

Lesson 11 - MEV mitigation

Today's Topics

- Approaches to MEV mitigation
 - DeFi projects that try to reduce MEV
 - MEV on L2
 - Oracle Extractable Value
 - Example of an MEV (Sandwich attack) bot
-

MEV Mitigation

Some approaches

Send transactions privately to miners via networks such as (Taichi - no longer running) or Flashbots Auction

Flashbots Auction

Flashbots Auction provides a private communication channel between Ethereum users and miners for efficiently communicating preferred transaction order within a block.

Flashbots Auction consists of [mev-geth](#), a patch on top of the go-ethereum client, along with the [mev-relay](#), a transaction bundle relayer.

There is a private transaction pool + a sealed bid blockspace auction mechanism which allows block producers to trustlessly outsource the work of finding optimal block construction.

Any miner or mining pool can run MEV-geth and receive additional income from MEV strictly more than what it would earn from running vanilla geth, without the need to enter into any bespoke deal with traders.

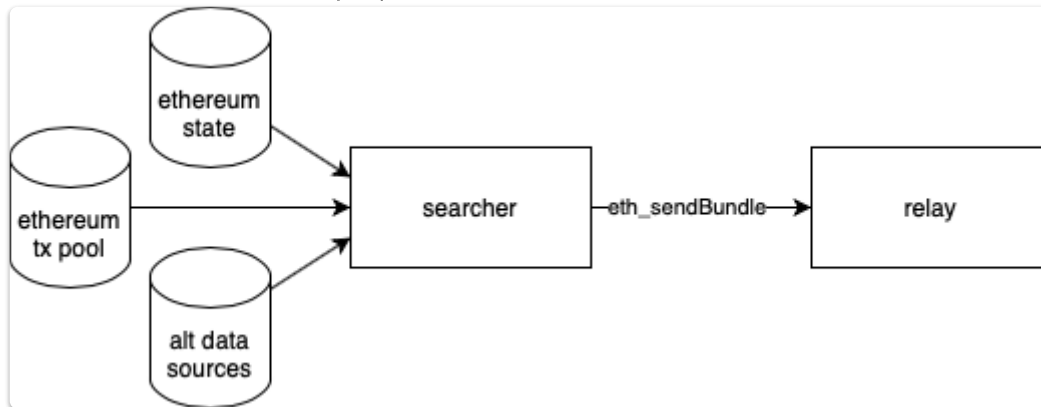
However we still rely on miners not to front run us.

The Actors involved are

1. Searchers

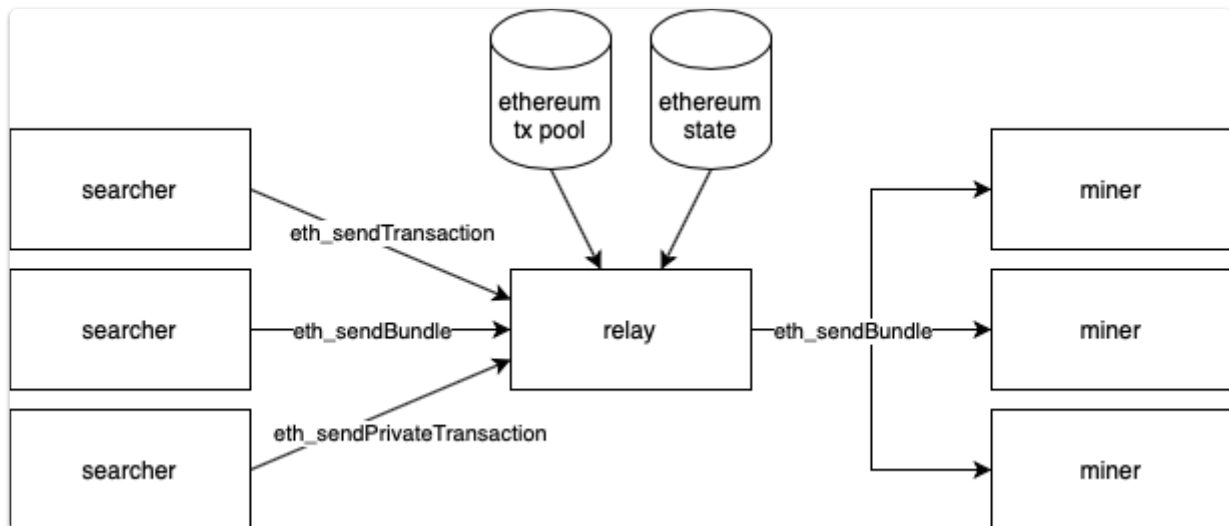
Typically these will be

1. Ethereum bot operators looking for fast, and risk free access to blockspace (for example, arbitrage and liquidation bots)
2. Ethereum users looking for frontrunning protection on their transactions (for example, Uniswap traders)
3. Ethereum Dapps with advanced use cases like account abstraction or gasless transactions (for example, tornado.cash and mistX)



2. Relayers

A relay is a bundle propagation service which receives bundles from searchers and forwards them to miners.



The searchers specify their bids by either

- gas price, or
- direct eth transfer to the coinbase address.

An important change to the crypto economics occurs because the searchers do not need to pay for failed bids, incentivising them to spam the system with bids.

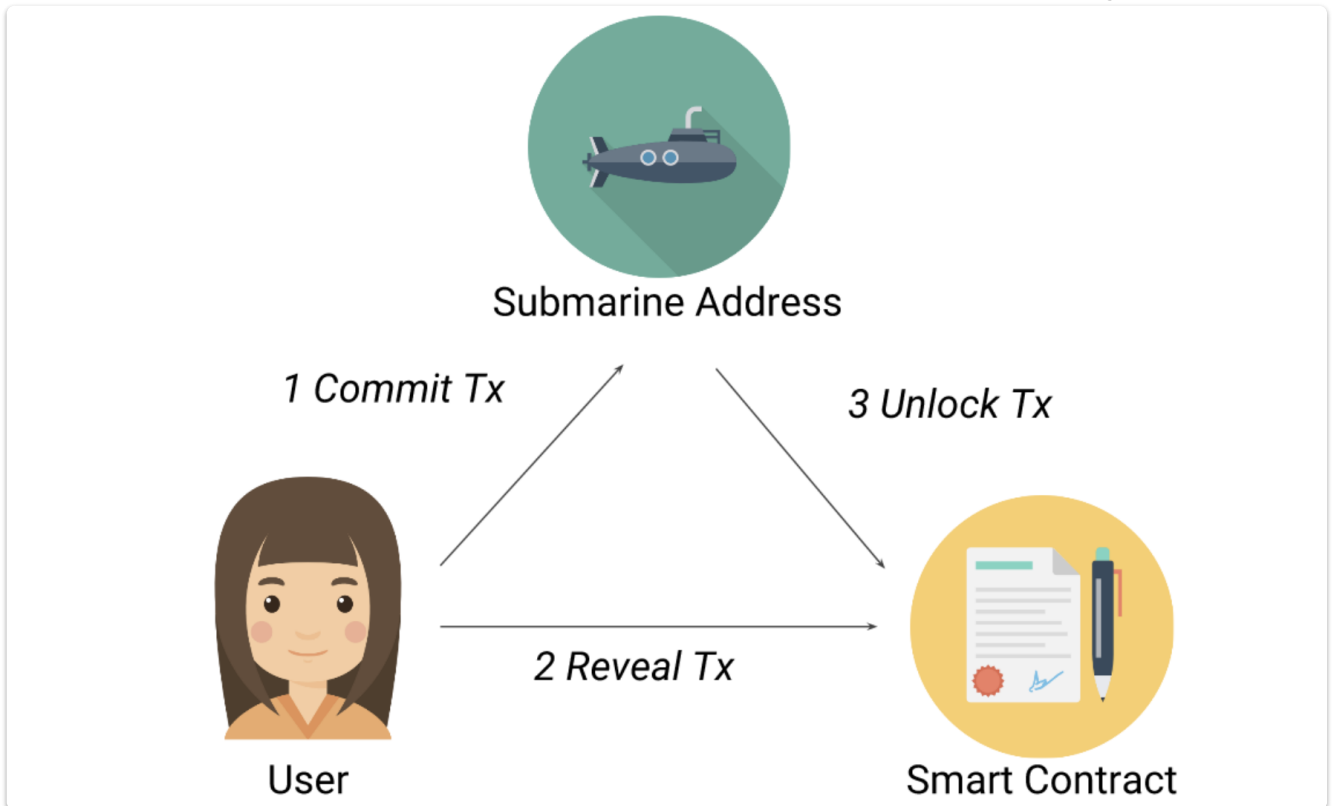
According to a Flashbots report (Feb 2021)

At the time of writing, there are 5 mining pools running MEV-geth, collectively accounting for over 12% of total Ethereum hashrate, collecting 0.13ETH per block of additional MEV revenue from Flashbots transaction bundles. On the MEV searcher side, we are seeing a 3x increase in unique searchers who have successfully landed bundles on chain.

Submarine Sends

See [Submarine sends](#)

This is a commit reveal scheme can be used (possibly with other obfuscating transactions)



Attempts to trick bots

Salmonella

See [Repo](#)

Salmonella intentionally exploits the generalised nature of front-running setups. The goal of sandwich trading is to exploit the slippage of unintended victims, so this strategy turns the tables on the exploiters. It's a regular ERC20 token, which behaves exactly like any other ERC20 token in normal use-cases. However, it has some special logic to detect when anyone other than the specified owner is transacting it, and in these situations it only returns 10% of the specified amount - despite emitting event logs which match a trade of the full amount.

DeFi protocol changes

1. Protocols can whitelist bots that will share the MEV from arbitrage or liquidation with the user being front run
 2. Enhancements to the DeFi protocols, for example with Request For Quote (RFQ) orders to specify which address will have their order filled, or progressive liquidations from [Euler](#)
-

Projects trying to reduce the MEV used

Mistx

launched by Alchemist using Flashbots technology

Features

- no Gas fees for transactions (bribes are paid to miners in tokens)
- MEV-proof

Archer Swap

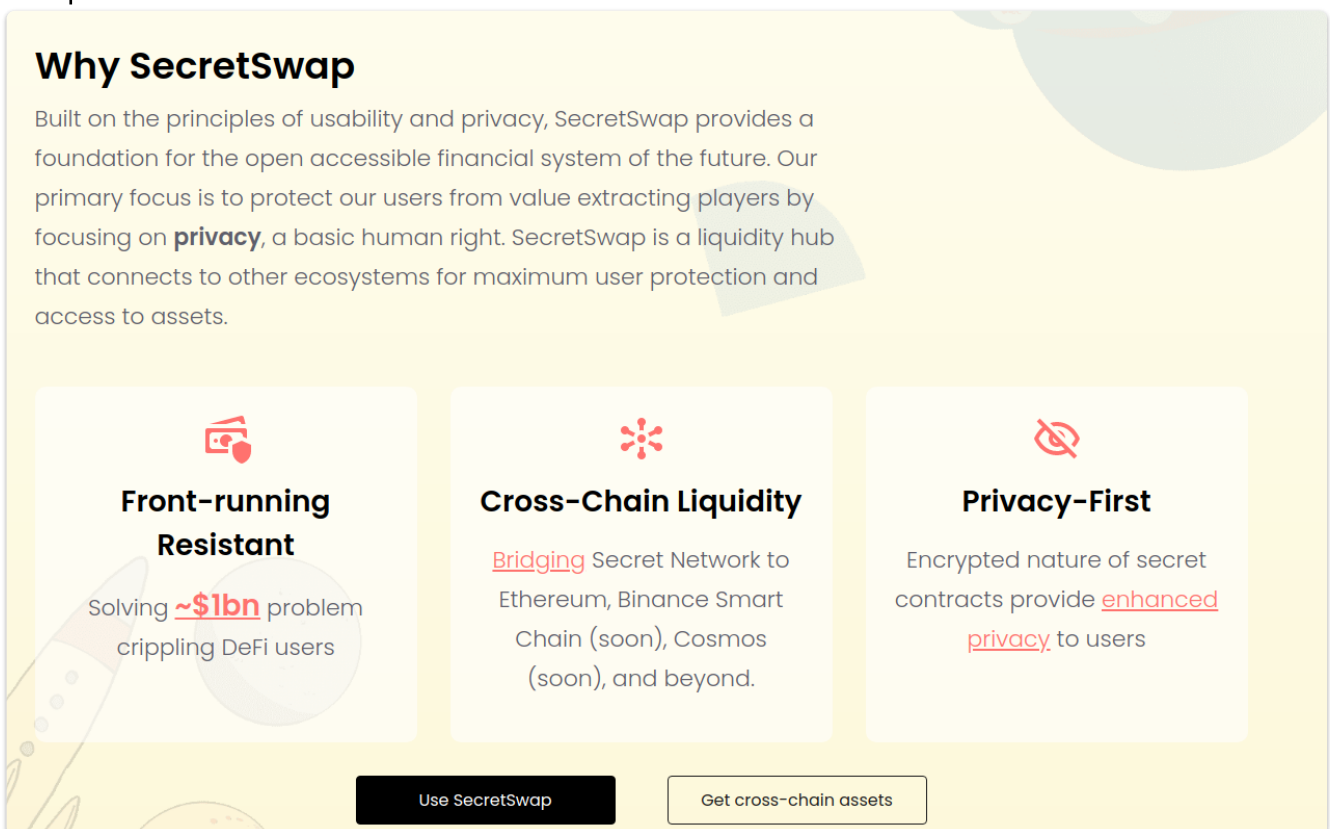
Uses Archer Relay which works with miners to find the most valuable trades for them and allows them to submit them to the ethereum mainnet.

Secret Swap

SecretSwap is a cross chain AMM built on Cosmos and Tendermint


It has an encrypted Mempool

Users will have to pay for gas and 0.3% swap fees with the \$SCRT token to use Secret Swap.

A screenshot of the SecretSwap website. The background is a light yellow with abstract green and blue shapes. At the top left, the heading "Why SecretSwap" is in bold black. Below it, a paragraph explains the project's focus on privacy and user protection. Below the text are three white boxes with red icons and text. The first box has a red icon of a wallet and a heart, with the text "Front-running Resistant" and "Solving ~\$1bn problem crippling DeFi users". The second box has a red icon of a network, with the text "Cross-Chain Liquidity" and "Bridging Secret Network to Ethereum, Binance Smart Chain (soon), Cosmos (soon), and beyond." The third box has a red icon of a crossed-out eye, with the text "Privacy-First" and "Encrypted nature of secret contracts provide enhanced privacy to users". At the bottom, there are two buttons: "Use SecretSwap" and "Get cross-chain assets".


Why SecretSwap

Built on the principles of usability and privacy, SecretSwap provides a foundation for the open accessible financial system of the future. Our primary focus is to protect our users from value extracting players by focusing on **privacy**, a basic human right. SecretSwap is a liquidity hub that connects to other ecosystems for maximum user protection and access to assets.




Front-running Resistant

Solving **~\$1bn** problem crippling DeFi users



Cross-Chain Liquidity

Bridging Secret Network to Ethereum, Binance Smart Chain (soon), Cosmos (soon), and beyond.



Privacy-First

Encrypted nature of secret contracts provide enhanced privacy to users

[Use SecretSwap](#)

[Get cross-chain assets](#)

Cow Swap

CowSwap is a DEX and DEX aggregator hybrid backed by Gnosis Protocol V2 (GPv2) which is developed by Gnosis team in order to provide MEV protection. GPv2 optimizes for coincidence of wants (CoWs), which can be explained as "an economic phenomenon where two parties each hold an item the other wants, so they exchange these items

directly.", i.e. peer-to-peer transactions can be matched without having to go through a regular AMMs like Uniswap or Sushiswap. One of the benefits of this is that off-chain transactions will cost a lot less and be faster.

CowSwap brings in 'Solver' conception to realize this function. Solvers are encouraged to compete against each other to deliver the best order settlement for traders in exchange for the reward of each batch. CowSwap will use a united price to settle all orders in the same batch, which is called batch auction mechanism. This process is very similar to Ethereum meta-transactions proposed in 2018.

Protocol Approaches

Some protocols have taken steps to prevent MEV such as using Verifiable Delay Functions in order to prevent gaming of transaction ordering, as [Solana has done on its base layer](#) to ensure transactions are ordered by time of arrival, or simply delegate ordering to something like Chainlink's Fair Sequencing Service (FSS)

Fair Sequencing Service

See [Blog](#)

"In a nutshell, the idea behind FSS is to *have an oracle network order the transactions sent to a particular contract SC*, including both user transactions and oracle reports.

[Oracle](#) nodes ingest transactions and then reach consensus on their ordering, rather than allowing a single leader to dictate it. Oracle nodes then forward the transactions to the contract [SC](#). They sequence these transactions by attaching nonce or sequence numbers to them or sending them in batches."

You can read more about Fair Sequencing Services in the Chainlink 2.0 White paper (Section5): <https://research.chain.link/whitepaper-v2.pdf>

5.2 FSS Details

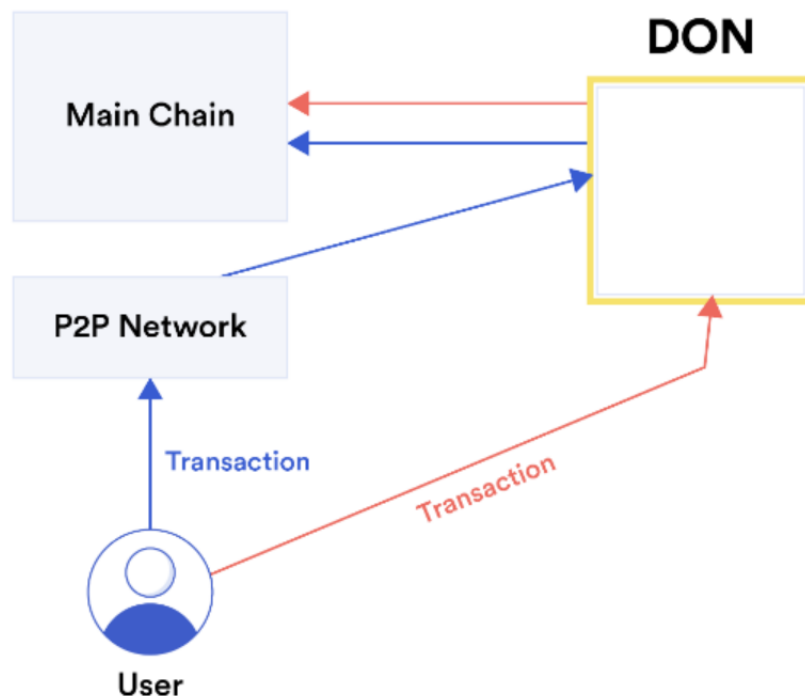


Figure 12: Order-fair mempool with two different transaction paths: direct and mempool-based.

1. Direct: The direct approach is conceptually simplest, but requires changes to user clients so that transactions are sent directly to the Decentralized Oracle 48 Network nodes, rather than to the nodes of the main chain.

The DON collects user transactions destined to a specific smart contract SC and orders them based on some ordering policy. The DON then sends the ordered transactions to the smart contract on the main chain. Some ordering mechanisms also require the direct approach because the user that creates a transaction must cryptographically protect it before sending it to FSS.

2. Mempool-based: To facilitate the integration of FSS with legacy clients, the DON can use Mempool Services (MS) to monitor the main chain's mempool and collect transactions.
-

MEV on L2s

MEV landscape is complex and rapidly evolving. Most L2 are actively working on upgrades to mitigate bad MEV and/or ensure MEV remains decentralised.

Community is split by:

1. Those who think MEV is bad and should be mitigated/designed out of the system.

...front-running and sandwich attacks are causing users millions of dollars worth of losses in terms of increased price slippage and lost arbitrage opportunities.

2. Those who see it as a natural part of the system where the focus should be increasing decentralisation of MEV not removing it all together.

...offering front-running as a service (FaaS) makes up for the miners' lost revenue caused by Ethereum's EIP-1559 fee-burning update. Hence, it indirectly increases Ethereum's security by incentivized miners to compete for MEV with higher hash power.

See [Panther Blog](#)

L2s and their approaches:

| L2 | Front Running | MEV mitigation | Status | Overview | Description |
|----------|---------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Arbitrum | No | Fair Sequencing Service | Not implemented but currently sequencing is centralised to prevent MEV | Oracles ensure TX order is fair | Decentralised Oracle Network used to ensure TX order is first in first out. |
| Optimism | Some | MEV Auction (MEVA) is in design but not implemented sequencing is centralised to prevent MEV | Not implemented | Elections contract for sequencers | 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. |
| Polygon | Yes | A flashbots implementation has been deployed on Polygon | Live but not battle tested | Link | |

|

Arbitrum

See [Hashflow x Arbitrum AMA](#)

The MEV landscape on Arbitrum is very different to Ethereum/L1s.

In general the Arbitrum system tries to mitigate MEV.

- Arbitrum has no mempool.
- Users send Tx directly to sequencers, Bots and the public can only see the transaction once it has been confirmed.
- In theory the sequencer could re-order transactions and extract value through MEV however Arbitrum currently runs the sequencer to prevent this.
- Arbitrum has plans to move towards a fair sequencing system which will decentralise the sequencing through a fair ordering consensus mechanism.

One interesting challenge is that consensus alone doesn't guarantee a 'first come first served' order for TXs.

Sequencers could conceivably reach consensus on the most profitable order not the fairest order. Therefore Arbitrum has worked extensively with Chainlink to research Fair Sequencing Services.

Additionally research has been done into fair ordering consensus mechanisms such as [Aequitas](#)

3 Modes of Arbitrum

1. Single Sequencer: L2 MEV-Potential (Mainnet Beta)

For Arbitrum's initial, flagship Mainnet beta release, the Sequencer will be controlled by a single entity. This entity has transaction ordering rights within the narrow / 15 minute window; users are trusting the Sequencer not to frontrun them.

2. Distributed Sequencer With Fair Ordering: L2-MEV-minimized (Mainnet Final Form)

The Arbitrum flagship chain will eventually have a distributed set of independent parties controlling the Sequencer. They will collectively propose state updates via the first BFT algorithm that enforces fair ordering within consensus (Aequitas). Here, L2 MEV is only possible if $>1/3$ of the sequencing-parties maliciously collude, hence "MEV-minimized."

3. No Sequencer: No L2 MEV

A chain can be created in which no permissioned entities have Sequencing rights. Ordering is determined entirely by the "Inbox" contract on L1.

No party involved in L2, including Arbitrum validators, has any say in transaction ordering, and thus no L2 MEV enters the picture.

[source*](#)

Optimism

Optimism is fairly similar to Arbitrum in that it relies on a centralised sequencer to prevent transaction reordering but is researching and building a decentralised sequencing system.

The Optimism thesis is:

- Prevent what MEV we can
- Democratise & extract the rest
- Redirect this as protocol revenue (retroactive public goods funding)

How Optimism works now:

- Optimism block production is primarily managed by a single party, called the "sequencer,"
- There is no mempool
- Transactions are immediately accepted or rejected in the order they were received

IS TRANSACTION FRONT RUNNING POSSIBLE ON OPTIMISM?

Right now front running is very difficult. You can't just do it by offering a higher transaction fee, because Optimism transactions are priced by the sequencer. In theory, you could do it by breaking into one of the routers between the sending system and the Optimism sequencer and dropping packets, but if you can do that you have better things to do than front running transactions.

Once we decentralize the sequencer, whoever runs the sequencer would be able to determine the order of transactions, so some front running might be possible.

Instead of a Fair Sequencing Consensus mechanism Optimism plans to auction the right to sequence transactions thereby redirecting the MEV value back into the protocol & toward retroactive public goods.

MEV AUCTIONS ON OPTIMISM

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.

1. Block producers which determine transaction inclusion, and
2. Sequencers which determine transaction ordering.

3. Block Producers

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.

4. Sequencers

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.

[Source](#)*

Starknet MEV

Sequencers can reorder transactions but currently Sequencing is not public/decentralized.

Multi Chain MEV

The more chains/layers you have the more complex the MEV landscape becomes and the larger the attack surface. As crypto becomes more layered and modular there is increasing economic incentive to centralise and collude to coordinate, i.e. control the sequencing and multiple layers to extract value.

Cross chain MEV is must more difficult to cordinate and is much more affected by economies of scale. The fair is that smaller players will be pushed out and MEV will become highly centralised.

See [Paper](#)

Oracle Extractable Value (OEV)

OEV is the value that can be extracted from the system by the address that updates an Oracle.

For example imagine an Oracle is providing price data to a DeFi lending protocol, if there is a sudden price change, then some positions could be at risk of liquidation.

The address updating the Oracle could exploit their advanced knowledge of the price change to submit a liquidation transaction.

The pros and cons of OEV pretty much follow that for MEV, it can be viewed as a good or a bad thing, and as unavoidable.

Example Sandwich Bot Contract

(We do not encourage people to run these types of bots)

See [Repo](#)

Overview

From the README

"In every Uniswap V2 trade, the user (victim) will specify a minimum amount of output tokens they're willing to receive.

The job of the sandwich bot is to calculate how much of the output tokens they should buy (to push the price of the token up) to match the victim's minimum out requirement. This minimum out requirement on most cases will be 2%, but on extreme cases it can be as high as 20% on volatile pairs (such as the SHIBA-WETH pair during the craze).

Once the sandwich bot has calculated the optimal number of tokens to buy, it'll wait for the victim to buy their tokens, and immediately sell to gain a profit."

The bot

1. Gets transactions from the mempool that are for the Uniswap router
2. Checks they don't have a receipt.
3. Parse the Uniswap data for 'swapExactETHForToken' transactions
4. Calculate a profitable sandwich
5. Work out what fees are likely to be involved
6. Submit the slices of the sandwich

Interestingly, the front and back slices are submitted via the Flashbots network.