RESPONSE TO
Blockchain Transaction
Ordering as Market Manipulation

B. Salman Banaei*

I. INTRODUCTION ................................................................. 90
II. PROPORTIONALITY + MARKET MANIPULATION ...................... 94
   A. Background on Proportionality ........................................... 94
   B. The Importance of Proportionality in the Law of Market Manipulation ................................................................. 95
III. THE COSTS AND BENEFITS OF SANDWICH TRADES IN DECENTRALIZED MARKETS ......................................................... 97
   A. Background on Sandwich Attacks ........................................ 97
   B. Private Sector Mitigants to Sandwich Attacks ...................... 98
IV. PROPORTIONALITY ANALYSIS BALANCING THE COSTS + BENEFITS ................................................................. 99
V. CONCLUSION + RECOMMENDATIONS .................................... 103

* Former CFTC official (2009–2013), IHS Markit Executive Director, including Head of Blockchain (2017–2021), Co-Head of Public Policy at Chainalysis (2021–2022), and Head of Public Policy at Uniswap Labs (2022–present). D.N.M., Ecole Nationale Supérieure du Pétrole et des Moteurs (2008); M.Sc., Colorado School of Mines (2008); J.D., University of Denver Sturm College of Law (2007); B.A., University of Virginia (2002). This Response represents the current views of the author and not of any current, past, or future employer of the author.
I. INTRODUCTION

While I agree with many of the arguments presented by Barczentewicz, Sarch, and Vasan, which urge caution to regulators in acting to address MEV sandwich attacks, I present an additional lens and framework to evaluate the question of whether sandwich attacks justify direct validator regulation or should be expressly prohibited as a specific form of market manipulation at this current moment in the development of blockchain-based financial market infrastructures.

As discussed in further detail below, my view is that private sector remedies like smart order routing, optimized slippage limits, and Flashbots Protect RPC have the potential to reduce the prevalence and extent of sandwich attacks and the like. Regulators should defer to the continued development and implementation of such efforts. Ex ante regulatory solutions like direct validator regulation are, in my view, disproportionate and undermine the open architecture necessary to achieve the inclusion and innovation benefits of open blockchains. Other solutions, including ex ante duties to mitigate MEV (and other similar costs to users) for service providers engaging in discretionary order routing (i.e., “non-held” orders where the service provider’s discretion is used to find most favorable price for the user under the circumstances) and ex post regulatory solutions like declaring sandwich attacks and other malicious MEV strategies a form of market manipulation could be justifiable, but only under three pre-conditions that do not currently exist: (1) a constructive, global approach to regulating crypto markets is implemented, enhancing the effectiveness of such a ban; (2) the growth by orders of magnitude of sandwich attacks and other malicious forms of MEV relative to overall on-chain volumes in the most widely used open blockchains; and (3) the demonstrated failure of private sector remedies at mitigating the harm.

Maximal Extractable Value or “MEV” entered the global policymaking discourse in 2022, prompting this category of blockchain-based trading practices most common in the Ethereum marketplace to become a subject of strong regulatory scrutiny. Regulators have gone so far as to call MEV an “existential risk to the integrity of the Ethereum ledger”, and legislation addressing the practice has been proposed (but,

---

1 See generally Raphael Auer, Jon Frost & Jose Maria Vidal Pastor, Miners as Intermediaries: Extractable Value and Market Manipulation in Crypto and DeFi, BANK FOR INT’L SETTLEMENTS BULL. (June 16, 2022), https://www.bis.org/publ/bisbull58.pdf.

2 Id.
notably, not passed). In Blockchain Transaction Ordering as Market Manipulation, Barczentewicz, Sarch and Vasan provide a thought-provoking first legal analysis of MEV extraction in which they shed light on the aspects of market structure, dynamics of power and privilege, and informational asymmetries which characterize the MEV supply chain on Ethereum. I am honored to provide this response.

Some analogies comparing MEV extraction to manipulative (and illegal) trading practices in traditional finance—such as broker frontrunning and insider trading—exist in policy discussions surrounding these practices. Yet these comparisons fail to acknowledge the real and significant differences between traditional finance and decentralized blockchain-based markets. Indeed, these differences in the core infrastructural underpinnings of crypto-markets relative to traditional markets shape a role for fair MEV extraction on Ethereum, where one may not exist in the realm of traditional finance. As highlighted in Blockchain Transaction Ordering as Market Manipulation, decentralized marketplaces on the Ethereum Layer-1 blockchain do not enshrine systems of transaction ordering based on send-time, as do the continuous limit order books (“CLOBs”) that are used for electronic trading in fiat markets. There are legitimate reasons for crypto markets opting to reject this approach, given the geographically centralizing practices like colocation which are common in the traditional financial system.

Financial regulators are accustomed to shaping their views through the lens of their familiarity with traditional markets. Alas, MEV does not have a precise analogue in traditional financial markets and so is not subject to the “same risk, same regulation” principle even if regulators were to follow that principle in extending the regulatory

---

4 See, e.g., Auer et al., supra note 1.
5 Mikołaj Barczentewicz, Alex Sarch & Natasha Vasan, Blockchain Transaction Ordering as Market Manipulation, 20 OHIO ST. TECH. L.J. 1, 80 (2023).
6 See, e.g., Eru_Iluvatar, FRP-24 Quantifying MEV on L2s, FLASHBOTS (May 10, 2023), https://collective.flashbots.net/t/frp-24-quantifying-mev-on-l2s/450/33?u%3Deru_iluvatar&sa=D&source=docs&ust=1689633645999717&usg=AOvVaw2YRxBIBwqXUwKdBLkMQclP [https://perma.cc/X7RN-ES2Q]. It is notable that layer 2 rollups are not an effective mitigant for MEV extraction.
perimeter over blockchain-related activities. Blockchain-based markets often do not operate under the same assumptions (i.e., first-in-time based transaction ordering) as traditional markets, so behavior that may be deemed manipulative in the latter may not necessarily be so in the former. Furthermore, the broad range of practices that fall within the category of “MEV extraction” vary in their market effects, with even the most harmful of these practices potentially generating positive externalities worthy of greater study.  

In this response to the work of Barczentewicz, Sarch, and Vasan, I will draw on the regulatory principle of proportionality to argue that, although some forms of MEV give rise to legitimate concerns, regulatory intervention is an inappropriate response to address even the most harmful of these practices—that is, MEV sandwich attacks.

Financial markets are extremely sensitive to regulatory intervention, and the real market consequences of any regulatory measure must be weighed in relation to the harm sought to be addressed. While a trading practice may generate some negative externalities—for instance, through rent extraction—it should not be subject to an ex ante regulatory intervention if the enforcement and compliance costs or negative impacts on market structure (e.g., through reduced liquidity) associated with such a prohibition exceed the harms of not implementing such an ex ante regulatory intervention. Within such a proportionality framework, reliance on ex post deterrents to the activities at issue, as well as mitigants arising from competitive market discipline, technology, and other adaptations to the activities at issue should also be incorporated. In short, ex ante regulation of validators would only be appropriate where it is net socially beneficial.

The Commodity Futures Trading Commission’s (“CFTC”) approach to regulating the negative externalities caused by “predatory trading” (also referred to as market-maker frontrunning) is exemplary here.  

---


10 Igor Makarov & Antoinette Schoar, Cryptocurrencies and Decentralized Finance, BANK FOR INT’L SETTLEMENTS 40–41 (2022) (“A natural place for regulatory oversight in this new ecosystem is at the level of developers and validators, which in turn control the network protocol.”).

trading in market making in swaps, the CFTC applied the principle of proportionality to determine that the costs of effectively enforcing a prohibition on predatory trading would have been disproportionate to the market benefits engendered by such a measure. Thus, rather than banning outright this ubiquitous but facially “manipulative” activity, the CFTC opted instead to pursue a less intrusive approach that limited access to the practice by limiting transparency in the market with respect to the information that enabled dealers to effectively frontrun a market maker’s need for liquidity. An explicit prohibition on this activity would have had a large deterrent effect on market making, resulting in a net negative social impact on markets.

In this Response, I will argue that MEV sandwich attacks pose at worst a similar problem to predatory trading, such that application of the principle of proportionality would lead to a parallel outcome (at least with respect to the current extent of sandwich attack occurrences). While sandwich attacks may cause—albeit expected and transparently measurable—harm to users of the Ethereum network, a blanket ban on MEV sandwich attacks would be disproportionate to the effects of such a measure as its enforcement would frustrate and, potentially, prohibit the success of the burgeoning digital asset industry in the United States. Thus, I posit that a better approach may turn on public-private discourse to promote the development of the already vibrant ecosystem of private sector solutions which—like the CFTC’s response to predatory trading—work to rid the market of the harms associated with sandwich attacks by cutting off access to their execution (i.e., by limiting market transparency). In addition to the rise of private market-led adaptations like Flashbots Protect, the looming risk of ex post regulatory interventions will increasingly deter large-scale MEV sandwich attacks as more of the decentralized ecosystem moves into the regulatory perimeter in the U.S. and beyond.

My Response proceeds as follows. In Section II, I will describe the regulatory principle of proportionality and its application in the context of ostensibly manipulative market practices, using predatory trading as a case study. In Section III, I will then provide background on MEV sandwich attacks and outline their positive and negative effects on the Ethereum marketplace, mindful of the current private sector efforts to limit the availability of sandwich attack opportunities. Section IV will synthesize the aforementioned concepts, using the principle of proportionality to argue that a regulatory prohibition on MEV sandwich attacks as illegal market manipulation would lead to a net negative social outcome. Additionally, Section IV will explore the appropriate
role of public-private dialogue in mitigating the negative externalities of sandwich attacks. Section V concludes.

II. PROPORTIONALITY + MARKET MANIPULATION

A. Background on Proportionality

“Do no harm” is a fundamental pillar in the realm of financial regulation.12 While financial regulatory authorities around the world seek to promote financial stability, market integrity, and consumer protection, regulation that overly interferes with the free functioning of the financial system may work against the attainment of these goals by “unduly constraining [a market’s] development, curbing competition or limiting the diversity of market participants.”13 Thus, rationales for implementing aggressive regulatory approaches against financial institutions and market participants must be hedged against the potential ramifications to long-term market health that may arise from such interventions.

The concept of “proportionality” has long codified this notion in the realm of global banking supervision, with the Basel Committee on Banking Supervision (“BCBS”) explicitly referencing proportionality in its Core Principles for Effective Banking Supervision14 and the Bank for International Settlements (“BIS”) highlighting the central role of proportionality in bank regulation and supervision.15 Yet, the utility of the principle of proportionality in regulatory analyses is not limited to the banking sector. Proportionality is ubiquitous as a force against over-regulation in the European Union, where a general guiding principle is

12 The principle is derived from the Hippocratic Oath which has its origins in the Greek physician Hippocrates principle that physicians should “make a habit of two things: to help, or at least do no harm.” See, e.g., Kenneth Lecroy, The Lie of Primum non Nocere, AM. FAMILY PHYSICIAN (Dec. 15, 2001), https://www.aafp.org/pubs/afp/issues/2001/1215/p1942.html [https://perma.cc/ADW6-F8TA].
15 Rostoy, supra note 13 (“In regulation, a proportionate approach means tailoring regulatory requirements to a firm’s size, systemic importance, complexity and risk profile . . . [i]n supervision, proportionality has a somewhat different focus: the main aim is to facilitate the efficient allocation of scarce supervisory resources and supervisory activities on firms that are either systemically important or are considered high risk”).
that all policy-imposed restrictions of rights must “not impose a burden on the individual that is excessive in relation to the objective sought to be achieved.”

16 In the United States, the statutory requirements on market regulators like the Securities and Exchange Commission (“SEC”) and the CFTC to engage in cost-benefit analyses prior to rulemaking are tantamount to “proportionality” by another name.17

This is all to say, the notion of proportionality offers a tried and tested tool to evaluate the appropriateness of regulatory action. I am not the first to argue in favor of the application of proportionality in the context of financial innovation,18 where it is nowhere more obvious how the potentially boundless upside of flourishing private sector efforts can be prohibitively stifled through early and overzealous regulatory intervention.

B. The Importance of Proportionality in the Law of Market Manipulation

The best (and, most likely, only) way to create a market totally free from fraud and manipulation is to shut down that market entirely. Yet, of course, such an approach would eviscerate all social and financial benefits offered by that market in the process. Thus, the law of market manipulation boils down to a matter of tradeoffs: because all potentially harmful market practices cannot be banned in a reasonably free and active market, the regulatory tool of proportionality is used—

---


18 See, e.g., Kern Alexander, Financial Inclusion and Banking Regulation: The Role of Proportionality, 84 L. & CONTEMP. PROBS. 129 (2001) (assessing “how the principle of proportionality can be applied to balance the risks associated with fintech innovations to promote financial inclusion, while not undermining other regulatory objectives”).
often implicitly—to determine when and in what circumstance a trading practice crosses the line from legitimate to manipulative.

In my time at the CFTC, I had the privilege of co-leading a rulemaking to designate a block size threshold for swaps at which a swap would be too large to be cost-efficiently exposed to the broader market.\textsuperscript{19} One core purpose of this rulemaking was to address the harmful market externalities of “predatory trading”—also referred to as dealer frontrunning—wherein the public disclosure of information regarding a large swap transaction alerts the market to the corresponding market maker’s (i.e., the swap counterparty) demand for future liquidity, needed to offset their accommodation of the large swap transaction, leading strategic traders to exact a premium from the market maker by front running them.\textsuperscript{20} One could argue, quite convincingly, that the strategic trader’s reaction to the market maker’s need for liquidity in a predatory trading scheme constitutes market manipulation under CFTC Rule 180.1 or 180.2.\textsuperscript{21} The trader’s front running transaction—that drains liquidity from the market in order to extract a premium from the market maker—could easily be deemed to create an “artificial price.”\textsuperscript{22}

Yet, while the agency very well could have, the CFTC opted not to explicitly prohibit predatory trading as a form of illegal market manipulation, instead addressing the harms associated with the practice through the less invasive regulatory measure of limiting market transparency for large block trades.\textsuperscript{23} The CFTC took the latter approach to predatory trading, rather than the former, because the costs to the market at large of enforcing a prohibition would have led to a net negative social outcome. That is, a prohibition on predatory trading would have required the CFTC to develop some means of distinguishing this practice of frontrunning market makers to extract liquidity from

\textsuperscript{19} See Procedures to Establish Appropriate Minimum Block Sizes for Large Notional Off-Facility Swaps and Block Trades, 78 Fed. Reg. 32870 (May 31, 2013) (outlining the final decision of the CFTC to limit the block size reporting threshold for large swap transactions).

\textsuperscript{20} See id. See generally Brunnermeier & Pederson supra note 11, at 1825.

\textsuperscript{21} See Barczentewicz et al., supra note 5, at Section III (giving an overview of commodities market manipulation).


\textsuperscript{23} See generally Procedures to Establish Appropriate Minimum Block Sizes for Large Notional Off-Facility Swaps and Block Trades, 78 Fed. Reg. 32870 (May 31, 2013).
legitimate market making. Inevitably, this would have added frictions to the provision of liquidity in affected markets—i.e., by requiring every market making transaction in the dealer market to be reviewed for compliance—harming market efficiency by decreasing access to liquidity in a manner that the agency deemed disproportionate to the perceived benefits of prohibiting predatory trading. The fact that a blanket prohibition may have eliminated (or, at least, decreased the instances of) predatory trading was outweighed by the commensurate liquidity cost that would have been imposed on the market as a compliance cost of such a regulatory intervention.

As demonstrated by the CFTC’s chosen avenue to regulate the practice of predatory trading, just because a trading practice can be deemed manipulative this does not mean that it should be. The principle of proportionality thus plays a crucial role in the realm of market manipulation by providing a framework to assess whether or not a facially “manipulative” practice should legally be considered so, in light of the sometimes-unbearable costs of heavy-handed market interference.

III. THE COSTS AND BENEFITS OF SANDWICH TRADES IN DECENTRALIZED MARKETS

A. Background on Sandwich Attacks

As noted by Barczentewicz, Sarch, and Vasan, MEV sandwich attacks (also referred to as sandwiches or sandwich trades) “[consist] of three elements: ‘(1) the front-run, (2) at least one sandwiched transaction, and (3) the back-run’”.24 Like predatory traders in traditional finance, sandwhichers exploit the transparency of a market and the sequencing of transactions to shift prices in a manner that is beneficial to themselves, at the expense of another market participant. While predatory traders frontrun market makers to extract a liquidity premium, sandwich traders place their own transactions around a public pending Ethereum transaction to profit from the difference between the execution price a user would receive absent the sandwich and the maximum price a user is willing to pay (i.e., the user’s self-selected slippage limit).25

While it is evident that sandwich attacks cause affected users harm by forcing them to suffer a worse execution price, the aggregate effect of sandwiches on decentralized crypto-markets at large is much

24 Barczentewicz et al., supra note 5, at 21.
25 Id. at 48.
smaller than one may initially perceive. The staunchly negative perception and strong criticisms against the practice by many in the crypto-native community portray sandwich attacks as a large-scale disaster that chronically pervades decentralized markets, and it is this sentiment that regulators have started to latch on to. Yet, the profits extracted through sandwich attacks represent a small percentage of transaction volume in crypto markets—according to a report by Eigenphi, sandwich attackers generated only $128 million in revenue in 2022 (and much less in profits, given that sandwiching searchers paid nearly 79% of their revenue to block builders and validators), while Ethereum on-chain volumes alone exceeded $1 trillion between June 2022 and June 2023. MEV sandwich attacks therefore amount to a vanishingly small rent extraction method.

Further, the detrimental effects of sandwich attacks are not distributed homogeneously across all crypto market participants. As sandwich bots generally target larger trades on decentralized exchanges (“DEXs”), it is likely that only the most sophisticated traders in this market bear the brunt of the harms caused by sandwich attacks. Retail-sized trades are generally too small and therefore too costly to sandwich attack. Given that sandwich attacks likely disproportionately impact only those market participants with the greatest resources, one could view sandwich trades as a progressive tax imposed on highly resourced participants of the decentralized financial ecosystem.

B. Private Sector Mitigants to Sandwich Attacks

While the harms associated with sandwich attacks should not be overlooked, these negative externalities are being successfully mitigated through private sector efforts.

An optimal DEX environment for sandwich attackers exists where: (1) pending swap transactions and pricing information are publicly viewable, (2) slippage limits are wide, and (3) swap transactions are large, creating a significant price discrepancy for sandwichers to exploit. By corollary, access to sandwich attack opportunities can be limited where any condition does not hold. For instance, private companies like Flashbots have developed and made

26 See, e.g., Dan Robinson & Georgios Konstantopoulos, Ethereumb is a Dark Forest, PARADIGM (Aug. 28, 2020), https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest [https://perma.cc/NTG9-349P].
available private RPC endpoints that enable Ethereum users to bypass the public mempool, where their pending transactions are at the highest risk of being sandwiched, and send their transactions privately to certain trusted blockbuilders. Likewise, users can independently set the slippage tolerance of their transaction in such a way as to mitigate the potential for their transaction to be sandwiched. To this end, Lioba Heimbach and Roger Wattenhofer propose an algorithm to aid DEX traders in selecting the optimal slippage limit for their trade that mitigates the likelihood of sandwich attacks, while not posing an unreasonably high risk of trade failure. Lastly, DEX trades become less attractive for sandwichers where they are smaller in volume as such trades will not create as large of a price impact and, therefore, generate less profit for a prospective sandwicher. Accordingly, smart order routing services—like that provided by the DEX aggregator 0x—can split large orders into smaller trades that are then optimally routed to particular trading venues, thereby minimizing the likelihood of sandwich attacks and equipping users with a best execution price.

Each of the described private sector efforts work to minimize the user harms caused by sandwich attacks by changing the characteristics of DEX trades such that they are less likely to be sandwiched. As a result, these solutions address the negative externalities of sandwich attacks without need for external regulatory (or other) intervention.

IV. PROPORTIONALITY ANALYSIS BALANCING THE COSTS + BENEFITS

In this Section, I will argue that the consequences of regulatory intervention to explicitly prohibit sandwich attacks as a specific form of illegal market manipulation would be disproportionate to the risks and negative externalities posed by the practice.

Any domestic prohibition on sandwich attacks would require the direct regulation of searchers, block-builders, and validators (collectively, “MEV extractors”). While there are varying degrees of
strictness with which a regulatory regime prohibiting sandwiching could regulate MEV extractors,\textsuperscript{31} any would impose a cost on domestic MEV extractors that MEV extractors outside of the US—or, at least, in jurisdictions without similar sandboxing bans—would not have to bear. Therefore, it is likely that at least some U.S.-based MEV extractors may move their operations to other jurisdictions where they would be unregulated and permitted to sandwich with impunity, and non-U.S.-based MEV extractors would retain a competitive advantage over any MEV extractors that would opt to remain in the U.S. Cryptocurrency markets are inherently global and operate in a borderless fashion. So, any benefits in terms of decreased user harm from sandwich attacks resulting from a sandboxing ban would be severely muted given the ease with which MEV extractors could avoid regulation by simply operating outside the bounds of U.S. regulation.

Meanwhile, the costs of such a regulatory intervention would be substantial. First, the direct regulation of validators would add friction and compliance costs in the form of controls to reject sandboxing attack-containing blocks that could, on a blockchain such as Ethereum, reduce validator incentives to stake. This would pose a threat to the liveness and censorship resistance of the entire blockchain network, given that “the key issue for the security of a blockchain like Ethereum is whether there is sufficient incentive for independent good-faith validators” to support the blockchain’s “security budget”\textsuperscript{32} Should the Ethereum network face an attack due to the decreased robustness of the network’s security that may arise from a ban on sandwiching, the costs of this to Ethereum users may be even greater than the total aggregate costs of sandwich attacks.

Additionally, direct regulation of actors in a pseudo-anonymous, permissionless blockchain-based market would inevitably be highly costly to enforce. In essence, it would require the CFTC—an already

understaffed and underfunded agency\textsuperscript{33}—to adopt, implement, and continuously oversee an entire new regime of disclosure/reporting, data collection, and, potentially, registration requirements targeted at the rapidly evolving and technically complex blockchain industry.

Finally, regulation of validators—as discussed above—would likely lead to a pattern of regulatory arbitrage that could push cryptocurrency markets overseas and cause the U.S. to lose any semblance of control over the industry’s future. Regardless of one’s views on the utility and desirability of cryptocurrencies (which admittedly is a topic of debate among U.S. domestic policymakers), the offshoring of this multi-billion dollar industry threatens to undermine the United States’ longstanding leadership in technology and financial sectors,\textsuperscript{34} and potentially our geopolitical standing as well.\textsuperscript{35} Other jurisdictions like the European Union and its members, Japan, Singapore, and the United Kingdom, among many others, are constructively engaging with open blockchains of the sort that can create opportunities for MEV sandwich attacks.

The consequences of responding to the harm caused by sandwich attacks to justify direct validator regulation are far too great to justify the intended aim. This is particularly true given the relatively small volume of harm caused by sandwich attacks, in the context of the massive and expanding cryptocurrency ecosystem, and the private sector approaches to limit access to sandwich attacks which are rapidly developing. The presence of sandwich attacks and their harmful effects on cryptocurrency users would not be effectively eliminated through validator regulation, given the fact that non-U.S.-based MEV extractors competing in the same market as domestic MEV extractors would not face the same prohibition. The substantial network security, financial,


and geopolitical costs of a domestic regulatory ban on sandwich attacks are disproportionate to the muted benefits of such a measure.

The analysis for an explicit regulatory ban on sandwich attacks as a form of market manipulation is much the same—at least at the current moment. The negative effect on open blockchain market structure and security outweighs the benefit in terms of reducing a harm that is still relatively insignificant as a percentage of overall open blockchain on-chain transactional volumes. The effect of such a prohibition is comparable to the calculus undertaken by the CFTC when it considered the liquidity costs of a ban on predatory trading (described above) as both actions would impose costs disproportionate to their prospective benefits.

Another approach to the problem of abusive MEV has recently been suggested by the International Organisation of Securities Commissions (“IOSCO”) in a recent consultation entitled “Policy Recommendations for Decentralized Finance (DeFi).” IOSCO suggested that “[r]egulators should seek to hold a provider of a DeFi product or service responsible for identifying and, to the extent practicable, managing and mitigating the impact of MEV strategies used by miners/validators on the underlying blockchain on which the provider chooses to operate or offer the product or service.” IOSCO suggests that the “the design of the trading mechanism could mitigate the impact of MEV to users/investors trading these instruments.” Elaborating on IOSCO’s proposal, a reasonable implementation of this suggestion might subject service providers engaging in discretionary order routing (i.e., “not-held” orders where the service provider’s discretion is used to find most favorable price for the user under the circumstances). A number of DeFi service providers currently use on-and off-chain methods to mitigate MEV exposure and this is increasingly emerging as an area of commercial competition among DeFi service providers. It should be highlighted that such a duty to

36 See INT’L ORG. SEC. COMM’N, POLICY RECOMMENDATIONS FOR DECENTRALIZED FINANCE (DeFi) (2022).
37 Id. at 32–33.
38 See, e.g., Regulation NMS, 70 Fed. Reg. 37496, 37538 (June 29, 2005) (discussing similar duties for securities broker-dealers).
39 Hayden Adams, Introducing the UniswapX Protocol (July 17, 2023), https://blog.uniswap.org/uniswapx-protocol [https://perma.cc/4YAS-7YEY] (“With UniswapX, MEV that would be left on the table to be captured by an arbitrage transaction is instead returned to swappers through improved prices. UniswapX also helps users avoid more explicitly extractive forms of MEV: orders executed with fillers’ inventory cannot be sandwiched, and fillers are incentivized to use private transaction relays when routing orders to onchain liquidity venues.”).
mitigate MEV would not be appropriate for interfaces or service providers that merely transmit order instructions to a specific protocol or liquidity pool, i.e., held or direct orders, because such services do not purport to mitigate transaction costs.\textsuperscript{40}

While I do not foresee a scenario where direct validator regulation would be warranted, there may be circumstances where \textit{ex ante} rules regarding MEV mitigation for discretionary order routing service providers or \textit{ex post} mitigants like a regulatory prohibition in the form of an express designation of sandwich attacks as a form of market manipulation (along with related enforcement action) could be warranted. The three pre-conditions for such a designation would include, first, the implementation of a constructive, global approach to regulating crypto markets, inclusive of open blockchains. A global regulatory framework would enhance the effectiveness of such a ban by providing far more touchpoints for regulators to detect, identify, and deter sandwich attacks, as well as the necessary expertise to bring such cases effectively. Second, in order to justify the costs of such an express prohibition, there would need to be substantial growth by orders of magnitude of sandwich attacks relative to overall on-chain volumes in the most widely used open blockchains.

Lastly, I submit that a final pre-condition would be the demonstrated failure of private sector remedies at mitigating the harm. In the case of both MEV mitigation as a duty for discretionary order routing service providers and an express ban, future regulatory interventions would be more efficient and effective if they are developed with a longer observation of private sector remedies. For example, specific practices adopted by blockbuilders, relayers, or validators\textsuperscript{41} or order routers could inform the specifics of such regulatory actions, enhancing these future regulatory actions’ efficiency and efficacy.

V. CONCLUSION + RECOMMENDATIONS

Decentralized, blockchain-based markets are in their nascency and have yet to develop into a long-term, steady state. The potential for

\textsuperscript{40} In such cases, tailored standardized disclosure of MEV and other material transaction costs could provide benefit for the users of such interfaces in the absence of a duty to mitigate MEV.

these markets to revolutionize the efficiency and inclusivity of the
global financial system is significant, but this technology—like other
global communication protocols such as the Internet—is not free from
opportunities for fraud and manipulation. In reality, no market is. In
considering a regulatory response to the problem of MEV sandwich
attacks, it is imperative that the consequences of regulatory intervention
on the future of this emerging market be taken into account. We can
learn from past agency decisions—like the CFTC’s choice not to
prohibit outright predatory trading—that teach us to proceed with
care when reacting to potentially “manipulative” market behaviors,
rather than immediately pursuing the most intrusive policy outcome.

The CFTC responded to predatory trading by limiting
transparency in swap markets, such that predatory traders no longer had
access to the information they needed to frontrun client orders. In effect,
the CFTC opted to regulate in such a way as to reduce opportunities for
predatory trading, rather than engaging in the more severe measure of
prohibiting the practice, which would have imposed significant frictions
on market makers and, consequently, market liquidity at large.
Likewise, my recommendation to policymakers in addressing the
problem of MEV sandwich attacks is to consider and promote
alternatives to harsh regulation that mitigate the admittedly harmful
negative externalities of sandwich attacks, while not producing the
centralizing, costly, and commercially unfriendly consequences of
direct validator regulation.

The crypto industry is itself currently developing solutions—
some which also operate to decrease market transparency (i.e.,
Flashbots Protect RPC), and others which target transaction
characteristics like slippage limits (i.e., Heimbach and Wattenhofer
algorithm\textsuperscript{42}) and order routing (i.e., 0x Slippage Protection)—to
mitigate the negative externalities of harmful MEV practices like
sandwich attacks, while retaining the role of healthy MEV within the
crypto ecosystem. Like the CFTC’s minimum block size rule, these
private sector solutions limit access to sandwich attacks, reducing the
opportunity surface area for their execution. The continued
development of these private sector solutions has the potential to
effectively mitigate the user harms caused by sandwich attacks (which
it would be the goal of heavy-handed regulation to address), while not
causing the aforementioned problems of direct validator regulation.
Therefore, I argue that the best way forward for policymakers is one
that requires \textit{no ex ante regulatory intervention}, but that simply fosters

\textsuperscript{42} See Heimbach & Wattenhofer, supra note 29.
a constructive public-private dialogue to monitor and facilitate the responsible and effective development of these burgeoning private sector solutions to the problem of sandwich attacks. Finally, the threat of possible enforcement action, even in the absence of an express designation of sandwich attacks as market manipulation or enforcement precedent, provides substantial deterrent value at this current moment.