Copyright 2023 by Verilog Solutions. All rights reserved.

April 26, 2023

by Verilog Solutions

TLDR

This research is aiming to be an easy-to-understand guide for everyday on-chain users on:

what is MEV

the lifecycle of a block-building process

the status quo of the MEV economics

some interesting ideas and discussions about the MEV

how to reduce your MEV exposure

MEV supply chain

MEV supply chain can be broken down into multiple segments, including wallet, RPC provider, searcher, builder, relay, and validators

Players in each segment compete both horizontally (against other players in the same segment) and vertically (against players in the upstream and downstream)

Each segment has its own unique ways of developing moat and varying degrees of the barrier of entry

There are also possibilities for horizontal and vertical integration within and across different segments

Not all MEVs are bad and malicious

Good side: Several DeFi projects depend on economically rational participants to maintain the effectiveness and stability of their protocols. One example is that decentralized exchange arbitrage, as a form of MEV opportunity, makes the market efficient by removing price discrepancies across different DEXes. In addition, back-running Oracle updates to quickly liquidate at-risk lending positions is a form of MEV opportunity that makes lending protocols economically solvent

Bad side: Some MEV opportunities such as sandwiching are malicious and harms the user's economic benefits. Sandwiching victims often encounter greater slippage and poorer trade execution.

1. Introduction

Maximal Extractable Value (MEV) refers to the maximum value a blockchain miner or validator can make by including, excluding, or changing the order of transactions during the block production process.

The term MEV, originated during the Proof-of-Work era of Ethereum when miners controlled which blocks and transactions were inserted into the blockchain. Ethereum's move to Proof-of-Stake (PoS) saw power over block proposal transition from miners to validators, but the pursuit of profit through manipulating transactions remained, so now the term "Maximal Extractable Value" is used.

MEV and transaction reordering are not just explained as a theoretical concept, but as a dynamic that is already occurring at scale in the form of transaction frontrunning on decentralized exchanges and which can have a significant impact on the user experience. From what has been able to be uncovered, over $908.3 million worth of MEV has been extracted since 2020. Quantifying the exact amount of MEV is challenging, given that many extraction techniques are designed to be concealed to maintain a competitive advantage.

MEV occurs when block producers in a blockchain (e.g. miners, validators) are able to extract value by arbitrarily reordering, including, or excluding transactions within a block, often to the detriment of users. Simply put, block producers can determine the order in which transactions are processed on the blockchain and exploit that power to their advantage.

The key players involved in MEV are wallets, searchers, validators, mempools, and relays .

View original

Credit: The MEV Supply Chain: a peek into the Future of this Industry by Thegostep and Flashbots

Wallet

A wallet is a digital or physical device that stores your private keys, which are used to access and manage cryptocurrency and blockchain-based assets, like NFTs. Most of the on-chain interactions for regular users are achieved through wallets.

Searchers

Searchers are individuals who interact with the mempool to monitor unconfirmed transactions and gain insight into imminent transactions before they are permanently recorded on the blockchain. Searchers implement algorithms that identify MEV opportunities from the pending transactions and generate transactions that extract value from found opportunities, such as front-running.

Validators

Validators are digital entities that are responsible for storing data, processing transactions, and proposing blocks to the blockchain. They are essential for ensuring the network's security and stability and are incentivized by staking typically 32 ETH.

Mempools

Mempools reside within nodes, acting as a holding memory pool of pending transactions waiting to be added to the blockchain. Note that there are public mempools exposed to everyone and private mempools exposed only to permitted entities. Transactions in a mempool are prioritized by fee, where a higher transaction fee increases the likelihood of a quicker inclusion into the blockchain, however, it is ultimately up to the block builder to determine the order of transactions being included in the next block.

Relays

A relay is a third-party intermediary between validators and block builders, relays provide block escrow service, which prevents validators from stealing MEV opportunities. It should be noted that relays are centralized at the current moment, and relays hold the power to censor transactions.

1. Different Types of MEV

2.1 Frontrunning

Front-running is the process by which an adversary observes transactions on the network layer and then acts upon this information by, for instance, issuing a competing transaction, with the hope that this transaction is mined before a victim transaction. It’s called front-running because the MEV searcher is trying to execute its own transaction before the victim transaction. An interesting note is that front-running is illegal in traditional finance as it breaks the fairness of the market.

2.2 Backrunning

Back-running occurs when a transaction sender wishes to have their transaction ordered immediately after some unconfirmed "target transaction". MEV searcher can finely control the order of transactions and ensure that its own transaction is ordered after the target transaction by submitting a transaction bundle. Some examples are:

The second transaction of a sandwich attack

Cross-DEX arbitrage

Liquidation after a price Oracle update

View original

Credit to: Demystify the dark forest on Ethereum — Sandwich Attacks by Liyi Zhou

As can be seen in the above picture, Tv is the target transaction intended to trade X for Y. Both TA1 and TA2 are transactions that are executed by the attacker. In this case, TA1 is performed in a front-running fashion trading X for Y to increase the price of asset Y. On the other hand, TA2 is executed after Tv (the target transaction). This transaction trades Y for X to recover the initial position after making a profit.

2.3 Just-in-Time Liquidity (JIT)

JIT is a type of on-chain liquidity provision behavior where an LP mints and burns a concentrated position immediately before and after a trade has been swapped. It has also been considered a type of sandwich attack that usually happens on Uniswap V3, below is an example:

Alice wants to swap 1000 ETH → 2.2 million USDC, the transaction has been sent to the public mempool.

Searchers found the pending tx, and this searcher is looking for opportunities to buy ETH for a lower price to perform more arbitrage. Thus, he sends:

1st transaction quickly flashloan huge amount of ETH and USDC & provided concentrated liquidity on Uni V3

2nd transaction after Alice executes the transaction of sell to withdraw liquidity and return all the fund

In this scenario:

Searcher found the opportunities to get ETH at a low cost

Searchers also enjoyed high trading fees paid by Alice

Alice enjoyed low slippage

Overall, JIT is neutral, the dark side lies in taking away the huge portion of fees that LP, who have been providing liquidity consistently, should earn, while the bright side is this behavior benefits the trader to have lower slippage.

2.4 Time-Bandit Attack

View original

Credit: What is MEV? A Simple Guide by RILEY

Time-Bandit Attack is a theoretical attack model. We illustrate a scenario with the above diagram. Let's assume Jane and George are two large miners in the market, and they are both mining the next three blocks of ETH.

The block reward for each block is roughly around $100.

When mining the first block, George suddenly discovers a $1000 arbitrage and MEV opportunity.

Rationally, George will choose to rework Block 4 and 5 that Jane has already mined, including his own arbitrage space, and mine the next block in advance. Therefore, George decides to rework Block 4.

After the reorganization, George now has the longest chain and can directly obtain the block reward for Block 6.

However, in this event, George may need to borrow some computing power from other platforms and miners in the short term. Such an MEV attack scheme is more applicable in a POW environment. In Ethereum with Tendermint or POS, this type of MEV will be greatly reduced.

1. Wallet/Builder/Proposer/Searcher Economic s

3.1 Different players in the MEV supply chain

View original

Credit: The MEV Supply Chain: a peek into the Future of this Industry by Thegostep and Flashbots

When a transaction is sent by a user, the transaction might go through a journey and be passed around to different players depicted above.

For example, when a user wishes to swap 10 ETH for USDC on Uniswap, the transaction is first composed by the wallet and signed by the user.

The signed transaction is then sent to the mempool of the RPC that the wallet is connected.

” Flashbots Protect ” in the above picture is an RPC provider, and it provides private mempool access to the trusted searcher, who promise won’t perform malicious MEV such as front-running

However, the RPC provider that the wallet is connected to can also be a public RPC provider, which sends the transaction to a public mempool. For example, the default RPC for Metamask is provided by Infura, which sends the transaction to the public mempool.

The searcher then runs a proprietary algorithm to find profitable MEV strategies, for example, cross-DEX arbitrage, and builds a transaction bundle that includes the target transaction with MEV opportunities and the transactions executed by the searchers that profit from the strategy.

The searcher then sends this bundle to builders , who might receive multiple bundles from different searchers.

Some bundles might be mutually exclusive, thus the builders also have to run an algorithm to pack the most profitable bundles by selecting the bundles that pay the most fees in a mutually exclusive bundle.

The most profitable bundles and other transactions in the mempool are packed as a block that is ready to be mined/proposed

The most profitable block is then sent to validators to be mined/proposed to the blockchain

In the current MEV landscape, the blocks are actually first sent to relays , which is a part of the MEV-boost design and acts as an aggregator of blocks

Each relay is connected to multiple block builders and receives packed blocks from each of the builders, the relay is responsible for picking the most profitable block for the validator and sending it to connected validators

Note that a validator can connect to multiple relays via MEV-boost

The relay is also responsible for a commit-reveal scheme to prevent validators from stealing the MEV opportunity

The relay will first only reveal the block header to the validator, which will then sign the header and sent the header back to relay

The relay will then send the full block content that includes the transaction to the validator

If the validator chooses to steal the MEV opportunity, which requires proposing a new block, the originally signed header will be published, and the validator will be slashed for double signing

3.2 Moat for each player

Wallet

The wallet is the first entity that receives transactions sent by the users. These transactions are valuable because they might contain MEV opportunities.

Wallet has the highest negotiating power in the supply chain, as it decides where the transaction will be sent, thus affecting who gets access to the valuable transaction order flow.

Profiting from transaction order flow is already widely practiced in traditional finance. Apps such as Robinhood offers free trading to users and sells the user's order flow to high-frequency trading firms

Although the value of the order flow is different in tradfi versus DeFi. In tradfi, retail order flow is valuable because most retails do not possess private information about the market, and thus are non-toxic

Defi order flow is valuable because DeFi transactions often contain MEV opportunities such as front-running and back-running.

Wallets have to compete against each other for onboarding new users. Wallets such as Metamask have already established their name in the industry and are integrated with many DeFi and Web3 applications, thus making it difficult for a new wallet to break into the business

However, we are seeing more and more DeFi and Web3 applications launching their on-wallet applications, such as Uniswap and StepN. These applications already amassed a large group of users, thus making it easier to onboard the existing users onto their wallet applications.

To summarize, the wallet is at the most upstream position in the MEV supply chain and holds the most negotiating power. Wallet applications compete with each other on user acquisition and user retention. Existing wallet applications such as Metamask have an advantage in their already established name and integration with many Web3 applications. New and upcoming wallet applications are often developed by teams that already built successful Web3 applications and thus can migrate existing users to their own wallets.

RPC provider/Node operator

The node operator is left out in the above depiction. Node operator provides RPC connection to wallet/users and helps pass the transaction onto the validators.

User transactions are “saved” in the RPC provider’s mempool, which can be public (accessible to all nodes and validators) or private (accessible to a select few searchers)

RPC provider is the second entity that touches users' transactions. Wallets often have a default RPC provider that it sends transactions, for example, the default RPC provider for Metamask is run by Infura

However, this does not mean that RPC Provider has to rely on wallets to receive transaction flow.

Wallets such as Metamask also allows users to switch RPC providers, thus making it possible for RPC Provider to directly market to retail users and encourage users to use their RPC.

Now many RPC providers encourage retail users to use their RPC for front-running protection. However, it is difficult for retail users to measure the performance of different RPC providers, thus it is expected that RPC providers will have to provide some other functionalities other than MEV protection in order to differentiate

RPC Provider holds some negotiating power over the searchers, as the RPC Provider has access to private transactions, which are transactions not available in the public mempool

Access to RPC Provider's private transaction pools is permission to only allow searchers who comply with the rules (i.e. no front-running) to access the transaction

But this permission access also provides the opportunity for RPC Provider to charge searchers for access to order flow, or even the RPC Provider can run its own searcher strategy

To summarize, the RPC provider is the second in the MEV supply chain and holds some negotiating power over the downstream searchers. RPC provider is responsible for maintaining and enforcing rules for private transactions sent to it. RPC providers compete with each other for transaction flows, either by working as wallets to become the default provider or market to retail users and encouraging the users to switch their RPC provider. RPC provider decides which searcher gets access to its private mempool and thus extracting MEV from it. Therefore, the RPC provider could seek payments from searchers for the order flow, or the RPC provider could implement their own searcher strategies.

Searcher

Searcher looks for MEV opportunities in others' transactions, whether coming from the public mempool or the private mempool that the searcher has access to

Searcher builds transaction bundles that extract the MEV opportunity, which can be either malicious (i.e. sandwiching) or benign (i.e. cross-DEX arbitrage). Note that some private mempool does not allow searchers to perform malicious MEV, and this rule is enforceable as access to private mempool is a permission process.

Searchers compete with each other on two fronts

Access to transaction flow. Searcher that can tap into more private mempools has a great universe to search MEV opportunity from. Thus the potential earnings per block are higher than searchers without access to more private mempools

Searching strategy. Searcher has to find the most profitable MEV opportunities and build transactions that extract the opportunity, all in a very short span of block time. This requires the algorithm to be highly efficient

The two competing front has different barriers to entry. Access to transaction flow has a higher barrier of entry, as some mempool might be proprietary and only accessible to the RPC provider's own searcher team

The search strategy has a lower barrier of entry. Anyone can write MEV strategies, with the difference that some can write very efficient ones. Also, searchers can look for more niche opportunities in more obscure chain or DeFi applications for less fierce competition

Searcher has no negotiating power over its downstream builders, as multiple searchers bid on the same MEV opportunities and undercut each other by offering a great fee to validators. Thus many searchers turn to look for niche MEV opportunities.

Therefore, the moat for a searcher will come from proprietary transaction flow. It is expected that the majority of individual searchers will be outcompeted by in-house searcher teams run by wallet and RPC providers.

To summarize, searchers look into public and private mempools and build transaction bundles that extract MEV opportunities. Searchers compete against each other on access to transaction flows and strategy efficiency. Searchers do not hold negotiating power over their downstream builders, and searchers are most likely to build their moat around access to proprietary transaction flows.

Builder

Builders receive transaction bundles from the searchers, pack as many profitable bundles into a block as possible, and send the block downstream to relays, which will then pass the block to validators

Builders decide how much transaction fees are earned by the validator and how much is earned by the builder

This does not mean that builders can just allocate 100% of the fees to themselves. As validators can connect to multiple builders and pick the block that yields the highest fee paid to the validator itself, builders who do not provide competitive fees to validators will not get their block built, thus not receiving any compensation at all.

In practice, the relay is connected to multiple builders and picks the most profitable block (to the validator), and sends it to the validator

Builders compete with each other on two fronts:

Builders compete with each other for the searcher’s bundle flow. Searchers most care about the stability/uptime of the builder, and how often the builder’s blocks get included

Websites such as https://www.mevboost.org/keep track of how many blocks a builder has built

The more searchers send bundles to the builder, the more MEV bundles can be packed into a block, and the higher fees can be earned by the block, which makes the blocks more valuable and more likely to be picked by validators, which the builder can also earn a share from the transaction fees. Therefore, more bundles sent from searchers equal higher profit for builders.

Builders compete with each other for access to block spaces, which are supplied by validators. The higher fees that the builder shares with validators, the higher probability that the blocks built by this builder will be mined/proposed in the blockchain

This competition process happens at the relay level, which will pick the block that gives the highest fees to the validators. Therefore, the more value that a block builder yields to validators, the higher probability the block will be proposed by the validators, but it also means lower profit for the builder.

As builders have access to full transactions, builders have the ability to steal MEV opportunities or censor transactions. Thus searcher will only work with builders that it trusts.

To summarize, builders pack transactions and MEV bundles into a block, and send the block to relay to be distributed to validators. Builder has the ability to choose what percentage of the transaction fees is shared with the validator and what percentage is kept by itself. This percentage is how builders undercut each other and compete for backspace. A builder competes for searcher bundle flow and backspace by producing more valuable blocks than other builders.

There is a flywheel effect where a builder that has better access to searcher bundle flows is able to produce more valuable blocks, which will attract even more searcher bundle flows as more valuable blocks equal greater access to block space. Therefore, it is expected that there will be a monopolistic tendency for the block builder space.

Relay

Relay functions as a block escrow between the builder and the validator.

To prevent the validator from stealing MEV opportunities, the relay will first ask the validator to sign the block header, followed by releasing the full block content. If the validator tries to steal the MEV opportunity by proposing an alternative block, the signed block header will be published and resulting in the validator getting slashed for double-signing

As of now, relay service is offered as a public good. Neither builders nor validators need to share transaction fees with the relay service.

However, as a relay has the observability into full transactions, the relay has the ability to steal MEV or censor transactions. Builder will only work with a relay that it trusts.

If the monopolistic block builder assumption from above holds true, it can be expected that block builder can also run their own relay service in the future.

Validator

Validators receive block from the relay and propose the block to be mined on the blockchain, essentially selling block space to builders/searchers/users

On Ethereum, the block proposer is selected randomly with the RANDAO algorithm, weighted by the effective ETH balance of each node, which is calculated as 32 ETH net of any penalties or rewards that the node receives

Therefore, individual validators do not have a competitive advantage against validator groups, such as staking services offered by centralized exchange or liquid staking protocols

For example, as an individual validator operating a few nodes, there is a lower probability that one of the nodes is being selected as the next block proposal. Therefore lesser rewards equal to one’s probability to become selected only grow by a minuscule amount as the rewards are factored into the effective ETH balance

However, in a validator group that operates many nodes, there is a higher probability that one of the nodes it operates being selected to propose the next block, thus higher amount of rewards are earned by the validator group, which increases the effective ETH balance and further increases the probability that one of the nodes in this group is selected as the block proposer

Therefore, there is an economy of scale for validator groups, operated by centralized exchange or liquid staking protocols. However, validator groups often compete with each other in attracting individual users to deposit ETH with them on these fronts:

Security

Operational security is paramount, as in the past there are operational errors that lead to a total loss of staked ETH with the protocol. See the StakeHound incident

Liquidity

Unstaking from the validator takes time. Therefore, staking service providers gives the user a derivative token that represents deposited ETH. Users can trade this derivative without waiting to withdraw their deposited ETH

However, some liquid derivative token (LST) has better liquidity than others, and users might prefer staking service providers that have higher liquidity for their LST

Additional yield source

Some staking service providers also provide its governance token emission as an additional source of yield, in order to attract users to deposit ETH with them

To summarize, an individual validator has very little negotiating power in the supply chain, as block space is a commodity, and there is no barrier to entry to become a validator. However, there are economies of scale when running validators. Therefore, a staking service provider is a valid business model that can extract revenue by providing a convenient service to users who want to stake their ETH. Staking service provider competes against each other on security, liquidity, and additional yield source for attracting more ETH deposits.

1. Some Interesting Discussions about MEV

To mitigate the negative impact of MEV, many interesting concepts and proposals have been created for discussion. We have selected two interesting proposals: one involves modifying the design at the application layer, while the other focuses on discussions about relays or more fundamental design changes.

4.1 Virtual Balance Design in the AMM Model

A few years ago, the Ethereum cofounder Vitalik Buterin posted research onEthresear.chabout potential solutions to improve front-running resistance of x*y=k market makers:

Improving front running resistance of x*y=k market makersTwo years ago I made a post where I suggested that we could run on-chain decentralized exchanges in a similar way to what Augur and Gnosis were proposing for on-chain market makers (eg. LMSR), and Martin Köppelmann from Gnosis suggested a simple approach for doing so, that I call the “*xy=k market maker”. The idea is that you have a contract that holds x coins of token A and y coins of token B, and always maintains the invariant that x*y=k for some constant k. Anyone can buy or sell coins by ess...https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281

The core principle of this design is to minimize modifications and let the frontrunner bear the economic losses, further reducing the potential profits of MEV and increasing the resistance of the market-making algorithm.

Currently, most Decentralized Exchanges use Logarithmic Market Scoring Rules (LMSR) market makers, e.g x*y=k, where x and y represent the in-pool token amount of token A and Token B respectively. Anyone can buy/sell tokens by essentially following the general rule:

x (amount of token A) * y (amount of token B) = k (equal to a constant)

The proposed design bought into a new accounting method: virtual balance. The A-side (x, y) and the B-side (x,y). Users who swap A token → B token (affects the B-side), users who swap B token → A token (affects the A side). Let’s simulate the difference after the above new design:

→ Regular AMM Design (Alice spotted Bob’s tx on the public mempool and decided to front-run Bob’s Tx, the below calculation has been rounded up):

Starting state (x = 10, y = 10)

Frontrunner Alice - Swap 1 A Token to B Token → (x = 11, y = 100 / 11 = 9.0909091), Alice got 10 - 9.0909091 = 0.909091 B Token

Innocent User Bob - Swap 1 A token to B Token → (x = 12, y = 100 / 12 = 8.333333), Bob got 9.0909091 - 8.333333 = 0.757576 B token

Frontrunner Alice - Swap 0.757576 B Token to A Token → (x = 11, y = 100 / 11 = 9.0909091), Alice got 1 A Token back

As the result, earns 0.151515 B Token as the profit

→ Proposed Virtual Balance Design

Starting state A-side (x = 10, y = 10), B-side (x = 10, y = 10)

Frontrunner Alice - Swap 1 A Token to B Token → A-side (11, 9.090909) | B-side (10, 10) | Alice got 0.909091 of B Token

Innocent User Bob - Swap 1 A Token to B Token → A-side (12, 8.333333) | B-side (10,10) | Bob got 0.757576 B Token

Frontrunner Alice - Swap 1.11111 B Token → A-side (12, 8.333333) | B-side (9, 11.11111) | Alice gets 1 A Token

As the result, Innocent User Bob still got 0.757576 B token same as Regular AMM, but frontrunner Alice is losing 1.111111 - 0.909091 = 0.202020 B token.

The larger the purchase, the more loss that frontrunner will be taken from the action.

Another important action for the project team is that they need to reset the virtual balances after a certain number of blocks. Or ideally, at the start of every block, set both virtual balances to qual the new actual quantities.

The Virtual Balances AMM design is for sure an interesting brain exercise. However, note that Bob still received the same amount of tokens under the virtual balance design compared to the vanilla design. In other words, the virtual balance design does not help the user to receive a better execution price. But, the virtual balance design creates a disincentive for malicious actors to execute sandwiching attacks, as evidenced by the fact that Alice lost 0.202020 under the new design.

In the end, Vitalik also mentioned the distribution of the MEV profits, if the MEV searcher ended up earning from the front-running scheme, these profits could be redistributed to the users who seem to have bought at worse prices. Another issue of this solution is the high maintenance fee to run such DEX, as users or project teams have to sync up the virtual balances & real balances at the beginning of every block.

4.2 MEV Redistribution

In the past year, many very creative solutions to the MEV problem have emerged, especially after PBS, and these designs have become increasingly interesting and complex. Some of these solutions mention a way for users to participate in the sharing of MEV profits, thereby better aligning the interest for everyone in the system. As we explore more in this direction, we also understand and discover that MEV is not just a technical problem, but more like a balance of interests amongst different stakeholders in the ecosystem. The challenge is to ensure that MEV is controllable and does not pose risks to consensus while minimizing the impact on user experience and accessibility. There is one interesting proposal been mentioned on the Flashbots forum:

MEV-Share: programmably private orderflow to share MEV with usersMEV-Share: Where transactions and bundles find their perfect match The following document outlines a design for MEV-Share, a permissionless and private matchmaking protocol between users and searchers. It has the following benefits: Users / wallets / applications: receive the MEV their transactions create Searchers: extract MEV from transactions they otherwise wouldn’t have access to Builders: build blocks with additional orderflow MEV-Share is designed to hand power back to users - they ...https://collective.flashbots.net/t/mev-share-programmably-private-orderflow-to-share-mev-with-users/1264/1

MEV-Share allows:

Users / Wallets / Applications: receive the MEV their transactions create

Searchers: extract MEV from transactions they otherwise wouldn't have access to

Builders: building blocks with additional orderflow

To achieve this, MEV-Share introduced a new entity called the Matchmaker

The matchmaker inserts users’ private transactions into searchers’ partially constructed bundles and simulates them, looking for matches. Matched bundles are sent to builders with a condition (“validity condition”) that MEV payments are made to users. Importantly, MEV-Share does not enshrine any individual builder.

Below is the system architecture:

View original

Credit to: MEV-Share: programmably private orderflow to share MEV with users by Bert

User - submit their transactions to the matchmaker, with the option to configure privacy preferences that specify which data to share (if any).

Searcher - monitors the matchmaker and receives selective data about user transactions based on their privacy preferences. sends bundles to the matchmaker that contain hints, or information, to assist in matching the bundles with user transactions. The bundles also specify where private transactions can be inserted

matchmaker - inserts its own private transactions into the bundles and tests them to identify those that can extract MEV successfully

Once a match is found, the matchmaker sends the bundle and a validity condition to the builders. The validity condition requires that the user receives payment for the MEV generated by their transaction. The details of how the payment is determined are discussed in the "further discussion" section of this document. Builders use the bundle to create a full block that includes the extracted MEV payment to the user, per the validity condition.

Essentially, users submit transactions that the matchmaker matches with searchers who compensate users for using their transactions. Initially, user transactions are concealed from searchers, who must construct partial bundles with non-atomic MEV strategies. However, programmable privacy preferences enable selective data sharing to help searchers optimize their bundles. As with the current system, searchers pay ETH to the builder, and validity conditions mandate that a portion of the MEV extracted must be paid to users.

In summary, introducing the privacy setting and matchmaker can enable searchers paying for validated users' transactions in ETH to let every participant in the MEV chain receive reasonable benefits / balance the profit sharing of MEV. This interesting idea took a balance between "Searcher has complete visibility over a user's transaction" and "Searcher has no visibility over a user's transaction", letting the open market bidding design manage the profit sharing and allowing average users to receive necessary privacy options.

1. How to Reduce Your Exposure

For different users/roles in the network, there are different exposures to the MEV and different ways to reduce your potential MEV exposure risk. In this chapter, we will only focus on discussing some suggested actions for the most common DeFi users when interacting with some DEX platforms:

Your RPC matters

In order to allow a software application or a decentralized application to interact with the Ethereum Blockchain (e.g token transfer, interaction with a smart contract, reading the data), it must connect to an Ethereum Node.

To achieve this goal, each Ethereum client incorporates a JSON-RPC specification. This ensures that applications can depend on a consistent set of methods regardless of the specific client implementation or node.

JSON-RPC is a lightweight and stateless remote procedure call (RPC) protocol that establishes rules for processing various data structures. It is transport agnostic, which means it can be utilized within the same process, over sockets, over HTTP, or in various message-passing environments. The protocol uses JSON (RFC 4627) as its data format.

In short, RPC is a communication protocol that your wallet (either Metamask, Uniswap Wallet or 1inch Wallet ..) needs to configure to ensure the success of communication and transaction broadcasting with the Ethereum Network.

5.1 Private Transactions

private transactions are transactions sent directly to validators(block proposers after PBS), instead of sending them and broadcasting them in the public mempools, and it is one way that traders can avoid exposing their transactions to frontrunning attacks. Essentially, you avoid the chances of MEV by hiding your transactions from the public mempool.

Flashbots

currently, the Flashbot offers such services where developers can use eth_sendPrivateTransaction() method as can be found below:

[Private Transactions | Flashbots DocsHow to send a single transaction to Flashbotshttps://docs.flashbots.net/flashbots-auction/searchers/advanced/private-transaction](https://docs.flashbots.net/flashbots-auction/searchers/advanced/private-transaction)

5.2 MEV Prevention RPC

In order to reduce the threshold for users to modify and configure their settings, some project teams have also developed their own relay system and RPC to promote the decentralization of MEV. This is intended to help users lower the risk of being exploited by MEV.

MEVBlocker

it's a simple website, just go and click → Get Protected, it will load an RPC secured by the MEV Blocker team and it offers Full protection from frontrunning and sandwich attacks on all types of transactions.

It also profits the users from any back-running opportunities your transactions create.

Besides, it is a fast, free, censorship-resistant solution open to all searchers and builders

MEV BlockerMEV Blocker is a fast and free RPC endpoint that protects users from frontrunning and sandwich attacks on a wide range of Ethereum transactions.https://mevblocker.io/

Flashbot Protect RPC

similar to the MEV Blocker, the Flashbot team also offers a Protect RPC that allows users to easily submit their transactions on the Flashbot Auction by using a custom RPC endpoint in their wallet. It has 2 major benefits:

Frontrunning Protection

No Failed Transactions: it will simulate the transactions if it will trigger any reverts, so do not need to pay for failed transactions.

Similar to how to set up MEVBlocker RPC, you just → connect the wallet to project and load the new RPC endpoint.

5.3 CoW Protocol

quick start | Flashbots DocsFlashbots Protect RPC allows regular users to easily submit their transactions to the Flashbots Auction by using a custom RPC endpoint in their wallet. Everything should be the same for users, except transactions are sent to the Flashbots builder instead of the public mempool.https://docs.flashbots.net/flashbots-protect/rpc/quick-start

CoW protocol is an interesting protocol that utilizes batch auctions as its price-finding mechanism. Essentially, user Alice needs to swap Token A to Token B, instead of comparing each of the DEX and making the decisions on which DEX to use, Alice's transactions will be sent to a batch auction list, where solvers are competing with each other to offer the best prices. Unlike the traditional AMM model where users need to be aware of the slippage tolerance or liquidity risks, the batch auctions transferred the MEV risks from users to professional solvers, who can handle and minimize these risks professionally.

View original

The CoW stands for Coincidence of Wants, is an optimization method that the CoW Protocol team designed to settle transactions among the trades within a batch, it has often been called ring trades, here is an example:

Alice wants to swap DAI → ETH

Bob wants to swap ETH → USDC

Daniel wants to swap USDC → DAI

(Ring Trades as DAI → ETH → USDC → DAI, 3 tx can be paired)

Then if all the above transactions are within one batch auction, the protocol can first be matching these transactions to offer everyone an ideal price without been worry about the arbitrage or slippage lost from the AMM model. In general, the core benefits of the CoW Protocol are to bring:

Lower prices and better solutions for fragmented liquidity on-chain

Can be considered as a DEX aggregator with Protection from MEV

Fewer fees due to the settlement are off-chain

No fee for failed transactions

Execute many orders at once

if during the batch settlement the price moves in your favor it will keep your surplus

In summary, for average users who do not have intensive trading experience on-chain, CoW can be a simple solution to reduce your MEV exposure and meanwhile aggregate and return you the best result.

1. Conclusion/Final Thoughts

MEV is a continuously evolving topic that still requires much research and exploration. It certainly represents an opportunity for users to make a profit on-chain but it also helps in the stability of the network, for example, by keeping decentralized exchanges efficient and consistent. Therefore, there are many reasons why getting a deeper understanding of the underlying mechanics is critical, probably the most important being finding solutions that can balance all the benefits and drawbacks of this phenomenon.

For everyday DeFi users, we suggest following the[How to Reduce Your Exposure]to minimize your MEV exposure to make sure your fund is safu.

1. References

https://blog.chain.link/maximal-extractable-value-mev/#:~:text=Maximal Extractable Value (MEV) refers,during the block production process.

https://blog.blockswap.network/from-niche-to-mainstream-a-complete-guide-to-mev-69b99658df8b

https://eigenphi-1.gitbook.io/classroom/glossary

https://docs.flashbots.net/

https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281

https://flashbots.mirror.xyz/bqCakwfQZkMsq63b50vib-nibo5eKai0QuK7m-Dsxpo

https://www.notion.so/MEV-Research-181da9f360034cf7a75a3faad91cb653

https://research.paradigm.xyz/MEV

https://rileygmi.substack.com/p/what-is-mev-a-simple-guide

https://medium.com/coinmonks/demystify-the-dark-forest-on-ethereum-sandwich-attacks-5a3aec9fa33e

Follow us on Twitter: @verilog_audit