PerpDEX Protocol

richmanbtc
richmanbtc@perpdex.com
@richmanbtc2

May 5, 2022

Abstract

We propose a new perpetual futures DEX protocol called PerpDEX. There are three problems in existing perpetual futures DEXs. First, they have low composability because they do not support tokenization. The second problem is security concerns in the oracle-dependent and liquidation-related parts. The third problem is that decentralization is incomplete because the source code is not open to the public or the centralized part remains. PerpDEX solves these problems. The features of PerpDEX are as follows: (1) A new method, called liquidation free funding (LFF), allows positions to be tokenized with ERC4626 (2) High security due to reduced oracle dependencies and security measures, as well as a new feature called two-stage price limit (TSPL). (3) It is fully decentralized and is available as open source without the centralized part that existed in the conventional protocol.

1 Introduction

Perpetual futures have the highest trading volume in the cryptocurrency market, with 43% of the cryptocurrency trading volume in 2021 being spot and 50% being perpetual futures [1]. By contrast, the transaction volume of perpetual futures in decentralized exchanges (DEX) is still insignificant. In 2021, the share of perpetual futures transaction volume of dYdX [2] (which has the largest transaction volume in perpetual futures DEX) was 2.2% or less [1]. If DEX's trading volume share increased to 50%, the growth potential of perpetual futures DEX would be approximately more than 20 times.

Perpetual futures DEX will grow depending on improvements in chain performance. Recently, non-ETH chains other than Ethereum have been growing significantly. The TVL share of non-ETH chains in January 2021 was 3%, while that of non-ETH chains in April 2022 was 46% [3]. These non-ETH chains (in descending order of TVL share [3]) are Terra, BSC, Avalanche, Solana, Fantom, Tron, Polygon, Cronos, and Arbitrum. They tend to be superior to Ethereum in terms of gas costs and transaction speed. There are two issues related to perpetual futures DEX. The first is the gas fee. DEX trading volume tends to move from chains with high gas prices to chains with low gas prices [4]. If the chain performance improves and the gas price goes down in the future, the transaction volume of the entire DEX, including the perpetual futures DEX, is expected to increase. The second issue is oracles, which are required to implement perpetual futures DEX. As the transaction speed of the chain increases, it becomes possible to create oracles with high update frequency, and it becomes easier to implement perpetual futures DEX. Therefore, from these two perspectives, it is expected that perpetual futures DEX will continue to grow as the performance of the chain improves.

1.1 Problem

As mentioned above, while perpetual futures DEX has potential for growth, current perpetual futures DEXs have problems. The first is composability, which allows free linking with other protocols, and is an important property of decentralized finance (DeFi). The importance of composability lies in tokenization, which improves composability by tokenizing various functions of the protocol, such as liquidity provider (LP) tokens of automated market maker (AMM). However, the conventional perpetual futures DEX does not support tokenization and its composability is low. The second problem is security. The traditional perpetual futures DEX has security concerns in the oracle-dependent and liquidation-related parts. The third problem about DEX is decentralization. Some conventional perpetual futures DEXs have a centralized part, and some cannot verify the correctness of the protocol because the source code is not open to the public. These issues are discussed in detail in Section 2.

1.2 Solution

PerpDEX can solve the above problems. First, a new feature called liquidation free funding (LFF) is used to solve the problem of composability by tokenizing the perpetual futures position as ERC4626. PerpDEX can issue long tokens and LP tokens that tokenize perpetual futures positions with 100% capital efficiency. A long token is similar to Synthetix's Synthetic assets [5] and Squeeth long token [6]; it is a token that tracks the oracle prices referenced by the market. LP tokens are similar to AMM's LP tokens; they track the square root of the oracle price referenced by the market and earn transaction fees. The key to tokenization is LFF. By using LFF, the perpetual futures positions contained in the token will not be liquidated. This allows positions to be tokenized without rebalance.

Next, the security concern can be addressed by reducing the dependence on oracles and taking various measures, including a new method called two-stage price limit (TSPL). Oracles are vulnerable to attacks owing to price manipulation and other factors. PerpDEX uses oracles only for funding rate calculations, making the protocol less susceptible to attacks or corruption. Moreover, even when using oracles, which are updated infrequently, it is possible to create a market, making it easier for chains to provide many markets.

Finally, the problem of decentralization is solved by eliminating the centralized part and developing it as open source. As the source code of PerpDEX is open to the public, anyone can verify the correctness of our protocol. Decentralization is improved by eliminating the need for the trusted liquidator, which was the centralized part of the traditional Perpetual Protocol V2 [7]. The trusted liquidator was introduced as a security measure, and its elimination can be achieved by introducing TSPL. These mechanisms will be explained in detail in Section 3.

2 Related Work

In this section, we introduce the features and problems of existing perpetual futures DEXs: composability, security, and decentralization.

2.1 Composability

Composability means that a protocol can freely cooperate with other protocols, and is an important property of DeFi. There are four important factors regarding composability.

The first factor is the architecture of the perpetual futures DEX. There are two different architectures: those using AMM and those using central limit order books (CLOB). Protocols using AMM include Perpetual Protocol V2, MCDEX [8], and Hubble Exchange [9]. CLOB-based protocols include dYdX and Mango Markets [10]. The advantages of AMM are low gas cost and tokenization of LPs. The advantage of CLOBs is that LPs are more capital efficient than AMMs [4]. The gas cost of CLOB can be avoided by implementing CLOB off-chain, similar to how it is done in dYdX. However, if implemented off-chain, it is not possible to link with other contracts; therefore, it is difficult to achieve both low gas cost and composability with CLOB. From the point of view of composability, AMM is superior because it can reduce the gas cost without using off-chain and can tokenize LPs.

The second factor is AMM's LPs. There are three types of AMM LPs. The first is fungible LP, which is used in Uniswap V2 [11] and Curve Finance [12]. The advantage of this LP is that it can be tokenized as ERC20, and no management is required. The second type is non-fungible LP, which provides liquidity by specifying a price range and is used in Uniswap V3 [13]; it has the advantage of high capital efficiency because it allows liquidity to be concentrated. However, it cannot be converted into ERC20 tokens and requires management effort. The third type is LP management, which is a method that automatically operates LPs such as Uniswap V3 and is used by Charm Finance [14] and ICHI's Angel Vaults [15]. It has the advantages of high capital efficiency, ERC20 tokenization, and no management effort. However, money can be lost in case of operational failure [16]. In the case of perpetual futures DEXs, the capital efficiency of AMM itself is not essential because it can be increased by leverage. Ignoring capital efficiency, fungible LP is suitable because it can be tokenized as ERC20, has high composability, and has low management risk.

The third factor is liquidation free, which in this paper designates the property by which the perpetual future position cannot be liquidated under any circumstances. Since the position of the conventional perpetual futures DEX is not liquidation free, it is difficult to tokenize it. The reason it is not liquidation free is funding payment. The conventional funding payment mechanism is to pay funding in quote tokens and reflect it in collateral as realized PnL. While this is similar to the method used in CEX, it has the disadvantage that all positions are exposed to liquidation risk. Specifically, if the cumulative loss due to funding exceeds the original position size, it will lead to liquidation. This makes position tokenization difficult and reduces composability. UXD Protocol [17] and Lemma Finance [18] are stablecoin protocols that build delta-neutral positions in perpetual futures DEX and tokenize those positions. The advantage is that the position is delta neutral; therefore, it is difficult for to liquidate it. The disadvantages are the need for regular rebalancing to maintain delta neutrality and the non-zero risk of liquidation. Squeeth [6] is a liquidation free derivative protocol. You can issue tokens whose value is linked to the square of the ETH price. The method called normalization factor used in this protocol is similar to the liquidation free funding proposed in Section 3.2 in that it uses global scaling variables to handle funding payments. The advantage is that there is no risk of liquidation. The disadvantage is that it is not a perpetual futures DEX; therefore, the degree of freedom in trading is low. In terms of composability, a liquidation free protocol such as Squeeth is suitable.

The fourth is ERC4626, which is an extension of ERC20 that can be used to standardize vaults such as staking and Yearn Finance [19]. Like ERC20 and ERC721, ERC4626 contributes to composability. ERC4626 will be implemented in Yearn Finance, Alchemix, Balancer, Rari Capital, Fei Protocol [20]. In the perpetual protocol DEX, ERC4626 can be used to tokenize positions.

Based on the aforementioned points, we will create a composable perpetual futures DEX with a new method called liquidation free funding (LFF) and ERC4626 tokenization. The details will be explained in Section 3.

2.2 Security

Security is important in DeFi. Oracles and liquidation are particularly prone to security issues in perpetual futures DEX.

2.2.1 Oracle

Oracles are used to implement the perpetual futures DEX. Although the purpose of using oracles differs depending on the protocol, oracles are used for funding rate calculation, liquidation judgment, trade price calculation, etc. All of the protocols mentioned in this whitepaper use oracles to calculate funding rates. In dYdX, Perpetual Protocol V2, MCDEX, and Synthetix [21], oracles are used for liquidation judgment. In MCDEX and Synthetix, oracles are used to determine the trade price.

Minimizing the use of oracles reduces security risks. We discuss two specific examples of attacks on perpetual futures DEX. First is when oracles are attacked with a protocol that uses oracles for liquidation determination. In this case, the attacker may forcibly liquidate other traders and generate bad debt, thereby robbing the assets of the insurance fund. The second example is when oracles are attacked with a protocol that uses them to determine trade prices. In this case, the attacker may steal the assets of other users by trading at a price favorable to the attacker.

PerpDEX solves these security problems by using oracles only when calculating the funding rate and otherwise minimizing its dependence on it. The details will be explained in Section 3.6.

2.2.2 Liquidation

Liquidation is required to implement the perpetual futures DEX, but liquidation is easily targeted by attackers. A liquidation attack is an attack in which an attacker profits by manipulating the price used for liquidation judgment and forcibly generating the liquidation of another trader [21]. Existing protocols provide countermeasures against this attack. Three measures taken in Perpetual Protocol V2 are given below.

The first measure is to use the TWAP of oracle price for liquidation judgment. This makes it difficult to manipulate the price used for liquidation judgment; therefore, it is effective for liquidation attacks. Its disadvantage is that it is vulnerable to liquidation price arbitrage attacks (Appendix D), which are caused by the difference between the price used for PnL calculation and the price used for liquidation determination.

The second measure is to allow only trusted liquidators authorized by administrators to liquidate bad debt traders. Bad debt is a state in which a trader's asset valuation is negative. When bad debt occurs, the negative amount is compensated from the insurance fund, which leads to the outflow of assets of the insurance fund. This measure reduces the risk of protocol bankruptcy by preventing attackers from using bad debt to steal insurance fund assets. The disadvantages are that it reduces decentralization and does not prevent the liquidation attack itself.

The third measure is price restrictions using the rate of price change from the previous timestamp. This is a method in which all orders are allowed if the limit is not exceeded, and only partial closing orders and partial liquidation are allowed if the limit is exceeded. The advantage of this method is that outside the price limit, it is not possible to perform a liquidation attack with an open order for a position, making the attack difficult. This measure has two disadvantages: first, a liquidation attack can be performed by a closing order even outside the price limit; second, because it does not control the priority of regular orders and liquidation orders, there is still the possibility that regular orders and MEV attacks will delay liquidation and increase bad debt.

PerpDEX proposes a new method called two-stage price limit (TSPL) to solve these problems. The details will be explained in Section 3.5.

2.3 Decentralization

Decentralization is an important value of DeFi, but some perpetual futures DEXs have problems with it. There are two main problems. The first is that the source code of the protocol is not open to the public. Since the latest version (V3) of dYdX and Hubble Exchange are not open source, the correctness of the contract logic cannot be verified. The second problem is that the protocol has a centralized part; dYdX uses a centralized orderbook and matching engine [22]. In Perpetual Protocol V2, liquidation for traders in bad debt is not permissionless, and only trusted liquidators permitted by administrators can liquidate. PerpDEX solves these problems and improves decentralization.

3 Proposed Methods

In this section, we explain the working of PerpDEX. PerpDEX is based on Perpetual Protocol V2, a perpetual futures DEX that uses vAMM, with some improvements. First, we made improvements for composability. This includes an improvement to create liquidation free perpetual future positions called LFF and ERC4626 tokenization for perpetual future positions using it. Next, we made improvements for security and decentralization. This includes a price limit called the two-stage price limit (TSPL), improvements to reduce oracle dependence, and improvements to liquidation. Figure 1 shows the architecture overview. Table 1 shows the differences between Perpetual Protocol V2 and PerpDEX.

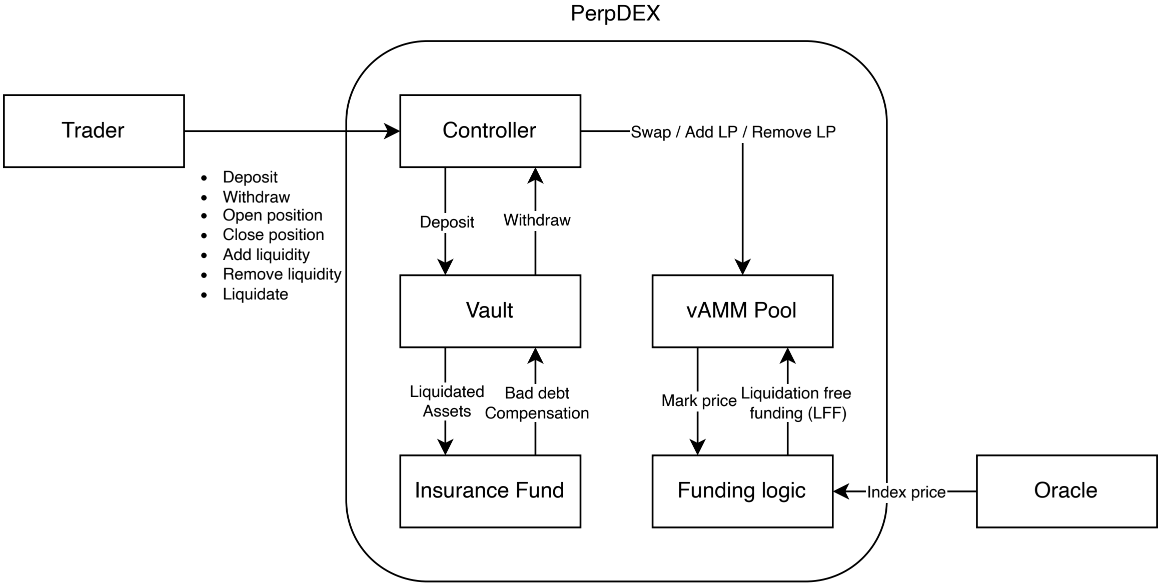

Figure 1: PerpDEX Architecture

Table 1: PerpDEX vs Perpetual Protocol V2

	PerpDEX (proposed)	Perpetual Protocol V2
Pool type	$xy = k$	Uniswap V3
Funding currency	Base	Quote
Funding target	Position or Liquidity	Collateral
Liquidation free	Yes in certain conditions	No
Price for PnL	vAMM price	vAMM price
Price for liquidation	vAMM price	TWAP of oracle price
Price limit	Two-stage (TSPL)	Single-stage
Liquidator	Permissionless	Trusted when bad debt
Liquidation reward	Part of liquidated position	Part of liquidated position
Insurance fund fee	Remaining assets after liquidation	Part of transaction fee

3.1 vAMM

PerpDEX implements perpetual futures using vAMM like Perpetual Protocol V2. vAMM was adopted because AMM is the mainstream in spot DEX, and therefore there is a high possibility that AMM will work in perpetual futures DEX, and it will be easier to tokenize LPs, which will lead to improved composability. The pool adopted a simple $xy = k$ type. There are two reasons. First, in the case of perpetual futures, unlike spots, it is possible to leverage and increase capital efficiency; therefore, there is little need to concentrate liquidity on the AMM side. Second, if the LP is fungible, the position can be tokenized as ERC4626, leading to improved composability.

3.2 Liquidation free funding (LFF)

We propose a new funding method called LFF that is needed to tokenize perpetual futures positions and improve composability. The mechanism of funding used in the conventional Perpetual Protocol V2 is to pay funding in quote tokens and reflect it in collateral as realized PnL. While this is similar to the method used in CEX, it has the disadvantage that all positions are exposed to liquidation risk. This makes position tokenization difficult and impairs composability. In LFF, funding is paid in base tokens and reflected in positions instead of collateral, making it easier to tokenize positions and improves composability.

Here, we explain the working of LFF. First, the funding rate is calculated from the premium, which is the difference between the mark price (vAMM pool price) and the index price (oracle price). The calculation method is the same as Perpetual Protocol V2; therefore, it is omitted. Next, the funding is paid using the funding rate. The amount of funding paid by each trader is the product of each trader's position (base token balance) and the funding rate. As funding is paid by base token in LFF, if the base token is treated as a rebase token, funding payment can be processed by changing the total supply of base tokens.

We will explain the above concepts using mathematical formulas. For a time $t \in \mathbb{Z}$, we denote the funding rate as $f(t)$, the total supply of the base token as $S(t)$, the balance of the base token as $b(t)$, and the shareholding of the base token as $h(t)$. Then, $S(t)$ and $b(t)$ can be as:

$$\begin{aligned} S(t+1) &= S(t) \cdot (1 - f(t)) && (1) \\ b(t) &= S(t) \cdot h(t) && (2) \end{aligned}$$

When the funding rate is positive, the total supply decreases, and when it is negative, the total supply increases.

3.3 Liquidation free region

We show that when using LFF, the trader's position is liquidation free if certain conditions are met. This is a property not found in conventional funding payments and is required for position tokenization. In PerpDEX, traders can freely combine the taker position and the LP position (maker position). The taker position is a typical perpetual futures position such as long or short. The LP position is a position that provides liquidity to vAMM. Figure 2 shows the liquidation free region for a trader who has a combined position with leverage u as a taker and leverage v as a maker. All positions in the liquidation free region are liquidation free. For example, 1x Long and 0.5x Long + 0.5x LP are liquidation free. Note that positions outside the liquidation free region are at risk of liquidation. The derivation method is described in Appendix B.

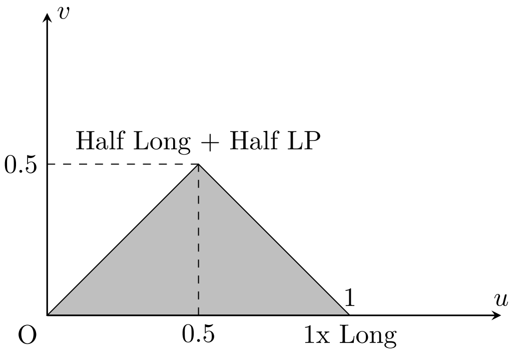

Figure 2: Liquidation free region

3.4 ERC4626 tokenization of liquidation free positions

We propose two types of ERC4626 tokens that tokenize liquidation free positions to improve composability. Note that these tokens are created as applications using PerpDEX and are not essential to it. The first token is the long token, which is a tokenized version of PerpDEX's 1x long position, and is a token that tracks oracle prices. The second token is the LP token. The LP token is a tokenized version of PerpDEX's 0.5x long and 0.5x LP combined positions, and is a token that tracks the square root of the oracle price and earns PerpDEX transaction fees. The features are summarized in Table 2. The architecture overview is shown in Figure 3. See Appendix C for details on deriving the token value.

These tokens have three characteristics. First, the perpetual future positions contained in the token are not liquidated because LFF is used. Second, it can represent all positions inside the liquidation free region. As you can see from Figure 2, these tokens are vertices of the liquidation free region; therefore, by creating a portfolio with these tokens, all the positions inside the liquidation free region can be represented. Third, it can be issued with 100% capital efficiency.

These tokens have various applications. Here are some examples. If you make a long token in the USD / ETH market (ETH / USD inverse), you can make stablecoins like UXD Protocol and Lemma Finance. If you have oracles, you can use long tokens to create tokens like Synthetix's synthetic assets. This allows you to track crypto market caps, volatility, tokens that are not on the chain, and more. If you create a market with the power of ETH / USD price oracle, you can issue tokens similar to Squeeth long token.

Table 2: ERC4626 tokens containing PerpDEX positions

Token	PerpDEX positions	Token value	Liquidation	Rebalancing
Long	1x Long	Price	Never	Not required
LP	0.5x Long + 0.5x LP	$\sqrt{\text{Price}}$	Never	Not required

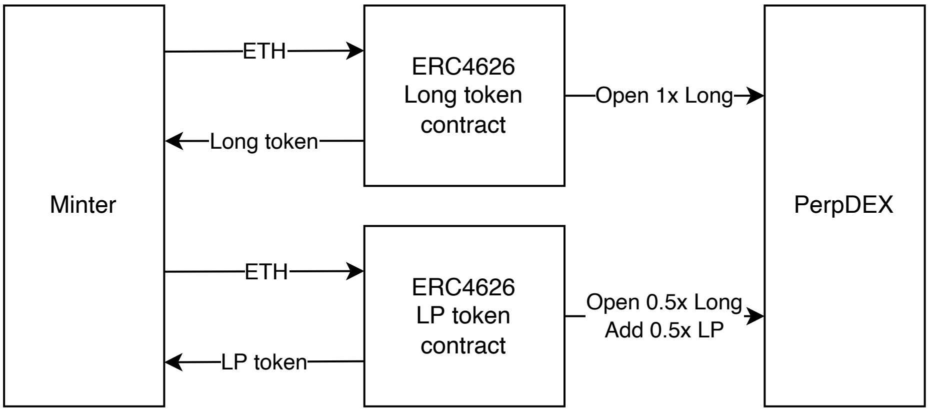

Figure 3: ERC4626 tokenization of PerpDEX positions when quote token is ETH

3.5 Two-stage price limit (TSPL)

We propose a new method called TSPL to improve security. Perpetual Protocol V2 introduced price restrictions using the rate of price change from the previous timestamp. Consequently, all orders are allowed if the limit is not exceeded, and only partial closing orders and partial liquidations are allowed if the limit is exceeded. PerpDEX uses a two-stage price limit with the following rules: (1) all orders are allowed as long as they do not violate price restrictions, (2) if the price limit of the first stage is exceeded, only liquidation is allowed, and (3) orders will be rejected if the price exceeds the second price limit. The details are shown in Table 3 and Figure

4, where r is the price change rate from the final price of the previous timestamp, and c_1 and c_2 are the limit values of the first and second stages, respectively.

TSPL is introduced to prioritize liquidation to prevent bad debt and improve security. Bad debt is a state in which the trader's asset valuation is negative. When bad debt occurs, the negative amount is compensated from the insurance fund, which leads to the outflow of assets of the insurance fund; therefore, the occurrence of bad debt should be decreased. Bad debt occurs when liquidation is delayed. With a simple one stage price limit, if normal orders are prioritized owing to bulk ordering of normal orders or MEV attacks, liquidation will not be processed and will be delayed, which is a problem. By setting a two-stage price limit and allowing only liquidation between the first and second stages, liquidation will not be delayed, and bad debt can be prevented.

Table 3: Two-stage price limit (TSPL)

Price changes	Normal orders	Liquidation
$\lvert r\rvert \leq c_1$	Accepted	Accepted
$c_1 < \lvert r\rvert \leq c_2$	Rejected	Accepted
$c_2 < \lvert r\rvert$	Rejected	Rejected

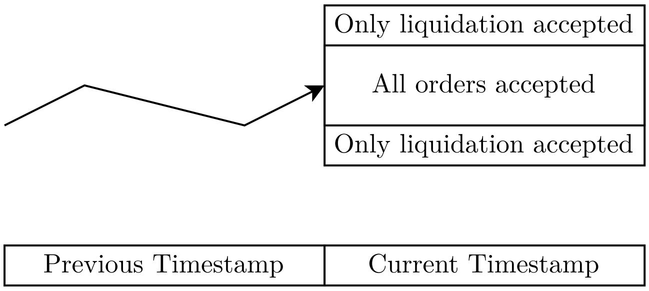

Figure 4: Two-stage price limit (TSPL)

3.6 Minimizing oracle dependencies

We minimized PerpDEX's dependence on oracles to improve security. In Perpetual Protocol V2, oracles are used for two purposes: calculating the funding rate and liquidation judgment. PerpDEX minimized its dependence on oracles by using the vAMM market price for liquidation determination and using oracles only for funding rate calculations.

There are three reasons for this change. The first is to reduce the effects of oracle attacks and errors. Oracles are vulnerable to attacks due to price manipulation and other factors. Reducing reliance on oracles makes the protocol less susceptible to attacks and corruptions of oracles. The second reason is to mitigate the liquidation price arbitrage attack (Appendix D) caused by the difference between the price used for PnL calculation and the price used for liquidation determination. The third reason is to make it easier to add a perpetual futures market. Since oracles are used only in funding rate calculations, it will be possible to create a market even if there are only oracles that are updated infrequently.

3.7 Liquidation

The liquidation process of PerpDEX is almost the same as Perpetual Protocol V2, but two changes have been made to improve decentralization and simplify protocol design.

The first change is to make liquidation permissionless. In Perpetual Protocol V2, bad debt traders could only be liquidated by trusted liquidators allowed by administrators, but in PerpDEX anyone can liquidate. The reason to limit liquidations is to deal with bad debt, but in PerpDEX, bad debt can be mitigated by TSPL; therefore, liquidation can be made permissionless. This change improves decentralization.

The second change is to use the remaining assets of liquidated traders as a source of income for the insurance fund. In Perpetual Protocol V2, the source of income for the insurance fund was part of the transaction fee, but in PerpDEX, assets remaining after liquidation are transferred to the insurance fund to make it a source of income. This is to simplify the analysis of the bankruptcy probability of the insurance fund and make it easier to design the protocol. With PerpDEX, bankruptcy probability can be analyzed as follows. Let a_i denote the remaining assets of the i-th liquidated trader. If $a_i < 0$, it means bad debt. Assuming that the balance of the insurance fund after the i-th liquidation is I_i, the initial balance of the insurance fund is I_{init}, and P_{bankrupt} is the bankruptcy probability, P_{bankrupt} can be calculated as follows:

$$\begin{aligned} I_i &= I_{\text{init}} + \sum_{j=0}^{i} a_i && (3) \\ P_{\text{bankrupt}} &= P[\exists i, I_i < 0] && (4) \end{aligned}$$

P_{bankrupt} is determined by the distribution of a_i and I_{init}. Since the distribution of a_i can be controlled by protocol parameters such as maintenance margin rate and TSPL, the protocol can be designed such that the insurance fund does not go bankrupt if the parameters are selected to keep P_{bankrupt} sufficiently small.

4 Conclusions

In this whitepaper, we proposed a new perpetual futures DEX protocol called PerpDEX, which improved three important features. First, with the proposal of liquidation free funding (LFF), it was possible to create a liquidation free position, making it easier to tokenize positions and improved composability. Next, security measures such as two-stage price limit (TSPL) and reduction of oracle dependency were considered to improve security. Finally, decentralization was improved by making the liquidator permissionless and removing the centralized part that existed in traditional protocols. In our future work, we will implement the PerpDEX protocol and demonstrate its effectiveness.

References

[1] TokenInsight Research. TokenInsight 2021 Crypto Trading Industry Annual Review, Jan 2022.

[2] dYdX. dYdX. https://dydx.exchange/. Accessed: 2022-04-30.

[3] Defi Llama. Total value locked all chains. https://defillama.com/chains. Accessed: 2022-04-22.

[4] KPMG. Crypto Insights #2. Decentralised Exchanges & Automated Market Makers – Innovations, Challenges & Prospects, Oct 2021.

[5] Synthetix. Welcome - Synthetix System Documentation. https://docs.synthetix.io/, Apr 2022.

[6] Opyn Inc. Squeeth. https://squeeth.opyn.co/. Accessed: 2022-04-30.

[7] Perpetual Protocol. Perpetual Protocol. https://perp.com/. Accessed: 2022-04-30.

[8] MCDEX. MCDEX | The Next-Gen Decentralized Perpetual Swap Exchange. https://mcdex.io/. Accessed: 2022-04-30.

[9] Hubble Exchange. Hubble Exchange. https://hubble.exchange/. Accessed: 2022-04-30.

[10] Mango Markets. Mango Markets. https://www.mango.markets/. Accessed: 2022-04-30.

[11] Uniswap Labs. Uniswap V2 Mainnet Launch! https://uniswap.org/blog/launch-uniswap-v2, May 2020. Accessed: 2022-04-30.

[12] Curve Finance. Curve.fi. https://curve.fi/. Accessed: 2022-04-30.

[13] Uniswap Labs. Introducing Uniswap V3. https://uniswap.org/blog/uniswap-v3, Mar 2021. Accessed: 2022-04-30.

[14] Charm. Charm Finance: an ecosystem of innovative products within DeFi. https://charm.fi/. Accessed: 2022-04-30.

[15] Daniel Tal. Angel Liquidity Vaults: Get Comfy this Crypto Winter. https://medium.com/ichifarm/angel-liquidity-vaults-uniswap-v3-supercharged-for-lps-and-crypto-projects-f15bc17b3946, Nov 2021. Accessed: 2022-04-30.

[16] Shaurya Malwa. How Ichi Tokens Plunged 90% After Bad Debt Fiasco on Rari. https://www.coindesk.com/tech/2022/04/12/how-ichi-tokens-plunged-90-after-bad-debt-fiasco-on-rari/, Apr 2022. Accessed: 2022-04-30.

[17] UXD Protocol. UXD Protocol. https://uxd.fi/. Accessed: 2022-04-30.

[18] Lemma Finance. Lemma Finance. https://www.lemma.finance/. Accessed: 2022-04-30.

[19] Joey Santoro, t11s, Jet Jadeja, Alberto Cuesta Cañada, and Señor Doggo. EIP-4626: Tokenized Vault Standard. https://eips.ethereum.org/EIPS/eip-4626, Dec 2021.

[20] Sage D. Young. DeFi Giant Yearn Leads the Way on ERC-4626 Token Standard Adoption. https://www.coindesk.com/layer2/2022/04/08/defi-giant-yearn-leads-the-way-on-erc-4626-token-standard-adoption/, Apr 2022. Accessed: 2022-04-30.

[21] Torgin Mackinga, Tejaswi Nadahalli, and Roger Wattenhofer. TWAP Oracle Attacks: Easier Done than Said? In *4th IEEE International Conference on Blockchain and Cryptocurrency, Virtual Conference*, May 2022.

[22] dYdX. dYdX V4 Full Decentralization. https://dydx.exchange/blog/v4-full-decentralization, Jan 2022. Accessed: 2022-04-30.

A vAMM with Rebase token

As explained in Section 3.2, LFF treats funding payments as a base of base tokens. Here, we analyze the behavior of vAMM when the base token is a rebase token. The LP fees are ignored here. Let p be the price, S be the total supply of base tokens, b be the reserve number of base tokens, and q be the reserve number of quote tokens. In the case of a rebase token, b and S increase and decrease at the same rate at the time of rebase; therefore, the invariant of vAMM of type $xy = k$ can be written as follows.

$$b \cdot q = S \cdot k \tag{5}$$

From Eq. (5), the relationships among total supply, price, and reserve are:

$$\begin{aligned} p &= \frac{q}{b} && (6)\\ b &= \sqrt{\frac{k \cdot S}{p}} && (7)\\ q &= \sqrt{k \cdot S \cdot p} && (8) \end{aligned}$$

It can be seen that the reserve amount is determined only from the total supply S and the price p.

B Liquidation free region

Here, we explain the derivation of the liquidation free region introduced in Section 3.3. Suppose a trader has a combined position of the taker position of leverage u and the LP of leverage v, where u and v are arbitrary real numbers and $v \geq 0$. When u is positive, it represents long, and when u is negative, it represents short. If t denotes time, then let $t = 0$ be the time when a trader creates a position. Let $S(t)$ be the total supply of base tokens and $p(t)$ be the price determined by vAMM at time t. The trader's collateral is $p(0)$. Assume that LP fees are ignored, and using Eq. (7) and Eq. (8), the trader's base token balance $b(t)$ and quote token balance $q(t)$ can be expressed as:

$$\begin{aligned} b(t) &= (u-v) \cdot \frac{S(t)}{S(0)} + v \cdot \sqrt{\frac{p(0)}{p(t)}} \sqrt{\frac{S(t)}{S(0)}} && (9)\\ q(t) &= -u \cdot p(0) - v \cdot p(0) + v \cdot \sqrt{p(t)p(0)} \sqrt{\frac{S(t)}{S(0)}} && (10) \end{aligned}$$

Assuming that unrealized PnL is $R(t)$, total account value is TotalAccountValue(t), total position notional is TotalPositionNotional(t), and margin fraction is MarginFraction(t) at time t, we have:

$$\begin{aligned} R(t) &= b(t) \cdot p(t) + q(t) && (11)\\ \text{TotalAccountValue}(t) &= p(0) + R(t) \\ &= p(0) + b(t) \cdot p(t) + q(t) && (12)\\ \text{TotalPositionNotional}(t) &= |b(t) \cdot p(t)| && (13)\\ \text{MarginFraction}(t) &= \frac{\text{TotalAccountValue(t)}}{\text{TotalPositionNotional(t)}} \\ &= \frac{p(0) + b(t) \cdot p(t) + q(t)}{|b(t) \cdot p(t)|} && (14) \end{aligned}$$

Let $z = b(t) \cdot p(t)$, $w = p(0) + q(t)$, then MarginFraction(t) can be written simply as:

$$\begin{aligned} \text{MarginFraction}(t) &= \frac{z(t) + w(t)}{|z(t)|} \\ &= \text{sign}\,(z(t)) + \frac{w(t)}{|z(t)|} && (15) \end{aligned}$$

Using the values of $b(t)$ and $q(t)$ obtained in Eq. (9), Eq. (10), $z(t)$ and $w(t)$ can be written as:

$$
\begin{aligned}
z(t) &= b(t) \cdot p(t) \\
&= \left((u-v) \cdot \frac{S(t)}{S(0)} + v \cdot \sqrt{\frac{p(0)}{p(t)}} \sqrt{\frac{S(t)}{S(0)}} \right) \cdot p(t) && (16) \\
w(t) &= p(0) + q(t) \\
&= (1-u-v) \cdot p(0) + v \cdot \sqrt{p(t)p(0)} \sqrt{\frac{S(t)}{S(0)}} && (17)
\end{aligned}
$$

If MarginFraction(t) is greater than or equal to the maintenance margin rate (any constant $\in (0,1)$) for any p, S, then the position is liquidation free. Consider these cases separately in relation to $z(t)$. When $z(t) = 0$, there is no position; therefore, it is liquidation free. When $z(t) > 0$, eq (15) can be rewritten as

$$
\text{MarginFraction}(t) = 1 + \frac{w(t)}{z(t)} \tag{18}
$$

If $w(t) \geq 0$, then MarginFraction(t) ≥ 1; therefore, it is liquidation free. If $w(t) < 0$, MarginFraction(t) can be made arbitrarily small by making $S(t)$ small for any $p(t)$; therefore, it is not liquidation free. When $z(t) < 0$, eq (15) can be rewritten as

$$
\text{MarginFraction}(t) = -1 - \frac{w(t)}{z(t)} \tag{19}
$$

MarginFraction(t) can be arbitrarily approached to -1 by increasing $S(t)$ for any $p(t)$; therefore, it is not liquidation free. Summarizing:

$$
\text{Liquidation free} \Leftrightarrow \forall p, \forall S, z(t) \geq 0 \text{ and } w(t) \geq 0 \tag{20}
$$

From Eq. (16) and Eq. (17), follow that

$$
\begin{aligned}
\forall p, \forall S, z(t) \geq 0 &\Leftrightarrow u - v \geq 0 && (21) \\
\forall p, \forall S, w(t) \geq 0 &\Leftrightarrow u + v \leq 1 && (22)
\end{aligned}
$$

The liquidation free region can be described as:

$$
\text{Liquidation free} \Leftrightarrow u - v \geq 0 \text{ and } u + v \leq 1 \tag{23}
$$

C Token value

Here, we describe how to derive the value of the ERC4626 token introduced in Section 3.4. LP fees are not considered in these equations. First, consider the value of long tokens. Since this is a tokenized version of the 1x long position, then $u = 1, v = 0$ and Eq. (9) and Eq. (10) become:

$$
\begin{aligned}
b(t) &= \frac{S(t)}{S(0)} && (24) \\
q(t) &= -p(0) && (25)
\end{aligned}
$$

Since the total account value represents the token value, substituting Eq. (24), Eq. (25) into Eq. (12) gives:

$$\text{TotalAccountValue}(t) \quad = \quad p(t) \cdot \frac{S(t)}{S(0)} \tag{26}$$

Next, consider the value of LP tokens. Since this is a tokenized composite position of 0.5x long and 0.5x LP, substituting $u = 0.5, v = 0.5$ in Eq. (9) and Eq. (10), we have:

$$b(t) \quad = \quad 0.5 \cdot \sqrt{\frac{p(0)}{p(t)}} \sqrt{\frac{S(t)}{S(0)}} \tag{27}$$

$$q(t) \quad = \quad -p(0) + 0.5 \cdot \sqrt{p(t)p(0)} \sqrt{\frac{S(t)}{S(0)}} \tag{28}$$

Since the total account value represents the token value, using the values of $b(t)$ and $q(t)$ given in Eq. (27) and Eq. (28), Eq. (12) can be written:

$$\text{TotalAccountValue}(t) \quad = \quad \sqrt{p(t)p(0)} \sqrt{\frac{S(t)}{S(0)}} \tag{29}$$

From Eq. (26) and Eq. (29), if $S(t)$ does not change, the value of the long token tracks $p(t)$ and the value of the LP token tracks $\sqrt{p(t)p(0)}$. The value of both tokens is uniquely determined when $S(t) \cdot p(t)$ is determined. The token value when $S(t)$ does not change is plotted in Figure 5.

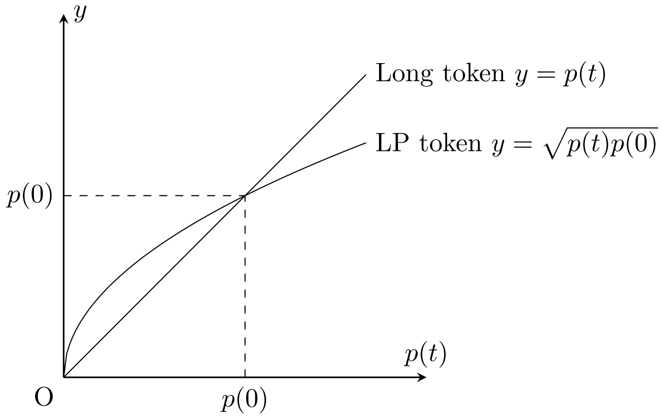

Figure 5: Token value without funding

D Liquidation price arbitrage attack

Here, we describe the liquidation price arbitrage attack. The attack occurs when the price used for liquidation judgment is different from the price used for opening or closing a position, or when calculating profit and loss. We refer to the former as price for liquidation (p_{liq}) and the latter as price for PnL (p_{pnl}). Here are two problematic cases. The first is the opening of infinite positions. Suppose $p_{\text{pnl}} < p_{\text{liq}}$. If the divergence between p_{pnl} and p_{liq} is large enough, when you open a long position, you will profit on the basis of p_{liq}. This profit makes the liquidation judgment false; therefore, you can open an infinite number of positions. The second problem is that bad debt is likely to occur during sudden price changes. For example, Perpetual Protocol V2 uses TWAP for liquidation determination; therefore, p_{liq} will be delayed relative to p_{pnl} if the price changes suddenly. This causes delayed liquidation and increased bad debt. The difference between p_{liq} and p_{pnl} in perpetual futures can be seen as putting the trader, which should be liquidated, on hold. This risk, which should be taken by the trader, is taken by the insurance fund. In many cases, p_{liq} and p_{pnl} are different to make p_{liq} a more stable price than p_{pnl} so that it will not be liquidated by sudden changes in p_{pnl}. This is an investor protection and has some benefits, but it should be done with caution from a security perspective.