On-chain data and transaction of MEV

**Introduction**

Maximum Extractable Value(MEV) robot attacks, like sandwich attacks and arbitrage attacks, are quite popular in DeFi, yet many people just have a conceptual understanding of them. On-chain transaction data tracking, however, really provides a more comprehensive understanding of MEV. Sentio, a Web3 observation platform, just released a blog that explains MEV with examples and on-chain data to help you understand it better.

**Body**

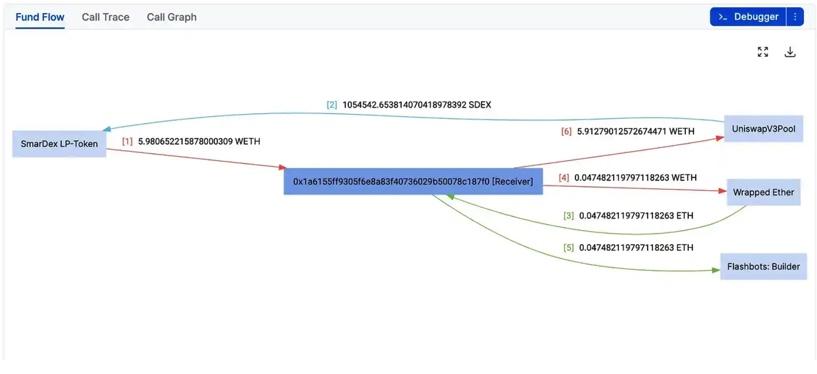
The chart below is the daily revenue and profit generated by two MEV strategies (i.e. Arbitrage and Sandwich) over the last 14 days to demonstrate how big the opportunity is with MEV. Daily gross revenue averages over $500,000, and daily profits average around $100,000. jaredfromsubway.eth (blue area) revenue alone accounts for half of the total profit and revenue generated by sandwich attacks.



How does MEV work?

**Arbitrage**

First, the MEV robot finds a price gap between the two liquidity pools; then the robot can buy from the low-price pool and sell from the high-price pool in a single transaction, thereby generating profits.

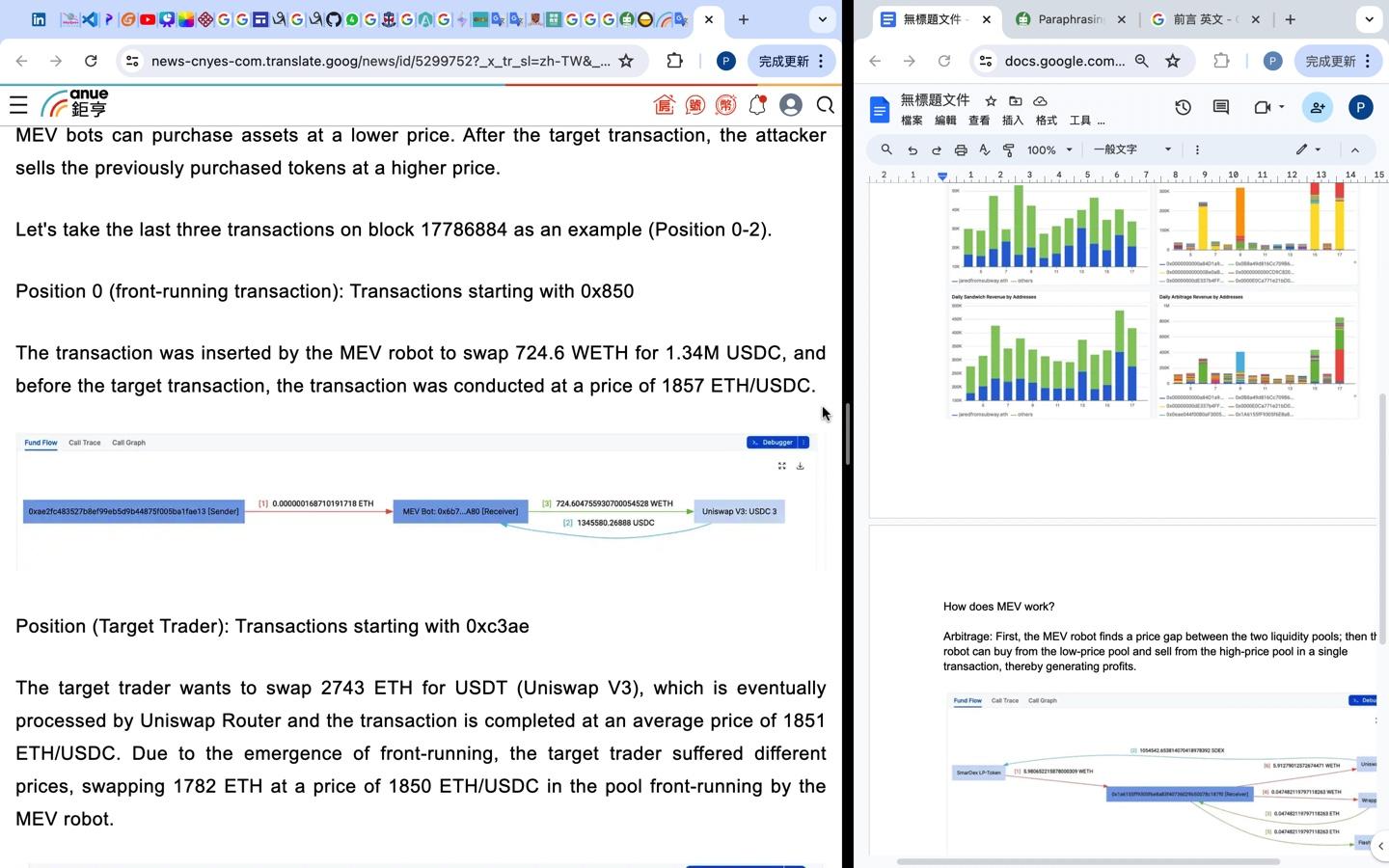


The trading robot started the MEV transaction depicted in the image with 0x1a6. The price of WETH in SDEX in the Uniswap V3 pool was less than the price of WETH in the SmarDex pool in this transaction, as detected by MEV-bot (SmarDex is a platform comparable to Uniswap V2 DEX). MEV-bot trades in the low-price pool initially, then proceeds to sell the WETH it has received to the high-price pool, ultimately realizing a 0.07 ETH profit (5.91-5.98).

**Sandwich attack**

An arbitrage strategy typically involves adding a trade after a profitable trade, but a sandwich attack is a strategy that makes money by adding 1 (or more) trade before and after a target trade and forcing those trades to execute sequentially. Let’s take a look at the operation process of a typical MEV sandwich attack from a God’s perspective, as shown below:

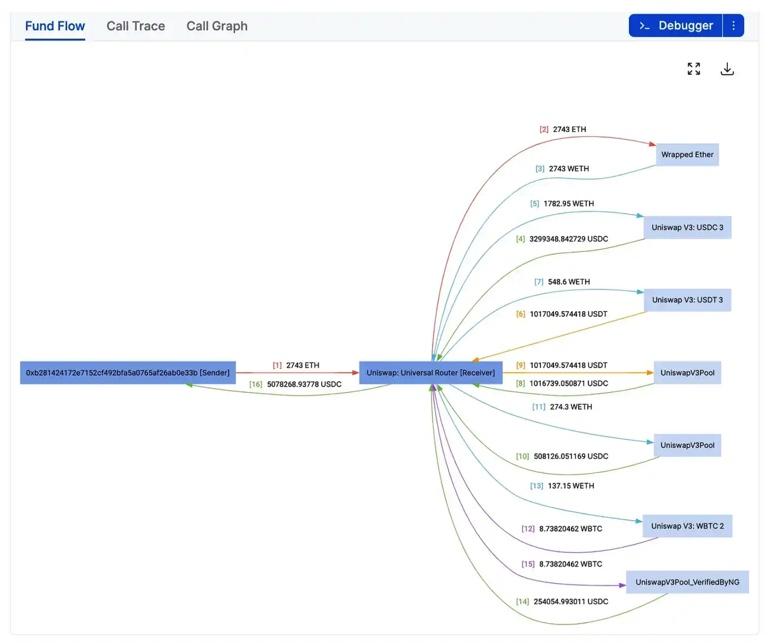
The user submits a transaction to mempool, and the MEV robot continuously monitors all mempool transactions and tracks the transaction and determines whether the transaction can become a profit opportunity for the sandwich. Once an opportunity is discovered, the MEV bot needs to create a bundle by inserting transactions before and after the target transaction (like a wrapped sandwich) and submit the bundle to the block builder.



The transaction was inserted by the MEV robot to swap 724.6 WETH for 1.34M USDC, and before the target transaction, the transaction was conducted at a price of 1857 ETH/USDC.

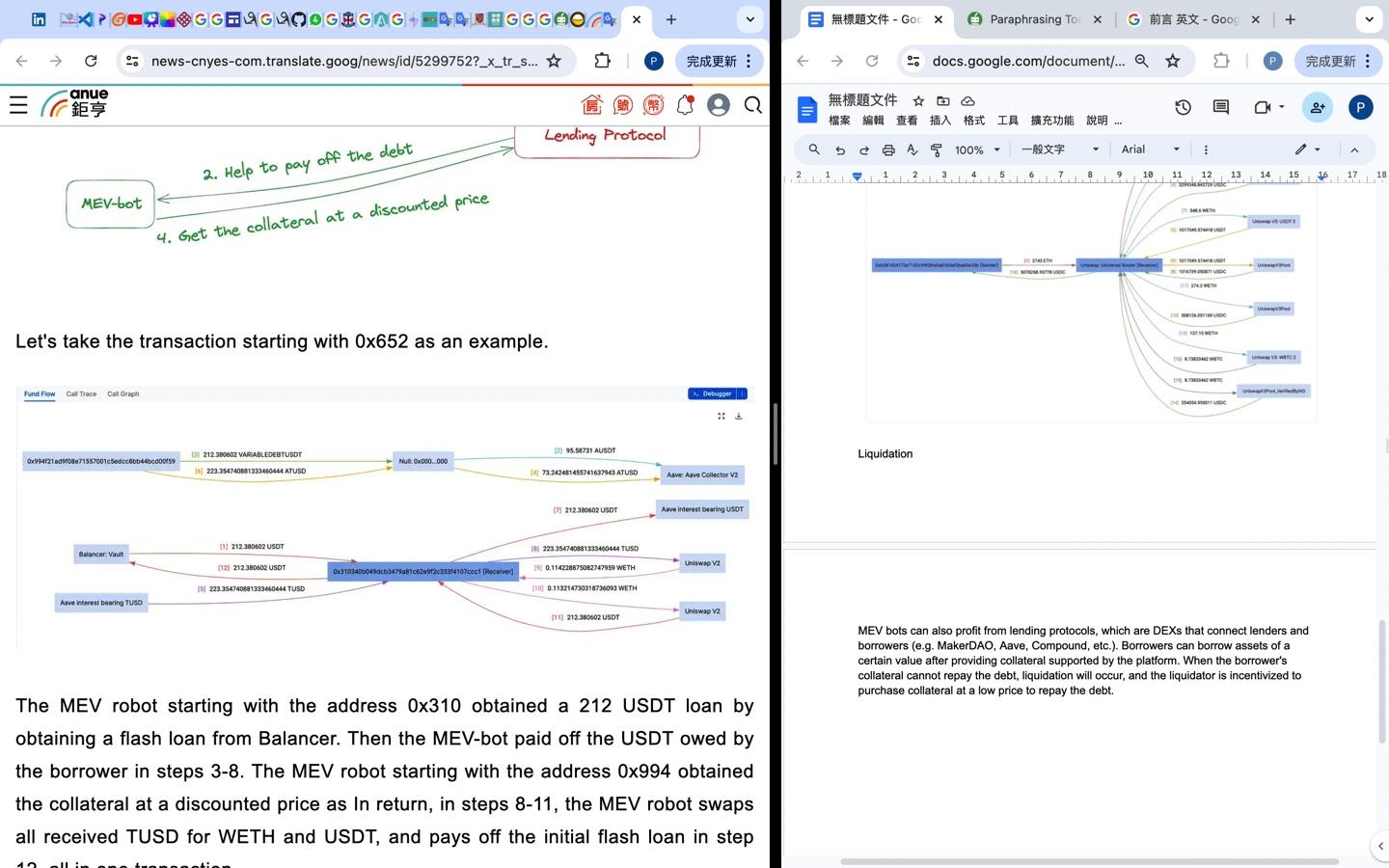
**Position** (Target Trader): Transactions starting with 0xc3ae

The target trader wants to swap 2743 ETH for USDT (Uniswap V3), which is eventually processed by Uniswap Router and the transaction is completed at an average price of 1851 ETH/USDC. Due to the emergence of front-running, the target trader suffered different prices, swapping 1782 ETH at a price of 1850 ETH/USDC in the pool front-running by the MEV robot.



**Liquidation**

MEV bots can also profit from lending protocols, which are DEXs that connect lenders and borrowers (e.g. MakerDAO, Aave, Compound, etc.). Borrowers can borrow assets of a certain value after providing collateral supported by the platform. When the borrower's collateral cannot repay the debt, liquidation will occur, and the liquidator is incentivized to purchase collateral at a low price to repay the debt.



The MEV robot starting with the address 0x310 obtained a 212 USDT loan by obtaining a flash loan from Balancer. Then the MEV-bot paid off the USDT owed by the borrower in steps 3-8. The MEV robot starting with the address 0x994 obtained the collateral at a discounted price as In return, in steps 8-11, the MEV robot swaps all received TUSD for WETH and USDT, and pays off the initial flash loan in step 12, all in one transaction.

**Conclusion**

As blockchain and DeFi continue to develop, Maximum Extractable Value (MEV) has become an attractive and controversial topic. This article delved into MEV-related topics through real transactions, data points and simple execution examples from Sentio, and unveiled the mystery of the MEV concept.

Arbitrage, sandwich attacks, and liquidation are the main ways to extract MEV. Additionally, there are other strategies within MEV that are niche, mysterious, and undiscovered (reference link), which are known as long-tail MEV.