Volmex Volatility Token v2 AMM

Volmex Labs

November 21, 2022

This paper describes the automated market making (AMM) algorithm that Volmex has developed and employs to calculate the exchange price of its new volatility tokens, Volmex volatility token v2.

1 Introduction

Volmex Labs provides implied volatility tokens for BTC and ETH. Each of these volatility tokens could be minted with their short exposures called an 'inverse token'.

A user could mint r volatility and r inverse volatility tokens by using their 400 USDC and $r = 1 - f$ where f is the fee. Alternatively, they could perform redemption by submitting 1 volatility token and 1 inverse volatility token in exchange for 400 USDC.

2 AMM for v1 tokens

Volmex v1 tokens can only be redeemed together (volatility and inverse volatility token) and swaps are performed using constant product market making (CPMM) formula.

$$x \times y = (x + dx) \times (y - dy) = K \tag{1}$$

where dx is the amount of Volmex token that user want to convert from, dy is the amount of token that user want to convert to (e.g. USDC, DAI or inverse token), and x and y are the initial amount of these tokens in the LP pool.

This swap could be performed at price P,

$$P = \frac{dx}{dy} \tag{2}$$

and the amount of base token to be received by user is,

$$dy = \frac{ydx}{x + dx} \tag{3}$$

assuming there is no fee. If we introduce a swap fee s, the amount to be received could be found as below:

$$x \times y = [x + (1 - s)dx] \times (y - dy) \tag{4}$$

$$\Rightarrow dy = \frac{y(1 - s)dx}{x + (1 - s)dx} \tag{5}$$

3 New AMM: Single-sided redemption

Volmex v1 tokens can individually be swapped on DEXes but can only be redeemed together with their inverses. For example, a user needs 1 inverse ETH volatility token to redeem 1 ETH volatility token.

In order to improve the user experience and efficiency, and reduce number of transactions in redemption mechanism, Volmex Labs have developed a new AMM algorithm which allows single-sided redemption. In other words, a user does not need to provide inverse token when they want to redeem the base asset (USDC, DAI, etc) by using a volatility token.

3.1 Redemption constraint

Assume a user would like to redeem z amount of volatility tokens. New AMM algorithm exchanges dx amount of volatility token for dy amount of inverse volatility token so that the remaining amount of volatility token, $z - dx$, could be equal to dy and redemption could be performed. Therefore, AMM algorithm imposes a new constraint:

$$z - dx = dy \tag{6}$$

3.2 Finding dx

Equation (5) tells us how many inverse volatility token to return to the user (i.e. dy), in exchange for dx amount on a volatility token. We apply the constraint in equation (6) to equation (5) to find dx, the amount of volatility token the new AMM algorithm swaps to get dy amount of inverse volatility token.

$$z - dx = \frac{y(1 - s)dx}{x + (1 - s)dx} \tag{7}$$

Equating both sides gives the following,

$$(1 - s)(dx)^2 + [x + (y - z)(1 - s)]dx - zx = 0 \tag{8}$$

which is a quadratic equation and we know the roots of quadratic equations.

$$aw^2 + bw + c = 0 \tag{9}$$

$$\Rightarrow w = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{10}$$

Using the solution in (10), we can write the solution for dx.

$$dx = \frac{-B \pm \sqrt{B^2 + 4(1-s)zx}}{2(1-s)} \tag{11}$$

where $B = x + (y - z)(1 - s)$. The term $4(1 - s)zx$ is always positive since $s < 1$ and $z, x > 0$.

Since the amount of volatility tokens to redeem cannot be more than the sum of the amounts of volatility and inverse volatility tokens in the LP,

$$x + y > z \tag{12}$$
$$\Rightarrow xs + (x + y - z)(1 - s) > 0 \tag{13}$$
$$\Rightarrow B > 0. \tag{14}$$

Therefore, $\sqrt{B^2 + 4(1 - s)zx} > B > 0$, which implies that there's only one solution:

$$\boxed{dx = \frac{\sqrt{B^2 + 4(1-s)zx} - B}{2(1-s)}}$$