Zeepr V3: PvP AMM Trading Layer for On-chain Perpetual Trading

May, 2024

Norah Song
Chris Lee
Partnership@Zeepr.io

Abstract

Zeepr V3 introduces the innovative PvP AMM model, positioning it as the "perpetual version of Uniswap." Zeepr V3 aims to revolutionize the current landscape of perpetual trading by addressing widespread issues such as liquidity, extreme and one-sided market conditions, capital efficiency, trading costs, and inclusivity of trading scenarios. It is set to become a truly open, permissionless perpetual trading infrastructure. From V1 to V2, we overcame the limitations of single-chain operations, advancing towards cross-chain capabilities and integrated oracles. We transitioned from a single-chain but fully functional, low-slippage, no-funding-fee Perpetual DEX (V1) to a foundational infrastructure that facilitates seamless access for all partners and accommodates a variety of trading scenarios for diverse token holders (V2).

1. Introduction

The primary venues for perpetual contract trading are currently centralized exchanges (CEXs), which often adopt the Central Limit Order Book (CLOB) model as their matching engine algorithm. To date, there is still a significant gap in the domain of on-chain perpetual contracts. According to a market analysis report by CoinGecko, decentralized exchanges (DEXs) accounted for only 1.9% of the total crypto derivatives trading volume in 2023, with centralized exchanges (CEXs) still dominating. For spot trading, this proportion is 8.6%. Additionally, when looking at the types of assets available for trading, the contract products on the market primarily support trading of mainstream assets pegged to the U.S. dollar. Coin-based users, especially those holding assets on-chain, lack direct perpetual contract trading scenarios. While on-chain spot trading now appears to have a definitive product form, as seen with projects like Uniswap, on-chain perpetual contract trading still lacks a mature product form.

In the GMX's AMM model, the multi-asset pool provides mixed liquidity, primarily focusing on assets with high liquidity such as ETH, BTC, and stablecoins. This model pools the liquidity of mainstream assets through significant incentives to on-chain whales and DeFi natives. Introducing assets with lower liquidity into this model, or in extreme market conditions, may become uncontrollable, posing significant risks and potential losses for liquidity providers (LPs).

To manage risks under the GMX model, it becomes necessary to control traders' positions during one-sided market movements, which can compromise the trading experience. Additionally, when expanding operations, the support for different types of tokens is limited, affecting its scalability.

Similarly, in the Zeepr V2 model, which also adopts a LP and Traders betting mechanism, we encountered issues similar to those faced by GMX. In terms of initiating liquidity, our V2 version started with coin-based positioning, where the liquidity was initially provided by token issuers or large holders, ensuring depth in early trades. Although this approach can quickly attract trading users, LPs also face significant uncertainty and risks during one-sided market movements.

Therefore, we embarked on the conceptualization and design of V3, adopting a synthetic asset model to develop our product. We define this as PvP AMM.

2. The Core Mechanism of PvP AMM

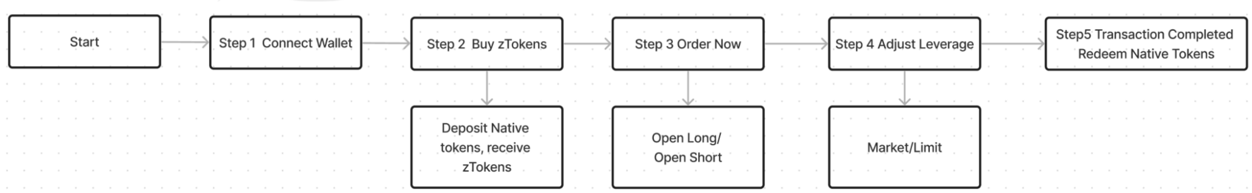
The core of the Zeepr V3 version lies in its use of synthetic assets and the exchange rates to manage risks, transforming the betting between LPs and traders into a game involving all network users, thereby introducing a novel decentralized price trading solution.

The concept of synthetic assets means that trading no longer depends on LPs, but instead views the synthetic assets themselves as the liquidity providers, addressing issues related to trading depth and one-sided markets. This mechanism not only changes the way trading is conducted but also eliminates problems such as funding fees, one-sided markets, and slippage, providing traders with a more efficient and barrier-free trading experience. In the V3 model, the impact of depth is transferred to the swap rate differences, and the algorithm for the swap rate is real-time, allowing users to precisely observe and engage with it.

Thus, users no longer need to worry about the order matching and the liquidity problem, and no longer face the uncertainties in their final PnL when liquidity is low. All they have to pay attention to is the PnL of the synthetic assets (zToken) caused by the trading itself – which exactly follows the math, and the swap rate between the zToken and the native token – if they want to swap their zToken back to the native token immediately.

In Zeepr V3, the profit and loss percentage of trading orders is calculated based on the index price, and the corresponding quantities are settled accordingly. This means that the actual final profit or loss for traders is determined by their relative gains and losses, and is no longer affected by one-sided market movements.

Users' Trading Process:



2.1 Unified Solution for Trading with Different Depth of Liquidity

Zeepr V3 effectively supports trading scenarios across different liquidity depths.

Let's assume,

- Alice opens 10x long with 100 zUSDC when BTC is priced at $10,000；
- Bob opens 10x short with 200 zUSDC at the same price；

At this time, the principal of both parties is 300 USDC (according to zUSDC:USDC = 1:1).

When BTC price dumps to $9,500,

- Alice generates: (10,000 - 9,500) / 10,000 * 1,000 = 50个zUSDC Loss
- Bob generates: (10,000 - 9,500) / 10,000 * 2,000 = 100个zUSDC Gain

The protocol executes the following:

- Burn Alice's zUSDC Loss (-50)
- Mint Bob's zUSDC Gain (+100)

Resulting in the zUSDC token price: 300 USDC / (300 zUSDC - 50 zUSDC + 100 zUSDC) = 0.86 USDC

- Alice's account value: (100 - 50) * 0.86 = 43 USDC
- Bob's account value: (200 + 100) * 0.86 = 258 USDC

Other possible scenarios are as follow:

Scenarios	BTC Price	Alice zUSDC	Alice USDC	Bob zUSDC	Bob USDC
Original	$10,000	100 zUSDC 10x Long	100	200 zUSDC 10x Short	200
1st	$9,500	Loss 50 zUSDC	43	Gain 100 zUSDC	258
2nd	$9,000	Loss 100 zUSDC	0	Gain 200 zUSDC	300
3rd	$10,500	Gain 50 zUSDC	180	Loss 100 zUSDC	120
4th	$11,000	Gain 100 zUSDC	300	Loss 200 zUSDC	0

The above example simply showcases four characteristics of the PvP AMM protocol and explains the different scenarios when the long-short balance in the PvP AMM model is disrupted compared to traditional trading:

- When the price moves towards the minority, the minority profits more, while the majority loses less.
  (Refer to the third scenario, when price increases to $10,500)

- When the price moves significantly towards the minority, the minority profits more, while the majority's loss remains unchanged.
  (Refer to the fourth scenario, when the price rises to $11,000)

- When the price moves towards the majority, the majority's profit decreases, while the minority's loss increases.
  (Refer to the first scenario, when the price drops to $9,500)

- When the price moves significantly towards the majority, the majority's profit decreases, while the minority's loss remains unchanged.
  (Refer to the second scenario, when the price drops to $9,000)

Under the PvP AMM Model, trading can be freely conducted even in low liquidity situations. In the example above, only 300 USDC liquidity is provided.

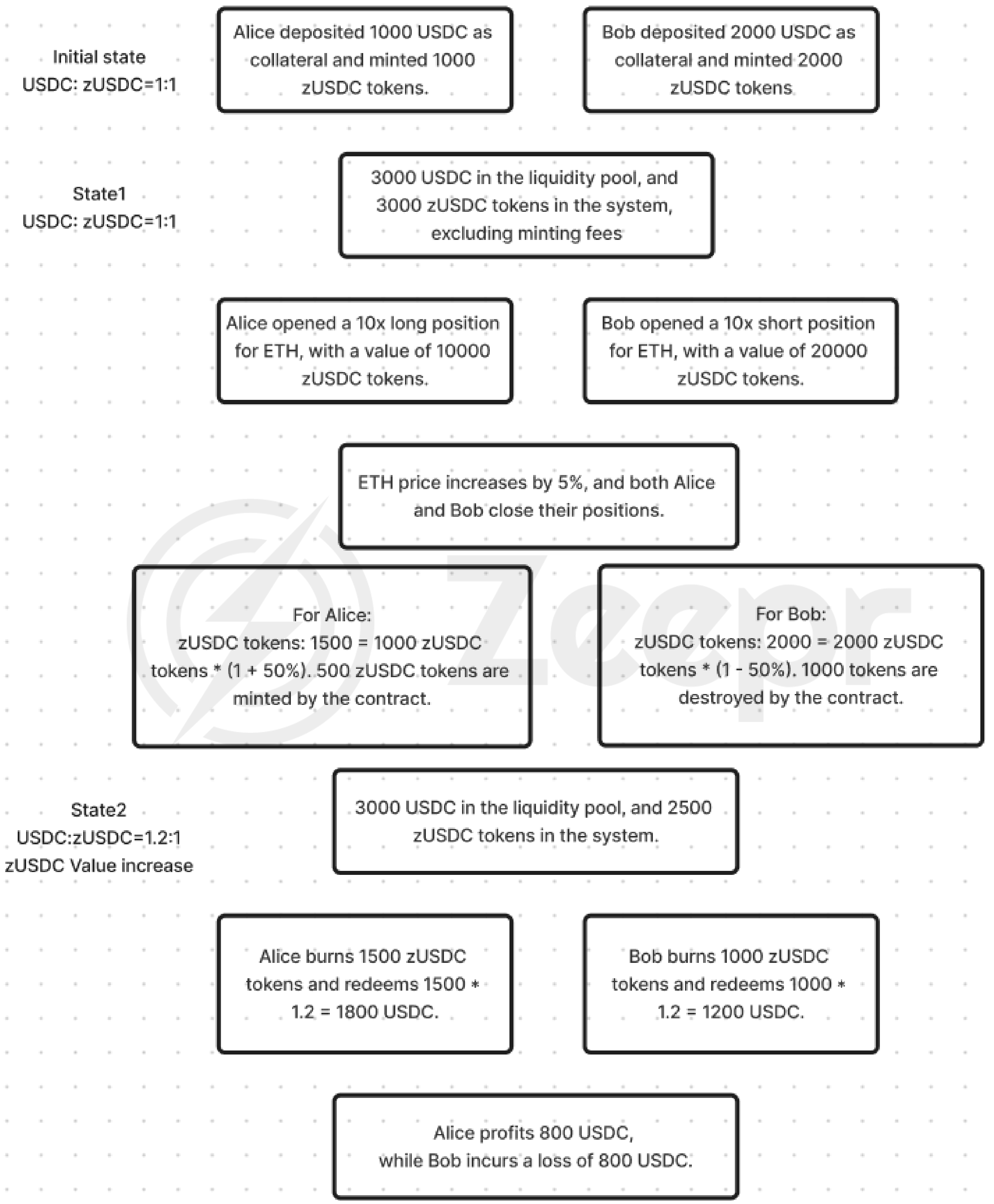
Even when only two people hold a certain asset, the moment they convert their assets into zTokens, they can form counter trades against each other, regardless of whether both place orders at the same time or only one does. In the order book model, the long and short orders need to be matched; whereas in the current mainstream AMM model, one must act as an LP, holding the zToken and unable to place orders.

Even if two people place orders in the same direction, transactions can occur, and the final gains of traders depend on their relative performance. This trading scenario cannot be supported by the order book model; while in the current mainstream AMM model, during one-sided market conditions, it is very common for a large number of traders in the entire system to open positions in the same direction, exposing LPs to extreme risk, or to protect LPs, traders might be forced to close positions.

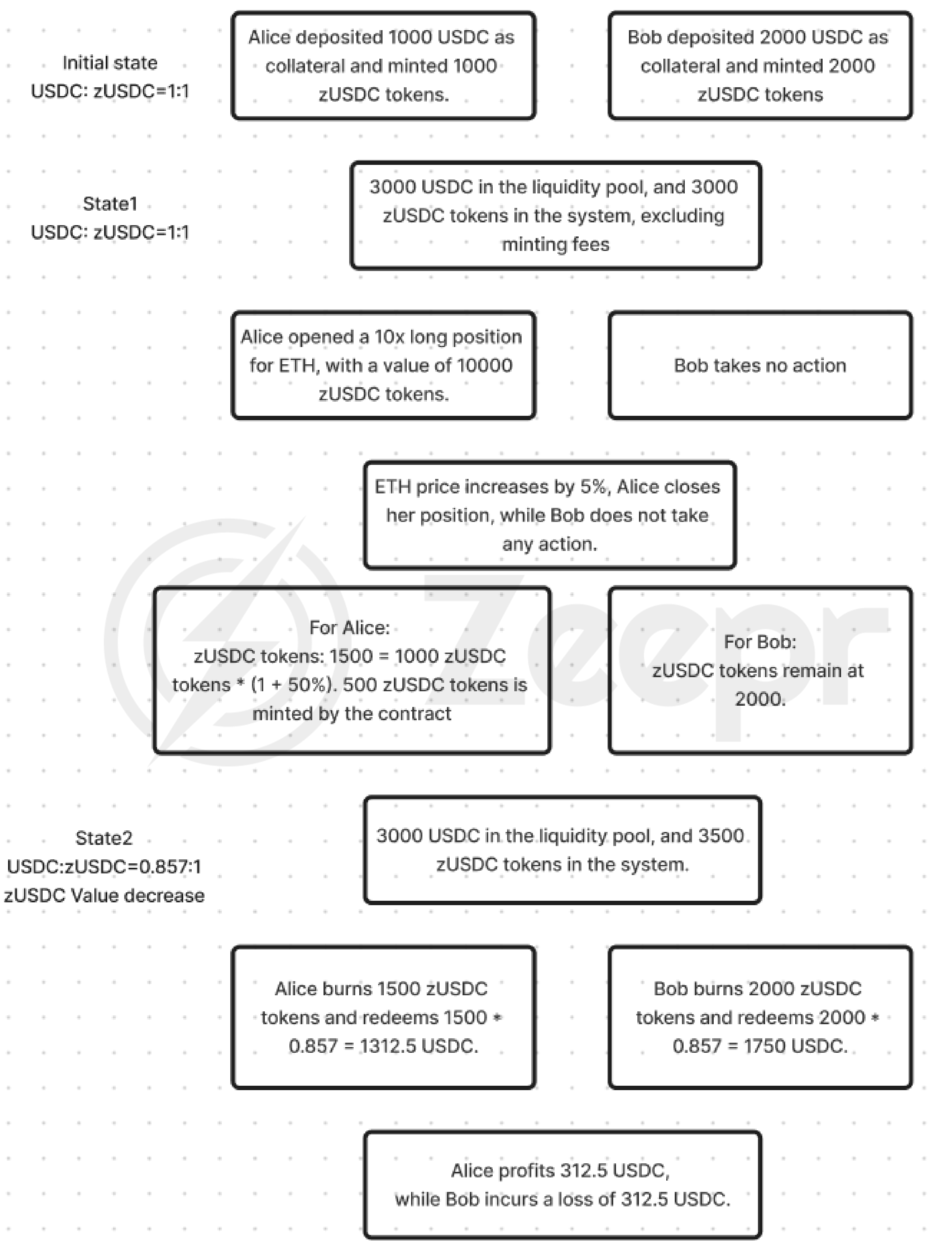
The above is just the case with two people. As more people join in, the long-short ratio will tend to balance, and the final results of trading will infinitely approach the arithmetic results of centralized perpetual trading under ideal conditions, while eliminating a series of inherent risks associated with centralized perpetual trading.

Below, we demonstrate how the protocol operates under various trading behaviors of users:

Case 1


Initial state
USDC: zUSDC=1:1
Alice deposited 1000 USDC as collateral and minted 1000 zUSDC tokens.
Bob deposited 2000 USDC as collateral and minted 2000 zUSDC tokens
State1
USDC: zUSDC=1:1
3000 USDC in the liquidity pool, and 3000 zUSDC tokens in the system, excluding minting fees
Alice opened a 10x long position for ETH, with a value of 10000 zUSDC tokens.
Bob opened a 10x short position for ETH, with a value of 20000 zUSDC tokens.
ETH price increases by 5%, and both Alice and Bob close their positions.
For Alice:
zUSDC tokens: 1500 = 1000 zUSDC tokens * (1 + 50%). 500 zUSDC tokens are minted by the contract.
For Bob:
zUSDC tokens: 2000 = 2000 zUSDC tokens * (1 - 50%). 1000 tokens are destroyed by the contract.
State2
USDC:zUSDC=1.2:1
zUSDC Value increase
3000 USDC in the liquidity pool, and 2500 zUSDC tokens in the system.
Alice burns 1500 zUSDC tokens and redeems 1500 * 1.2 = 1800 USDC.
Bob burns 1000 zUSDC tokens and redeems 1000 * 1.2 = 1200 USDC.
Alice profits 800 USDC,
while Bob incurs a loss of 800 USDC.

Case 2


Initial state
USDC: zUSDC=1:1
Alice deposited 1000 USDC as collateral and minted 1000 zUSDC tokens.
Bob deposited 2000 USDC as collateral and minted 2000 zUSDC tokens
State1
USDC: zUSDC=1:1
3000 USDC in the liquidity pool, and 3000 zUSDC tokens in the system, excluding minting fees
Alice opened a 10x long position for ETH, with a value of 10000 zUSDC tokens.
Bob takes no action
ETH price increases by 5%, Alice closes her position, while Bob does not take any action.
For Alice:
zUSDC tokens: 1500 = 1000 zUSDC tokens * (1 + 50%). 500 zUSDC tokens is minted by the contract
For Bob:
zUSDC tokens remain at 2000.
State2
USDC:zUSDC=0.857:1
zUSDC Value decrease
3000 USDC in the liquidity pool, and 3500 zUSDC tokens in the system.
Alice burns 1500 zUSDC tokens and redeems 1500 * 0.857 = 1312.5 USDC.
Bob burns 2000 zUSDC tokens and redeems 2000 * 0.857 = 1750 USDC.
Alice profits 312.5 USDC,
while Bob incurs a loss of 312.5 USDC.

2.2 Self-Balanced Liquidity Pools

PvP AMM achieves an automatic balance between long and short positions by attracting new orders from the minority side.

In the previous example with Alice and Bob, the long-short ratio was set at 1:2. For Alice, who is long, there are two favorable expected profit outcomes: the 3rd and 4th scenarios, where the price rises to $10,500 and $11,000, respectively. There is one constant and complete loss outcome, the 2nd scenario, where the price drops to $9,000. Additionally, there is one unfavorable loss outcome, the 1st scenario, where the price drops to $9,500.

At this point, Charlie joins Alice's minority side in the PvP AMM model (going long) while simultaneously going short on Binance or another CEX with an equivalent scale. The outcomes are as follows:

- In scenarios 3rd and 4th, Charlie's profits from the long positions in PvP-AMM will exceed his losses from the short positions on Binance;
- In scenario 2nd, Charlie's profits from the short positions on Binance will exactly equal his losses in the PvP AMM model;
- In scenario 1st, Charlie's profits from the short positions on Binance will not cover his losses in the PvP AMM model.

Scenario 1st can potentially transform into scenarios 2nd, 3rd, and 4th by waiting for market changes, providing a safe space for arbitrage. In traditional trading, APIs/robots/SmartMoney often pose a threat to ordinary traders. In the PvP-AMM model, they are entirely harmless and consistently maintain the balance of long and short positions in the protocol.

2.3 The Stabilization of the Swap Rate

The example in section 2.1 illustrates that a critical factor affecting both parties' profits and losses is their net PnL. When the net PnL is negative, the outcome is favorable for all traders, regardless of whether they are making a profit or a loss.

The first scenario mentioned is the least advantageous, but by incorporating neutral zToken stakers, the protocol can minimize this impact. When the size of the GLP Pool on GMX.IO is $500,000,000, the daily net PnL usually does not exceed $1,000,000, which is only 0.2% of the Pool.

In this scenario, if both parties' net PnL is +100 zUSDC, introducing GMX.IO's ratio of 0.2% into this calculation results in：

- 100 / 0.2% + 300 USDC /（100 / 0.2% + 300 zUSDC - 100 zUSDC + 200 zUSDC) = 0.998 USDC
- A’s account value: (100 - 100) * 0.998 = 0 USDC
- B’s account value: (200 + 200) * 0.998 = 399.2 USDC

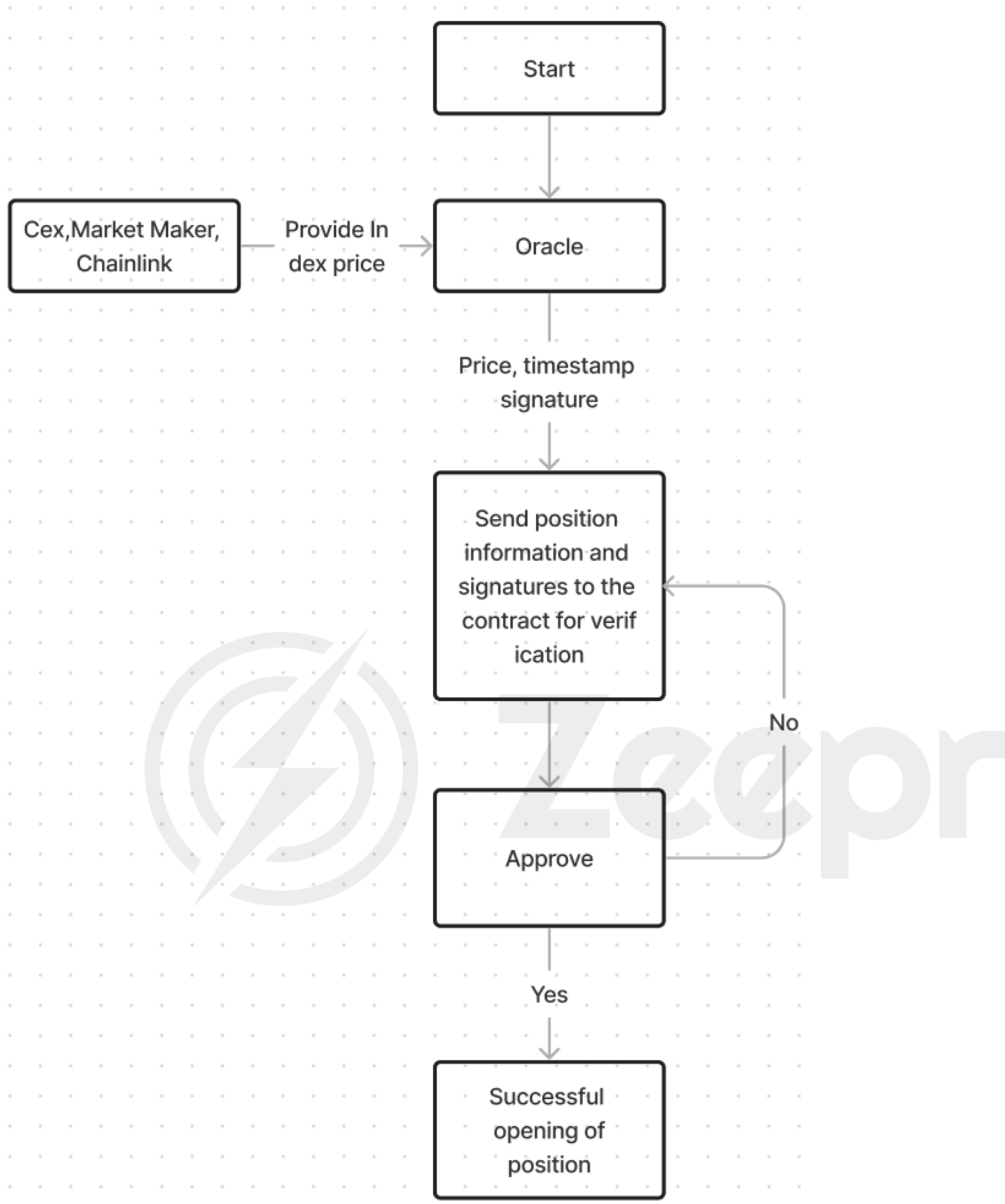
This result indicates that when the size of the neutral collateral pool far exceeds the net PnL, the impact of local trading on the overall zToken price is extremely limited. Even if the net PnL is increased tenfold, the final zToken price remains at: 100 / 0.2% + 300 USDC /（100 / 0.2% + 300 zToken + 1000 zToken) = 0.98 USDC.

2.4 Instant Order Initiation and Settlement, Unaffected by One-Sided and Extreme Market Conditions

In traditional contract trading, opening and closing positions require matching and order matching with a counterparty. If one encounters one-sided or extreme market conditions, the matching engine may struggle to quickly find a counterparty for order matching, which can adversely affect traders' profits.

The PVP-AMM, due to the absence of a trading counterparty, allows users to immediately create and close position sizes using the current oracle price upon placing their orders, with no spread or trading slippage.

Order Opening Process:



Code Example:

```
function openMarketOrder(string memory symbol,address settle,uint256 marginAmount,uint256 price,uint8 multi,
    OrderType orderType,uint256 deadline,bytes memory signature,address inviter) public{
    require(multi > 0,"PerpetualProxy: multi must be over zero");
    require(priceVerify.verifyOrder(msg.sender,signature,price,symbol,deadline),"PerpetualProxy: signer is error");
    invite.bind(inviter,msg.sender);
    exchanger.openMarketOrder(msg.sender,symbol, settle, marginAmount, price,multi, orderType);
}
```

Type	Variable
String	Symbol
Address	Settle
uint256	Margin
Uint256	Price
uint8	Multi
uint8	OrderDirect
uint256	createTime
Bytes	Signature
address	Inviter

2.5 Maximum Capital Utilization

The margin is used only to peg the swap rate of zToken and does not participate in settlements, so the protocol does not incur borrowing costs. Additionally, since the protocol does not need to match counterpart orders, there are no limits on one-sided positions, which maximizes capital utilization.

The swap rate calculation formula for zToken is as follows:

$$zToken\ Swap\ Rate\ = \frac{Total\ amount\ of\ settlement\ token\ \ in\ the\ pool}{Current\ total\ circulation\ of\ zToken + Total\ floating\ PnL\ \ of\ users'\ positions}$$

Here is a specific example:

Suppose Alice uses USDC to exchange for 100 zTokens at a 1:1 ratio. Currently, there are 100 USDC in the pool, and the circulation of zUSDC is 100. When the price of ETH is $1000, Alice uses 100 zUSDC as margin to go long on ETH with 10x leverage. When the ETH price rises to $1100, Alice's floating profit is 100 zUSDC. At this point, the zToken swap rate becomes:

$$Swap\ Rate\ = \frac{100}{100+100} = 0.5$$

This means that when new users buy zUSDC, they will do so at a swap rate of 0.5.

The calculation method for unrealized gains and losses of single settlement currency zToken can be summarized as follows:

a. Sum of all users' open position amounts and values:

$$\Sigma a1\ = \sum(Long\ position\ opening\ margin\ amount \times Leverage)$$

$$\Sigma b1\ = \sum(Long\ position\ opening\ \ margin\ amount \times Leverage \times Opening\ price)$$

$$\Sigma c1\ = \sum((Short\ position\ opening\ margin\ amount \times Leverage)$$

$$\Sigma d1\ = \sum(Short\ position\ opening\ margin\ amount \times Leverage \times Opening\ price)$$

For example:

If a user goes long on the BTC/USD index, the margin for opening the position is 100 zTokens, the leverage is N1, and the opening price is p1. Then, the user's opening amount is 100 * N1 and the opening value is 100 * N1 * p1.

b. Sum of all users' closing position amounts and values:

$\Sigma a2 = \sum(Long\ position\ closing\ margin\ amount \times Leverage)$

$\Sigma b2 = \sum(Long\ position\ closing\ margin\ amount \times Leverage \times Opening\ price)$

$\Sigma c2 = \sum(Short\ position\ closing\ margin\ amount \times Leverage)$

$\Sigma d2 = \sum(Short\ position\ closing\ margin\ amount \times Leverage \times Opening\ price)$

For example:

If a user closes a position on the BTC/USD index, the closing amount is 50 zToken, the leverage at position opening was N1, and the opening price was p1. Then, the user's closing amount is 50 * N1 and the closing value is 50 * N1 * p1.

c. Calculation of total unrealized profit and loss:

$\Sigma\ Total\ Unrealized\ Profit\ and\ Loss = \sum(Unrealized\ PnL\ of\ individual\ index\ open\ positions)$

Where the unrealized PnL of individual index open positions are calculated as follows: PnL for long positions:

- Unrealized PnL for open orders of a single index = Unrealized PnL for long positions of a single index + Unrealized PnL for short positions of a single index

Unrealized PnL for long positions:

- Long positions open amount not yet closed: $x1 = a1 - a2$
- Long positions open value not yet closed: $x2 = b1 - b2$
- Average opening price of long open positions : p = $\frac{x1}{x2}$
- Unrealized PnL for Long Positions = (Latest price - p) × $\frac{x1}{p}$

Unrealized PnL for short positions:

- Short positions open amount not yet closed: $y1 = c1 - c2$
- Short positions open value not yet closed: $y2 = d1 - d2$
- Average opening price of short open positions : p = $\frac{y1}{y2}$
- Unrealized PnL for short positions = (p - Latest price) × $\frac{y1}{p}$

3. Self-governed On-chain Perpetual Trading Ecosystem

3.1 Governance

In the Zeepr V3 model, governance tokens will play a crucial role within the Zeepr ecosystem, providing a more open and transparent environment and acting as a hub for protocol governance and ecological balance. Firstly, governance token holders can influence V3 product parameters through voting and staking, such as the fees for different asset pools and the types of tradable assets corresponding to different token pools. Additionally, as the types of liquidity pools and collateral are no longer restricted, we can envisage a system similar to the Curve protocol, where governance token holders can decide which trading pools should receive more incentives, thus balancing and stabilizing the entire ecosystem.

Token holders contribute to balancing and stabilizing the Zeepr ecosystem by holding and voting on different trading pairs' fees and reward pools. The participation and decision-making of governance token holders ensure that the ecosystem can develop in a healthier and more sustainable way while safeguarding user interests and involvement.

Furthermore, recognizing the importance of incentivizing long-term users, the incentive design can also incorporate boosting features and vesting functions, skewing incentives towards users who contribute to the system over time and encouraging user retention.

Our team's original intent was to build an on-chain trading layer that serves traders of all types with services across all chains and assets, and that fosters a highly inclusive and open trading environment governed by the community. We believe that with the launch of V3, the introduction of governance tokens, and the advancement of DAO implementation, we will take a milestone step towards realizing our vision.

3.2 Product Parameters

Based on the V3 model, Zeepr has achieved a high degree of product flexibility. Users can use any asset for collateral and liquidity pool creation, trading perpetual contracts on any asset price index under any market conditions and liquidity depth. Zeepr V3 opens this product flexibility to the market, supporting the openness of different product parameters, and truly achieving community self-governance and DAO management.

Different pools created by different users are able to co-existed for the same assets, and users can customize exclusive zToken pools for their margin token to create a contract trading platform unique to their community. When customizing zToken pools, users can specify the following information:

- **zToken Name**: Users can designate a specific zToken settlement token name for their margin token.
- **Initial swap rate between zToken and the native token**
- **Index assets that zToken can trade**
- **Maximum leverage for different index assets**
- **Trading fee ratios for zToken swap**
- **Trading fee for opening and closing positions**
- Other customizable parameters for the zToken liquidity pool, such as **whether liquidity is locked and the duration of the lock**