Regulation of Crypto-Finance Research Project
CryptoFinReg.org

October 2023

Public Comment on IOSCO's Consultation Report on Policy Recommendations for Decentralized Finance (DeFi)

Re: MEV and IOSCO Recommendations 4 & 5

Dr Mikołaj Barczentewicz

Associate Professor of Law, University of Surrey; Project Leader, Regulation of Crypto-Finance Research Project (CryptoFinReg.org); Research Associate, University of Oxford; Senior Scholar, International Center for Law and Economics

I am the author and co-author of the leading academic papers on the legal and policy aspects of MEV (maximum extractable value).[1] I am submitting this comment in my personal capacity. I have received no financial support for the preparation of this comment.[2]

IOSCO is correct to identify conflicts of interest (Recommendation 4) and operational and technological risks (Recommendation 5) as issues of concern in DeFi that need to be addressed by providers of DeFi products and services. However, to the extent that these are also appropriate concerns for regulators, it is essential to apply the 'same activity, same risk, same regulatory outcome' principle correctly. This requires a sound understanding of what activities and risks are the same between traditional financial markets and DeFi. In this brief commentary, I focus on the difficulties of analogizing activities known as MEV—discussed in the Report—with traditional finance. I also note

---

[1] Mikołaj Barczentewicz, 'MEV on Ethereum: A Policy Analysis' (*International Center for Law & Economics White Paper,* 23 January 2023) <https://ssrn.com/abstract=4332703>; Mikołaj Barczentewicz, Alex F Sarch and Natasha Vasan, 'Blockchain Transaction Ordering as Market Manipulation' (forthcoming) Ohio State Technology Law Journal <https://ssrn.com/abstract=4187752>; Mikołaj Barczentewicz, Alex F Sarch and Natasha Vasan, 'Battle of the Crypto Bots: Automated Transaction Copying in Decentralized Finance' (forthcoming) University of Pennsylvania Journal of Business Law <https://ssrn.com/abstract=4411448>; Mikołaj Barczentewicz and André de Gândara Gomes, 'Crypto-Asset Market Abuse Under EU MiCA' [2023] <https://ssrn.com/abstract=4375201>. See also https://MEVlaw.xyz/.

[2] I am a recipient of an Ethereum Foundation grant for the 'Legally credible neutrality' project, which is indirectly related to this comment.

the experimental and rapidly evolving nature of the mechanisms that DeFi service providers can adopt in response to MEV. Hence, I argue that it is premature for regulators to intervene by imposing specific solutions. Instead, I suggest in-depth engagement with the industry and academic experts.

More research is needed on the undesirability and illegality of MEV

IOSCO is right to suggest that regulators should understand DeFi arrangements at a technical level (p. 21). This is particularly true for MEV strategies, as a superficial understanding of this phenomenon will likely lead to ineffective or counterproductive policy responses. Most discussions of MEV are riddled with conceptual confusion, mainly due to the borrowing of terms from traditional financial markets and their application to phenomena that are not analogous. Unfortunately, some key aspects of the Report's treatment of MEV (pp. 32-33, 56-59) exemplify this problem.

DeFi 'front-running' would not be illegal in traditional markets

For example, the term 'front-running' in its proper legal sense refers not just to 'trading ahead' of another, but to a situation involving the use of non-public information or a breach of a specific duty owed by a service provider (e.g. a broker) to its client.[3] 'Trading ahead'—for example, using latency arbitrage—that does not rely on non-public information and does not breach a duty to a client is not considered illegal in traditional financial markets.[4] The Report's assertion that an activity such as DeFi's 'front-running' 'would be classified as market manipulation in traditional markets' (p. 57) is, therefore, too hasty. Strictly speaking, DeFi 'front-running' merely means 'trading ahead' of some other transaction: a lawful activity both in DeFi and traditional markets.

Some 'trading ahead' may involve additional circumstances that could make it illegal in some jurisdictions, but that doesn't justify branding the entire phenomenon as illegal or analogous to illegal activities. The special circumstances could include relying on non-public information (e.g., in some 'private order flow' arrangements)[5] or a breach of a relevant legal duty to a client (although this may be even rarer in DeFi than insider trading because DeFi 'front-runners' are likely not 'front-running' their *clients*).[6]

Branding DeFi 'front-running' as illegal or analogous to illegal activities is counterproductive, distracting from the actual policy concerns. Such concerns come not from 'front-running' as understood in DeFi (i.e., 'trading ahead') but from insider trading or breaches of legally protected customer trust.

---

[3] 'Blockchain Transaction Ordering as Market Manipulation' (n 1), sections III.D, IV.A.2.v.

[4] *Id.*

[5] For a detailed discussion of this question, under US law, see *Id.*, section IV.B.

[6] *Id.*, section IV.A.2.v.

Ethereum sequencers 'order' transactions; 'reordering' is only possible if there is a natural ordering, here absent

As noted in the Report, what gives rise to MEV is the ability to decide which transactions are to be included on the blockchain and in what order. However, the Report refers to the ability to 'reorder' transactions. Talking about 'reordering' transactions is potentially confusing. Blockchain networks like Ethereum do not have a natural order of transaction execution.[7] In such networks, transactions do not come to sequencers (validators, block builders) in some sort of queue. Sequencers have access to a set of pending transactions, and it is up to them to choose which transactions to include in a block, and what order. The reason for this is the geographically decentralized design of the network.

This is one of the main reasons why analogies with traditional finance are difficult in this context. Talking about 'reordering' transactions assumes that there is or should be a privileged baseline order. But this is an assertion that requires a robust argument. It is possible that imposing something like a first-in-first-out transaction order would undermine the main benefits of blockchain networks such as Ethereum, including their resilience to various types of global attacks. However, there may also be technological solutions that would make first-in-first-out arrangements viable for networks of the scale of Ethereum, and it remains to be seen whether such solutions will be successful.[8]

Even the criticized kinds of MEV (like sandwiching) could be overall beneficial for the market

As I argued elsewhere, MEV 'may have complex and positive effects on various aspects of on-chain markets. The mechanisms of those positive effects may be specific to blockchains, in which case, intuitions and analogies from traditional finance may be of limited help."[9] In an important study, Kulkarni, Diamandis, & Chitra suggested that 'while individual trades that are sandwiched undoubtedly receive worse prices, sandwiches can cause more effective routing patterns as some flow avoids sandwiches edges."[10] Thus, even the criticized MEV types might benefit the market overall. Also, even though a trader might experience some negative impact due to some kinds of MEV, they might not be worse off overall if they also gain from the positive effects of

[7] *Id.*, sections I, VI.
[8] See eg Alex Watts, 'Polygon FastLane White Paper', https://www.fastlane.finance/PFL_WHITE_PAPER_1_5.pdf.
[9] 'MEV on Ethereum: A Policy Analysis' (n 1) 18.
[10] Kshitij Kulkarni, Theo Diamandis and Tarun Chitra, 'Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers' (2022) <https://arxiv.org/abs/2207.11835> 8.

MEV.[11] More empirical research is required to establish whether such beneficial effects are sufficiently significant in practice.[12]

Moreover, MEV may be important to provide sufficient incentives for network participants (like validators) to perform their function and to ensure the economic security of the network at an optimal level.[13]

'Solutions' to MEV are contested and rapidly evolving

Even assuming that it would be desirable to mitigate *some* kinds of MEV (even if they are not illegal), there is no consensus over what should be mitigated, how, and by whom.[14]

For instance, 'sandwiching' is enabled by access to information about pending transactions. This could be addressed at the level of the blockchain network (the protocol level) by making transactions private until they are included in a finalized block.[15] However, aside from technical challenges, this could make it impossible for block producers (block builders, validators) or relays to screen pending transactions, e.g., for sanctions-compliance purposes.[16] Moreover, too much transaction privacy can be undesirable for users unless it is optional, because users may want to share information about their transactions to enable others to leverage those transactions and share the resulting revenue with the users.[17]

More importantly for the Report, most DeFi service providers are unlikely to be able to affect what MEV-aware design choices are made on the level of the blockchain network

[11] 'MEV on Ethereum: A Policy Analysis' (n 1) 18.
[12] See also Tarun Chitra, 'Towards a Theory of Maximal Extractable Value II: Uncertainty' (2023) <https://drive.google.com/file/d/1mLrlYTy6SLPVg4by-PJ9wqEuFZJOjhG4/preview> 2 ('There have been a number of articles that have attempted to quantify [MEV effects on users - MB] (...) and the conclusions on the magnitude of user impact are inconsistent.').
[13] 'MEV on Ethereum: A Policy Analysis' (n 1) 18.
[14] For a recent overview and discussion of mitigation strategies, see, e.g., Conor McMenamin, 'SoK: Cross-Domain MEV' (2023) <https://arxiv.org/abs/2308.04159> section 3. See also 'Towards a Theory of Maximal Extractable Value II: Uncertainty' (n 12).
[15] See, e.g., Vitalik Buterin, 'Should Ethereum be okay with enshrining more things in the protocol?' (30 September 2023) < https://vitalik.eth.limo/general/2023/09/30/enshrinement.html >.
[16] I am not suggesting compliance efforts of this kind are effective or desirable, merely that there may be a tension between different policy solutions. See Mikołaj Barczentewicz, *Response to the U.S. Treasury Department's Consultation 'Ensuring Responsible Development of Digital Assets'*, Docket No. TREAS-DO-2022-0018 (3 November 2022) https://www.regulations.gov/comment/TREAS-DO-2022-0018-0039
[17] See, e.g., Flashbots, 'The Future of MEV is SUAVE' (23 November 2022) https://writings.flashbots.net/the-future-of-mev-is-suave/

(the protocol).[18] The Report is right to qualify its MEV-related recommendation (p. 33, emphasis added):

> Regulators should seek to hold a provider of a DeFi product or service responsible for identifying and, **to the extent practicable**, managing and mitigating the impact of MEV strategies used by miners/validators on the underlying blockchain on which the provider chooses to operate or offer the product or service.

It is vital to be realistic about the practicable extent of what service providers can do, especially in light of the lack of consensus over MEV-mitigating measures.

Service providers may be able to monitor the MEV strategies that could affect their users and inform the users about the mitigation measures that the users can take, but users may be uninterested in heeding the advice. For example, users may use Flashbots Protect[19] or MEVBlocker[20] to submit their transactions to the Ethereum network in a way that usually protects those transactions from being sandwiched.

Some DeFi service providers may be able to implement MEV-mitigating measures in their own services, but such efforts constitute experimentation in the context of rapid technological and economic change. For instance, the on-chain trading aggregator CoW Swap uses 'batch auctions with uniform clearing prices for all trades in the same batch.'[21] In effect, all CoW Swap transactions in one block have the same price, so the relative ordering of those transactions does not matter. However, such solutions also carry risks for users that may require mitigation.[22]

Conclusions: it's premature for regulators to intervene by imposing specific solutions

Regulators wanting to 'address' MEV face several challenges. First, we don't know which kinds of MEV —if any—have overall negative effects and may potentially call for policy responses. Analogies with traditional financial markets, especially ones that rely on the used language and not on the substance of the market practices, may be unhelpful. Second, even assuming that some instances of MEV should be mitigated, aside from the clearest cases that may call for enforcement (e.g., some uses of inside information), the best course of action for the regulators is to engage in a dialogue with the industry and academia. There is no one-size-fits-all 'solution' to MEV, and all the measures currently used or proposed come with trade-offs.

---

[18] Also, protocol-level measures may be less desirable than application-level measures, see 'Towards a Theory of Maximal Extractable Value II: Uncertainty' (n 12).
[19] Flashbots, 'Flashbots Protect: Overview' https://docs.flashbots.net/flashbots-protect/overview
[20] 'MEVBlocker' https://mevblocker.io
[21] CoW Swap, 'FAQ' https://swap.cow.fi/#/faq
[22] See, e.g., 'SoK: Cross-Domain MEV' (n 14) section 3.8 ('Batch Auctions/Batch Settlement').