Bizantine Capital 

MEV Trilemma

How Zero-Knowledge Proofs Will Reduce MEV on Ethereum

Co-written by Andrew Bakst, March Zheng, and Cameron Sepahi
Published on the 15th of July, 2021

Introduction

Historically, miners of public blockchains have generated revenue through a combination of inflation and transaction fees. However, as one blockchain, Ethereum, has grown to subsume the world's financial sector, a new revenue source arrived, known in the crypto industry as miner or maximal extractable value (MEV). MEV is the additional revenue generated by miners through determining the order of transactions on the Ethereum blockchain.

Background - Why Order Matters

Users broadcast transactions to the Ethereum network and specify a gas price which indicates how much they are willing to pay for miners to execute their transaction. Historically, miners, as economically-incentivized actors, attempted to maximize the value received from fees from transactions through ordering the blocks by gas price. They executed this algorithmically by ordering transactions in the mempool, a data structure inside an Ethereum node that stores candidate transactions before they are mined [1].

MEV was the realization that transaction fees were not the only way that miners could maximize revenue from transactions. As decentralized finance boomed, miners realized that they could extract further value by reordering transactions to take advantage of arbitrage and liquidation opportunities. For instance, an arbitrage opportunity might allow a miner to obtain $10k of revenue, whereas the transaction fee for that opportunity might only be $10. Miners then become incentivized to execute the arbitrage opportunity, ignoring the person who sent the initial arbitrage transaction, making 1000x the revenue from that transaction.

This process has collectively resulted in ~$765M USD of value extracted on Ethereum, with decentralized finance only about a year old [2]. Miners can extract value through dropping or postponing transactions within a block, freely re-ordering all transactions (with some limits), or creating their own transactions in response to seeing transactions in their local pool.

There effectively exist six instances (a 2 x 3 matrix, although one column is much larger than the other) of MEV: 97% are associated with arbitrage trades and 3% are associated with liquidations of undercollateralized loans [3]; within these buckets, MEV is extracted through tactics known as frontrunning, backrunning, and sandwich attacking [4] [5]. In almost all cases of MEV, many arbitrage and liquidation bots compete for the same transactions, resulting in congestion and higher gas prices on Ethereum. This problem, however, has been suppressed through flashbots, an MEV solution that will be elaborated on later in this article.

Solutions With Negative Tradeoffs

Given how MEV continues to instigate negative externalities and reduced user experience on Ethereum, there have been both theoretical and applied solutions to the problem [6]. One of the first proposed solutions to MEV was put forward by Optimism; on the Optimism layer-two network, the traditional role of "miners" would be divided into sequencers and validators. The sequencers (a role auctioned off to the free market by validators) would have the responsibility of ordering transactions, while validators would be responsible for submitting these transactions

to the Optimism blockchain. In this free-market auction construction, those who attempt to extract MEV need to bid for the right to reorder transactions. Optimism further proposed that a portion of the funds from sequencer auctions be transferred to the Optimism team to sustainably fund their development. Optimism has just launched, and it remains to be seen if they push forward their past proposal on their mainnet, or they could attempt to run a significant portion of validator nodes, which would have a similar effect.

A similar solution was proposed by Futureswap, where trusted entities would be in charge of sequencing transactions and then signing them to an oracle relayer network [7]. This, however, would fall under the same fate as Optimism, where the users have to trust a central entity to perform some form of work, should Futureswap or Optimism derive most of their value from their auction revenue share. It remains to be seen whether crypto users would trust centralized entities to such an extent on layer-two networks; some data argues yes, others no.

Arbitrum, extending Optimism's proposal, theorized the creation of a fair ordering mechanism where the majority of the network agrees on the state of ordering before execution. These fair ordering algorithms would be implemented by having ⅔ of the network agree on the state of ordering before execution (similar to Tendermint/BFT consensus). Although this partially addresses MEV mitigation and decentralization, it decreases efficiency by introducing an extra state load operation than Optimism or Futureswap's solution, thereby reducing throughput on the execution layer.

Flashbot Auctions - The First Success Story

Just this year, a successful solution finally reached mainstream. Flashbots is an off-chain three party marketplace that consists of searches, relayers, and miners. Each individual party specializes in performing a certain type of job to maintain the correct state of communication. Flashbots' innovation was to use a first-price sealed bid-auction mechanism to give users the option to privately communicate their bid and transaction order preference without paying for failed bids or revealing the content of the bid.

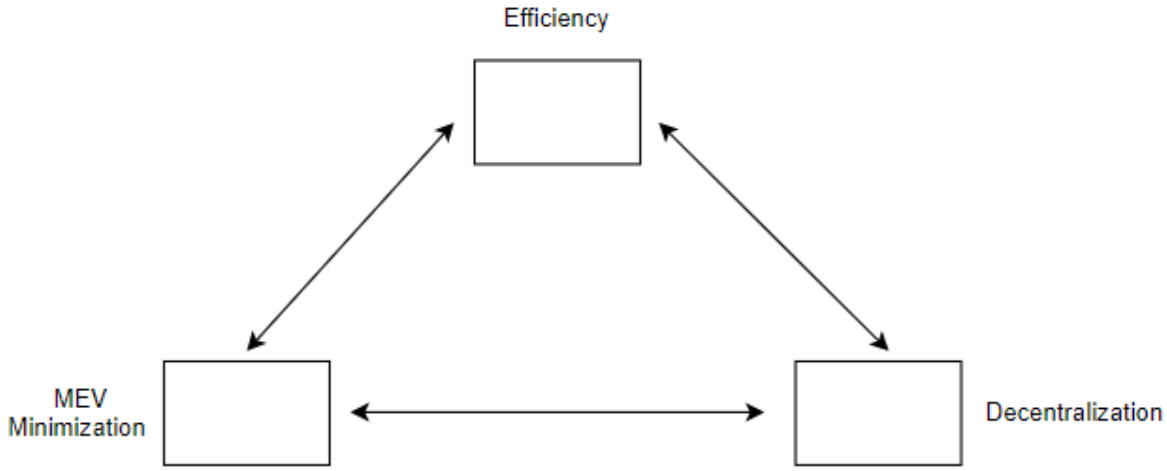
Searchers typically include bot operators that scan for arbitrage/liquidation opportunities, users looking for frontrunning protection, or projects/frontends that are seeking to abstract MEV from end-users. Their job is to bundle transactions within a private transaction pool and send that state to the **relayers**. Before propagating this state to miners, relayers first validate the transaction bundle to mitigate DoS (denial of service) attacks. Subsequently, this new state is transferred over to the **miners**, who run an mev-geth client connected to the flashbots network to begin mining the most profitable blocks [8].

Although the mev-geth client has been adopted by many miners, flashbots has not minimized MEV, but rather democratized it. Some may even argue that flashbot auctions has increased

MEV by making it easier for miners to extract the most value possible from users' transactions. With that being said, however, flashbot auctions is very efficient and relatively decentralized (because anyone can become any party in the flashbots marketplace, meaning centralization via the existence of relayers is only driven by economies of scale) [9].

MEV Trilemma

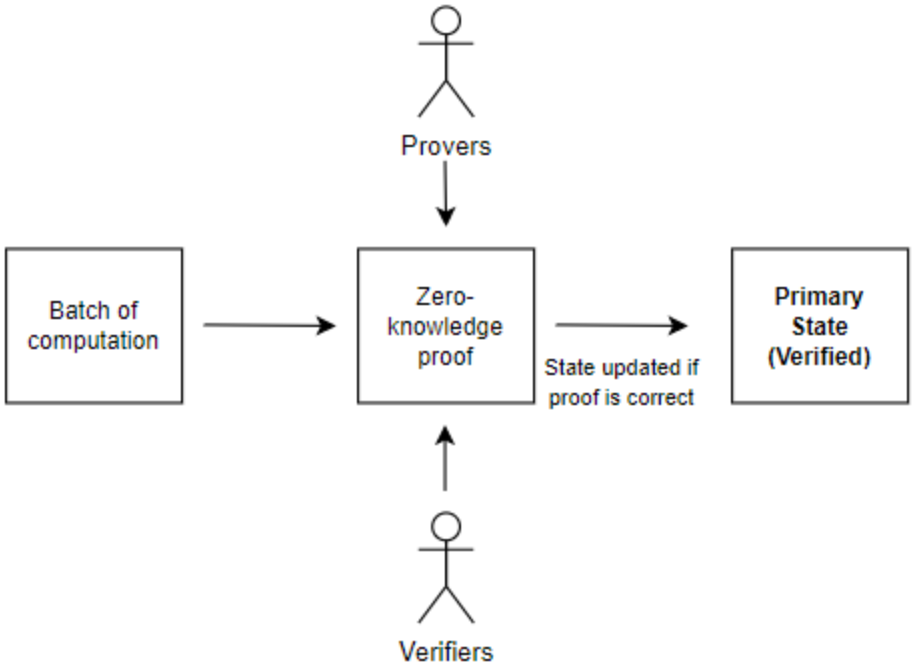
Given these solutions and the current tools proposed and implemented, no current methodology exists that can reduce MEV and not have some degree of negative implications on users. This is because of a fundamental MEV trilemma that currently exists on public blockchains, but really just Ethereum since Ethereum is the only public blockchain:



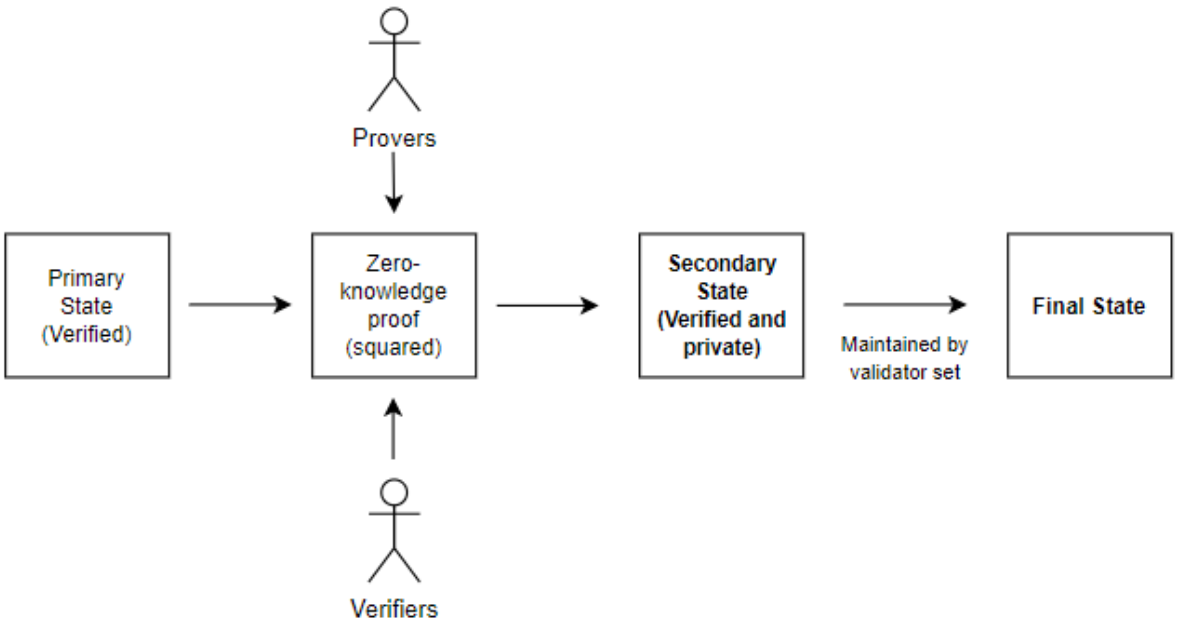
Zero-knowledge Rollups

The fundamental problem resulting in the MEV trilemma stems from miners being able to see transactions. If transactions are obscure, MEV is effectively solved. Ironically, the same technology that enables privacy also enables scalability of public blockchains. Zero knowledge proofs are the solution to all of our problems.

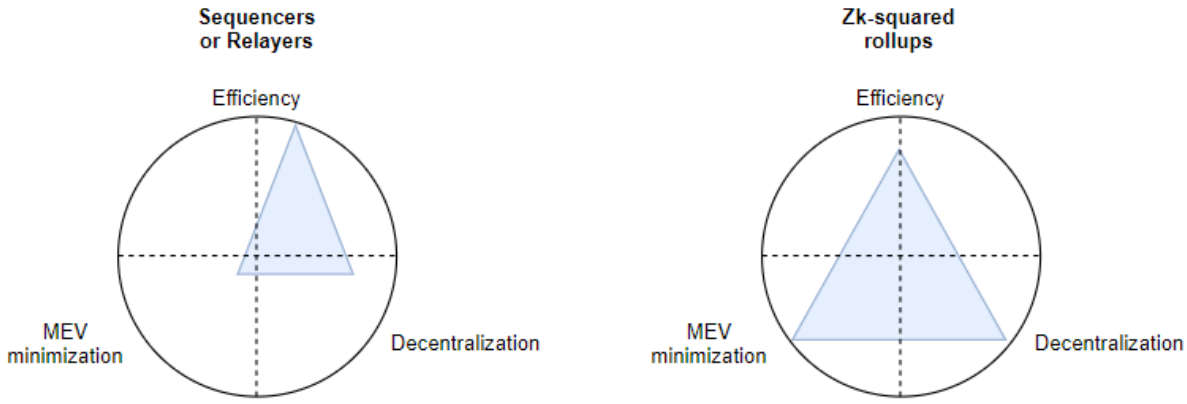
Zk-rollups batch computation in a multi-threaded fashion. Subsequently, this state is validated by verifiers, who only update the state of the thread if the proof is correct (significant computational load is abstracted away because validators only need to verify the correctness of the thread rather than the full computation of it).



Although zk-rollups are capable of achieving up to 100,000 transactions per second with data sharding, MEV would still occur as all transactions remain public and thereby capable of being reordered [10]. However, if a secondary state containing another layer of zero-knowledge proofs is introduced, transactions could be made private, making it impossible for MEV to be extracted. We refer to this as zk-squared:



In this scenario, however, an extra state load operation is still introduced, rendering less efficiency. Therefore, individual markets with zk-squared rollups could be introduced, giving Ethereum users more options so they don't have to be subject to MEV. As zero knowledge proofs continue to scale, the cost of the inefficiency would only decrease over time.



As illustrated in Bizantine's Law, the exponential increase in efficiency of zero-knowledge proofs and other cryptographic technologies will happen, accelerating this inevitable process.

In the short-medium term, it seems MEV will be maximized on Ethereum, through efficient and decentralized marketplaces. However, with time, MEV will be sufficiently minimized through zero-knowledge proof efficiency gains. Ethereum will continue to become a more user-friendly network over time, as its network effects render it the most valuable asset known to mankind [11].

Endnotes

[1] Mempool

[2] Flashbots MEV Dashboard

[3] Because Ethereum is an open network, anyone with internet connection can attempt to take advantage of these lucrative financial opportunities)

[4] Frontrunning the MEV Crisis

[5] Liquidity attracts MEV, which is why 66% of all extracted MEV occur on Uniswap and Sushiswap, the two most used decentralized exchanges (MEV does not exist on centralized exchanges, although one could argue that Robinhood's popular payment for order flow model is a form of MEV in traditional finance)

[6] During the ICO boom of 2017, market participants bid high gas prices on Ethereum to receive priority on their transactions; as a result, several projects came up with a possible solution involving setting a limit on gas prices so users won't be able to bid beyond a certain threshold. This did not bode well for the projects as users spammed the network by executing many transactions with lower gas prices.

[7] In charge of confirming transaction validity and updating that state on-chain with current asset pricing: Oracle Relayer Network - Futureswap v2

[8] Mev-geth is a fork of Ethereum's geth client (command line interface for running an Ethereum node) that includes the flashbot auctions mechanism illustrated above.

[9] Flashbot Docs

[10] Shard Chains

[11] ETH, The World's Most Valuable Asset