Swaap v2: Optimal liquidity infrastructure

Swaap Labs

interface: gm@swaap.finance;

June 1, 2023

Abstract

Swaap v2 is a non-custodial RfQ[*] market-making infrastructure. It provides optimal liquidity services with built-in defensive modules – or "safeguards” – allowing for on-chain max drawdown circuit breaker[†], last look, and other dynamic forms of funds protection. LPs passively benefit from state-of-the-art market-making strategies originating from the stochastic control theory. Liquidity pools automatically compound fees, and are represented as ERC-20 tokens for simpler auditability and composability. The first strategy available will focus on optimizing LPs returns against “HODLing”.

Keywords: Decentralized Finance, Automated Market Maker, RfQ

Contents

[*] In a request-for-quote (RfQ) system, traders receive signed quotes in response to trading requests. Actual transactions can later be concluded by accepting the provided quotes.

[†] The max drawdown circuit breaker prevents a trade from happening if the pool performance compared to HODL on a given period of time (eg: last 24h) would be lesser than a given threshold if the latter trade would have been executed.

1 Motivation

A market-maker is an agent that quotes both a buy and a sell price in a tradable asset held in inventory, hoping to make a profit on the bid–ask spread. Additionally to generating profit to the agent, the market also benefits from it through the overall reduction in price volatility and trading costs that come as a result.

Consequently, market-maker services are usually appealing to both yield-seekers, and marketplaces or entities willing to improve liquidity on a given set of assets.

In the crypto industry, two main types of players operate as market-maker today: the centralized players (traditional market-makers like Wintermute, Jump Trading but also bankrupted actors like Alameda Research or Three Arrows Capital) and the decentralized ones, usually implemented as automated market-makers – or "AMMs" – in the like of Uniswap, Curve, and Balancer.

These different players address the same problem: bringing liquidity to the market efficiently. This most generally means getting a combination of a bid-ask spread compression with additional revenues for the LPs. Because of the structural differences between these two families, very different trade-offs are being made under the hood. In section 1.1, we will expose what we see as desirable properties for a market-maker to have. In section 1.2, we will expose how the trade-offs made by current actors fail to meet those properties.

1.1 Desirable properties for market-making services

We establish the following desirable properties for market-making solutions with safety and efficiency in mind:

1. Open: efficient financial primitives should be mainstream products.
2. Transparent: past and current performances (APR, volatility, max drawdowns, etc.) should be programmatically accessible, and auditable by anyone, anytime.
3. Non-custodial: market-makers should not have access to the LPs' funds – outside a well-defined scope (trade execution, etc.).
4. Composable: LP positions should be easily composable.
5. Secure: contracts should be immutable and open source, with strong defensive mechanisms for LPs' funds safety.
6. Adaptive: strategies should be able to continuously integrate context changes (such as price, volatility, etc.) with a very high frequency.

1.2 Limitations of existing market-making solutions

While being able to deploy complex strategies, centralized players suffer from:

1. Lack of openness: they usually require large initial investments and are hence not available to retail investors seeking yields.
2. Opacity: open positions are most generally not publicly available which makes the assessment of market making strategies difficult. This could eventually lead to important loss, for instance in case of over leveraged strategies, etc.
3. Custody risk: market-makers typically operate on centralized exchanges, which means that investors face the additional custody risk associated with it. The collapse of FTX remains a striking example of such risk.
4. Limited composability: programmatic finance, as DeFi is, opens new use cases that traditional market-makers can't benefit from with their off-chain positions (CEX, etc.), thus reducing their competitiveness in the long run.

Today's AMMs solve all the aforementioned problems. They also facilitate the creation of permissionless liquidity pools, increasing the depth of markets for which professional market-makers might decide not to quote, such as long-tail asset pairs.

However, today's AMMs tend to offer poor performances – negative returns with high risk – as suggested by several studies. It was found in [1] that 49.5% of Uniswap v3 [2] LP positions displayed negative returns. The authors of [3] noted that Uniswap v2 [4] and Curve v2 [5] pools were on average associated with negative returns and high variance when simulated on volatile-to-stable pairs. In [6] showed that constant function formula LPs are at risk of capital losses linked to under-priced fees as compared to volatility, and proposed new AMM designs including oracle-based quotation or volatility-indexed fees.

2 Architecture

An automated market-making system can be abstracted down to 3 core functionalities:

1. Inventory: manage asset accounting and execution, usually in a non-custodial way.
2. Quotation: propose trading quotes to be executed on-chain by the trader.
3. Settlement: run authenticity and performance checks before execution.

In Swaap v2, inventory and settlement functionalities remain on-chain and non-custodial, whereas the quotation becomes off-chain. This way we are able to deploy state-of-the-art market-making strategies, while maintaining security, transparency, composability, and openness at the highest standards.

The 3 following sections cover in greater details the aforementioned functionalities.

2.1 Inventory

Asset reserves are managed on-chain by the `SwaapV2Vault`, which is also the main interface contract for `join` / `exit` / `swap` actions.

As a plain fork of the Balancer v2 [7] Vault it inherits from all of its benefits – notably a tremendous gas optimization when it comes to multi-hop routes – as well as the same security guarantees that a highly audited and battle tested contract can offer.

Another interesting feature inherited from this architecture is the concept of "Asset Manager" allowing idle funds to be allocated to other venues such as Aave [8], Compound [9], Spark [10], Fraxlend [11], or Morpho [12] to get additional yield – the so-called "Boosted Pools" – in a safe and transparent manner.

2.2 Quotation

Swaap Labs, the first whitelisted quote provider, will broadcast quotes following the model described in [3].

This kind of approach aims at maximizing LPs' PnL against a given benchmark, while dealing with stochastic constraints such as trading appetite, market price, volatility, and toxic flow.

$$\delta^* = \sup_{(\delta^{\text{buy}},\delta^{\text{sell}})\in\mathcal{A}} \mathbb{E}\left[PnL - B\right]$$

Where $\mathcal{A}$ is the space of markups, and PnL (resp. B) represents the LPs' PnL (resp. the Benchmark) stochastic process, as defined in [3].

The first strategy available will have HODL as benchmark, and so will optimize LPs returns against “HODLing”.

This module is managed off-chain for multiple reasons, among the most salient are:

1. Adaptivity: market conditions are evolving constantly. Highly complex and dynamic models are a prerequisite to delivering high yields consistently.
2. Signal: market-making models need rich and up-to-date signals to operate efficiently – such as market prices or proprietary alphas. Today, most of this information is accessible solely off-chain.
3. Composability: integration process with DEX aggregators can be a hurdle when complex models are involved, requiring tedious reimplementations from scratch, each time. Thanks to our RfQ architecture partners looking to integrate Swaap will just need to use a simple, consistent API.
4. Security: crypto trading is a highly adverse environment. In addition to our on-chain "safeguards", we also implement important off-chain measures such as arbitrage bot detection, increasing further LPs funds safety.

2.3 Settlement

Before any execution occurs, a quote goes through a multi-stage settlement process designed to revise or reject outdated, underpriced, and invalid quotes.

They are safety measures designed to prevent value extraction from LPs' funds, notably during extreme events (flash crash, stablecoin depegging, quotation module compromise, etc.) These safeguards are implemented on-chain and rely on Chainlink [13] price feeds for some.

In the following:
r_i*: represents the reserves of* i*-th token attached to* 1 *pool token, at time* t
o_i*: represents the* i*-th token oracle price, at time* t

2.3.1 Max drawdown circuit breaker

A trade will revert if the pool underperforms HODL on the current time epoch $e_{\phi(t)}$ (eg: last 24h) by more than $y > 0$, as measured if the trade would have been executed:

$$\texttt{require} \qquad \frac{\sum_{i=0}^{n} r_i^t \cdot o_i^t}{\sum_{i=0}^{n} [r_i]^{e_{\phi(t)}} \cdot o_i^t} > 1 - y$$

Where:
$\phi : \mathbb{N} \to \mathbb{N}$ the time $\leftrightarrow$ epoch mapping .
$e_{\phi(t)}$: represents the epoch corresponding to time t
$[r_i]^{e_{\phi(t)}}$ represents the reserves of asset i attached to 1 pool token, at the beginning of epoch $e_{\phi(t)}$.

2.3.2 Last look

This feature is designed to reject trades with an outdated price. The buy-price for a given asset i - as expressed by the quote - cannot deviate from the on-chain price more than $d > 0$.

$$\texttt{require} \qquad \frac{q_i^t}{o_i^t} > 1 - d$$

Where:
q_i: represents the quote price for token i, at time t

2.3.3 Max imbalance

A trade will revert if the reserves of the bought token i deviate by more than $s > 0$ compared to its fee-augmented initial reserves, as measured if the trade would have been executed:

$$\texttt{require} \qquad \frac{r_i^t}{[r_i]^{e_{\phi(0)}}} \cdot \prod_{k=1}^{\phi(t)} \frac{\sum_{j=0}^{n} [r_j]^{e_{\phi(k)}} \cdot [o_i^*]^{e_{\phi(k)}}}{\sum_{j=0}^{n} [r_j]^{e_{\phi(k+1)}} \cdot [o_i^*]^{e_{\phi(k+1)}}} > 1 - s$$

Where:
$[o_i]^{e_{\phi(t)}}$ represents the oracle price of asset i, at the beginning of epoch $e_{\phi(t)}$.

3 Governance

The `SwaapV2Vault` and the `SafeguardFactory` are owned by the DAO – initially implemented by a multiset before a proper decentralization takes place through our governance token – and will be granted the permissions to:

1. Set safeguards hyperparameters such as max drawdown threshold. Note that, to limit risks, immutable constraints are set on-chain at deployment time.
2. Set and revoke quote providers' rights to sign quotes. At the start, Swaap Labs will be the quote provider.
3. Pause and unpause the protocol, except withdrawal which is always permitted.
4. Set and collect management fees[1]. At the start, protocol fees will be 0%.
5. Transfer those permissions to another address.

4 Use cases

4.1 Investors: the most advanced market-making strategies

By being LP on Swaap v2, investors benefit from the most advanced marker-making strategies in a passive and permissionless manner.

The RfQ architecture allows for leveraging highly complex models as well as low latency data feeds, while maintaining very high security and performance standards thanks to the on-chain safeguards.

[1] The management fee is calculated as a percentage of assets under management.

Additionally, Swaap v2 LP positions are represented as ERC-20 making them convenient as building blocks to create leveraged products with even higher APRs.

4.2 DAOs: transparent and sustainable liquidity

Swaap v2 offers DAOs the ability to increase liquidity on their token and treasury in a transparent and sustainable way.

1. Compared to traditional AMMs, protocols get access to the most advanced market-making strategies available on the market, hence limiting risks arising from the use of over-simplistic quotation logic such as the constant product formula.
2. Compared to traditional market-makers, protocols benefit from additional security brought by the on-chain safeguards, such as the max drawdown, while being 100% a non-custodial solution.

4.3 DAOs: real yield for the community

Swaap v2 amplifies DAO token utility by creating additional passive yield opportunities. As ERC-20 tokens, Swaap v2 LP positions are highly composable and can appeal to a wide range of profiles once integrated into structured products.

References

[1] Loesch, S., Hindman, N., Richardson, M.B., Welch, N.: Impermanent Loss in Uniswap v3. https://arxiv.org/pdf/2111.09192.pdf (2021)

[2] Adams, H., Zinsmeister, N., Salem, M., Keefer, R., Robinson, D.: Uniswap v3 Core. https://uniswap.org/whitepaper-v3.pdf (2021)

[3] Bergault, P., Bertucci, L., Bouba, D., Guéant, O.: Automated Market Makers: Mean-Variance Analysis of LPs Payoffs and Design of Pricing Functions. https://arxiv.org/pdf/2212.00336.pdf (2022)

[4] Adams, H., Zinsmeister, N., Robinson, D.: Uniswap v2 core. https://uniswap.org/whitepaper.pdf (2020)

[5] Egorov, H.: Automatic market-making with dynamic peg. https://classic.curve.fi/files/crypto-pools-paper.pdf (2021)

[6] Milionis, J., Moallemi, C.C., Roughgarden, T., Zhang, A.L.: Automated Market Making and Loss-Versus-Rebalancing. https://arxiv.org/pdf/2208.06046.pdf (2022)

[7] Martinelli, F.: Introducing Balancer V2: Generalized AMMs. https://medium.com/balancer-protocol/balancer-v2-generalizing-amms-16343c4563ff (2021)

[8] AAVE, Protocol Whitepaper V1.0. https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf (2020)

[9] Leshner, R., Hayes, G.: Compound:The Money Market Protocol. https://compound.finance/documents/Compound.Whitepaper.pdf (2019)

[10] Spark Protocol. https://www.sparkprotocol.io/ (2023)

[11] Fraxlend. https://docs.frax.finance/fraxlend/fraxlend-overview (2022)

[12] Frambot, P., Delaunay, M.G., Danos, V., Husson, A., Babbar, K.: Optimizing Decentralized Liquidity Protocols. https://whitepaper.morpho.xyz/ (2022)

[13] Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., Koushanfar, F., Miller, A., Magauran, B., Moroz, D., Nazarov, S., Topliceanu, A., Tramer, F., Zhang, F.: Optimizing Decentralized Liquidity Protocols. https://research.chain.link/whitepaper-v2.pdf (2021)