ICLE International Center for Law & Economics

MEV on Ethereum: A Policy Analysis

January 23, 2023

Mikołaj Barczentewicz

ICLE White Paper 2023-01-23

MEV on Ethereum: A Policy Analysis

January 2023

Mikołaj Barczentewicz[*]

Contents

I. Introduction 3

II. How Is MEV Extracted? 5

A. A Simple Model of MEV Extraction 6

B. MEV Extraction Under Proposer-Builder Separation 8

III. Is MEV Extraction a Policy Problem? 11

A. Classifying MEV 12

1. Toxic and Nontoxic 12

2. Oracle Manipulation 13

3. Mafia, Moloch, & Monarch 15

B. Individual Welfare and Legally Relevant Harm 16

1. Is MEV Extraction Ever Unfair? 16

2. Market Efficiency and Social Welfare 18

IV. Difficulties in Applying Existing Legal Frameworks 21

A. Theft and Simple Fraud 21

B. Private Information, Private Order Flow, & Fiduciary Duties 22

C. Market Manipulation 25

V. Conclusion: Is There a Need for State Action? 28

A. Cost of Government Intervention 28

B. Technical Solutions Are Likely Preferrable, but May Require Tradeoffs 29

[*] Mikołaj Barczentewicz is a senior scholar with the International Center for Law & Economics; senior lecturer in law and research director of the Law and Technology Hub of the University of Surrey School of Law. He also leads the Regulation of Crypto-Finance research project (https://cryptofinreg.org) and tweets at @0xMikolaj and @MBarczentewicz. For comments on earlier drafts and related discussions, the author thanks Claudia Biancotti, breeze, Phil Daian, Michele Fabi, Arthur Gervais, TuongVy Le, Barnabé Monnot, Nicolás Della Penna, Alex Obadia, Puja Ohlhaver, Pmcgoohan, Alex Sarch, Jake Senftinger, Martin Schmidt, Stalkopat, Thogard, Anton Wahrstätter, Natasha Vasan, and Evan Zinaman.

I. Introduction

In cryptocurrency markets, maximal extractable value ("MEV") is typically defined as "excess profit that a miner [validator] can extract by adjusting execution of user transactions."[1] MEV extraction has slowly been gaining broader recognition, *e.g.*, from the Bank of International Settlements,[2] the International Organization of Securities Commissions ("IOSCO"),[3] and mainstream publications like *Forbes*.[4] The Bank of International Settlements estimates that there has been between $550 and $650 million of total MEV volume since 2020.[5]

The aim of this paper is to provide an overview for policymakers regarding what we know today about MEV, but perhaps even more importantly, how much we do not know. I will offer general critical analysis of policy questions raised by MEV extraction on the Ethereum blockchain.[6] The paper is intended both for those unfamiliar with MEV and those who are broadly familiar (the latter of whom can probably skip at least part of Section II).

Terms like "market manipulation" and "victim" tend to be used loosely in describing MEV extraction, often without thoughtful reflection on whether they are appropriate. The term "MEV searchers" was even included in a recent anti-money-laundering bill introduced by Sen. Elizabeth Warren

[1] Kshitij Kulkarni, Theo Diamandis & Tarun Chitra, *Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers*, 4 (2022), https://arxiv.org/abs/2207.11835. *See also* Philip Daian *et al.*, *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, 2 (2019), https://arxiv.org/abs/1904.05234.

[2] Raphael Auer *et al.*, *Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi*, BIS BULLETIN (2022), *available at* https://www.bis.org/publ/bisbull58.pdf [https://perma.cc/3R75-T9TY].

[3] IOSCO Decentralized Finance Report, OR01/2022, 37 (March 2022), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf.

[4] Jeff Kauflin, *The Secretive World of MEV, Where Bots Front-Run Crypto Investors for Big Profits*, FORBES (Oct. 11, 2022), https://www.forbes.com/sites/jeffkauflin/2022/10/11/the-secretive-world-of-mev-where-crypto-bots-scalp-investors-for-big-profits.

[5] Auer *et al.*, *supra* note 2.

[6] Much of this analysis also applies to other blockchains, such as, *e.g.*, Solana or Polygon. I chose to focus on the Ethereum MEV ecosystem because it is the best-studied and already the subject of a burgeoning policy debate.

(D-Mass.), although in a context that suggested a misapprehension of what such searchers actually do.[7]

In January 2023, the U.S. Commodity Futures Trading Commission ("CFTC") brought its first-ever "oracle manipulation" case, charging Avraham Eisenberg with illegal manipulation of the decentralized exchange Mango Markets, which operates on the Solana blockchain.[8] While this case did not involve the Ethereum blockchain, it is nonetheless illustrative of similar schemes that could occur in Ethereum. The case also likely signals that regulators like the CFTC are beginning to take a closer look at decentralized blockchain markets, which could include scrutiny of MEV extraction.

MEV extraction may involve arbitrage between crypto-asset markets, which tends to be seen as a beneficial contribution to price accuracy, because it leads to equalizing prices of the same asset across markets. It may also, however, involve so-called "front-running" of transactions, which can be enabled by the ability of at least some market participants to see the details of pending transactions before they are executed.

The most prominent example of this type of transaction is called "sandwiching": buying an asset ahead of another known pending buy transaction, and then selling the asset, thereby profiting from the positive price impact of the transaction in the middle of the "sandwich." Sandwiching normally results in a worse execution price for the sandwiched trade and tends to be seen as an undesirable practice. According to the data-analysis platform EigenPhi, the volume of sandwich attacks reached $54.37 billion in the first half of 2022, causing traders to lose $87.7 million.[9]

This suggests that MEV extraction is a significant phenomenon that may adversely affect some market participants in some transactions. Moreover, some forms of MEV extraction—particularly so-called "time-bandit attacks"[10]—could pose a systemic threat to Ethereum, although they remain, for now, mostly theoretical. Nonetheless, as I discuss, to assess whether strategies like sandwiching should be seen as a policy problem requires more robust evidence and analysis than has been offered to date.

In this paper, I consider whether MEV extraction poses a problem that merits public-policy intervention. I argue that the mere fact that MEV extraction may adversely affect some market participants is not sufficient to answer that question. As in stock trading, which may likewise appear to be

[7] S.5267 - Digital Asset Anti-Money Laundering Act of 2022, 117th Congress (2021-2022).

[8] Press release, *CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate Over $110 million from Mango Markets, a Digital Asset Exchange*, COMMODITY FUTURES TRADING COMMISSION (Jan. 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8647-23.

[9] *Flash Boy's Gain, Everybody's Pain: 2022 Mid-Year Report of Sandwich MEV on Ethereum*, EIGENPHI RESEARCH (2022), https://eigenphi.substack.com/p/flash-boys-gain-everybodys-pain

[10] Daian *et al.*, *supra* note 1 at 16.

a zero-sum game with a "winner" and "loser" in each transaction, the nature and effects of MEV extraction have more dimensions that need to be considered.

It is important to carefully consider the costs and benefits of regulatory responses to MEV extraction. For example, while licensing requirements for dealers and brokers may be appropriate in the current "traditional" finance context, they may be inadvisable for block builders or relay operators. At the risk of sounding hyperbolic, a country that adopts such measures could be giving up on the benefits of decentralized and permissionless public blockchains like Ethereum. Hence, the benefits of such regulations should be carefully weighed against the potential cost of lost social benefits.

Moreover, regulation and regulatory enforcement in the realm of public blockchains faces the problem of regulatory arbitrage. Operators may choose the most favorable jurisdictions, while retaining influence on markets in other jurisdictions. This provides a strong argument to prefer and support technical solutions (*e.g.*, on the level of the Ethereum protocol) that would apply globally over national or even international legal rules.

This paper is intended to be accessible to non-technical readers, and therefore employs simplified technical explanations. For greater detail, please follow the references provided. I also do not aim to provide comprehensive legal analysis, but merely note some of the *prima facie* legal issues. I build here on a working paper I co-authored with Alex Sarch,[11] and on my brief comment published on the Flashbots forum.[12]

II. How Is MEV Extracted?

This section provides a brief overview of what MEV extraction is, as well as the actors involved in the MEV ecosystem. The overview is intended for those who are *not* familiar with MEV in general (Section II.A) and the developments in MEV extraction since Ethereum's move to "proof of stake" (Section II.B). Readers familiar with both can skip this section and proceed directly to Section III.

[11] Mikołaj Barczentewicz & Alex F Sarch, *Shedding Light in the Dark Forest: A Theory of Liability for Cryptocurrency "MEV" Sandwich Attacks*, SSRN (2022), https://ssrn.com/abstract=4187752.

[12] Mikolaj Barczentewicz, *Law and Regulation vs MEV Extraction*, FLASHBOTS (Oct. 7, 2022), https://collective.flashbots.net/t/law-and-regulation-vs-mev-extraction/477.

A. A Simple Model of MEV Extraction

To understand the core case of MEV extraction, we need two basic concepts: a "transaction" and a "block." As the name suggests, the Ethereum *blockchain* is a chain of blocks. For our purposes, we'll consider blocks as ordered batches of transactions (typically up to several hundred). A transaction can be a simple transfer of some amount of Ether (or ETH, the cryptocurrency) from one account to another. It may also be a trade of some token (*e.g.*, DAI) for another token, using one of the decentralized exchanges, which run as smart contracts on Ethereum (*e.g.*, Uniswap). The latter case is one of the key sources of MEV. Without getting into more technical detail about "automated market makers" and "liquidity pools,"[13] it should not be surprising that it matters *in what order* exchange trades are executed. A trade executed earlier (or later) may have a more attractive price. Also, trading just *before* or *after* another trade may create profit opportunities, as in the cases of "back-running" or a "sandwich."[14] As I wrote with Alex Sarch:

> Consider "what happened on 16 February 2022 to a person using the Ethereum address 0x61…38 (we will call them '0x61'). 0x61 attempted to exchange just over 79 Ethereum (then worth around $250,000) for DAI (a stablecoin targeting a 1 to 1 exchange ratio with US Dollar), using the decentralized exchange Uniswap V2. Instead of receiving, after fees, around $225,000-worth of DAI, as 0x61 may have expected, they ended with around $179,000 – $46,000 less. What seems to have occurred here, was a 'sandwich' attack. An automated 'searcher bot' (using the address 0x26…af) noticed 0x61's transaction while it was still waiting to be executed (in the 'mempool') and calculated that it presents an opportunity for a profitable sandwich.
>
> A sandwich consists of three elements: (1) the front-run, (2) at least one sandwiched transaction (in this case 0x61's trade), and (3) the back-run. The general idea is to buy an asset at a lower price (the front-run) and then profit from selling it at a higher price (the back-run).
>
> In this case, the price of DAI against Ethereum rose due to two purchase transactions: the sandwicher's transaction (the front-run) and then the sandwiched transaction itself. To execute this sandwich, the bot first traded 850 Ethereum for 2,273,029 DAI on Uniswap (the front-run). This trade was large enough to affect the Ethereum/DAI exchange rate to such an extent that 0x61 'lost' $46,083.7 Finally, the bot traded 2,273,029

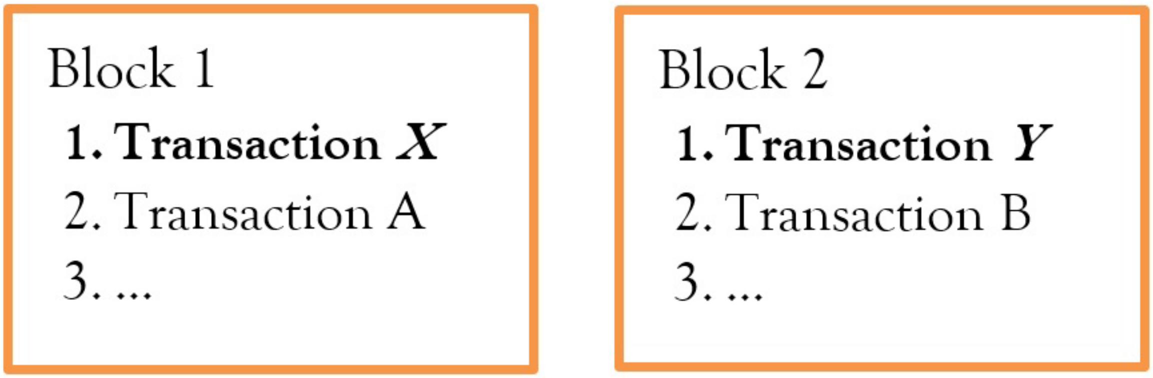
[13] For an accessible introduction, *see* Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *Trading in the DeFi Era: Automated Market-Maker*, BIS QUARTERLY REVIEW (2021), https://www.bis.org/publ/qtrpdf/r_qt2112v.htm. *See also* Jiahua Xu *et al.*, *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols*, ACM COMPUT. SURV. (2022), https://doi.org/10.1145/3570639.

[14] For a more technical explanation, *see* Liyi Zhou *et al.*, *High-Frequency Trading on Decentralized On-Chain Exchanges*, *in* 2021 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) 428 (2021), https://ieeexplore.ieee.org/document/9519421.

> DAI for 868 Ethereum, ending with 18 Ethereum (worth over $56,000) more than they started with."[15]

The order of transactions in a block is decided by the validator.[16] On Ethereum, a new "slot" opens every 12 seconds and a randomly chosen validator is given the power to propose a block. The Ethereum protocol constrains the validator only as to the maximum amount of content (measured by computational complexity) that can be included in a block. There is no minimum (a block can contain, *e.g.*, one transaction), and no requirements as to *which* pending transactions are to be included and in *what order*.

Let's distinguish two transaction-ordering scenarios. Transaction *X* could be executed earlier than Transaction *Y*, because Transaction *X* is included in an earlier block than *Y*. In this case, *X* and *Y* are executed at different clock times (at least 12 seconds apart, assuming that Blocks 1 and 2 are consecutive).



Block 1

1. Transaction *X*
2. Transaction A
3. ...

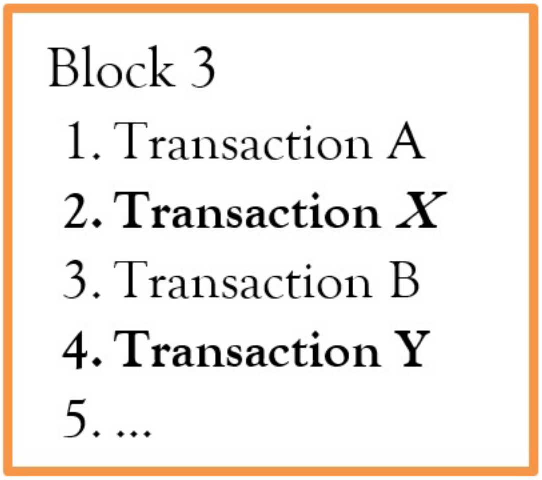
Block 2

1. Transaction *Y*
2. Transaction B
3. ...

Note, however, that there is also an order of execution of transactions *within a block*. Hence, in Block 3, *X* could also be executed before *Y* because *X* is listed in an earlier position than *Y* within the same block.

[15] Barczentewicz & Sarch, *supra* note 11.

[16] A validator, or a group (pool) of validators, may also find themselves in control of several consecutive blocks, as illustrated, *e.g.*, in Metrika's research on the first weeks of proof-of-stake Ethereum; *see Validators or Value-Takers?*, METRIKA (2022), https://blog.metrika.co/validators-or-value-takers-e71f46047437.



Block 3

1. Transaction A
2. **Transaction *X***
3. Transaction B
4. **Transaction Y**
5. …

Given this freedom in block building, validators can profit (extract MEV), for example, by constructing sandwiches or performing liquidations or arbitrage (see Section III below for a discussion of which of those strategies are considered desirable or undesirable). Validators can also accept payments for ordering blocks in a specific way from specialized operators (the "searchers") who are proficient in identifying MEV-extraction opportunities.

In this simple model, the validator has three potential sources for transactions to include in a block: "(1) their own transactions, (2) transactions delivered to them privately, or (3) transactions from the mempool, which is a public collection of pending transactions broadcasted to the Ethereum network."[17]

B. MEV Extraction Under Proposer-Builder Separation

The simple model of MEV extraction—involving only searchers and miners (validators)—was prevalent on Ethereum until the widespread adoption of the Flashbots "relay," initially introduced in November 2020.[18] The service provided by Flashbots changed fundamentally with Ethereum's move from "proof of work" to "proof of stake" ("the Merge") on Sept. 15, 2022.[19] Here, I will cover only the current version, which introduced Proposer-Builder Separation ("PBS") to Ethereum.[20]

[17] Barczentewicz & Sarch, *supra* note 11.

[18] @phildaian, Twitter (Nov. 23, 2020, 8:37 AM), https://twitter.com/phildaian/status/1330868049092747267.

[19] Mikhail Kalinin, Danny Ryan & Vitalik Buterin, *EIP-3675: Upgrade Consensus to Proof-of-Stake*, Ethereum.org (2021), https://eips.ethereum.org/EIPS/eip-3675; *The Merge*, Ethereum.org, https://ethereum.org/en/upgrades/merge.

[20] Brock Smedley, *Searching Post-Merge*, Flashbots (Aug. 24, 2022), https://writings.flashbots.net/searching-post-merge.

Under PBS, as currently implemented on Ethereum, the role of a validator is split into two parts: block *building* and block *proposing*. Acting as a mere proposer, a validator adopts a block entirely constructed by a specialist block builder, thus relinquishing control over the contents of a block.[21] Typically, validators do not connect directly to block builders, but to *relays*, which in turn collect candidate blocks from block builders and choose the best one.[22] Hence, the MEV-extraction ecosystem currently includes: searchers, block builders, relays, and validators.

Given that PBS is optional for validators, they remain free to control the contents of a block (and thus extract MEV on their own). However, a validator that does so forgoes the benefits of outsourcing control to block builders, who are likely better at identifying MEV-extraction opportunities.

Block builders have the same three sources of transactions as validators did before the Merge:

1. They can act as searchers and include their own MEV-extracting transactions.
2. They can include transactions submitted to them *privately*, including those submitted by external searchers. A searcher may offer the block builder a fee (a "bribe") as an incentive to include a transaction.
3. They can include pending transactions broadcast *publicly* in the Ethereum peer-to-peer network ("mempool" transactions).[23]

Notably, in addition to accepting individual transactions submitted by searchers, block builders like the one operated by Flashbots also accept "bundles" of transactions. Through this process, the block builder ensures "that all transactions in a bundle are executed in the set order or none of them are

[21] This does not mean that proposers will never have control over block contents under PBS. One currently discussed scheme, which could involve proposers requiring inclusion of at least some transactions in blocks that they do not build, is known as "crlists." *See Censorship Resistance: Crlists in Mev-Boost #215*, FLASHBOTS (Jul. 15, 2022), https://github.com/flashbots/mev-boost/issues/215; Vitalik Buterin, *How Much Can We Constrain Builders Without Bringing Back Heavy Burdens to Proposers?*, ETH RESEARCH (October 2022), https://ethresear.ch/t/how-much-can-we-constrain-builders-without-bringing-back-heavy-burdens-to-proposers/13808.

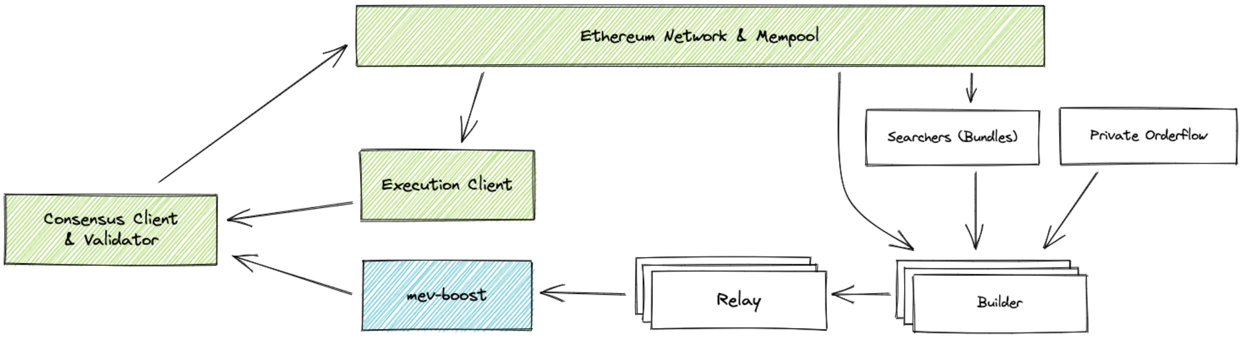
[22] The "best" block is the block that offers the highest fee while satisfying the conditions of a given relay, such as by not including transactions that interact with addresses on the Specially Designated Nationals and Blocked Persons ("SDN") list maintained by the U.S. Treasury Department's Office of Foreign Asset Control.

[23] The standard way to broadcast an Ethereum transaction is to send it to at least one "node," which is a computer running Ethereum-execution client software, such as Go Ethereum (geth). Nodes communicate peer-to-peer, broadcasting transactions that they receive from users and other nodes. Each node keeps a "mempool," which is a collection of all pending transactions (not yet included in the blockchain), received directly by that node or from other nodes. There is no single mempool, strictly speaking, as the contents of node mempools diverge—*e.g.*, because it takes time for information about new transactions submitted by users to reach all the nodes. It is, however, also customary to simplify this picture and speak of "the mempool," referring to a set of pending transactions that are publicly broadcasted and received by at least some nodes. *See*, generally, *What Is the Mempool?*, BLOCKNATIVE (2020), https://www.blocknative.com/blog/mempool-intro; Sahil Sen, *How to Access Ethereum Mempool*, QUICKNODE (2022), https://www.quicknode.com/guides/defi/how-to-access-ethereum-mempool; see *Id.*

executed. This makes MEV-extraction strategies like sandwiches easier and less risky than going through the public route. A searcher may notice a publicly broadcasted transaction including a potentially sandwichable trade and then bundle that transaction with the searcher's own front-run and back-run, and submit the whole bundle of three transactions to a block builder (*e.g.*, Flashbots). Note that this involves the searcher taking (copying) a transaction submitted by someone else and then resubmitting it as a part of the searcher's bundle."[24]

They can include pending transactions broadcasted *publicly* in the Ethereum peer-to-peer network ("mempool" transactions).

Figure 1: Schematic Illustration of the Current MEV-Extraction Pipeline



Source: Flashbots, *What Is MEV-Boost?*[25]

The final piece of the puzzle needed to ground the following discussion is to explain how Ethereum transactions are broadcast from a user to the network. Normally, a user submits a transaction with the use of "wallet" software, such MetaMask. The key issue is *to whom* a user submit their transaction. As I note later, if—as is typical—the user submits their transaction only to one operator, this puts the operator in a privileged position, enabling them to treat user transactions as a kind of "private order flow," potentially for the purposes of MEV extraction. Note that nothing about how Ethereum works *guarantees* that a transaction submitted by a user will be public information while pending.[26]

The services where users submit transactions through wallet software are known as "RPC endpoints." An RPC endpoint responds to a set of instructions, to which nodes of the Ethereum network also respond. It does not, however, have to perform the functions usually associated with a network node, particularly re-broadcasting (forwarding) the transaction to other nodes. An RPC endpoint operator faces a choice among (1) doing nothing (in a sense, censoring the transaction);

[24] Barczentewicz & Sarch, *supra* note 11 (citations omitted).

[25] *What Is MEV-Boost?*, FLASHBOTS, https://docs.flashbots.net/flashbots-mev-boost/introduction.

[26] *See also supra* note 23.

(2) re-broadcasting the pending transaction in a way that makes it *public*; or (3) keeping it *private* and forwarding it directly to some block-builders or validators. In fact, the third choice is the advertised way in which some *privacy RPCs* operate (*e.g.*, Flashbots Protect[27]). The primary reason that privacy RPCs were developed was to offer users protection against unwanted kinds of MEV extraction.

III. Is MEV Extraction a Policy Problem?

As in many other aspects of blockchain, discussions of MEV are rife with ill-considered or emotionally charged language borrowed from other contexts, such as "harm," "attack," "victim," and "theft." Descriptions of MEV in terms of "harm" and "victimhood" are based on the question-begging assumption that the "victim" has been deprived of something that was rightfully hers. Whether that is the case is likely to be a more complicated question, because MEV extraction rarely involves depriving someone of a good they already possess. Instead, it tends to involve some actor achieving smaller economic gains than they might have in a counterfactual scenario in which MEV had not been extracted. Moreover, some kinds of MEV extraction—like so-called "generalized front-running"—may be analogous to hunters chasing a prey. The law does not necessarily reward an unsuccessful hunter, irrespective of the effort they put in or their claim to being the first to spot an opportunity.

This is important context to consider when evaluating statistics like EigenPhi's estimate that there were $54.37 billion of sandwich attacks in the first half of 2022, which caused traders to "lose" $87.7 million,[28] or the Bank of International Settlements' estimate that there has been between $550 and $650 million of total MEV since 2020.[29] The statistics suggest that MEV extraction is a relatively significant phenomenon that adversely affects (at least, compared to a non-MEV counterfactual) some market participants in some transactions. But they do not, on their own, show that those adverse effects are a policy problem.

Rather than attempt to resolve the question definitively of whether there are any kinds of MEV extraction might potentially pose a policy problem, I instead propose a framework to think about the issue. To begin, I will summarize previous attempts to classify various kinds of MEV extraction into "good" and "bad" categories, ultimately finding that a binary classification is unhelpful, especially from a policy perspective. I then consider a more sophisticated framework to think about

[27] *Quick Start*, FLASHBOTS, https://docs.flashbots.net/flashbots-protect/rpc/quick-start.

[28] EigenPhi Research, *supra* note 9.

[29] Auer et al., *supra* note 2.

different types of MEV ("Mafia, Moloch, and Monarch"). With that, I turn to a discussion of effects of MEV extraction on individual and social welfare. I suggest that social-welfare considerations—especially market efficiency—should be pivotal in policy analysis of phenomena like MEV extraction.

A. Classifying MEV

1. *Toxic and Nontoxic*

A first step to understand MEV is to consider the various value-extraction strategies that blockchain validators are in a privileged position to execute or control. In addition to sandwiching (discussed in Section II), the paradigmatic cases include: arbitrage, liquidations, generalized front-running, and specialized front-running (*e.g.*, mints of nonfungible-tokens, or NFTs).[30] Sandwiching and most of other front-running are often labelled "toxic MEV," because the transaction that is front-run either executes at worse conditions than otherwise (*e.g.*, a worse trade price) or fails to execute (*e.g.*, because the front-running transactions scoops a limited opportunity, like minting an NFT). Though this is often-overlooked, strategies that only involve back-running—*i.e.*, placing a transaction *after* some target transaction—also may execute in worse conditions. This could happen when the would-be MEV extractors can delay the transaction's inclusion until the moment when it will create the best profit-making opportunity.

"Nontoxic MEV" is said to include arbitrage and liquidations. Arbitrage refers to "the process of simultaneously selling and buying assets in different markets in order to profit from the market price differences."[31] As Kaihua Qin *et al.* note, it "helps to promote market efficiency and is typically considered benign."[32] Liquidations occur in on-chain lending applications and involve purchasing collateral that secures a loan where the value of the collateral has fallen below the set-safe level for the loan. Anyone could repay the "bad" debt, while being rewarded with the ability to purchase the collateral at a discount.[33] Arbitrages help to keep prices aligned across decentralized markets, while liquidations help to secure lending systems from being stuck with bad debt. Those competitive strategies constitute MEV because there is value in being able to control who has the opportunity to

[30] *See, e.g.*, Kaihua Qin, Liyi Zhou & Arthur Gervais, *Quantifying Blockchain Extractable Value: How Dark Is the Forest?*, in 2022 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) 198 (2022); *Extractable Value*, AMBER GROUP (2022), https://medium.com/amber-group/extractable-value-7b0d4356a843.

[31] *Id.* at 6.

[32] *Id.*

[33] *Id.* at 2.

benefit from a given arbitrage or liquidation opportunity, which requires the ability to control the ordering of transactions within a block.

The distinction between toxic and nontoxic MEV is grounded solely in the effect of MEV extraction on the directly affected transaction. Arguably, this makes "toxic" and "nontoxic" unhelpful designations, because the terms presuppose that the phenomenon is on-balance bad. But as I note in the discussion below of market efficiency, even if a user "loses" on a single transaction, she may still derive indirect benefits from the existence of MEV extraction that outweigh those losses. On the other hand, even arbitrages or liquidations that don't qualify as "toxic"—because they don't adversely affect any single transaction—may still have significant negative effects on the market as a whole (*e.g.*, spam and network clogging where MEV searchers must resort to priority gas auctions).[34]

2. Oracle Manipulation

Among the undesirable MEV-extraction strategies that do not need to adversely affect any specific transactions is "oracle manipulation,"[35] the only market strategy discussed here that has, thus far, resulted in a government-enforcement action.[36] Oracle manipulation can take different forms, but it generally involves manipulation of a benchmark mechanism (an "oracle") on which some on-chain application (smart contract) relies. Given that on-chain applications like lending systems and decentralized exchanges typically do not have robust internal price-discovery mechanisms, they rely on external sources of information about asset prices to provide a positive user experience (users expect asset prices to be similar across different applications and markets) and to prevent manipulation. It is often publicly known upon which external sources an on-chain application relies and how a specific price change reported by a source would affect the application. Hence, it may sometimes be profitable to affect the price on a market that serves as an external benchmark: *e.g.*, to lower that price, in order to cause a liquidation opportunity on some lending application, which relies on the price from that reference market ("liquidation attack").[37]

Oracles can report prices from other on-chain applications, but they can also report prices from outside the blockchain, *e.g.*, from a centralized exchange like Coinbase or Binance. This means that oracle manipulation can be done either fully on-chain or in a mixed on-/off-chain strategy, where someone attempts to affect off-chain prices—*e.g.*, on Coinbase—to profit from the effect this will have

[34] Daian *et al.*, *supra* note 1.

[35] Torgin Mackinga, Tejaswi Nadahalli, & Roger Wattenhofer, *TWAP Oracle Attacks: Easier Done than Said?*, in 2022 IEEE INTERNATIONAL CONFERENCE ON BLOCKCHAIN AND CRYPTOCURRENCY (ICBC) 1 (2022).

[36] *See supra* note 9.

[37] Mackinga, Nadahalli, & Wattenhofer, *supra* note 35 at 2.

on some on-chain application.[38] Strictly speaking, the off-chain stage of a mixed oracle-manipulation strategy does not constitute MEV extraction, but its on-chain element may. The Mango Markets oracle-manipulation strategy deployed by Avi Eisenberg, which resulted in his prosecution by the U.S. government,[39] reportedly involved a successful attempt to raise prices both on off-chain (FTX) and on-chain (Raydium) markets.[40]

Both fully on-chain and mixed on-/off-chain versions of oracle manipulation may involve MEV, because an agent who succeeds in affecting the price in a reference market may create at least one profit opportunity (*e.g.*, arbitrage, liquidation) that is publicly visible and that, in principle, *anyone could realize*. The challenge is to be the first. Thus, attempting the first stage of this strategy, which is likely to be costly, is only rational if the agent is confident that they will be the one to profit from the second stage. A guarantee that one will be able to realize such an opportunity is likely to come from controlling the contents of a block. One of the beneficial effects of the competition among sophisticated actors for liquidation opportunities is that actors who are not colluding with the would-be manipulator may spot the liquidation opportunity and be able to out-bid them. Because they did not incur the cost of the first stage of the strategy (affecting the price on the reference market), they may be well-positioned to offer a higher fee to the validator (proposer). This risk to would-be manipulators makes this kind of oracle manipulation less likely to be profitable. Similarly, arbitrage strategies can help to counteract "undercollateralized loan attack" oracle manipulations.[41]

If an oracle-manipulation strategy is executed as a *multi-block MEV extraction*, however, the standard MEV-extraction strategies (liquidations, arbitrage) may not help to prevent the manipulation. If an agent controls two consecutive Ethereum blocks (*e.g.*, because they are selected as the proposer for those two blocks), then they would be able to execute an oracle attack in a virtually riskless way, as demonstrated by Torgin Mackinga *et al.*[42] To be randomly selected as a proposer of two consecutive blocks once a month may currently require running around 1,250 validators—*i.e.*, staking 40,000

[38] *See, e.g.*, Scott Chipolina, *Oracle Exploit Sees $89 Million Liquidated on Compound*, DECRYPT (Nov. 26, 2020), https://decrypt.co/49657/oracle-exploit-sees-100-million-liquidated-on-compound; *Coinbase & the Oracle*, REKT (Nov. 26, 2020), https://rekt.news/coinbase-the-oracle.

[39] *See supra* note 9.

[40] Khor Win Win, *Insights and Implications of the Mango Squeeze*, COINGECKO (Nov. 21, 2022), https://www.coingecko.com/research/publications/insights-and-implications-of-the-mango-squeeze.

[41] Mackinga, Nadahalli, & Wattenhofer, *supra* note 35 at 2.

[42] *Id.* at 6.

ETH (over $53 million).[43] This capital would not necessarily be lost, however, as an oracle manipulation would not breach Ethereum consensus rules.[44]

3. Mafia, Moloch, & Monarch

Flashbots researcher Xinyuan Sun has proposed a different classification of MEV, attempting to place what had been previously understood as MEV in a broader framework of extractable value.[45] He distinguished three types of extractable value:

- "Monarch" extractable value refers to the more broadly accepted understanding of MEV, as value extractable due to the power to order and allocate (block) space.
- "Mafia" extractable value "arises when one agent (coalition of agents) gains an asymmetric knowledge of another agent's private information (asymmetric sophistication)."[46]
- "Moloch" extractable value arises from inefficient coordination methods.[47]

As examples of Mafia EV, Sun provided sandwiching and generalized front-running, which may appear to be extractable due to Monarch EV—*i.e.*, due to control of block space. But in my reading, the value of the distinction lies in the fact that, if asymmetric informational sophistication (Mafia EV) is reduced, then sandwiching may also be reduced. In other words, the true source of sandwiching is not control of block space (Monarch), but in the lack of privacy about user intentions and in asymmetries of sophistication in acting on information about user intentions (Mafia).

Moloch EV stems from inefficient coordination methods like "first come, first served" or random ordering of transactions. Time-based ordering may, at first glance, appear to be fair, in that it puts users (market participants) on equal footing. This equality may be illusory, however, because time ordering can create incentives for an arms race in speed, similar to the techniques used by high-frequency traders in traditional finance. Participating in this arms race requires skill and resources, undermining the understanding of fairness as equality of access. In turn, random ordering creates incentives for spamming (submitting many transactions, hoping that some will be executed at the

[43] Own calculation assuming a total number of 500,000 validators using the code provided by Alvaro Revuelta. *See* Alvaro Revuelta, *Statistical Analysis on Ethereum K-Consecutive Block Proposal Probabilities and Case Study* (Aug. 14, 2022), https://alrevuelta.github.io/posts/ethereum-mev-multiblock; *See also supra* note 16.

[44] Mackinga, Nadahalli, & Wattenhofer, *supra* note 35 at 6.

[45] Xinyuan Sun, *This Is MEV*, DEVCON BOGOTA (Oct. 11-14, 2022) https://www.youtube.com/watch?v=8qPpiMDz_hw; *see also* Xinyuan Sun, *PBS and Layer 2s*, SCIENCE OF BLOCKCHAIN CONFERENCE: MEV WORKSHOP (Sep. 1, 2022) https://www.youtube.com/watch?v=JCZDd0iCMsg.

[46] *Id.*

[47] *Id.*

right position to realize some profit opportunity), which also requires skill and resources to execute effectively. To reduce Moloch EV, Sun recommends explicit auction mechanisms to allow aggregating user preferences efficiently.

Sun advocates reducing the amount of value extractable from asymmetric informational sophistication (Mafia) and inefficient coordination (Moloch), but stresses that this will leave us with value that is extractable solely due to control over block space (Monarch). Given that the most profitable kinds of MEV extraction today—*e.g.*, sandwiching—depend on a lack of privacy, the "[Mafia] 0%, [Moloch] 0%, [Monarch] 100%" scenario would mean less value extracted, and possibly much less, but not zero. Like some others,[48] Sun advocates distributing the remaining Monarch EV in ways that maximize social welfare, instead of distributing value associated with a transaction to the user who submitted that transaction.

B. Individual Welfare and Legally Relevant Harm

Not every subjectively perceived harm is relevant to public policy, nor does every harm qualify as the kind of harm with which the law should be concerned. The law rightly protects only some interests. If the market price of an asset you have purchased depreciates, you may consider yourself harmed. But only under certain special conditions should the law respond (*e.g.*, if you were defrauded). The law rightly protects only selected interests. You don't have a legally protected interest in making as much money as possible on any given trade, but you do have a legally protected interest in avoiding fraud or prohibited market manipulation. I discuss the difficulties in applying legal concepts like fraud and theft to MEV extraction in Section IV.

1. Is MEV Extraction Ever Unfair?

A policy response will be most straightforwardly justifiable when harm to individual welfare is significantly unfair. Unfairness in trading could arise, *e.g.*, due to asymmetries of information or of market power, although most would agree that superior skill and luck in a trade do not render a trade unfair.[49] Notably, only some information asymmetries are considered legally relevant, as in the case of trading on material nonpublic information (insider trading).

In our discussion of sandwiching under U.S. commodities law, Sarch and I considered the argument that sandwiching is not unfair, because the sandwiched traders *expressly consent* to their transaction

[48] *See, e.g.*, Tarun Chitra & Kshitij Kulkarni, *Improving Proof of Stake Economic Security via MEV Redistribution*, *in* PROCEEDINGS OF THE 2022 ACM CCS WORKSHOP ON DECENTRALIZED FINANCE AND SECURITY 1 (2022).

[49] Gina-Gail S Fletcher, *Legitimate yet Manipulative: The Conundrum of Open-Market Manipulation*, 68 DUKE LJ 479, 493, 530 (2018).

being executed at the price they obtain while being sandwiched (similar to a limit order on a book exchange).[50] We noted a possible rejoinder that traders may sometimes become, *e.g.*, "forced" sellers during a time of heightened market volatility in that they must set wide limits for their transaction (*i.e.*, slippage tolerance). But traditional securities exchanges also experience periods of heightened volatility, which are not seen as negating the consensual nature of trading. Volatility *could* be either a sign of or an instrument in market manipulation, but that conclusion requires more evidence.

We concluded our discussion on this point by noting that, as on traditional exchanges, the key issue is whether abnormal and "manipulative" market activity occurred. Issues like express consent to the conditions of the trade or the existence of market volatility (and who induced it) may be factors in assessing whether there has been manipulation, but they are not necessarily dispositive in that assessment.

My purpose in referencing the above discussion of trader consent was to illustrate some of the difficulties in reasoning about unfairness.[51] Due to those difficulties, it may be that the best approach to *legal prohibitions* of market activities is to focus not on unfairness, as such, but on harms to market efficiency. Gina-Gail Fletcher suggested that "claims for open-market manipulation based on" "transactions between anonymous counterparties on public exchanges" "should be limited to claims based on harm to market efficiency."[52] In other words, in Fletcher's view and for reasons discussed in her work, if a market strategy—in this case, various kinds of MEV extraction—does not harm market efficiency (and might possibly even increase it), it should not be deemed impermissible market manipulation. It is possible, however, that some jurisdictions will approach this issue differently, deriving rules from other moral precepts regarding market orderliness (integrity) or the protection of settled expectations about how trades are to be executed, even where there is no evidence of harm to market efficiency.[53]

Setting aside purely legal questions, it may be a *policy* problem that there is a widespread *perception of unfairness* of some practice or that the practice jeopardizes "market integrity,"[54] even if that practice does not otherwise harm market efficiency. Perceptions of market integrity may, however, also push in the opposite direction, particularly with respect to concerns that are at least partially alleviated by some kinds of MEV extraction. Examples might include the accrual of bad debt (which can be

[50] Barczentewicz & Sarch, *supra* note 11.

[51] For a discussion of the difficulties inherent in applying the standard of fairness, *see also* MERRITT B FOX, LAWRENCE GLOSTEN, & GABRIEL RAUTERBERG, THE NEW STOCK MARKET: LAW, ECONOMICS, AND POLICY 49–55 (2019).

[52] Fletcher, *supra* note 49 at 533.

[53] Barczentewicz & Sarch, *supra* note 11 at 16. *See also infra* notes 84-85 and the accompanying text.

[54] Fletcher, *supra* note 49 at 492–493.

addressed by liquidations) or widely varying prices across decentralized-finance (DeFi) markets (which can be addressed by arbitrage).

I suggest that, rather than attempting to enforce existing legal prohibitions against some MEV extraction practices or imposing new prohibitions, the optimal policy response to perceptions of unfairness connected with MEV extraction may be to create incentives for—and otherwise facilitate—market solutions to the perceived problem. I discuss such alternative solutions in Section V.

2. Market Efficiency and Social Welfare

I cannot answer here the question of what net effect any particular kind of MEV extraction has on market efficiency, or on social welfare more broadly. Doing so would require significantly more research on the economics of MEV extraction than has been conducted to date. Given the differences between decentralized crypto-assets markets and traditional finance, it cannot be assumed that empirical findings about the latter can be applied to the former. From a policy perspective, this research gap should prompt caution in resorting to "hard" measures like enforcement or rulemaking on MEV extraction. In what follows, I outline some of the considerations that will likely need to be developed to address the question of how to estimate the net social-welfare effects of MEV extraction. This is not meant as a comprehensive survey, but rather an illustration of how the relevant issues differ significantly from traditional finance.

In traditional finance, market efficiency is typically analyzed with reference to factors like price accuracy, degree of market liquidity, and efficient allocation of resources or risk.[55] However, maximizing all of those factors is likely impossible and would, in any case, not achieve maximal market efficiency, as some goals may conflict. For example, insider trading may improve price accuracy, but negatively affect market liquidity (traders without inside information will trade less if they expect to trade against insiders).[56]

Since the basic "plumbing" of decentralized crypto markets is different from traditional markets, concerns about market efficiency may also differ significantly. Decentralized exchanges (DEX) on Ethereum, such as Uniswap V3, are code that runs directly on the blockchain. The existence and security of the market is tied to the existence and security of the blockchain. Thus, arguably, market efficiency for DEX-es is more closely connected to the overall health of the underlying blockchain than in traditional finance—where, *e.g.*, the existence and security of a stock exchange can more often be abstracted from (taken as a given) when assessing the net market effects of some trading strategy.

[55] *See, e.g.*, Fletcher, *supra* note 49; Fox, Glosten, & Rauterberg, *supra* note 51.

[56] Fox, Glosten, & Rauterberg, *supra* note 51 at 67–75.

Moreover, the scope of the "market" in a policy analysis of MEV extraction should arguably be broader than an analogy with traditional finance would suggest. MEV extraction is not limited to DeFi, where "finance" is understood as exchanging assets or lending them. For example, some very valuable MEV also arises in the context of NFT minting and sales. All products or services that are offered through on-chain mechanisms—many of which are not yet invented—potentially give rise to MEV. This also counts in favor of including effects on the overall functioning of a blockchain in the scope of market-efficiency analysis.

MEV-extraction strategies may have complex and positive effects on various aspects of on-chain markets. The mechanisms of those positive effects may be specific to blockchains, in which case, intuitions and analogies from traditional finance may be of limited help. For example, Kulkarni, Diamandis, & Chitra recently suggested that "while individual trades that are sandwiched undoubtedly receive worse prices, sandwiches can cause more effective routing patterns as some flow avoids sandwiches edges."[57] This result was found through theoretical analysis (algorithmic game theory); we would therefore need additional empirical research to know how significant such positive effect is for overall market efficiency. If effects like this are relatively significant, however, then it is possible that at least some kinds of MEV extraction are net-beneficial for market efficiency. It could also be the case that the welfare of an individual trader who is made worse off by MEV extraction in some specific trades is not worse off on balance, because she also benefits from positive effects of MEV (this also applies to the security-budget consideration raised below).[58]

The key issue for the security of a blockchain like Ethereum is whether there is sufficient incentive for independent good-faith validators (with enough ETH being "staked" to provide economic security)[59] as to ensure "liveness" (*i.e.*, that the blockchain will not stop operating) and to make an attack on the blockchain too expensive to be worth attempting.[60] Some have argued that allowing Ethereum validators to profit from MEV extraction may be helpful in providing this incentive, because standard validator rewards are insufficient.[61] Even if the standard rewards are sufficient relative to *current* threats, those threats could increase and require a significant increase in Ethereum's

[57] Kulkarni, Diamandis, & Chitra, *supra* note 1 at 8.

[58] *Cf.* Fox, Glosten, & Rauterberg, *supra* note 51 at 52.

[59] The website Ultra Sound Money introduced the helpful concept of the "security ratio," which it defines as "[t]he ratio of total value secured (TVS) to economic security. It measures attacker leverage—lower is better." Ethereum's TVS is currently 17.5x; https://ultrasound.money.

[60] Tarun Chitra, *Competitive Equilibria Between Staking and On-chain Lending*, 1 CRYPTOECONOMIC SYSTEMS (2021), https://cryptoeconomicsystems.pubpub.org/pub/chitra-staking-lending-equilibria; Chitra & Kulkarni, *supra* note 51.

[61] Chitra & Kulkarni, *supra* note 48. *See also* the referenced tweets and associated discussion on the role of MEV extraction in chains without block subsidy (this does not apply directly to Ethereum, as it has a block subsidy):
@gakonst, TWITTER (Feb. 26, 2021, 7:47 AM), https://twitter.com/gakonst/status/1365191821375193088; @DZack23, TWITTER (Mar. 3, 2021, 8:51 PM), https://twitter.com/DZack23/status/1367201076269772802.

"security budget" (the amount of ETH staked) to defend against such a risk. Moreover, staking—*i.e.*, contributing to the security budget—competes with other capital uses, such as on-chain lending. The relative attractiveness of those alternatives reduces the incentives to engage in staking.[62] Theoretically, the security budget could be increased by increasing standard validator rewards, but malicious validators (would-be attackers) would also benefit both from that *and* from a potential attack.

Raising the standard validator rewards would also effectively constitute an additional tax on Ethereum users. Such a tax would also likely be at a nonoptimal rate, given that it would have to be sufficiently large to respond to unpredictable and dynamic risks without being pegged to the level of those risks. In contrast, MEV is correlated with at least some risks (like the profitability of on-chain lending).[63] Proposed solutions include the redistribution of extracted MEV across validators.[64] Note that the argument about the contribution of MEV extraction to Ethereum's security budget is controversial. It could be that staking is, and will continue to be, sufficiently profitable even without significant profits from MEV extraction, especially with new mechanisms like restaking.[65]

Moreover, for some effects on market efficiency, *how* MEV is extracted may be more important than what type of MEV extraction (sandwiching, liquidations, arbitrage back-running, etc.) it is. Early MEV extraction on Ethereum (see the "simple model" in Section II.A) had negative externalities on Ethereum users, because it resulted in spamming the network with large numbers of transactions, thereby raising transaction costs and causing delays. This was remedied by the old Flashbots relay, which has since been replaced by the mechanism described in Section II.B (which also remedies the problem). The relay introduced an auction mechanism, allowing MEV searchers to express their preferences for inclusion of their transactions (or bundles) at the beginning of a block.

Some negative effects of MEV extraction on the broader market are more difficult, though not necessarily impossible, to remove. Given that the security model of a public permissionless blockchain like Ethereum depends on decentralization, it is concerning that MEV extraction currently provides incentives for centralization.[66] Decentralization can be understood in this context as dispersing control over key aspects of the network (especially over which transactions are included on the blockchain) among so many independent actors as to make collusion too costly. The key reasons why MEV extraction encourages centralization are that extracting MEV may require special skills and infrastructure, as well as that some MEV can be captured if an actor (or a group) controls several

[62] Chitra, *supra* note 60.

[63] *Id.*; Chitra & Kulkarni, *supra* note 48.

[64] Chitra & Kulkarni, *supra* note 48.

[65] *See, e.g.*, Westie, *EigenLayer: Supercharging ETH Through Restaking*, BLOCKWORKS RESEARCH (Oct. 18, 2022), https://www.blockworksresearch.com/research/eigenlayer-supercharging-eth-through-restaking.

[66] Amber Group, *supra* note 30; Simon Brown, *MEV Driven Centralization in Ethereum: Part 2*, MEDIUM (Dec. 5, 2022), https://simbro.medium.com/mev-driven-centralization-in-ethereum-part-2-97e4cb612e69.

consecutive blocks.[67] Currently implemented technology (in particular, MEV-Boost) tends to move the nexus of centralization from validators to block builders and relays, without significantly reducing overall centralization. Other solutions to reduce the centralizing effects of MEV extraction are in development (*e.g.*, "the Scourge,"[68] Flashbots SUAVE[69]).

IV. Difficulties in Applying Existing Legal Frameworks

It is not this paper's purpose to provide detailed legal analysis, but an overview of some of the key legal issues is needed to understand the policy landscape surrounding MEV extraction. The legal issues I will mention here fall into two broad categories: relatively straightforward charges (like theft and simple fraud) and infractions that are much more difficult to assess, due to our limited understanding of the net effects of MEV extraction (market-manipulation prohibitions). In both cases, it may be difficult to apply existing legal frameworks to MEV extraction, either because those frameworks clearly don't apply or because it would require showing that the MEV-extraction practice in question is harmful in a relevant way.

A. Theft and Simple Fraud

As Sarch and I noted, MEV extraction may involve fraud, *e.g.*, if someone (like a block builder) extracts MEV from their users despite promising them that they will not.[70] Although this is not currently common, MEV extraction could also relate to (attempted) theft or criminal hacking—*e.g.*, due to generalized front-running of a transaction with the intent to exploit a vulnerability in a smart contract.[71] In the latter case, the important question is whether and at what point the MEV operator

[67] *See, e.g.*, Brown, *supra* note 66; Amber Group, *supra* note 30.

[68] @VitalikButerin, TWITTER (Nov. 5, 2022, 7:09 PM), https://twitter.com/vitalikbuterin/status/1588669782471368704; *see also* Brown, *supra* note 66.

[69] *The Future of MEV is SUAVE*, FLASHBOTS (Nov. 22, 2022), https://writings.flashbots.net/the-future-of-mev-is-suave Chris Powers, *MEV's New Chapter: Beyond Ethereum's Borders*, DOSE OF DEFI (Dec. 9, 2022), https://doseofdefi.substack.com/p/mevs-new-chapter-beyond-ethereums

[70] Barczentewicz & Sarch, *supra* note 11.

[71] Researchers Robert Miller and Yannick recently noted an interesting case of what appears to be a bot (automated software) designed specifically to front-run profitable exploits (hacks) of smart contracts, thereby executing those exploits and profiting from them; *see* @bertcmiller, TWITTER (Jan. 12, 2023, 10:59 AM), https://twitter.com/bertcmiller/status/1613566397954621442; @YannickCrypto, TWITTER (Jan. 12, 2023, 8:04 PM), https://twitter.com/YannickCrypto/status/1613341008032415749.

who unintentionally (but perhaps negligently) copies an exploiting transaction becomes liable civilly or criminally. Similar questions could arise if some or many of the especially profitable MEV-extraction opportunities arise due to someone else's criminal actions (*e.g.*, hacks, ransom/blackmail), but I am not aware of evidence that this is the case.

However interesting such cases of fraud or theft are, it is important to note that they are not currently common or relatively significant. Despite references to, *e.g.*, sandwiches as "theft" or "fraud," neither theft, nor (simple) fraud, apply to the most significant kinds of MEV extraction, without some additional circumstances like the ones mentioned here.

Simple fraud would not normally apply where MEV extractors have not promised anyone that they will not engage in MEV extraction. There may be differences among jurisdictions but, *e.g.*, the 2nd U.S. Circuit Court of Appeals recently emphasized in a LIBOR-manipulation case that, for a finding of wire fraud, it is not sufficient that the defendants' actions "may have violated any reasonable notion of fairness."[72] The prosecution has to prove "false, fraudulent, or misleading" representations.[73] Similarly, in English law under the Fraud Act 2006, fraud requires not just "dishonesty," but also a false representation, a failure to disclose information (where there is a duty to disclose), or an abuse of position (in which the defendant was, at the least, expected not to act against the financial interests of another).

The reason that theft does not usually apply is that "victims" of strategies like sandwiching do not typically lose something they already own. We can speak of a "loss" in such circumstances only by comparing the actual execution of a transaction with a counterfactual. Strictly speaking, we are dealing with a kind of "loss of opportunity."

B. Private Information, Private Order Flow, & Fiduciary Duties

Fraud and potentially some other kinds of civil and criminal liability could arise if, by extracting MEV, someone breaches a legal duty they have toward a user, due to some special legal relationship between the extractor and the user. This may appear unlikely, given the absence of direct service relationships between Ethereum users and various other participants of the Ethereum network. Ethereum, after all, consists of a distributed network of actors (*e.g.*, node operators, validators) who do not have privileged access to users or to information about users. But this view is overly simplistic. There are, in fact, at least three groups of actors who provide services directly to Ethereum users in ways that offer them privileged access to information or to control over user transactions:

[72] *United States v. Connolly*, 24 F.4th 821, 843 (2d Cir. 2022).

[73] *Id.*

1) Operators of Ethereum nodes or private relays (RPC endpoints) to which users submit their transactions.
2) Operators of Ethereum nodes (RPC endpoints) used to query the blockchain (*e.g.*, to estimate gas/transaction fees for a potential transaction).
3) Operators of off-chain applications (websites, mobile apps) who facilitate the use of on-chain applications—*e.g.*, software wallets and web "front ends" for smart contracts.[74]

All three groups may be in a privileged position to extract MEV from their users' transactions through their ability to analyze the trading intent associated with a pending transaction, either earlier than other MEV extractors or based on better information (*e.g.*, by knowing the user's blockchain queries that did not yet result in submitted transactions). Moreover, those in group (1) may be able to treat user transactions as "private order flow" and either delay rebroadcasting transactions publicly or forgo public rebroadcasting altogether (see below), potentially selling exclusive access to information about those transactions in a kind of "payment for order flow" (PFOF) arrangement.

In traditional finance, PFOF refers to a payment that an "internalizer" makes to a broker in exchange for the broker routing her retail clients' orders to the internalizer, who can then execute trades against those orders.[75] A "DeFi PFOF internalizer" can extract MEV from transactions in a various ways, not only in the context of asset swaps (trades), but also, *e.g.*, in other uses of smart contracts, like NFT mints. Unlike in traditional PFOF, it is relatively rare for an MEV extractor to be a counterparty in a trade from which she is extracting MEV (although this arguably happens in just-in-time liquidity provision),[76] due to the use of automated market makers in DeFi.[77]

[74] *See, e.g.*, Sebastian Bürgel, *DERP Example 3: Uniswap MEV*, (2022), https://medium.com/hoprnet/derp-example-3-uniswap-mev-c2a8d3417c8

[75] Fox, Glosten, & Rauterberg, *supra* note 51 at 289.

[76] In just-in-time liquidity provision, an MEV extractor becomes—for an instant—one of the liquidity providers in the liquidity pool with which the user's transaction swaps assets. As Sarch and I explained: "Just-in-time ("JIT") liquidity provision may be structured as a sandwich where the sandwiched transaction is front-run by a transaction providing more liquidity to a given smart contract market ('liquidity pool'), thus improving the price of execution for the sandwiched transaction, and then back-run by removing the liquidity added earlier and realizing profits. JIT is profitable if the liquidity provider can obtain sufficient trade fees for providing a large proportion of liquidity during the sandwiched trade." *See* @bertcmiller, TWITTER (Nov. 12, 2021, 4:04 PM), https://twitter.com/bertcmiller/status/1459175377591541768. By providing this momentary liquidity, JIT reduces the share of fees collected by 'passive' liquidity providers and thus reduces incentives to engage in 'passive' liquidity provision; *See*, *e.g.*, @ChainsightLabs, TWITTER (Nov. 9, 2021, 7:30 AM), https://twitter.com/ChainsightLabs/status/1457958811243778052."

[77] Another difference from traditional PFOF is that, in "DeFi PFOF," internalizers may be able to enjoy virtually riskless strategies (due to atomicity), instead of relying on a probabilistically grounded expectation of profit when trading against uninformed traders.

Sarch and I discussed the mechanism by which pending Ethereum transactions are propagated and under what circumstances pending transactions can be considered *public*:

> When a user submits a transaction to an Ethereum node, this node is in a privileged position and is dealing with non-public information until the moment that node re-broadcasts the transaction to other nodes in Ethereum's peer-to-peer network. Delaying the rebroadcasting by seconds (or even by fractions of a second) may give the first node a significant advantage. For example, it may allow the node to assess (by performing a simulation) whether the transaction presents a profitable MEV extraction opportunity and – if it does – to submit the node's own transactions aiming to take advantage of the opportunity. All of that could happen before the transaction becomes public in a meaningful sense. Such action may resemble "front-running" as this term is understood outside of the crypto markets. The scenario where only one node possesses non-public information could be further complicated by the theoretical possibility of a cartel of nodes that share information about pending transactions among each other but either (1) do not re-broadcast transactions presenting MEV extraction opportunities to the broader network at all (e.g., using relays instead), or (2) re-broadcast to the broader network only after a sufficient delay. [78]

We proposed defining the *publicness of pending transactions* in the following way:

> … a transaction is public when an actor who did not receive the transaction directly from a user who submitted the transaction, can access it in an unencrypted state without too much delay and without special arrangements with the node that originally received the transaction.[79]

Even if the kind of MEV extraction in question does not, on balance, negatively affect market efficiency (see Section III), cases of privileged access to information about pending transactions or of exclusive control over pending transactions may require additional analysis. Some of the insights developed regarding informed (including "insider") trading and PFOF in traditional finance may be applicable here. For example, it could be the case that service providers would be able to provide a better user experience (lower cost of trading) due to an exclusive opportunity to extract MEV from the user's transactions. This is what services like Rook and OpenMEV promise to Ethereum users.[80] Selling access to information about user transactions or blockchain queries may also provide revenue

[78] Barczentewicz & Sarch, *supra* note 11.

[79] We added: "This standard would be satisfied even if reliably detecting public transactions requires maintaining 'watcher' nodes simultaneously in several geographic zones (*e.g.*, running on virtual servers in various Amazon Web Services regions). Admittedly, transactions 'public' by this standard are only meaningfully public to professional operators, not to an average user." *Id.*

[80] https://docs.rook.fi; https://docs.openmev.org.

for wallet software or front-end developers of smart contracts, thus allowing them to operate without needing other sources of revenue.

Even if such arrangements *may be* beneficial for users, however, there is no guarantee that this will be the case in any individual case. Moreover, it could be that the service provider in question is under a duty to obtain express user consent for such uses of their data (*e.g.*, under privacy laws) and they fail to do so. It could also be that the terms of the contract between the user and the service provider don't allow for using user data for MEV extraction. Finally, even in the absence of explicit contractual terms, in some cases, the nature of the relationship between the user and the service provider may give rise to fiduciary duties, or to duties under consumer-protection legislation, toward the user.

If service providers of any of the groups (1)-(3) do indeed have fiduciary duties toward their users, this would bring them closer to the situation of financial professionals, like investment advisors, brokers, and dealers. Note that a broker's "duty of best execution" originally emerged from the common law of agency, not from legislated financial regulation.[81] The same is true of the related duty not to "front-run" clients' orders.[82] Whether any fiduciary duties apply to our groups (1)-(3) requires further analysis. One reason for skepticism is that it is not obvious whether anyone in (1)-(3) acts to bind the principal (the user) with obligations created with third parties.

It is not only *end users* who may potentially be harmed in analogous ways by various service providers. Currently, block builders submit their draft blocks to relays, which can use the information provided by a block builder without rewarding them (*e.g.*, to copy a complex arbitrage transaction and include it in a block built and forwarded to proposers by the relay operator). Reputational mechanisms are important in alleviating such risks, but their existence may not be sufficient to exclude the possibility of liability for a relay operator, stemming from breaches of duties grounded in the direct service relationship between a block builder and the relay.

C. Market Manipulation

Whether anti-market-manipulation rules apply to any MEV-extraction strategies should depend on whether those strategies harm market efficiency. Because we don't know the net effect of any MEV-extraction strategy on the market, enforcement of anti-market-manipulation rules should be based on robust and comprehensive empirical research. I adopt this view, following scholars like Fletcher,[83] because the alternative could easily lead to prosecution of market activities with greater positive

[81] *See, e.g.,* Fox, Glosten, & Rauterberg, *supra* note 51 at 266.

[82] *Id.* at 97, 313.

[83] Fletcher, *supra* note 49.

externalities than negative effects. It is important, however, to note that some jurisdictions may take a different approach in practice.[84]

U.S. anti-market-manipulation rules—like CFTC Rules 180.1 and 180.2, which Sarch and I discuss in the MEV context[85]—employ general phrases like "manipulative device, scheme, or artifice to defraud." The same is true in the EU, where the Market Abuse Regulation prohibits, *e.g.*, the use of "a fictitious device or any other form of deception or contrivance," as well as giving "false or misleading signals as to the supply" or demand.[86]

Given such vague terminology, it may be tempting for law enforcement or regulators to act relying on superficial descriptions like "toxic MEV" or on some unfortunate word choices in the MEV-extraction ecosystem, like "bribes" that searchers offer to block producers. Doing so would likely apply what Sarch and I call "a *moralized* conception of market fairness," built on experiences from traditional finance, which may seem analogous but may not be.[87] Sarch and I note that a case that may *seem* particularly problematic is sandwiching with the use of bundles (by sending a bundle, *e.g.*, to a block builder):

> … in this scenario, the sandwicher, in a sense, "appropriates" another's trade. They do so by copying the publicly available data of a pending transaction and bundling it with their own front- and back-running transactions. The sandwicher pays a "bribe" for their bundle to be included with all three (or more) transactions precisely in the order set by the sandwicher. This could be seen as an express instruction to order transactions in a way that adversely affects another trader.[88]

Given that we don't know the net effect of any MEV extraction on the market (see Section III), such enforcement actions would likely either disregard the issue of effect, or rely on an incomplete picture of effect (likely just the effect on the transaction directly affected by MEV extraction).

Government agencies like the U.S. Securities and Exchange Commission also sometimes rely primarily on a defendant's alleged intent to manipulate markets. Fletcher criticized this intent-centric approach as under- and over-inclusive, and as ignoring the key question of harm to the market.[89] But I believe there is an even more fundamental problem with relying on intent to manipulate in

[84] *See supra* notes 51-54 and the accompanying text.

[85] Barczentewicz & Sarch, *supra* note 11.

[86] The EU Market Abuse Regulation (MAR) applies to "financial instruments," and it remains a largely open question whether crypto-assets qualify as such. The planned Markets in Crypto-Assets Regulation (MiCA) copies some of MAR's key anti-manipulation provisions, however, and makes them applicable to nearly all economically significant crypto-assets.

[87] Barczentewicz & Sarch, *supra* note 11 at 16.

[88] *Id.* at 10.

[89] Fletcher, *supra* note 49 at 515–518.

the case of MEV extraction. The problem is that we don't know whether any MEV-extraction strategies *do manipulate the market*. It hasn't yet been established what constitutes "normal" behavior on a decentralized crypto market. Arguably, such determination should consider all positive and negative external effects on the underlying blockchain network of various trading strategies and mechanisms. Relying on intent to do some bad thing is only meaningful if we are certain that the thing is indeed bad. Consider the following analogy: it would be difficult to justify criminalizing intending to form a cartel if there were no reliable evidence that cartels are, on balance, harmful to social welfare.

A similar concern arises with respect to the "manipulation-as-fraud" theory that Sarch and I discussed.[90] Under this theory, "when a person engages in manipulative trading practices in the markets and does not let others know of his manipulative acts, the fraud derives from the failure to inform the other market participants, who are entitled to rely on their belief that the market is free of such improper behavior."[91] If it cannot be shown that the practices in questions are manipulative, then a "failure to inform" should not matter.

Relying on a failure to inform may face another hurdle, as Sarch and I noted. The MEV-extraction phenomenon appears to be well-known among DeFi users. It is at least arguable that most, if not virtually all, traders who are negatively affected by strategies like sandwiching are aware of the risk. Whether this impression is correct, however, may require further study.

I do not mean to suggest that no MEV extraction involves market manipulation. In fact, it is very likely that some or even virtually all cases of oracle manipulation or of the so-far theoretical time-bandit attacks would constitute illegal market manipulation. The already-mentioned CFTC action against Avi Eisenberg in connection with the Mango Markets oracle manipulation presents a strong case for liability. Eisenberg was involved in an "undercollateralized loan attack," meaning that he manipulated the benchmark prices of collateral that he used to take out a loan, which he did not intend to repay.[92] Several features of Eisenberg's strategy—like the fact that it included a wash trade and that he took out a loan that he did not intend to repay—distinguish it from other market strategies discussed here, where the argument that they involve open-market trading in good faith is much stronger.

Difficult questions about whom, exactly, could be held liable may arise and policy considerations about the negative externalities of some enforcement actions—*e.g.*, against validators who did not instigate but may have indirectly profited from a given manipulation—should be properly weighed

[90] Barczentewicz & Sarch, *supra* note 11 at 14–19.

[91] Gregory Scopino, *The (Questionable) Legality of High-Speed 'Pinging' and 'Front Running' in the Futures Markets*, 47 CONN. L. REV. 607, 673 (2015).

[92] Mackinga, Nadahalli, & Wattenhofer, *supra* note 35 at 2.

(see Section V). It is advisable to prioritize prosecutions with evidence of both market harm and intent to manipulate, as appears to be the case in the CFTC's enforcement action in the Eisenberg/Mango Markets case.

Despite the concerns discussed above, it is likely that MEV extraction will soon attract regulatory attention, focused not only on clear simple fraud, but also on market manipulation. Hopefully, this will be accompanied by robust research, answering the question of net social (market) effect in a way that is appropriate to decentralized blockchain networks (*i.e.*, considering issues like blockchain security). There is also a risk, however, that no such research will be undertaken, and officials will be inclined to approach the perceived problems by relying solely on analogies with traditional finance. Some forms of enforcement or other regulatory interventions may have relatively little effect on the broader Ethereum ecosystem, but some may have significant negative externalities (see Section V).

V. Conclusion: Is There a Need for State Action?

One of the key conclusions from the preceding discussion is that we don't currently know the net social-welfare effect of any kind of MEV extraction, even if we limit the social-welfare analysis to market efficiency. This is a strong reason for government officials to exercise caution before attempting to address perceived problems with MEV extraction, either through legislation or enforcement of existing rules. Naturally, this only applies to concerns based on harm to market efficiency, as is arguably the case with, *e.g.*, anti-market-manipulation rules. It does not apply in case of fraud or other legal liability not defined by reference to harm to market efficiency.

A. Cost of Government Intervention

Even if some MEV extraction is both harmful to individual market participants and reduces social welfare, it may still be the case that some legal and regulatory responses could be misplaced. A legal response could, for instance, reduce social welfare even more than the harm that it is meant to remedy. Legal and regulatory failures are arguably common, although it is usually hard to find consensus as to what things count as such (*e.g.*, modern airport security).

Therefore, it is important to perform rigorous cost-benefit analysis of regulatory interventions, especially where they are meant to be applied in new technological and organizational contexts like decentralized crypto markets. For example, dealer-broker licensing may be a sensible measure in its current context (in "traditional" finance), but similar licensing—*e.g.*, for block builders or relay operators—could be problematic. At the risk of sounding hyperbolic, a country that adopts such measures could be giving up on the benefits of decentralized and permissionless public blockchains like Ethereum. To the extent that that risk exists, the benefits of intervention should be measured against the social benefits that would be lost.

Not every state intervention is likely to have such serious systemic effects. For example, prosecution of some individual MEV extractors may push such activity to other jurisdictions and thus give a competitive advantage to those not located in the prosecuting jurisdiction. But if only independent MEV searchers are prosecuted, not base-layer operators like validators, then it might be that the risk of reducing geographic decentralization of the Ethereum network will not be overly significant.

Moreover, depending on what kinds of MEV extraction is deemed illegal, it may be possible for Ethereum to prioritize protocol development in directions that would reduce opportunities for such behavior. If no one can extract value this way, then there would be no benefit to fleeing to jurisdictions where it is legal. This point is worth stressing. Regulation and regulatory enforcement in the realm of public blockchains faces the problem of regulatory arbitrage: operators being able to choose the most favorable jurisdictions, while retaining influence on markets in other jurisdictions. This provides a strong argument for preferring and supporting technical solutions (*e.g.*, on the level of the Ethereum protocol), which would apply globally, over national or even international legal rules, which would face the problem of regulatory arbitrage.

B. Technical Solutions Are Likely Preferrable, but May Require Tradeoffs

It is impossible to technically disable willing validators entirely from extracting at least some kinds of MEV (or, in other words, to remove all MEV). Where feasible, however, technical solutions to undesirable kinds of MEV extraction may be preferable over legal intervention. Hence, it is worth advocating for such technical work to be undertaken. For example, introducing more on-chain privacy on Ethereum could significantly reduce, if not solve, what Sun defines as "Mafia EV"—*i.e.*, MEV that is possible because of the lack of privacy. This could be done by some form of "encrypted mempool," ensuring that pending Ethereum transactions are not visible to MEV extractors.[93]

Importantly, it is also worth advocating for the law not to disincentivize technical development. The latter point is important because, for example, introducing an encrypted mempool would turn Ethereum into more of a "privacy-coin." This would come with significant social benefits, but also with the risk of a conflict with some approaches to enforcing anti-money-laundering (AML) rules or economic-sanctions regimes.

[93] Currently, it is possible to use *privacy RPCs* (like Flashbots Protect), but this requires users to trust the service providers involved, because transactions are not encrypted.

As I argued in a submission to the U.S. Treasury Department, AML and sanctions compliance is likely to be more effective and more proportionate if undertaken not on the level of blockchain infrastructure (the base layer), but on the application layer, *i.e.*, services that interact primarily with end users, especially on- and off-ramp services (services that intermediate between crypto assets and the rest of the financial system).[94] User privacy can be preserved in a blockchain network when AML and sanctions compliance is facilitated by tools like selective disclosure at the point where users exchange crypto-assets or non-crypto-assets (like fiat currencies).[95]

[94] Mikolaj Barczentewicz, *Comments of the International Center for Law & Economics, Ensuring Responsible Development of Digital Assets*, Docket No. TREAS-DO-2022-0018 (Nov. 3, 2022) https://www.regulations.gov/comment/TREAS-DO-2022-0018-0039.

[95] *Id.* at 4-5.