Overview

In this post, we present a tool (TWAMM) tailor-made for executing large on-chain swaps in a gas-constrained and MEV adversarial environment (Ethereum L1). TWAMMs act as shock absorbers for protocols during high trading volatility or volume. A few use cases where TWAMMs can help MakerDAO include:

- Buybacks: MakerBurn
- Liquidations: 7 siblings
- New Tokenomics: SubDAO tokens
- Increasing Capital Efficiency: Sagittarius Engine
- Diversification: PSM re-balancing

TWAMMs enable traders (long-term, non-toxic) to execute large swaps on-chain over multiple blocks, effectively an on-chain TWAP order. Furthermore, the trader only pays gas for starting, canceling, and withdrawing proceeds, benefiting from the gas costs paid by other market participants, primarily arbitrageurs (short-term, toxic).

LPs benefit by passively (Uni V2 style) providing liquidity to mostly non-toxic order flow and controlling fees charged to toxic order flow via payment for order flow (PFoF) or dynamic fee mechanisms. Additionally, since TWAMM trades are non-aggregatable (executed in a single pool), all the fees accrue to LPs of the pool.

Versus Smart Burn Engine

During the development of DSSKiln, we presented TWAMM to thePECU team and discussed the merits. However, at that time our protocol was still under development and not ready to be used in production. Both the products are fully on-chain, transparent, permissionless, and enable trustless execution, however, there are a few significant benefits of TWAMM worth considering at this time:

- Gas Savings: TWAMM sub-trades are virtual and only written to the chain when there's a new interaction, thus traders save immensely on gas costs. With the initial parameter of 5000 bump, Maker was spending ~$550,314

per year in gas and the recent parameter update to 20,000 bump has reduced the cost but still costs ~$137,578

in gas fees (source: Flapper Config). With TWAMM, Maker would only pay to start/cancel the trade or withdraw proceeds and these operations cost roughly ~200,000 in gas on average (source: TWAMM gas costs).

- Higher Granularity: the latest parameter update reduced the frequency of purchase and increased the size of the buyback to curb the high gas costs. With TWAMMs, MakerDAO can get a much higher granularity without being constrained by rising gas costs. Also, instead of worrying about executing the trade during a low gas period, the long-term trade gets the average gas price over the trade duration.
- Dynamic Fees: once the trade is complete, the liquidity pool used in this trade (Uniswap V2) is set to 0.3% and cannot be changed. However, in TWAMM pools the administrator (MakerDAO) can dynamically change the fees for both short-term and long-term traders to incentivize desired behaviors.

MakerBurn Trade Analysis

We did a coarse simulation for the MakerBurn trade to illustrate how it could perform with TWAMM. Below is a technical diagram of the simulation infrastructure used to estimate the results.

[

Simulation MKR - DAI LT Swap-MKR 2

1322×762 127 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/a/b/abe1db972e5d440c6b5a517d1fc892df0520fd79.jpeg)

The figures presented in the chart below for the simulation were inspired by the Maker Burn simulation spreadsheet. We varied the gas costs, Ethereum prices, and MKR prices to get a sense of how TWAMM trade would perform under different liquidity conditions.

Given the current pool has roughly $24M in liquidity, the swap cost would roughly be ~0.5%

which is in line with the current Uniswap V2 TWAP trade.

[

dai_mkr_gas_sweep_2

1121×692 237 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/6/9/69dffe207cf14eb445e3ff81d43ccf148cc31d21.png)

To get a better sense of the potential performance of TWAMM, we quickly assembled a simulation based on an analysis of 5 days of actual Maker Burn data. The Maker Burn transactions from Sept 8 - Sept 12, 2023, inclusive, were analyzed to determine minimum, average and maximum figures for gas fees and the amount of MKR received:

[

table1

974×150 49.6 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/8/0/8013323a6e63330b6dcfadea0bb8635b719adcc1.png)

The values were then extrapolated to a 30-day month and compared with CronFi TWAMM simulations in the system diagrammed above. However, parameters were swept as follows:

- Average gas: 20 gwei, 30 gwei
- TWAMM Liquidity: $12M, $24M
- ETH: $1540.63, $1597.00, $1643.36
- MKR: $1073.65, $1112.63, $1151.61

The amount of minimum, maximum, and average amount of MKR received is shown below for the aforementioned parameter sweeps. Note the significantly reduced estimated gas fees with improved amounts of MKR received for the average and maximum values:

[

table2

1105×188 88.1 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/d/2/d2d6d8b56c8ad32b173696881f315387d70191b8.png)

Risks & Mitigations

We have been researching and developing TWAMMs since the original paper release. During that time we have published monthly updates on the progress and risk evaluations, see documentation. Here are a few of the most pertinent risks and how we have mitigated them:

- Audit: our code was fully audited by SpearbitDAO with 0 critical bugs found, seereport
- Live Trade: we successfully completed a $1M treasury diversification trade for NounsDAO with <$185k in pool liquidity, see report.
- Smart contract:
- Hack Risks: built on Balancer V2 Vaults which have been battle-tested for 2+ years. Each pool on Balancer is isolated from risks with other pools.
- Bricked Pools: we've done extensive research and mitigations for gas, order DDoS, numerical underflows, incorrect TWAMM parameters, etc – more information.
- Loss of Funds: open-source code, audited, non-custodial, users in full control of funds, trade happens over multiple blocks so it can be canceled at any time by the user.
- Malicious Pool Admin: all pool administrators can do is pause the pool or alter fees at which point traders can cancel and withdraw their funds
- Hack Risks: built on Balancer V2 Vaults which have been battle-tested for 2+ years. Each pool on Balancer is isolated from risks with other pools.

- Bricked Pools: we've done extensive research and mitigations for gas, order DDoS, numerical underflows, incorrect TWAMM parameters, etc – more information.
- Loss of Funds: open-source code, audited, non-custodial, users in full control of funds, trade happens over multiple blocks so it can be canceled at any time by the user.
- Malicious Pool Admin: all pool administrators can do is pause the pool or alter fees at which point traders can cancel and withdraw their funds
- Lack of Arbitrage: we have built our own arbitrage bots and have teamed up with BloXroute to provide dedicated arbitrage service. On the off chance neither service arbitrages the pool, the open market will arbitrage the pool as seen in the Nouns DAO trade.
- Poor Execution: orders are cancellable at any time i.e. if the price escapes preferred bounds restart the order at another time. We will work with the Risk team to provide an analytics dashboard for the community to monitor the trade performance
- Information Leakage: this is not a big concern since the MKR/DAI trade has been ongoing for a few months already
- MEV/Sandwich Attacks: mitigated by DCA and furthermore virtual trades require multi-block MEV techniques

Infrastructure Changes

There are a few changes needed to substitute TWAMMs for Maker Burn. Here's a high-level picture of the new infrastructure:

[

updatedDesign

1078×716 68.2 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/d/4/d47410627f94fd0444dd003ff49756db5995c9c8.png)

Proposed changes:

- Deposit liquidity into TWAMM pool, similar to 50/50 Uniswap V2 style
- Issue long-term trade when surplus is over $3M
- Withdraw proceeds from TWAMM pool and pair with DAI to LP back into the pool

We are happy to work with MakerDAO to transition the system from DSSKiln to TWAMM and help review/support the proposed changes.

Future Costs & Upgrades

Although DSSKiln development has been completed, future changes, upgrades, audits, and maintenance costs plus engineering hours would be better spent on other more pertinent needs. As TWAMMs are our primary focus, we are constantly iterating and improving the protocol to give traders and liquidity providers more control. Some interesting features we are currently developing:

- Modifying Trade Rate/Duration: increase/decrease rate of asset purchase in-flight without having to cancel or restart orders
- Pause Order: limit potential bad fills by pausing trades when the price of assets is outside the desired bounds
- Directional Fees: set separate fees for a → b swap vs b → a swaps to incentivize traders to purchase or sell assets in the preferred direction