Abstract

The Archimedes Protocol(AKA AKMD) is a permissionless, decentralized protocol that enables the creation of synthetic or commodity-backed derivatives by leveraging application standards pioneered by first-generation DeFi protocols. It allows anyone to freely list cryptocurrencies or value collateral, such as gold or rice, to serve as the underlying asset for derivative contracts. This article outlines the core designs of the Archimedes Protocol and how it addresses key challenges faced by perpetual contracts and derivative products. The protocol builds upon foundations laid by DeFi's first generation to introduce a permissionless derivative market where anyone can create contracts based on listed or 'unlisted' collateral assets.

Challenges of Perpetual Contract Products

The perpetual contract represents the problems encountered by the product. As of today, GMX has brought a total of $167M in revenue to its LP and token holders. Let's briefly introduce GMX and its profit model with an example.

Alice wants to open a casino but has no money. She found Bob, who was very interested in this, and decided to invest a certain amount of money to own a particular share. Alice is responsible for all the execution. If it makes a profit, Bob will enjoy 70% of the revenue and the rest will go to Alice.

In total, Bob invested $1 million, which also meant that the money the casino could ultimately earn from various games could not exceed $1 million.

The casino has a magnification function. You need to exchange your principal into chips when you enter the casino and choose a multiple between 2 times and 50 times. The multiple-choice amplifies the player's losses and gains and determines the player's maximum gain. Alice locks up the part where the user can get the maximum gain in advance. For example, if the first user enters the casino with $10,000 and chooses 50 times, it means the player can earn up to $500,000 at most. Then the casino will lock up $500,000, and all other players can only share the remaining $500,000 quota to play the game, allowing the casino to always have enough money to pay each player. From the moment the player chooses the multiple and exchanges chips, Alice will charge interest according to each player's principal, multiple choices, and remaining quota until the player leaves. In addition, players also have to pay a certain fee when entering and leaving.

In GMX, many Bobs constitute LP, multiples are equivalent to leverage, players are equivalent to each person who comes to GMX to trade contracts, and entrance and exit fees are equivalent to Alice's intermediate interest charges. You can think of some casino games as trading pairs, and this is also one of GMX's few complaints from users — fewer trading pairs.

Currently, GMX only has four index tokens on the Arbitrum network: BTC, ETH, LINK, and UNI. GMX uses Chainlink price prediction machines to obtain the overall pricing of its assets, meaning:

- Transactions on GMX will not directly affect asset prices

- There is a risk of off-site price manipulation

Last year, GMX's AVAX price was manipulated, forcing GMX to adjust the size of open positions. This is one of the important reasons for the small number of trading pairs.

[

AVAX price manipulation

1320×690 266 KB

](https://ethresear.ch/uploads/default/original/2X/8/83a0ebd2564cf06d2255e65bf277dee8aa795035.png)

Manipulated AVAX prices.

On the other hand, GMX is essentially a USD-margined trading model. For example, when you short ETH with BTC, your BTC will be exchanged for ETH to deal with the imbalance between the rise and fall of the two assets, facing the risk of being unable to pay enough.

GLP is more like a combination of several tokens. Its revenue is relatively stable but will be affected by the risks of related assets. The currencies will share risks in a certain proportion. The trading process in GMX is shown in the gray area of the figure below. You will find that users use a specific currency to pay but the counterparty is not a specific currency. In other words, the trader does not pay GLP.

[

The gray area represents the current process of GMX.

1400×653 484 KB

](https://ethresear.ch/uploads/default/original/2X/7/71a0966c283b676378a751591cefbd85a6bad589.png)

The gray area represents the current process of GMX.

We can make it more atomic and composable.

Solutions

ERC4626 Single Coin Pool and Coin-margined Trading Pairs

The AKMD protocol provides an optimized and unified revenue pool technology parameter standard, ERC-4626, that enables single coin pools. For each collateralized asset, an asset certificate compliant with ERC-20 standards is generated, enabling transfer and other operations. Furthermore, the AKMD protocol provides a range of interfaces that enable easier management of aggregator and gun pool operations.

Uniswap-like trading pair

The AKMD protocol is designed to address the need for coin-margined trading pairs. Trading pairs require four components: a treasury, index token information, collateral, and index token price sources. The protocol leverages ERC-20 standard synthetic assets for the creation of index tokens, enabling trading pairs for any tokenizable asset. This approach provides a more efficient and flexible mechanism for trading any tokenizable asset.

Interest Rate Feedback Control and ADL

Maintaining sustainability is critical for the long-term benefits of DeFi applications. AKMD offers an innovative mechanism for maintaining multilateral positions, comparing the net value of long and short positions to savings and consumption. This mechanism leverages the market interest rate as a funding rate and utilizes arithmetic increase arithmetic decrease (AIMD) as the congestion control strategy.

[

AIMD in computer network

1400×695 178 KB

](https://ethresear.ch/uploads/default/original/2X/f/f64bf4015fef6800a7e06e915f6876376c8338e2.jpeg)

AIMD(arithmetic increase arithmetic decrease) in computer network

AIMD is widely used in congestion algorithms and is integrated into the AKMD protocol to address the congestion challenges faced by multilateral positions.

In addition to AIMD, the protocol leverages interest rate feedback control and ADL(auto decrease leverage) mechanisms to maintain the sustainability of the DeFi protocol.

Parameterization and Modularization

AKMD provides a parameterization mechanism that enables custom configuration of the protocol. This feature allows users to build specific trading markets for their fields of interest, enabling more effective and dynamic DeFi applications. Additionally, parameters enable the accumulation and transfer of workload and facilitate seamless interaction with other DeFi protocols.

New Features

- Copy trading

Completely on-chain copy-trading module

- Coindays

Quantitative Dimension of Satoshi Nakamoto's Cryptocurrency

- NFT hold assets

Position, debt, and Pow are bound to NFTs

- Low-Latency oracle

A better pricing mechanism for derivative markets

- Account abstraction

More interactive experience closer to Web 2.0

- Data-driven assisted trading

Aggregated CEX and DEX exchange trading data

- ...

Conclusion

The AKMD protocol is a revolutionary DeFi protocol that addresses the significant challenges faced by the decentralized finance market. The protocol leverages innovative mechanisms, including ERC4626 single coin pool, coin-margined trading pairs, AIMD congestion control, Interest Rate Feedback Control and ADL mechanisms, and parameterization, to provide a comprehensive solution to the existing challenges of the DeFi market. The AKMD protocol provides a platform for a new generation of DeFi applications with increased efficiency, sustainability, and accessibility.