University of Pennsylvania Journal of Business Law
Vol. 26 (forthcoming 2023)

[This is a draft subject to revision, comments welcome!]

BATTLE OF THE CRYPTO BOTS: AUTOMATED TRANSACTION COPYING IN DECENTRALIZED FINANCE

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

Abstract: *Markets built on public, permissionless blockchains like Ethereum are radically transparent. This creates opportunities and strategies that are rarely, if ever, seen in traditional markets. Among the most interesting but understudied of these is the use of sophisticated algorithms ("bots") to automatically copy and front-run or otherwise exploit other users' trades, as these are typically publicly viewable while they wait to be executed. In crypto markets like Ethereum, Generalized Profit-Seeker (GPS) bots can access publicly available pending orders (blockchain transactions), simulate them to determine if they will be profitable, and copy (or otherwise piggy-back on) those transactions deemed profitable according to the parameters of the bot. Sometimes, this benefits the sender of the copied order—the copier effectively facilitates, even subsidizes, its execution. Other times, the sender of the copied order is blocked from a profit opportunity because the copier manages to get there first, thus making it entirely unavailable or at least less profitable for anyone who comes second. To further complicate matters, such automated "strategy copying" may involve replicating or facilitating criminal or otherwise illicit transactions, such as attempted hacks of blockchain applications or platforms.*

---

† 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 of the issues in this, 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.

This Article explores the legal implications of this type of radical transparency found in crypto markets and offers the first sustained legal analysis in the academic literature of the use of Generalized Profit-Seeking bots in crypto markets. This Article is part of a series on the legality of so-called Maximal Extractable Value ("MEV") extraction techniques, which exploit the ability to order transactions in profitable ways including through the use of GPS bots which are the focus of this Article.

In particular, we argue that, given the public and competitive nature of transaction ordering in crypto markets, the operation of GPS bots to copy profitable transactions submitted publicly is generally unlikely to be a legal violation in run-of-the-mill-cases. However, we highlight several exceptions to this default permissibility, for example where the GPS bot is operated by a validator, or when the bot copies criminal or illicit transactions. The Article provides a technical introduction of transaction ordering and execution on Ethereum to serve as a necessary resource for pressing legal and policy discussions. It then examines relevant U.S. laws governing market manipulation, insider trading, and front-running in securities and commodities markets, and analyzes what these entail for the use of GPS bots in crypto markets. Ultimately, the Article aims to offer guidance to regulators and policymakers, as well as courts and practitioners, on the legality of GPS bots and MEV extraction more generally under U.S. law, as well offering suggestions and questions for further research about how the use of crypto bots should be regulated going forward.

CONTENTS:

I. INTRODUCTION

On 16 June 2022, there was a shootout. It did not involve cowboys quarreling over cattle, but crypto trading bots racing to see who could copy or exploit another Ethereum user's transaction first. To make matters worse, the underlying transaction they were racing to copy, which had been submitted to the publicly viewable mempool where it was waiting to be executed by being built into a block on the blockchain, was itself criminal – a hack of another's system.

What happened was this. The case commenced when someone attempted to exploit Inverse Finance, a decentralized finance application on the Ethereum blockchain, for over $1 million.[1] To do so, the exploiter submitted a set of Ethereum transactions aiming to 'trick' the application.[2] The precise mechanics of this exploit, which if successful would provide unauthorized access to drain Inverse Finance funds, are of little importance here. What is important is that—

[1] Shaurya Malwa, *DeFi Protocol Inverse Finance Exploited for $1.2M*, COINDESK (2022), https://www.coindesk.com/tech/2022/06/16/defi-protocol-inverse-finance-exploited-for-12m/.
[2] *Id.* The exploiter's transactions can be viewed on Etherscan, the Ethereum blockchain explorer: https://etherscan.io/tx/0xfb5a4d1aef98458f673f301c2e713613662ad621e8f57065a4da58a6401c0b4d (creating a contract) and https://etherscan.io/tx/0x958236266991bc3fe3b77feaacea120f172c0708ad01c7a715b255f218f9313c (calling on that contract).

probably unbeknownst to the exploiter—the second of their transactions was spotted while it was still pending by at least two "MEV searchers", most likely automated bots watching the pool of all pending transactions for profit opportunities.[3] Both searchers learned—through simulation—what will be the economic effect of that transaction and realized that the transaction (1) will make a great deal of money to whoever is set as the beneficiary of the transaction and (2) will create price imbalance across blockchain exchanges, creating an opportunity for a riskless arbitrage (buy low on one exchange, sell high on another).[4]

Because the code of the exploiter's two transactions was public, one of the searchers—we'll refer to them using the first characters of their Ethereum address: 0xFD3—copied the code and submitted their own two transactions, identical except for the fact that the searcher set herself as the beneficiary—thus "aiming" to capture the profits from the exploit.[5] (Importantly, the human operator behind 0xFD3 was likely unaware that any of this was happening: at most she was aware of a likelihood that something like this may happen.) To ensure that the copycat transaction will execute ahead of the copied transaction, 0xFD3 attached a very high transaction fees totaling over 6 ETH (over $6,000) for the miner.[6] Those fees were much higher than the transaction fee set by the exploiter, so 0xFD3's transactions had a good chance to be executed ahead of the exploiter's main transaction. Had 0xFD3 succeeded, she would have "deprived" the exploiter of their illicit gains, realizing them herself. However, 0xFD3 failed.

0xFD3 failed, because the second searcher, 0xEef, offered a much higher transaction fee to the miner than 0xFD3—almost $100,000—to ensure that the exploiter's transaction gets executed. This way, 0xEef was instrumental in the exploiter's successful attack on Inverse Finance. Why would a stranger pay so much to ensure execution of someone else's trade? 0xEef did so to realize the other profit opportunity created by the exploit transaction: the arbitrage.[7] And,

---

[3] @MevRefund, Twitter (Jun. 16, 2022) https://twitter.com/MevRefund/status/1537421091697836032

[4] Such strategies are normally considered to be riskless, but a recent action of a "rogue" Ethereum validator illustrated that there may be code vulnerabilities or ecosystem participants who break the implicit trust arrangement; *see infra* notes 31-32 and the accompanying text.

[5] 0xFD3's transactions on Etherscan: https://etherscan.io/tx/0xdefd26033d38e1e48a15aeab790fb7481b4d8c8ca3832ff99cac178d21327f5d and https://etherscan.io/tx/0x111e5fe228576359aeb650f52e7493b030c91f3ae9077f5e9e638edf159cfa8d. *See also* Etherscan's "similar contracts" analysis showing an exact match between the exploiter's contract and 0xFD3's contract: https://etherscan.io/find-similar-contracts?a=0xf508c58ce37ce40a40997C715075172691F92e2D&lvl=5.

[6] *Id.* Transactions are usually ordered through an auction of fees, *see* Section II.

[7] 0xEef's transaction on Etherscan: https://etherscan.io/tx/0xfa15c45e5d9f7fdc2a32de50f03cbf0a9d678eac87c71e630fc2afc552d3e6bd.

in fact, 0xEef profited over $111,000, despite the high fee.[8] The mechanism through which 0xEef was able to pay a fee to advantage someone else's transaction is known as "bundling" and is also a form of copying of transactions.[9] However, in bundling, the copier does not make any changes to the copied transaction, they only copy it into a "bundle" containing also the copier's own transactions and pay for privileged execution of the whole bundle.[10] In this case, the 0xEef's reason to bundle the exploiter's transaction was that the imbalance across markets created by the exploit was about to create a very competitive and lucrative arbitrage opportunity. To profit from such an arbitrage it is essential to have one's trades executed as closely as possible after the transactions that create the imbalance across markets. Hence, it was worthwhile for 0xEef to facilitate the exploit by bundling it with 0xEef's own "back-running" arbitrage, because this way 0xEef made sure that (1) the exploit created a market imbalance and that (2) it was 0xEef who profited from that imbalance through arbitrage.

The tactics of searchers like 0xFD3 and 0xEef are widespread in the Ethereum's decentralized finance ("DeFi") ecosystem, so much so that a vibrant body of game-theoretical and empirical research exists unpacking their implications.[11] What 0xFD3 and 0xEef were attempting to do is *extract Maximal*

---

[8] See EigenPhi's analysis: https://eigenphi.io/mev/ethereum/tx/0xfa15c45e5d9f7fdc2a32de50f03cbf0a9d678eac87c71e630fc2afc552d3e6bd.

[9] Mikołaj Barczentewicz, Alex F Sarch & Natasha Vasan, *Blockchain Transaction Ordering as Market Manipulation*, OHIO STATE TECHNOLOGY LAW JOURNAL (forthcoming), https://ssrn.com/abstract=4187752.

[10] *See Id.* Note that when bundling, the copier puts the copied transaction in a set with at least one other transaction, which will provide payment to the validator (at that time: the miner), and then strike a deal with the validator (the miner) through intermediaries (now: block-builders and MEV-Boost relays, then: the old Flashbots MEV-Geth relay) that if the miner accepts the fee, then they will successfully execute the transactions from the bundle exactly and do so in the desired order. *See also infra* Section II.A.

[11] *See, e.g.,* Philip Daian et al., *Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges*, (2019), https://arxiv.org/abs/1904.05234; Liyi Zhou et al., *High-Frequency Trading on Decentralized On-Chain Exchanges*, *in* 2021 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) 428 (2021), https://ieeexplore.ieee.org/document/9519421; Kaihua Qin et al., *Attacking the defi ecosystem with flash loans for fun and profit*, *in* INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 3 (2021); Liyi Zhou et al., *Sok: Decentralized finance (defi) attacks*, CRYPTOLOGY EPRINT ARCHIVE (2022); 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); 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; 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).

Extractable Value (MEV), formerly called Miner Extractable Value.[12] Because it had occurred through on-chain transactions, the Inverse Finance exploit would become codified as part of Ethereum's future state as one transaction within the ordered series of transactions called a *block*. Actors called "validators" (formerly "miners") have the power to determine the order of transactions within blocks, and they do so based on user-specified transaction fees which the validators pocket as additional rewards for assisting in the process of transaction validation on Ethereum's proof-of-stake consensus mechanism.[13] Both 0xFD3 and 0xEef were competing—based on transaction fees—to have their transactions executed in strategic positions relative to the exploit transaction. Ultimately, it was 0xEef who won, while effectively assisting the Inverse Finance exploiter.

Nearly $700,000,000 in profits have been accrued through the extraction of MEV on Ethereum.[14] This category of crypto-native, order-based trading strategies has not escaped the attention of policymakers. While MEV extraction has been occurring for nearly as long as the Ethereum ecosystem has been in existence—that is, nearly eight years—only over the past year have financial regulators globally started to acknowledge these practices.[15] Yet, the language and context in which these regulators have contemplated MEV extraction reflects a lack of understanding regarding the role and economic realities of MEV extraction in blockchain markets. That is, policymakers seem to view MEV inherently and collectively as illicit, categorizing MEV generally as a form of "market-manipulation",[16] and resorting quickly to labels such as "insider trading," "front-running," and "fraud" to categorically describe what is really a

[12] In this Article, we focus on MEV extracted in the Ethereum ecosystem. Yet, the phenomenon of MEV extraction is common to many other blockchain networks (i.e. Solana, Cosmos, etc.), and much of our legal analysis is likely to apply equally to MEV extraction on those other chains.

[13] In traditional finance, transactions are ordered continuously (at least, during the course of the trading day) on the basis of user-send time, so order-based trading strategies analogous to MEV extraction generally do not occur in the absence of illegal front-running or insider trading. Transactions on Ethereum, on the other hand, are ordered in discrete batches – blocks – according to the self-interested discretion of validators. This difference in the transaction ordering specifications of blockchain-based networks like Ethereum, compared to that of traditional finance, engenders a novel arena of trading practices, market norms, and legal/ ethical questions which it is our purpose in this Paper to investigate.

[14] *See* https://explore.flashbots.net/. Note that MEV is also extracted on other blockchains like Solana, Cosmos, and BSC.

[15] *See, e.g.,* 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; 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.;

[16] Auer et al., *supra* note 15.

broad, nuanced class of trading practices.[17] This Article aims to serve as a partial corrective to such views. We suspect these mischaracterizations may arise as policymakers have not had the benefit of sustained legal analysis of these issues and therefore tend to view MEV extraction through the normative lens of traditional finance. However, MEV, including the use of MEV bots like those sketched above, are inherently a blockchain-based phenomenon native to decentralized financial markets (DeFi), and thus must be analyzed in terms of their actual workings in order to correctly understand their legal status under existing securities and commodities laws.

What is essential to understand for a proper legal analysis of MEV bots like the above is that crypto markets work differently than traditional financial markets. This Article is thus part of a series of papers exploring how such differences generate sometimes counter-intuitive legal results, particularly where expectations from traditional finance do not carry over to the distinctive workings of crypto markets. In a companion piece, we explored the legal implications of a validator-proposer's market power to order Ethereum transactions as they please, including to carry out a common MEV extraction strategy known as "sandwich attacks."[18] This Article explores the implications of a distinct feature of crypto markets: *their radical transparency*. In DeFi, orders to trade assets are virtually always known to some other market participants, and often constitute public knowledge. Because pending transactions on Ethereum can be publicly viewable, a cottage industry has arisen of sophisticated users building generalized bots which scan transactions in the public mempool, simulate them to determine their profitability, and copy (or otherwise piggy-back on by accelerating their execution) those transactions deemed sufficiently profitable according to the bot's parameters. Sometimes, this is beneficial to the original sender of the copied order—the copier effectively facilitates, even subsidizes, its execution. Other times, the sender of the copied order loses out on a limited profitable opportunity because the copier manages to benefit from the opportunity first, thus making it unavailable, or at least smaller, for anyone who comes second.

We call these bots *Generalized Profit-Seekers*—or *GPS bots* for short. They come in many varieties and carry a wide range of novel legal risks depending on how they operate, which transactions they copy or accelerate, whether these underlying transactions themselves are illegal, and whether the operator of the GPS bot is aware of the illicit nature of those underlying transactions.

Such "strategy copying" trading patterns by GPS bots raise novel legal questions and ethical issues, which it is the aim of this Article to explore. First

---

[17] 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, *supra* note 15 at 37; U.S. TREASURY DEPARTMENT, *supra* note 15 at 36; Auer et al., *supra* note 15.;

[18] Barczentewicz, Sarch, and Vasan, *supra* note 9.

and foremost, we address the question: Can it ever be legal to *copy* other people's transactions? We argue that, given the novel publicness and competitive ordering mechanisms native to crypto markets, the operation of GPS bots to copy or exploit profitable transactions devised by other users submitted publicly (that is, via the mempool) is *generally* not likely to amount to a legal violation given the distinct way that crypto markets operate. Yet, we also demonstrate several important exceptions to this general rule, including where: 1) the GPS bot is operated by a validator/block producer who use their ability to order transactions in order to profit for themselves through strategy copying, 2) cases in which the GPS bot copies *explicit private order flow* (i.e. non-public mempool transactions), and 3) cases in which the GPS bot copies criminal or otherwise illicit transactions where the GPS bot operator is aware of a substantial risk that this is happening. In such cases, plausible theories of liability exist under which the GPS bot operator is likely to have committed a violation that could be pursued by regulators or prosecutors.

The Article proceeds as follows. Section II explains the technical background necessary for a legal understanding of strategy copying on blockchain networks. We introduce the process of transaction ordering and execution on Ethereum and explain how the mechanisms inherent in that process give rise to two main forms of strategy copying: *generalized front-running* and *transaction bundling.* We also provide a high-level overview of Maximal Extractable Value ("MEV") extraction more generally, identifying some of the core MEV profit-making strategies, which may be implemented with the use of techniques like generalized front-running or bundling. In Section III, we introduce the arenas of U.S. law most relevant to our analysis, focusing on the laws governing market manipulation, insider trading, and front-running in securities and commodities markets. We highlight the *moralized,* normatively influenced nature of legal reasoning in this context which guides the application of market manipulation laws.

Section IV applies the legal and regulatory frameworks sketched in Section III to the technical phenomena of Ethereum-native transaction copying described in Section II. We begin by analyzing a simple case of strategy copying, where the transaction copied is a legal, public transaction and the copier is a searcher who is not also a validator-proposer. Grounding our argument in the longstanding property law canon that the law does not "protect the chase,"[19] as well as the publicness and highly competitive nature of DeFi markets, we conclude that market manipulation liability is unlikely to be imposed in a general case of strategy copying. We then address several exceptions to this general rule. First, we note that a strategy copier who is also a validator-proposer may face market manipulation liability due to her exploitation of a position of control over transaction ordering. Next, we discuss the case where the copied transaction is sent through a private channel intended to bypass the public mempool. We find

[19] Pierson v. Post, 3 Cai. 175 (N.Y. Sup. Ct. 1805).

that market manipulation and insider trading liability may be possible for a recipient of such private order flow who, in violation of a relationship of trust with the sender, copies the private transaction and/or discloses it to another actor who copies it. Finally, we return to the fascinating shootout between 0xFD3 and 0xEef in their pursuits to reap the profits of the Inverse Finance hack. We investigate the risk of liability for a bot operator (like 0xFD3, had she succeeded) whose bot copies and front-runs an illicit transaction, finding that such a bot operator can be held liable in certain instances for the offense involved in the underlying illicit transaction, though this will depend largely on the bot operator's mental state as to the illicit nature of the copied transaction. We conclude the Section by arguing that a bot operator (like 0xEef, who succeeded) who boosts and back-runs an illicit transaction is a likely target for market manipulation liability due to their role in facilitating and profiting from the arbitrage opportunity created by an illicit transaction.

Section V concludes by offering recommendations for policymakers and raising questions for further research that is urgently needed to properly tackle the quickly growing phenomenon of GPS bots in crypto markets.

II. TECHNICAL BACKGROUND: MEV EXTRACTION AND TRANSACTION COPYING

Copying of blockchain transactions, including DeFi trades, is possible and profitable due to unique characteristics of blockchain networks. We explored many of those features in depth in the companion article.[20] We did not, however, focus there on transaction copying, and thus our legal analysis in this paper requires additional investigation into the technical and economic aspects of MEV extraction and DeFi trading. In this section, we will briefly recount the general features of MEV extraction, while focusing more closely on the aspects of transaction copying, which we have not covered elsewhere.

A. Blockchain Transactions: Why is Transaction Copying Possible?

In a most general sense, transaction copying is made possible by the fact that other traders have access to pending transactions, *i.e.,* transactions which are not yet executed by being added to the blockchain. But to understand how this is possible, we first need to consider: *what is a blockchain transaction?* A blockchain transaction is not necessarily a transaction in a financial sense. It is an instruction to change the state of the blockchain submitted by a user and then included in a blockchain "block". For example, to reduce the amount of ETH

[20] Barczentewicz, Sarch, and Vasan, *supra* note 9.

(Ether, the native token of the Ethereum blockchain) in one account and to add the same amount to another account. But it can also be an instruction to update some information stored on the blockchain, like meta-data associated with an Ethereum-based domain name.[21]

Such instructions may include analogues to orders to trade assets in traditional markets. However, in a potentially confusing twist, a blockchain transaction may at the same time constitute an order *and* a trade (transaction in a financial sense). This is because DeFi markets tend to be automated and operate as "smart contracts", *i.e.,* software deployed on a blockchain, which anyone can use without asking for permission: simply by submitting a valid instruction. So, a blockchain transaction with a valid instruction to trade (an order), ends up also being the trade itself. But it only becomes a trade when it is included in a block. Until that moment, a pending transaction is akin to a cancellable order.

As we discussed extensively elsewhere, the contents of pending Ethereum transactions are currently always known to at least some other actors than the user who submitted a transaction.[22] Because users submit transactions from their wallet software to specific servers, known as RPCs[23], operators of those servers initially have exclusive knowledge about pending transactions, thus potentially possessing material non-public information. We considered the legal consequences of that elsewhere.[24] Some transactions remain private information until they are included on the blockchain, but many become public information by being transmitted among computers acting as "nodes" of the Ethereum's peer-to-peer network. By being transmitted this way, transactions make their way to block producers (like validators) who include those transactions in blocks.

Each of the computers acting as nodes of the Ethereum network keeps a list of pending transactions, which were transmitted to this node. This list is known as the node's "mempool" (or "transaction pool").[25] Given that information about a pending transaction propagates from node to node in a peer-to-peer way, some nodes learn about pending transactions faster than others. Due to geographic distances and other network issues, it may even happen that a transaction will be included on the blockchain faster than the information about it being pending reaches some nodes. Thus, even though it is common to do so and we also do so below, it is a simplification to speak of "the mempool" as a

---

[21] *See, e.g.,* Ethereum Name Service (ENS) Documentation, https://docs.ens.domains.

[22] Mikołaj Barczentewicz, *MEV on Ethereum: A Policy Analysis*, INTERNATIONAL CENTER FOR LAW & ECONOMICS WHITE PAPER 2023-01-23 (2023), https://ssrn.com/abstract=4332703; Barczentewicz, Sarch, and Vasan, *supra* note 9.

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

[24] Barczentewicz, Sarch, and Vasan, *supra* note 9.

[25] *Id. See also* Blocknative, *What is the Mempool?*, Blocknative (2020), https://www.blocknative.com/blog/mempool-intro [https://perma.cc/P3ND-F94N].

set of all pending Ethereum transactions. There are many mempools and their contents are not perfectly synchronized. No single actor has a "god's eye" view of all pending transactions. Nevertheless, when a transaction is in someone's mempool, it means that this actor can copy the transaction in either of the two ways we consider below.

We are concerned here with two kinds of transaction copying, both of which were illustrated in the example with which we began the paper: (1) copying done by "generalized front-runners" (like the first searcher, 0xFD3) and (2) copying involved in "bundling" (exemplified by the second searcher, 0xEef). We begin with the latter.

1. Copying by bundling

To understand bundling and its rationale, it is useful to consider the concept of "atomicity".[26] "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.[27] This can also be achieved for *a sequence of transactions*, if they are submitted as a "bundle" to a block producer who provides this guarantee for bundles. Atomicity can imply a certainty of profit from resources expended, which mitigates risk and increases the competitiveness of a profit-making opportunity.[28]

Bundling multiple transactions with a guarantee of atomicity is not a core feature of the Ethereum protocol. It is made possible by a voluntary arrangement between various operators in the Ethereum network, initially developed by the Flashbots organization and currently requiring the use of MEV-Boost software (by validators) or the use of software that interoperates with MEV-Boost (by "relays", and then—indirectly—by "block builders").[29] However, this arrangement is extremely popular: over 90% of new Ethereum blocks are currently produced through it.[30]

Using bundling is normally considered to be riskless because of the advertised atomicity guarantee. However, recent events illustrated that this assumption may not hold if there are code vulnerabilities in the bundling system or if one of the trusted ecosystem participants decides to breach the trust placed on them. A validator participating in the MEV-Boost scheme effectively

[26] *Id.*

[27] Daian et al., *supra* note 11 at 4.

[28] *Id.* at 2.

[29] *Introduction - What is MEV*-Boost, Flashbots Docs, https://docs.flashbots.net/flashbots-mev-boost/introduction.

[30] *See* Anton Wahrstätter, https://mevboost.pics.

"unbundled" transaction batches in a block that was submitted to this validator, who was thus able to profit $20 million at the expense of users who expected the atomicity guarantees to hold.[31] What strengthens the case that the validator breached the conditions of the arrangement in which they participated, is that the validator committed a "slashable offence", which resulted in their staked 32 ETH being deleted (around $53,000—much less than the profit they realized).[32]

As illustrated by the strategy chosen by 0xEef, the second searcher from the introductory example,[33] copying by bundling involves three steps: (1) identifying another user's pending transaction to be copied, (2) preparing at least one new transaction, at minimum to provide fee payment for the bundle, (3) preparing and submitting an instruction to execute transactions from steps (1) and (2) as a bundle, while offering the payment specified in (2). As was also well-illustrated by the introductory example, if the fee offered by the bundle author is attractive enough to the block producer (in particular: if the fee is higher than fees offered by other bundle authors) and the transactions in the bundle are viable,[34] then the bundle is very likely to be executed successfully.

Trading ahead and trading behind. Among the main techniques that bundling is used for are so-called "front-running" and "back-running". As we discussed elsewhere, this choice of words is unfortunate, because "front-running" has a technical legal meaning, likely to refer to only one of many situations described as "front-running" in DeFi.[35] To avoid such unnecessary confusion we will generally refer to "trading ahead" and "trading behind". What is important for us here, is that trading ahead and trading behind other transactions creates opportunities for profit. We consider the economic nature of those opportunities below.[36] In the introductory example, the second searcher—0xEef—used bundling to trade immediately behind ("back-run") a transaction creating a price imbalance across markets.

---

[31] Vishal Chawla, *Ethereum MEV bots lose over $25 million in sophisticated attack*, THE BLOCK, April 3, 2023, https://www.theblock.co/post/224482/ethereum-mev-bots-lose-over-25-million-in-sophisticated-attack. *See also* @BlockSecTeam, Twitter (Apr. 3, 2023), https://twitter.com/BlockSecTeam/status/1642971478458249227; Robert Miller, *Post mortem: April 3rd, 2023 mev-boost relay incident and related timing issue*, COLLECTIVE.FLASHBOTS.NET, April 4, 2023, https://collective.flashbots.net/t/post-mortem-april-3rd-2023-mev-boost-relay-incident-and-related-timing-issue/1540.

[32] @mikeneuder, Twitter (Apr. 3, 2023), https://twitter.com/mikeneuder/status/1642899865288994816

[33] *See supra* Section I.

[34] Due to the guarantee of atomicity, if any of the bundled transactions would have failed to execute successfully, then the bundle is not going to be included on the blockchain. This avoids the standard situation, where a transaction is included on the blockchain—thus incurring transaction fees—but fails (is reverted), for example, because there is an error in its code, or because it contains an instruction to execute a trade at outdated prices (*e.g.,* to sell an asset for more than a market is now willing to pay).

[35] Barczentewicz, Sarch, and Vasan, *supra* note 9. *See also* Mikołaj Barczentewicz (@0xMikolaj), Twitter (Jan. 31, 2023) https://twitter.com/0xMikolaj/status/1620356686174392321.

[36] *See infra* Section II.B.

Bundling was a very effective tool for 0xEef for several reasons. First, bundling guaranteed that 0xEef's arbitrage trade will *execute immediately behind* the transaction creating market imbalance, hence no one else will be able to benefit from (and thus reduce) the arbitrage opportunity ahead of 0xEef. Second, even though 0xEef offered a very high transaction fee (over $100,000), bundling guaranteed that 0xEef will only pay that fee if she makes the profit she expected to make—the strategy was thus virtually *riskless* for 0xEef.[37] Third, bundling currently comes with promises of transaction privacy, so unlike the exploiter's trade, the only other market participants who had information about 0xEef bundle were the ones who at least implicitly promise not to copy or trade ahead ("unbundle") 0xEef's transaction.[38]

2. Copying by generalized front-runners

While bundling involves copying of a transaction into a bundle, and thus facilitating the execution of the copied transaction, generalized front-running has been labelled as "destructive" of the copied transaction.[39] In a sense, a generalized front-runner does not copy a whole transaction: they only copy its code (its logic), while creating a new transaction from the front-runner's own account. Such actors are known as "front-runners" because they aim for their copycat transactions to be executed ahead of the copied transactions—usually causing copied transactions to fail, because the copy fully realizes a limited profit opportunity. As we mentioned earlier, the label "front-running" is unfortunate because it creates an unwarranted connection with a technical legal term, which may only sometimes be applicable here.[40] However, the label "generalized front-runners" is so entrenched that we believe that it would add even more confusion to jettison it. That said, we believe that it would have been better to adopt a label like, for example, "generalized (transaction) copiers".

Generalized front-running is a practice primarily used by automated bots. These bots monitor the mempool(s), looking for pending trades that, if executed, would immediately generate a profit for the user who submitted the pending trade. The generalized front-running bot then copies the profitable pending transaction and submits its own version, while offering a higher transaction fee. Theoretically, generalized front-runners could submit their transactions privately, using the same out-of-protocol arrangement that is used for bundling (currently: MEV-Boost), but in practice we often observe that they choose not to. Instead, they offer higher "gas prices", which is the standard way of paying

[37] *See supra* notes 31-32 and the accompanying text.
[38] This implicit promise is not currently enforced by software, but by the risk of a boycott and other adverse reactions by other market participants if it had become known that one of the trusted intermediaries ("block-builders", "relays") engaged in such behavior. *See supra* notes 31-32 and the accompanying text.
[39] Qin, Zhou, and Gervais, *supra* note 11 at 7.
[40] *See supra* note 35 and the accompanying text.

transaction fees, but comes with risk: the fee will be paid even if transaction fails to return profit. This is what the first searcher from our introductory example—0xFD3—did and that choice costed them over $6,000, despite not making any profit. One possible reason why generalized front-runners do not submit their transactions privately is that, fearing legal liability, they believe that they can better protect their anonymity by not interacting with providers of private transaction relaying services.

Generalized front-running bots do not seek out a specific type of transaction to front-run, but instead target all transactions that they determine – by simulating the change in blockchain state resulting from the execution of the pending transaction – have a high probability of generating immediate profits for the transaction originator.[41] Thus, the descriptor *generalized* is appropriate. Because generalized front-runners do not discriminate in their activity based on anything other than local profitability, their impact extends beyond DEX trades to centralized exchanges, derivative protocols that rely on oracle price updates,[42] and non-fungible token purchases. In essence, generalized front-runners profit by mimicking profitable pending trades submitted to the mempool by other traders in order to capture the profits that those other traders would have made.

B. MEV Extraction: Why is Transaction Copying Profitable?

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.[43] 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.

Transaction bundling and generalized front-running are among technical methods used for MEV extraction. Economic strategies for profit-making

---

[41] 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.

[42] *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.

[43] 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*.

through MEV extraction are as varied as opportunistic trading practices in traditional finance. Out of this great variety, several main identifiable categories of MEV extraction strategies have been the most studied and discussed. Nearly all those prominent categories may involve either bundling or generalized front-running. Here we give a very brief overview of those strategies.

DEX arbitrage. Arbitrage across markets is likely the most economically prominent and the most common MEV extraction strategy. As discussed above, the second searcher from our introductory example—0xEef—used transaction bundling to execute a very profitable arbitrage across on-chain markets, *i.e.,* decentralized exchanges (DEX-es). DEX arbitrage constitutes MEV because arbitrage opportunities are usually very competitive, and whoever ultimately controls the inclusion and ordering of transactions in a block, is in a privileged position to profit (extract value) from the arbitrage opportunity.

CEX/DEX arbitrage. The other main kind of arbitrage involving on-chain markets is arbitrage where a part of the strategy involves trading on an off-chain market—a centralized exchange (CEX)—like Binance or Coinbase.[44] We are not aware of specific examples of bundling or generalized front-running being used for CEX/DEX arbitrage, but this is not impossible.

Sandwiching.[45] Sandwiching is probably the most discussed MEV extraction strategy,[46] and it is arguably the paradigmatic MEV strategy. 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, for example, buy an asset at a lower price (the front-run), then allow the sandwiched transaction to raise the market price, and then profit from selling the asset at a higher price (the back-run). Transaction bundling is widely used for sandwiching because it is the only way for a sandwicher who is not the block producer to execute sandwiches without any financial risk. The adverse price effect of the front-run part of a sandwich on the sandwiched transaction is among the main reasons why many object to this practice. In the companion article we have analyzed the legality of sandwiching in depth.[47]

---

[44] Price discrepancies arise also between centralized crypto exchanges (CEX; *e.g.,* Binance, Coinbase, Kraken) and DEXs; *see* Amber Group, *Extractable Value*, AMBER GROUP (2022), https://medium.com/amber-group/extractable-value-7b0d4356a843.

[45] For an extensive discussion of sandwiching, *see* Barczentewicz, Sarch, and Vasan, *supra* note 9.

[46] *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; Kulkarni, Diamandis, and Chitra, *supra* note 11; Julien Piet, Jaiden Fairoze & Nicholas Weaver, *Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value*, (2022), https://arxiv.org/abs/2203.15930.

[47] Barczentewicz, Sarch, and Vasan, *supra* note 9.

Loan liquidations. Liquidations operate in a similar manner to margin calls in traditional finance.[48] 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.[49] Such *liquidators* are remunerated in the form of a discount on the price of collateral.[50] 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 elsewhere, liquidation opportunities may be artificially created with the use of "oracle manipulation."[51] It may be possible to execute profitable liquidations with the use of transaction bundling if, for example, a trader could bundle a transaction updating the state of an on-chain lending application—updating its reference prices in such a way as to create a liquidation opportunity—with a transaction executing a liquidation immediately behind.

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 competitive valuable use of blockspace can be identified. This may include, *e.g.,* NFT "minting" and trading opportunities.[52]

1. Copying of exploits and other illicit activity

Our introductory example has shown that profitability of transaction copying can be due to illicit activity like exploits (hacks) of blockchain applications. In that example, both searchers attempted to benefit from the exploit of Inverse Finance: one indirectly—through arbitrage—and the other more directly—by copying the exploit and executing it on their own account (*i.e.,* performing the exploit themselves).

Given that bundling and generalized front-running tend to be executed with the use of automated bots and given the speed at which those techniques can be deployed, it is likely that human operators behind the bots learn about the connection between the bot's success and illicit activity only ex post. However, bot operators likely do—and in any case should—realize that it is possible that

---

[48] 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.

[49] 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 11 at 5.

[50] ARAMONTE ET AL., *supra* note 48.

[51] *See* Barczentewicz, Sarch, and Vasan, *supra* note 9 Section IV.C.

[52] *See, e.g.,* Zhou et al., *supra* note 11; Amber Group, *supra* note 44.

their bots may end up executing strategies that amount to supporting (by bundling) or directly performing actions like exploits. We do not know whether any bot operators take any measures to reduce such risk.

Naturally, when a bot operator learns that their bot executed an exploit, they may decide to return the funds. In fact, some bot operators openly advertise that they are looking for cases of attempted hacks, executing the hacks themselves and then returning the funds to the rightful owners. This is referred to as "white hat" hacking.[53] There seem to be good reasons for this kind of service: due to permissionlessness of blockchain networks like Ethereum, once a strategy through which some smart contract can be exploited becomes known, then it is almost guaranteed that someone will use that opportunity.[54] Many smart contract operators are not capable of reacting fast enough to attempted exploits by moving the vulnerable funds, modifying the smart contract parameters to close the vulnerability (if that is at all possible, which it may not be), or—if neither of the two earlier options is available—by "self-hacking" (exploiting the vulnerability themselves). Hence, a white hat intervention may be the only way to ensure that an "honest" party ends in possession of the vulnerable funds. However, there is a delicate balance between the desirability of white hat activity and the practice of "bounties" that exploiters either implicitly or explicitly require from those they—usually involuntarily—assist. The amounts paid in such bounties—*e.g.,* 10% of the "recovered" funds—may be so high as to raise questions whether what is really taking place is something more akin to extortion, rather than a legitimate service.

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

---

[53] *See, e.g.,* Miranda Bryant, *'White hat' hacker behind $610m crypto heist returns most of money*, THE GUARDIAN, August 13, 2021, https://www.theguardian.com/technology/2021/aug/13/white-hat-hacker-behind-610m-crypto-heist-returns-most-of-money.; Anish Agnihotri (@_anishagnihotri), Twitter (May 27, 2021), https://twitter.com/_anishagnihotri/status/1397971686482493443; @MevRefund, Twitter (Jun. 17, 2022), https://twitter.com/MevRefund/status/1537572886055108610; @kryptoklob, Twitter (Jan. 13, 2023), https://twitter.com/kryptoklob/status/1613909568983281664.

[54] *See, e.g.,* Edward Oosterbaan, *Why White Hat Hackers Are Vital to the Crypto Ecosystem*, COINDESK (2022), https://www.coindesk.com/layer2/2022/02/23/why-white-hat-hackers-are-vital-to-the-crypto-ecosystem/.

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.[55] 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 class of crypto assets.[56] 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.[57] Commentators have also joined this debate to offer important practical, legal, and technical considerations implicated in this issue.[58] 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

---

[55] *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.").

[56] *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.").

[57] *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).

[58] *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").

relating to market manipulation relevant to MEV are the same regardless of whether the asset is classified as a security or a commodity.[59]

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.[60] Yet, this authority is fluid: "the word 'manipulation'... in its use is so broad as to include any operation of the … market that does not suit the gentleman who is speaking at the moment".[61] 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 surrounding the law of manipulation 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.[62] 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)[63] 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.[64]

---

[59] *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).

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

[61] 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.).

[62] Gina-Gail S Fletcher, *Legitimate yet manipulative: The conundrum of open-market manipulation*, 68 DUKE L. J. 479 (2018).

[63] *Id.* at 490.

[64] 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.

1. Price Manipulation

Both section 9(a)(2) of the SEA and Section 6(c)(3) of the CEA prohibit price manipulation.[65] 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,[66] because it was largely their only means of anti-manipulation enforcement prior to the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[67] Meanwhile, the SEC has tended more often to pursue price manipulation cases under SEA s10(b) and Rule 10b-5,[68] the agency's longstanding authority to police fraud-based manipulation, when possible.[69]

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".[70] 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.[71]

(1) An artificial price is a price which "does not reflect the market or economic forces of supply and demand".[72] A price is considered artificial where it is "affected by a factor which is not legitimate."[73] Price artificiality is often called the *sine qua non* of price manipulation,[74] yet, no binding tests exists for determining which *forces* or *factors* informing a price are legitimate and which

[65] *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").

[66] 17 C.F.R. § 180.2 (2012).

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

[68] *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).

[69] Fox, Glosten, and Rauterberg, *supra* note 67 at 117.

[70] 17 CFR § 180.2 (2012).

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

[72] *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").

[73] *In re* Cox, ¶ 23,786 at 26,060.

[74] *See, e.g.,* Pirrong, *supra* note 59 at 956.

are not.[75] Thus, some scholars question the meaningfulness of an artificiality-based standard.[76] As such, determinations of price artificiality generally depend on a variety of considerations including, but not limited to, i) the competitiveness of a market,[77] ii) the presence of fraud or deceptive omission which misleads market participants[78] and iii) whether the trading pattern of the accused is supported by a "legitimate economic rationale"[79] (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.[80] 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.[81]

(3) The "*ability to influence a market price"* element of price manipulation is sometimes built into this causation analysis, with courts looking to evidence

---

[75] 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").

[76] 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'").

[77] *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).

[78] *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").

[79] *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").

[80] *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").

[81] *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").

of a defendant's market dominance as indicators of both their ability to have caused and actual causation of an artificial price.[82]

(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.[83] In *Indiana Farm*, the court held that price manipulation 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".[84] 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".[85]

Price manipulation liability alone has proved inadequate as a vehicle for protecting the efficiency and integrity of markets.[86] 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.[87] 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.[88]

Realizing the inadequacy of this approach, Congress imbued the CFTC with expanded authority, modeled explicitly after the SEC's Rule 10b-5, to

---

[82] *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).

[83] 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.

[84] *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).

[85] *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).

[86] 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.").

[87] 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).

[88] *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.

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.[89]

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 futures.[90] CEA s6(c)(1), codified through CFTC Rule 180.1,[91] 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.[92] 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[.] [93]

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.[94] That is, the interpretation of Rule 180.1 in the context of commodities markets draws explicitly from Rule 10b-5 precedent in securities markets.[95]

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."[96] Like Rule 10b-5, Rule 180.1 is intended be a "broad catch-all provision" capturing all instances of

---

[89] CFTC OFF. OF PUB. AFFAIRS, ANTI-MANIPULATION AND ANTI-FRAUD FINAL RULES (2011).
[90] 7 U.S.C. §9(1) (2011).
[91] 17 C.F.R. §180.1 (2012).
[92] 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).
[93] 17 C.F.R. §180.1 (2012).
[94] *Supra* note 90.
[95] Gregory Scopino, *The (questionable) legality of high-speed pinging and front running in the futures market*, 47 CONN. L. REV. 607, 617–618 (2015).
[96] 17 C.F.R. §180.1 (2012).

fraud-based manipulation, and it has been applied as such.[97] 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[98] to the alleged corporate misconduct of Samuel Bankman-Fried and related entities in the FTX debacle.[99]

Yet, 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".[100] 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.[101] 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."[102] A promising means for establishing fraud-based manipulation is the *fraud-on-the-market* (FOTM) theory.[103] 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.[104] 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,

---

[97] *Supra* note 90 at 41403.

[98] For an overview of significant insider trading cases brought by the CFTC, see Latham & Watkins, *Insider 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.

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

[100] *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").

[101] 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").

[102] *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.'").

[103] 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 90 at 41402 n.50.

[104] 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.

> unbeknownst to them, a wrongdoer manipulates the market and distorts the way that the market prices securities.[105]

Given the capacious language of these rules, it is clear that much space remains for *moralized* reasoning regarding what exactly makes a device, scheme, or artifice "manipulative" or intended to "defraud". Of course, this may have been the statutory drafters' very intent as the nature of market manipulation is such that no definition can ever precisely cover all forms of manipulation as manipulators constantly adapt to circumvent codified rules, while not being so overbroad as to chill healthy trading activity.[106] The role of moralized reasoning in the law of market manipulation may well operate to fill the definitional gap, using contemporary but ever-evolving notions of market unfairness as a flexible proxy for a binding legal definition of "manipulation."[107] Indeed, the Hearing Officer in *In re Henner* stated that, "manipulation is a vague term used in a wide and inclusive manner, possessing varying shades of meaning, and almost always conveying the idea of *blame-worthiness* deserving of censure."[108] We find more recent support for this notion in James Park's characterization of the SEC's Rule 10b-5 as primarily targeting acts resulting in *unjust enrichment* for individuals, with what constitutes *unjust enrichment* being grounded in moral considerations and perceived public values .[109]

The interconnection between moral conceptions of market fairness and the law of market manipulation can also be derived through case law. At common law, market manipulation "connotes willful conduct designed to deceive or defraud investors by controlling or artificially affecting the price of securities."[110] Generally required to establish that some market activity "artificially [affected] the price of securities" is a showing that the market activity in question was "aimed at deceiving investors as to how other market

---

[105] Scopino, *supra* note 95 at 672.

[106] *Compare* Cargill v Secretary of Agriculture Hardin (8th Cir 1971) ("the methods and techniques of manipulation are limited only by the ingenuity of man") *with* Pirrong, *supra* note 50 ("the word 'manipulation'... in its use is so broad as to include any operation of the … market that does not suit the gentleman who is speaking at the moment"); *see also* 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., 362 (2013) (discussing the absence of a binding legal definition of 'manipulation').

[107] There exists a fascinating debate regarding the extent to which securities and commodities regulations exist to enforce public values, rather than to police compliance with written administrative rules. *See* James J Park, *The Competing Paradigms of Securities Regulation*, 57 DUKE LJ 625 (2007) (expanding the connection between common moral perceptions and the law to all securities regulation by distinguishing principles [public values]-based enforcement of securities laws from an administrative [rules]-based approach).

[108] 30 Agric. Dec. 1151 (U.S.D.A. 1971) (emphasis added).

[109] *See generally* James J Park, *Rule 10B-5 and the rise of the unjust enrichment principle*, 60 DUKE LJ 345 (2010).

[110] Ernst & Ernst, 425 U.S. at 199, 96 S.Ct. 1375.

participants have valued a security... [by misleading investors] to believe that prices at which they purchase and sell securities are determined by the natural interplay of supply and demand, not rigged by manipulators."[111] In this way, the reasonable expectations of general market participants as to what a market free of manipulative *rigging* looks like is a necessary element of a manipulation analysis. That is, market activity constitutes fraud-based manipulation where it *deceives* market participants by representing a deviation in *actual* market activity from that *expected* by investors in a *fair*, manipulation-free market, and market participants have not received disclosure that such a "rigging" activity would occur.

Much like the *fraud-on-the-market* theory of Gregory Scopino, this framing brings the expectations and norms familiar to reasonable investors to the forefront of the manipulation analysis. We posit, therefore, that moralized reasoning which centers on public perceptions of what constitutes fair/ unfair or just/ unjust market behavior is a key factor in determinations of whether or not particular market activity is deemed manipulative.

3. Insider Trading

The SEC, CFTC, and Department of Justice (DoJ) each prohibit insider trading in their respective markets.[112] While there has been scholarly debate about the applicability of insider trading laws to crypto assets,[113] 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.[114] 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

---

[111] *ATSI Communications, Inc. V Shaar Fund* (pg 100) , quoting Gurary v. Winehouse, 190 F.3d 37, 45 (2d Cir.1999).

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

[113] *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).

[114] 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.

are charged as Rule 10b-5 violations,[115] 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,[116] 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,[117] until the recent expansion of their anti-manipulation authority following the Dodd Frank amendments to the CEA and passage of Rule 180.1.[118]

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."[119] This theory finds liability for trading on information learned "in a context that implies confidentiality, even if the trader is not a corporate insider."[120] 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[121] also applies in the context of commodities insider trading.[122]

---

[115] 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 112 at 14.

[116] *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).

[117] 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)).

[118] 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 90 at 41403.

[119] *Id.* at 41402 ; *see also O'Hagan*, 521 U.S. 642; Verstein, *supra* note 112 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").

[120] *Id.*

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

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

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."[123] 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.[124] 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 confidential and abstain from trading on the material nonpublic information.[125] This will become important particularly when it comes to MEV extractors who deal with private order flow (see IV.B).

C. 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.[126] 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."[127] However, commentators pointed out that latency arbitrage should not be confused with

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

[124] 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).

[125] 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).

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

[127] 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").

illegal front-running, insofar as high frequency trading involves only public information accessed through superior infrastructure.[128]

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."[129] Neither the SEC nor the CFTC has promulgated any rule generally prohibiting front-running (outside of specific, highly regulated contexts),[130] but instead rely on self-regulatory organizations like FINRA (the Financial Industry Regulatory Authority, Inc.), to establish and enforce front-running prohibitions among member firms.[131] 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.[132] 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.[133]

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.

---

[128] *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).

[129] 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").

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

[131] *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).

[132] *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).

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

IV. LEGALITY OF AUTOMATED MEV PIGGY-BACKING STRATEGIES

This Section examines the liability of those who carry out automated MEV piggy-backing strategies, which involve generalized profit-seeking ("GPS") bots that piggy back (*i.e.,* copy and front-run or accelerate and back-run) the trades of others when the bot deems it profitable to do so. It is theoretically possible to run such bots on pending transaction, which are not publicly known, and this likely would constitute a breach of implicit or explicit representations of confidentiality.[134] However, here we focus on the more interesting and far more common case of using GPS bots to copy or accelerate transactions in the *public mempool*, i.e. pending transactions that are publicly known.[135] This Section argues that, as a general rule, the use of GPS bots to copy the strategies devised by other users who submitted their transactions to the public mempool is unlikely to generate legal liability insofar as unexecuted public transactions are not going to be protected by a legal right. Nonetheless, we contend that there are several important cases that stand as crucial exceptions to this rule of thumb, in which liability for the GPS bot operator *is* likely. The most important of these are cases where: 1) the GPS bot is operated by a block producer in such as way as to exploit their privileged position of control over ordering the contents of blocks to order transactions to benefit themselves, and 2) where the bot copies criminal or otherwise illicit transactions and the bot-operator is aware of a substantial risk that this is happening. In such cases, the GPS bot operator is likely to have committed violations that could be pursued by regulators or prosecutors who choose to prioritize enforcement in this area of activity.

To structure the discussion in this Section, we return to the case we started the paper with: the Inverse Finance hack and the shootout between the two bots that ensued.[136] Abstracting away from the details, what occurred in that case, schematically put, is this:

1) A submitted a transaction to the mempool to be executed. The nature of that transaction was to exploit (syphon off funds) from Inverse Finance.

2) B's GPS bot detected (through running simulations of execution of transactions in the mempool) that A's transaction would be profitable and attempted to front-run it by paying a larger transaction fee for B's own copy of A's transaction to be executed before (and likely instead of) A's version.

3) C's eventually more successful GPS bot detected that if A's transaction succeeds this would create a price imbalance across exchanges, which would be profitable to exploit via a traditional arbitrage trade (trading behind, or "back-running", A's trade). However, because of how competitive such arbitrage opportunities are C can only be sure to realize the profits of this arbitrage if C can guarantee that her arbitrage trade is executed closely after A's trade creating the price imbalance. Thus, C bundles A's trade with C's back-run arbitrage

---

[134] Barczentewicz, Sarch, and Vasan, *supra* note 9.

[135] *See supra* note 25 and the accompanying text.

[136] *See supra* Section I.

trades and pays the extremely high transaction fee (almost $100,000) to ensure that A's trade goes through with C's back-run immediately afterwards. C thus piggy-backs on A's trade – gives it a boost or accelerates it – in order to ensure that C can realize the arbitrage profits through C's back run. In this way, C blocks B's effort to copy A's trade (wins the shootout) and facilitates A's trade by pushing it through into an earlier position in a block, so C can profit from the immediate back-run that is her primary aim.

To map out the risks of liability that attach to using GPS bots to copy or otherwise piggyback on the trading strategies of others, we will consider three variations on this case.

Case 1: B's liability when A's transaction is legitimate, and B succeeds. To start, let us make two assumptions that are contrary to what seems likely to have been the case in the real Inverse Finance scenario. For one, assume that B's effort to copy and front-run A's trade succeeds. Thus, we set aside C in this case. Second, assume that A's trade is entirely legitimate. On this assumption, we begin in Section IV.A by analyzing B's potential liability for copying and front-running A's legitimate trading strategy. We argue that liability for B is unlikely – at least outside of a few discrete exceptions where this presumption of legality does not hold.[137]

Case 2: B's liability when A's transaction is illicit, and B succeeds. Next, jettison the assumption of legality of A's trade. Assume A's trade (or trading strategy) is illegal, but B succeeds, via the use of her GPS bot, in copying and front-running it. What is B's liability? This sort of scenario involving B's own liability for using a bot to automatically copy and execute another's illegal trade, plausibly without much awareness of the underlying content of the trades the bot is copying, will be analyzed in Section B.

Case 3: C's liability when A's transaction is illicit, and C (not B) succeeds. In the final variation, to be discussed in Section C, we now return to the Inverse Finance case itself. We again assume that A's transaction is illicit in some way, but now we assume C not B wins the shootout. C takes steps to accelerate A's trade so C can guarantee her own back-run arbitrage trade immediately follows A's trade. In the process, C prevents B's front-run of A, though this is of little legal relevance for C. C merely blocked someone who sought to herself sought to carry out an illicit trade – not likely to be of concern to the law. Instead, we focus on C's liability for her own actions: boosting A's illicit transaction and then carrying out the highly profitable back-run arbitrage on the back of it. Section C argues that C may possibly face aiding and abetting liability, but in any event very likely faces market manipulation liability.

In this way, we provide an overview of the most likely liability outcomes for various actors engaged in different forms of MEV bot usage like B and C in

[137] If A's trade is legitimate and if B is not at risk of legal liability, then C would most likely be under no risk of legal liability as well ("a maiori ad minus"), given that C's intervention is even less likely to be harmful or to violate anyone's rights (C merely accelerates A's trade). Thus, we can set aside C for purposes of analyzing the case where A's transaction is legitimate.

the above scenario. We show where liability is likely to attach and where the bot operator more plausibly seems in the clear.

A. Piggybacking on (copying or accelerating) a legitimate profitable transaction

This Section focuses on Case 1 from above and argues that using MEV bots to search the public mempool for profitable transactions, which the bot then automatically copies and succeeds in having them executed ahead of the original user's transaction, is unlikely to generate legal liability where the underlying transaction (A's transaction in Case 1) is assumed to be entirely legitimate.

However, we argue that there are some exceptions where liability may look more likely – although we accept that this will remain contestable insofar as it relies on moralized reasoning of a kind that courts or regulators may be hesitant to rely on at least directly and explicitly. The first concerns block builders who exploit their ability to order transactions. The second involves front-running private order flow. There may be other exceptions to the default position that copying or piggybacking on legitimate transactions is not going to attract liability – but those would have to be explored separately. We are not trying to come up with an exhaustive list of exceptions to the general assumption of legal permissibility for operating GPS bots.

1. Default Permissibility of MEV Bots Piggybacking on Legitimate Transactions

In investigating the legality of generalized front-running, and of strategy copying more generally, we confront the age-old question: *does the* law *protect the chase?* In other words, are the efforts expended by a trader in seeking out, identifying, and preparing to execute upon a profitable opportunity protected such that she is entitled a legal remedy when – after doing all the work (*i.e.,* completing the "chase") – another actor swoops in and executes the opportunity, capturing the profit the unlucky trader toiled to gain?

In brief, the answer is "no" insofar as one does not obtain a legally cognizable right to the profits from a trade one is planning until it is executed and legal ownership of the relevant assets or rights have been transferred. Before that, during the process of the chase, one is on an even playing field with other competitors chasing the same profit opportunity. If one of them gets there first, and breaks no relevant rules in the process, then she has won the race and obtained the benefit of the transaction. In Ethereum, transactions are executed when built into a block, not simply when submitted by a user. Therefore, even if one was first to submit, one does not acquire legal rights to the relevant profits unless one's transaction is executed by being taken up and built into a block. So, if another user pays to have her version of the profitable trade built into a block first – which is expressly made possible by the infrastructure of the Ethereum

ecosystem – then the first to execute is the winner, even if she was not the first to submit.

This question was the subject of significant debate and discussion in early American history, albeit in the context wild animal property rights among hunters rather than profit-seeking in financial trading. As far back as the 17th century, philosopher John Locke expressed a view known as the "labor theory of property" according to which man acquires property rights through the fruits of his own labor, implying that the pursuit equates to possession.[138] To contrast, the Supreme Court of New York famously held in *Pierson v. Post* that "pursuit alone vests no property or right in the huntsman,"[139] The Court described the facts of that case as follows:

> Post, being in possession of certain dogs and hounds under his command, did, 'upon a certain wild and uninhabited, unpossessed and waste land, called the beach, find and start one of those noxious beasts called a fox,' and whilst there hunting, chasing and pursuing the same with his dogs and hounds, and when in view thereof, Pierson, well knowing the fox was so hunted and pursued, did, in the sight of Post, to prevent his catching the same, kill and carry it off.[140]

In an opinion which has been the subject of immeasurable commentary[141], the *Pierson v. Post* majority found against Post (the hunter who had chased the prey) for Pierson (who ultimately killed the prey, knowing of Post's pursuit) on the ground that the legal rights of possession, in the context of wild animals, accrue only through the killing, mortal wounding, or physical capture of the animal.[142] While starkly at odds with the Lockean "labor theory of property", the "rule of capture"[143] expressed in *Pierson v. Post* has been expanded in its application from wild animals to valuable natural resources like precious

---

[138] John Locke's views on property are noted in many sources, but explicitly noted his views of property rights in the context of hunting in *Two Treatises of Government.* John Locke, *Two Treatises of Government*, Book 2 §§30 (1690) ("the hare that anyone is hunting, is thought his who pursues her during the chase. For being a beast that is still looked upon as common … whoever has employed so much labor about any of that kind, as to find and pursue her, has thereby removed her from the state of nature, wherein she was common, and hath begun a property").

[139] Pierson v. Post, 3 Cai. 175 (N.Y. Sup. Ct. 1805).

[140] *Id.*

[141] The appellate opinion of *Pierson v. Post* is featured in countless property law textbooks and law review articles. *See* Angela Fernandez, *The Lost Record of "Pierson v. Post," the Famous Fox Case,* 27 L. & Hist. Rev. 149, 150 n.6; Andrea McDowell, *Legal Fictions in Pierson v. Post*, 105 Mich. L. Rev. 735, 736 n.2.

[142] *Pierson*, 3 Cai. at 175.

[143] The "rule of capture" provides that the first person to capture a natural resource owns that resource.

metals,[144] groundwater (in some states),[145] and oil and gas.[146] It appears, then, that the common law finds the activities of generalized front-running bots wholly permissible as they simply *capture* a profit opportunity that is the subject of another actor's *pursuit.* In other words, the law simply *does not* protect the chase.

Might one reject our claim by arguing that front-running a merely submitted transaction, which has yet to be executed by being built into a block, is nonetheless unfair? Is there something unfair or undesirable about copying as such, which might make the impact of this kind of front-running activity amount to an illegitimate price effect that creates artificial prices, thereby amounting to manipulative activity? (In the companion paper to this one, we argue something similar applies in cases of MEV sandwiching.[147]) A user whose strategy is copied and executed by a bot before the user's own transaction is executed, thus deprived of their profit, appears to be wrongfully deprived of the fruits of their labor. In selecting language so capacious as *deceptive* and *manipulative* in the CEA and SEA anti-fraud provisions*,* it seems as though Congress left room within the anti-fraud-based-manipulation provisions of these statutes for this kind of "normative criticism of the relative conduct" to guide enforcement.[148] If guided by such "normative criticism[s]" in their application of Rule 180.1 or Rule 10b-5,[149] a court familiar with the expectations and norms of traditional finance may be inclined to consider generalized front-running a kind of deceptive or manipulative act which interferes with users' reasonable assumption that the markets in which they trade are free of improper or unfair conduct like strategy copying. Hence, a plausible theory of liability under CFTC Rule 180.1 or SEC Rule 10b-5 may arise for strategy copying, including generalized front-running.

Yet, an inquiry grounded in market norms and perceived public standards of morality must be adapted to the context in which the questioned practices are occurring. Of course, it would be far from *normal* in traditional finance to see one's transaction copied and executed ahead of themself (the originator) by another trader. In actuality, this would be largely impossible unless the *copier*

---

[144] *See* Hener v. United States, 525 F.Supp. 350, 366 (S.D.N.Y. 1981) ("the mere chase of silver no more establishes its possession than the chase of wild beasts").

[145] *See, e.g.,* Joseph W. Dellapenna, *A Primer on Groundwater Law,* 49 IDAHO L. REV. 265, 271-276, (2013) (discussing the rule of capture, referenced as the *absolute dominion rule*, as applied to the common law of groundwater property rights).

[146] For a detailed discussion of the history, modern application, and complexities associated with the rule of capture in the context of oil and gas extraction, *see* Bruce M. Kramer & Owen L. Anderson, *The Rule of Capture – an Oil and Gas Perspective*, 35 Env't. L. 899 (2005).

[147] Barczentewicz, Sarch, and Vasan, *supra* note 9.

[148] MERRITT B FOX, LAWRENCE GLOSTEN & GABRIEL RAUTERBERG, THE NEW STOCK MARKET: LAW, ECONOMICS, AND POLICY 339 n.10 (2019).

[149] *Id.*

was an insider with private information about a firm's trading practices/ plans[150] or a broker with privileged access to customer orders.[151] In both cases where copying would be possible in traditional finance, it would be possible as the copier is privy to some *private information*. For that exact reason, as well, both cases would fall squarely within statutory or self-regulatory organization (i.e. exchange) prohibitions of insider trading and/or front-running, claims which hinge on trades made with some kind of unfair use of information.[152] Yet, in DeFi markets, transaction copying can occur without any misappropriation or exploitation of private information because pending transaction information is oftentimes viewable *publicly* in the mempool.[153]

This important difference between traditional and decentralized financial markets—*i.e.,* that pending transaction information is viewable only by certain privileged actors in the former, and largely public in the latter—uncovers a weakness in the intuitive normative framing of strategy copying leading to the plausible theory of fraud-based manipulation liability discussed above. Transaction copying seems intuitively *unfair* and strange for those of us accustomed to the traditional financial system as, in that context, it implies some kind of misappropriation or exploitation of a position of informational privilege. Yet, the public nature of most pending transactions in DeFi markets engenders the possibility of strategy copying *without* this dynamic of exploitation. One important implication of this is that, while in traditional finance transaction copying is only available to privileged and trusted actors with access to private information, *anyone* in DeFi has access to the informational resources necessary to engage in strategy copying.[154]

Another point of moral "ickiness" we may associate with strategy copying is that there appears to be some *finality* to a transaction originator's submission of a transaction to the mempool that extends *beyond* a mere "pursuit". In other words, it seems that identifying and submitting a transaction opportunity seems more like killing a fox than simply pursuing it (as in the case of Post). This intuition also tracks norms and expectations drawn from traditional finance, where the time-based priority rules of exchanges ensure that an order's send time secures its "place in line" with respect to ultimate execution. Yet, on Ethereum, transactions are *not* ordered on the basis of send-time but at the discretion of a rationally self-interested validator who likely orders transactions on the basis of transaction fee attached. As we noted elsewhere, "there is no natural ordering of

---

[150] *See e.g.* Order Instituting Proceedings, In the Matter of Arya Motazedi, CFTC No. 16-02 (Dec. 2, 2015) (charging an employee of a commodities trading firm with insider trading for front-running his employer's transactions by trading on his personal account).

[151] *See e.g.* D'Alessio v. SEC, 380 F.3d 112, 2004 U.S. App. LEXIS 16743, Fed. Sec. L. Rep. (CCH) P92,884 (sustaining an NYSE order terminating a broker's NYSE membership on the grounds that the broker violated NYSE rules by front-running trades to benefit his own accounts).

[152] *See supra* sections III.A(3) and III.B.

[153] *See supra* note 25 and the accompanying text.

[154] *Id.*

transactions within this space, no first-in-time queue that operates by default to determine who trades first."[155]

Moreover, it is important to note that no pending transaction is guaranteed a place on the Ethereum blockchain. By transacting publicly in DeFi (*i.e.,* broadcasting one's transaction to multiple nodes through Ethereum's peer-to-peer network), it can be argued that one assumes the risk of their profit opportunity being outcompeted by another transaction. In fact, it seems well-known, at least by MEV extractors, that private transaction routing serves as a safer way to submit one's profit-bearing transactions.[156] In essence, generalized front-running bots operated by searchers who are not block producers profit by copying another user's profitable pending transaction and attaching a higher transaction fee to their front-runs, so that they execute ahead. As the act of outbidding another user's transaction fee in the mempool is not independently improper, it may seem that a generalized front-runner making a business out of one-upping other traders' transaction fees is simply a clever, yet legitimate, means of leveraging market structure to one's own benefit. By corollary, the perceived loss suffered by a user front-ran by a generalized front-runner may simply be perceived as a legitimate trading risk assumed by trading publicly and not attaching a high enough fee to their transaction. As such, the financial harm caused by generalized front-runners may not be perceived as warranting legal protection, just as Post's chase did not grant him legal possession.

In sum, given that i) pending transaction information in DeFi markets can be *publicly* accessible, and ii) Ethereum transactions are ordered primarily on the basis of competitive transaction fee bidding rather than send time, we find that strategy copying generally – with exceptions, as the rest of this Article will explore – aligns with the norms and expectations of DeFi markets.

2. First Exception: Block Validator-Proposers

The main exception is if it is a block proposer that exploits their position of control to front-run or sandwich the original user (assuming this transaction is legitimate). We presented the substance of this argument in detail elsewhere and merely summarize it again here for present purposes.[157]

Using generalized bots that seek out profitable trades to copy, a validator-proposers can insert their version of the copied trade ahead of the original user's

---

[155] Barczentewicz, Sarch, and Vasan, *supra* note 9 at 6.

[156] Xingyu Lyu et al., *An Empirical Study on Ethereum Private Transactions and the Security Implications*, ARXIV, 5 (2022), https://arxiv.org/pdf/2208.02858.pdf (finding that 28.6% of private transactions on Ethereum are related to MEV extraction – for instance, transferring funds to the wallet addresses of MEV bots --, which indicates the increasing appeal of private transactions for MEV searchers who understand that public submission risks their MEV opportunity being copied and lost). S*ee* Dan Robinson & Georgios Konstantopoulos, *Ethereum is a Dark Forest*, PARADIGM.XYZ (2020), https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest (highlighting the risks of frontrunning for transactions publicized through Ethereum's mempool).

[157] Barczentewicz, Sarch, and Vasan, *supra* note 9, Section IV.A.

version. Thus, being a validator-proposer entails inherent advantages not in running the generalized bot to identify profitable transactions to copy, but rather is advantageous in enabling the validator-proposer (B) to trade ahead of the original user (A).

There is a colorable argument that this may amount to a form of market manipulation if courts or regulators adopt particular moralized assumptions about how markets ought to operate. Specifically, block validator-proposers have a privileged position of control over the contents of the blocks they build and when they use this power to trade ahead of other users, this may be seen as illicit use of a position of power over key financial infrastructure. Thus, when a validator-proposer's generalized bot identifies a profitable trade and she uses her position of dominance over key market infrastructure (the execution of transactions) to trade ahead of the original user, this could be viewed as having an illegitimate and thus *artificial* effect on the prices of the relevant crypto assets.

This could amount to a form of 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).[158] 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."[159]

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.[160] 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

[158] 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.

[159] Scopino, *supra* note 95 at 673.

[160] *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").

justifiably rely on the assumption that the market for those securities is functioning normally and not being manipulated."[161]

As the Second Circuit explained in 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.'"[162] For assessing manipulation, "[t]he critical question then becomes what activity 'artificially' affects a security's price in a deceptive manner."[163]

The court in *CFTC v. Cox* held that a price is considered artificial where it is "affected by a factor which is not legitimate."[164] Yet, no binding test exists for determining which forces or factors informing a price are legitimate and which are not.[165] Accordingly, courts and regulators are likely to draw on background moral assumptions to decide whether the prices obtained as a result of validator-proposers using their control over the machinery of transaction ordering to trade ahead of other users reflect only the forces of supply and demand or rather are artificial prices because they are influenced by a force that is not legitimate. 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."[166]

Here, a validator-proposer who runs a generalized bot to copy another user's transaction can exploit her position of (temporary) power over the machinery of processing transactions, in order to trade ahead of the original user's transaction. Courts and regulators might plausibly view this as an illicit exploitation of a position of control over financial infrastructure to benefit oneself at the expense of other traders. While it's true that anyone could in principle become a validator, this doesn't change the fact that validators engaged in generalized front-running can exploit their privileged position within the ecosystem/infrastructure of the financial structure. Given that *market power* or *dominance* often plays a major role in courts' price artificiality analysis,[167] it seems plausible that a court could determine that generalized front-running that

---

[161] Scopino, *supra* note 95 at 674. *See also* GREGORY SCOPINO, ALGO BOTS AND THE LAW: TECHNOLOGY, AUTOMATION, AND THE REGULATION OF FUTURES AND OTHER DERIVATIVES 307–312 (2020).

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

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

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

[165] 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").

[166] FOX, GLOSTEN, AND RAUTERBERG, *supra* note 148 at 339 n.10.

[167] *See supra* note 104.

overtly leverages the validator-proposer's power to control a piece of blockspace, thus amounts an illegitimate and artificial force on market prices. Competent validator-proposers who operate generalized front-running bots 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. 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 [bot operator] was not aware of what he was doing."[168] This is the gravamen of market manipulation.

As a result, we suggest that a block producer (validator-proposer) who exploits their transaction ordering discretion in order to favor their generalized strategy-copying and front-running bot faces a higher risk of liability than a bot operator who is not a block producer.[169]

3. Second Exception: Private Order Flow

A third example might be copying private order flow (POF) – that is, user order flow that does *not* enter the mempool and does not become meaningfully public. We can distinguish between *explicit* and *non-explicit* POF.[170] Explicit POF is the case 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).[171] *Non-explicit* POF occurs where a user's transaction is made private through the conduct of third-parties acting without regard to the intent of the user themself.[172] We limit our analysis here to the copying of *explicit* POF transactions. That is, where an Ethereum user routes their transaction through a privacy RPC to a particular block builder (or block-builders), who proceed to copy and execute the user's private transaction

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

[169] Competition between a block producer and other users:

An interesting, related question arises where a block producer receives an MEV-extracting bundle at the same time, or even earlier, than she spots the same opportunity on her own. It may be difficult for an external observer to distinguish whether a block producer copies someone else's strategy and whether they happen to come up with the same idea independently, while privileging their own execution of the strategy. But abstracting from the evidentiary problem and in the absence of any express promises not do so, can a block producer be liable for preferencing her own – independently sourced – transaction over another user's transaction? This is also a version of "market power" and "conflict of interest" arguments discussed earlier in Section IV.A. Whether a court would consider this as use of a "manipulative device, scheme, or artifice to defraud" would likely be influenced by the arguments considered there. What is worth noting here, however, is that any unfairness in this scenario is not the same as unfairness in a case of copying a transaction, by generalized front-running, or otherwise.

[170] Barczentewicz, Sarch, and Vasan, *supra* note 9, Section IV.B.

[171] *Id.* at 55.

[172] *Id.* at 60.

themselves *or* share the transaction with others who then copy and execute the user's private transaction. Admittedly, we are unsure regarding the extent to which copying or front-running of explicit order flow occurs in the wild, but it's a theoretical possibility that has been floated by others.[173]

As we explained above, users who route their transactions to the mempool through public RPC endpoints can be said to *assume the risk* that their transaction will be copied and front-ran, given the public nature of mempool transactions and the fact that transaction ordering occurs through fee-based competition. In anticipation of this risk, many Ethereum users intentionally route their transactions through private channels like privacy RPCs.[174] If the basic guarantee of a privacy RPC is not broken[175] and the user does not also route their transaction through any public channel, the user should reasonably expect that their transaction will remain private until finally broadcast to the network as part of Ethereum's future state. In this situation, the user does *not* expect their transaction to become the prey of strategy copying bots which monitor the public mempool. Indeed, MEV (including front-running) protection is often one of the core promises made by privacy RPC providers.[176] Thus, the argument that users adversely affected by strategy copying *assumed this risk* by transacting in the mempool – which supported our general rule that strategy copying bears a low risk of market manipulation liability – no longer applies where the transaction copied is explicit POF.

Moreover, where a privacy RPC and/or block-builder advertises or promises that explicit POF they receive will be protected from GPS or other MEV bots, and subsequently copies or allows to be copied a user's explicit POF, a strong claim of fraud-by-misrepresentation liability under 180.1(2) would likely exist.[177]

There is also a route to *insider trading* liability for a block-builder who receives explicit POF and proceeds to either strategy copy the explicit POF herself *or* discloses the private transaction to another searcher who strategy copies it. Recall that insider trading liability under 10b-5/180.1 requires the *misappropriation* of confidential information regarding a security or commodity in *breach* of a duty owed to the source of the information.[178] The transaction information at issue here (that is, the explicit POF) is *confidential* information, given to the recipient block-builder by the user at least arguably through a

---

[173] Barczentewicz, Sarch, and Vasan, *supra* note 9.

[174] For an empirically-grounded discussion regarding the landscape of private transactions on Ethereum, *see* Lyu et al., *supra* note 156.

[175] *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. *See also supra* notes 31-32 and the accompanying text.

[176] *See, e.g.,* https://www.rook.fi/.

[177] 17 C.F.R. §180.1(2) (2012).

[178] *See supra* notes 117-121 and accompanying text.

relationship of trust and confidence.[179] This relationship of trust and confidence, giving rise to a duty of confidentiality on the part of the block-builder, may arise from any of several sources: i) an explicit promise by the block-builder to the user that, upon receipt of the user's explicit POF, they would keep private and refrain from engaging in strategy copying on the basis of that POF, ii) an agreement made as a condition of a block-builder's integration with a privacy RPC guaranteeing that they would not strategy copy user order flow, or iii) a block-builder feigning loyalty to the user for the purpose of accessing their explicit POF.[180] If a block-builder was found to owe such a duty to a user upon receiving their explicit POF, and that block-builder subsequently breached that duty by copying and executing that user's private transactions (probably by front-running them), that block-builder would likely face insider trading liability.

Additionally, both the SEC and CFTC find that *tipper* liability for insider trading exists where an individual with a pre-existing duty of confidentiality to sources of material non-public information (i.e. *the tipper*) shares that nonpublic information to benefit others (i.e. *the tippees*), rather than to benefit themselves.[181] As such, a block-builder who does not themselves strategy copy explicit POF transactions may still be liable for insider trading if they disclose private user transactions to searchers who subsequently strategy copy those transactions.

For these reasons, we find that the risk of liability for a strategy copier who is the recipient of and copies an explicit POF transaction is *higher* than that for a strategy copier who acts on a public, legal transaction.[182]

---

[179] Courts 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." This may be particularly true in the context of blockchain-based networks, where novel and unprecedented trust relationships and power dynamics abound. *See* SEC v. Cuban, 620 F.3d 551, 555 (5th Cir. 2010).

[180] Barczentewicz, Sarch, and Vasan, *supra* note 9 at 58.

[181] *See, e.g.,* Dirks v. SEC, 463 U.S. 646 (1983); Salman v. United States, 137 S. Ct. 420, 428 (2016); CFTC v. EOX Holdings L.L.C., No. H-19-2901, 2021 WL 4482145, at *45 n.112 (S.D. Tex. Sept. 30, 2021).

[182] Another scenario where piggybacking on legitimate transactions generates liability is if there is a specific promise or expectation that is violated -- for example if there is a promise to bundle the transactions in this or that way, but the relay or block builder unbundles.

An MEV-Boost-participating validator "unbundled" a sandwich and front-ran a sandwicher's back-run. So it seems like there was a validator who went at least against the trust expectation implicit in MEV-Boost, and there seems to be some price effect - so perhaps an interesting case of market manipulation in the wild

https://twitter.com/dippudo/status/1642830900382818305

Expectation of trust placed in validators:

https://twitter.com/SiegeRhino2/status/1642819726786146304

https://twitter.com/flashfish0x/status/1642809630404354048

https://twitter.com/adanthar/status/1642839436911050755

B. Copying and Front-running Another's Illicit Transaction

This Section analyzes Case 2 from above. That is, it looks at what B's liability would be in the Inverse Finance hack example if B's bot had succeeded in its effort to front-run A's illicit transaction (*i.e.,* amounting to criminal conduct or conduct prohibited by regulators that would incur civil liability).

For this section, we assume that B is *not* a block proposer who exploits their privileged position of control over the contents of a block; instead, we assume B is just a searcher scanning the public mempool in a way that anyone in principle is welcome to. If B were a block proposer, then issues of market dominance and special positions of trust, discussed in the previous sections, would become relevant again. We do not duplicate that discussion here, but set those issues aside to determine what it is the distinctive problem, if any, with copying A's underlying trade.

Further, we limit our analysis here to *single-transaction* violations, *i.e.* where A's transaction by itself is a violation (*e.g.,* an instance of insider trading or a smart-contract that carries out an illegal hack), or violations that involve a bundle of transactions which are guaranteed to be executed together.[183] This is because MEV bots commonly copy single transactions or bundles of transaction, but do not generally have the capability to copy and execute unconnected sets of distinct transactions, particularly where these occur across multiple blocks. This, in turn, is because the bots are designed to secure guaranteed profits, but that guarantee is not present when it comes to multiple separate transactions whose profitability may be affected by intervening trades. Thus, it is single transactions, or perhaps bundles of transactions that are guaranteed to be included in the same block, that MEV bots focus on copying.

Now, the first step in determining B's liability is identifying the nature of the violation that A's trade would amount to. This is the underlying transaction which B – through strategy-copying – ultimately executes first instead of A. What violation A's transaction would amount to determines whether B will become liable for the same violation in virtue of B's bot copying and executing its own version of A's illegal trade. Particularly the mens rea component of the underlying violation will be crucial here.

1. Strict Liability Violations

The simplest case would be where A's violation is one of *strict liability* - for instance, a violation of international sanctions by trading with a prohibited

---

One question seems to be - was this just competition and someone being smarter (like under CFTC v DRW & Wilson) or is it more important that the validator used their privileged position / monopoly control over a market and violated the (implicit) trust assumptions. This validator committed a "slashable" offence which means their 32 ETH staked will likely be deleted - but they profited way more $15M+. so this "slashability" could strengthen the argument that there was something deceitful / fraudulent about this action, beyond any badness of doing a sandwich.

[183] *See supra* Section II.A(1).

wallet address.[184] Violating sanctions law in this way can result in regulators imposing civil fines on a strict liability.[185] Accordingly, in such a case, B would simply inherit A's liability by being the first to execute A's transaction, as strict liability offenses attract liability regardless of the offender's mental state.

2. Knowledge Offenses

Matters are more difficult where the offense A's transaction constitutes requires a higher mens rea, such a recklessness, knowledge or intent. In that case, it is much less clear that B will face liability for copying and executing of A's transaction, even though it is assumed to be illegal if A had executed it.

Most importantly, in the Inverse Finance case, A's transaction involved exploiting a vulnerability to exploit Inverse Finance smart contracts and drain its assets. This would amount to theft by unauthorized access of a computer system in violation of 18 U.S.C. § 1030. The relevant offense here is § 1030(4), which makes it a crime to "knowingly and with intent to defraud, accesses a protected computer without authorization…and by means of such conduct further[] the intended fraud and obtains anything of value."[186] This involves a mens rea of knowledge with respect to the lack of authorization to access the relevant computer system, together with the relevant intent to defraud.

Of crucial importance, when A submits her transaction, which we will assume amounts to a hack of Inverse Finance that meets the requirements of § 1030(4), to the public mempool, it contains within it all the instructions necessary for a smart contract to carry out the exploit of Inverse Finance. Thus, when B's bot spies A's profitable transaction in the mempool and copies it, it will likewise follow these instructions to carry out the exploit of Inverse Finance, only now on B's behalf not A's. This means B's bot will carry out the same hack as A would have carried out. As a result, B will in effect step directly into A's shoes and be guilty of the same § 1030(4) offense as A would have been – *provided B has the requisite mens rea of knowledge and intent to defraud.* (A similar analysis will apply if A's transaction is insider trading, for example, which also requires knowledge that the information the tippee traded on was improperly obtained.[187])

---

[184] *See, e.g.,* Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry,* (October 15, 2021) (slide 6) https://ofac.treasury.gov/media/913571/download?inline.

[185] *Id.* at 6 ("OFAC may impose civil penalties for sanctions violations generally based on a strict liability standard."). OFAC has placed several crypto wallet addresses on its Specially Designated Nationals (SDN) sanctions list. *See* Office of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons List (*April 4, 2023), https://www.treasury.gov/ofac/downloads/sdnlist.pdf.

[186] 18 U.S.C. § 1030(4).

[187] United States v. Newman, 773 F. 3d 438, 455 (2d Cir. 2014) (overturning conviction because "[n]o reasonable jury could have found beyond a reasonable doubt that [the defendant-tippees]

However, this is where the difficulty arises. After all, it is very likely that B—a person—does not have advance knowledge of the details of A's transaction, which B's bot automatically copies and executes. Suppose B does not and cannot closely monitor the details of every transaction her bot copies, since it is meant to run autonomously and at scale. If B had known of A's transaction specifically, suppose all B would have seen is that it was so profitable that in such a competitive environment it could only be the result of illegal activity, very likely a hack. But B does not have particularized knowledge of A's precise transaction because B's GF bot simulates and copies many transactions independently and B has no capacity to review them all. (Manually reviewing all transactions would defeat the purpose of running the bot in the first place.) As a result, it appears unlikely that B will have the mens rea of knowledge required to violate § 1030(4).

There are two rejoinders to this, though it's unclear if they succeed. First, it is very plausible that B will be aware of the general risk – indeed the *statistical certainty* – that her bot will end up copying and front-running some illegal transactions of precisely this kind in the course of its normal operations. That is to say, B is likely to be aware of the practical certainty, at least in general terms, that scenarios exactly like this one will arise as a result of running her GF bot. This means there is an argument that she will have at least statistical knowledge that some of her own transactions, executed by the GF bot, will be illegal transactions – perhaps especially that some will involve hacking of other computer systems.

However, there are well-known difficulties with taking statistical knowledge to satisfy the knowledge element of an offense.[188] Indeed, in this instance B seems not to have advance knowledge of the fact that this particular transaction of A's is a hack – even if B knows that such transactions are statistically likely. Instead, we have at best an instance of *recklessness*: awareness of a substantial and unjustified risk that the transaction at issue that B's bot copies from A and executes involves the unauthorized access to another's computer system (here Inverse Finance) to illegally obtain funds therefrom. Mere recklessness, however, would not suffice to meet the

knew, or deliberately avoided knowing, that the information originated with corporate insiders," i.e. was improperly obtained).

[188] *See* Ken Simons, *Statistical Knowledge Deconstructed,* Boston Univ. Law Working Paper (March 1, 2011), https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1531&context=faculty_scholarship ("The law frequently distinguishes between individualized knowledge (awareness that one's act will harm a particular victim, e.g., driving through an intersection while aware that one's automobile is likely to injure a pedestrian) and statistical knowledge (awareness that one's activity or multiple acts will, to a high statistical likelihood, harm one or more potential victims, e.g., proceeding with a large construction project that one confidently predicts will result in worker injuries). Under tort and criminal law doctrine, acting with individualized knowledge is ordinarily much more difficult to justify, and, if unjustified, much more culpable, than acting with statistical knowledge. Yet the distinction is very difficult to explain and defend").

knowledge element required for B to have committed the hacking offense under § 1030(4).

Nonetheless, the second rejoinder is that B, who is at least reckless with respect to the illegality of A's transaction that B's bot copies, is acting in a way that amounts to *willful blindness*.[189] This would indeed satisfy the knowledge element of the § 1030(4) offense (or if A's transaction were insider trading instead[190]). Willful blindness involves being aware of a risk of an inculpatory fact and being able to investigate it, but deliberately choosing not to.[191] Thus, argument that B was willfully blind is that B could have constructed her bot to take active steps *ex ante* in order to mitigate the likelihood of his bot copying illegal transactions. For instance, a bot operator could write parameters into the code governing the bot's operations and strategies which capped the size and/or profit rate of transactions it copied at some level beyond which the likelihood of transactions being crime is significantly high. Likewise, a bot operator could write a parameter blocking the bot from copying transactions sent by or received from certain wallet addresses -- for instance, those sanctioned by the Office of Foreign Assets Control (OFAC).[192] Even less severely, a bot operator could simply program the bot to *notify* the bot operator prior to copying a transaction above a certain size or profit rate, or sent by/received from a sanctioned wallet address. However, assuming B has taken no such steps to identify and prevent her bot from executing illegal or dubious trades being, or at least alerting B to the possibility of such a trade which would have to be reviewed, B has acted in willful blindness of the illicit nature of the trades her bot is copying and carrying out. B could have taken steps to obtain more information about the risks of illegality she is running through her bot copying the transactions of others, but she decided not to, thereby arguably intentionally preserving her ignorance.[193] (This may even have been part of a deliberate scheme to obtain the benefits of crime while seeking to evade liability for it should their conduct be investigated – although that would need to be investigated on a case by case basis.)

Whether the willful blindness argument will succeed, however, depends on the degree of particularized risk B was aware of, and how feasible it was in the particular case for B to have taken steps to investigate her suspicions (awareness of the risk) that her bot was copying and carrying out illegal transactions. If such investigations are not deemed to be practically feasible, B would count only as reckless and not willfully blind. Thus, we cannot confidently conclude that either of the above rejoinders will succeed in providing a basis for finding B to have committed the knowledge offense that A's transaction would have constituted.

---

[189] *Global-Tech Appliances, Inc. v. SEB S.A.*, 131 S. Ct. 2060, 2070 (2011); *United States v. Heredia*, 483 F.3d 913, 920 (9th Cir. 2007).

[190] See supra note 187.

[191] See supra note 189; *see generally* ALEX SARCH, CRIMINALLY IGNORANT 17-21 (2019).

[192] OFAC has placed several crypto wallet addresses on its Specially Designated Nationals (SDN) sanctions list. See https://www.treasury.gov/ofac/downloads/sdnlist.pdf.

[193] *See supra* note 189.

There is a non-trivial chance that B could evade liability for knowledge offenses like computer fraud in 18 U.S.C. § 1030(4).

3. Recklessness Offenses

By contrast, where A's transaction would amount to a recklessness offense, it is more plausible that B, by virtue of copying it, would end up facing liability for that offense.

Most importantly, it is plausible that A's transaction might constitute an act of fraud or deception in violation of CFTC Rule 180.1 or SEC Rule 10b-5, for which the requisite mens rea is recklessness.[194] A's transaction, recall, was a hack of Inverse Finance: the exploitation of a code vulnerability to gain access to their system and dishonestly drain the platform of its assets. This likely would amount to a "manipulative device," in contravention of 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).[195]

We argued in the previous section that B very plausibly could be found reckless – *i.e.*, aware of a substantial risk that some of the trades her bot copies are illicit. Where such recklessness suffices for the relevant offense or violation, then B may plausibly find herself on the hook in virtue of her copying A's transaction. In applying Rule 180.1, for example, the CFTC defines recklessness as "an act or omission 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 or she was doing.''[196] It is likely that an actor like B, who is sophisticated enough to operate a generalized MEV bot such as this one will surely, based on the available evidence about what happens in crypto markets and the prevalence of hacks and fraud therein,[197] be actually aware of the relevant risks about her own transactions. This risk is going to be objectively clear and obvious to anyone as sophisticated as B, given their operation of the GF bot. So, a plausible case for recklessness under 180.1 and 10b-5 is likely to exist in such cases.

This means that B, in virtue of her recklessness as to the manipulative or fraudulent nature of the transactions her bot carries out stands a good chance of

---

[194] 17 CFR § 180.1 (2012).

[195] 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.

[196] CFTC Final Rule 180.1 Release at 41404, quoting Drexel Burnham Lambert Inc. v. CFTC, 850 F.2d 742, 748 (D.C. Cir. 1988).

[197] *See, e.g.,* Chainalysis, *2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers*, CHAINALYSIS (2023), https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/.

violating CFTC Rule 180.1 or SEC Rule 10b-5 (depending on whether the crypto assets are commodities or securities) by virtue of her bot copying A's particular illicit transaction in the instant case. Given her recklessness, her generalized front-running of transactions that would be criminal if carried out – such as the unauthorized access of Inverse Finance's system to drain their funds – amount to a "manipulative device" or a scheme that "would operate as a fraud or deceit."[198] This is the strongest basis for a finding of fraud or manipulation liability for B in virtue of her operation of the generalized bot to copy A's illicit transaction.

4. Concluding Remarks

Thus, we have seen that B will face liability for copying A's illegal transaction at least where A's transaction amounts to a strict liability offense or a recklessness offense. B in this scenario is unlikely to end up qualifying as guilty of knowledge offenses given that she will not generally have particularized knowledge – at best statistical knowledge, or recklessness, as to – the illicit nature of the transactions she copies.

C. Automatically facilitating and piggy backing on (accelerating) an illegal transaction

This Section returns to the actual Inverse Finance case and analyzes C's liability for facilitating A's illicit trade and then running the highly profitable arbitrage back run immediately after A's trade. Unlike the prior section, we assume here that C (and not B) succeeds in their effort to piggyback on A's trade. This is a true "battle of the bots" scenario: C intervenes to block B's front-run. Instead, C boosts A's original transaction to ensure it goes through, thus facilitating A's criminal transaction. Then, C exploits the arbitrage opportunity created by A's illicit transaction by paying a sufficiently high fee to the validator to be guaranteed execution directly following A's original (illegal) trade.

In particular, we consider whether C becomes guilty of A's crime in virtue of aiding and abetting it, and then we consider C's own liability for fraud or manipulation in virtue of her back-run of A to exploit the arbitrage opportunity A's transaction creates. We argue it is doubtful that aiding and abetting liability is present due to C's lack of proper mens rea, but market manipulation liability is likely to be incurred because her conduct manipulatively or deceitfully creates the arbitrage opportunity that she then goes on to exploit.

[198] *See supra* notes 194-196.

1. Aiding and Abetting Liability

Supposing that A's transaction is a crime, particularly a hack of Inverse Finance's system to drain their funds in violation of 18 U.S.C. § 1030(4), what is C's criminal liability as an aider and abettor of A's offense?

Under the federal aiding and abetting statute, "[w]hoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal."[199] There is widespread agreement that to be guilty under this provision, one must not only perform an action in aid of the conduct of the principal wrongdoer, but also perform that action with some mens rea (or mental state) towards the principal's underlying crime.[200] There is debate about what precise mens rea toward the underlying crime is required.[201] Some courts have held that it is enough to aid the principal's conduct while merely having *knowledge* that the crime will be committed.[202] Some propose that the mens rea required for complicity tracks the mens rea of the underlying crime—the so-called "derivative approach."[203]

There is little doubt that C has carried out an act that aids or facilitates A's transaction. As LaFave notes, "[t]he assistance given" can be very minimal, and "need not contribute to the criminal result in the sense that but for it the [criminal] result would not have ensued."[204] In this case, by bundling it and paying the high transaction fee needed to ensure A's transaction is executed, C smooths the way for A's transaction. Indeed, C also aids A by blocking B's interference with A's transaction. So, there is little doubt that C performs the actus reus of aiding and abetting.

---

[199] 18 U.S.C. § 2(a).

[200] As Wayne LaFave explains, "[i]t may generally be said that one is liable as an accomplice to the crime of another if he (a) gave assistance or encouragement or failed to perform a legal duty to prevent it (b) with the intent thereby to promote or facilitate commission of the crime." Wayne LaFave, SUBSTANTIVE CRIMINAL LAW, 2d ed., § 13.2 (2003). *See also Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 181 (1994) ("those who provide knowing aid to persons committing federal crimes, with the intent to facilitate the crime, are themselves committing a crime."); *Rosemond v. United States*, 134 S. Ct. 1240, 1245 (2014) (same). *See* Baruch Weiss, *What Were They Thinking?: The Mental States of the Aider and Abettor and the Causer Under Federal Law*, 70 FORDHAM L. REV. 1341, 1351-52 (2002) (dicusing how "intent" in these authorities can sometimes mean something less than full intention or purpose, such as knowledge or at times perhaps even recklessness).

[201] LaFave observes that "[t]here is a split of authority as to whether some lesser mental state will suffice for accomplice liability, such as mere knowledge that one is aiding a crime or knowledge that one is aiding reckless or negligent conduct which may produce a criminal result." LaFave, *supra* note at § 13.2.

[202] For example, as the Supreme Court recently noted with respect to what it termed the "intent" required for being an accomplice, it had "previously found that intent requirement satisfied when a person actively participates in a criminal venture with full *knowledge* of the circumstances constituting the charged offense." *Rosemond*, 134 S. Ct. at 1248-49 (emphasis added). *See also* Weiss, *supra* note 200 at 1396-1409 (discussing cases requiring only knowledge).

[203] *See* Weiss, *supra* note 200 at 1410-14 (discussing the derivative approach).

[204] *State ex rel. Martin v. Tally*, 102 Ala. 25, 15 So. 722 (1894), quoted in LaFave, *supra* note at § 13.2.722 (1894), quoted in LaFave, *supra* note at § 13.2.

The complexity comes in connection with the mens rea of aiding and abetting. For the same reasons laid out in Section B in assessing B's liability, where A's crime is one that requires knowledge – such as 18 U.S.C. § 1030(4) – C is unlikely to have the requisite mens rea to count as an aider and abettor of A's crime. Regardless of whether courts take knowledge of the underlying crime to be the mens rea for aiding and abetting, or adopt the derivative approach, C is unlikely to have the mens rea of knowledge as to A's crime.[205] As argued above, this is because C is likely to be aware only of a general risk that some transactions her bot facilitates through its automated conduct will be illegal.

By contrast, if A's conduct amounts to a recklessness crime – perhaps a criminal violation of CFTC Rule 180.1 for taking funds from Inverse Finance in a way that operates as a "fraud or deceit"[206] – then courts applying the derivative approach could find C to be guilty of A's crime as an accomplice. As argued for B in the previous Section, C will also likely have the mental state of recklessness about her bot's facilitation of others' illegal transactions. Because 180.1 similarly has a recklessness standard,[207] courts applying the derivative approach might find C to have aided and abetted A's crime.[208]

(Note also that because C is likely to at most be reckless, not knowing, as to A's crime, it is unlikely that C would face aiding and abetting liability under the CEA as well. CEA Section 13(a) states that anyone who "willfully aids, abets, counsels, commands, induces, or procures the commission of, a violation of [the CEA or CFTC rules] ... may be held responsible for such violation as a principal."[209] Such a willful violation, in turn, requires "that [defendant] (1) had knowledge of the principal's ... intent to commit a violation of the Act; (2) had the intent to further that violation; and (3) committed some act in furtherance of the principal's objective."[210] Insofar as C is only reckless as to A's crime, not knowing, it's doubtful that C would face CEA aiding and abetting liability.[211])

2. Fraud/Manipulation liability

Even if liability could not be imposed on C for aiding and abetting A's offense (for instance due to a court insisting on knowledge of the underlying

---

[205] *See supra* notes 201-203.

[206] ("When the Division obtains evidence that criminal violations of the CEA have occurred, it may refer the matter to the Department of Justice for prosecution.").

[207] 17 CFR § 180.1 (2012).

[208] *See supra* note 203.

[209] 7 U.S. Code § 13c (1992).

[210] Nicholas v. Saul Stone & Co., 224 F.3d 179, 189 (3d Cir. 2000).

[211] *But see* Jonathan Marcus, Stuart Levi, Trevor Levine and Daniel O'Connell, *Smart Contract Coders May Face Aiding And Abetting Risk (*Feb. 27, 2019) https://corpgov.law.harvard.edu/wp-content/uploads/2019/02/SmartContractCodersMayFaceAidingandAbettingRisk.pdf (discussing the prospect of smart contract developers being found to be aiders and abettors under the CEA for facilitating illegal transactions).

crime as the mens rea for aiding and abetting), we argue that C would still face liability under Rules 180.1 or 10b-5 for illicitly creating the arbitrage opportunity that C's bot goes on to exploit through its back-run of A's trade.

Both Rules 10b-5 and 180.1 prohibit the execution of any manipulative device, scheme, or artifice to defraud.[212] By boosting A's illicit transaction, C did not just exploit an existing arbitrage opportunity which arose independently of C's involvement, but actually helped to *create* the arbitrage opportunity and C did so by facilitating A's illegal transaction constituting the hack of Inverse Finance.[213] Thus, this was not a run-of-the-mill DEX arbitrage or other standard arbitrage opportunity, but a disruption in prices caused by A's illicit transaction, which C facilitated. This is important to note as not all transaction fee bidding wars lead to the conclusion that their winner is a market manipulator. Claims for fraud-based manipulation require misconduct such as the use of a "manipulative device" or an act that "would operate as a fraud or deceit."[214] That exists, we submit, when one recklessly facilitates a crime that creates an *artificial price imbalance*[215] that provides the opportunity for profitable arbitrage. The price imbalance C exploits is not one that arose through the "natural interplay of supply and demand,"[216] but rather was deceitfully created by C via her reckless facilitation of A's criminal transaction that constituted the hack of Inverse Finance. Because C has at least the mens rea of recklessness as to the reliance on a criminal transaction to create this arbitrage opportunity, as required for a violation of CFTC 180.1 or SEC 10b-5, we submit that courts should have little trouble concluding that C's back-run of A's trade to exploit the arbitrage opportunity C recklessly helped create amounts to a prohibited form of manipulation of the market.

---

[212] 17 CFR § 180.1 (2012).

[213] 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. 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)").

[214] CFTC Rule 180.1(a)(1) and SEC Rule 10b-5(a) (prohibiting manipulative devices), CFTC Rule 180.1(a)(3) and SEC Rule 10b-5(c) (prohibiting schemes that "would operate as a fraud or deceit").

[215] ATSI Commc'ns, Inc. v. Shaar Fund, Ltd., 493 F.3d 101 (2d Cir. 2007), *quoting* Gurary v. Winehouse, 190 F.3d 37, 45 (2d Cir. 1999) (a manipulator artificially affects prices by misleading investors "to believe 'that prices at which they purchase and sell securities are determined by the natural interplay of supply and demand, not rigged by manipulators.").

[216] *Id.*

D. Legal Conclusions

We argued in Section IV.A that generalized MEV bots copying others' legitimate transactions is unlikely to generate liability – unless one is a proposer-validator who exploits one's control over the transactions in a block to enable one to trade ahead of others for one's own benefit or one breaches confidences by trading ahead of explicit private order flow.

Furthermore, we argued in IV.B that when B copies and trades ahead of a transaction by A that is illegal, this will suffice for B to become liable for the violation A would have committed only in relatively narrow circumstances. These are if A's trade (or bundle of trades) amounts to a strict liability violation, or A's trade (or bundle) would amount to an offense of recklessness, such as a violation of CFTC Rule 180.1 or SEC 10b-5. In the latter case, B also would likely end up committing a 180.1 or 10b-5 violation, as B is likely to be at least reckless herself.

Finally, we argued that C, who facilitates A's crime and then carries out a back-run arbitrage immediately following its execution, faces legal peril as well. C may or may not end up qualifying as an aider and abettor, depending on whether the relevant courts requiring knowledge of A's underlying offense (as indeed CEA 13(a) does), or whether they adopt the derivative approach, which allows recklessness to suffice for aiding and abetting when the underlying offense itself is a crime of recklessness. In any case, we argued that C will still end up violating Rule 180.1 or 10b-5 herself based on her manipulative or deceitful creation of the artificial price imbalance that C's back-run arbitrage exploits. C deceitfully creates this artificial price imbalance because it arises not due to natural forces of supply and demand but due to C's facilitation of A's underlying criminal transaction (the hack of Inverse Finance) that C boosted to ensure its execution. Capitalizing on that artificially created price imbalance plausibly represents a manipulative device or scheme that operates as a fraud or deceit.

In sum, we have argued that copying or facilitating illegal transactions via an automated MEV bot is fraught with legal risk.

V. CONCLUSIONS

In this Article, we have assessed the legal and ethical implications of *strategy copying* in blockchain-based financial systems, focusing on the Ethereum blockchain. While acknowledging that transaction copying may violate the norms and moral standards of traditional finance, we have argued that there are important differences in the economic, technical, and competitive dynamics of DeFi which render strategy copying in its prototypical case – that is, when executed by a searcher who is not a block proposer to copy or take advantage of public, legal transactions – *not* a case of impermissible market

manipulation. Yet, there are important exceptions to this general rule – instances where we find that the power relationships and incentives at play warrant legal intervention. Specifically, we find that liability may be appropriate for strategy copying in three main scenarios: i) the strategy copier is a privileged block producer (validator/proposer), exploiting their market power through their monopoly over transaction ordering in a particular block to trade ahead of regular users who lack this power; ii) the copied transactions are explicit private order flow, such that their recipient block-builder has a relationship of trust with the originator which they violate by strategy copying; or iii) the transaction copied is in itself illicit.

With respect to the latter exception, we find ourselves dissatisfied with the results of our inquiry in Section IV.B regarding the legal treatment of a bot who *copies and front-runs,* thus himself executing, an illicit transaction. In that section, we concluded that there remains some likelihood that B – who we assumed copied and front-ran A's illicit transaction – would not be held liable for knowledge offenses like criminal hacking. Perhaps, judicial or legislative extension of willful blindness liability to such cases is warranted. This may be especially advisable in situations where a bot operator does not take any effective measures to limit the risk that their bot will behave in such a way. Moreover, the bot operator's actions after she learns about their bot's transaction, and especially whether they restore the assets to their rightful owners, may also be relevant – and indeed may be an independent basis for liability if the proceeds are not returned upon the bot owner learning what happened.

Nevertheless, there is a risk in extending liability for copying and front-running of illicit transactions too widely. As we noted, at least some of those who do it are genuine "white hats", aiming to protect those who are already under attack by securing the assets and then returning them to the rightful owners.[217] It may not always be easy to distinguish between genuine white hats and those who may want to pretend to be white hats, but in fact engage in a kind of extortion. This is so especially because white hats sometimes expect "bounties", for example of 10% of the funds recovered, which may amount to very significant sums. Perhaps a different system of bounties, tied more closely to the risk taken on by and the efforts made by a white hat—rather than the value of the assets recovered—would lead to superior alignment of incentives.

To the extent that transaction copying is undesirable, it is important to note that technical solutions may be more effective than legal enforcement in alleviating the problems. The key enabling factor for transaction copying is that many pending transactions are public. Technical and operational solutions bringing more privacy for pending transactions naturally reduce the possibilities for transaction copying. This would not affect directly copying enabled by knowledge about *private* transactions—potentially constituting illegal insider

[217] *See supra* notes 53-54 and the accompanying text.

trading—but given that at least some kinds of arrangements offering transaction privacy are voluntary, users may simply be able to boycott service providers who breach their trust.

These policy questions merit much more debate.[218] Our main contribution here has been to map the most plausible legal outcomes for MEV bot owners in key scenarios under applicable US law at the present time. Regulation of some form or other would be valuable if for no other reason than that clarity breeds the confidence that is essential to innovation and a sense of security for market participants. But to know what legal changes are needed, we must begin with an understanding of what the law is. Shedding light on that essential first question has been our main aim here.

[218] We have offered several considerations on the proper policy response to MEV in general elsewhere. See Barczentewicz, Sarch, and Vasan, *supra* note 9; see also Barczentewicz, *supra* note 22.