi protocol, may create opportunities for potentially harmful methods of MEV realization in the public mempool when they transact; however, the potential negative externalities that can be associated with MEV realization, such as network congestion and elevated transaction fees, have generally been addressed by various solutions[63] integrated at the level of the most commonly used MEV-Boost relays.[64]

- MEV shield protocols[65] can separately offer end users of Ethereum protection against common potentially harmful MEV strategies, even when users are interacting directly with Ethereum or a DEX or DeFi protocol, typically addressing users' potential exposure to negative externalities of the block building process by enhancing transaction security and fairness.

- MEV shield protocols,[66] including protected mempools and order flow auctions, also can help to reduce if not eliminate opportunities for potentially harmful forms of MEV realization typically by offering preferential ordering for increased fees or adding users' transactions directly to a protected mempool that follows a set of fair ordering rules.

4. *Theoretical Equilibrium*

- Identifying a theoretical equilibrium in the new Ethereum environment is challenging due to the dynamic nature of MEV opportunities and the continuous evolution of strategies by both solvers and validators.

- The solutions in effect generally allow MEV opportunities to be realized in ways that minimize potential negative externalities, and rewards are distributed in a manner that seeks to maintain the security and integrity of the network.

---

[63] Relays are the intermediation channels that serve as the source for all blocks ultimately proposed and validated on Ethereum; they facilitate more efficient markets for block space aimed at aligning validators' incentives with network health.

[64] *See supra* note 30.

[65] See Section II.B (*User protection interests on Ethereum*).

[66] *See* Section II.B (*User protection interests on Ethereum*).

- While the Ethereum community's goal to achieve a state where the network operates efficiently persists, the incentive structures of validators and solvers may change in response to a variety of factors, including changing market conditions. Achieving any form of equilibrium going forward likely will continue to require the community's constant adaptation and innovation from all network participants.

As Ethereum and the newer blockchains mentioned above continue to mature and evolve, the economic considerations surrounding MEV will undoubtedly remain a critical area of focus. Community efforts to balance efficiency, fairness, and security in the face of these evolving challenges underscore the importance of economic analysis in shaping the future of these networks and their ability to sustain healthy and vibrant and secure networks and ecosystems.

VI. MEV Fair Market Principles

The permissionless nature of blockchains and MEV itself is critical; it ensures that anyone can participate in and contribute to the economic activities in a blockchain-based environment. This openness is fundamental to the ethos of blockchain networks and systems, preserving their decentralized character. If MEV realization becomes restricted, it could not only stifle innovation but also contradict the very essence of permissionless blockchains. MEV, in its various forms, is therefore not merely a byproduct of blockchain network operations but a necessary component that sustains and enriches the network and the systems it supports. As blockchain technology continues to evolve, so too will the strategies for realizing and managing MEV, requiring ongoing vigilance and innovation from all stakeholders involved.

With this background in mind, we advance the following MEV fair market principles.[67] These principles aim to balance the benefits of MEV with the need to maintain a fair and secure network. By ensuring transparency and neutrality, we can foster a healthier ecosystem that encourages innovation without compromising security.

- **Allow open blockchain communities to flourish by innovating solutions themselves**.
    - Adopting MEV fair market principles is in many ways essential to advancing the neutrality, security, and scalability of decentralized and permissionless blockchain networks.
    - This includes ensuring that validators act neutrally and that block builders provide execution that best reflects user intent, all while, to the fullest extent practical, respecting transaction privacy.
- **Advance Network Neutrality**

[67] All principles can be modified by user agreement insofar as they only affect that user.

- Blockchain developers should always seek to ensure that base layer actors operate as neutral actors to support the principle of open and permissionless blockchain infrastructure, which is fundamental for ensuring a network's long-term economic security and upholding the core values underlying blockchain technology.
- On PoS systems, specifically, validators should be neutral actors functioning in their capacity as block proposers and validators of transactions on the network. Validators should, therefore, be able to access the most maximal-value blocks without having to act as specialized actors (searching or building their own blocks) or reviewing, testing, or simulating the contents of blocks with regards to MEV.

- **Encourage Broad Participation**
  - The availability of MEV-related practices on any given blockchain network should support a diverse range of participants depending on the principal aims and functions behind the underlying network infrastructure (*e.g.*, on PoS systems, everyone from sophisticated providers to solo stakers/delegators).
  - This helps to maintain base layer neutrality and ensure that anyone (*e.g.*, on PoS systems, everyone from sophisticated staking-as-a-service providers to solo at home stakers) can participate in securing the network. Greater breadth and diversity of participants supports the resilience of blockchain networks.
- **Ensure Transparency and Accountability**
  - Whichever specific set of base layer actors is responsible for the block building process on a given blockchain network should be transparent about how blocks are constructed. For example, block builders should provide clear documentation of their bundle merging algorithm, as well as any guidance the builder wishes to provide on how conflicts are resolved. Builders should also agree to share non-sensitive data for public analysis, monitoring, and tracking purposes. This transparency helps to ensure trust and support a fair and efficient system.
  - Block builders should provide execution that best reflects user intent, and they should not take actions that negatively impact the execution of the bundle (*e.g.,* effective price or refund amount).
- **No manipulation of blocks once proposed**
  - Base layer actors should not break the atomicity of bundles. This means that either all database transactions in a bundle are included in the intended order with no other transactions inserted between them, or no transactions from that bundle are included. Where two bundles' MEV extraction is non-conflicting, it is acceptable to discard transactions from a bundle to allow for merging with another bundle if the user has opted in to this feature.
- **Respect Privacy and Data Security**

  - Blockchain developers generally (with sole exception to where doing so undermines a network or project's intended use or purpose) should always strive to ensure the privacy of non-broadcasted database transactions and bundles, including failed-trade privacy.
  - More broadly, sensitive data should not be shared beyond the intended parties, ensuring user confidentiality and reducing the possibility for potentially harmful trading practices that might be deployed when third parties are able to leverage that sensitive data.
  - At least in Ethereum environments, this means block builders should not share any sensitive data about their bundles with others (*e.g.*, with other builders, internal or external searchers, or the public), except with the party who submitted the input to MEV-Share. Additionally, block builders as well as external and or internal searchers should not sell or share bundles with other parties. This includes other builders as well as external or internal searchers. Bundles are shared with the builder and the builder alone.
  - Off-chain intermediaries also should not step ahead of their customers when they have visibility into customer transaction information and are simultaneously acting (*e.g.*, as validator).
- **Promote End User Awareness and Education**
  - Companies and developers launching or maintaining decentralized applications (dApps) or other end user-facing applications or interfaces must provide information to users about their onchain actions. Applications should be MEV-aware and therefore should try to ensure pertinent MEV-related information is conspicuously presented to end users.
  - This might include providing end users with clear information about their requested operations and the potential implications affecting those operations at the time they are requested (*e.g.*, informing end users of the price impact their requested operations might have, the ranges in potential fees or other costs that their operations might incur, etc.).
  - These kinds of transparency efforts help to ensure end users understand the potential outcomes of their database transactions, which, in turn, promotes a fairer and more attractive experience for users and helps to mitigate potentially related regulatory or consumer liability risks.
  - It is also the responsibility of the application developer to execute the user's operation in the quoted manner or communicate to the user the implications for their onchain operation based on their fee, slippage, or the manner in which the application submits their operation for inclusion.
- **Drive Toward Long-Term Network Stability and Market-Efficient Outcomes**

- MEV-related activities should align with principles of market efficiency and fairness while also seeking to advance and maintain a set of base layer activities that are stable and predictable.
- In decentralized blockchain network environments, developers should seek to avoid the potential for power concentrations among base layer actors (and other network participants, as applicable), or else they could face the potential for informational asymmetries that could negatively impact the network or any network-supported environment.
- Blockchain developers should also consider and attempt to master an understanding of potential systemic risks and market stability as they might relate to MEV-related practices; available MEV realization methods should be designed to minimize negative externalities on end users (and other network participants, as applicable) and promote long-term network stability, including in how base layer activities might play out over time.