Special thanks to Vitalik for much of this, Phil Daian as well (& his amazing research on MEV), Barry Whitehat for also coming up with this idea, and Ben Jones

for the rest!

Blockchain miners (also known as validators, block producers, or aggregators) are nominally rewarded for their services by some combination of block rewards and transaction fees. However, being a block producer tasked with producing a particular block gives you a lot of power within the span of that block, letting you arbitrarily reorder transactions, insert your own transactions before or after other transactions, and delay transactions outright until the next block, and it turns out that there are a lot of ways that one can earn money from this. For example, one can front-run decentralized exchanges (both Uniswap-style and the order book variety), be the first to claim whistleblower rewards, have a favorable position in ICOs, as well as many other forms of mild manipulation of applications. Recent research shows that the revenue that can be extracted from this (called "miner-extractable value" or MEV) is potentially significantly higher than transaction fee revenue.

Frequent batch auctions are one traditional response to market manipulation by reordering. In an FBA, instead of processing transactions "as they come", a market gathers all transactions submitted within the same time span (could be short eg. 100 ms, or a minute or longer), reorders them according to a standard algorithm that does not depend on order of submission, and then processes them in that new order. This makes micro-scale timing manipulation nearly irrelevant.

We propose a technique in a similar spirit to how FBAs remove micro-scale timing manipulation, with one major difference. In an FBA, there is only one application, and so there is one natural "optimal" order for transactions (orders): process them in order of price. In a general-purpose blockchain, there are many applications with arbitrary properties, and so coming up with a "correct" order is virtually impossible for a fixed algorithm. Instead, we simply auction off the right to reorder transactions within an N-block window to the highest bidder

. That is, we create a MEV Auction (MEVA), in which the winner of the auction has the right to reorder submitted transactions and insert their own, as long as they do not delay any specific transaction by more than N blocks.

This creates a form of "managed centralization": a single sophisticated party wins the auction and can capture all

of the MEV. We call this party a "sequencer." Having a single sequencer reduces the benefit to other block proposers of using "clever" algorithms to near-zero, thereby increasing the chance that "dumb" block proposers will be long-term viable and hence promoting decentralization at the block proposal layer. This technique can theoretically be used at layer 1, though we also show how it is a perfect fit for layer 2 systems, particularly systems such as Optimistic Rollup, zkRollup, or Plasma.

This mechanism is designed to extract MEV for the sole purpose of supporting our (inclusive) blockchain community. In fact, this mechanism could be the revenue stream for opt-in self governance built to fund the internet's public goods. We mustn't participate in an MEVA which funds things we don't like!

MEV Auction on top of Gas Price Auction

Control over transaction ordering has become extremely profitable especially as smart contracts like Uniswap have gained popularity. There have been multiple occasions where trades on Uniswap with high slippage caused tens of thousands of dollars in free arbitrage profits.

These arbitrage opportunities are taken advantage of by arbitrage bots that watch the blockchain and participate in the gas price auction. These bots outbid each other at high frequency as long as the price they pay for the transaction is not excess of the amount of money they stand to make. Frontrun.me has great information collected on these auctions happening in the background of Ethereum every day.

Counter-intuitively, the real winner of these auctions is Ethereum miners

, as bots which outbid each other raise the gas price. This increased gas price increases miner fees and revenue. By introducing an MEV Auction in addition

to this gas price auction we can employ the same market mechanism that extracts frontrunning fees to be directed at miners, and redirect that profit back to the community.

[

1482×462 73.8 KB

](https://ethresear.ch/uploads/default/original/2X/2/29eefa9820ab10319cf522474a17798c420748a5.png)

Implementing the Auction

The auction is able to extract MEV from miners by separating two functions which are often conflated: 1) Transaction inclusion; and 2) transaction ordering. In order to implement our MEVA we can define a role for each function. Block producers

which determine transaction inclusion, and sequencers

which determine transaction ordering.

Block producers // Transaction Inclusion

Block proposers are most analogous to traditional blockchain miners. It is critical that they preserve the censorship resistance that we see in blockchains today. However, instead of proposing blocks with an ordering, they simply propose a set of transactions to eventually be included before N blocks.

Sequencers // Transaction Ordering

Sequencers are elected by a smart contract managed auction run by the block producers called the MEVA contract. This auction assigns the right to sequence the last N transactions. If, within a timeout the sequencer has not submitted an ordering which is included by block proposers, a new sequencer is elected.

Sequencers and Instant Transaction Inclusion

In addition to extracting MEV, the MEVA provides the current sequencer the ability to provide instant cryptoeconomic guarantees on transaction inclusion. They do this by signing off on an ordering immediately after receiving a transaction from a user – even before it is sent to a block producer. If the sequencer equivocates and does not include the transaction at the index which they promised, the user may submit a fraud proof to the MEVA contract to slash the sequencer. As long as the sequencer stands to lose more than it can gain from an equivocation, we can expect the sequencer to provide realtime feed of blockchain state which can be monitored, providing, for instance, realtime price updates on Uniswap.

Implementation on Layer 2

It is possible to enshrine this MEVA contract directly on layer 1 (L1) blockchain consensus protocols. However, it is also possible to non-invasively add this mechanism in layer 2 (L2) and use it to manage Optimistic Rollup transaction ordering.

In layer 2, we simply repurpose L1 miners and utilize them as block proposers. We then implement the MEVA contract and designate a single sequencer at a time. (Note: Interestingly the single sequencer can also be run by a sub-consensus protocol if desired.)

In fact, using MEVA for layer 2 is a perfect fit as it allows us to permissionlessly experiment with different parameters for the auction while simultaneously realigning Ethereum incentives to direct revenue back into the ecosystem. This may serve as the primary revenue stream for blockchain self-sustenance.

Considerations

MEV Auction Collusion

One concern is auction collusion. Bidders colluding to reduce competition and keep the auction price artificially low breaks the ability to accurately discover and tax the MEV.

A mitigation is to simply increase the ease of entering the aggregation market by releasing open source sequencer software. This can help to establish a price floor because with low barriers of entry we can expect enough competition that there will be at least one honest sequencer bid.

Long term incentive alignment

The most naive way to implement MEVA is by holding a first-price auction once a day, giving the winner of the auction a monopoly on block production for that day. All proceeds raised by the auction are then sent into a public goods fund. Unfortunately, this approach has a serious problem: an attacker need only outbid the aggregation costs for a single time-slot in order to become the selected sequencer and degrade network quality.

Adding the equivalent of a security deposit for the sequencer goes a long way to help mitigating this problem. If the sequencer degrades network quality at any point during their slot, they should be penalized in proportion to the amount of harm they cause to the network. This can be implemented as a simple bond which can be slashed by a subjective judgement of misbehavior, or by locking up an asset which has a price correlated with the health of the network. Note that sequencer misbehavior can often come as a non-uniquely attributable fault and so unfortunately require subjective judgements to enforce.

The Parasitic L2 Problem

Layer 2 mining has gotten bad press for diverting revenue away from L1 miners who secure the network. Diverting revenue from L1 implicitly decreases the security budget, and thereby makes it less costly to perform 51% attacks.

While I wish there was a clear mitigation, in reality the parasitic L2 problem deserves much more research & risk analysis. It could be the case that L2 chains drive up demand for L1 enough to keep the price of ETH high, or ETH remains valuable because it is seen as money, or we simply use out-of-protocol means to protect our most critical blockchains. This remains to be seen and is a great area of research.

Path Forward

Designs like these are critical for framing the coming wave of Ethereum upgrades as not only innovations in scalability, but also as an opportunity to realign incentives to be pro-community, pro-commons, and pro-public goods. Without serious thought around how we will sustain blockchain technology we risk creating resilient decentralized architectures which eventually crumble due to massive economic centralization. This is not a future anyone wants to live in.

Thankfully, these designs show the possibility of encapsulating and reinvesting MEV back into the community. Further research and economic models will be key as we bring these systems into production. Let’s do it!