MEV capturing AMM (McAMM):

A prevailing thought is that the power of transaction ordering is mostly in the hands of block-builders in the current MEV-Boost and PBS specifications. In this write-up, ideas for new AMM designs are presented that would shift the transaction ordering power, at least partly, to AMM designers and liquidity providers. These constructions would allow AMMs to capture part of the MEV that is currently only harvested by block-builders and proposers.

High-level idea:

New MEV capturing AMMs can auction off the right of the first trade per block via a smart contract auction. This would imply that normal users can only trade against the McAMMs after the auction winner has traded, as otherwise, their trade will fail. It turns out that in such a setup, it is game theoretically optimal for block-builders to respect the first execution right of the AMMs and sort trades such that the first trade is done by the auction winner and normal user trades are not reverting. By auctioning off the first trade per block, AMMs can basically sell their MEV and capture a revenue from it. Since most MEV can usually be extracted with the first trade in a block, McAMMs and their LPs can capture most of their MEV with this mechanism.

Specification

There is one global contract that manages all McAMMs' first execution right. For gas efficiency reasons, that contract should be the standard router contract for all McAMMs pools. The first execution right is assigned to the so-called leadsearcher. The global router contract will store per block the information whether the leadsearcher has already traded on any of the deployed AMM contracts. Only if the leadsearcher has already traded, then others are allowed to trade against the McAMMs. Otherwise, the trades revert.

This mechanism works as block-builders have a natural incentive to put the leadsearcher transaction before the other trades, as explained in the next paragraph.

To become the leadsearcher, one has to win the auction for the first execution right. The auction will be held by the router contract and could be similarly structured to the eden networks auction for the first slot in a block.

Leadsearchers become automatically deselected by the router contract if they missed more than 3 blocks. This prevents them from blocking trades for a longer period. If leadsearchers don't wanna trade in a block, they should anyway send a transaction that just signals that they touched the McAMMs such that others can trade against the McAMMs. (This costs only 40k gas for the lead searcher). To enable the leadsearcher to capture all arbitrage opportunities, not just the ones that are profitable after paying the AMM fees, the lead searcher should not pay any normal AMM fees. Thereby, the McAMMs grant the leadsearcher a more flexible fee structure, but still harvest the fee, as it will be priced into the auction.

Incentive structure for block-builders:

Block builders have an incentive to propose blocks with the highest priority fee gas consumption, as they can charge the priority fee and thereby they are more likely to win the MEV boost auction. Since failing trades have a lower priority fee gas consumption than fully executed trades - assuming each trade has a priority-fee > 0 -, the block builder are incentivized to make the trades of the McAMM not revert. Hence, they will put leadsearcher's tx before the regular user's trades.

(Only for full blocks, there might be from time to time situations in which a failed trade would maximize the consumed priority fee.)

Additionally, users of the McAMM have a high incentive to only broadcast their trades to block-builders respecting the enforced ordering by the McAMM, as otherwise, they have to carry the failed transaction gas costs.

Both factors are expected to drive all block-builders to respect the ordering necessary for McAMMs, once one block-builder with a bigger marketshare is starting to offer this service.

Analysis:

- Using data from the Eden network, the MEV extracted per block by the first transaction is currently estimated at around 9$ per block. This MEV value is expected to increase over time with more sophistication of the MEV extraction and deeper on-chain liquidity. The 9$ was derived by looking at the Eden auctions for the first slot in a block: Daily fees paid by the current slot 0 holder are currently 693,775 * 0.033 * 0.13$=3000$ and on average 325 blocks are produced by Eden Network per day that put the slot holder at the first position. Hence searchers are paying these days 3000/325 =9$ per block to be at the leading position. Compare to this dune query.
- McAMMs have the disadvantage of an additional gas cost of ~2.1k (2100gas read storage) per trade compared with usual AMMs since the transaction would have to read a storage variable in the router contract to check whether the leadsearcher has already traded. Assuming 20 trades per block, the gas cost increases are 2.8$ (=2100 * 20 * 40 /10^9 *1700) at 40 Gwei gas prices and 1700$ eth prices for all users. However, especially on L2, this additional cost seems to be negligible.

- There might be additional costs for the leadsearcher to always touch the McAMM router to enable others to trade, even if there is no arbitrage opportunity. However, this is expected to happen very rarely, as between two blocks (in 15 secs) usually some price of some token that is traded on DEXes and CEXes moves and thereby creates a profitable arbitrage opportunity for the leadsearcher.
- The upper numbers allow us to estimate very roughly McAMM's additional revenue by ~9$ on L2s and ~ 9-2.8 = 6.2$ per block on ethereum. Hence, this construction is particular valuable on L2s. The estimated revenue from MEV would be roughly 1/30 of the current AMM fees that Uniswap is earning.
- Eden data also shows that the first position in a block is by a factor of 10 more valuable than the second position - currently the first slot costs 693,775 * 0.033 Eden per day compared to the second slot 65,847 * 0.033 Eden per day. Hence, it makes sense for McAMMs to auction off only the first execution right. This would probably reduce the AMMs MEV footprint already by 2/3.

Potential issues:

- Not all proposers will run MEV boost, hence naturally blocks will be missed in which the McAMMs are not traded by users - assuming users only broadcast their transactions to block-builders supporting the protocol. This might increase the waiting time for users. The leadsearcher will always trade in each block. Their transaction can not revert and hence can be broadcasted into the public mem-pool. But users are expected to migrate to block-builders as they offer valuable features like MEV-protection and revert-protection.
- For the AMM smart contract, it is not detectable whether a missing leadsearcher transaction is caused by censoring from block-builders/proposers or by the misbehavior of the leadsearcher. However, since block-builders have a natural incentive to include the leadsearcher transaction, this might not be a real issue and one can expect that it is due to a fault of the leadsearcher.
- Asking users to pick a reliable block builder that respects the ordering, might be a small UX challenge.

Philosophical comparison to HFT:

In TradeFi, exchanges sell speed technology to high-frequency traders to be the first ones trading. One could argue that this proposed mechanism is similar, as AMMs are again selling the "first trade". However, a fundamental difference is that in tradeFi the proceeds of the selling of the speed technology go to the exchange - a value extracting middle-man -, while for this proposed mechanism, the proceeds are going back to the liquidity providers of the AMMs. Assuming more revenue for LPs leads to deeper liquidity, the end-users are also benefiting.

Further research topics:

- In the upper specification the leadsearcher is only one entity. Probably this is suboptimal, and a more optimized construction could resell the first execution right to different parties.
- For further efficiency, the first execution right might be set on a smart contract level not per global router contract, but per eco-system: E.g. all AMM projects could define the contract that maintains their "leadsearcher"

CowSwap team has further ideas for such McAMMs. If you are interested, please connect to us.