MEV-capturing AMMs

Federico Giacon
Smart contract developer at CoW Swap
Maximal extractable value (MEV)

Block builders can include, exclude, and reorder transactions in a block.

MEV is the value extracted on top of fees and rewards.
Sandwich attack

Block

User tx

Sell 100 ETH for 100,000 USDC (max 1% slippage)
Sandwich attack

Block builder tx
Buy USDC: move AMM price to 990 ETH/USDC

Block

User tx
Sell 100 ETH for 99,000 USDC (1% slippage)

Block builder tx
Sell back USDC at new price
### Loss versus rebalancing

<table>
<thead>
<tr>
<th>Market</th>
<th>1 ETH = 1400 DAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMM</td>
<td>1 ETH → 1400 DAI</td>
</tr>
</tbody>
</table>
Loss versus rebalancing

<table>
<thead>
<tr>
<th>Market</th>
<th>1 ETH = 1400 DAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMM</td>
<td>1 ETH → 1400 DAI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Market</th>
<th>1 ETH = 1300 DAI</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMM</td>
<td>1 ETH → 1400 DAI</td>
</tr>
</tbody>
</table>
Loss versus rebalancing

LVR is an information cost to the liquidity provider: the pool doesn't have access to current market prices.

This is not impermanent loss!

<table>
<thead>
<tr>
<th></th>
<th>Market</th>
<th>AMM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 ETH = 1300 DAI</td>
<td>1 ETH → 1400 DAI</td>
</tr>
</tbody>
</table>
Build an AMM that auctions off the right to the first transaction to the highest bidder (*lead searcher*).

Proceeds go to liquidity providers.

- Lead searcher captures LVR instead of block builders!

**A concrete example**

<table>
<thead>
<tr>
<th>Trades</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEV-extracting trade</td>
</tr>
<tr>
<td>Trade 2</td>
</tr>
<tr>
<td>Trade 3</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>
Enforcing first transaction right

No users can trade until the lead searcher has traded—otherwise the transaction \( \times \) reverts \( \times \).

Block builder cooperation needed: the lead searcher transaction is included before any trade.

- Incentive: if the transaction doesn't revert then it uses more gas.
Estimated MEV profit for lead searcher: +9 $/block
● Based on the value of the first transaction slot on the Eden network

Estimated additional costs: -3 $/block
● From the extra gas cost of enforcing AMM rules (much lower in L2!)

Expected captured MEV on mainnet: +6 $/block

Details: https://ethresear.ch/t/mev-capturing-amm-mcamm/13336
MEV extraction potential

Source: https://transparency.flashbots.net
Conclusion

AMMs have hidden fees:
- for users: sandwich attacks
- for liquidity providers: loss versus rebalancing (LVR)

In current AMM designs, these fees are paid to arbitrageurs and block builders.

Goal: efficient AMM designs that distribute these fees away from block builders.
Join the discussion!

https://ethresear.ch/t/mev-capturing-amm-mcamm/13336
Thank you!

Speaker: Federico Giacon
federico@cow.fi

An idea from: Alexander Herrmann
alex@cow.fi