ReHold V2

Renat Gafarov (re@rehold.io)
Michael Semin (michael@rehold.io)

July 17, 2023

Introduction

ReHold is an innovative multi-chain protocol developed to maximize your crypto earnings by facilitating positions in CLMM (Concentrated Liquidity Market Maker) with a fixed annual percentage rate (APR). This unique algorithmic derivative, originally designed over Uniswap V3, empowers investors to generate short trades with substantial annual returns by setting precise price ranges within the concentrated liquidity pools. Offering substantial annual returns, ReHold optimizes your investments by utilizing concise, 12- or 24-hour investment cycles.

In its updated iteration, ReHold V2 employs a two-layer scaling system. The advent of new contracts significantly reduces gas costs, making them comparable to those of standard token transfers. This innovative approach to scaling showcases ReHold's commitment to creating a user-friendly, affordable, and accessible crypto platform.

ReHold has the distinct honor of being the first to decentralize Dual Investments. While similar products exist on some centralized exchanges, ReHold stands out with its considerably more user-friendly interface, which is specially tailored for beginners. It allows those new to financial products, particularly derivatives, to navigate the DeFi landscape with ease. In its essence, ReHold combines cutting-edge technology and advanced financial strategies to offer an unrivaled DeFi experience.

Dual Investment

Dual Investment is a short-term staking feature offering high APRs. It's a pair of tokens, like ETH/USDT, where you pick only one and lock it for hours depending on the staking plan.

Then, you claim the locked amount plus the guaranteed yield — and it is paid out irrespective of where the price went. After the claim, an output amount will be returned to the user wallet with the yield (which is fixed after the creation of Dual Investment).

The ReHold protocol imposes limits on the minimum and maximum amount for each Dual Investment, aiming to mitigate risks associated with market slippage. These limits are determined based on the trading volume of Concentrated Liquidity Market Makers (CLMMs).

The result of Dual Investment depends on the close price: if the close price is equal to or greater than the entry price, then the output ticker will be the quote ticker; if the close price is less than the entry price, then the output ticker will be the base ticker.

	Input Ticker = Base Ticker	**Input Ticker = Quote Ticker**
Close Price >= Entry Price	$OA_q = IA_b * EP * (1 + SP\frac{APR}{365*24})$	$OA_q = IA_q * (1 + SP\frac{APR}{365*24})$
Close Price < Entry Price	$OA_b = IA_b * (1 + SP\frac{APR}{365*24})$	$OA_b = \frac{IA_q}{EP} * (1 + SP\frac{APR}{365*24})$

Table 1: Dual calculation

IA_b – Input amount in the base ticker
IA_q – Input amount in the quote ticker
OA_b – Output amount in the base ticker
OA_q – Output amount in the quote ticker

b - Base Ticker
q - Quote Ticker

EP - Entry Price
SP - Staking Period

Approve & Permit

With the release of ERC20Permit tokens based on EIP712, it became possible to perform a targeted action and approve tokens in one transaction, which makes it possible to simplify the flow of interaction with contracts and reduce gas costs.

The ReHold protocol provides support for two token approval methods, namely ERC20Permit and standard ERC20, with ERC20Permit being the default option implemented to minimize user gas costs.

Replay

This feature allows users to **replay** their trade (reinvest) after the staking period ends instead of claiming with no gas fees (**gas-free**). After the replay, an output amount with the yield of the finished trade will be the input amount in a new Dual Investment

on the same pair of tokens. If the staking plan of the finished trade has been changed, the ReHold protocol will find the most similar parameters for the user.

Auto-Replay

This feature allows users to automate the **replay** function with no gas costs (**gas-free**). Till the Auto-Replay is disabled or the input amount has not reached the minimum or maximum limits, each Dual Investment will be replayed after the staking period is over with the actual APR at the moment of replay. Crucially, the Auto-Replay function streamlines this process without requiring users to pay for gas fees, embodying ReHold's commitment to a cost-effective and user-friendly DeFi experience.

Limit Duals

This feature allows users to create a Dual Investment when a certain price is reached above or below the current market price. Limit Duals do not lock the user's tokens, and users are allowed to create an unlimited number of orders. These orders will be processed with no gas fees (**gas-free**) in the order of the price levels being reached.

By extending the core concept of the product, Limit Duals pave the way for innovative usage strategies. The "buy low" strategy comes into play when users set a price lower than the current market rate, providing an avenue to increase purchasing volume or expand their initial investment at this reduced price. On the other hand, the "sell high" approach enables users to fix a selling price that's higher than the prevailing market rate, presenting an opportunity to sell their assets for higher profits or boost their token holdings.

Referral Program

ReHold's referral program is designed around the first-touch revenue share model, which rewards inviter with a portion of their invitees' profit for each transaction they perform. Simply put, you earn a commission every time someone you've invited to ReHold completes a profitable transaction.

It is available to withdraw the payouts at any time on any supported blockchain, and the gas costs are covered by ReHold.

Architecture

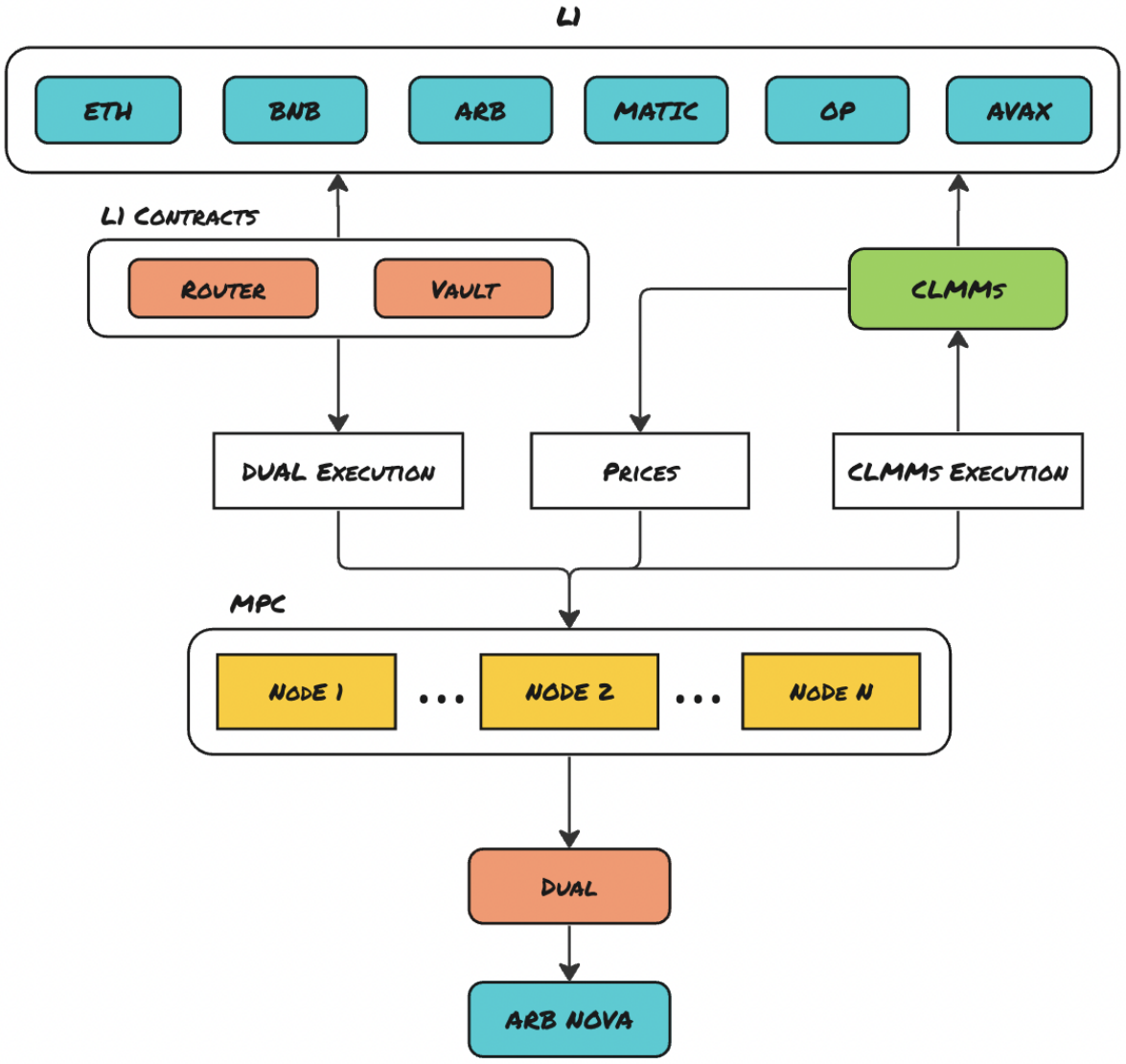


Figure 1: Architecture Principal Scheme

L1

Layer One (L1) serves as the entry level for users to interact with the protocol. Each L1 has its own Dual Investment options with tokens exclusively available on this network.

**L1 in our architecture facilitates direct communication with the user and includes ARB, OP, and potential integration with other L2 networks in the future. It differs from the concept of L1 in the Ethereum ecosystem.*

The Router is a contract that allows users to create and claim their Dual Investments. Through it, the first Dual Investment is initiated in a possible chain of replays or auto-replays.

The Vault is a contract that stores the protocol and users' tokens and makes all settlement operations (such as deposits and withdrawals). Approves and permits are issued to this contract.

MPC

In a general sense, MPC enables multiple parties – each holding their own private data – to evaluate a computation without ever revealing any of the private data held by each party (or any otherwise related secret information).

With MPC, private keys (as well as other sensitive information, such as authentication credentials) no longer need to be stored in a single place. The risk involved with storing private keys in a single location is referred to as a "single point of compromise." With MPC, the private key is broken up into shares, encrypted, and divided among multiple parties.

These parties will independently compute their part of the private key share they hold to produce a signature without revealing the encryption to the other parties. This means there is never a time when the private key is formed in one place; instead, it exists in a fully "liquid" form.

The ReHold MPC aids in decision-making for placement of positions on CLMM, price collection, and confirmation, signing signatures for the Router, managing contracts on L1 and L2, and creating duals on L2.

The process of integrating MPC into the ReHold protocol ensures that all contracts have a **timelock of 48 hours** for changing the MPC, providing a reasonable latency period for awareness of privileged operations.

CLMM

The ReHold protocol earns from providing liquidity into Concentrated Liquidity Market Makers (CLMMs) via Liquidity Pools (LPs). ReHold's innovative algorithm allows users to optimize their earnings and choose the most effective price ranges to provide liquidity into Uniswap, Pancakeswap, Trader Joe, and Quickswap.

The defining idea of Uniswap V3[1] is that of concentrated liquidity: liquidity bounded within some price range. In earlier versions, liquidity was distributed uniformly along the $x \cdot y = k$ reserves curve, where x and y are the respective reserves of two assets X and Y, and k is a constant. This is simple to implement and allows liquidity to be efficiently aggregated, but means that much of the assets held in a pool are never touched. Having considered this, it seems reasonable to allow LPs to concentrate their liquidity to smaller price ranges than $(0, \infty)$. We call liquidity concentrated to a finite range a position. A position only needs to maintain enough reserves to support trading within its range, and therefore can act like a constant product pool with larger reserves (the virtual reserves) within that range.

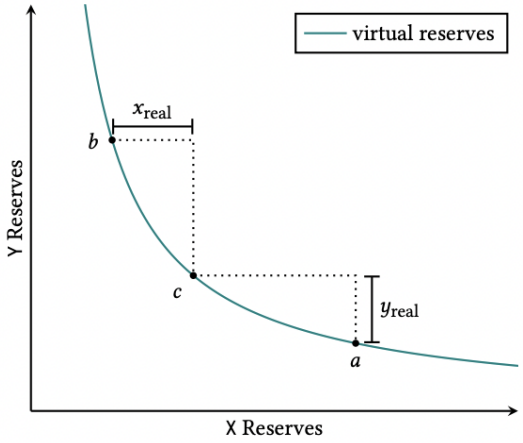


Figure 1: Simulation of Virtual Liquidity

Specifically, a position only needs to hold enough of asset X to cover price movement to its upper bound, because upwards price movement1 corresponds to depletion of the X reserves. Similarly, it only needs to hold enough of asset Y to cover price movement to its lower bound. Fig. 1 depicts this relationship for a position on a range $[pa, pb]$ and a current price $pc \in [pa, pb]$. $x$real and $y$real denote the position's real reserves. When the price exits a position's range, the position's liquidity is no longer active, and no longer earns fees. At that poInt, its liquidity is composed entirely of a single asset, because the reserves of the other asset must have been entirely depleted. If the price ever reenters the range, the liquidity becomes active again. The amount of liquidity provided can be measured by the value L, which is equal to $\sqrt{k}$. The real reserves of a position are described by the curve:

$$(x + \frac{L}{\sqrt{p_b}})(y + L\sqrt{p_a}) = L^2$$

This curve is a translation of a formula such that the position is solvent exactly within its range (Fig. 2).

[1] Uniswap V3 operation description is taken from the original whitepaper (https://uniswap.org/whitepaper-v3.pdf)

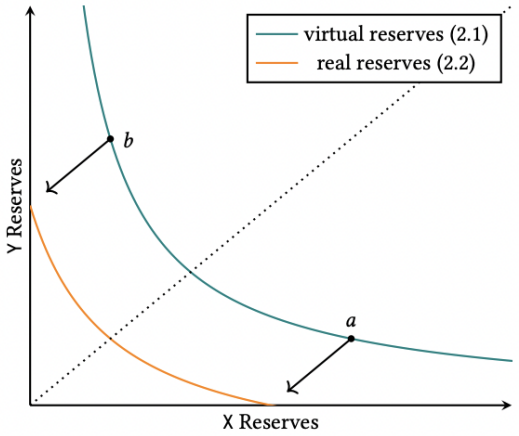
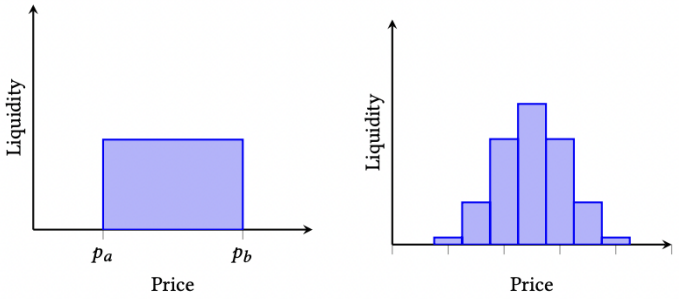


Figure 2: Real Reserves

Liquidity providers are free to create as many positions as they see fit, each on its own price range. In this way, LPs can approximate any desired distribution of liquidity on the price space. Moreover, this serves as a mechanism to let the market decide where liquidity should be allocated. Rational LPs can reduce their capital costs by concentrating their liquidity in a narrow band around the current price, and adding or removing tokens as the price moves to keep their liquidity active.



(II) A single position on $[p_a, p_b]$ **(III)** A collection of custom positions

Execution

The ReHold protocol determines the appropriate blockchain for a Dual Investment based on the position volume and pair. Subsequently, the protocol selects the most liquid Concentrated Liquidity Market Maker (CLMM) for the chosen pair on the designated blockchain.

In situations where the volume within a single CLMM is insufficient, the trade amount is distributed across multiple CLMMs. Additionally, if the selected blockchain lacks the necessary volume, a portion of the trade amount is bridged to another blockchain, allowing placement on a different CLMM to meet liquidity requirements effectively.

For smaller trades that cannot be executed directly, they are accumulated in an internal pool. Once the pool reaches its capacity, the accumulated trades are directed towards a CLMM in a single transaction, effectively reducing gas costs.

Limits

The ReHold protocol sets the specific limits for each trading pair, depending on CLMMs volume and blockchain to mitigate the imbalance risks while providing liquidity.

Additionally, each pair within the protocol has its own Total Value Locked (TVL). When a Dual Investment is created, it enters a pending status until it is executed. If the total TVL for the specific pair is exceeded, the transaction will be canceled, and the funds will be returned to the user’s wallet.

Prices

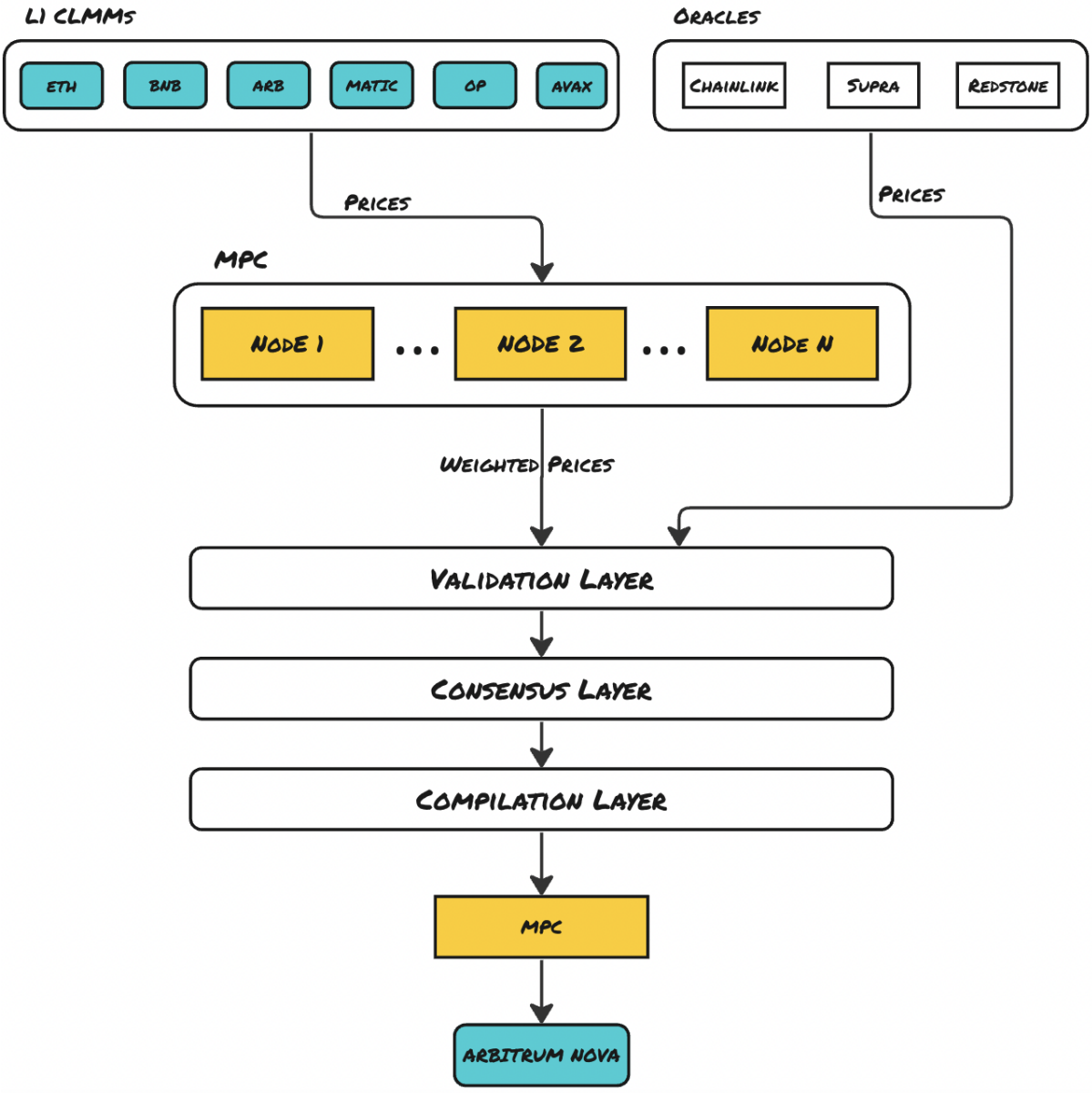


Figure 2: Prices Data Flow

The process begins with MPC nodes collecting prices from CLMMs. These gathered prices then undergo a series of steps to determine the final price, which involves weight-based aggregation. The final price is then validated using on-chain oracles like Chainlink, Supra, and Redstone.

Once a consensus approves the validated price, it is utilized in the creation transaction for the Dual Investment. This transaction includes the final price and is signed by the MPC. The final step is to send the signed transaction to L2 (Arbitrum Nova) where it is batched to Ethereum by the sequencer to prove the Dual Investment execution.

Dual

Dual is a Layer 2 contract that serves as a repository for all duals originating from various Layer 1 Routers. It functions as an aggregated database, consolidating the data from multiple sources.

L2 refers to a Layer 2 blockchain within the Ethereum ecosystem. It acts as a secondary blockchain that sequences transaction information to the Ethereum Mainnet. This ensures the validity and legitimacy of transactions executed in contracts on L2, including Dual Investments operations.

The ReHold team selected the Arbitrum Nova network due to its cost-effectiveness and TPS. Compared to other L2 solutions, Arbitrum Nova offers significantly lower transaction fees, making it 150+ times more affordable for users.

Network	TPS[2]	Txn Cost[3]
Arbitrum One[4]	8.64	$0.036
Arbitrum Nova[5]	1.10	$0.0015
Optimism[6]	5.63	$0.12
zkEVM[7]	0.52	$0.26

Table 2: Networks' Key Metrics

[2] The TPS data is derived from L2BEAT and their research on Layer 2 (L2) solutions
[3] The txn cost means the cost of Dual Investment creation on the selected network
[4] The calculations are based on a 203,000 gas limit and 0.1 gwei
[5] The calculations are based on a 83,108 gas limit and 0.01 gwei
[6] The calculations are based on a 58,210 gas limit and 665 wei
[7] The calculations are based on a 58,210 gas limit and 2.5 gwei

Effective Gas Costs

Action	Gas Usage[8]	Txn Cost[9]
Create Dual Investment	94,512	$3.61
Create Dual Investment w/ ETH	59,918	$2.29
USDT Transfer	54,128	$2.07
Claim Dual Investment	95,387	$3.65
Uniswap V3: Swap	184,523	$7.05
Uniswap V3: Add liquidity	216,912	$8.29
Replay[10]	Gas-Free	Gas-Free
Auto-Replay[11]	Gas-Free	Gas-Free

Table 3: Transactions' Costs

[8] The gas usage data is derived from Etherscan and the protocol smart-contracts
[9] The calculations are based on 20 gwei and an ETH/USD price of $1,911
[10] The ReHold protocol covers the gas fees of the replay function for users
[11] The ReHold protocol covers the gas fees of the auto-replay function for users