Numoen Core: Automated Liquidity Provisioning and Exchange of Perpetual Options

Kyle Scott
kyle@numoen.com

Robert Leifke
robert@numoen.com

October 2022

Abstract

Numoen Core describes a permissionless protocol for the automated liquidity provisioning of perpetual options via a constant function market maker (CFMM). The result is a fully permissionless and autonomous options exchange with zero external dependencies or privileged actors that mirrors the principles of decentralization and censorship-resistance core to the Ethereum protocol.

1 Background

1.1 Constant Function Market Makers (CFMMs)

A subclass of Automated Market Makers (AMM) that utilize a trading function φ to maintain a desired ratio of reserves $R \in {\boldsymbol{R}_+}^n$ held by the AMM. This creates a generalized pricing algorithm, represented as a curve that multiple agents pool liquidity to. Thereby, a liquidity provider is in effect holding a portfolio of tokens and exposed to the volatility risks of the underliers. More importantly, the invariant quotes a price to an agent for some quantity in a two-asset trade. This proposal (Δ, Λ) is accepted by the AMM if the trading function $\varphi(R)$ is unchanged, the fee γ is < 1, and the amount of reserves R is sufficient as described by

$$\varphi(R + \gamma\Delta - \Lambda) = \varphi(R) \tag{1}$$

Due to the computational constraints of a blockchain, exchange mechanisms are limited by constant-time complexity, O(1). Making CFMMs superior to a computationally expensive order-book system.

Another benefit, is a single trading rule, $\varphi(R_1, R_2)$ that all liquidity providers must abide too. Offering the ability for anyone with capital to stake. Making

CFMMs especially effective in sparsely liquid markets such as those for "low cap" tokens where sophisticated liquidity providers are hard to bootstrap. These benefits were key to Uniswap's success.

1.1.1 Replicating Market Maker

A replicating market maker (RMM) is a CFMM whose portfolio value is composed by a trading function such that it follows a desired payoff. In this case, the portfolio of a risky and a numeraire has a function with a constant k, that ψ is non-decreasing. If the CFMM is path independent we can define our portfolio value function V to be:

$$V(p) = \inf\{p^T Q | \psi(R) \geq k, R \in R^n\} \tag{2}$$

where $k \in R$ is some constant, R is the set of our reserve asset quantities, and $p \in R^n$ is the associated price vector of our reserve set after arbitrage. Since the discrete space of particular concave payoff functions and the space of a Constant Function Market Maker (CFMM) are equivalent by conjecture, every CFMM has a consistent portfolio value function that can be equivalent to each other (add citation). This makes it possible to construct a trading function from certain replicated payoff. Hence the name.

1.2 Perpetual Futures

The most traded cryptocurrency derivative and arguably the most innovative financial product of the last five years is the perpetual future. Perpetual futures provide futures exposure without having to roll over the futures contract. These new types of derivatives have helped concentrate the liquidity between different expiry's making them both easier to trade and price due to the continuous premium known as *funding*.

Perpetual futures attempt to replicate a payoff or portfolio value through a stability mechanism using a variable funding rate. Many perpetual futures protocols exist on-chain, but dependency on centralized infrastructure and oracles has caused them to suffer many shortcomings. Current problems included but are not limited to reliance on sophisticated market makers and dependency on centralized infrastructure such as oracles.

2 Numoen Perpetual Options

Numoen perpetual options apply the structure of perpetual futures to options. The perpetual option aims to replicate the payoff of a call and put option on-chain without the typical liquidity fragmentation caused by strikes and expiry's. Introduced in the paper "Power Perpetual" by David White et. al. (2021), the derivative tracks the price of a risky asset in terms of a numeraire to the power of two. Perpetual options have the property of convexity or asymmetry, meaning

holders make money faster as prices move in their favor and lose money more slowly as prices move against them. While the continuous leverage is attractive, the constant gamma exposure could also open the door to hedging Uniswap LP positions. So far, Squeeth has been the only mainstream implementation of a power perpetual, but implemented with the tradition perpetual future mechanism.

Numoen derivatives are able to be minted and redeemed at the same price, removing the need for an external market to trade them. Unlike traditional 2x replicating derivatives, the power replicating derivative is fungible independent of entry price and liquidation free. Holders of the replicating power derivative have to pay a continuous funding rate for the asymmetric exposure they posses.

3 Market Model

In this mechanism, there are two parties taking positions that results in the creation of our derivatives market. According the paper, *Replicating Monotonic Payoffs* by Angeris et. al. (2021) the first party provides liquidity into a constant function market maker with the given trading function when the power α is equal to 2 and an upper bound on the exchange rate p_1:

$$\varphi(R_1, R_2) = R_1 - \left(p_1^2 - \frac{1}{2}R_2\right)^2 \tag{3}$$

It has been shown that this results in a portfolio value with p being the price of speculative asset in terms of base asset:

$$V(p) = \begin{cases} 2p * p_1 - p^2 & 0 \leq p \leq p_1 \\ p_1^2 & p > p_1 \end{cases} \tag{4}$$

Liquidity providers receive a share representing their deposit into the underlying liquidity pool. This share is then deposited in a specialized lending pool and made available to borrowers. Liquidity provider positions are represented as a struct with extra variables to account for accrued funding rewards in an algorithm introduced by

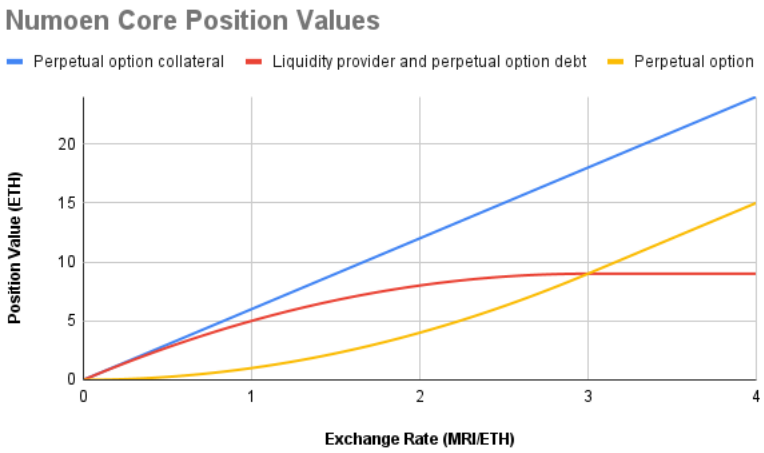
uint256	**liquidity**
uint256	**rewardPerLiquidityPaid**
uint256	**tokensOwed**

Those wishing to receive the perpetual option payoff are the borrowers of the liquidity shares. This second party of users determines the maximum amount of speculative asset that will ever be in a liquidity provider shares i. i can be found by taking $\lim_{p \to 0^+} V(p) = 2p_1$ with a value $I(p) = 2p * p_1$. Numoen perpetual options are then constructed by taking i speculative tokens as collateral and

borrowing one share of the underlying liquidity pool. This position with $I(p)$ collateral and $V(p)$ debt is

$$N(p) = \begin{cases} p^2 & 0 \leq p \leq p_1 \\ 2p * p_1 - p_1^2 & p > p_1 \end{cases} \tag{5}$$

Numoen Core implements the perpetual option as a single ERC-20 token for each specified base asset, speculative asset and upper bound.



It is important to note that because the liquidity shares are non-fee accruing, $I(p) \geq V(P) \; \forall \; p \geq 0$, so that once the reserves in perpetual option run out, then payoff ends. Thereby liquidations are impossible, avoided, and not implemented.

3.1 LP Share Redemptions

This mechanism differs from the system described in the Replicating Monotonic Payoff paper where the LP share splits the speculative and base token. In that system, the long payoff of the speculative is given to the holder of the base, and the short is holding the speculative, receiving funding in the base asset. For our use case, that mechanism is susceptible to an internal oracle flash attack.

4 Interest Rate Algorithm

Used by the most popular money markets today, the jump rate model is a statically parameterized curve that dictates an interest rate based on utilization of funds. The jump rate model determines the funding rate that must be paid from the holders of perpetual options to liquidity providers.

In *On-chain Volatility and Uniswap V3* by Lambert (2021), it is demonstrated that LP positions are analogous selling an option and pricing follows a

Geometric Brownian Motion. Using the liquidity on token pairs on Uniswap V3, we can derive the on-chain implied volatility, σ for each token pair. Jump rate paratmers are found by taking the square root of the quotient of daily volume α over the tick liquidity β multiplied by the fee tier φ * 2. The equation is as follows:

$$\sigma = 2\varphi\sqrt{\frac{\alpha}{\beta}} \tag{6}$$

So using the most recent data on the most liquid pairs on the .3% fee tier, we estimate **105.1%** to be the average implied volatility.

uint256	**kink**	.8 ether
uint256	**multiplier**	1.375 ether
uint256	**jumpMultiplier**	44.5 ether

The borrow rate between liquidity providers and perpetual options holders is calculated as multiplier $*$ $min(U_a, kink)$ + jumpMultiplier $max(0, U_a - kink)$.

4.1 Loss Versus Rebalancing (LVR)

All constant function market makers have a property called loss versus rebalancing (LVR) that refers to the aggregate loss incurred by the liquidity provider over a continuous time. Because the the LP share of a CFMM with no leverage mimics the payoff of selling a short straddle, the LP earns from fees when volatility is at a minimum. Otherwise, the LP has the potential to lose capital when providing liquidity. Therefore, LVR can quantify the economic cost of providing liquidity.

In the Numoen Core protocol the LVR is offset by a dynamic funding rate. As the paper, Automated Market Making: Loss Versus Rebalancing by Milanosis et al. (2022) notes, the LVR is equal to the floating leg of a variance swap on the speculative asset. Because the funding for a capped power perpetual is equal to the variance of the underlying asset, funding should perfectly offset the LVR. If not, arbitrageurs can also pocket the premium differences between a Numoen perpetual call option and that offered on different exchanges.

4.1.1 Arbitrage

An arbitrage takes places when their is an opportunity to buy or sell either one of the two assets, $Token_a$ or $Token_b$ for a profit on the open market in one atomic transaction so that the arbitrageur takes zero directional risk on the trade. By doing so, arbitrageurs keep the prices of the two underlying tokens, equal to the price of the same asset on an external reference market and profit on the difference $\Delta' - \Delta$. Arbitrageurs are always looking to maximize their

returns and minimize the value of the assets in the pool reserves. The relationship between the arbitrageur and the liquidity providers is zero sum.

To keep the portfolio value, $V(p)$ equal to an external market price, we want to maximize arbitrageur revenues. Therefore the system opts for no fees charges on swaps. Liquidity providers are incentivized purely by the funding rate.

References

[1] Guillermo Angeris, Alex Evans, Tarun Chitra, *Replicating Monotonic Payoffs*, Papers 2111.13740.pdf, arxiv.org, September 2021.

[2] Guillermo Angeris, Tarun Chitra, Alex Evans, *Replicating Market Makers*, Papers 2103.14769, arXiv.org, March 2021.

[3] Estelle Sterrett, Alexander Angel, Matt Czernik *Primitive RMM-01*, primitive.xyz, October 2021.

[4] Guillaume Lambert, *On-chain Implied Volatility and Uniswap v3*, lambert-guillaume.medium.com, November 2021.

[5] Guillermo Angeris, Tarun Chitra *Improved Price Oracles: Constant Function Market Makers*, Papers 2003.10001, arxiv.org, June 2020.