

Maximal Extractable Value

Blockchain-based Systems Engineering

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de

1. Motivation
2. Maximal Extractable Value
 - Overview
 - The Impact of MEV on the Blockchain Ecosystem
3. MEV Assessment
4. Outlook

- Block proposers add any transaction they hear about into their mempool.
- Since the **block size is limited**, block proposers usually select a **subset of transactions** from their mempool.
- *What is the **motivation** for a block proposer to include transaction A over B in a block?*
 - **Transaction fees** - While issuing a transaction, the wallet owner also sets a transaction fee (*bribe*) to be given to the block proposer
- We can assume that any *rational*¹ block proposer will order transactions in mempool based on the transaction fee they offer.
- However, this may not always be the case...

Remember

- In typical blockchains (e.g., Ethereum 1.0), miners, or more generally block proposers, can see the content of transactions in the mempool (**transparency**), choose the ones to be included in a block, and determine their order inside the block.
- Before including a transaction in a block, miners can simulate it and see if they can make a profit by issuing the same transaction themselves (e.g., a transaction that buys some token on exchange *A* and sells it on *B*).
- If a transaction yields profit, a miner can just issue a duplicate transaction and place it in front of the “original” transaction, in order to be the first to leverage an opportunity.
- Hence, miners hold the **ultimate power** in typical blockchains.

1. Motivation

2. Maximal Extractable Value

- Overview
- The Impact of MEV on the Blockchain Ecosystem

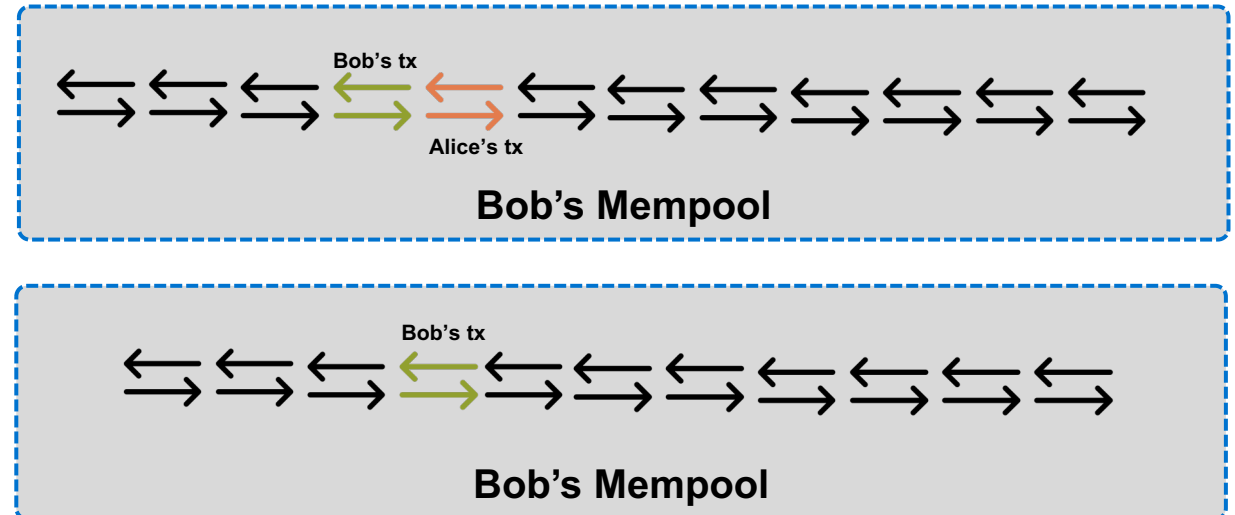
3. MEV Assessment

4. Outlook

Miner Extractable Value

Imagine a scenario where a trader conducts a large trade on one of the exchanges (in form of a dApp) available on Ethereum. The trade causes a **price slippage**¹ and creates a \$10,000 **arbitrage**² opportunity.

1. Alice issues a transaction to leverage the arbitrage opportunity.
2. Miner Bob sees Alice's transaction in the mempool and simulates it to see if it yields profit. Since it does in this case, he decides to leverage the arbitrage opportunity before Alice does. At this point, Bob can either:
 - Place his transaction in front of Alice's. This way, he will be the first to leverage the opportunity. In this case, Alice would either make less profit, or she would lose money (since the price will increase after Bob's transaction takes place)
 - Leave out (censor) Alice's transaction and insert his transaction



The potential profit (\$10,000) that can be captured by Bob (miner) is called Miner Extractable Value (MEV).

¹ Difference between the expected price of a trade and the price at which the trade is executed.

² Simultaneous purchase and sale of the same asset in different markets.

read more: <https://research.paradigm.xyz/MEV>

Miner Maximal Extractable Value

Although the term was first coined as “Miner Extractable Value” by Phil Daian et al. in their seminal paper *Flashboys 2.0* (2019),¹ soon it was changed to **Maximal Extractable Value**.

There are two motivations for this change:

1. **MEV can also be extracted by other participants** of the network, it is **not specific to miners**.

- Today, miners are hesitant with collecting MEV since this may decrease the trust in the system. Instead, MEV is mostly collected by other participants...
 - Assume Charlie runs a full node and monitors the mempool. After Alice issues the arbitrage transaction, Charlie also becomes aware of the opportunity, and he wants to profit from it before Alice does.
 - Since Bob is a rational miner, he always orders the transactions by their offered transaction fee. Thus, Charlie can issue a transaction with a larger fee than Alice's and be the first one to leverage the opportunity.
 - This strategy is called **frontrunning** since Bob inserts a transaction in front of Alice's transaction.

2. In blockchains that don't utilize PoW, there still exists block proposer nodes (e.g., validators, bakers) that have the right to order the transactions in a block. Thus, they can also collect MEV.

“MEV (Maximal Extractable Value) is the total value that can be extracted permissionlessly (i.e. without any special rights) from the re-ordering, insertion or censorship of transactions within a block being produced. As miners currently have the ultimate say on transaction ordering and inclusion in Ethereum, they can be seen as the most powerful player in this game, hence the commonly used term Miner Extractable Value. Yet, MEV exists on any blockchain and layers where there is a party responsible for transaction ordering (e.g., validators, rollup providers).”

<https://explore.flashbots.net/faq>

A Real-world MEV Example



OverviewInternal TxnsLogs (13)StateComments

Transaction Hash:

0xb72689042f313adbffbe4d192b0febc4c8a8346b75a549d5b4d4795b37180488

Status:

Success

Block:

118149292703000 Block Confirmations

Timestamp:

419 days 21 hrs ago (Feb-08-2021 09:15:55 AM +UTC)

Transaction Action:

Swap 139.095043641361099086 Ether For 5.7648024 WBTC On Sushiswap

Swap 5.76480241 WBTC For 2,269,314.669822 USDT On 0x Protocol

Swap 2,269,314.669822 USDT For 1,352.124212080924112964 Ether On Uniswap V2

Transaction Fee:

0.044577852 Ether (\$156.24)

Gas Price:

0.000000132 Ether (132 Gwei)

Ether Price:

\$1,752.87 / ETH

As of April 4th, 2022

<https://etherscan.io/tx/0xb72689042f313adbffbe4d192b0febc4c8a8346b75a549d5b4d4795b37180488>

- Although MEV was always existing,¹ its impact became significant with the increasing use of smart contracts (especially in DeFi use cases).
- With more MEV being discovered in blockchains, the incentives of block proposers (especially miners')² got updated.
- Until now, we claimed that miners had two main monetary incentives for finding the next block:
 - *Block reward (6.25 BTC in Bitcoin, 2 ETH in Ethereum)*
 - *Transaction Fees*
- However, this is not entirely correct anymore as miners can be **incentivized by the MEV a block offers** as well.

“MEV is an invisible tax that miners can collect from users.”

Charlie Noyes – MEV and Me

¹ Although Phil Daian et. al. coined the term MEV in [Flashboys 2.0](#) back in 2019, MEV was always existing.

² In Proof-of-Stake blockchains, block proposers (validators) can be penalized/slashed if they misbehave. As this is not the case in Proof-of-Work (PoW) blockchains, we can claim that the incentives of miners will be impacted more significantly than the incentives of block proposers in non-PoW blockchains.

- Besides re-ordering the transactions in the block they are proposing, miners can also be **incentivized to re-organize the block history** in order to claim the MEV in a previous block.
- This can be seen as a **threat to the consensus stability** of a blockchain as history can get re-written frequently. As a result, transactions may get reverted and user experience can be seriously harmed.
- Two of the most dangerous attacks that can be executed by miners to capture the MEV in previous blocks are time-bandit attacks and undercutting attacks.

“You think your transaction is confirmed and then suddenly it goes away, and it may or may not be included in the next block. So it breaks user experience to a certain extent, and is not really good for the stability of the blockchain.”

[‘Time Bandit’ Attacks on Ethereum: What They Are and How They Work](#)

Time-bandit attack

- A time-bandit attack is a strategy in which previous blocks are reorganized and rewritten by miners in order to capture MEV.
- Miners may be incentivized to propose competing blocks containing at the expense of users and other network stakeholders if the reward (MEV) is high enough.

Undercutting attack

Example scenario:

Head of the longest chain contains 500 units of MEV. 20 units remain in the current mempool.



Option one: Extend the longest chain. Claim 20 units for self, leave 0 for the next miner.



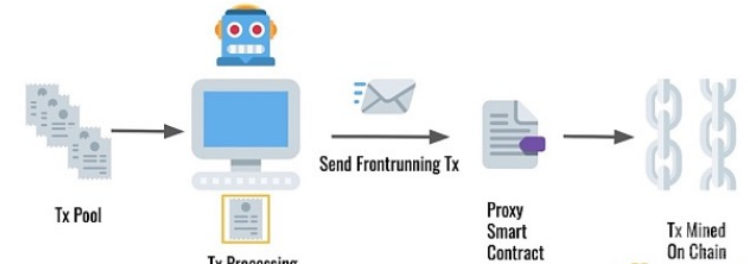
Option two: Fork the longest chain (ignore the current block). Claim 270 units for self, leave 250 for the next miner.



In the example above, option one shows honest mining, where a miner builds on the longest chain. In option two, an undercutting attack is performed such that the miner forks the longest chain and claims more reward (MEV) in comparison to option one.

The Impact of MEV on the Blockchain Ecosystem – Bidding Wars

- As mentioned previously, MEV is not only captured by miners (or block proposers), but also by other members of the network (called **MEV searchers**).
- To capture the available MEV, trading bots (MEV bots) are implemented.
- These **bots will bid against each other**, trying to offer the highest transaction fee in order to be the first to leverage an MEV opportunity. This is called **bidding wars** (or gas wars).
- However, the bidding wars have their toll on both the MEV searchers and the other participants of the network:
 - Besides the winner searcher, **the rest of the searchers usually lose money** since they offer a high fee for a transaction that is not going to make a profit for them as the opportunity will already be gone.
 - Due to the fierce competition between search, **transaction fees can increase significantly**. As a result, participants of the network who don't have anything to do with a bidding war may also be forced to **pay high transaction fees** in order to get their transactions included in the next block.




The Impact of MEV on the Blockchain Ecosystem – Flashbots

Flashbots,¹ a research organization working for providing a fair ecosystem for MEV extraction, developed a new Geth client (**MEV-Geth**) that would **end bidding wars**.

- Instead of submitting their bids to a public mempool, MEV searchers now submit **sealed-bids** (with a preferred transaction order) to a **private mempool** which is then utilized by miners running the MEV-Geth client.
- Since bids are not exposed until the next block is mined, bidders cannot iteratively try to frontrun each other.
- The MEV-Geth client refunds any tips back to the bidder whose bid is not accepted (i.e., not included in the preferred transaction order).

Note

- MEV-Geth is not a solution for ending the MEV scene in Ethereum. 
- It is merely a mechanism for bidders to bypass the Ethereum public mempool (i.e. avoid getting frontrun) and save money by getting a refund for gas fees of failed transactions.

1. Motivation
2. Maximal Extractable Value
 - Overview
 - The Impact of MEV on the Blockchain Ecosystem

3. MEV Assessment

4. Outlook

- Although arbitrage strategies are the most popular way of collecting MEV, there are many others:
 - Sandwich Attacks, Liquidation, Smart Contract Vulnerabilities,¹ Transaction Replay (“Generalized Frontrunning”), Just-In-Time (JIT) Liquidity,² ...
- *Is MEV quantifiable?*
 - Short answer, **NO**
 - MEV can be generated almost from any interaction of a user with a blockchain. Since smart contracts offer almost infinitely many ways for interaction, it is **infeasible** to precisely calculate the maximal extractable value available on a blockchain.
 - What can be done at this point is to come up with a **lower bound** for MEV by adding up the amount that’s been extracted by known forms of MEV (e.g. arbitrage, sandwich attacks, liquidation, ...).
 - [MEV-Explore](#) is a tool which is developed by Flashbots that quantifies the arbitrage MEV extracted on-chain on the Ethereum blockchain.

¹ <https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest>

² <https://twitter.com/ChainsightLabs/status/1457958811243778052>

Quantifying MEV (cont.)



\$607,141,706
Total Extracted MEV

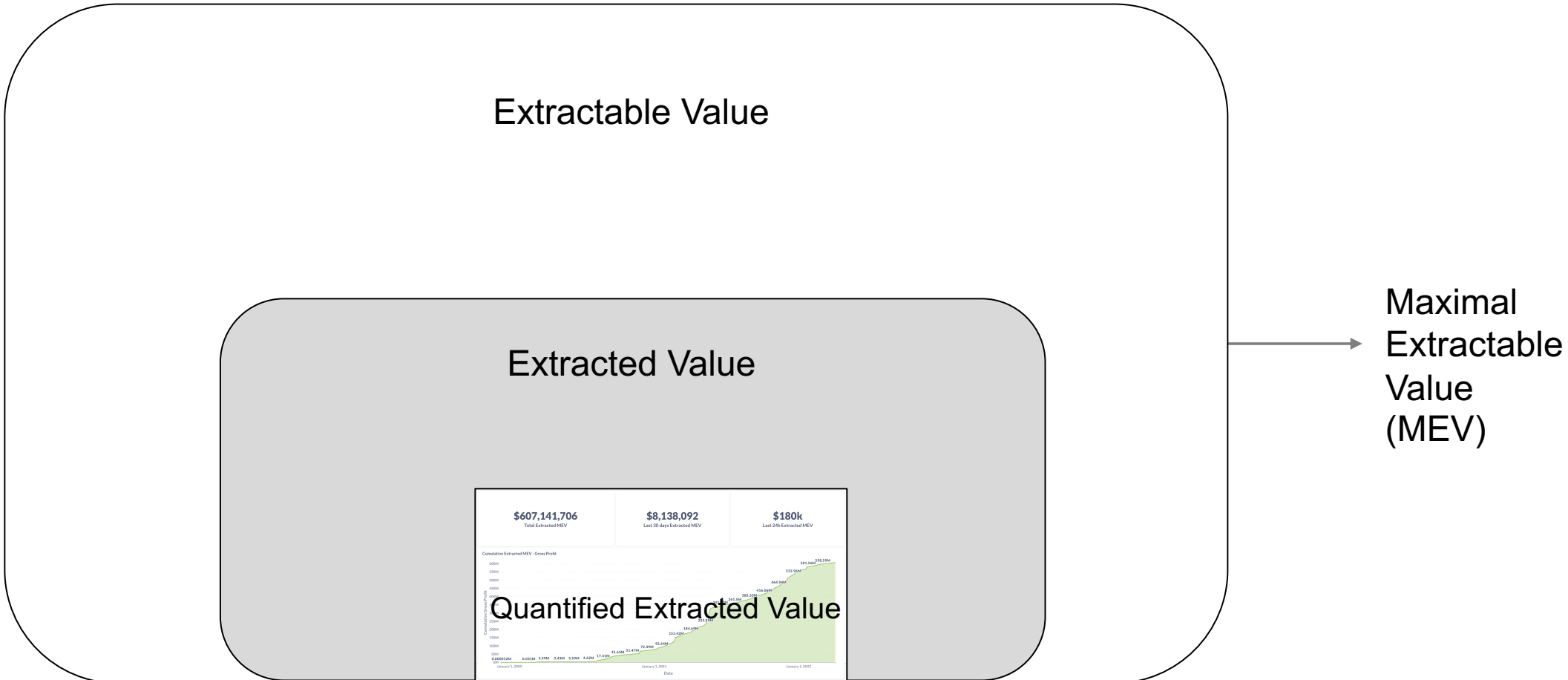
\$8,138,092
Last 30 days Extracted MEV

\$180k
Last 24h Extracted MEV

Cumulative Extracted MEV - Gross Profit



As of April 4th, 2022



Note: This visualization is not to scale

- Theoretically, Bitcoin also includes MEV (e.g., ordering transactions from Lightning channels). However, compared to Ethereum, the **amount of MEV is significantly less in Bitcoin** due to the difference in its **complexity of application-layer behavior** (i.e., Bitcoin is much more limited).
- On Ethereum, the MEV surface is rapidly expanding due to the growth of the DeFi ecosystem.
 - *Financial incentives for investing in DeFi X MEV*
- On Bitcoin, the capability of the Lightning Network, a payment protocol built on top of Bitcoin, can be **limited down** if it starts to create harmful MEV (e.g., removing some operations from the already limited scope of Bitcoin Script).
- However, on Ethereum, it would be **impossible to restrict all possible implementations of an application pattern** (e.g., DeFi protocols), without constraining the general behavior of **permissionless smart contracts**.

Ethereum's programmability, which opens the doors for powerful applications, is also its curse against MEV.

- MEV **cannot be eliminated totally**, however, there exist mitigation strategies that can be **additive** to the **security** of Ethereum's consensus stability:
 - Offering other stable miner revenue streams (e.g., EIP 1559 BASEFEE) besides the block reward
 - Designing applications to minimize the MEV exposed
 - Proof-of-Stake (PoS) based blockchains can penalize (*slash*) validators that attempt history re-write attacks (e.g., time-bandit)
 - Auctioning off the right to order transactions, in order to reduce the incentive to re-write history
- None of these approaches is a definite solution to the harmful implications of MEV and almost all of them require **significant changes in the core Ethereum protocol**.

1. Motivation
2. Maximal Extractable Value
 - Overview
 - The Impact of MEV on the Blockchain Ecosystem
3. MEV Assessment
4. Outlook

- MEV is undeniably out there and as a non-mev searcher, there is a limited scope of measures that you can take.
- If you are interested in working on MEV, contact [Burak Öz](#).
 - Some possible topics include:
 - Detecting and quantifying MEV in blockchains other than Ethereum
 - MEV minimizing best practices in consensus and application layer
- You can find more MEV resources [here](#).