My aim here is to give a general overview of potential legal and regulatory problems for MEV extraction and what could be done about that. Much of what I say here builds on a working paper that I co-wrote with my colleague, Alex Sarch: "Shedding Light in the Dark Forest: A Theory of Liability For Cryptocurrency 'MEV' Sandwich Attacks" (comments welcome!). This is not a detailed legal analysis and much more work still needs to be done on nearly every aspect of what I mention below. Please note that I'm a law academic, not a legal practitioner, so my perspective is likely more "big picture"-oriented.

The immediate issue: some MEV extraction looks like market abuse

Alex and I noted in the "Shedding Light" paper that at least some features of MEV extraction will likely look very suspicious to a regulator used to policing traditional finance. Bill Hughes and Gabriel Shapiro agree. The strategy that may look especially bad is sandwiching with the use of bundles (by sending a bundle e.g. to a block builder under MEV-Boost). As we suggested in the paper:

… in this scenario, the sandwicher, in a sense, "appropriates" another's trade. They do so by copying the publicly available data of a pending transaction and bundling it with their own front- and back-running transactions. The sandwicher pays a "bribe" for their bundle to be included with all three (or more) transactions precisely in the order set by the sandwicher. This could be seen as an express instruction to order transactions in a way that adversely affects another trader. We are not saying that this is necessarily manipulative in a legal sense, but merely that it is a situation different enough from what the courts and regulators are familiar with in traditional finance, that there is a risk they will be inclined to see it as manipulative.

Thus, MEV is very likely to attract regulatory attention in the near future. One thing that regulators may be inclined to do "by default" is to treat the problem by close analogy with traditional finance and begin enforcement actions based on theories of "fraud on the market" or "artificially affecting prices". Some forms of enforcement or other regulatory interventions may have relatively little effect on the broader DeFi and Ethereum ecosystem, but some may be very problematic (see the last heading below). Below, I flag some of the questions, which I think are very important for the choice of an appropriate legal and regulatory response. I suggest that there may not be too much time left for the community to think through those problems and to make the best case for the kind of policy response that would be truly social welfare-enhancing.

The big picture policy question: which MEV good, which MEV bad?

Individual welfare and legally relevant harm

Just because something is subjectively harmful to a person, it does not mean it is harmful in a sense that the law should be concerned with. If you buy an asset and the market price of that asset goes down, then you may consider yourself harmed, but the law should respond to that only if something special happened beyond merely losing money (e.g. if you were defrauded).

In the "Shedding Light" paper, Alex and I focused on sandwiches. In the section entitled "Are (All) Sandwiches Bad?" we went through considerations like the analogy between Uniswap V3 orders (with "amountOutMinimum" above 0) to limit orders and thus the possibility of arguing that a sandwiched user consents to any execution price that they get. Ultimately, we concluded that what is key for deciding whether the sandwiched users' loss constitutes legally relevant harm is whether the worse-than-non-sandwiched execution price is a result of "normal" or "manipulative" market activity. There are various ways to reason about that and I recommend the whole paper for our discussion (comments welcome!). At this stage we don't take a position, but we suggest that there is a significant risk that the regulators and the courts will see at least some sandwich attacks as manipulative (especially when using out-of-mempool bundling).

Social welfare / market efficiency

Even if some MEV extraction is - in a relevant sense - harmful to individual market participants, it could be that all-things-considered it is not reducing social welfare (e.g. through increasing market efficiency by a big enough margin). Some arguments that potentially could go in this direction are:

- "there can be scenarios where sandwich attacks increase efficiency and/or social welfare for users when n trades are routed across a network of CFMMs" (Kulkarni, Diamandis, and Chitra),
- MEV as a meaningful contribution to Ethereum's "security budget",
- block auctions (to the extent necessarily come with MEV extraction opportunities) as a superior solution to priority gas auctions.

Those arguments could work, but I'm not aware of anyone convincingly making the case for social-welfare-enhancing quality of some (all?) MEV extraction in a way that would be sufficient to convince policymakers or regulators. It may sound glib, but more research is definitely needed. What the crypto community should definitely not expect is that the policymakers will do this research on their own. It is much more likely that they will adopt the plausible assumption that what is individually harmful (and "weird" or "icky") is also socially harmful. The burden of proof is thus on the defenders of MEV extraction.

The other big policy question: can the law and regulation improve things?

Even if some MEV extraction is both harmful to individual market participants and reduces social welfare, it may still be that some - or all - possible legal and regulatory responses could be misplaced. For example, a legal response could reduce social welfare even more than the harm that it is meant to remedy. Legal and regulatory failures are arguably common, although it is usually hard to find consensus as to what things count as such (e.g. modern airport security - more of a compliance theater than a genuine benefit? what about AML / financial surveillance?).

This is why it is important to do rigorous cost-benefit analysis of regulatory interventions - especially if they are meant to apply in new contexts. Dealer-broker licensing may be a sensible measure in its current context, but licensing for block-builders or relay operators could be problematic. At the risk of sounding hyperbolic, a country that adopts such measures could be giving up on the benefits of decentralized and permissionless public blockchains, like Ethereum. And if that is a risk, then the benefits of intervention should be measured against the social benefits that would be lost.

I'm not suggesting that every state intervention is likely to have such serious systemic effects. If otherwise justified, individual prosecutions of searchers for out-of-mempool sandwiching may push such activity to other jurisdictions and thus give a competitive advantage to actors located there. But if only searchers are prosecuted (not base layer operators), then the risk of reducing geographic decentralization of the Ethereum network could be not too significant. Also, depending on what kind of MEV extraction is deemed illegal, it may be possible for Ethereum (and other blockchains) to prioritize protocol development in directions that would reduce the opportunity for such behavior (see my rough draft: Validator control as liability - comments welcome!). And if no one can extract value this way, then there is no benefit in fleeing to jurisdictions where it is legal.

My final point is that technical - especially protocol-level - solutions may be preferable to legal intervention. Hence, it is worth advocating for such technical work to be undertaken. But it is also worth advocating for the law not to disincentivize technical development. The latter point is important because, for example, introducing more on-chain privacy on Ethereum could turn it into more of a "privacy-coin" - with all the social benefits of that, but also with the risk of a conflict with AML or economic sanctions. This is not to say that sanctions or AML should not apply to Ethereum, but some sort of accommodation on both sides (software/protocol and the law) may be necessary.