Raphael Auer
raphael.auer@bis.org

Jon Frost
jon.frost@bis.org

Jose Maria Vidal Pastor
JoseMaria.VidalPastor@bis.org

Miners as intermediaries: extractable value and market manipulation in crypto and DeFi – online appendix

This online appendix further explains the concept of miner extractable value (MEV) and how it is measured.

The mechanics of miner extractable value

In a blockchain such as Ethereum, a decentralised network of validators or miners competes to add new entries ("blocks") to the public ledger (the blockchain). Users wishing to transact can put in transaction requests, together with a base fee (that is destroyed or "burned") and a priority fee (the "Tip" that goes to the miner); pending transactions are included in the memory pool or "mempool". MEV arises from the power of miners to include, exclude or reorder transactions in the blocks they add to the blockchain.

In the bulletin, we discuss an example of sandwich trading by a miner with transactions in USD Coin (USDC) and Ether (ETH). Specifically, we start from a situation in which there are four transactions (TX) in the mempool – two for buying and two for selling ETH, with varying levels of Tips. In this case, the miner should select TX1 and TX4, as these offer the highest Tip. However, the miner also observes TX3, a sell order for 10,000 USDC, at the exchange rate observed at that moment, which could have a market-moving impact on the price of ETH. Even though this transaction has a lower Tip, the miner intervenes by selecting this transaction and placing its own trades just in front of and behind the selected transaction. The miner sells 5,000 USDC and receives 2.3 ETH just before adding the sell order transaction of 10,000 USDC, which now exchanges for 3.5 ETH. Then the miner includes a second transaction (MEV2) just after transaction 3, this time to sell the 2.3 ETH previously obtained in MEV1.

In a decentralised exchange (DEX) such as Uniswap, the exchange rate between USDC and ETH is determined by the following constant product function that links relative prices and quantities (also known as the bonding curve):

$$\text{Amount of token X} * \text{Amount of token Y} = \text{constant}$$

As can be seen in Table 1, before the pending transactions within the mempool are included in a block, the price of 1 ETH is equal to 2,000 USDC or $2,000 in our example. The miner can calculate by how much the price would move, given the large purchase order in the mempool (TX3).

Liquidity pool with sandwich attack[1] Table 1

	USDC	ETH	constant	Δ in USDC	Δ in ETH	ETH/USDC
initial state	50,000	25.0	1,250,000			2000
MEV1	55,000	22.7	1,250,000	5,000	-2.3	2420
TX3	65,000	19.2	1,250,000	10,000	-3.5	3380
MEV2	58,130	21.5	1,250,000	-6,870	2.3	2703

[1] Assuming 1USDC=$1. MEV = miner transaction; TX = transaction.

Source: Authors' elaboration.

After verification, the miner acts by entering a buy transaction (MEV1) just before TX3, and immediately afterwards a sell transaction (MEV2) in the same amount as MEV1. In a matter of minutes, the miner can earn a profit since, as can be seen in the table, the price of ETH has appreciated in value.

Further miner extractable value strategies

Front-running: this is the most common strategy used to extract value from the managing of the blocks. Transactions are "announced" in what is called a priority gas auction (PGA). Miners can give priority to a new transaction with a higher gas price than the existing pending ones, realising an instant profit with a very simple strategy. An example would be to assure execution of a needed transaction to rebalance a pool.

Back-running: in this strategy, the miner places a lower-fee transaction just after a higher-paying one. For example, this can be to execute a sell transaction immediately after a buy order, or buying new tokens just after they are issued.

DEX arbitrage: this is a common strategy that exploits the arbitrage between the price differences of the same asset/token/coin in different DEXs. It consists in buying the token in the DEX with a lower price and selling it afterwards in the higher-paying DEX.

Liquidations: in lending protocols, users can borrow a certain percentage of the collateral posted (token) in a different token. Since the value of the collateral fluctuates with the market this can trigger a liquidation of the collateral. The borrower is asked to pay a substantial liquidation fee as a penalty. Searchers (miners) look for possible liquidation transactions to enter into and collect the liquidation fee.

Replay attacks: these attacks involve cloning and front-running a victim's trade (Qin et al (2021)).

Time-bandit attacks: in this strategy, miners rewrite blockchain history to steal funds allocated by smart contracts in the past. These attacks can be especially damaging to the ledger's integrity as they can reverse transactions that users thought were already final. It has been argued that these attacks may increase over time and even pose existential risks to the Ethereum blockchain (Daian et al (2019)).

There are other emerging strategies that are arising at the same time that the development of the crypto markets such as in the non-fungible token (NFT) space.

Methodology for the measurement of MEV

This bulletin uses data from MEV-Explore and Qin et al (2021).

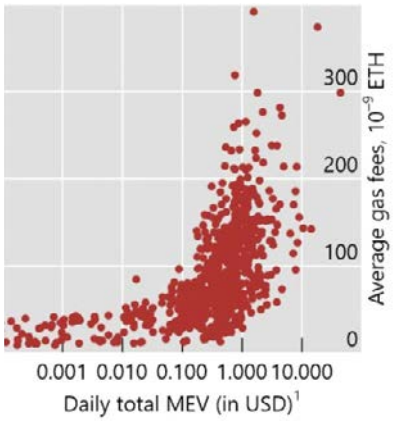
MEV-Explore focuses on the MEV actually extracted on-chain rather than the total MEV potentially available in any given block. The estimated MEV metric used constitutes a lower-bound estimate, limited by the current set of nine DeFi protocols covered by MEV-Explore (Aave, Balancer, Bancor, Compound, Cream, Curve, Uniswap V2, Uniswap v3, 0x). In addition, it does not cover all types of market manipulation. The data are collected by fetching each transaction's trace and "decoding" it using protocol-specific inspectors and action-specific reducers. These transactions are then inserted into a common database. Inspecting them allows users to see the full token flow during the transaction, and to get higher-order information, eg the profit amount and token of an arbitrage transaction. After all transactions have been aggregated, data are expressed in USD at market values at the time of the trade.

Data coverage starts in the first block of 1 January 2020. Extracted MEV is the result of adding successful MEV transactions, the gas fees (paid to miners) from successful MEV transactions and the gas fees from failed MEV transactions.

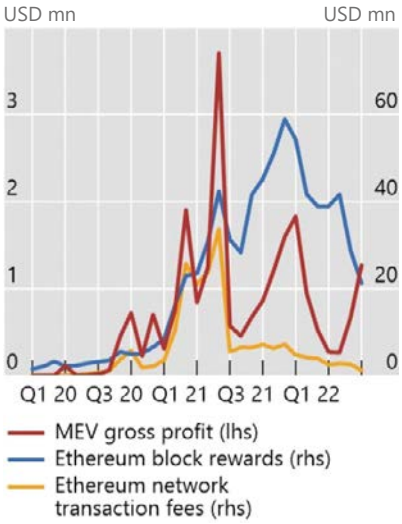
MEV has costs beyond the direct costs for users. In particular, it uses up scarce network capacity and bids up gas fees. Indeed, measures of MEV are higher on days with higher gas fees (Graph A1, left-hand panel). In some cases, successful MEV transactions have used up to 3% of total block gas (centre panel). MEV-Explore estimate that the majority of MEV has come from Uniswap V2 and V3 (right-hand panel).

MEV rises on days with higher ETH gas prices, and it uses up network capacity Graph A1

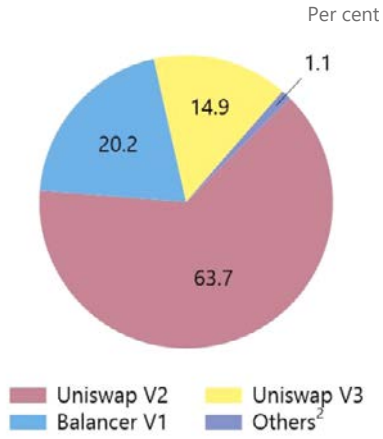
Gas fees are higher on days with more MEV



Rewards to miners in the Ethereum network



Cumulative extractable MEV by protocol



[1] Logarithmic scale. [2] Includes Aave, Bancor, Compound V2 and Curve.

Sources: Bloomberg; Etherscan.io; MEV-Explore v1; authors' calculations.

Qin et al (2021) quantify extracted value from the Ethereum blockchain focusing on four types of attack. They look at arbitrage and sandwich attacks on eight decentralised exchanges (Uniswap V1/V2/V3, Sushiswap, Curve, Swerve, 1inch and Bancor), liquidations on four lending platforms (Aave V1/V2, Compound and dYdX) and transaction replay in all Ethereum transactions. The data cover the period from December 2018 (block 6,803,256) until August 2021 (block 12,965,000).