I am posting this to gauge whether others have spent any amount of time thinking about how regulations might interact with MEV. Crypto is borderless, it does not exist within imaginary lines drawn on a globe. However, due to the nature of the geopolitical landscape, certain jurisdictions are in a position where they can impose their will much easier than others. With the recent crackdown on crypto banks, it is time to start thinking about what are the next possible attack vectors from the eyes of a regulator. So far it has only been the on and off ramps, not any crypto infrastructure.

I used to work at a think tank in Washington DC and focused on DeFi policy issues. There I noticed that government officials only paid attention to crypto things when they blew up in their face (FTX, Tornado Cash after the hacks, etc.). So this made me look at the learning curve of crypto and start to find areas on it that government officials have not gotten to yet, but they inevitably will. This is how I came across MEV and started researching it. What scared me the most in DC is that regulators have a much higher desire to learn than most lobbyists that represent the crypto industry. Government is already slow to react to things, but most lobbyists just react to what the government does, instead of being proactive on cutting edge issues. I think this also stems from a lack of education since crypto gets so deep and there are a million rabbit holes. Different regulators will probably care about different aspects of MEV. Commodities and Securities regulators will probably focus more on sandwich attacks and order flow topics, whereas sanctions and financial crimes regulators might care more about censorship topics.

Elizabeth Warren released a bill calling for unhosted wallets, miners, validators, nodes, and MEV searchers to register as Money Service Businesses with the Financial Crimes Enforcement Network. This would require them to KYC and collect information on every single party they interact with.

Let's theorize if this were to happen.

1. Wallet providers would send all information to some sort of government database. I imagine that only wallets that are created and maintained by a US company would comply, such as MetaMask. Since they would know who is initiating the transaction, they could censor transactions that originate from someone on a sanctions list. This would probably push people to use wallets that do not comply, at least those entities that are being censored. This would lead to less order flow origination to the wallet provider, possibly hurting their ability to be a major participant in the exclusive order flow game because users would switch wallets.

2. At which point, the government would probably go after the RPCs. This could get really interesting because some of the biggest RPC providers are US based: Alchemy and Infura. They would be forced to comply. Maybe they believe in decentralization so much they discontinue their services, but who knows. This would move customers to possibly adopt non-censoring RPCs. This could provide an opportunity for wallets that offer a good UX to switch RPCs.

3. Requiring a searcher to KYC makes no sense to me. Maybe someone has some good thoughts. Seems like she just wanted to put the words "MEV Searcher ‘' out there to scare people. I cannot imagine many searchers willingly KYCing themselves. Who would be in a position to force them to KYC? Maybe builders, if they comply, would not accept blocks from non-KYCed searchers. This would probably cause the builder to lose an edge because they would not have as profitable blocks.

4. The next entity on the MEV supply chain is the relay. Maybe relays run by American companies would not accept blocks from builders that do not KYC. This too would lead to a loss in competitive advantage.

5. Validators forcing KYC could be scary, considering Coinbase and Kraken are two of the biggest. Also some Lido node operators are American. Maybe Lido just could stay away from node operators that KYC. Validators that KYC would also lose market share if they are unable to validate some blocks because they are not KYCed. This would lead to a reduction in rewards which would cause people to go stake elsewhere, leading to less market share for KYCing validators.

This would probably just move a lot of entities offshore so they do not have to comply. I think the United States would be overplaying its hand if it were to go to these measures. It would be interesting to see how US companies that offer these services react.

Also sequencers are an obvious attack vector. Even though rollups have escape hatches, a censoring sequencer would make that rollup less used IMO. I think BASE will be a great case study for this. The race to decentralize the sequencer is more important than ever! In a world where there are rotating sequencers, those that censor will likely lose their edge.

I think sandwich attacks are an easy narrative to exploit for right now, but as solutions such as MEV Share become reality, it will be harder to push that narrative. MEV Share and Order Flow Auctions might present an opportunity to write the narrative of "best price execution" in a good way if there are some sort of rebates or kickbacks to users.

Something that I have not thought too deeply on, but could raise some eyebrows is blocks being built in an SGX. I do not know what attack vector the government could take, but maybe someone else has an idea.

The United States Treasury just released a report about the risks of DeFi. It basically calls for a change to the regulatory regime to make sure DeFi falls under the watch of the government so it can be in compliance. It does not explicitly mention MEV but it does allude to it in the following:

"This could enable a small group of persons to make decisions about the types of transactions that are supported by the blockchain, including the ability to approve certain transactions, or the order in which transactions are settled."

I would love to hear others' thoughts on any of the above.

Some questions to think about

1. While I personally think the US is on the decline over the coming decades, and crypto will be around a lot longer than the US, it is worth determining the extent to which we should engage with policymakers to support what we're trying to build (or at least so they don't kill it). There's a lot of muscle memory on the Hill left over from the high frequency trading / hedge fund hearings back in the day, and there may well be a reflexive policymaker response that mirrors that. How much effort should we put into trying to shape the story, when there are limited resources and that energy could be spent building?

2. If it is worth putting considerable resources towards this effort, what are the best ways to approach it? There are multiple industry groups. From my experience, the one who thinks about MEV the most is the Proof of Stake Alliance. Maybe we put resources behind them? Do we form an MEV specific group? Do we try to find lobbyists with shared principles relating to MEV?

3. Is the United States the only government worth trying to influence? What about the EU? Emerging markets?

4. What aspect of MEV do you think is of the most concern? Censoring? Sandwich attacks? Other areas?

5. How do we prevent centralization vectors from being attacked, such as RPCs, sequencers, relays, etc?

Thanks to Fred for the inspiration to write this post, editing my drafts, and challenging my thought process

Thanks to Tom Schmidt, Nick Matthew, & Alex Grieve for their thoughtful feedback and suggestions