*Ohio State Technology Law Journal*
Vol. 20 (forthcoming 2023)

# BLOCKCHAIN TRANSACTION ORDERING AS MARKET MANIPULATION

Mikołaj Barczentewicz,† Alex Sarch†† and Natasha Vasan†††

***Abstract**: On public, permissionless blockchains like Ethereum, space is scarce and crypto traders must compete to use it for executing their transactions. That means those who control this space in the form of blocks resemble landlords who can extract rent. "Maximal Extractable Value" (MEV) refers to trading strategies that exploit the ability to decide what transactions go into a block. Those who control the contents of a block (validators) can obtain rents not only for including transactions in a block, but also for ordering them in profitable ways—say, by letting transactions "front-run" others. Since rising to prominence in 2019, MEV has quickly become a major market phenomenon, generating $600 million in profit between 2020 and 2022 alone, while affecting tens of billions of dollars in transaction value.*

*MEV is often condemned. Techniques like "sandwich attacks" which involve trading ahead of other users' trades, have been described as toxic, fraudulent, manipulative – even theft. However, this broad denunciation of MEV is too quick, as the technical nuances of how each kind of MEV extraction operates are determinative of the legal risk it entails. The legality of MEV extraction under U.S. financial laws has yet to be subject to sustained scholarly analysis, and the present Article aims to fill this gap. We undertake the first systematic analysis of how U.S. securities and commodities law, particularly the broad anti-manipulation rules wielded by the SEC (Rule 10b-5) and CFTC (Rule 180.1), apply to core MEV extraction techniques on Ethereum.*

---

† Senior Lecturer (Associate Professor), University of Surrey School of Law, Research Associate of the University of Oxford Centre for Technology and Global Affairs, Fellow of the Stanford Law School and University of Vienna Transatlantic Technology Law Forum, and Senior Scholar at the International Center for Law & Economics.

†† Professor and Director of Research, University of Surrey School of Law, Fellow of the Surrey Institute for People-Centred AI.

††† University of Michigan Law School.

All authors contributed equally to this Article and names are listed in alphabetical order. For their valuable comments and discussion, the authors wish to thank Shahab Asghar, Salman Banaei, Claudia Biancotti, breeze, Phil Daian, Michele Fabi, Arthur Gervais, Vikramaditya Khanna, Guha Krishnamurthi, TuongVy Le, Barnabé Monnot, Nicolás Della Penna, Alex Obadia, Puja Ohlhaver, Pmcgoohan, Jake Senftinger, Martin Schmidt, Stalkopat, Martin Schmidt, Gregory Scopino, Gregory Shill, Thogard, Anton Wahrstätter, and Evan Zinaman.

*In so doing, the Article confronts how basic notions of fairness and trust play out differently in a world of discretionary transaction ordering in crypto markets compared to the first-come first-serve world of traditional finance. Behaviors that might seem outrageous off-chain look very different when examined in light of how blockchains actually work.*

*Nonetheless, this Article argues that some forms of MEV extraction entail a significant risk of market manipulation liability. Focusing on sandwiching in particular, we provide novel arguments showing that there is a route for courts that adopt a moralized lens, focused on behavior that exploits privileged control over financial infrastructure, to find sandwiching impermissibly manipulative. We argue, further, that the legal hazards are even greater when it comes to sandwiching* private *transactions, which more clearly involves a heightened trust relationship, as well as disruptive schemes like oracle manipulation, wherein MEV is part of an independently manipulative strategy. Nonetheless, we argue, this alone does not mean a sweeping ban on these forms of MEV is necessarily a desirable policy. It remains unclear whether a strict ban on MEV sandwiching, for instance, would be prudent, given the unknowns about the net effects of MEV extraction and behavioral impact that a ban on MEV sandwiching would entail.*

## I. INTRODUCTION

Applying the assumptions of traditional finance to the radically different infrastructure of crypto markets is risky business. On February 16, 2022, an Ethereum user we will call 0x61 (based on her address) appears to have noticed a profit opportunity. Since the beginning of February, the price of ETH[1] (the native token of the Ethereum blockchain) had recovered somewhat from a prior drop, and 0x61 likely decided that the recovery wouldn't last much longer. 0x61 used the decentralized exchange Uniswap V2 to sell 79 ETH, then worth around $250,000, in exchange for DAI (roughly put, 1 DAI corresponds to 1 dollar), and logged off perhaps feeling content about the day's work.[2] Little did 0x61

[1] Strictly speaking, this was Wrapped Ethereum (WETH). *See, e.g.*, Ivan Cryptoslav, *What Is Wrapped Ethereum (WETH)?*, COINMARKETCAP.COM ALEXANDRIA (2022), https://coinmarketcap.com/alexandria/article/what-is-wrapped-ethereum-weth [https://perma.cc/BK23-W2NC].

[2] 0x61's transaction can be viewed on Etherscan, the Ethereum blockchain explorer: https://etherscan.io/tx/0x9760b7dedcbfbc37e6feb491a9bdf33c98c99d8d339fde49f2c3e97828cd4b6b. The transaction can also be analyzed on ZeroMEV: https://www.zeromev.org/block?txh=0x9760b7dedcbfbc37e6feb491a9bdf33c98c99d8d339fde49f2c3e97828cd4b6b.

know that others were watching in the "dark forest"[3] of Ethereum's public "mempool,"[4] where submitted transactions sit waiting to be executed by being built into blocks and recorded on the blockchain. It is only once the submitted transaction is executed in this way that 0x61's effort to capitalize on the profit opportunity she saw would be complete.

However, things did not turn out exactly as 0x61 may have expected. A few minutes after pressing the button on her transaction, it became clear that someone else had interfered in her plans. The transaction she likely had thought would provide her about $225,000 (adjusted for $25,000 in transaction fees) in DAI, ended up garnering just $179,000.[5]

*Where* did the extra $46,000 that 0x61 expected go?[6] It had been captured by what has become known in the crypto community as a *MEV extractor*.[7] "MEV" stands for Maximal Extractable Value[8] and paradigmatically involves the direct or indirect exploitation of the ability to control the order in which transactions are executed, a power which is possessed by those who construct the blockchain on which crypto assets are traded.[9] Despite its very recent formalization in 2019,[10] MEV extraction has quickly become a major market phenomenon, with a conservative estimate at roughly $600 million in profit between 2020 and 2022 alone, while affecting tens of billions of dollars in transaction value.[11]

More specifically, what happened to 0x61 was a *sandwich*,[12] the classic example of MEV extraction. Upon spying her transaction pending in the

---

[3] Dan Robinson & Georgios Konstantopoulos, *Ethereum is a Dark Forest*, PARADIGM.XYZ (2020), https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest.

[4] *See infra* Section II.A.

[5] *See supra* note 2.

[6] Had 0x61 not been front-run by the bot's trade, they would have ended with $46,083-worth more of DAI. For the source of that calculation see the Ethereum block 14217123 in the Zeromev explorer: https://www.zeromev.org/block?num=14217123.

[7] *Maximal Extractable Value*, https://ethereum.org/en/developers/docs/mev/ (last accessed, 31 Jan., 2023).

[8] *Id*.

[9] Philip Daian et al., *Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges*, (2019), https://arxiv.org/abs/1904.05234.

[10] *Id.*

[11] *See* Raphael Auer et al., *Miners as intermediaries: extractable value and market manipulation in crypto and DeFi*, BIS BULLETIN (2022), https://www.bis.org/publ/bisbull58.pdf; EIGENPHI RESEARCH, *Flash Boy's Gain, Everybody's Pain: 2022 Mid-Year Report of Sandwich MEV on Ethereum*, (2022), https://eigenphi.substack.com/p/flash-boys-gain-everybodys-pain..

[12] Sandwiches have been widely discussed. *See, e.g.*, Lioba Heimbach & Roger Wattenhofer, *Eliminating Sandwich Attacks with the Help of Game Theory*, *in* PROCEEDINGS OF THE 2022 ACM ON ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 153 (2022), https://doi.org/10.1145/3488932.3517390; Kshitij Kulkarni, Theo Diamandis & Tarun Chitra, *Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers*, (2022), https://arxiv.org/abs/2207.11835; Julien Piet, Jaiden Fairoze & Nicholas Weaver, *Extracting Godl*

mempool, an automated "searcher bot" (our metaphorical "lurker" in this case) sniffed out the potential profits exploitable from 0x61's trade. That is, the bot employed its algorithm to simulate the transaction's execution, finding that it would produce an increase in the price of DAI relative to that of ETH on the decentralized exchange. The searcher bot then knew precisely what to do: get there first. While 0x61's trade was still pending, waiting in the mempool to be executed by being included in a block, the searcher swooped in and was able to influence a block builder to execute the bot's own trade first, which swapped 850 ETH for 2.27 million DAI before 0x61's trade went through.[13] As a result, the price of DAI against ETH increased, and so 0x61 failed to realize as much value from her trade as anticipated. This loss, however, became the searcher's gain. It purchased the DAI low, and then when its trade plus 0x61's trade moved the price of DAI against ETH upwards, it sold high. Specifically, it used its new 2.27 million DAI to purchase 868 Ethereum, netting a profit of 18 ETH (worth over $56,000).[14]

On a natural way of thinking, this might seem *outrageous*. Someone in 0x61's position – whose trade ended up being tens of thousands of dollars less profitable than expected due to someone who effectively "cut in front" of her to trade first – might be forgiven for alleging that the searcher *stole* some of the profits she reasonably believed were coming her way.

But appearances can be deceiving. Careful analysis is needed before jumping to the conclusion that sandwich attacks, or other forms of MEV, are unfair, manipulative or fraudulent – as is sometimes claimed.[15] This, we will argue, is because the intuitions and expectations derived from traditional finance, which naturally fuel the criticisms of MEV as "toxic," unfair or manipulative, do not automatically carry over to crypto trading, which operates in fundamentally different ways than traditional finance. This Article seeks to explain why. It is the first to systematically analyze the legality and broader normative defensibility of the main questionable MEV extraction techniques employed on public, permissionless blockchains like Ethereum today.

---

*[sic] from the Salt Mines: Ethereum Miners Extracting Value*, (2022), https://arxiv.org/abs/2203.15930.

[13] *See supra* note 2.

[14] For the purpose of clarity, we assume here that the searcher bot was operated by a validator-proposer, meaning that it would net all 18 ETH as its own profit. Yet, as we will soon discuss, in Section II.C., if the searcher were *not* operated by a proposer, it would have to give some of those profits up to validators in exchange for the ability to have its own transactions ordered directly before and directly after that of 0x61.

[15] Ari Juels, Ittay Eyal & Mahimna Kelkar, *Miners, Front-Running-as-a-Service Is Theft*, COINDESK (2021), https://www.coindesk.com/markets/2021/04/07/miners-front-running-as-a-service-is-theft/; IOSCO, *IOSCO Decentralized Finance Report. Report of the Board of IOSCO*, 37 (2022), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf; U.S. TREASURY DEPARTMENT, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, 36 (2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf; Auer et al., *supra* note 11.;

What might seem outrageous based on the first-in-time (first-come first-serve) method of transaction execution that pervades traditional finance is far more complicated when analyzed within the context of the "timeless" method of transaction ordering on Ethereum,[16] which obeys a logic all its own. On blockchains like Ethereum, transactions are ordered in a manner distinct from that familiar to legacy finance. Most fiat-based electronic trading takes place on continuous limit order books, which process transactions in the order of the time when they were submitted. However, transaction processing systems, like continuous limit order books, which operate on a first-in, first-out model, inherently privilege traders located physically *closer* to the ultimate location of transaction execution. This is because those traders have the lowest *latency* – they receive and can transmit transaction information faster than other market participants.

By contrast, public blockchains are meant to operate globally in a decentralized fashion that does not privilege particular locations. As such, time-based transaction processing has been eschewed for blockchain systems like Ethereum, which have sought a different approach to transaction ordering, in which constructors of blocks on the blockchain (known as validators) can determine transaction order in a variety of ways.[17] Accordingly, there is *no natural ordering* of transactions within this space, no first-in-time queue that operates by default to determine who trades first. This means that claims that MEV extractors jump the queue to "steal" some of the profits of the affected trades are much too simple and not obviously defensible – even if they also are psychologically understandable for traders like 0x61. To get to the bottom of these issues, this Article explores the complex machinery through which trading operates on Ethereum and we unpack how its fundamental differences with traditional finance impact the legality under existing US financial law of the main MEV techniques.

Despite the rapidly growing importance of MEV, there has so far been no in-depth analysis of the legality specifically of MEV extraction in the legal literature.[18] This is the gap our Article aims to fill. We undertake the first systematic analysis of how US securities and commodities law, particularly the

---

[16] We focus our analysis in this Article on Ethereum, as this is where MEV extraction is most prevalent and most discussed. With this said, much of our analysis is likely to apply to other public, smart contract-enabling blockchains (*e.g.,* Solana).

[17] *See infra* Section II.

[18] There have been valuable analyses of how securities law applies to fraud and other forms of abuse in crypto markets in general, although they do not discuss MEV techniques like sandwiching or oracle manipulation, which we confront in depth. *See, e.g.,* Menesh Patel, *Fraud on the Crypto Market*, FORTHCOMING IN HARVARD J. L. & TECH. (2023). Moreover, there have also been quick comments on the legality of MEV, though these only scratch the surface and do not systematically examine the depth of technical and legal nuance that these issues present; *see, e.g.,* Auer et al., *supra* note 11; Mikołaj Barczentewicz, *MEV on Ethereum: A Policy Analysis*, INTERNATIONAL CENTER FOR LAW & ECONOMICS WHITE PAPER 2023-01-23 (2023), https://ssrn.com/abstract=4332703.

broad anti-manipulation rules that figure centrally in the regulatory arsenals of the Securities Exchange Commission and Commodities Futures Trading Commission (*i.e*. SEC Rule 10b-5 and CFTC Rule 180.1), apply to core MEV extraction techniques on Ethereum. The topic is especially ripe for exploration because MEV extraction raises numerous legal and policy questions of first impression, which courts, regulators and lawmakers will need to address.[19] Our Article contributes insights about the novel phenomenon of MEV to the growing body of scholarship about the regulation of decentralized finance (DeFi) in general[20] and contributes to lively literature on how the law of market manipulation is evolving to keep pace with rapidly changing trading practices.[21]

In assessing what sorts of liability under existing US financial law are risked by MEV extractors, a cluster of important but unsettled questions arise about the importance of the special forms of control over key financial infrastructure that MEV extractors exploit – especially the essential function of transaction processing through block building. Transactions on Ethereum are not ordered via a first-in-time principle but the matter sits within the control of block producers (especially: validators), as rational and self-interested agents. It is thus predictable that they will *extract rents* from those who need to use their block-production-controlling services to execute their trades – much like rents charged for one's control of a piece of limited physical space. In the highly competitive environment of crypto markets, we can expect that advantages will tend to be exploited – including by those who control the system infrastructure itself. This suggest that MEV may be understood as the extraction of rents by those who control "blockspace," extracted from traders who require access to that space to be able to trade.

This peculiar set-up, we will argue, carries its own distinctive legal and ethical hazards, which impact not only the legal risks that MEV extractors face under US financial law but also the policy responses that legislators may wish to pursue in response to MEV extraction. As we will see, users *trust* blockchain validators to verify and process transactions added to the blockchain and, in order to accomplish this task, validators possess the privileged role (from which

[19] For example, MEV is mentioned in the crypto-regulation bill introduced by Senator Elizabeth Warren: *Digital Assets Anti-Money Laundering Act of 2022*, S.5267, 117th Cong. §3(a) (2022).

[20] *See, e.g.,* Kristin N Johnson, *Decentralized finance: Regulating cryptocurrency exchanges*, 62 WM. & MARY L. REV. 1911 (2021); Chris Brummer, *Disclosure, Dapps and DeFi*, 5.2 STAN. J. OF BLOCKCHAIN L. & POL'Y 137 (2022); Dirk A Zetzsche, Douglas W Arner & Ross P Buckley, *Decentralized finance*, 6 J. OF FIN. REG. 172 (2020); Proceedings of the 2021 Spring Conference: The Impact of Blockchain on the Practice of Law, 17 NYU J. OF L. & BUS. 681 (2021).

[21] Gina-Gail S Fletcher, *Legitimate yet manipulative: The conundrum of open-market manipulation*, 68 DUKE L. J. 479 (2018); Tom CW Lin, *The new market manipulation*, 66 EMORY L. J. 1253 (2017); Jakob Arnoldi, *Computer algorithms, market manipulation and the institutionalization of high frequency trading*, 33 THEORY CULT. SOC. 29 (2016); MERRITT B FOX, LAWRENCE GLOSTEN & GABRIEL RAUTERBERG, THE NEW STOCK MARKET: LAW, ECONOMICS, AND POLICY (2019).

they can extract rents) of ordering and including transactions.[22] Thus, the central question we confront in this Article is whether the sort of rent extraction MEV arguably involves, flowing from privileged control over or access to key financial infrastructure in which users place their trust, might make it count as a form of manipulation.

We argue in Section IV that there are narrow contexts in which MEV extractors plausibly can be seen as occupying a position of heightened trust and thus we contend that existing anti-manipulation law would be violated by some forms of MEV. But especially because of the differences from traditional finance, we also find that much MEV extraction – especially when carried out through open market trades at arms' length – fit within familiar economic rationales that the courts widely accept as legitimate within legacy finance. Furthermore, we argue in Section V, at a policy level, that because of the open empirical questions about whether MEV behavior has a net positive impact on the efficiency of crypto markets (*e.g.*, through properly incentivizing essential financial functions on which all crypto market participants rely), regulators and lawmakers should be very careful about introducing blanket MEV prohibitions. We argue that prohibitions are likely to be defensible, if at all, only in narrowly circumscribed cases such as those involving i) express representations that are false or misleading,[23] ii) a special relationship of trust between MEV extractors and particular traders (such as when private order flow is involved),[24] or iii) harmful kinds of benchmark manipulation (known as "oracle manipulation,"[25] and which DOJ, CFTC, and SEC are already prosecuting[26]).[27]

MEV extraction thus forces us to re-examine the normative assumptions and principles underlying market manipulation law in order to determine

---

[22] For instance, blockchain users rely on validators to maintain the integrity of the network by ensuring that "double spending" does not occur. *See, e.g.,* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (2008), https://bitcoin.org/bitcoin.pdf.

[23] *See generally infra* Section IV.

[24] *See infra* Section IV.B.

[25] *See infra* Section IV.C; an "oracle" is essentially a communication channel which provides external data to closed blockchain systems. While this data can come from on-chain or off-chain sources, price oracles in decentralized finance– the focus of our discussion here – are a specific kind of oracle which pull data exclusively from on-chain sources to determine prices for DeFi protocols. For more information regarding oracles s*ee* Cryptopedia, Blockchain Oracles Explained: Decentralized Oracles in DeFi (Feb. 4, 2022), https://www.gemini.com/cryptopedia/crypto-oracle-blockchain-overview#section-inbound-versus-outbound-oracles (discussing oracles which bring off-chain data to blockchain systems).

[26] 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; Press release, *SEC Charges Avraham Eisenberg with Manipulating Mango Markets' "Governance Token" to Steal $116 Million of Crypto Assets*, SECURITIES AND EXCHANGE COMMISSION (Jan. 20, 2023), https://www.sec.gov/news/press-release/2023-13.

[27] *See infra* Section IV.C.

whether the effects of MEV extraction are legitimate and compatible with market integrity or whether they fall afoul of basic notions of fairness and well-ordered markets. In our analysis, the key ends up being to determine the extent to which various types of MEV extractors, involved in different types of trading strategies and techniques, can be said to occupy positions of trust that carry special responsibilities to avoid interfering with the reasonable expectations of other market participants.[28] A core contribution of this Article thus is to frame the central legal and normative questions to be answered – whether by courts, regulator or legislators – and we argue for an approach to this question that takes a holistic look at the costs and benefits of MEV extraction and allocates legal duties on that basis.[29]

The remainder of this Article will proceed as follows. Section II introduces the technical background necessary for a legal understanding of MEV. We explain the process of transaction validation on Ethereum and show how it allows MEV extraction. We describe the most common forms of MEV extraction, including sandwiching, arbitrage, and liquidations. Section III introduces relevant aspects of US law governing market manipulation in securities and commodities markets. Beyond sketching the statutory and regulatory backdrop of anti-manipulation law, we discuss the law's treatment of particularly salient categories of manipulative trading like open market manipulation, insider trading, and front-running.

In Section IV, we apply the law of market manipulation to core cases of MEV extraction. We begin with MEV sandwich trades targeting public transactions, addressing the main arguments for and against market manipulation liability for this practice. We provide novel arguments showing that a court drawing on moralized conceptions of market fairness may have a route to concluding that the sandwiching of public transactions is manipulative in violation of CFTC Rule 180.1 or SEC Rule 10b-5 on the grounds that a sandwicher at least recklessly creates an artificial price effect by unfairly exploiting their position of privilege and control over essential financial infrastructure. That said, we note that the practical hurdles for succeeding with this cause of action make it unlikely to be pursued as a high regulatory priority in the near term. Turning then to sandwiching of *private* transactions, we find that a broader scope for market manipulation liability exists here as actors trusted to act in confidence are more likely to end up behaving in misleading ways when handling private transaction information. Finally, we examine trading strategies that involve MEV only incidentally or as a means to further increase the profitability of other schemes, including harmful oracle manipulation. As we will argue, a number of these techniques are likely to attract market manipulation liability.

Section V then moves from analyzing liability for MEV under existing law to considering the policy question of how to respond to such practices. We

[28] *See infra* Section IV.
[29] *See infra* Sections V and VI.

caution that it remains far from clear that a flat ban on questionable forms of MEV sandwiching would be good policy. There are at present too many unknowns about the net impact on market efficiency and social welfare of MEV sandwiching, as well as the behavioral effects that a sweeping sandwiching prohibition would have, to be confident that this is a desirable way forward at present. More empirical research on the issue is imperative. We conclude in Section VI by offering four recommendations to policymakers, courts, researchers, and the Ethereum community. In these ways, we hope to shed light on the dark art of MEV extraction on Ethereum.

## II. WHAT IS MEV EXTRACTION? TECHNICAL AND ECONOMIC BACKGROUND

Referenced by many as a "dark forest,"[30] Ethereum's mempool[31] is home to lurking monsters, attacking other forest dwellers and particularly visitors not well-versed with the ways of the forest. These metaphorical "monsters" are strategic network participants on Ethereum who monitor pending transactions to find and extract value from profitable MEV opportunities—instances where the inclusion, ordering, or censoring of pending transactions turns them a profit. As we shall see, these actors "attack" ordinary, likely unsuspecting network users because, in many cases, their profit is correlated with another user's financial loss.[32]

Blockchain networks like Ethereum rely on validators (or miners) to verify and process user transactions, and these validators are privileged with a temporary monopoly power over a block, to discretionarily include, order, and censor transactions.[33] Network users place differing degrees of value on the certainty, speed, and placement of their transactions, meaning that validators can charge rents for the exercise of their power to control transaction ordering in a manner that aligns with a party's execution preferences. The maximal possible revenue that a validator can earn through their ability to control the contents and sequencing of Ethereum blocks – either independently or by collecting rents from searchers – is known as "Maximal Extractable Value" or MEV.[34] It is worth noting that MEV refers to *extractable* value, and not all MEV gets

[30] Robinson and Konstantopoulos, *supra* note 3.

[31] *See infra* Section II.A.

[32] Daian et al., *supra* note 9; Liyi Zhou et al., *Sok: Decentralized finance (defi) attacks*, CRYPTOLOGY EPRINT ARCHIVE (2022); Piet, Fairoze, and Weaver, *supra* note 12.

[33] A "block" is an ordered batch of transactions which is added to a blockchain. Ethereum Organization, *Blocks* https://ethereum.org/en/developers/docs/blocks/ (accessed 1 Feb 2023). Ethereum, like all blockchains, is essentially a chain of such blocks which are created and validated by the nodes of the Ethereum blockchain. *Id*.

[34] *See supra* notes 7-9.

extracted in reality – we refer to the portion of MEV which is in fact extracted as *extracted* MEV.

In this section, we will describe the technical and economic mechanics of MEV extraction on Ethereum and provide a taxonomy of MEV extraction practices, making distinctions along legally relevant lines.

### *A. The Journey of an Ethereum Transaction*

MEV only arises because Ethereum users have things they want to do on the blockchain (transfer or exchange various crypto assets, "mint NFTs,"[35] and so on) and because the space in which those things can be done, "the blockspace," is scarce. Users express their preferences as to what they want to do on the blockchain using "transactions." What makes things slightly complicated is that Ethereum is not simply a single program, running on a single computer, but a distributed, even global, network, with many participants performing various roles – a network meant to perform its functions in the conditions of limited trust among the participants, or even impossibility of legal recourse if something goes awry. This is, of course, what distinguishes public, permissionless blockchains from other forms of human interaction through technology. It requires a bit of patience to understand how it is that users get to do the things they want to do but is essential for the legal analysis to come.

#### 1. From wallet software to "the mempool"

To express their preference with a transaction, a user first needs to construct this transaction, which would be rather tedious to do with a pen and paper, hence users typically use "wallet software." Wallet software allows users both to query what is happening on the blockchain ("the blockchain state") and to prepare their own interactions with the network, *e.g.,* by assembling a transaction in which the user will transfer 1 ETH from their account to someone else's account.[36] Once the user authorizes and directs their wallet software to submit the transaction, the transaction begins its journey into the dark forest. Later in this section, we will introduce an important complication about what exactly may happen with the transaction at this stage. But for now, let's assume that it follows the "standard," "public" way.

---

[35] Amber Group, *Extractable Value*, AMBER GROUP (2022), https://medium.com/amber-group/extractable-value-7b0d4356a843.

[36] Our description omits a large amount of technical detail not immediately required to understand the mechanisms of MEV extraction. For more technical detail *see, e.g.,* Daian et al., *supra* note 9; Zhou et al., *supra* note 32.

The user's transaction is thus received by an "RPC operator,"[37] who – in our standard picture – is a full "node" of the Ethereum peer-to-peer network. Note, that we are still quite far from the *blockchain*. The dark forest is the peer-to-peer network where transactions travel until they reach their final destination: the validator who will "propose" a block including this transaction, hopefully resulting in the addition of this transaction to the blockchain. Network nodes keep all pending transactions they receive, either directly from users, or from other nodes (this is how transactions propagate in the network: through "gossiping"[38]) in their local "mempools."[39] It is common to speak of "the mempool," though this is just an abstraction referring to transactions that are in the mempools of some significant number of nodes in the peer-to-peer network.

What is key for us to know about "the mempool" is that transactions that travel in the peer-to-peer network can be seen, in principle, by anyone.[40] Setting aside the issue of cost, anyone can either operate a node (preferably multiple, just to be sure they get as many transactions and as early as possible), or to pay one of the service providers who give access to data feeds with information on pending transactions.

2. Block production

Transactions only manage to become effective on the blockchain if they make their way there. Once a transaction becomes a mempool transaction (is in "the mempool"), then it can be spotted by a block producer. Since Ethereum's transition from "proof-of-work" to "proof-of-stake" in September 2022,[41] there are two kinds of block producers looking for transactions: validators-proposers and specialist block builders.

The most straightforward case is that of a validator-proposer. Each Ethereum "epoch" (lasting just over six minutes), a new set of proposers is randomly selected from among validators (around 500,000).[42] Epochs are

---

[37] "RPC" stands for "remote procedure call." *See, e.g., JSON-RPC API*, Ethereum.org, https://ethereum.org/en/developers/docs/apis/json-rpc/.

[38] *See, e.g.,* Lucianna Kiffer et al., *Under the hood of the ethereum gossip protocol*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY: 25TH INTERNATIONAL CONFERENCE, FC 2021, VIRTUAL EVENT, MARCH 1–5, 2021, REVISED SELECTED PAPERS, PART II 25 437 (2021).

[39] Strictly speaking, in Go Ethereum (geth) software they are called "transaction pools." See generally Blocknative, *What is the Mempool?*, Blocknative (2020), https://www.blocknative.com/blog/mempool-intro [https://perma.cc/P3ND-F94N].

[40] *Id*.

[41] Mikhail Kalinin, Danny Ryan & Vitalin Buterin, EIP-3675: Upgrade consensus to Proof-of-Stake, (2021), https://eips.ethereum.org/EIPS/eip-3675; Ulysse Pavloff, Yackolley Amoussou-Guenou & Sara Tucci-Piergiovanni, *Ethereum Proof-of-Stake under Scrutiny*, ARXIV PREPRINT ARXIV:2210.16070 (2022).

[42] *Id.* at 5. Every validator needs to be a "staker." "Staking" is the means through which network users participate in the validation process (as validators) of Proof of Stake (PoS) blockchains like

divided in 12-second "slots," and in every slot one specific proposer has the power to tell the network what the next block should be.[43] If she decides to construct the block on her own, then she assembles as many transactions from the mempool as will "fit" in the block, maybe adding some of her own transactions.

However, the proposer has an option of outsourcing the block-building process to specialist block builders. Those block builders also monitor the mempool and also can submit any transactions they want from outside the mempool. Typically, block builders do not have direct relations with proposers—both sides rely on an intermediary, a "relay."[44] The relay process, popularized by the Flashbots organization,[45] involves two auctions. First, block builders compete for their block to be chosen by a relay as the one block the relay will submit to the second auction. Second, relays compete for their block to be chosen by the proposer, so that the proposer declares that this block is to be added to the blockchain. In both auctions, to win one must offer the highest fee.[46]

Whoever produces a block can decide not only *which* transactions will be included, but also in *what order* will they be executed.[47] Both of those things can be valuable, because many profitable opportunities – like the example of sandwiching introduced at the beginning of this Article – depend on the order of transactions.

### *B. What is MEV?*

This brings us to the question: what is MEV? One way to think about it is that MEV is like maximal extractable ground rent, but for blockspace. Because the validator-proposer controls her piece of blockspace (a block), and because users have rivalrous, valuable uses for the scarce space, the proposer can charge users proportionately to the value they attach to what can be done in the space. Note, that the power of the proposer is not only to choose which transactions will be included in a block, but also in what order. And both inclusion and

---

Ethereum. On Ethereum, any network participant who seeks to become a validator must lock up (*stake*) 32 ETH in a sort of escrow account in order to propose blocks to the rest of the network. *See Proof-of-stake (POS)*, Ethereum.org, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[43] *Id.*

[44] *Introduction - What is MEV*-Boost, Flashbots Docs, https://docs.flashbots.net/flashbots-mev-boost/introduction. The main relays are include those operated by Flashbots, BloXroute, Blocknative, and Eden. Both block builders and block proposers can connect to multiple competing relays. Anish Agnihotri, MEVBOOST.ORG, https://www.mevboost.org/ (last visited 1/23/2023).

[45] *Id*.

[46] *Id*.

[47] Daian et al., *supra* note 9.

ordering constitute sources of value that may accrue to the proposer. Consider the following example of *arbitrage*.

Ethereum is the largest public permissionless blockchain by market capitalization to enable smart contract[48] functionality. This has given rise to a vibrant ecosystem of decentralized applications (dApps) on Ethereum but is also largely the cause of MEV on Ethereum. To illustrate, consider a smart contract which stores multiple crypto assets and provides Ethereum users with automated crypto asset exchange services. This describes a popular kind of dApp called a decentralized exchange (DEX). Notably, DEXs are magnets for MEV extraction.[49] There are many such DEXs operating on the Ethereum blockchain (as well as other blockchains), and the prices of a particular crypto asset on different DEXs may diverge. Accordingly, arbitrage opportunities arise where it becomes profitable for a strategic actor to buy the crypto asset on one DEX which offers it for a lower price and sell the crypto asset on another DEX which offers it for a higher price. This describes a common MEV extraction strategy known as "DEX arbitrage," in which the arbitrageur earns a riskless profit because of a cross-DEX price discrepancy.

Given that, on its face, this profitmaking strategy seems independent of transaction ordering and inclusion, one may wonder what exactly makes DEX arbitrage a form of MEV extraction. In a blockchain ecosystem with many sophisticated users, arbitrage opportunities have become very competitive.[50] Accordingly, in practice, multiple arbitrageurs will almost always be competing for a particular arbitrage opportunity. Because competition for a particular profit opportunity necessarily implicates transaction ordering and inclusion, it is the existence of competition that transforms an otherwise ordinary trading practice into a form of MEV extraction. To put it simply, only those who can process their arbitrage transactions earliest will be able to exploit the price discrepancy before others erase it through similar trades. Accordingly, the transaction ordering characteristic of MEV becomes necessary to exploit arbitrage opportunities. Thus, one way to look at MEV is as the theoretical maximum profit that a block proposer can extract through the strategic ordering and placement of transactions in a block.[51]

---

[48] Smart contracts are segments of code and data used to program money to autonomously perform functions or series of transactions upon the occurrence of predefined conditions. Smart contracts can even be grouped or linked together to execute increasingly complex transaction chains and/or create decentralized applications (dApps).

[49] *See, e.g.,* Jiahua Xu et al., *SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols*, ACM COMPUT. SURV. (2022), https://doi.org/10.1145/3570639; 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).

[50] *See, e.g.,* Amber Group, *supra* note 35.

[51] Alejjo Salles, *On the Formalization of MEV,* Flashbots Docs (March 21, 2021), https://writings.flashbots.net/formalization-mev/ (noting the shortcomings of most formalized definitions of MEV, and concluding that an appropriately generalized definition of MEV must

*Multi-block MEV*. The discussion so far focused on MEV extraction opportunities that arise if an agent controls a single block. However, one validator may control more than one block in a short time span, or – even if they do not – they may cooperate with others who control other single blocks.[52] This may give rise to a different class of multi-block MEV opportunities. As we discuss later, this may allow manipulation of benchmark prices that, *e.g.,* on-chain lending systems rely on.[53]

### *C. The MEV Extraction Ecosystem*

We already met three key players in the MEV extraction ecosystem: validators-proposers, specialist block builders, and relay operators intermediating between the first two. Given that many MEV extraction opportunities can be spotted, in principle, by anyone looking in the mempool, there are also Ethereum users, who are not block producers, but who extract MEV. Those users are known as "searchers." The category of searchers includes both sophisticated hedge funds and amateur solo players who are able to identify profitable MEV opportunities.[54] A searcher's difficulty is that they need to get their transactions included, usually in a specific place in a block, without being able to control block production.

What ensues is a competitive game among searchers and other MEV extractors, especially block builders. The competition is to spot valuable opportunity the fastest, and to execute them in the most efficient way. But also, it is to induce those further up in the supply chain (block builders, relays, the proposer), to include the searcher's transactions precisely at a position when they need to be executed. The last aspect of the game happens through transaction fees, either using Ethereum's in-built fee mechanism for inducing block builders to include one's transactions in their next block,[55] or outside of this formal mechanism.[56] In essence, these transaction fees play the ordering role of

incorporate both permissionlessness and the potential for a MEV opportunity to require some amount of initial capital).

[52] In proof-of-stake Ethereum it is known some time in advance who will have the right to propose (control) which block in a given "epoch," which may facilitate either cooperation or single-actor strategies. According to Barczentewicz: "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 ETH (over $53 million)"; Barczentewicz, *supra* note 18 at 13–14.

[53] *See infra* Section IV.C.

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

[55] *See, e.g.,* Daian et al., *supra* note 9.

[56] *See, e.g.,* Flashbots, *Flashbots Auction Overview,* FLASHBOTS DOCS, https://docs.flashbots.net/flashbots-auction/overview.

transaction "send time" in the continuous limit-order books of fiat-based finance.

The issue of transaction fees paid outside of the standard mechanism is closely connected with the final piece of the ecosystem puzzle: what we will call "privacy RPCs." Remember that users submit their transactions, through their wallet software, to RPC operators. In our "standard" case, RPC operators then forward transactions to "the mempool." But if a transaction is made public this way, then anyone can, *e.g.,* sandwich it – like in the example from the beginning of this Article. Avoiding this risk is one of the main rationales of privacy RPCs.[57] A privacy RPC is a service that accepts transactions and promises to forward them only to select operators, *e.g.,* select block builders.[58] Privacy RPCs may be free or paid, public or permissioned.

### *D. The Importance of Order Flow: Publicness vs. Exclusivity of Ethereum Transactions*

We began this section by describing the "standard" case, where a transaction submitted by a user lands in the public mempool. We then noted that users may protect their transactions from becoming public by submitting them to privacy RPCs. It is now time to discuss possibly the darkest of the paths of the dark forest: where a seemingly ordinary, non-private RPC treats a transaction – even if for a very short time – as their exclusive possession. We will treat these actors, namely (i) RPC operators briefly keeping private control of transactions meant to be immediately made public, together with two other kinds of actors who may have privileged access to and control over user information[59]: (ii) operators of RPCs used to query the blockchain (*e.g.,* wallet software providers) and (iii) operators of off-chain applications (websites, mobile applications) who facilitate access to on-chain applications, *e.g.,* internet-based "front-ends" for smart contracts.[60]

Given their privileged position, these three groups may be able to analyze the trading preferences associated with their users' pending transactions faster and/or more accurately than other node operators or validators, meaning that they are in a superior position to extract MEV from their users' transactions.

---

[57] The other one is bundle atomicity, *see infra* Section II.E. One qualification to this promise is that transactions routed through privacy RPCs may become public due to risks endemic to the protocol. *See* Flashbots, Uncle Bandit Risk, FLASHBOTS DOCS, https://docs.flashbots.net/flashbots-protect/rpc/uncle-bandits.

[58] *See, e.g.,* Alchemy, *How to Send Private Transactions on Ethereum,* ALCHEMY DOCS (Sept. 7, 2022), https://www.alchemy.com/overviews/ethereum-private-transactions.

[59] Barczentewicz, *supra* note 18 at 21.

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

Cases (ii) and (iii) cover situations where service providers do not control the broadcasting of pending transactions, but may exclusively possess earlier or more complete information about the user's trading intent than other network participants. Hence, these groups may possess material non-public information about their users' trades. For instance, those in group (ii) can know which of their users' blockchain queries did not end up in submitted transactions, giving those nodes an information advantage regarding their users' potential upcoming trades. Likewise, those in group (iii) may have the ability to track the activity of their users on their front-end interfaces, equipping them with valuable data about their users' trading preferences and behaviors.

Moreover, when a user (or, more likely, a wallet provider) submits a transaction to an RPC operator in group (i), this operator is in a privileged position as they possess non-public information until the moment where they rebroadcast the transaction to other nodes in the network. While reputational considerations tend to incentivize nodes to act honestly (*i.e.,* to rebroadcast the mempool transactions they receive in a timely manner), there may be cases in which these incentives are not strong enough. For instance, a node who is the first recipient of a mempool transaction may treat that transaction as private order flow (POF), intentionally delaying rebroadcasting that transaction for just fractions of a second such that it would be very difficult for external observers to detect their misbehavior. With a delay of several hundred milliseconds, the misbehaving node could assess whether the transaction presents a profitable MEV extraction opportunity and, if so, submit the node's own transactions to take advantage of the opportunity. This series of events could all occur before the transaction actually becomes public (i.e. accessible to other nodes in the network).

In sum, transactions are not assured to be public or private on the basis of their purported routing. It is important to understand the nuance involved in transaction routing on Ethereum prior to classifying transactions as *public* or *non-public*, given the significant legal consequences associated with the publicness of information. We suggest that a meaningful standard of publicness for a pending transaction would be the following: 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.[61] This standard would be satisfied even if reliably detecting public transactions requires maintaining "watcher" nodes simultaneously in several

[61] The qualification about accessing a pending transaction in an unencrypted state is important because transactions may be transmitted in an encrypted state, *e.g.,* in commit-reveal schemes; *see* M. Arulprakash & R. Jebakumar, *Commit-reveal strategy to increase the transaction confidentiality in order to counter the issue of front running in blockchain*, 2460 AIP CONFERENCE PROCEEDINGS 020016 (2022). To the extent a transaction is encrypted, it does not give access to material information. There may be encryption schemes that only encrypt some parts of a transaction: in that case, some – but not all – information about a pending transaction may be public.

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.

### *E. Strategies for Generating Profit through MEV*

Like opportunistic trading practices in traditional finance, the strategies through which MEV extractors seek out profits are virtually infinite and constantly evolving. There are several identifiable categories of MEV extraction strategies on the Ethereum blockchain, which have been the most studied and discussed. Even though in our legal analysis we only consider sandwiches and liquidations, we very briefly describe here all the main strategies, to give the reader a more complete picture.

*Sandwiches (sandwich trades).*[62] We started this paper with an example of sandwiching.[63] As is apparent from that example, a sandwich consists of three elements: (1) the front-run, (2) at least one sandwiched transaction, 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). Because the validator controls the order of transactions, they can place the front-run before the sandwiched transaction, and the back-run just after it. Sandwiched traders are harmed by sandwiches mainly by obtaining a worse trade execution price (*i.e.*, paying more of X for the same amount of Y) than they would have gotten in the absence of a sandwich. We are aware of two situations where a sandwich may not result in that kind of harm: i) "just-in-time liquidity" provision through a sandwich[64] and ii) sandwiches where the front-running transaction is so relatively small that it does not meaningfully affect the execution price of the

[62] Sandwich trades are often referred to as "sandwich attacks." Instead, throughout the rest of this paper, we refer to this practice as a "sandwich trade" or a "sandwich". In doing so, we seek to avoid unhelpful and premature normative implications, allowing for genuine debate regarding the normative and legal character of sandwich trades.

[63] *See supra* Section I.

[64] 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* Robert Miller (@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.,* Chainsight (@ChainsightLabs), Twitter (Nov. 9, 2021, 7:30 AM), https://twitter.com/ChainsightLabs/status/1457958811243778052.

sandwiched transaction.[65] According to a recent analysis, only in the first six months of 2022 sandwich attacks resulted in $87.7 million in loses to Ethereum users, bringing $17.85 millions of profit to the sandwichers.[66] Most Ethereum addresses that were identified as victims of sandwich attacks, lost "between $50 and $500."[67] 80% of aggregate losses have been incurred by Ethereum addresses that were sandwiched less than 20 times.[68]

*DEX arbitrage.* As described earlier in this section,[69] arbitrage between decentralized exchanges is among the simplest, most common, and most competitive MEV opportunities.

*CEX/DEX arbitrage*. Price discrepancies arise also between centralized crypto exchanges (CEX; *e.g.,* Binance, Coinbase, Kraken) and DEXs. This kind of arbitrage requires off-chain actions, on a CEX, so only partially may constitute MEV extraction.[70]

*Loan liquidations*. Liquidations operate in a similar manner to margin calls in traditional finance.[71] However, they are not performed by the lender, but by anyone who is willing to step in and buy the collateral, thus repaying the loan. If a borrower's loan becomes undercollateralized because the price of the collateral on some benchmark market has fallen, the decentralized lending protocol permits anyone to trigger a liquidation of the borrower's remaining collateral.[72] Such *liquidators* are remunerated in the form of a discount on the price of collateral.[73] Liquidations constitute MEV, because they are usually competitive and only the first actor to execute a liquidation will be able to profit from it. Thus, having control over whose liquidation-attempting transaction will be included first on the blockchain, entails having control over who will profit. As we discuss below, liquidation opportunities may be artificially created with the use of "oracle manipulation."[74]

*Long tail MEV.* The main types of strategies just listed do not exhaust the universe of profitable MEV extraction opportunities that may arise whenever a

---

[65] This is more likely to happen if the asset that is expected to rise in price cannot be leveraged for a riskless back-run from a different on-chain market (*e.g.* is not available in any other "liquidity pool"). *See, e.g.,* Stalkopat, Flashbots Discord server (Aug. 8, 2022, 7:53 PM); Hasu (@hasufl), Twitter (Sep. 26, 2021, 5:14 PM), https://twitter.com/hasufl/status/1442145582978674713.

[66] EIGENPHI RESEARCH, *supra* note 11 at 5.

[67] *Id.* at 26.

[68] *Id.* at 27.

[69] *See supra* Section II.C.

[70] Amber Group, *supra* note 35.

[71] SIRIO ARAMONTE ET AL., *DeFi lending: intermediation without information?*, (2022); Kaihua Qin et al., *An empirical study of DeFi liquidations*, *in* PROCEEDINGS OF THE 21ST ACM INTERNET MEASUREMENT CONFERENCE (2021), https://doi.org/10.1145%2F3487552.3487811.

[72] We refer to what Qin et al. call "fixed spread liquidation" (used, e.g., by Aave, Compound, and dYdX) as distinguished from "auction liquidations" (used, e.g., by MakerDAO); only a fixed spread liquidation "allows to extract value in a single, atomic transaction"; Qin, Zhou, and Gervais, *supra* note 49 at 5.

[73] ARAMONTE ET AL., *supra* note 71.

[74] *See infra* Section IV.C. For an introduction to the concept of an "oracle," *see supra* note 25.

competitive valuable use of blockspace can be identified. This may include, *e.g.,* NFT "minting" and trading opportunities.[75]

### *F. The Techniques for Executing MEV Strategies*

The profit-making strategies introduced above are executed using several main techniques, which are not necessarily mutually exclusive. Front-running and back-running of some target transactions are the main and the most basic ones. Those techniques are used for sandwiching, arbitrages, and liquidations. Front-running refers to placing a transaction ahead of a target transaction, back-running to placing it after. In some contexts, like for sandwiching, it may matter that front- or back-running transactions are immediately adjacent to the target transaction, but this is not always the case.

*Generalized front-running.* Generalized front-running is a practice engaged in primarily by automated bots. These bots monitor the mempool, seeking to detect pending transactions which yield immediate profits to the user who submitted the pending transaction upon execution. The generalized front-running bot then copies the profitable pending transaction and submits their own version with a higher gas price. As a result, the bot's version of the profitable transaction will be executed on the blockchain state, and the user who originally found the profitable opportunity is deprived of their anticipated profit.[76] Generalized front-running bots do not seek out a particular transaction type to front-run, but target any-and-all transactions which they determine -- by simulating the blockchain state-change resulting from the pending transaction's execution – to have a high probability of producing immediate profits to the transaction originator.[77] As generalized front-runners do not discriminate in their activity on the basis of anything other than local profitability, their effects extend beyond DEX trades to centralized exchanges, derivative protocols that rely on oracle price updates,[78] and non-fungible token purchases.

---

[75] One example of Long tail MEV is the practice of NFT sniping. NFT sniping involves a MEV extractor identifying a NFT offered at a price which is significantly lower than both i) the previous lowest offer for the collection and ii) the average of prices for NFTs within the collection listed before and after the instance of NFT sniping. The MEV extractor would then offer a high bribe payment to validators in order to front-run other potential purchasers and "snipe" the NFT at the low price. *See, e.g.,* Zhou et al., *supra* note 32; Amber Group, *supra* note 35.

[76] Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen & Lorenzo Gentile, *SoK: Mitigation of Front-running in Decentralized Finance,* IACR CRYPTOL. EPRINT ARCH. (2021) at 4, https://eprint.iacr.org/2021/1628.pdf.

[77] Peyman Momeni, Sergey Gorbunov, and Bohan Zhang, *FairBlock: Preventing Blockchain Front-running with Minimal Overheads,* IACR CRYPTOL. EPRINT ARCH. (2022) at 21-22, https://eprint.iacr.org/2022/1066.pdf.

[78] *See* Zach, *Miner-Extractable Value, Oracle Front-running, and the Rise of Arbitrage Bots,* SMART CONTRACT RESEARCH FORUM (Jan. 2021), https://www.smartcontractresearch.org/t/miner-extractable-value-oracle-front-running-and-the-rise-of-arbitrage-bots/179.

*Atomicity*. "Atomicity" means that a sequence of instructions packaged together will be executed in an "all or nothing" manner: either all will be executed in the set order, or none will. This can be achieved for *single transaction* that uses a smart contract to execute a number of instructions—effectively allowing one transaction to have several steps, with a guarantee that if something goes wrong with one step, no part of the transaction will have consequences.[79] This can also be achieved for *a sequence of transactions*, if they are submitted as a "bundle" to a block builder who provides this guarantee for bundles. Whether a MEV opportunity is atomic is relevant to our discussion for two interconnected reasons: first, atomicity can imply a certainty of profit from resources expended, which mitigates risk and increases the competitiveness of an opportunity;[80] and second, atomic transaction sequences are less likely than non-atomic transaction sequences to create a lasting price impact on a decentralized exchange. Specifically, sandwichers strongly prefer relying on atomicity because this strategy may require significant amounts of upfront capital. However, sandwichers are not always able to use atomistic bundles.[81]

## III. THE LAW OF MARKET MANIPULATION

### *A. Scope of Legal Analysis*

This Part provides an overview of the legal frameworks which guide our analysis of the legality of MEV extraction. We focus on the law of market manipulation governing securities and commodities markets in the United States. After sketching the relevant statutory regimes, we dive deeper into open market manipulation, insider trading, and front-running.

In the United States, market regulation occurs on a bifurcated basis, with the Securities and Exchange Commission (SEC) governing securities markets and the Commodities and Futures Trading Commission (CFTC) overseeing markets in commodities and most derivatives.[82] The regulation of any instance of MEV extraction will depend on the asset classification of the crypto asset(s) used in the MEV extraction strategy as securities or commodities.

However, an unresolved jurisdictional "turf war" exists between the SEC and CFTC, who both seek regulatory authority over the burgeoning new asset

---

[79] Daian et al., *supra* note 9 at 4.

[80] *Id.* at 2.

[81] In their work quantifying the effects and properties of sandwich attacks, Qin. et al. found that some sandwich attacks take place where the front-run and back-run are separated by more than 200 transactions; Qin, Zhou, and Gervais, *supra* note 49 at 4–5.

[82] *See* A JOINT REPORT OF THE SEC AND THE CFTC ON HARMONIZATION OF REGULATION (2009) ("Since the 1930s, securities and futures have been subject to separate regulatory regimes.").

class of crypto assets.[83] Both the SEC and CFTC have opted for an adjudication-based (as opposed to rule-based) approach to policymaking with respect to crypto assets, with both agencies currently pursuing enforcement actions grounded in claims that particular crypto assets belong within their respective jurisdictional domains.[84] Commentators have also joined this debate to offer important practical, legal, and technical considerations implicated in this issue.[85] We do not attempt to resolve these tensions and proceed throughout this paper on the assumption that either the SEC's or CFTC's regulatory regime may apply to crypto assets affected by the MEV extraction strategies we discuss. Conveniently, as we'll see, the substance of most of the applicable standards relating to market manipulation relevant to MEV are the same regardless of whether the asset is classified as a security or a commodity.[86]

### *B. Anti-Market Manipulation Rules*

The Securities Exchange Act of 1934 (SEA) and the Commodities Exchange Act (CEA) equip the SEC and CFTC, respectively, with broad statutory authority to police market manipulation in their respective markets.[87] Yet, this authority is fluid: "the word 'manipulation'... in its use is so broad as

---

[83] *Compare* SEC Chair Gary Gensler, Speech: "Kennedy and Crypto", September 8, 2022, available at https://www.sec.gov/news/speech/gensler-sec-speaks-090822 ("Of the nearly 10,000 tokens in the crypto market, I believe the vast majority are securities" (footnote omitted)) ("Kennedy and Crypto") *with Digital Commodities Consumer Protection Act: Hearing to Review S.4760 Before the S. Comm. on Agriculture, Nutrition, and Forestry,* 117th Congress (2022) (statement of The Honorable Rostin Behnam, Chairman, Commodity Futures Trading Commission)("as has been recognized by federal courts, many digital assets constitute commodities. As recognized by the DCCPA, the CFTC's expertise and experience make it the right regulator for the digital asset commodity market"). *See also CFTC v. McDonnell*, 332 F. Supp. 3d 641, 651 (E.D.N.Y. 2018) ("Virtual currency may be regulated by the CFTC as a commodity.").

[84] *See, e.g.,* Complaint at 2, CFTC v. FTX Trading et al, No. 1:22-cv-10503 (S.D.N.Y. filed Dec. 13, 2022) (treating relevant the digital assets as commodities); Complaint at 6, SEC v. Eisenberg, No. 1:23-cv-503 (S.D.N.Y. filed Jan. 20, 2023) (treating other digital assets, specifically governance tokens on Mango Markets, as securities).

[85] *See, e.g.,* Cohen, Lewis R., Strong, Gregory, Lewin, Freeman & Chen, Sara, The *Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are Not Securities* (Nov. 10, 2022), https://dlxlaw.com/wp-content/uploads/2022/11/The-Ineluctable-Modality-of-Securities-Law-%E2%80%93-DLx-Law-Discussion-Draft-Nov.-10-2022.pdf (discussion draft)*;* Thomas L. Hazen, *Tulips, Oranges, Worms, and Coins – Virtual, Digital, or Crypto Currency and the Securities Laws*, 20 N.C. J.L. & Tech. 493 (2019) ("under most, if not all, circumstances, crypto currencies are likely to be securities").

[86] *See*, *e.g*., *Prohibition on Manipulative and Deceptive Devices*, 76 Fed. Reg. at 41399 ("The language of CEA section 6(c)(1), particularly the operative phrase 'manipulative or deceptive device or contrivance, is virtually identical to the terms used in section 10(b) of the Securities Exchange Act of 1934") (internal quotation marks omitted).

[87] *See* 7 U.S.C. § 6(c) and 9(a)(2) *and* 15 U.S.C. § 78(i) and 78(j).

to include any operation of the … market that does not suit the gentleman who is speaking at the moment".[88] As we'll see this challenge is posed in especially stark terms by the complex phenomenon of MEV extraction. As such, MEV is an ideal vehicle for illuminating operative assumptions and crystallizing issues that require clarity.

Despite the jurisdictional differences of the SEC and CFTC, the purpose motivating each agency's anti-manipulation enforcement is the same. According to Professor Gina-Gail Fletcher, market manipulation, if left unchecked, "can eventually lead to the demise of the market" because it i) "[interferes] with price accuracy" by injecting false information into the market and creating false impressions of liquidity, and ii) "adversely impacts market integrity" by harming the actual and perceived fairness of the market.[89] Accordingly, the SEC and CFTC are concerned with market manipulation in their respective markets for the same reason: because it undermines the efficiency (including, but not limited to, price accuracy)[90] and integrity of the markets which it is their role to protect. They root out manipulative behavior which harms price accuracy by prohibiting price manipulation, and that which harms market integrity by prohibiting fraud and misstatements with respect to the asset class they regulate. We address each of these broad prohibitions in turn.[91]

1. Price Manipulation

Both section 9(a)(2) of the SEA and Section 6(c)(3) of the CEA prohibit price manipulation.[92] Historically, the CFTC has been more active than the SEC in exercising their price manipulation authority under CEA s6(c)(3), codified by the agency as Rule 180.2,[93] because it was largely their only means of anti-manipulation enforcement prior to the passage of the Dodd-Frank Wall Street

[88] Craig Pirrong, *Commodity Market Manipulation Law: A (Very) Critical Analysis and a Proposed Alternative,* 51 Wash. & Lee L. Rev. 944, 949 (1994), quoting 2 FEDERAL TRADE COMM'N, THE COTTON TRADE, S. Doc. No. 100, 68th Cong., Ist Sess. 148 (1924), mtcroformed on CIS No. 8242 (Congressional Info. Serv.).

[89] Fletcher, *supra* note 21.

[90] *Id.* at 490.

[91] The SEC and CFTC also prohibit "fictitious trades", another broad category of manipulative practices. We focus our discussion here on price manipulation and fraud/misstatements as these classes of manipulative behavior are most relevant to our legal analysis of MEV extraction practices. For a discussion of fictitious trades, *see Id.* at 499.

[92] *See* SEA s9(a)(2) [15 U.S.C. s78i(a)(2)] (prohibiting transactions in a security which "creat[e] actual or apparent active trading" or "rais[e] or [depress] the price of such a security, for the purpose of inducing the purchase or sale of such security by others") *and* CEA s6(c)(3) [7 U.S.C. s9(3)] (making it unlawful to "manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity").

[93] 17 C.F.R. § 180.2 (2012).

Reform and Consumer Protection Act (Dodd-Frank).[94] Meanwhile, the SEC has tended more often to pursue price manipulation cases under SEA s10(b) and Rule 10b-5,[95] the agency's longstanding authority to police fraud-based manipulation, when possible.[96] Accordingly, and as reflected below, much of the defining features of price manipulation are expounded in the case law of enforcement actions brought by the CFTC.

CFTC Rule 180.2 renders it unlawful for "any person, directly or indirectly, to manipulate or attempt to manipulate the price of any swap, or of any commodity in interstate commerce".[97] There are four requisite elements to a successful claim for price manipulation: (1) an artificial price existed; (2) the accused caused the artificial price; (3) the accused had the ability to influence a market price; and (4) the accused specifically intended to cause the artificial price.[98]

(1) An artificial price is a price which "does not reflect the market or economic forces of supply and demand".[99] A price is considered artificial where it is "affected by a factor which is not legitimate."[100] Price artificiality is often called the *sine qua non* of price manipulation,[101] yet, no binding tests exists for determining which *forces* or *factors* informing a price are legitimate and which are not.[102] Thus, some scholars question the meaningfulness of an artificiality-based standard.[103] As such, determinations of price artificiality generally depend on a variety of considerations including, but not limited to, i) the competitiveness

---

[94] Merritt B Fox, Lawrence R Glosten & Gabriel V Rauterberg, *Stock market manipulation and its regulation*, 35 YALE J. ON REG. 67, 117 (2018).

[95] *See* 15 U.S.C. §78j (2014) and 17 C.F.R. §240.10b-5 (codifying the SEC's authority to prohibit fraud-based manipulation as the SEC's regulation 10b-5).

[96] Fox, Glosten, and Rauterberg, *supra* note 94 at 117.

[97] 17 CFR § 180.2.

[98] *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 531 (S.D.N.Y. 2008).

[99] *In re* Cox, [1986-1987 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 23,786, at 24,060 (CFTC July 15, 1987); *see also* SEC v. Resch-Cassin & Co., 362 F. Supp. 964, 978 (S.D.N.Y. 1973) (finding manipulation of the price of a security in violation of SEA §9(a)(2) because defendant made "it appear to be the product of the independent forces of supply and demand when... in reality, it was completely a creature of defendants' subterfuge").

[100] *In re* Cox, ¶ 23,786 at 26,060.

[101] *See, e.g.,* Pirrong, *supra* note 88 at 956.

[102] In re Indiana Farm Bureau Coop. Ass'n, Inc., [1982-1984 Transfer Binder] Comm. Fut. L. Rep. (CCH) 21,796, at 80-81,281(CFTC Dec. 17, 1982)(Johnson, C., concurring) ("Legitimacy with respect to supply and demand is undefined in law and economics, unless the sole question is whether the forces were put in motion by an illegal act").

[103] Frank H. Easterbrook, Monopoly, Manipulation, and the Regulation of Futures Markets, 59 J. BUS. S103, S117 (1986) ("An effort to isolate which "forces of supply and demand" are "basic" and which are not is doomed to failure. (…) Economists think of supply and demand as givens. (…) There is no way to say what demand is real and what is artificial."); Matthijs Nelemans, Redefining Trade-Based Market Manipulation, 42 VAL. U. L. REV. 1169 (2008)(arguing that "prohibitions to counteract traders who cause artificial prices" are problematic because they "lack a precise delineation of 'non-artificial price' versus 'artificial price'").

of a market,[104] ii) the presence of fraud or deceptive omission which misleads market participants[105] and iii) whether the trading pattern of the accused is supported by a "legitimate economic rationale"[106] (although the term "legitimate" renders this consideration circular).

(2) After establishing price artificiality, a causal relationship between the artificial price and an identifiable trader or group of traders must be shown.[107] Artificial prices do not arise merely because of volatile market conditions, government action, or other forces beyond the defendant's control. In practice, courts often engage in effectively a *'but-for'* price assessment – looking to what the price would have been but-for the defendant's trading activity.[108]

(3) The "*ability to influence a market price"* element of price manipulation is sometimes built into this causation analysis, with courts looking to evidence of a defendant's market dominance as indicators of both their ability to have caused and actual causation of an artificial price.[109]

(4) The final and, oftentimes, most difficult element of a price manipulation claim to prove is the 'specific intent' of an alleged price manipulator to cause an artificial price.[110] In *Indiana Farm*, the court held that price manipulation

---

[104] *See, e.g.,* United States CFTC v. Donald R. Wilson & Drw Invs., No. 13 Civ. 7884, 2018 LEXIS 207376, at *40 (S.D.N.Y. Nov. 30, 2018) ("a price is artificial when it has been set by some mechanism which … prevent[s] the determination of those prices from free competition alone") (internal citations omitted).

[105] *See, e.g.,* In re Tether & Bitfinex Crypto Asset Litig., 576 F. Supp. 3d 55 (S.D.N.Y. 2021)( Plaintiffs sufficiently alleged price manipulation on the basis of defendants' fraudulent issuances of unbacked Tether (USDT), which defendants' publicly stated were backed by the US dollar); *Resch-Cassin & Co*., 362 F. Supp. at 964, 977 (S.D.N.Y. 1973)(defendants engaged in price manipulation because they "create[d] a false appearance of activity in the over-the-counter market [which tended] to support the price at an inflated level" by using their "dominion and control of the market"); Easterbrook, *supra* note 103 at 118 ("manipulation is a form of fraud [in which]…the profit flows solely from the trader's ability to conceal his position from other traders").

[106] *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 535 (S.D.N.Y 2008) ("If a trading pattern is supported by a legitimate economic rationale, it cannot be the basis for liability under the CEA because it does not send a false signal").

[107] *In re Cox,* ¶ 23,786, at 35-36,060 (CFTC July 15, 1987) ("Once the Division of Enforcement shows that the respondents had the ability to influence prices and that the prices in question were artificial, it must then show that the respondents caused the artificial prices").

[108] *See, e.g.,* CFTC v. Parnon Energy Inc., 875 F. Supp. 2d 233, 246 (S.D.N.Y. 2012) (applying but-for test in this context); *In re Cox,* ¶ 23,786 at 11,060 ("accused lacks the ability to influence prices if other market participants can bypass his demands and extinguish their obligations elsewhere").

[109] *In re Cox,* ¶ 23,786 at 12-13, 060 ("the acquisition of market dominance is the hallmark of a long manipulative squeeze"); *Resch-Cassin & Co*., 362 F. Supp. at 977 ("dominion and control of the market for the security" are factors establishing causation of an artificial price).

[110] In securities price manipulation cases under SEA s9(a)(2), the language used in reference to this element is sometimes different. In the context of securities price manipulation, courts often use terms like *"*purpose" (see *Resch-Cassin & Co*., 362 F. Supp. at 977), *"*motive", and *"*willfulness" (see Crane Co. v. Westinghouse Air Brake Co., 419 F.2d 787, 795 (2d Cir. 1969)) when referring to the requisite scienter for a violation.

liability requires a showing that the defendant "acted (or failed to act) with the purpose or conscious object of causing or effecting a price or price trend in the market that did not reflect the legitimate forces of supply and demand".[111] The CFTC's recent defeat in *CFTC v DRW & Wilson* re-emphasized that "mere intent to affect prices is not enough" to establish a price manipulation claim, but the defendant must have "intended to cause artificial prices".[112]

Price manipulation liability alone has proved inadequate as a vehicle for protecting the efficiency and integrity of markets.[113] Given the stringent requirements of establishing price artificiality and intent to manipulate prices, the SEC has consistently strayed away from exercising its anti-price manipulation authority in securities market manipulation cases, opting instead to rely on the fraud-based manipulation prohibition under SEA s10(b) and Rule 10b-5.[114] More remarkably, the CFTC – who was until recently left with no other choice but to police commodities market manipulation through price manipulation charges – tried time and again to bring price manipulation claims, but has only a single court victory to show for it.[115]

Realizing the inadequacy of this approach, Congress imbued the CFTC with expanded authority, modeled explicitly after the SEC's Rule 10b-5, to effectively police commodities market manipulation in 2010, through the passage of s753 of Dodd-Frank and codified in CFTC Rule 180.1, to which we now turn.[116]

2. Fraud-Based Manipulation

S753 of Dodd-Frank amended CEA s6(c) to give the CFTC the authority – long exercised by the SEC for securities under SEA s10(b) and Rule 10b-5 – to prohibit the use of any "manipulative or deceptive or contrivance" in contravention of CFTC rules in connection with commodities, swaps, or

---

[111] *In re* Indiana Farm Bureau Coop. Ass'n, Inc., [1982-1984 Transfer Binder] Comm. Fut. L. Rep. (CCH) 21,796, at 8,281(CFTC Dec. 17, 1982).

[112] *CFTC v. Wilson*, No. 13 Civ. 7884 (RJS), 2018 LEXIS 207376 (S.D.N.Y. Nov. 23, 2018) at *39, quoting *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 535 (S.D.N.Y 2008).

[113] Rosa M. Abrantes-Metz, Gabriel Rauterberg, & Andrew Verstein, *Revolution in Manipulation Law: The New CFTC Rules and the Urgent Need For Economic and Empirical Analyses*, 15 Penn. J. Bus. L., 357 (2013); Jerry W. Markham, *Manipulation of Commodity Futures Prices-The Unprosecutable Crime*, 8 Yale J. On Reg. 281 (1991) (noting that price manipulation is "virtually unprosecutable" as "Plaintiffs must establish a manipulative intent that is conceptually and doctrinally among the most demanding mental state requirements anywhere in financial law.").

[114] Maxwell K. Multer, *Open-Market Manipulation Under SEC Rule 10b-5 and its Analogues: Inappropriate Distinctions, Judicial Disagreement and Case Study: FERC's Anti-Manipulation Rule*, 39 SEC. REG. L.J. 97, 98 n.3 (2011).

[115] *See* DiPlacido v. CFTC, 364 F. App'x 657 (2d Cir. 200*9);* this does not include settlements received by the CFTC in price manipulation actions.

[116] CFTC OFF. OF PUB. AFFAIRS, ANTI-MANIPULATION AND ANTI-FRAUD FINAL RULES (2011).

futures.[117] CEA s6(c)(1), codified through CFTC Rule 180.1,[118] empowered the CFTC to police market manipulation even in the absence of evidence establishing a defendant's specific intent to manipulate prices or the existence of an artificial price.[119] In relevant part, Rule 180.1 makes it unlawful for those engaged in commodities trades "to intentionally or recklessly":

> (1) Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;
>
> (2) Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;
>
> (3) Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person[.] [120]

In the adopting release accompanying the CFTC's enactment of Rule 180.1, the agency clarified that its application would be "guided, but not controlled, by the substantial body of judicial precedent" interpreting the Securities and Exchange Commission's Rule 10b-5.[121] That is, the interpretation of Rule 180.1 in the context of commodities markets draws explicitly from Rule 10b-5 precedent in securities markets.[122]

The requisite elements of a successful 180.1 enforcement action include evidence of: i) reckless or intentional conduct by the accused, and ii) a "manipulative device, scheme, or artifice to defraud."[123] Like Rule 10b-5, Rule 180.1 is intended be a "broad catch-all provision" capturing all instances of fraud-based manipulation, and it has been applied as such.[124] Rule 180.1, in its relatively few years of existence, has been used by the CFTC to prosecute conduct ranging from insider trading in commodities[125] to the alleged corporate misconduct of Samuel Bankman-Fried and related entities in the FTX debacle.[126]

---

[117] 7 U.S.C. §9(1) (2011).

[118] 17 C.F.R. §180.1 (2012).

[119] Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41398, 41403 (July 14, 2011) (codified at 17 CFR pt. 180).

[120] 17 C.F.R. §180.1 (2012).

[121] *Supra* note 119.

[122] Gregory Scopino, *The (questionable) legality of high-speed pinging and front running in the futures market*, 47 CONN. L. REV. 607, 617–618 (2015).

[123] 17 C.F.R. §180.1 (2012).

[124] *Supra* note 119 at 41403.

[125] For an overview of significant insider trading cases brought by the CFTC, see Latham & Watkins, I*nsider Trading in Commodities Markets: An Evolving Enforcement Priority,* Client Alert White Paper (March 11, 2021), https://www.lw.com/admin/upload/SiteAttachments/Alert%202827.v5.pdf.

[126] *See* Complaint at 2, CFTC v. FTX Trading et al, No. 1:22-cv-10503 (S.D.N.Y. filed Dec. 13, 2022).

Yet, while capacious, Rule 180.1 still has discrete limits in its application. Most importantly, Rule 180.1 parallels SEC Rule 10b-5 in that it is "described as a catchall provision, but what it catches must be fraud".[127] With this said, it is important to note that *fraud* in the context of fraud-based manipulation is not just fraud in its common sense, as express misrepresentation or deceptive omission.[128] Rather, fraud-based manipulation under Rule 10b-5 and Rule 180.1 can include both claims of fraud by misleading statements or deceptive omissions, and manipulative action which send a "false pricing signal to the market."[129] A promising means for establishing fraud-based manipulation is the *fraud-on-the-market* (FOTM) theory.[130] While the FOTM theory has long been used in the securities fraud context, the advent of Rule 180.1 suggests that it may have some success in commodities' manipulation cases as well.[131] More specifically, Gregory Scopino proposes a variant of FOTM which he calls, and we will refer to, as the *manipulation-as-fraud* legal theory, which provides:

> market participants are entitled to rely on the assumption that the securities market is free of manipulation and they are therefore deceived when, unbeknownst to them, a wrongdoer manipulates the market and distorts the way that the market prices securities.[132]

It is important to note here that the courts themselves disagree as to whether trading activity alone is a form of manipulative *action* that can constitute fraud-based manipulation in the absence of express misrepresentations or other independent unlawful acts.[133] This raises a concept that will figure into our analysis below: open-market manipulation. 'Open-market manipulation' refers

---

[127] *See* Chiarella v. United States, 445 U.S. 222, 235-236(1980) (describing SEC's Rule 10b-5) ; United States CFTC v. Kraft Foods Grp., Inc., 153 F. Supp. 3d 996, 1010 (N.D. Ill. 2015) ("this Court finds that Section 6(c)(1) and Regulation 180.1 prohibit only fraudulent conduct").

[128] ATSI Commc'ns, Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 100 (2d Cir. 2007) ("Section 10(b), in proscribing the use of a 'manipulative or deceptive device or contrivance,'... prohibits not only material misstatements but also manipulative acts").

[129] *In re* Tether & Bitfinex Crypto Asset Litig., 576 F. Supp. 3d 55, 114 (S.D.N.Y. 2021), quoting *ATSI Commc'ns*, 493 F.3d at 100 (observing that both SEA 10(b) and the CEA plus Rule 180.1 "'prohibit[] not only material misstatments but also manipulative acts,' including 'a transaction that sends a false pricing signal to the market.'").

[130] In the securities context, the FOTM theory "establishes a rebuttable presumption in private rights of action under Exchange Act 10(b) and SEC Rule 10b-5 that in an efficient market for a security a plaintiff can be held to have relied on a defendant's fraudulent misrepresentation or omission in connection with the purchase or sale of a security—even if the plaintiff was not aware of the misrepresentation or omission—by virtue of the plaintiff's reliance on the fact that a security's price reflects the fraudulent misrepresentation and omission". *Supra* note 119 at 41402 n.50.

[131] In the enacting release of Rule 180.1, the CFTC "decline[d] to adopt comments recommending outright rejection of the potential application of the 'fraud-on-the-market' theory under final Rule 180.1." *Id.* at 41403.

[132] Scopino, *supra* note 122 at 672.

[133] *See* Fox, Glosten, and Rauterberg, *supra* note 94 at 119–122 (discussing the circuit split with respect to whether trading activity -- i.e. "open market manipulation" -- on its own can constitute fraud-based manipulation under Rule 10b-5).

to manipulative schemes which involve facially legitimate, open-market trading practices.[134] While the Second and D.C. Circuits have found open-market manipulation to violate Rule 10b-5[135] when it is combined with manipulative intent,[136] the Third circuit has rejected the notion that a facially legitimate trade alone can be considered manipulative because it does not "[inject] inaccurate information" into the market.[137]

Some examples of open market manipulation, such as banging the close, are clearly seen as prohibited forms of manipulation, however. Banging the close involves executing many trades at the end of the trading period (settlement window) to give a false impression of high trading volume.[138] Often, this will be in order to benefit their position in a derivative (for instance, an option or swap) which is priced based on the settlement price of the asset traded.[139] Generally, banging the close involves transactions which are, in themselves, uneconomic, but become profitable to the manipulator based on their outsized impact on the

---

[134] For a more in-depth discussion of open-market manipulation, see Fletcher, *supra* note 21.

[135] While many instances of open-market manipulation could theoretically be brought as price manipulation charges, the aforementioned challenges of successful price manipulation actions make the agencies' fraud-based manipulation prohibitions (10b-5 and Rule 180.1) better suited to open-market manipulation.

[136] *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 535 (S.D.N.Y 2008) ("a legitimate transaction combined with an improper motive is commodities manipulation"); SEC v. Masri, 523 F. Supp. 2d 361, 373 (S.D.N.Y. 2007)("if an investor conducts an open-market transaction with the intent of artificially affecting the price of the security, and not for any legitimate economic reason, it can constitute market manipulation"); Markowski v. SEC, 274 F.3d 525 (D.C. Cir. 2001)(holding that Rule 10b-5 prohibits manipulations involving trades "solely because of the actor's purpose" regardless of whether any unlawful act occurred).

[137] GFL Advantage Fund, Ltd. v. Colkitt, 272 F.3d 189, 206(3d Cir. 2001), quoting In re Olympia Brewing Co. Securities Litigation, 613 F. Supp. 1286, 1292 (N.D. Ill. 1985)("[r]egardless of whether market manipulation is achieved through deceptive trading activities or deceptive statements….it is clear that the essential element of the claim is that inaccurate information is being injected into the marketplace").

[138] *CFTC v. Amaranth Advisors*, L.L.C., 554 F. Supp. 2d 523, 528 (S.D.N.Y. 2008) ("purchasing a substantial number of futures contracts leading up to the closing range on expiration day, followed by the sale of those contracts several minutes before the close of trading[] is known as "marking the close"); *id*. at 534 ("there is no doubt that marking the close or any other trading practices, without an allegation of fraudulent conduct, can also constitute manipulation in contravention of the CEA, so long as they are pursued with a manipulative intent").

[139] CFTC, 'Banging the Close', *CFTC Glossary*, https://www.cftc.gov/LearnAndProtect/EducationCenter/CFTCGlossary/glossary_b.html#:~:text=Banging%20the%20Close%3A%20A%20manipulative,position%20in%20an%20option%2C%20swap (last visited Jan. 25, 2023); *Koch v SEC* (finding market manipulation in violation of SEA s10(b) for marking the close).

pricing of a different, but related position.[140] These trading strategies have been ruled out as deceptive forms of manipulation.[141]

In its paradigmatic sense, banging the close constitutes what has been called a *covered* open-market manipulation scheme.[142] Covered open-market manipulation derives its name from the fact that the trading activity involves (is covered by) a structural mechanism or arrangement that generates heightened duties of trust and honest dealing. Thus, covered open-market manipulation typically involves trades in some financial instrument X with the purpose of moving the price of financial instrument Y, where the pricing of Y is explicitly determined (i.e. through a benchmark or other formal dependent pricing mechanism) by reference to the price of X.[143] It is this pricing mechanism for Y, which explicitly references X, that creates the relationship of trust which entails heightened duties to avoid manipulation (e.g. an implied expectation that one will avoid affecting Y's price through exploiting trades in X, rather than simply allowing Y's price to be set independently by uninterested third parties' good faith demand for X).

By contrast, *naked* open-market manipulation is not covered by any trust relationship resulting in heightened duties. A paradigmatic example would be a simple "buy-low, sell-high" profitmaking strategy, with the added element that the trader has "some way of preventing the price from increasing as she purchased, decreasing as she sells, or both."[144] Covered open-market manipulation schemes involve some explicit or implicit agreement – that is, an agreement not to manipulate a predetermined formal pricing mechanism – which is interfered with by the manipulator.[145] By contrast, naked open-market manipulation schemes involve no such agreements or relations of trust, whether express or implied, which would be breached by their occurrence. As such, naked open market manipulation schemes tend to be both more difficult to pull off, at least profitably, and predictably will be more difficult to prosecute than covered open-market manipulation. We return to these issues in discussing sandwiching public versus private transactions in Sections IV.A-B.

---

[140] CFTC v. Wilson, No. 13 Civ. 7884 (RJS), 2018 LEXIS 207376 (S.D.N.Y. Nov. 23, 2018) at *57 (defining 'banging the close' as involving "someone putting in a disproportionate number of trades to push the price up or down to affect the closing price, typically in a noneconomic fashion, to benefit a position that they held elsewhere").

[141] See *supra* notes 138, 139.

[142] *Covered* open-market manipulation has also been referred to as open-market manipulation with an external interest and contract-based manipulation. *See* Fox, Glosten, and Rauterberg, *supra* note 94 at 75.; Daniel R. Fischel & David J. Ross, *Should the Law Prohibit "Manipulation" in Financial Markets?*, 105 Harv. L. Rev. 503, 523 (Dec. 1991).

[143] *See* Fletcher, *supra* note 21 at 503.

[144] *Id.*

[145] *Id.* at 403.

### *C. Insider Trading*

The SEC, CFTC, and Department of Justice (DoJ) each prohibit insider trading in their respective markets.[146] While there has been scholarly debate about the applicability of insider trading laws to crypto assets,[147] the SEC and DoJ recently clarified their stance when charging Ishan Wahi (a former Coinbase employee) and associates with wire fraud in the first ever crypto asset insider trading case.[148] We focus on the SEC and CFTC's insider trading enforcement, as the analogous criminal law regime is beyond the scope of this paper.

Neither the SEC nor the CFTC's authority to police insider trading comes from a statutory or regulatory prohibition. Rather, each agency views insider trading as a form of fraud and uses their respective anti-fraud provisions to pursue cases of insider trading. That is, insider trading cases brought by the SEC are charged as Rule 10b-5 violations,[149] those brought by the CFTC are charged as Rule 180.1 violations.

Much of the major precedent in the realm of insider trading law comes from securities regulation,[150] simply because SEA s10(b) is the oldest vehicle for pursuing insider trading actions. Notably, the CFTC lacked the authority to bring insider trading actions in commodities markets, with few exceptions,[151] until the

---

[146] See Andrew Verstein, *Crypto Assets and Insider Trading Law's Domain*, 105 IOWA L. REV. 1, 13–17 (2019).

[147] *Compare Id.* (arguing that insider trading law should apply to crypto assets) *with* Mihailis E. Diamantis, *The Light Touch of Caveat Emptor in Crypto's Wild West,* 104 Iowa L. R. 113 (2020) (noting that "there exists a strong argument that insider trading laws would be unconstitutionally void for vagueness as applied to cryptocurrency insiders," and arguing for a light-touch approach to the enforcement of insider trading laws against crypto asset traders).

[148] Press Release, SEC, SEC Charges Former Coinbase Manager, Two Others in Crypto Asset Insider Trading Action (July 21, 2022), https://www.sec.gov/news/press-release/2022-127; Press Release, DoJ U.S. Attn'y's Off. S.D.N.Y, Three Charged In First Ever Cryptocurrency Insider Trading Tipping Scheme (July 21, 2022), https://www.justice.gov/usao-sdny/pr/three-charged-first-ever-cryptocurrency-insider-trading-tipping-scheme.

[149] Some specific insider trading actions can also be brought by the SEC through other provisions of the SEA – like SEA s16 and SEA s14e-3. Yet, the SEC pursues most insider trading cases under SEA s10(b) and Rule 10b-5, because these provisions equip the agency with the broadest authority. *See* Verstein, *supra* note 146 at 14.

[150] *See* Chiarella v. United States, 445 U.S. 222, 234 (1980) (rejecting the notion that the possession of insider information by traders in an open-market creates any general duty absent a specific duty to disclose); Dirks v. SEC, 463 U.S. 646, 661 (1983) (holding that, in cases where an insider does not themselves trade on material nonpublic information, but provides an insider tip to a "tippee" who then trades on the material nonpublic information, the tippee is liable for insider trading only where the insider tipper breached their fiduciary duty to the source of the inside information); United States v. O'Hagan, 521 U.S. 642, 666 (1997) (upholding the misappropriation theory).

[151] The only insider trading prohibition enforced by the CFTC prior to Dodd Frank were those against misuse of information by the CFTC's own staff and employees of the exchanges and self-regulatory organizations overseen by the agency (7 U.S.C. § 13(d) (2008); U.S.C. § 13(e) (2008)).

recent expansion of their anti-manipulation authority following the Dodd Frank amendments to the CEA and passage of Rule 180.1.[152]

Both the SEC and CFTC adopt the *misappropriation* theory of insider trading, under which liability turns on whether "one misappropriates confidential information for securities [or commodities] trading purposes, in breach of a duty owed to the source of the information."[153] This theory finds liability for trading on information learned "in a context that implies confidentiality, even if the trader is not a corporate insider."[154] Likewise, the court in *CFTC v EOX Holdings* – the first insider trading action brought to trial by the CFTC – indicated that the "tipper/tippee" theory of insider trading commonly used in Rule 10b-5 insider trading cases[155] also applies in the context of commodities insider trading.[156]

Accordingly, an important element of any insider trading action is the existence of an adequate "relationship of trust and confidence" owed by the accused to the source of the insider information. The Supreme Court in *Chiarella* held that a "duty to disclose under section 10(b) does not arise from the mere possession of nonpublic market information", but rather arises where "one party has information that the other party is entitled to know because of a *fiduciary or other similar relation of trust and confidence* between them."[157] While most insider trading cases involve a fiduciary relationship possessed by the accused trader or tipper, recent cases have made clear that fiduciary relationships – while sufficient-- are not necessary for there to be a "duty to disclose" that generates insider trading liability.[158] Rather, courts have expressed willingness to find such a duty absent a preexisting fiduciary relationship where other indicators of a "relationship of trust and confidence" exist. The district court in *SEC v. Cuban* found that such a relationship might arise from a private agreement between parties to a transaction which includes an explicit or implicit promise to keep

---

[152] In enacting Rule 180.1, the CFTC "recognize[d] that unlike securities markets, derivatives markets have long operated in a way that allows for market participants to trade on the basis of lawfully obtained material nonpublic information." The agency then stated that the new rule may prohibit "trading on the basis of material nonpublic information in breach of a pre-existing duty". *Supra* note 119 at 41403.

[153] *Id.* at 41402 ; *see also O'Hagan*, 521 U.S. 642; Verstein, *supra* note 146 at 15 ("the misappropriation theory holds that a trader who feigns loyalty to a company or person to gain access to secrets ultimately defrauds his source out of information when he misuses the information for trading").

[154] *Id.*

[155] *See, e.g.,* Dirks v. SEC, 463 U.S. 646 (1983); Salman v. United States, 137 S. Ct. 420, 428 (2016).

[156] CFTC v. EOX Holdings L.L.C., No. H-19-2901, 2021 WL 4482145, at *45 n.112 (S.D. Tex. Sept. 30, 2021).

[157] Chiarella v. United States, 445 U.S. 222, 229 (1980).

[158] SEC v. Dorozhko, 574 F.3d 42, 49 (2nd Cir. 2009) ("[what] is sufficient is not always…necessary, and none of the Supreme Court opinions *require* a fiduciary relationship [for] an actionable securities claim under s10(b)); CFTC v. EOX Holdings LLC, No. 19-cv-02901 (S.D. Tex. Sept. 26, 2019) at *713 (misappropriation theory is not limited to fiduciary relationships).

confidential and abstain from trading on the material nonpublic information.[159] This will become important particularly when it comes to MEV extractors who deal with private order flow (see IV.B).

### *D. Front-running*

In closing, we set aside a source of confusion for crypto markets: "front-running." A familiar critique of MEV techniques like sandwiching (discussed in IV.A-B) is that they involve front-running.[160] This follows a colloquial usage likely derived from Michael Lewis's influential book *Flash Boys*, which referred to a form of High Frequency Trading latency arbitrage (focused on colocation and other speed advantages) as "electronic front-running."[161] However, commentators pointed out that latency arbitrage should not be confused with *illegal* front-running, insofar as high frequency trading involves only public information accessed through superior infrastructure.[162]

In legal contexts, front-running prototypically refers to the illegal practice of a trusted person (usually, a broker or investment advisor) "trading a security, option, or future while in possession of non-public information regarding an imminent block transaction that is likely to affect the price of the stock, option, or future."[163] Neither the SEC nor the CFTC has promulgated any rule generally prohibiting front-running (outside of specific, highly regulated contexts),[164] but

---

[159] SEC v. Cuban, 634 F. Supp. 2d 713, 726 (N.D. Tex., 2009) (holding that a "duty sufficient to support liability under the misappropriation theory can arise *by agreement* absent a preexisting fiduciary or fiduciary-like relationship"), *vacated on other grounds in* SEC v. Cuban, 620 F.3d 551, 559 (5th Cir. 2010).

[160] *See, e.g. Auer,* supra note 11.

[161] Michael Lewis, Flash Boys (2014) ("They created a taxonomy of predatory behavior in the stock market [involving] 'electronic front-running'—seeing an investor trying to do something in one place and racing him to the next").

[162] *See, e.g.,* Merrit B. Fox, Lawrence Glosten, & Gabriel Rauterberg, The New Stock Market: Law, Economics, and Policy 96-99 (noting that "electronic front-running" is different form front-running in its traditional, legal sense, and that the name is "inapt because the HFT is not even accused of taking a position in anticipation of another trader's order," thus suggesting "anticipatory order cancelation" as a more accurate label).

[163] Christopher Gibson, Initial Decision Release No. 1398 (ALJ March 24, 2020) (initial decision), http://www.sechistorical.org/museum /papers/1980/page-14.php (scroll to May 13); *see also* CFTC, 'Front-running', *CFTC Glossary*, https://www.cftc.gov/LearnAndProtect/EducationCenter/CFTCGlossary/glossary_f.html (last visited Jan. 25, 2023) (front-running is the illegal practice of "taking a futures or options position based upon non-public information regarding an impending transaction by another person in the same or related future or option").

[164] Agency prohibitions on front-running exist only in specific contexts. For instance, CFTC Rule 37.203(a) requires Swap Execution Facilities (SEFs) to prohibit abusive trading practices including front-running on their markets. 17 CFR § 37.203 (2013). Similarly, SEC Rule 17(j)-1 has been

instead rely on self-regulatory organizations like FINRA (the Financial Industry Regulatory Authority, Inc.), to establish and front-running prohibitions among member firms.[165] Additionally, the CFTC has recently leveraged its expanded anti-fraud authority to prosecute front-running as a form of insider trading constituting fraud-based manipulation in violation of CEA s6(1) and Rule 180.1.[166] In discussing this issue within securities markets, Professor Jerry Markham noted that insider trading liability is only likely to apply to front-running in limited situations where a clear duty arising from a "fiduciary or comparable relationship with the block trader" exists – for instance, where a stock broker trades ahead of his clients orders.[167]

We will consider below whether MEV techniques involving front-running of these prohibited kinds, focusing especially on the key issue of whether MEV extraction contravenes any special duty (fiduciary or otherwise) that would be breached by front-running. Absent such a special duty, front-running is unlikely to be prohibited.

## IV. LEGALITY OF MEV EXTRACTION

In this section, we apply the law of market manipulation to the facts of MEV extraction and argue that there are numerous forms of liability to be taken seriously in different MEV contexts. Our analysis covers both securities and commodities law.[168] We do not take a position as to whether any specific crypto assets are securities or commodities, but we assume that some assets involved in the types of MEV extraction we discuss are likely to at least be considered commodities (e.g., Ether).

We focus largely on *sandwiching*, given its paradigmatic status in MEV extraction.[169] First, we consider the sandwiching of *public* transactions, focusing primarily on an application of the SEC and CFTC's prohibitions against fraud-based manipulation.[170] We then analyze sandwiching of *private* transactions, drawing out theories of fraud-based manipulation and insider trading liability for privileged actors (block-builders, wallet operators, node operators). We end

interpreted to prohibit portfolio managers from front-running their clients. 17 C.F.R. § 270.17j-I (2005).

[165] *See* FINRA, RULE 5270 (2013). For the early history of efforts to regulate front-running, see Markham, *"Front-Running" - Insider Trading Under the Commodity Exchange Act,* 38 Cath. U. L. Rev. 69, 72-83 (1988).

[166] *See* Order Instituting Proceedings, *In the Matter of* Arya Motazedi, CFTC No. 16-02 (Dec. 2, 2015) (insider trading claim in violation of CEA s6(c)(1) for front-running one's employers).

[167] Markham, *supra* note 113 at 86.

[168] *See supra* Section II.A.

[169] *See supra* definition and description of sandwich trades in Section III.C.

[170] *See supra* discussion of CFTC Rule 180.1 and SEC Rule 10b-5 in Section II.B.

with cases of disruptive schemes like oracle manipulation in which MEV extraction is part of an independently manipulative strategy.[171]

This Section argues that potential liability for MEV extraction abounds, albeit in different ways for different forms of MEV. In Section A, we provide novel arguments for thinking that liability based on public sandwiching plausibly constitutes a manipulative act, although this conclusion requires particular forms of moralized reasoning about market integrity. Still, we think this is unlikely to be pursued as a high regulatory priority in present conditions.

However, as argued in section B, there is a stronger case to be made for thinking liability (particularly insider trading liability) would be found for the sandwiching of *private order flow*. This is because private order flow plausibly involves a position of trust and confidence in relation to the user – if not also (as sometimes may occur) express representations to keep order flow private and to refrain from various forms of MEV extraction including sandwiching. Wallet operators, we will argue, should be particularly careful about legitimate user expectations about transaction privacy and freedom from MEV sandwiching. Finally, in section C, we explain the high risk of legal liability that remains for oracle manipulation (in which benchmarks are manipulated to create deceptive liquidation opportunities), which regulators have recently pursued a flagrant example of in the Mango Markets case.[172]

At bottom, we conclude that MEV extraction can sometimes carry substantial legal risk depending on the type of activity involved and the factors generating relations of trust or heightened duties to other market participants.

### *A. Sandwiching Public Transactions*

Sandwiches are usually referenced as the key example of "toxic" MEV extraction both because they are relatively common and because they adversely affect the sandwiched trade.[173] In this subsection we analyse whether sandwiching of *public* transactions[174] violates anti-manipulation rules under the CEA and the SEA. We consider sandwiching of *non-public* transactions separately in the next subsection.[175]

As discussed above, on our view a pending 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

[171] For a definition of oracles, see *supra* note 25. For in-depth discussions regarding the mechanics of how price oracles can be manipulated in decentralized finance, *see infra* note 284.

[172] *See generally* Complaint, CFTC v. Eisenberg, No. 23-cv-00173 (S.D.N.Y. filed Jan. 9, 2023).
[173] See *supra* our explanation of sandwiches in Section II.E.
[174] *See supra* for our definition of publicness of pending transactions in Section II.D.
[175] *See infra* Section IV.B.

transaction.[176] We also noted that transactions "public" by this standard are only meaningfully public to professional operators, not to an average user.

In what follows, we will argue that there is a plausible case for thinking that sandwich attacks constitute a manipulative act within the meaning of the CFTC Rule 180.1(a)(3) or SEC Rule 10b-5 – at least if courts or regulators were to adopt a moralized form of inquiry focused on protecting particular (if widespread) notions of fairness in financial markets, which of course is a big if. Should courts decide to crack down on the exploitation of privileged positions of control of the machinery involved in processing transactions on Ethereum (*i.e.,* control over "blockspace") in order to extract rents, the courts could determine that execution prices in sandwiched trades have been subject to an illegitimate and therefore artificial price effect, amounting to a manipulative practice. Nonetheless, we argue that this conduct, to the extent it constitutes a form of naked open market manipulation (not covered by an agreement or other relationship), is unlikely to rise to the top of the list of the regulatory agencies' enforcement priorities. Our focus here, nonetheless, is on the theoretical case, as much can be learned about the legally salient features of this paradigmatic form of MEV extraction.

1. Price Manipulation

Although we will focus on the SEC and CFTC's fraud-based manipulation prohibitions, we start by applying the agencies' largely dormant price manipulation prohibitions to the sandwiching of public transactions, if only to demonstrate why we do not discuss this cause of action further. Recall that a successful claim for price manipulation requires proof of four elements: i) an artificial price, ii) the intent to cause that artificial price, iii) having the ability to cause the artificial price (typically through market dominance), and iv) actually causing the artificial price.[177] Yet, the evidentiary burdens of proving both specific intent and price artificiality have posed too high a bar for both the SEC and CFTC to experience much luck in enforcing their anti-price manipulation authorities. One scholar notes the cause of action has become "virtually unprosecutable":[178]

> Plaintiffs must establish a manipulative intent that is conceptually and doctrinally among the most demanding mental state requirements anywhere in financial law. Moreover, the evidence for such intent is typically only highly ambiguous public behavior.[179]

In a sandwich targeting public transactions, the sandwicher's actions – that is, the *front-run* and *back-run* of the sandwiched transaction – are open-market transactions. In other words, they involve the "transacting party simply

[176] *See supra* II.D.

[177] *See supra* discussion of price manipulation Section III.B.

[178] Markham, *supra* note 113.

[179] Abrantes-Metz, *supra* note 113 at 359.

purchasing or selling securities in the open market without any prior arrangement with the counterparty."[180] More specifically, sandwiching involves *naked* open-market trades because a sandwicher profits through their "buy-low, sell-high" scheme with respect to a pair of crypto assets, rather than the price impact of their transactions on an external interest.[181] According to Professor Fletcher, pursuing open-market manipulation claims under the current price manipulation standard is rarely, if ever, done because price manipulation generally requires a showing of market power or dominance.[182] In naked open-market trading, on the other hand, prices are affected through ordinary trading activity between anonymous counterparties who need not dominate or control a given market.[183] Given the challenges of establishing the elements of price manipulation, it is unlikely that a court would hold a sandwich to constitute price manipulation if no independent evidence of the sandwicher's market dominance existed. Therefore, we turn instead to sandwiching under the law of fraud-based manipulation, which is more interesting in the present context. In so doing, we will come back to the question of what is an "artificial price," as the related question of whether a price is artificially *affected* is also crucial for fraud-based manipulation.

2. Fraud-Based Manipulation

7 U.S.C. § 9(1) prohibits any person to "use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity…any manipulative or deceptive device or contrivance," in contravention of CFTC Rules. The CFTC clarified this prohibition with its Rule 180.1, which mirrors the content of SEC rule 10b-5 (prohibiting securities fraud).[184] Rule 180.1, like SEC 10b-5, makes it unlawful for those engaged in commodities trades to "to intentionally or recklessly":

> (1) Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;
>
> (2) Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact…;
>
> (3) Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person[.][185]

---

[180] Michael A. Asaro, *'Masri' and Open-market Manipulation Schemes*, 239 N.Y. L. J., May 12, 2008, https://www.akingump.com/a/web/1243/aogHP/07005080021aking.pdf (Akin Gump reprint).

[181] *See supra* discussion of covered and naked open-market manipulation in Section II.C.

[182] *See* Fletcher, *supra* note 21 at 539–540.

[183] *See Id.* at 533.

[184] In promulgating Rule 180.1 which accompanies section 6(c)(1), the CFTC stated that "the Commission deems it appropriate and in the public interest to model final Rule 180.1 on SEC Rule 10b-5." *See supra* note 119 at 41399.

[185] 17 CFR § 180.1; 17 CFR § 240.10b-5.

Violating Rule 180.1 requires only reckless action, which is defined for CEA purposes as "one that departs so far from the standards of ordinary care that it is very difficult to believe the [actor] was not aware of what he was doing."[186] This means "the Commission need not prove that the defendant's…primary motive was to interfere with the forces of supply and demand."[187]

Our analysis will focus on liability for manipulative devices or acts under (a)(1) and (a)(3), and analogous provisions of SEC Rule 10b-5, as it is unlikely that sandwiching public transactions will involve untrue or misleading statements such as under 180.1(a)(2). By itself, sandwiching does not clearly involve an express false statement. Searchers typically do not make any representations to the public or to specific traders. Matters might be different, of course, if some actors who facilitate sandwiching were to make express representations that they know to be falsehoods. For example, a block builder could publicly promise not to engage in sandwiching (e.g., by including their own front- and back-running transactions), but then break that promise. Similarly, there may be a risk of liability if a relay operator or a block builder promised to "try its best" not to include transactions attempting to sandwich but then either (1) they did not try or (2) their efforts were manifestly below the reasonable level under the circumstances.[188]

Instead, our focus will be the idea that a standard sandwich involves prohibited manipulation: either a "manipulative device," CFTC 180.1(a)(1) and SEC 10b-5(a), or an act that "would operate as a fraud or deceit," CFTC 180.1(a)(3) and SEC 10b-5(c).[189] That is, we will explore the manipulation-as-fraud theory, which maintains that:

> [W]hen 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."[190]

---

[186] *Drexel Burnham Lambert Inc. v. CFTC*, 850 F.2d 742, 748 (D.C. Cir. 1988).

[187] *In the Matter of JPMorgan Chase Bank*, 2013 WL 6057042, at *11 ("even if a trader were motivated by a desire to obtain compensation rather than by a desire to affect a market price, if the trader recklessly effected the manipulative trades, he will be held liable").

[188] As will be discussed in section B, liability based on express misrepresentations may also arise in private order flow arrangements where users are promised that their transactions will not be sandwiched as an inducement to receive exclusive access to their order flow, but where the promise is broken. Still, this is not the case we are concerned with here, namely sandwiching public transactions.

[189] It's arguable that some of the manipulative acts in question here could be recast as deceptive omissions in contravention of 180.1(a)(2). For example, one might maintain that the failure to disclose a potentially manipulative act is itself a deceptive omission for (a)(2) purposes. However, this makes the omission theory of liability parasitic on the theory of manipulative act, which is more fundamental. Therefore, we set aside this conceptual possibility as it is not especially important in practice. For clarity, we focus chiefly on manipulative acts.

[190] Scopino, *supra* note 122 at 673.

For example, this covers deceptive trading practices such as "banging the close" – executing many trades at the end of the trading day e.g. to give a false impression of high trading volume.[191] Even though such practices do not involve affirmative false statements, they count as fraud because they "artificially affect the price of securities without informing other market participants, who justifiably rely on the assumption that the market for those securities is functioning normally and not being manipulated."[192] (This theory of liability is similar in spirit to a "fraud on the market" theory, applicable in other contexts.[193])

As the Second Circuit explained the securities context, a manipulative act "'refers generally to practices…that are intended to mislead investors by artificially affecting market activity,' and 'connotes intentional or willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities.'"[194] For assessing manipulation, "[t]he critical question then becomes what activity 'artificially' affects a security's price in a deceptive manner."[195]

There are several theories for why sandwiching might contravene CFTC Rule 180.1 or SEC 10b-5 that are worth exploring – the most plausible of which, we argue, is that it involves manipulation through having an artificial impact on prices. But first, let's focus on deception. Is sandwiching an act or business practice that "would operate as a fraud or deceit" under 180.1(a)(3) and 10b-5(c)? Sandwiching might be seen as fraudulent if it misleads either the sandwiched user or the market generally. We consider each in turn.

(i) First simple theory: the sandwiched user is at least recklessly misled

First, one might ask whether sandwiching is likely to involve knowingly or at least recklessly misleading the sandwiched user herself. The idea would be

---

[191] *CFTC v. Amaranth Advisors*, L.L.C., 554 F. Supp. 2d 523, 528 (S.D.N.Y. 2008) ("purchasing a substantial number of futures contracts leading up to the closing range on expiration day, followed by the sale of those contracts several minutes before the close of trading[] is known as "[banging]the close"); *id*. at 534 ("there is no doubt that [banging] the close or any other trading practices, without an allegation of fraudulent conduct, can also constitute manipulation in contravention of the CEA, so long as they are pursued with a manipulative intent").

[192] Scopino, *supra* note 122 at 674. *See also* GREGORY SCOPINO, ALGO BOTS AND THE LAW: TECHNOLOGY, AUTOMATION, AND THE REGULATION OF FUTURES AND OTHER DERIVATIVES 307–312 (2020).

[193] *Halliburton Co. v. Erica P. John Fund, Inc*., 573 U.S. 258, 268 (2014) (upholding "fraud on the market" presumption, under which "the market price of shares traded on well-developed markets reflects all publicly available information, and, hence, any material misrepresentations," and as a result "the typical 'investor who buys or sells stock at the price set by the market does so in reliance on the integrity of that price'"; therefore, "whenever the investor buys or sells stock at the market price, his 'reliance on any public material misrepresentations ... may be presumed for purposes of a Rule 10b–5 action.'").

[194] Set Capital LLC v. Credit Suisse Grp. AG, 996 F.3d 64, 76 (2d Cir. 2021).

[195] ATSI Communications, Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 100 (2d Cir. 2007).

that when a searcher sandwiches another user, the first trade within the sandwich (which front-runs the original user) affects the natural price of the underlying crypto asset.[196] Specifically, it worsens the sandwiched user's execution price – and a competent searcher will inevitably be aware of this effect, since it is integral to making the sandwich more profitable. For example, if it is a buy order being sandwiched, the front-run will slightly raise the asset's price before building the original buy order into the relevant block, and so the sandwiched user purchases the asset at a slightly higher price than she otherwise would have. Trades on DEX-es like Uniswap V2 are only executed if the execution price is within the specified slippage limit, as competent sandwichers will be aware. One might think that because the searcher fails to disclose this practice *to the sandwiched user*, thereby harming her by increasing the slippage of her trade, this involves at least recklessness (awareness of a substantial risk) as to interfering with the original user's justifiable reliance on the integrity of the market, *i.e*. the reasonable assumption that prices accurately reflect only the forces of supply and demand.

Setting aside whether sandwiching has an artificial effect on prices (which we consider in a moment), we think this simple theory of liability is unlikely to succeed, since we doubt the sandwiched user is likely to be misled by the sandwicher. This means recklessness by the sandwicher is unlikely to exist.[197] There are two reasons to expect that the sandwiched user will not be misled by the sandwicher's conduct. First, sandwiching and other MEV extraction strategies generally are common on Ethereum at present, and so it is arguable that users may reasonably be expected to know that being sandwiched is a substantial risk for any trade she executes, given how the relevant markets work.[198] However, as Wang et al have shown based on their interviews of DeFi users, not all users potentially affected by sandwiches are aware of the phenomenon of sandwiching, and some users who are aware of sandwiching are not able to recognize whether their transaction has been sandwiched.[199] That said, the authors also noted that "[w]hen the financial loss from a sandwich attack is not significant, traders do not care whether they are being attacked."[200]

---

[196] Depending on the size of the searcher's purchase order as well as other conditions (amount of liquidity in the liquidity pool, details of the algorithm with which the AMM calculates prices), the price impact may vary: from very small, likely imperceptible for the sandwiched user, to very large. Thus, it could be that appreciable harm to the sandwiched user happens only in some, but not all, sandwiches. *See supra* II.C.

[197] *Drexel Burnham Lambert Inc. v. CFTC*, 850 F.2d 742, 748 (D.C. Cir. 1988) (observing that recklessness is made out in the CEA context when "it is very difficult to believe the [actor] was not aware of what he was doing" – i.e. when there is an obvious risk).

[198] See *supra* Section II.

[199] Over the second half of 2021, Wang et al conducted interviews with 15 DeFi users; Ye Wang et al., *Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem*, *in* Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (2022) at 6-12, https://doi.org/10.1145/3491102.3517585.

[200] *Id.* at 8.

It is likely that traders whose trading volume is large enough for sandwiching to become noticeable are also more likely to be aware of sandwiching. Thus, because sandwiching is likely common knowledge among those traders who are potentially meaningfully affected by sandwiching, it seems not very likely to interfere with users' expectations of what is likely to happen in the market.[201]

Second, and more importantly, in each trade that is carried out on a DEX like Uniswap, users are alerted to the prospect of their transaction executing at a price significantly different from the currently estimated price because they are asked to specify a slippage limit beyond which their trade will not be executed (a slippage limit may also be suggested by default). We shall assume that the sandwicher only worsens the sandwiched user's execution price without preventing the underlying trade from being executed altogether. This could happen if the front-run moves the price to a level beyond the target transaction's slippage limit, but a sandwicher rationally would not want to cause that, since this means he or she will not profit from the sandwich. Assuming the sandwiched trade goes through despite the increased slippage from the front-run in the sandwich, the sandwiched user arguably will have consented to the trade being processed with this worse but still acceptable execution price. In this way, because users are alerted to the prospect of slippage particularly through the need to set a slippage limit on their trades, the sandwich is unlikely to mislead or deceive sandwiched users in fact. As a result, it is unlikely that a sandwicher would be found to have the mental state of recklessness as to the prospect of misleading the sandwiched user.

(ii) Second simple theory: the market is at least recklessly misled

If the sandwiched user (or users) in the particular case will be unlikely to be seen as being misled by the conduct of the sandwicher, then might other market participants end up being at least recklessly misled by this conduct? For this to be the case, (1) a sandwich would need to have an adverse effect on non-sandwiched traders, (2) those affected traders would need to be misled in some way, *e.g.*, as to the true price of the relevant assets, and (3) the sandwicher would need to be reckless as to the prospect of misleading others. However, we'll argue that in standard, economically rational sandwiches we would expect no adverse price effect on the wider market, which negates the prospect of other (non-sandwiched) users being misled as to true price as well as the sandwicher's recklessness as to the risk thereof. Let us examine why economically rational sandwiches are not likely to involve a price effect outside of the sandwiched user, i.e. on the market more broadly.

*"Standard" sandwiching.* By a standard sandwich we mean a sandwich where the back-run transaction completely reverses the front-run transaction. In

[201] This is not to say that users have *normatively positive* attitudes towards sandwiching, but only that it is a risk known to them. As Wang et al noted, some of their "interviewees identified sandwich attacks as malicious towards traders"; *id.* at 9.

other words, if the front-run is a purchase of 1,000 DAI for 1 ETH, then a standard back-run would sell 1,000 DAI. Qin et al. operationalized this intuition with a notion of "perfect" sandwiching.[202] The authors found that 80% of sandwiches in their sample were "perfect," and 100% would count as "perfect" on a definition using a wider 90-110% range.[203]

A sandwicher maximizes their economic return from a sandwich by completely reversing the front-run transaction.[204] In fact, if sandwiching is the sandwicher's only goal, there is no economic reason for them to do anything other than strive for a full reversal of their position. If a sandwicher does not manage fully to reverse their position before any other market activity occurs, then their strategy is not entirely market neutral and they take a kind of "inventory" risk, because it is possible that the price will later move in a way that reduces the profitability of their sandwich.

*Atomic way of executing sandwiches*. If a sandwich is executed *atomically*, the MEV extractor is guaranteed that all the transactions they submit will be executed in the precise set order or none of the transactions will be executed at all. Atomicity may be guaranteed if the MEV extractor controls block production (because they are a validator or non-validating block builder) or if the MEV extractor uses a private relay accepting atomic bundles of transactions (like the Flashbots Auction). This method of sandwiching is much less financially risky than non-atomistic approaches, where there is a risk of other users' transactions being included between the front-run, the sandwiched trade(s), and the back-run. When an actor controls the contents of a block and can order the transactions in the "perfect" manner that fully reverses the front run, this will eliminate the risk that others might profit from carrying out an interfering trade before the MEV extractor has realized her profit through the back-run. As a result, atomistic sandwiches are preferred by MEV extractors compared to non-atomistic alternatives, which are riskier in financial terms. We do not know precisely what proportion of sandwiches use the less risky atomistic method today. As measured by Qin et al., from late 2018 to late 2021, 32% of sandwiches were privately relayed to miners or added by miners themselves, which strongly suggests that those MEV extractors had guarantees of atomicity.[205] Unsurprisingly, nearly all the privately relayed sandwiches had *zero* intermediate, unrelated transactions (submitted by other users) between the front-run, the sandwiched trade, and the back-run.[206]

*Most sandwiches don't affect non-sandwiched trades*. However, even when – for any reason – sandwichers cannot rely on a guarantee of atomicity, they seem mostly to succeed in executing the strategy without having any intermediate, unrelated transactions "within" a sandwich. Taking all sandwiches

---

[202] Qin, *supra* note 49.
[203] *Id.*
[204] *Id.*
[205] Qin, Zhou, and Gervais, *supra* note 49 at 4.
[206] *Id.* at 5.

in the Qin et al. study, both privately relayed and not, *most* of them had no intermediate transactions.[207]

*Impossibility of adverse price effect on non-sandwiched traders*. Even if most sandwiches do not include intermediary non-sandwiched transactions, a non-trivial proportion of sandwiches still might. It is possible that some affected transactions in this minority group are transactions interacting with the same DEX, which means that these non-sandwiched trades would be affected by the sandwich. This involves two possibilities: either a) these other trades go in the same direction as the sandwich's front-run (buy/sell) or b) they go in the opposite direction.

a) If those trades are in the *same* direction as the sandwich's front-run, then they are *effectively sandwiched* even if that was not intended by the sandwicher. It will be so, because same-direction trades following a front-run receive worse price execution than they would have otherwise in the absence of the front-run. This situation persists until someone (the sandwicher – in their back-run – or someone else, likely an arbitrageur) will execute an opposite-direction trade. In those cases, our discussion from the previous subsection applies. There we found there was no risk of misleading sandwiched users themselves, as they are likely to be aware of the risk of sandwiches hurting their execution price through setting their slippage tolerance. Still, as discussed in the next section, it's conceivable that courts might find such users to have been affected by an artificial price to the extent sandwiching is deemed to have an unnatural impact on price. Hence, the situation for such users remains complex and we defer the conclusion as to this situation until the next sub-section.

b) On the other hand, if the intermediate trades are in the *opposite* direction than the front-run, then they *benefit* from the front-run's price effect. The front-run's price effect allows the opposite-direction trade to sell higher (or buy lower) than they otherwise would have. Moreover, those intermediate opposite-direction trades reduce the profitability of the sandwich. This is the reason why an economically rational sandwicher strives to reverse their position before anyone else does that. Thus, crucially, non-sandwiched users are not adversely affected. And if they are not adversely affected – in fact, they benefit – then it would be unlikely that they would be deemed to have been recklessly misled by the sandwicher. As a result, a successful cause of action for fraud-based manipulation likely could not be brought against the sandwicher on this theory.

By contrast, if a sandwicher – besides their aim to sandwich – also intends to take a longer-lasting position in the market (and thus intentionally does not fully reverse the front-run), then there would be little to doubt that the sandwicher's lasting market position is a legitimate trade, just with the use of a front-running transaction (akin to arbitrage with the use of front-running[208]). Of course, if this lasting market position is part of a manipulative scheme, then that

---

[207] *Id.*

[208] *See infra* Section IV.D.

scheme is of a different nature than a sandwich and would require separate analysis.

For the above reasons, significant challenges exist for a claim for fraud-based manipulation based on the sandwicher recklessly misleading non-sandwiched users as to true price. To recap, either the sandwich is economically optimal (what an economically rational sandwicher would prefer) or it is not. If it is, *i.e.,* the back-run fully reverses the price effect of the front-run, then the wider market of non-sandwiched users will not be detrimentally affected and so they'll face no risk of being misled as to true price. Thus, the sandwicher's recklessness as to misleading others will not be made out either. By contrast, if it is a non-economically optimal sandwich, then there could be a price effect on non-sandwiched users. If this price effect is beneficial, no claim of being misled is likely to be successful. But if the price effect is harmful, they will count as being effectively sandwiched themselves. It is possible they might count as having been misled, however, insofar as courts deem sandwiching to have an artificial price effect, as we discuss in the next sub-section.

The upshot is that liability for non-economically rational sandwiching is likely to depend on the final theory of liability for all sandwiching, which is that sandwiching entails an artificial price effect. So it is to this theory we now turn.

#### (iii) More sophisticated theory: artificial effect on prices created at least recklessly

This suggests that the most likely way in which a sandwich strategy – for both "standard" sandwiches (economically optimal) or non-standard ones – could generate liability under Rule 180.1 is this: it could be found to constitute manipulation via at least recklessly affecting the price for the asset at issue in the sandwiched user's trade in an *artificial* manner. The Second Circuit clarified that, in determining what constitutes a manipulative act, "[f]or market activity to 'artificially' affect a security's price, we generally ask whether the transaction or series of transactions 'sends a false pricing signal to the market' or otherwise distorts estimates of the 'underlying economic value' of the securities traded."[209]

The most obvious implication of a sandwich front-run is the worse execution price received by the sandwiched user. Yet, this alone is by no means indicative of whether the practice is "artificial" – trading in traditional financial markets is characterized by zero-sum games in which one trader's gain is another trader's loss.[210] Rather, courts generally define an artificial price as a price which "does not reflect basic forces of supply and demand."[211] The court in *CFTC v. Cox* held that a price is considered artificial where it is "affected by a factor

[209] Set Capital LLC v. Credit Suisse Grp. AG, 996 F.3d 64, 79 (2d Cir. 2021).

[210] What is a zero-sum game between the two directly involved traders may at the same time be positive-sum for the market (or more broadly: from the perspective of social welfare), *e.g.,* by contributing to effective price discovery.

[211] Cargill, Inc. v. Hardin, Secretary of Agriculture, 452 F.2d 1154, 1163 (8th Cir. 1971).

which is not legitimate."[212] Yet, no binding tests exists for determining which forces or factors informing a price are legitimate and which are not.[213]

This suggests that in considering whether sandwiches create artificial prices, or have an artificial price effect, it is conceivable that courts or regulators might draw on background moral assumptions in order to decide whether the prices obtained by sandwiched users – although technically consented to by way of the user's preselected slippage limit – reflect only the forces of supply and demand or rather are artificial prices because they are influenced by a force that is not legitimate. This would be an instance of an approach to conceptualizing market manipulation which gives pride of place to moral criticisms. As Fox et al put it, in such cases "the normative criticism of the relevant conduct is doing all the work in identifying exactly what kind of behavior is supposed to be prohibited."[214]

To take one example of how such moralized reasoning could play out, the court in *Set Capital* found that plaintiffs had adequately alleged that the defendant bank (an issuer and seller of the relevant securities) had "knowingly or recklessly exacerbated [a] liquidity squeeze" in futures market through its trading behavior, which it knew would affect prices of certain derivatives that its hedge positions depended on, and the court further held that this was enough to constitute evidence of "conscious misbehavior or recklessness," as required for a finding of "manipulative intent."[215] Thus, the court reasoned, in effect, that the defendant bank's actions had an illegitimate price effect because they "exacerbated" a liquidity squeeze, which falls on the wrong side of the distinction between *creating* a liquidity disturbance for one's own benefit and merely taking advantage of such a disturbance that already existed. Professor Stuart Green argues that this distinction between creating a disturbance versus merely taking advantage of one that already exists is key to separating unfair or illegitimate trading practices from those that do not violate norms of fair play.[216]

Although it is not certain a court or regulators will approach the inquiry by applying this sort of moralized reasoning about legitimate versus illegitimate price factors, it is conceivable that decisionmakers might take the sandwicher's

---

[212] *In re Cox,* [1986-1987 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 23,786 at 26,060 (CFTC July 15, 1987).

[213] In re Indiana Farm Bureau Coop. Ass'n, Inc., [1982-1984 Transfer Binder] Comm. Fut. L. Rep. (CCH) 21,796, at 80-81,281(CFTC Dec. 17, 1982)(Johnson, C., concurring) ("Legitimacy with respect to supply and demand is undefined in law and economics, unless the sole question is whether the forces were put in motion by an illegal act").

[214] FOX, GLOSTEN, AND RAUTERBERG, *supra* note 21 at 339 n.10.

[215] Set Capital LLC v. Credit Suisse Grp. AG, 996 F.3d 64, 79 (2d Cir. 2021).

[216] STUART P. GREEN, LYING, CHEATING, AND STEALING: A MORAL THEORY OF WHITE COLLAR CRIME 242 (2006) (discussing, in the insider trading context, "[t]he distinction between creating an unfair informational disparity and exploiting an informational disparity that already exists. (…) The disclose or abstain rule should be construed so as not to apply to cases in which an investor comes across non-public information fortuitously (say by overhearing it in an elevator or on the train)").

impact on the execution price of the sandwiched trade to be an illegitimate one in cases where the *privileged position of the block producer* is relied on for sandwiching and thus amounts to exploiting a key part of the financial infrastructure on Ethereum to gain an advantage over other traders. Note the following argument applies only to sandwiching that relies on control of block production, which is one central case of sandwiching – although not the only one (*i.e.,* it may not apply to, likely rare, cases of non-competitive sandwiching[217]). To make out the argument for thinking that sandwiching involves artificiality affecting prices amounting to manipulation, let us review how sandwiching can rely on control of block production. Then we explain how this might be seen as improperly exploiting access to the basic machinery of the financial ecosystem on Ethereum.

*Sandwiching relying on control of block production.* Sandwiching is often conducted by leveraging control over block production. A proposer-validator who does not rely on an external block-builder has full control over which transactions to include in a block and in what order, and she can thus order available pending transactions in a way that creates profitable (to her) sandwiches, arbitrage, and so on. Given that the proposer has this control over one piece of "blockspace," they can allow others to extract valuable opportunities that can be realized in their block, just like a landowner can let others use their land and in return for rent. And like ground rent, the rent that can be extracted by the proposer will, in a competitive environment of value extraction, tend towards the total value extractable from the space they control.

Three types of players currently compete to extract value from blocks by leveraging the proposer's power to control a piece of blockspace, while directly or indirectly paying a rent to the proposer: relay operators, block-builders, and other MEV searchers. A block-builder can use the same strategies as a proposer when constructing a draft block (adding their own transactions, choosing and ordering other users' transactions), but for their block to be chosen by a proposer and included on the blockchain, they need to compete with other block-builders in an auction and offer the highest fee (rent) to a relay. In turn, relays compete in a rent auction for their block to be chosen by the proposer. Other users who aim to extract MEV, *i.e.* searchers, do not attempt to construct whole blocks, but some block-builders allow them privately to submit bundles of transactions realizing valuable opportunities. Searchers compete against other searchers, and presumably against the builders' own value extraction efforts, to have their value-extracting transactions included on the blockchain.

An argument could be made that searchers may be able to extract value, *e.g.*, by sandwiching, without leveraging the proposer's control of blockspace, at least in the *overt* sense discussed above. If a profitable opportunity is not competitive (no other searchers, block-builders are attempting to realize it), then a searcher may be able to realize the opportunity simply by setting higher/lower

[217] *See infra* market power (dominance) argument in this subsection.

gas settings for their transactions, to place them in front or behind some target transaction, as needed. Such a searcher still pays a rent to the proposer (in the form of the "tip" part of a transaction fee), but the rent may not be proportionate to the value of the profitable opportunity. Instead, the rent is based the transaction fee set by the target transaction (*e.g.,* the transaction to be sandwiched). However, this is unlikely to be significant as profitable opportunities – especially for sandwiching – tend to be competitive. This competition may take place through the auction process described above or through so-called priority gas auctions.[218] In both cases, the proposer's rent will tend toward the total value of the opportunity (although more efficiently in overt auctions than in priority gas auctions). (Note that validators-proposers in principle could attempt to avoid participating in, or facilitating, MEV extraction.[219]

*Illegitimacy of relying on control of block production for sandwiching.* It could be argued that, insofar as sandwiching leverages control over blockspace as described above, one might see the validator-proposer's involvement in sandwiches as exploiting a key part of the financial infrastructure on Ethereum to give some market participants an advantage that others. In this way, their position as being in charge of the machinery of processing transactions gives validators an unfair advantage, which users generally do not and cannot have unless they too become validators in charge of building blocks. We propose that there are two main ways in which courts and regulators engaged in a moralized form of inquiry to determine where manipulation exists might deem the exploitation of one's control over blockspace through sandwiching to constitute an illegitimate price factor, thus artificially affecting prices. One builds on intuitions about market power (or dominance), while the other flows from intuitions about conflicts of interest.[220]

*Market power (dominance) argument.* First, one might see facilitation of sandwiching by validator-proposers as exploitation of a key position of (temporary) monopoly power within the machinery of processing transactions, giving those exploiting the power an unfair vantage point in the ecosystem from which to extract rents for themselves. While it's true that anyone could in principle become a validator (just as anyone could in theory become a landlord who charges rents), this doesn't change the fact that validators engaged in sandwiching exploit their privileged position within the ecosystem/infrastructure of the financial structure. Given that *market power* or

---

[218] Daian, *supra* note 9.

[219] For example, a validator could order transactions randomly or on a "first-observed, first-included" basis, but while this is likely to reduce her profits, it is unlikely to reduce the amount of competition for blockspace and push it into a different stage of the supply chain, causing issues like latency races or spam.

[220] Note that if a proposer could be liable under this theory, then arguably those who leverage the proposer's power in cooperation with the proposer (relays, block-builders, searchers) for sandwiching, may also be liable.

*dominance* often plays a major role in courts' price artificiality analysis,[221] it seems plausible that a court could determine that sandwiching that overtly leverages the proposer's power to control a piece of blockspace, thus amounts an illegitimate and artificial force on market prices. Competent sandwichers will be aware of these facts, and so there is at least a colorable argument that they would be at least recklessly creating an artificial price, i.e. aware of at least a substantial risk that their activities produce prices that do not reflect solely the legitimate forces of supply and demand.

*Conflict of interest argument.* A second way to draw out the intuition that there is something unfair or illegitimate about the way in which sandwichers use the proposer's power to control a piece of blockspace to give themselves special advantages is to note that the situation presents something in the vicinity of a conflict of interest. After all, in such a situation, a proposer does not act only as neutral infrastructure, on whose services all traders rely and cannot trade without, but also as a self-interested trader or a profit-sharing enabler of other traders, leveraging a privileged position over other user's transactions.

For either reason, a morally-minded court or regulator might see sandwiching as creating an artificial price for the users they sandwich under circumstances where "it is very difficult to believe the [sandwicher] was not aware of what he was doing."[222] In other words, the impact that a sandwicher knows he will have on the execution price of the sandwiched user's trade might well be seen as an illegitimate one for either of the two reasons offered above. If so, there is a route to seeing the sandwich as at least recklessly sending a false price signal, *i.e.*, creating an artificial effect on a price, thereby amounting to manipulative act. It would admittedly be a very common form of manipulation within the ecosystem, but manipulative and unfair nonetheless – at least by this reasoning. In this way, a Rule 180.1(1) or (3) violation might be in play.[223]

Note that there are other arguments one might adduce in this context, such as that MEV amounts to an illegitimate form of queue-jumping, but we think this argument clearly fails as there is no first-in-time queue in the Ethereum context in which to jump.[224] Hence the market control (domination) and conflict

---

[221] *See supra* note 104.

[222] *Drexel Burnham Lambert Inc. v. CFTC*, 850 F.2d 742, 748 (D.C. Cir. 1988).

[223] To be clear, this theory of liability does not hinge on "untrue of misleading statements" by any participants of the MEV extraction ecosystem. If a validator, block-builder, or a relay operator, publicly promise not to sandwich or not to include sandwiching transactions in blocks they control, and they break that promise, that could be a separate ground of liability, as discussed above.

[224] While it might be tempting at first blush to regard MEV front-running as a form of illegitimate or immoral queue-jumping, this, we think, would be a clear mistake. The reason is that before the relevant transactions are selected and ordered by a validator in order to become one block, there *is* no pre-existing transaction ordering which could allow the sandwiched user to claim that the sandwicher cut in line in front of them. That is, transaction order in this context is not established through a *first in time* rule, but rather through the auction process, whereby higher bids lead to greater prospects of having one's transactions executed earlier. This was by design, as a first in

of intuitions provide the strongest basis for the manipulation argument in the present context.

(iv) Rejoinders

Let us close this section by considering some rejoinders. First, and most fundamentally, courts and regulators might eschew the form of moralized inquiry outlined above in their approach to determining what constitutes prohibited manipulation. Thus, they might instead prefer to take an empirical look at what behaviors produce efficient markets in traditional economic terms in order to decide what behaviors should be deemed manipulative.[225]

However as argued earlier,[226] much more empirical work is needed to determine the extent to which MEV sandwiching is a behavior with net positive effects for the ecosystem construed in the aggregate. Hence, the liability outcome on this approach remains uncertain.

The second sort of rejoinder one might raise would arise within the moralized inquiry we gestured at above and argue that the domination and conflict of interest arguments sketched a moment ago are not decisive because of other conflicting normative principles. Let us consider a few of these, though we do not propose to resolve the matter conclusively.

First, then, one might respond that the price impact of a sandwich is quite similar to Uber's 'surge pricing' model, wherein Uber's pricing model algorithmically increases prices at times where potential Uber customers may be willing to pay more.[227] So, to the extent that a sandwicher changes the execution price of a sandwiched user's transaction through their front-run, they do so solely on the basis of a user's publicly expressed price preferences (i.e. their slippage limit), rather than any false or deceptive information. Nonetheless, one might see a difference between price effects due to sandwiching and the Uber surge pricing model. Surge pricing benefits are meant to be redistributed to drivers to ensure there is enough driver supply to meet rider demand.[228] In the

time rule for transaction ordering would have invited the sort of race to be first that one sees in latency arbitrage from high frequency traders. Accordingly, given the current architecture for transaction ordering through auctions, there is no plausible argument that the sandwicher's front-run is unfair or sends an illegitimate price signal due to "cutting in line" in front of the sandwiched user's trade.

[225] Many scholars have advocated for such an approach. *See, e.g.,* Pirrong*,* supr*a* note 88 (arguing for an approach to manipulation determinations which focuses on the economic effects of market manipulation and statistical analysis); Abrentez-Metz, *supra* note 113 at Part III (proposing the use of empirical economic and statistical tools, such as econometric screens, in the evaluation of manipulation claims, particularly at the pleading stage).

[226] *See also* Barczentewicz, *supra* note 18.

[227] Brett Helling, *Surge Pricing: What It Is & How It Works For Riders & Drivers*, Ridester (Jan. 13th 2023) (https://www.ridester.com/surge-pricing/).

[228] *Id*. ("Making sure riders can always find rides when they need them is one of the main reasons Uber implemented surge pricing.").

sandwiching case, the extra profit generated in the sandwich is shared among those involved in sandwiching (searcher, block-builder, relay, proposer-validator), with the most value like to go to the proposer, *i.e.*, the actor who controls a key piece of financial infrastructure and extracts rents for themselves through it. On one view, that would be as if Uber raised prices in times of great rider demand such as a natural disaster or other crisis solely because the market would bear it – arguably a form of price gouging.[229] Outside of disaster situations, however, one might argue that even if all the monetary value from competition for space (cars) accrues to Uber or to sandwichers, users may derive a significant non-monetary benefit in being able to express the strength of their preference for the use of space and thus have their preferences satisfied according to their strength. Of course, this in turn raises questions about the accuracy of willingness-to-pay as a proxy for well-being effects, particularly for actors with limited ability to pay.[230] But the point is that one might bring duelling normative principles to bear in order to debate the legitimacy of the relevant form of rent extraction.

Second, and more importantly, one might counter the domination and conflict of interest arguments we introduced above by contending that the profit motive with which MEV sandwiching is pursued provides a legitimate economic rationale for sandwiching by those who control the construction of blocks. As some courts have maintained, trading with the purpose of receiving the best possible price for oneself is a "legitimate economic rationale," even where it detrimentally impacts another trader.[231] Still, it is clear that this principle must have limits, as any paradigmatically manipulative trading strategy like spoofing[232] or banging the close[233] is also pursued primarily from a profit

---

[229] Ryan Lawler, *Uber Caps Surge Pricing During Emergencies Nationwide* (Jul 8th 2014) (https://techcrunch.com/2014/07/08/uber-caps-surge-pricing-during-emergencies/) (noting that Uber agreed with the Attorney General of New York to avoid such practices).

[230] Ronald Dworkin, *Is Wealth a Value?* 9 J. Legal Studies 191-226 (1980) (arguing that wealth understood in willingness to pay terms is normatively problematic, particularly when considering differences in ability to pay prevents the accurate expression of one's actual preferences – particularly as between rich and poor).

[231] *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 535 (S.D.N.Y. 2008); *In re* Indiana Farm Bureau Coop. Ass'n, Inc., [1982-1984 Transfer Binder] Comm. Fut. L. Rep. (CCH) 21,796, at 24,281(CFTC Dec. 17, 1982). ("It is imperative that each [side] of the market seek the best price in order for price discovery to occur and that 'best' price is, of necessity, at the expense of the other side").

[232] United States v. Coscia, 4 F.4th 454, (7th Cir. 2021) (upholding conviction for commodities fraud based on a strategy of spoofing).

[233] *In the Matter of JPmorgan Chase Bank*, 2013 WL 6057042, at *11 ("In a properly functioning market, prices reflect the competing judgments of buyers and sellers as to the fair price of a commodity or, in this instance, swaps. Here, acting on behalf of JPMorgan, the…traders' activities…constituted a manipulative device in connection with swaps because they sold enormous volumes of [a credit default index] in a very short period of time at month-end."); CFTC v. Wilson, No. 13 Civ. 7884 (RJS), 2018 LEXIS 207376 (S.D.N.Y. Nov. 23, 2018) at *57 (defining 'banging

motive, and this alone does not suffice to bless the relevant form of activity. Something more than the appeal to a profit motive for the specific transaction in question is needed to separate permissible transactions from those that form part of a manipulative scheme premised on illegitimately produced artificial prices, though it is no easy matter to specify with perfect generality precisely what more is required. In the end we suspect that the matter will be decided by the extent to which courts wish to protect notions of market integrity that exclude domination based on control of infrastructure that most traders do not have access to but all rely on.[234] While we think the argument will surely continue to rage on, this strikes us as the most plausible going theory of liability for open market sandwiching in general sounding in manipulation premised on illegitimate price effects.

Nonetheless, there is a final problem, which is of particular practical importance: we suspect that liability for standard open market sandwiching is unlikely to be pursued as a regulatory priority in the near term. In principle, someone could argue that an atomic sandwich constitutes a *naked open-market manipulation* scheme because the atomic condition of the sandwich equips the sandwicher with a "good reason to believe" that the average price at which they purchased (or sold) a crypto asset (in the front-run) would be larger than that when they sold (or purchased) the crypto asset (in the back-run) due to the price impact of the sandwiched transaction.[235] Nonetheless, very few cases – to our knowledge, only one – have found fraud-based manipulation liability on the basis of naked open market manipulation schemes alone.[236]

Our main explanation for why this is the case simply boils down to a matter of enforcement discretion. The limited precedent with respect to CFTC or SEC enforcement against naked open-market manipulation could simply stem from the fact that these practices are low on the totem pole of enforcement priorities given the high evidentiary costs associated with establishing the requisite scienter which differentiates legitimate from manipulative naked open market

---

the close' as involving "someone putting in a disproportionate number of trades to push the price up or down to affect the closing price, typically in a noneconomic fashion, to benefit a position that they held elsewhere").

[234] Lindsay Farmer, *Taking Market Crime Seriously*, 42 Legal Studies 508, 523-24 (2022).

[235] Fox, Glosten, and Rauterberg, *supra* note 94 at 74 (stating that naked open market manipulation schemes should be the subject of legal sanctions "only where it can be proved that [the trader] had, at the time of her purchase, good reason to believe that" an asymmetric price reaction would occur on the basis of their trades).

[236] *See* Markowski v. SEC, 274 F.3d 525 (D.C. Cir. 2001).

trades.[237] This would explain why practices like predatory trading,[238] which seem to meet the definition of *naked open-market manipulation,* are left unchallenged by the agencies.[239] As a result, a claim of fraud-based manipulation liability on the grounds that sandwiching constitutes an open market manipulation scheme involving at least recklessly creating artificial prices would be relatively unlikely to be brought in practice even if theoretically there is a plausible argument for this conclusion to be tested.

Of course, more debate always remains possible. As explained above,[240] naked open-market market manipulation is characterized by the lack of relations of trust between the party accused of manipulation and other traders, while covered market-manipulation (such as paradigmatic banging the close or oracle manipulation) do involve some such trust relations, which are at least implied (*e.g*. based on a formal mechanisms for pricing one asset that references another). The considerations adduced above, about block builders' control and exploitation of crypto market infrastructure, on which other traders rely, might similarly be seen as generating implied relations of trust, which could move MEV sandwiching of public trades more in the direction of covered open-market

---

[237] *See, e.g., Id.* at 530 ("We cannot find the Commission's interpretation to be unreasonable in light of what appears to be Congress's determination that manipulation can be illegal solely because of the actor's purpose"); SEC v. Masri, 523 F. Supp. 2d 361, 373 (S.D.N.Y. 2007) ("The court concludes, therefore, that if an investor conducts an open-market transaction with the intent of artificially affecting the price of the security, and not for any legitimate economic reason, it can constitute market manipulation"); *In re* Amaranth Natural Gas Commodities Litig., 587 F. Supp. 2d 513, 540 (S.D.N.Y. 2008) ("Entering into a legitimate transaction knowing that it will distort the market is not manipulation – only intent, not knowledge, can transform a legitimate transaction into manipulation").

[238] Predatory trading involves a strategic trader becoming aware (on the basis of public or private information) of an impending large transaction by another trader. For instance, a hedge fund with a nearing margin call may need to make a large liquidation. In response, the strategic trader first trades in the same direction as the distressed trader and subsequently reverses his position following the distressed trader's large transaction. As such, the strategic trader effectively profits by forcing the distressed trader to suffer a worse price on their large transaction. For an in-depth look at predatory trading, *see* Markus K. Brunnermeier and Lasses Heje Pederson*, Predatory Trading,* 60 J. of Fin. 1825, 1825 (August 2005).

[239] *See* Procedures To Establish Appropriate Minimum Block Sizes for Large Notional Off-Facility Swaps and Block Trades, 78 Fed. Reg. 32870, n.46 (May 31, 2003) (discussing predatory trading as a consequence of a regulatory regime requiring the "publication of detailed information regarding ''outsize swap transactions''); Alternatively, it may be the case that courts are hesitant to find fraud-based manipulation liability on the basis of purely *naked* trades because there is some implicit theory that a contractual relationship, or other kind of relationship that generates expectations between parties, makes some kinds of conduct manipulative which otherwise are not. As applied to open-market trades, it would follow from this theory that *covered* open-market manipulation schemes are more likely to be manipulative because they generally involve some contractual relationship or expectation-setting between parties to a transaction, while the same cannot be said for naked open market manipulation.
However, we explore this issue in more depth below.

[240] *Supra* Section III.C.

manipulation. But this is a speculative argument, again exploiting moralized forms of argument about when relations of trust, based on reliance upon market infrastructure that bock builders' control, should be found to exist. The closer MEV sandwiching of public trades appears to covered open-market manipulation, the more likely a regulatory response would be.

In the end, we think there remains a route to CTFC Rule 180.1 and SEC 10b-5 liability for public sandwiching provided courts and regulators adopt a moralized form of inquiry. It is by no means clear they will, but given that no binding tests exists for determining which *forces* or *factors* informing a price are legitimate and which are not,[241] we think this possibility cannot be conclusively ruled out ex ante.

(v) Front-running

We close this section by seeking to dispel a common misconception about sandwiching. A familiar critique of the first stage in a sandwich – rather unfortunately labelled the "front-run" – is that it resembles illegal front-running.[242] As discussed in Section III, illegal front-running entails a breach of a special duty (e.g., fiduciary duty) that a trusted person, like a broker or investment advisor, has toward their client.[243] Breaching the duty, a trusted person – or someone they tipped off – trades ahead of the client to benefit from the price impact of the clients' order.

*Existence of a special duty—relationships of trust.* The key question for applying this theory of liability is whether anyone involved in executing sandwiches has a relevant special duty towards the sandwiched trader, which would make trading ahead in this context (the "front-run") a "manipulative device, scheme, or artifice to defraud." This duty may be part of, e.g., a fiduciary duty of an agent to their client or it may arise because someone promises in a different context that they will not trade ahead. In the latter case, the illegality of front-running boils down to liability for untrue or misleading statements discussed above.

An investment adviser, regulated under the Investment Advisers Act of 1940 (IAA), or a broker, regulated under the SEA, are most likely to have duties that could, under some circumstances, be breached by trading ahead of a client. We are not, however, aware of examples of registered investment advisors or brokers being involved in sandwiching or other kinds of MEV extraction. If an investment adviser were to consider engaging in sandwiching, then they might need to consider the breadth of their duties under *SEC v Capital Gains Research Bureau*: of "utmost good faith, and full and fair disclosure of all material facts"

---

[241] *Supra* note 213.

[242] *See, e.g.,* Auer et al., *supra* note 11; Piet, Fairoze, and Weaver, *supra* note 12; IOSCO, *supra* note 15 at 37; U.S. TREASURY DEPARTMENT, *supra* note 15 at 36.

[243] *See supra* Section III.D.

and "to employ reasonable care to avoid misleading" clients.[244] Such duties may apply not just to clients with personal relationships with an adviser. In *Capital Gains Research Bureau* mere recommendation of the adviser's own investments in a newsletter, without appropriate disclosure (scalping), was held to be a breach of the advisers' legal duties. Much more could be said about the special cases of investment advisers and brokers but given that they do not appear to be prominent among MEV extractors, we will not do so here.

An MEV searcher who relies only on public information about a pending transaction and has no other knowledge about the transaction seems unlikely to have the special duty.

*Unclear whether sandwiching would breach the duty in all cases.* It could be that being involved in sandwiching of a user to whom one *does have* the special duty discussed here, would constitute a breach of that duty and thus illegal front-running. But this need not be so, if it could be shown that the practice is fully disclosed and that it is in the best interest of the user. The consideration of best interest could include aspects like "MEV rebates" or other services offered to a user (like faster execution) in return for assent to sandwiching.

*Front-running as misappropriation of private information.* By definition, sandwiching a public transaction does not involve the use of private information, hence the "insider trading" version of front-running is not applicable here. We will, however, come back to this point while discussing sandwiching of *private* transactions below.

### *B. Sandwiching Private Transactions*

The above discussion focused exclusively on sandwiches which target public transaction information. Yet, additional theories of liability – for instance, those finding insider trading and prohibited front-running[245] – become plausible where material non-public information is the basis of trading activity. On our view, a pending transaction constitutes private (non-public) information by default and remains private until the moment 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 network node that originally received the transaction.[246]

Users sometimes intend for their transactions to remain private while in a pending state (before they are included on the blockchain). To achieve that, users submit transactions to privacy RPCs.[247] However, transactions may be kept

[244] 375 U.S. 180 (1963) 365.

[245] *See supra* Sections III.C and III.D.

[246] *See supra* Section II.D.

[247] *See supra* Section II.B.

private by actors who are not expected to do so by users.[248] For example, an operator of an RPC that receives a user's transaction may decide to keep this transaction for herself before re-broadcasting it, even if only for several hundred milliseconds, to have a head start in identifying potential MEV extraction opportunities created by this transaction.[249] While an operator keeps the knowledge of the existence of a pending transaction to herself (and possible some collaborating operators), without making it public, she effectively treats the transaction as private order flow (POF). Given the potential to profit from having exclusive, even if only temporarily exclusive, knowledge about pending transactions, there are incentives for payment for order flow (PFOF) arrangements to arise.

In this section, we discuss the kinds of market manipulation liability – ranging from traditional fraud-based manipulation to price manipulation to insider trading – possible where private transactions are sandwiched. We argue that, in the absence of appropriate disclosure, liability is likely for actors who sandwich or are complicit in the sandwiching of (*i.e.,* by "tipping" transaction information to others who sandwich or by receiving payment in exchange for leaking order flow which is subsequently sandwiched) private transactions. The risk of liability is significant here not only because of the additional avenues of market manipulation liability which exist where a trading practice involves *non-public* information, but also due to the heightened trust relationships involved where an actor is the recipient of a user's private transaction information. As we find that different theories of liability exist in the case where a user intends to keep their transaction private and where they do not, we divide our discussion here accordingly.

1. Explicit Private Order Flow

Where Ethereum users submit their transaction to a privacy RPC, intending for those transactions to be forwarded privately to a particular block builder (or several block builders), we consider that a kind of private order flow (POF). We refer to it as "explicit" POF, because here the user manifests the intention for these transactions to be private by choosing a privacy RPC. We consider "non-explicit" POF in the next subsection. A transaction sent to a privacy RPC is meant not only never to become public while pending, but also to be shared only with specific parties (block-builders). We argue that MEV extracted through explicit POF faces a heightened risk of liability under the fraud-based manipulation prong of the CFTC and SEC's anti-manipulation authority.

To contextualize the following discussion, it is useful to understand *why* Ethereum users may want to route their transactions directly to a validator. One obvious reason may be that they are interested in being paid for agreeing to do so. For instance, some MEV rebate programs offer privacy RPCs with the

[248] *Id.*
[249] *Id.*

guarantee that a portion of the MEV extracted from users' POF will actually be given *back* to the user.[250] Alternatively, a user may route their transaction through a privacy RPC out of fear that sending their transaction to the mempool may serve as blood in the water, luring searcher bots who seek to exploit their trade and cause them to suffer a worse execution price. Rebate programs also tend to promise users that, in addition to MEV redistribution, the users will be protected from front-running (including sandwiching), and will receive "best execution."[251] POF arrangements generally involve off-chain communication wherein searchers and block-builders with access to POF make promises (either explicitly or implicitly, through their integration with a privacy RPC which advertises itself as offering privacy, front-running-protection, etc. as a service) to users in exchange for exclusive access to their order flow. Hence, POF is appealing for users because it provides them with both i) monetary rewards and ii) certain non-monetary guarantees with respect to their transaction such as pre-execution privacy and front-running protection.

When a user exclusively routes their order flow to a particular block builder (or set of builders), they are also *not* publicizing their transaction to the rest of the network. If the basic guarantee of a privacy RPC is not broken,[252] and the user herself does not submit the same transaction to a non-privacy (ordinary) RPC, then the information about a pending transaction submitted to a privacy RPC remains *non-public information* until the transaction is included on the blockchain.

The implicit and explicit promises made by block builders and searchers to the users who provide them with POF, we argue, create a relationship of *trust* between those operators and those users.[253] That is, users providing their POF to network operators *trust* that their transactions will remain private, will not be front-run (including sandwiching), and more. The involvement of *non-public information* and the existence of a *relationship of trust* thus paves a route to insider trading liability for block builders and searchers who sandwich user trades they received as POF.

Recall that both the CFTC and SEC police insider trading in their associated markets as a form of fraud-based manipulation prohibited under Rule 180.1 and Rule 10b-5, respectively.[254] Both agencies rely on the *misappropriation theory* of insider trading, which finds liability for trades made

---

[250] *See, e.g.,* ROOK, https://www.rook.fi/#How-It-Works; OPENMEV, https://docs.openmev.org/router.

[251] *Id.*

[252] *See, e.g., Ethermine Private RPC Endpoint,* BITFLY, https://ethermine.org/private-rpc (last accessed Jan. 30, 2023) (promising that "Ethermine will never leak nor act on the information received via this relay"); *Frontrunning Protection*; BLOXROUTE DOCUMENTATION, https://docs.bloxroute.com/apis/frontrunning-protection.

[253] For an analysis of the trust relationships endemic to blockchain based systems - including that of network transactors to blockchain validators, *see* generally Primavera De Filippi, Morshed Mannan & Wessel Reijers, *Blockchain as a confidence machine: The problem of trust & challenges of governance*, 62 TECHN. IN SOCIETY 1 (2020).

[254] *See supra* Section III.B.

on the "basis of material nonpublic information in breach of a pre-existing duty (established by another law or rule, or agreement, understanding, or some other source), or by trading on the basis of material nonpublic information that was obtained through fraud or deception."[255] Additionally, both agencies find insider trading liability for *tippers* – insiders owing a duty of confidentiality to the source of nonpublic information who do not themselves trade on the basis of material nonpublic information, but share such nonpublic information with others who proceed to trade on it.[256] A duty giving rise to insider trading liability under the misappropriation theory arises between the source of some nonpublic information and its recipient wherever that recipient "learns information in a context that implies confidentiality, even if the trader is not a corporate insider."[257]

Where a MEV extractor interacts with POF transactions, they could be held liable for insider trading where it is established that i) the MEV extractor had a "pre-existing duty" with the user from whom they received POF, and ii) the MEV extractor breached this duty in the process of either extracting MEV from the user's POF transactions *or* by "tipping" the user's transaction to another who then extracts MEV from the user's transaction. To establish the requisite "duty of confidentiality" for insider trading liability, it is not necessary that a trader or tipper owe a fiduciary duty to the source of some nonpublic information.[258]

In his work applying insider trading law to the realm of crypto assets, Andrew Verstein notes that "relationships of trust and confidence are widespread in the crypto asset economy," even though "it is common to refer to cryptocurrency systems as 'trustless.'"[259] In the context of POF, relationships of trust and confidence between an MEV extractor and a user are likely to be even more apparent than elsewhere in the crypto-economy, since explicit off-chain agreements are often formed laying out the obligations each of these parties owes to the other.[260] The recipient of this trust and confidence, a searcher or block builder with access to POF may owe a duty to keep private and to not front-run or sandwich the transactions of the user who provided that order flow. Such a duty forming the basis of insider trading liability could arise from a number of sources, including the following. First, there might be evidence of a specific, explicit promise by the MEV extractor to the user that they would not disclose and would not extract at least some kinds of MEV on the basis of a

---

[255] *See supra* note 119 at 41403.

[256] *See* Dirks v. SEC, 463 U.S. 646, 661 (1983) (establishing the "personal benefit test" for tippers in securities insider trading cases); CFTC v. EOX Holdings L.L.C., No. H-19-2901, 2021 WL 4482145, at *19 (S.D. Tex. Sept. 30, 2021) (holding that tippers can be liable for insider trading in commodities markets).

[257] Verstein, *supra* note 146 at 15.

[258] CFTC v. EOX Holdings L.L.C., 405 F. Supp. 3d 697, 709 (S.D. Tex. 2019) (rejecting the defendants' argument that the misappropriation theory applies only "when an individual owes a fiduciary duty to the principal whose information was allegedly misappropriated").

[259] Verstein, *supra* note 146 at 32.

[260] *See, e.g., supra* note 252.

user's nonpublic transaction information.[261] Second, there might be an agreement made (even based on the expectation of compliance with a privacy RPC's terms and conditions) as a condition of a MEV extractor's integration with a privacy RPC guaranteeing that a user's order flow would not be subject to some kinds of MEV extraction and that it would only be made available to the operators who were exclusively granted access. Third, a relationship of trust between the user and MEV extractor might arise from the fact that the MEV extractor "feigns loyalty" to the user for the purpose of accessing their material, nonpublic transaction information.[262] There could well be other sources of such a trust relationship.

Should such a duty be found to apply to a recipient of explicit POF, it is likely that a successful claim for insider trading under Rule 180.1 would arise. If the same MEV extractor who owes a duty of trust and confidence to a user sandwiches that user's POF, that MEV extractor arguably would be liable under the traditional misappropriation theory of insider trading liability. Alternatively, if it is not the MEV extractor with a duty who sandwiches the user, but another MEV extractor who they "tipped" and who subsequently sandwiched the user's transaction, the "tipper" searcher or block builder may still be held liable.

Admittedly, what constitutes a pre-existing duty sufficient to serve as the basis for an insider trading action under CFTC Rule 180.1 or SEC Rule 10b-5 is by no means settled. Courts dealing with securities and commodities fraud claims have long struggled to define "the contours of a relationship of trust and confidence giving rise to the duty to disclose or abstain and misappropriation liability."[263] Yet, even if an agency is unable to establish the existence of such a duty between an MEV extractor and user, the explicit representations made by MEV extractors in acquiring POF make plausible fraud-based manipulation claims on the basis of misrepresentations.[264] Fraud by material misrepresentation and omission claims under Rule 180.1(a)(2) and 10b-5(b) typically require that an accused engaged in a specific misrepresentation or omission.[265] Consider the experience of a user who provides POF to a MEV

---

[261] *EOX Holdings L.L.C.*, 405 F. Supp. 3d at 713 (discussing the conception of "duty" defined by the court in *SEC v. Cuban (Cuban I)* -- undisturbed by the Fifth Circuit in *Cuban II* -- that "insider trading could arise where there was an express … agreement to maintain the confidentiality of material, nonpublic information and not to trade on or otherwise use the information").

[262] Verstein, *supra* note 146 at 15. *See also* United States v. O'Hagan, 521 U.S. 642, 670(1997) (holding that ""the deception essential to the misappropriation theory involves feigning fidelity to the source of information").

[263] SEC v. Cuban, 620 F.3d 551, 555 (5th Cir. 2010)*;* CFTC v. EOX Holdings L.L.C., No. H-19-2901, 2021 WL 4482145, at *53 (S.D. Tex. Sept. 30, 2021) ("Defendants' argument that 'there is no need for an exegesis on the law of duty in this context,' fails to recognize that courts have been struggling with this precise issue for some time").

[264] *See* 17 C.F.R. §180.1(a)(2) (2012).

[265] The court in *CFTC v. Kraft* noted that fraud-based manipulation claims "based upon a misstatement" require the plaintiff to allege a material misrepresentation (or omission), scienter,

extractor in reliance on that MEV extractor's promise that their transaction would not be sandwiched, whose transaction is subsequently sandwiched by that MEV extractor resulting in a worse execution price for their transaction. Such a user's experience certainly "[sounds] in fraud" in a manner sufficient to satisfy the requirements of a fraud-by-misrepresentation claim,[266] such that only the requisite scienter of recklessness or intent would need to be established for the CFTC to bring a successful claim for fraud-based manipulation liability under Rule 180.1.

Additionally, it may be possible to attach price manipulation liability under CFTC Rule 180.2 to the conduct of a block builder who becomes a dominant player in the block-building market due to their access to POF. MEV extraction based on public transactions, including sandwiching, generally stimulates competition among searchers.[267] Yet, the same MEV extraction practices targeting POF transactions can generate anti-competitive effects. This is because a block-builder who receives POF is at a competitive advantage relative to other block-builders, as they have exclusive access to a source of order flow. As such, they may be able to build blocks from which they can extract more value than their counterparts, value which they can invest in better block-building infrastructure and/or obtaining more POF.[268] This "vicious cycle" of builder centralization may ensue until a block-builder captures a majority, or even a monopoly, of the block builder market Commodities regulators have long looked to a trader's "acquisition of market dominance" as a hallmark of manipulative conduct.[269] Should an informed block builder acquire a dominant position in the block building market, and should they exercise that power – for instance, by censoring transactions for a fee or engaging in multi-block MEV strategies etc. (premised on the control of transaction ordering within multiple blocks) – it is possible that they will be held to have intentionally caused the creation of a price which does not reflect legitimate forces of supply and demand.[270] Admittedly, a claim for traditional price manipulation might be

connection with the purchase or sale of a commodity, reliance, economic loss, and causation. United States CFTC v. Kraft Foods Grp., Inc., 153 F. Supp. 3d 996, 1012 (N.D. Ill. 2015), *quoting* Dura Pharms., Inc. v. Broudo, 544 U.S. 336, 341 (2005).

[266] Ploss v. Kraft Foods Grp., Inc., 197 F. Supp. 3d 1037, 1058 (N.D. Ill. 2016)("The court agrees that manipulation based on explicit misrepresentations sound in fraud").

[267] Daian, *supra* note 9 at 5 ("Because each pure profit opportunity carries some computable profit *p* and is broadcast globally, a competitive game naturally ensues among arbitrage bots to be the first to execute an atomic transaction that exploits the opportunity").

[268] *See* Quintus, *Order flow, auctions and centralisation I: a warning*, https://collective.flashbots.net/t/order-flow-auctions-and-centralisation-i-a-warning/258.

[269] *In re Cox,* ¶ 23,786 at 12-13, 060 ("the acquisition of market dominance is the hallmark of a long manipulative squeeze"); *Resch-Cassin & Co*., 362 F. Supp. at 977 ("dominion and control of the market for the security" are factors establishing causation of an artificial price).

[270] The exercise of market dominance in a commodities market is often seen as a paradigmatic form of price manipulation. *See, e.g.,* Pirrong, *supra* note 88 at 947 ("The most important form of manipulation consists of the exercise of market power in a commodity market").

difficult to make out given its higher requirement of intent to cause an artificial price. But Rule 180.1's lower standard of recklessness toward the creation of prices not reflecting only the forces of supply and demand, as involved in 180.1(a)(3) manipulative acts, may offer a more achievable route to imposing liability for exploiting a position of market dominance obtained through access to POF in the manner just described. While price manipulation liability is more plausible in this context relative to the context of sandwiching public information, it is still relatively unlikely given the prosecutorial burdens involved in establishing price manipulation.

2. Non-Explicit Private Order Flow and Payment For Order Flow

Recall from our discussion in the previous section that an Ethereum user, submitting transactions otherwise than to a privacy RPC, may *think* that their pending transaction is public while, in reality, it is not meaningfully so. In general, there are two ways in which this could happen. First, the default RPC used by the wallet software could treat such transactions as private, not re-broadcasting them in the Ethereum peer-to-peer network, instead forwarding them, *e.g.,* only to selected, cooperating block-builders. Second, the default RPC, or even the wallet software provider herself, could delay forwarding transactions long enough to have a sufficient advantage in extracting MEV from those transactions.

In traditional finance, payment for order flow (PFOF) refers to an arrangement in which an "internalizer" (*e.g.,* Citadel) pays a broker (*e.g.,* Robinhood) in exchange for the broker routing her retail clients' orders to the internalizer, who then executes trades against those orders.[271] In an analogous fashion, service providers like wallet software providers and RPC operators can, in a sense, sell the order flow of their customers to MEV extractors, acting as internalizers.[272] A wallet software provider could do this by setting an internalizer-operated RPC as the default option, which could – but in practice may be unlikely to be – changed by users. But this could also be done by not giving users the choice as to which RPC the wallet software will use. Finally, a wallet software provider could delay sending transactions to a public RPC, while sending the information about new transactions to paying internalizers first, thus guaranteeing them an advantage in extracting MEV. A popular RPC operator may be able to use similar methods (exclusive transaction forwarding, temporal priority in forwarding).

Both in the standard case of non-explicit POF, and in its special case – PFOF arrangements, user transactions constitute, at least temporarily, *non-*

[271] FOX, GLOSTEN, AND RAUTERBERG, *supra* note 21 at 289 n.34.

[272] *See, e.g.,* Quintus, *Order flow, auctions and centralisation I: a warning*, https://collective.flashbots.net/t/order-flow-auctions-and-centralisation-i-a-warning/258; 0xC8e7, *MEV Markets Part 3: Payment for Order Flow*, 0XSHITTRADER.ETH BLOG (Aug. 2022), https://mirror.xyz/0xshittrader.eth/f2VSuoZ91vAbCv82MtWM-Gosyf_DeUXfPlDx3EYV3RM .

*public* information which is only available to selected operators.[273] The key difference between explicit and non-explicit POF is that in the latter case, the users are not informed about the practice.

It is arguable that an ordinary user is likely to assume - if not informed otherwise - that, when they submit transactions otherwise than to a privacy RPC, those transactions are routed publicly and that no one has privileged access to those transactions.[274] Where any of the situations described earlier in this subsection arise, it may be that the wallet provider's customers are *misled* in a legally relevant way.

The CFTC's Rule 180.1(a)(2) renders it unlawful for a market participant to "omit to state a material fact necessary in order to make the statements made not untrue or misleading."[275] The SEC's Rule 10b-5(b) contains a nearly identical prohibition.[276] As recklessness is the requisite scienter for both Rule 180.1 and Rule 10b-5, an accused need not have intended or desired to artificially affect prices.[277] The CFTC and SEC's prohibitions against fraud-by-omission suggest a route to liability for RPC operators and wallet software providers who privatize their user's transactions in order to extract MEV themselves or gain PFOF without disclosing such a practice to their users. In particular, if Ethereum users are entitled to believe that their transactions submitted with wallet software will not be treated as private order flow – at least on our definition – then it could be argued that a wallet software provider who treats transactions as private order flow must disclose this to users for users not to be misled.

Pursuant to this theory, the wallet provider or RPC operator could be *recklessly* engaging in a deceptive omission potentially warranting liability under Rule 180.1(a)(2) and 10b-5(b). Their actions could be deemed *reckless* even where their primary motive was simply to profit from PFOF.

One may respond to this by challenging the assumption that Ethereum users do, in fact, assume that software providers or RPC operators route their transactions in a public way. More research needs to be done regarding the frequency of routing practices used by wallet providers and other trusted DeFi intermediaries, and user perceptions of such routing patterns, in order to unpack the strength of this assumption. With this said, it is illustrative that the SEC requires securities brokers in traditional finance to publicly disclose their customer order routing practices, including those involving PFOF

---

[273] See *supra* our proposed definition of *public* in Section II.D.

[274] *See* De Filippi, Mannan, and Reijers, *supra* note 253 at 10 & n.7 (stating that "a participant in a blockchain-based system may expect that a miner will always act in accordance with the consensus algorithm of that system but empirical research has shown that [validators] can deviate from the standard protocol…").

[275] 17 CFR § 180.1(a)(2) (2012).

[276] 17 CFR § 240.10b-5(b) (1951).

[277] In the Matter of JPMorgan Chase Bank, 2013 WL 6057042, at *11 ("even if a trader were motivated by a desire to obtain compensation rather than by a desire to affect a market price, if the trader recklessly effected the manipulative trades, he will be held liable").

arrangements.[278] While not directly applicable in this DeFi context, this rule plausibly indicates a policy judgment that some fiduciary or other trust-based obligation exists requiring actors with privileged access to transaction information to act honestly and transparently with respect to the actual originators of that transaction information. It would not be unreasonable to assume a similar policy judgment might be implemented for DeFi as CFTC and SEC begin to flex their regulatory muscles in the crypto space more fully in the near term.

### *C. Other Ways to Extract MEV: Oracle Manipulation*

There are many sources of, and many ways to extract, MEV. Sandwiching, discussed in the previous subsections, receives the most attention from external observers. However, though highly profitable and with a significant effect on the market, sandwiching is not even considered to be the most valuable kind of MEV.[279] Strategies like liquidations and arbitrage, especially between centralized crypto exchanges and decentralized, on-chain exchanges ("CEX/DEX"), may be both more profitable and more likely to stay as a permanent feature of crypto markets, even if sandwiching is alleviated by technical developments.[280]

Legally speaking, strategies like arbitrage and liquidations are likely to be of less interest as a source of liability at least where they involve merely taking advantage of "natural market events."[281] Matters are different if these strategies involve independent wrongdoing, of course (such as fraudulent statements), or perhaps in other narrow circumstances.[282] Because we focus here on the strongest going theories of direct liability for MEV, however, we do not discuss MEV arbitrage or liquidations further, instead exploring these issues in other work.[283]

Instead, we end by discussing one final important way MEV extraction may be facilitated, which in our view carries especially high legal risk: so-called "oracle manipulation."

---

[278] 17 CFR § 242.606 (2018).

[279] Amber Group, *supra* note 35.

[280] *Id.*

[281] United States v. Coscia, 866 F.3d 782, 786 (7th Cir. 2017); s*ee also* Green, *supra* note 217 (discussing the normative importance of taking advantage of an event or disturbance caused naturally by factors outside one's control rather than causing it oneself).

[282] *See, e.g.,* Qin, Zhou, and Gervais, *supra* note 49 at 6; Barczentewicz, *supra* note 18 at 11–12.

[283] In our related work on arbitrages and liquidations we consider issues like possible adverse consequences for trades that create an arbitrage opportunity, as well as whether the competition for exploiting arbitrage and liquidation opportunities can be said to be fair (non-manipulative) when it entails leveraging the privileged position of a block producer.

1. Oracle manipulation to create loan liquidation opportunities

Though this may change, currently the paradigmatic case of the use of oracle manipulation is to attack on-chain lending systems; notably, but not only, to create artificial *loan liquidation* opportunities.[284] For on-chain liquidations to work, lending systems require external information about prices of the assets involved. Technically, the smart contracts that are the lending systems rely on other "oracle" smart contracts. The oracle smart contracts are meant to faithfully report prices (or other information), *e.g.,* based on what happens on some other on-chain (DEX) or off-chain (CEX) markets.

Hence, a liquidation opportunity can be created *artificially* in two scenarios: i) if an oracle can be made to report an incorrect (low) price of the asset used as collateral or ii) if the benchmark markets from which an oracle collects price information can be manipulated. Here, we only focus on the second strategy, as it is a more central case of market manipulation, without the complicating factor of hacking that would likely be needed for the first strategy. Strictly speaking, the second strategy does not manipulate the oracle itself, because the oracle functions as intended: it is just that the prices that it reports may result from manipulation. It may thus be more precise to refer, e.g., to "loan liquidation price benchmark manipulation," but the label of "oracle manipulation" is already established.[285]

Not all oracle manipulations involve MEV extraction. Yet, as Mackinga et al. show, the profitability of a self-created liquidation opportunity is often contingent on control over transaction ordering.[286] That is, where a liquidation opportunity is triggered by an instance of oracle manipulation, it is publicly visible and able to be captured *not only* by the oracle manipulator but *also* by any other strategic actors paying attention. Because oracle manipulation generally requires a significant initial investment to create a sufficiently large change in the benchmark price, a rational manipulator will only expend that capital if they harbor a degree of *certainty* that i) they will be the first to execute the profit opportunity created by their oracle manipulation, *and* ii) that they will be able to reverse (*de-manipulate)* their oracle manipulation transaction in order to redeem the upfront capital expended.[287]

---

[284] For a general description of loan liquidations, *see supra* Section II.C. For in-depth discussions regarding the mechanics of how price oracles can be manipulated in decentralized finance, *see* Austin Adams, Xin Wan, and Noah Zinsmeister, *Uniswap v3 Price Oracles in Proof of Stake,* UNISWAP BLOG (Oct. 27, 2022), https://uniswap.org/blog/uniswap-v3-oracles; 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).

[285] *See also* Barczentewicz, *supra* note 18 at 12–14.

[286] *See generally* Mackinga, Nadahalli, and Wattenhofer, *supra* note 284.

[287] *Id.* at 2. ("the attack's profitability ... rests on whether the [manipulator] can *de-manipulate* the price [of the collateralized crypto asset] back to market price without other users front-running the [manipulator]").

To acquire that *certainty* of first execution and de-manipulation, a manipulator requires control over transaction ordering, i.e., engaging in MEV extraction and, specifically, *multi-block* MEV extraction.[288] Where an oracle manipulator controls the ordering of not just one, but two consecutive blocks, or where two different agents who jointly control consecutive blocks collude, the manipulator(s) guarantee to themselves the profit from the liquidation opportunity they create through their oracle manipulation.[289] After depressing a benchmark price (manipulating an oracle) in one block, the manipulator(s) can then control the transaction ordering of the next block so as to place their own de-manipulation and liquidation transactions *first* regardless of whether any other actors paid a higher bribe for their own version of those transactions.

2. Fraud-based manipulation liability

While "standard" instances of liquidations which merely take advantage of "natural market events" are unlikely to constitute impermissible market manipulation, those cases need to be distinguished from intentional creation of a liquidation opportunity. That is, from situations where a liquidation does not arise from a "natural market event." When a MEV extractor engages in independently uneconomic activity with the purpose of triggering a liquidation opportunity, they likely cross the fine line from legitimate trading to illegal manipulation. Specifically, a MEV extractor who engages in oracle manipulation to trigger a liquidation/arbitrage opportunity may be liable for covered open-market manipulation[290] in violation of the SEC and CFTC anti-fraud rules.

Covered open-market manipulation involves a trader "[trading] to trigger payments or rights in a separate contract or financial instrument, the pricing of which is affected by the trades".[291] Thus, when the trader *intentionally* depresses the DEX price in order to trigger a liquidation (or other profitable opportunity)

---

[288] On multi-block MEV, *see supra* Section II.B.

[289] Mackinga, Nadahalli, and Wattenhofer, *supra* note 284 at 6.

[290] *See* discussion of covered open-market manipulation in Section III.B**.** While many covered open-market manipulation schemes involve contractual arrangements (i.e. financial derivatives) between two or more parties, the existence of a contract between two parties whose pay-outs are determined by a common benchmark is not a necessary component of a covered open-market manipulation scheme. Wherever a manipulator "tilts what ought to be a neutral contract or financial instrument into an arrangement that benefits her by interfering with the objective valuation methods on which the parties agreed," they act in contravention of the reasonable expectations of the others who rely on the objectiveness of that valuation method. Accordingly, covered open-market manipulation schemes can occur in the absence of explicit contractual arrangements – for instance, in the context of DeFi markets where parties transact anonymously but still harbor reasonable expectations regarding the integrity of benchmark-based valuation methods like oracles. *See* Fletcher, *supra* note 21 at 533.

[291] *Id.* at 503.

reliant on a price oracle affected by the DEX price, that trader has engaged in a form of covered open-market manipulation.

Notably, oracle manipulation is one of few DeFi market practices which has been directly challenged by the CFTC and the SEC.[292] While Avi Eisenberg's manipulation of Mango Markets was not a direct result of MEV extraction, the instance of multi-block MEV described above may produce analogous results. As such, there is a high likelihood that oracle manipulation strategies triggering liquidations and other profitable, publicly viewable opportunities -- thus implicating MEV extraction -- would be considered impermissible manipulative trading practices.

## V. A NOTE OF CAUTION ON THE POLICY QUESTION

Should regulators and lawmakers find some of the theories of liability we explored in Section IV compelling, they may be inclined to pursue a blanket ban on certain disfavored MEV extraction practices, like sandwich trades. Likewise, it's conceivable that courts might converge on an interpretation of "manipulative device" that encompasses all sandwich trades – not only POF sandwiching or schemes like oracle manipulation. In this section, we want to sound a note of caution about the extent to which this would be *good policy*.

While purely legal considerations in favor of or against a liability-based approach to the regulation of MEV extraction must have weight, they should not be viewed in a vacuum as this is in essence a technical, economic, and social phenomenon. The question of whether a strict prohibition against at least some kinds of MEV extraction would be desirable policy is distinct from that of how existing law would most likely treat MEV extraction. It is an important question nonetheless. We conclude by advising caution on this policy question. It is important for courts and regulators to bear in mind that *even if* sandwiching (or other forms of MEV extraction) turns out to be manipulative on the best legal interpretation, it's not obvious that a blanket ban on the practice would be good policy.

We begin with the unknowns. There are gaping holes in the existing state of knowledge regarding the economics of MEV extraction practices like sandwich trades which render it impossible to fully understand the net effect of sandwiching – on market efficiency, and on social welfare more broadly. By corollary, we are not in a position at present to know what effects a domestic ban on sandwich trades would have on these criteria either. The implications of sandwich trades (indeed, all forms of MEV extraction) on market efficiency are shrouded in uncertainty and remain contested.[293] The only research which has

[292] *Supra* note 26.

[293] *See* Barczentewicz, *supra* note 18 at 16 (discussing the uncertainty regarding the implications of MEV extraction on market efficiency and social welfare).

substantively inquired into the efficiency effects of sandwich trades has done so through the lens of algorithmic game theory, rather than empirical analysis.[294] Notably, this research found that sandwich trades, under some circumstances, can actually *increase* market efficiency and social welfare at the *network level* by causing more effective transaction routing patterns[295] and stronger incentives for validators to stake (i.e. participate in block construction).[296] This research indicates that limiting one's analysis of the market efficiency implications of sandwich trades and other MEV extraction practices to their purely local implications on individual trades is insufficient, as the individual harm to a sandwiched user may be outweighed by the market-wide efficiency gains produced by sandwich trades considered in the aggregate. Yet, because this research is theoretical in nature, we cannot currently predict the extent to which the social welfare and market efficiency gains it proposes does in fact affect the market. Further research on this point is crucial for the instant policy question.

Complicating the efficiency calculus further are the differences in underlying settlement technologies and market structures employed by DeFi and traditional financial systems. For instance, the security and strength of a blockchain's distributed consensus mechanism – i.e. for Ethereum, the network of independent and honest validators – can have significant implications for the efficiency of a DEX which is built on top of that blockchain. Meanwhile, there is no direct analogue for such a consideration in traditional markets.[297] Additionally, the scope of a "market" for the purposes of a market efficiency analysis is broader in the context of MEV extraction than an examination of this concept in traditional finance may suggest. [298] In traditional finance, one thinks of a "market" where manipulation can occur as any locus of the buying, selling, and lending of a financial instrument. Yet, MEV can be extracted in blockchain-based markets *beyond* the realm of DeFi – MEV extraction can arise in the context of non-fungible token (NFT) sales,[299] and other decentralized application functionalities. As such, it may prove advisable to broaden the scope of a market efficiency analysis for MEV extraction beyond what would have been standard in traditional finance.

---

[294] *See generally* Kulkarni, Diamandis, and Chitra, *supra* note 12 at 22–24.

[295] *Id.*

[296] *See generally* 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).

[297] In traditional finance, the connection between the backbone infrastructure of a market and that market's efficiency still exists, but is more indirect and fragmented than this connection is in decentralized crypt oasset markets. In traditional finance, market structure factors like supply chain, clearing/settlement processes, and trading rules implicate market efficiency considerations like a market's competition, liquidity, transparency, and price formation. Whereas, in the context of decentralized crypto asset markets, there is a more direct and coherent link between network/ consensus security and market efficiency.

[298] Barczentewicz, *supra* note 18 at 17.

[299] *See supra* note 75.

Knowing so little about local and broader market effects of sandwiching and other forms of MEV extraction, the possibility cannot be ruled out that the costs associated with regulatory measures which implicate MEV could be as severe as "giving up on the benefits of decentralized and permissionless public blockchains."[300] For instance, as alluded to by Chitra and Kulkarni, validators in a proof-of-stake system like Ethereum will only rationally lock in the capital required to be a validator, if this use of capital is approximately as profitable than alternatives. Should validators' profits from MEV extraction significantly decrease due to a legal prohibition, there is a risk that they would stop validating altogether, opting to put their assets to more profitable uses.[301] The consequence of this asset migration taking place on a large scale should not be underestimated. Because the security of a blockchain like Ethereum is contingent on the volume of assets locked within the protocol itself by validators, the security of the blockchain record could be significantly undermined. This could, for instance, increase the ease with which a malicious validator could execute a 51% attack[302] or increase the likelihood of double-spending[303] – risks which are reduced by the existence of a larger, more diverse group of validators engaged in building blocks. While the purpose of this paper is not to outline the virtues of decentralized systems built on public blockchains, the current market capitalization of Ethereum at nearly $200 billion and that of the entire crypto asset market at $1.08 trillion should speak for itself with respect to what is here at stake.[304] Risks created by regulatory intervention to the basic infrastructure of such a substantial market should not be taken lightly.

Of course, it's possible that a court or regulator with an eye toward consumer protection may find the potential costs outlined above, even at their most severe, to be small compared to the benefit of meaningfully protecting consumers from being *attacked* by purportedly malicious sandwichers. Nonetheless, there is a significant risk that a policy banning sandwich trades in the U.S. would not have as great an effect on the protection of users as might be hoped. For one thing, the Ethereum network, and markets built on it, are

---

[300] Barczentewicz, *supra* note 18 at 27.

[301] *See generally* Chitra and Kulkarni, *supra* note 296.

[302] A 51% attack involves a validator (or group of colluding validator) with control over more than 50% of the nodes in a blockchain network altering the blockchain record. While PoS blockchains like Ethereum are often considered resistant to 51% attacks, it is still possible for a malicious validator who acquires a large proportion of Ethereum's total stake to engage in a profitable 51% attack. For instance, this can be done through short-selling. *See generally* Suhyeon Lee and Seungjoo Kim, Short Selling Attack: *A Self-Destructive But Profitable 51% Attack On PoS Blockchains,* CIST (2020), https://eprint.iacr.org/2020/019.pdf.

[303] Double-spending occurs on blockchain networks where the same crypto asset is spent more than once; *see* Nakamoto, *supra* note 22.

[304] *Ethereum Market Cap*, YCHARTS, https://ycharts.com/indicators/ethereum_market_cap#:~:text=Ethereum%20Market%20Cap%20is%20at,36.70%25%20from%20one%20year%20ago ; https://coinmarketcap.com/ (accessed January 29 , 2023).

borderless in nature, a U.S. ban on sandwich trades would still leave U.S. users vulnerable to the activity of sandwichers from other jurisdictions – particularly where the enforcement of U.S. laws are difficult (either due to restrictions on the extraterritorial application of securities laws or the difficulty of enforcing a judgment from U.S. courts in certain foreign jurisdictions).[305] Moreover, there are well-known difficulties with enforcing securities laws within crypto markets in particular, given the heightened levels of anonymity these markets currently involve. Together these enforcement difficulties likely limit the benefit to consumer protection that a broad ban on certain forms of MEV extraction would have in practice.

Accordingly, rather than jumping the regulatory gun with a sweeping ban, it is crucial to explore whether consumer protection concerns surrounding sandwich attacks might not be better assuaged through technical solutions tailored to global blockchain networks, as opposed to regulatory measures bound by jurisdictional limits.[306]

## VI. PROPOSALS AND CONCLUSIONS

This Article has examined how key differences in the operation of traditional finance as opposed to crypto markets can make a normative and, therefore, legally significant difference. We saw how basic notions of fair versus unfair conduct play out differently in a world of discretionary transaction ordering compared to the more familiar world of first-come first-serve execution of transactions. Because Ethereum is, among other things, a financial system where discretionary transaction ordering can prevent the transactions submitted first from being executed first, we saw that users like our sandwiched trader, 0x61, from the introduction cannot claim unfairness merely on the basis of queue-jumping. As we observed, there is no such natural temporally ordered queue in networks like Ethereum.[307]

Nonetheless, by itself, this does not settle the question of whether sandwiching and other forms of MEV extraction really are unfair – and more importantly, whether they are ever legally out of bounds. It is the latter legality question that this Article sought to illuminate through the first in-depth Article-length treatment of MEV under U.S. securities and commodities law. We argued that some forms of MEV extraction including certain common forms of

---

[305] *See, e.g.,* Rebecca Cloeter, *The Extraterritorial Application of the Commodity Exchange Act*, 41 ENERGY L. J. 387 (2020).

[306] For an in-depth overview of current private sector approaches to mitigating the negative externalities of MEV extraction, *see S*en Yang, Fan Zhang, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu, *SoK: MEV Countermeasures: Theory and Practice* (Dec. 2022), https://arxiv.org/pdf/2212.05111.pdf.

[307] *See supra* Section I, Section IV.A.

sandwiching entail a significant risk of amounting to a manipulative practice in contravention of CFTC Rule 180.1 or SEC Rule 10b-5 (depending on whether the crypto assets at issue end up being classified as commodities or securities). We found that the key question on which the issue of manipulation liability depends, in many ways, is how much various MEV extractors, involved in different types of trading strategies and arrangements with other traders, can be said to occupy positions of *trust* that carry special responsibilities to avoid interfering with the reasonable expectations of other market participants.

In particular, Section IV developed novel arguments showing that even garden-variety MEV sandwiching of public transactions might amount to manipulation. We saw that especially courts drawing on moralized conceptions of market fairness – which would eschew the exploitation of privileged access to core financial infrastructure that other market participants lack (namely, the ability to order transaction while building blocks) – have a route to concluding that sandwiching of public transactions constitutes manipulation, in violation of CFTC Rule 180.1 or SEC Rule 10b-5, because such activity would typically at least recklessly create an artificial price effect. In the end, this turned on whether the requisite trust relation is found to run from MEV extractors like validators to other market participants. That said, we also stressed the significant practical hurdles for successfully bringing a manipulation claim against sandwiching public transactions, which we suspect make it unlikely to be pursued as a regulatory priority in the near term.

We then argued that the legal hazards are substantially greater when it comes to sandwiching of *private* transactions. When the crypto version of *private order flow* is involved, we saw there was a particularly strong case for thinking that validators, and others who may be involved in including transactions on the blockchain, have been trusted to act in confidence and thus are more likely to end up behaving in misleading or manipulative ways when engaging in sandwich attacks or otherwise handling private transaction information. Insider trading liability was a particular concern here in addition to the bite of anti-manipulation rules more generally. Finally, we observed that the case for liability is particularly strong when it comes to large disruptive schemes, such as oracle manipulation, involving the interference with financial benchmarks to which the prices of other crypto assets are pegged.

While there thus is a serious case for viewing some forms of MEV extraction as manipulative or otherwise in contravention of the relevant securities or commodities laws (as the case may be), we closed by arguing that this should not be taken to mean a sweeping ban on these forms of MEV should automatically be pursued. Section V moved to discussing matters of policy, aimed at regulators and other policymakers, and we argued that it remains far from clear that a strict ban on the offending forms specifically of MEV *sandwiching* would be good policy. There are at present too many unknowns about the net impact on market efficiency and social welfare, whether negative or perhaps positive, of MEV sandwiching, particularly when considered in the aggregate. Likewise, due to enforcement difficulties within crypto markets, we

saw questions remain about the benefits to consumer protection that such prohibitions can produce. More empirical research on both questions is imperative.

Where does this leave the debates both about permissibility under existing law of MEV extraction and the proper policy response thereto? To guide future conversations, we close with four general recommendations:

*1. Focusing regulatory attention on MEV extraction practices that cause harm:* The phenomenon of MEV extraction presents far more nuance than initially meets the eye. As discussed in Section IV, the publicness of transaction information, the atomicity of a MEV extraction opportunity, and the trust relationship between a user and MEV extractor are all crucial factors for determining whether a particular instance of MEV extraction is manipulative. Moreover, as we saw, there are myriad varieties of MEV extraction.

Accordingly, given all the technical and legal nuance that this presents, we warn against viewing "MEV extraction" as a singular phenomenon, and recommend an approach that recognizes that there may be as many different varieties of MEV extraction as there are opportunistic trading practices in traditional finance. Thus, it is not really "MEV extraction" that should be the subject of regulatory attention, but rather specific MEV practices which harm ordinary traders or the market at large. For instance, while DEX arbitrage – akin to cross-exchange arbitrage in traditional markets – usually supports price discovery without harming consumers, intentional self-created liquidations like those involving oracle manipulation strike a close resemblance to covered open-market manipulation schemes like "banging the close."[308] Likewise, the presence of express fraud (*i.e.,* a node operator, wallet operator, or block-builder promising not to front-run or sandwich a user, and subsequently proceeding to do so), or the existence of a relationship of trust that gives rise to legitimate expectations that then are contravened, are also indicators of manipulative conduct worthy of legal action. Accordingly, a regulator would understandably opt to expend limited resources pursuing the more obviously harmful MEV practices than to launch a broadside against MEV extraction in general, given its multiplicity and pervasiveness.

*2. Cross-Disciplinary Research:* Knowing which MEV practices rise to the level of harm that might make them a regulatory priority, however, requires more empirical research, as seen in Section V. Thus, we recommend that economists, technical researchers, and legal scholars engage in cooperative research to better understand the market efficiency and social welfare effects – on an individual and system-wide scale – of the many different strategies of MEV extraction. Such research, particularly when focused on individually harmful MEV extraction practices like sandwich trades, is the only way to shed light on the metaphorical dark forest of MEV.

---

[308] *See supra* notes 138-140.

*3. Clarity within the law of market manipulation:* To enhance the clarity and predictability of the law, we further recommend a beneficial step that regulators and courts could take in this arena is to inject more certainty into the capacious anti-fraud standards within CTFC Rule 180.1 and SEC 10b-5 – which make use of moralized concepts like "deceit" and "manipulative device" – and to clarify the place of moral reasoning within the interpretation of these standards. Such calls for clarity have been subject of entire scholarly contributions,[309] but we raise it here specifically with respect to the place of moralized criticisms in the applicable anti-manipulation standards. We saw in Section IV how the adoption of a moralized form of reasoning regarding how to protect market integrity from the exploitation of block builders' privileged position of control led to an increased likelihood of finding liability for sandwiching. Thus, a crucial step to increasing the clarity and predictability of the law in this area is to further clarify which conceptions about the morally unfair exploitation of positions of control (or even domination) will take open market transactions out of the realm of fair play and place them under a cloud of potential liability.

*4. Terminology*. Our final recommendation is primarily addressed to the Ethereum community, though it also involves a note of caution for courts and regulators. In particular, it is important for Ethereum community members to choose their words carefully, as implicit associations – once formed – can become indelible.

The language used to describe many practices and concepts of the MEV ecosystem (and the crypto-economy more generally) is often derived from traditional finance. For instance, we use terms like "bribe" and "front-running" to describe concepts native to MEV extraction on public blockchains. Within ordinary language, such terms naturally connote crime and illegitimacy. But this is often misleading when we depart from context and expectations of traditional finance and move to the distinct architecture of crypto markets. We saw earlier why "front-running" used to describe the MEV extraction practice of seeking to have one's order executed ahead of another's is distinct from the legal notion of front-running as an illegitimate market practice. With respect to "bribes," the term as used in the MEV context refers to the transaction fee a searcher pays to a block-builder or validator. Where such terms are used, it becomes easier for commentators and regulators to critique these practices as illegal *front-running* or immoral *bribing* without undertaking sufficient legal or technical investigation to justify these normative conclusions. Similarly, MEV extraction is often defined as involving the "reordering" of transactions,[310] which implies that a *different* ordering of transactions once existed and was altered by the

[309] *See, e.g.,* Pirrong, *supra* note 88; Janet Austen, *What Exactly is Market Integrity? An Analysis of One of the Core Objectives of Securities Regulation,* 8 Wm. & Mary Bus. L. Rev. 215 (2017).

[310] *See, e.g.,* Piet, *supra* note 12 at 5; Kulkarni, *supra* note 12 at 4; *What is Maximal Extractable Value (MEV*), BINANCE ACADEMY (Jan. 2023), https://academy.binance.com/en/articles/what-is-maximal-extractable-value-mev.

conduct of MEV extractors. But as we have stressed repeatedly in this Article, in a world of discretionary transaction ordering like Ethereum there is no obvious or natural ordering to serve as the default. Therefore, a block which includes MEV extraction opportunities has not necessarily been *reordered* by a validator but was simply *ordered*. Given that moralized conceptions of market fairness can play a significant role in legal determinations of trading practices as manipulative,[311] a conceptualization of MEV extraction as "reordering" transactions (as opposed to just an outcome of ordering) may have adverse legal consequences.

We therefore urge members of the Ethereum community to be careful about the terminology chosen for on-chain concepts given their off-chain connotations. Likewise, we would caution courts and regulators wading into these matters afresh to be mindful that the concepts informally adopted for describing the workings of crypto-finance may not always mean what they naturally seem to when used in the rather different world of traditional finance.

[311] *See supra* Section IV.A.