MEV… do this.

Pmcgoohan

Follow

--

Listen

Share

(This article is a response to Philip Daian's blog post 'Mev… wat do?')

"MEV is not a fundamental law of the universe, it is the exploitation of a network vulnerability that is our responsibility as developers to fix"

Dear Phil,

I wanted to respond to your blog post.

Debating the issue of Miner Extractable Value (MEV) is vital, so I'll go through your points in turn:

On Cryptographic transcriptability

"All distributed systems that can function as currencies must contain the key property of auditability, or the ability to validate system state transitions and/or user actions"

A well designed content consensus layer is publicly auditable. In my example the behaviour of all participants is visible and block content is fully recreatable from it.

On Interoperability under heterogeneous trust

"even if ETH had 0 MEV, there would likely be MEV available arbitraging Binance Smart Chain with ETH, especially available to those validating both"

Absolutely this will always exist, and this kind of arbitrage is vital to price discovery. I would never suggest that it is possible or even desirable to avoid it.

MEV is not simple latency arbitrage. MEV is when you see a transaction in the pool that the originator cannot retract and insert your transactions before or after it or both.

There is no transfer of information in this case, no greater efficiency, no invisible hand of the market. It is the base extortion of a powerless victim by a privileged one. MEV is not a fundamental law of the universe, it is the exploitation of a network vulnerability that is our responsibility as developers to fix.

By selling block content to the highest bidder, a new attack vector has been inadvertently created: order flow manipulation. This was unworkable when content creation was fragmented between miners, but now the richest can pay to trade against the poorest when it suits them, as well as hoovering up all the usual MEV.

There is currently no visibility of this kind of order flow manipulation in MEV-Inspect.

Permissionlessness

"in Uniswap, without the MEV provided arbitraging markets with external/centralized exchanges and fellow dexes, the price would not reflect the market and not provide a useful trading product for users"

See above. Again this is conflating price discovery by arbitrage with MEV the exploitation of a vulnerability.

"Assuming you buy my arguments up until here"

I don't and I have explained why, so please take that into account as I continue.

"every validator must extract available MEV at around the same rate…a system where validators 'leave MEV on the table' is one where an obvious attacker subsidy is readily available. To keep our economic assumptions strong, we must therefore keep MEV extraction efficient and democratic."

Not if you change attestation so that it requires valid consensus content or will fail. Then validators can't exploit users for MEV at all.

"One natural question to those new to the MEV landscape is 'why not slap a fairness protocol on it (Layer 1) and be done?… claims that any of these designs are silver-bullets for better fairness often stems from their analysis in an isolated model that

does not adequately capture real-world complexity”

Well I’m not new to the MEV landscape. I was the first to identify the issue pre-genesis in 2014.

On fairness, consider these two systems and you tell me which one is more fair:

(A) allow a single actor full control over transaction inclusion and ordering so that they can frontrun, backrun, sandwich and generally exploit every other user’s transaction in a block with impunity. Now create an auction market so that the wealthiest will always be that actor.

OR

(B) build a consensus view of the mempool ordering transactions by time where it is discoverable.

It’s surely (B), because if it isn’t you wouldn’t be working in blockchain technology. If you were to choose (A) instead it would mean that you are opposed to consensus mechanisms. If that is the case, why not hand the structural layer of the blockchain to a centralized authority as well as the content layer? Imagine the MEV we could extract then! Epoch upon epoch of it… But that is not the Ethereum project. We are decentralizing.

Back to fairness… we then have that some fairness protocols will work for some users. Others will work for others. Which protocol is more fair?

No one would seriously call (A) (what we have now) a candidate for a fairness protocol. You ask which of several Aequitas protocol variants are more fair than this:

The truth is that any of the protocols you have circled are more fair. Pin that table on the wall. Now blindfold yourself and throw a bun at it and you’ll hit a protocol which is a vast improvement over the literal worst case of total miner dominance that we have now.

This leads me to an observation. As lead author of Flashboys 2.0 you are responsible for one of the most academically rigorous papers ever published on the Ethereum experiment. It is certainly one of the most important. You clearly spent years researching it and I, for one, am extremely grateful to you for this hard work.

This seems incongruent with your thesis that MEV is inevitable. How did you arrive at this conclusion? Where is the paper produced with the same intellectual rigor as Flashboys 2.0 debating this point? Where is the trail of Github repos where you tried in vain to address MEV, the failure of which led you to declare the problem insoluble? Democratizing the exploit of a vulnerability is surely the last resort once every other attempt to fix it has failed.

Imagine if when the Heartbleed vulnerability was discovered, the OpenSSL devs decided it was too difficult to fix. Instead they released code that enabled everyone to read everyone else’s encrypted passwords, emails, messages, etc because at least that would democratize access. I doubt anyone would still be using OpenSSL.

You and Flashbots are perfectly positioned to tackle this problem because you have done exactly what needs to be done already: create a distributed content layer. The MEV-Geth project is perhaps the only content layer possible on mainnet right now without creating an unacceptable fork risk.

But… if released on eth2 and rollups, MEV Auctions would enshrine the right of those securing the network to exploit it. Once that sense of entitlement exists with validators as it does now with miners, there is no turning back without fork risk.

So please, question your assumption that MEV is inevitable. Apply the same scrutiny to the idea that you did to MEV in 2019 and join those that are looking for solutions. Expectations are being set now for eth2 and rollups and for the future of the network. As the recent miner reaction to EIP 1559 shows, there is heavy resistance to even trivial changes once those expectations become feelings of entitlement.

What you choose to do now will decide the success and integrity of Ethereum forever.

Please choose well.

Sincerely pmcgoohan.