

MCDEX: DeFi Platform for Trading Perpetuals

By Liu Jie, Founder of MCDEX

1. Overview

People have been continuously exploring scenarios where blockchain technology can realize its true potential through decentralized financial services. Some DeFi projects in the context of stable coins, lending, and trading have achieved initial success in terms of the number of users and the size of collateralized funds. However, the current DeFi products still have the following problems:

- Current DeFi products are mainly aimed at traders who have advanced trading skills and are not accessible to ordinary users.
- The lack of structured products that will meet the investment needs of users with different risk appetites.

The mission of MCDEX is to make investing in DeFi more accessible by creating a secure and easy-to-use blockchain-based decentralized financial platform.

Our main product currently available on the MCDEX platform is our fully functional Decentralized Perpetual Contract which is our most important underlying asset for providing financial services.

The financial architecture of our perpetual contract is based on the proven design of perpetual contracts in the CeFi space. The trading price is soft pegged to the index price. The maximum leverage of the MCDEX perpetual contract is 10x. In addition, we provide a working mechanism that can be completely decoupled from off-chain operations.

Our perpetual contract introduces an AMM (Automated Market Maker) to provide on-chain liquidity and generate the funding rate to ensure complete decentralization. The AMM acts as a gateway to trade perpetual contracts with other smart contracts on-chain.

Since the AMM has higher slippage than traditional CeFi exchanges, we have introduced an off-chain high-speed order book for liquidity sensitive users. The order book, which provides better liquidity, is used as the main entry point for trading with the perpetual contracts. Because the arbitrageurs transmit liquidity and trading demand from the order book to the AMM, the AMM can provide funding rates for the whole market.

Perpetual contracts are very flexible underlying assets, but a large number of regular traders lack the financial literacy to effectively trade them. Using our upcoming structured financial products namely the automated robotic and social trading smart contracts, more users will profit by investing in DeFi. The funds deposited in these smart contracts are locked (for safety purposes) and the contract trades our perpetual contract based on its trading strategy to make profits for the users.

The trading strategy of the robot smart contract is fully disclosed on chain, whereas the trading strategy of the social trading smart contract is specified by traders or quantitative funds.

The security of our exchange, our contracts, and most importantly, funds deposited is our top priority. To ensure the highest order of security, OpenZeppelin and ConsenSys Diligence have audited our smart contract codes. We will continuously improve our system's security architecture, including oracles, risk control, and global settlement mechanisms.

We will issue the platform's native token, the MCB. MCB token will be used for governance, capturing value for holders, providing liquidity for AMM, taking the risk of liquidation and enjoying its benefits. Our token will form an integral part of our platform and will function better with increased network usage. Regarding distribution, 25% will be allocated to the team and initial investors, 25% will be allocated to the foundation for token sales, 50% will be used as incentives for stakeholders. After the fund product is released, we will launch the liquidity mining and allocate MCB to fund holders.

2. Perpetual contracts

The perpetual smart contract is at the core of MCDEX, and its design is based on the perpetual contracts used in CeFi. The MCDEX Perpetual contract enables trading with margin, providing up to 10x leverage, by using a funding mechanism that keeps prices anchored to an index. Unlike

traditional perpetual contracts, the MCDEX perpetual is decentralized and its logic is written in the smart contract. Because of this on-chain logic design, the MCDEX perpetual provides opportunities to build new kinds of decentralized financial products and services.

2.1 Funding payment mechanism

A perpetual contract is a financial contract without an expiration date. Its trading price is anchored to the underlying asset price index through a funding payment mechanism. Perpetual contracts are based on margin, which allows leverage.

The funding payment mechanism simulates the mechanism in the spot margin trade market. In margin trading, a third-party (e.g. a brokerage firm) lends assets to a trader who borrows assets in order to trade with leverage. A perpetual contract is traded without the need for a third-party who lends assets, with the long and short sides of the contract borrowing each other's assets and receiving interest from each other. For example, for a BTC-USD perpetual contract, the long party is the equivalent of borrowing dollars from the short party to buy bitcoin. The short party is the equivalent of borrowing bitcoin from the long to buy dollars. When the longs in the market are strong, the demand to borrow dollars rises, and the interest rate to borrow dollars rises as well. This increases the cost of holding a long position, and dampens the market demand for them. Conversely, when the market demand for short positions is strong, the demand to borrow bitcoin rises with it. The interest rate for borrowing bitcoin rises as well, increasing the cost of short positions and dampening market demand for shorting. The perpetual contract cleverly simulates the above process, when the market is trading above the index due to stronger long demand than short demand. The interest rate of longs is higher than that of shorts and thus the net interest rate paid by longs to shorts is positive, i.e., longs pay shorts, thus suppressing longs to encourage the shorts to make the price return to the index; conversely, when short demand is stronger than long demand, the market will trade below the index, interest rates of longs are lower than that of shorts, and thus the net interest rate paid by longs to shorts is negative. Shorts pay longs, thus suppressing shorting, and incentivizing the price to return to the index.

For practical reasons, instead of setting the long and short rates separately, we use the difference between the long rate and the short rate directly as the funding rate. When the market price is higher than the index, the funding rate

becomes positive and makes the long side pay the short side, suppressing the long side and lowering the market price. Conversely, when the market price is below the index, the funding rate becomes negative and makes the shorts pay the longs, hence suppressing short-sellers and raising the market price.

As can be seen from the above description, the key mechanism of a perpetual contract is to set a reasonable funding rate according to the long and short demand in the market, adjust to the market demand, and thus stabilizing the market price within a reasonable range around the index.

The funding rate calculation for the MCDEX perpetual contract is based on the funding rate methodology of the Deribit perpetual contract. First, a Fair Price is calculated from the order book. The fair price is defined as the mid price of the average price of a long order at a given depth (e.g. 1BTC) and the average price of a short order at a given depth. With a fair price, the Mark Price can be calculated. The Mark price is used to calculate the initial and maintenance margin of a position.

$$\text{Mark Price} = \text{Index Price} + \text{EMA}(\text{Fair Price} - \text{Ind$$



In the above equation, EMA is an exponential moving average function that calculates the moving average of the spread between the fair price and the index price. In practice, the mark price will be limited to a certain range of the index price (e.g. $\pm 0.6\%$).

In turn, we can define the Premium Rate as:

$$\text{Premium Rate} = (\text{Mark Price} - \text{Index Price}) / \text{Ind$$

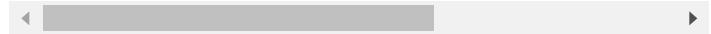


The Premium Rate reflects the market demand for long and short, and when the Premium Rate is positive, it indicates that long demand is stronger than short, and the opposite indicates that the demand for shorts is stronger than the demand for longs.

The Funding Rate for a perpetual contract is set to a value that is positively correlated with the premium rate. There is often a natural spread between the fair price and the index price. To eliminate the effects of this spread, we filter the Premium Rate through a dampener function to

obtain the funding rate. The Dampener parameter is a constant set for the system.

$$\text{Funding Rate} = \text{Max} (\text{Dampener}, \text{Premium Rate}) + M$$



In practice, the funding rate is bound to a certain range (e.g. +- 0.45%) through a threshold function. Once the funding rate is obtained, it is used as the interest rate to calculate the amount that needs to be paid to the short position within a certain period of time.

$$\text{Interest} = \text{Position Value} * \text{Funding Rate} * \text{Time}$$



When the `Funding Rate` is negative, it indicates the amount of interest that a short position has to pay to a long position.

Even if no orders are filled, as long as there are long and short orders in the order book, the `Fair Price` can be obtained, and the `Funding Rate` can be calculated from the order book, which is an advantage of calculating the funding rate from the order book.

When designing a decentralized perpetual contract, the most critical issue is how to calculate the funding rate. A simple approach is to move the order book directly on-chain and calculate the funding rate from the on-chain order book in the same way as traditional CeFi. The disadvantage of this approach is that the on-chain order book is very inefficient and the costs of placing and canceling orders can be pretty high. Thus, moving the whole order book on chain is not conducive to market making, and would lead to less liquidity. Another simple approach is to use an off-chain order book, where the orders are matched off-chain, execute the transaction on-chain, and calculate the funding rate from the order book. The drawback of this approach is its centralization. The funding rate, as a key parameter of perpetual contracts, still relies on off-chain computations. When the order book is down, the funding rate cannot be updated. Another disadvantage of this approach is that transactions must be made through the off-chain order book, thus other smart contracts cannot interact with the off-chain order book, preventing the opportunity to build other structured products on top of the perpetual contract.

MCDEX perpetual contract solves the above problem by introducing an automated market maker, or AMM, which

can be regarded as a smart contract that provides market-making services according to a preset market maker strategy. Both long and short traders can acquire positions by trading against the AMM. The pricing formula of AMM provides a continuous depth for market-making and adjusts the price according to market demand. Hence, the price of the AMM is the natural "fair price". We use the AMM fair price into the above formulas and get a reasonable Mark Price and Funding Rate. This design allows the calculation of funding rates for MCDEX done fully on-chain. On the other hand, other smart contracts can obtain perpetual positions by trading against the AMM, thus offering the possibility to build structured products on top of the perpetual contract.

We regard AMM as an important kernel of the MCDEX perpetual contract. However, off-chain order book liquidity is still superior to AMM's liquidity most of the time due to current public blockchain performance. Therefore, we have also introduced an off-chain order book to provide better liquidity. But there is no direct link between the off-chain order book and the AMM, and we do not calculate the funding rate from the order book. The demand for trades in the off-chain order book is passed on to the AMM through the arbitrageurs, thereby changing the fair price of the AMM and indirectly affecting the funding rate.

More technical details on the MCDEX perpetual contract funding rate calculation can be found in [1][7].

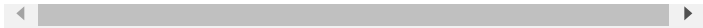
2.2 Contract Rules

The MCDEX perpetual contract has similar rules to the perpetual contracts in CeFi space:

When a trader and his counterparty enter a contract long or short position at a certain entry price, the trader's margin balance must be larger than the initial margin (IM=10%). When the margin balance falls below the maintenance margin (MM=7.5%), the system will liquidate part of the position to ensure the margin balance is larger than the maintenance margin.

The P&L (Profit and Loss) and margin are calculated as follows:

```
Long P&L = (Mark Price - Entry Price) * Size
Short P&L = (Entry Price - Mark Price) * Size
Initial Margin = Mark Price * Size * IM
Maintenance Margin = Mark Price * Size * MM
```



where Mark Price is determined by the sum of Index and Premium of AMM. A trader can change the effective leverage at any time by depositing or withdrawing margin to or from the margin account. The profit of the MCDEX perpetual position can be withdrawn at any time, i.e. the P&L is always the realized P&L.

A trader can close a position at an exit price. The P&L after the trader closes the position is:

$$\begin{aligned}\text{Long P\&L} &= (\text{Exit Price} - \text{Entry Price}) * \text{Size} \\ \text{Short P\&L} &= (\text{Entry Price} - \text{Exit Price}) * \text{Size}\end{aligned}$$



It is important to note that the prices in the above formula are all denominated in the collateral. For example, for an ETH perpetual contract that uses USDC as collateral, the price is the ETH in USDC Price (the dollar price of ETH). However, MCDEX perpetual contracts can use a variety of tokens as collateral, as such the corresponding prices need to be converted first to be used in the above formula, in the case where the collateral does not match with the denominated unit. For example, the ETH-PERP on MCDEX is a contract using ETH as collateral, denominated in the U.S. dollar price of ETH (also known as "inverse contract"). We need to take the inverse of the dollar-denominated ETH price to get the dollar price in ETH, and then substitute it into the P&L formula above.

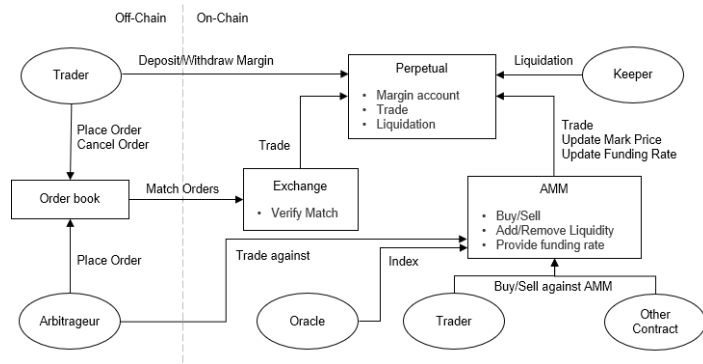
$$\begin{aligned}\text{ETH Long P\&L} &= (1/\text{Entry Price} - 1/\text{Mark Price}) * \\ \text{ETH Short P\&L} &= (1/\text{Mark Price} - 1/\text{Entry Price})\end{aligned}$$



Finally, the MCDEX perpetual contract charge/give interest to all margin accounts with opened positions. This process is continuous as the funding fee is settled on the balances of margin accounts every second.

2.3 Smart Contracts

As shown below, MCDEX's perpetual contract consists of three smart contracts on Ethereum: the Perpetual, the AMM, and the Exchange. The relationships and functions of these three smart contracts are described below:



2.3.1 Perpetual

The perpetual smart contract manages margin accounts, stores data on margin balances, positions, etc, and implements basic functions such as trading, liquidation, funding payment and social loss. A trader can trade via the AMM or the Order Book after opening a margin account by depositing collateral in the smart contract. If the trader has no position, he can withdraw the entire margin balance at any time. But if the trader has a position, the trader can withdraw from the margin account as long as the remaining balance stays over the initial margin (10%). The margin account pays/receives interest at the funding rate on a continuous basis when there is a position in the margin account. When the balance of a margin account falls below the maintenance margin (7.5%), the keeper will liquidate the margin account at the mark price. Accounts that are liquidated are charged with a penalty (2.5%). If the margin account cannot be liquidated in time before bankruptcy, the losses are first covered by the insurance fund. The losses that cannot be covered by the insurance fund will be covered by all counterparties divided by the number of positions held (Socialize the Loss). Anyone can call the liquidation interface to become a keeper, and more keepers will improve the system's liquidation capabilities.

2.3.2 AMM

The AMM is the core of the MCDEX Perpetual Contract for it provides an on-chain funding rate, and an on-chain trading interface. Like a regular trader, the AMM has its own margin account in the Perpetual smart contract. The AMM gets the index price from the oracle to calculate the Premium Rate (the gap between the index price and the Fair Price), the Funding Rate and the Mark Price. Additionally, traders can provide liquidity to the AMM and in return receive transaction fees. Anyone can become a liquidity provider and participate in increasing the AMM's liquidity. A regular trader or a smart contract can also trade (long or short) with the AMM at the price returned by its pricing formula.

The current AMM uses the classical constant product ($xy=k$) pricing formula [2], which has been fully validated in projects such as Uniswap. We believe this choice is a good place for us to get started. When applying this pricing formula, we first limit the AMM's margin account to only hold long positions that are fully collateralized, to ensure that the AMM's account can never be liquidated. The AMM's margin account is always safe. Secondly, we substitute the available margin balance of the AMM for x and the number of long positions in the AMM account for y . When a trader goes long through AMM, the trader's long position increases, while the number of long positions in the AMM (y) decreases, and the available margin balance (x) increases. Conversely, when a trader goes short via AMM, the trader's short position increases and the AMM's number of longs (y) increases, and the available margin balance (x) decreases. In this way, the pricing formula provides the price to trade against the AMM. The x/y is also used as the "FairPrice" of AMM. More technical details on the constant product pricing formula of MCDEX perpetual contracts can be found in [7].

However, the drawbacks of the constant product pricing formula are also evident: low capital efficiency and high slippage. The MCDEX community is actively exploring better pricing formulas that are better suited for perpetual contracts. The community has proposed an AMM pricing formula that is based on the Oracle and risk exposure. The new formula would use the oracle for rapid market price discovery to reduce potential arbitrages. This new formula would adjust prices based on the risk exposure of AMM, encouraging AMM to return to risk neutrality while improving capital efficiency. Specific details and discussions of the new formula can be found in [3]. When we have fully verified the feasibility of the new formula, we will upgrade the AMM pricing formula accordingly.

At last, the relationship between AMM and the order book (see 2.3.3) is noteworthy. There is no direct link between the order book and the AMM, nor do we calculate the funding rate from the order book. Due to the presence of an arbitrageur, the demand for trades in the order book is passed on to the AMM, which changes the fair price of the AMM, and thus indirectly affects the overall funding rate. In other words, the AMM funding rate adjusts the overall market supply and demand, including the on-chain AMM and off-chain order book, so that the trading price anchors the index price.

2.3.3 Exchange

The Exchange contract is the trading interface for the off-chain order book. The order book is currently the most important liquidity portal for MCDEX perpetual contracts. First, a trader submits orders to the order book, and the orders are matched with other orders on the order book. Then, the order book server calls the Exchange contract's interface to submit the match results. The order signature and the match result are checked by the Exchange smart contract on-chain, and once the check is successful, the exchange contract calls the perpetual contract to complete the transaction.

The AMM and the Order Book have different use cases. Since the off-chain order book currently has better liquidity than the AMM, we recommend that traders directly use the order book, and use the AMM as an on-chain liquidity for smart contracts. For example, our upcoming on-chain trading robot provides trading strategies and trades directly with the AMM.

Lastly, exchange contracts have a delegate feature where each perpetual contract account can designate another one to be its delegate. The delegate may place orders using the principal's account, but cannot withdraw assets from it. This feature enhances the account's security. For example, a user can create a margin account with a cold wallet and set up another hot wallet as a delegate, then place orders using the hot wallet. Additionally, the delegate function extends the scenarios of MCDEX perpetual contracts, and we will develop a "social fund" based on this functionality. (see chapter 3)

2.3.4 Oracle

The oracle contract provides the index price of the perpetual contract's underlying asset. The current MCDEX perpetual contract uses Chainlink's Oracle, which has a data accuracy of 0.5. Based on our back-testing, this accuracy is sufficiently accurate to meet the current market demand. As the industry evolves, we will continue to use the latest Oracle technology to improve the quality and security of our perpetual contracts.

More technical details about the MCDEX perpetual contract can be found in [7].

2.4 Security

Security is always a top priority for MCDEX. Decentralized perpetual contracts are relatively complex, and require comprehensive measures to safeguard against potential

harm or issues. Our main focus is to work on security measures, including software security, global settlement mechanisms, oracle security, risks assessment.

2.4.1 Code security

As a DeFi product based on smart contracts, the security of the contracts' code is key to the entire ecosystem. We always consider security as our top priority, by using mature and robust technology. We have fully tested the MCDEX perpetual contract code and achieved 100% test coverage for all possible code branches that could be run.

As well, MCDEX has partnered with the industry's best security teams and entrusted them with the task of performing a comprehensive review of MCDEX's smart contracts via security audits:

- MCDEX Mai Protocol V1 smart Contracts based on Market Protocol are audited by Chain Security (Chain Security also did the audit for Market Protocol)[5].
- MCDEX Mai Protocol V2, which is for perpetual contracts, are audited by Open Zeppelin and Consensys, respectively[6].

MCDEX's future upgrades and new products will continue to commit code audits from the industry's best security teams.

2.4.2 Admin privileges

When we were building MCDEX, we strived to have no admin key. However, due to the complexity of the perpetual contracts, there is still an admin key in the perpetual smart contracts. After MCB tokens((see Chapter 4) are issued, we will transfer the admin privileges to the on-chain voting contract, and all the holders can use MCB to vote. In addition to the admin key, there are two other administrative privileges in the perpetual contract:

- Suspend/resume withdrawal
- Suspend/resume contract functions

Both of the two privileges require authorization from the admin key holder. These two privileges are mainly used for risk control (see 2.4.5)

See [7] for a detailed list of perpetual contract admin privileges.

2.4.3 Global settlement mechanisms

In extreme situations, a global settlement of the perpetual contract can be triggered. A global settlement is the last line of security mechanism to defend against large penetrations due to extreme market volatility and other issues caused by security attacks. The global settlement is a two-stage process. In the first stage, if the system data is maliciously corrupted (e.g. wrong index price), the wrong data can be forced to be corrected and accounts with insufficient margin will also be liquidated at this stage. In the second stage, traders can claim the remaining margin in their accounts at the price when the global settlement was initiated.

The global settlement requires admin privilege, which are currently held by the development team, to initiate and execute. After the admin privileges are transferred to the voting contract, the platform token(MCB) holders will be able to vote on when to initiate a global settlement.

2.4.4 Oracle Security

The overall mechanism of the perpetual contract depends on the oracle's correctness. A wrong index price can seriously undermine the correctness of the perpetual contract, and inflict damages upon traders. To this end, MCDEX is introducing multiple check mechanisms to avoid the potential risks of a single oracle. We will be utilizing Coinbase and MarkerDao's oracles as alternate oracles. When the delta between the Chainlink's price index and the alternate oracles exceeds the threshold (5%), Chainlink's data will be prevented from updating the MCDEX perpetual contract, and the trading function will be automatically suspended. At the same time, it will also trigger the off-chain risk control mechanism. If the situation is serious, we will initiate a global settlement mechanism to force the settlement of the contracts to protect the traders' assets. Enhancing oracle security is not a quick fix, and as oracle technology in the industry continues to develop, we will also continue to update our oracles in order to maximize contract security through a decentralized governance approach.

2.4.5 Risk Control

The logic of MCDEX perpetual contracts is relatively complex and the risk challenges are relatively high. We use both on-chain and off-chain methods for risk control to maximize the safety of our users' assets.

On-chain risk control is a completely decentralized and automated risk control mechanism implemented through smart contracts. On-chain risk control programs are

implemented in smart contracts and deployed by the administrator, who permits the program to "suspend contractual functions". When an on-chain risk policy is triggered, the on-chain risk control program can suspend the entire contract. After this, the administrator can take further action on a case-by-case basis, such as initiating a global settlement or restoring contract functionality. However, limited by the capabilities of smart contracts, there is currently only a simple risk control strategy on-chain: stop the contract when the size of the social loss reaches a certain threshold.

Additionally, we have also set up a risk control mechanism that automatically initiates and executes off-chain monitoring programs. The advantage of off-chain risk control is that a variety of complex risk control strategies can be implemented. The disadvantage is that this risk control approach is relatively more centralized. We minimize off-chain risk control privileges and only authorize off-chain risk control procedures to "suspend withdrawal privilege". When the off-chain risk control is triggered, the risk program sends an alarm and suspends the withdrawal function of the contract, while deposits, transactions, and other functionalities are unaffected. The administrator may then intervene for further investigation, and if the situation requires it, the administrator can also trigger a global settlement process. In a global settlement process, administrators can fix the erroneous data in contracts, thereby maximizing the security of users' assets.

The main data monitored by the off-chain monitoring program are:

- Status of assets in the contract
- Oracle Data Correctness
- Margin pledge ratio and settlement
- Trades in the contracts

As with on-chain risk control, we will open source all the off-chain risk control mechanisms. As MCDEX's community continues to grow, we will involve more empowered experienced and capable teams to work with us on off-chain risk control.

3. Structured Products

Perpetual contracts are the base assets of MCDEX, and are completely permissionless. As the AMM provides the on-chain liquidity interface, apps and services can be built

using the AMM to expand the usage of our perpetual contracts and thereby increasing market liquidity.

As the financial architecture of our perpetual contract is well suited for hedging and has a wide range of applications, we will integrate our perpetual contract with other products and services in the DeFi space.

To significantly lower the investment threshold for users who lack the ability to trade perpetual contracts but want to invest in DeFi, we are building a structured fund based on our perpetual contracts. This product comes in two forms: a robot fund and a social fund.

3.1 Robot Fund

A Robot fund is an open-source, cost-free smart contract that automatically trades our perpetual contract without taking any commission for trading.

The Robot Fund can be viewed as a regular trader but with a separate margin account whose trading strategy is fully disclosed on the chain. The Fund automatically executes the trades based on market data (e.g. index prices) to provide target positions, it indicates the maximum slippage relative to the mark price allowing anyone to call its interface to trade with the AMM thereby acquiring the target positions. To make profits, the arbitrageur will call the robot's interface to make the robot trade against the AMM. This way, the robot's position is always in line with its trading strategy.

Anyone can deposit funds into the Robot Fund's smart contract to earn a share of the fund. Users can opt-out of fund shares after a minimum holding period has passed. When a user exits the fund, the position attributed to the user gets closed.

3.2 Leveraged Tokens

Leveraged tokens are a popular kind of investment asset for regular traders. The effective leverage of a perpetual contract varies with the profit and loss of the position. It decreases when the position is profitable and increases when the position is in a loss. For users to obtain fixed leverage, the positions must be balanced. Leveraged tokens are based on perpetual contracts and provide constant leverage, such as 3x long ETH or 3x short ETH. In CeFi, the fund manager constantly rebalances the fund's position thereby locking the effective leverage at a fixed

value. The share tokens issued for such funds are leverage tokens.

Leveraged tokens can be easily implemented based on automated trading robots. We can deploy a Robot Fund whose strategy is fixed effective leverage. And the share tokens of the fund are exactly the decentralized leveraged tokens. This kind of leverage tokens provide greater security over centralized products, making it a great asset class.

3.3 Social Fund

A Social Fund is an investment fund that resembles the traditional GP/LP (General Partner/Limited Partner) structure. The Social Trader acts as a General Partner and is responsible for the development and execution of the fund's trading strategy. Investors can invest in the fund to become Limited Partners of the fund. When the fund achieves profitability, the General Partner takes a percentage of the profits.

Similar to the Robo Fund, every Social Fund has a separate perpetual contract account. Users can invest in the fund to get an equivalent amount of shares and exit the fund at any time. Unlike Robo Funds, Social Funds are managed by Social Traders, who are the delegates of the fund account (see section 2.3.3). They develop and execute their own trading strategies by placing orders via the order book through the platform's user interface as well as the API. The Social Traders cannot withdraw user's funds from the Social Fund's account except for the dividends on achieving profitability.

It's easier for trading firms and teams to become Social Traders as they are familiar with the API. Here's why this concept is a win-win for Social Traders and Investors: Social Traders will focus on their trades instead of spending their energy on dealing with the otherwise tedious processes of LP deposits, withdrawals, dividends, and other issues. Investors will only focus on the returns without having to worry about the misappropriation of funds. Hence, the Social Fund will be a useful platform connecting Investors and Social Traders.

3.4 Liquidity Mining

We will use part of the MCB(see Chapter 4) token distribution to incentivize users to invest in the funds, leading to the platform liquidity increment. When users

deposit assets in the fund, they become fundholders and receive MCB tokens, which is called Liquidity Mining. The total amount of MCB mined every day is fixed, and MCB tokens are distributed to the funds based on their net asset value. The better the performance of the fund, and the faster the net asset value growth, which encourages users to mine in funds with better performance. Besides, social traders will get MCB from their funds' mining reward.

3.5 More Application Scenarios

We will take feedback from the community and work with them to create more structured products based on perpetual contracts to meet the needs of users with different risk preferences. For example, people can design a structured product having two layers: the bottom layer and the top layer. The bottom layer is a priority layer with a safety cushion for users with low-risk preference aimed at smaller returns. The upper layer is a high-risk layer without a safety cushion for users with high-risk preference aimed at bigger returns.

4. Governance and MCB

As we develop the various products on the MCDEX platform, we want to ensure that our products, once deployed, require no governance or tweaking; like the MCDEX V1 - Mai Protocol used for trading Market Protocol contracts. However, a relatively complex product like perpetual contracts has a lot of governance involved which includes:

- Modification of contract parameters: commission rate, initial/maintenance margin rate, liquidation penalty rate, etc.
- Approval of contract upgrades.
- Authorization of on-chain and off-chain risk control.
- Launching a global settlement.

We will issue the MCB token which will enable decentralized governance and hence pave the way for a fully decentralized DeFi platform. The MCB token will have the following features:

- Governance: MCB will be the governance token of the MCDEX Platform. The governance rights of our platform will be owned by MCB holders which can be exercised by voting.

- Value Capture: 100% of the MCDEX order book transaction fee and 20% of the AMM transaction fee (the remaining 80% will go to liquidity providers) will be used to buy MCB and redeem.
- Providing AMM liquidity: We will gradually upgrade the AMM and use MCB as logical collateral for the AMM, enabling the MCB to provide liquidity.
- Taking the risk of liquidation and enjoying its benefits: We will upgrade the system for the holders of MCB to act as liquidators and take all the liquidation risk. Meanwhile, we will also use all the liquidation penalties to purchase and redeem the MCB token, thereby allowing the MCB to capture the value of liquidations.

Features 2-4 rely heavily on the liquidity of the MCB. The last two functions, in particular, operate successfully on the premise that MCB has a good value base and liquidity. It is why we have chosen to add those features gradually. We hope that with the development of the MCDEX, we will gradually add MCB features as the liquidity of MCB grows along with the network.

The total supply of MCB tokens is 100,000,000, distributed as follows:

- 25% to the founding team and early investors. 2.25% has a 2-year linear vesting period and 22.75% has a 4-year linear vesting period.
- 25% to the MCDEX Foundation for token sales to cover expenses such as development, audits, market making, marketing, etc..
- 50% to user incentives with a limit of up to 5% per year.

(On September 1st, 2020, team vesting will suspend for 6 months - lock up for 6 months. On March 1st, 2020, team vesting will be resumed.)

As the platform continues to grow and evolve, new products will be launched on an ongoing basis which will bring different sets of users with different motivations. Going forward, there will be many types of user incentives for takers, liquidity providers, contributors of open-source trading strategies, social traders, holders of structured products, DeFi developers, and other stakeholders of the MCDEX ecosystem. The community will actively propose the incentives but the approval will be done by voting (by MCB holders).

MCB Contract Address:

0x4e352cf164e64adcbad318c3a1e222e9eba4ce42

5. Road map

- Q2 2020
 - Launch of the perpetual contract
- Q3 2020
 - Launch automated trading and social trading products
 - Initial MCB token sale
 - Liquidity mining
- Q4 2020
 - New AMM formula for perpetual contracts
 - Decentralized leveraged tokens
 - MCB for AMM liquidity incentive
 - MCB for on-chain governance
 - MCB capturing platform fees
 - Decentralized leveraged tokens
 - IDO (Initial DEX Offering)
- 2021
 - Enhancement of MCB
 - Use of MCB to provide liquidity for AMM
 - Use of MCB to cover social losses
 - Use of MCB to capture liquidation penalties
 - Introducing an optimistic rollup mechanism to improve trading performance.
 - Introducing more types of financial assets to the MCDEX platform.

References

[1] Perpetual Reference.

[2] Y. Zhang, X. Chen, and D. Park, "Formal specification of constant product ($xy=k$) market maker model and implementation," 2018.

[3] M. Lei and T. Zhu, MIP2: Proposal: A New Perpetual AMM Pricing Formula With High Capital Efficiency.

[4] Perpetual Technical Guide.

[5] CHAINSECURITY, Security Audit of Mai Protocol Smart Contracts.

[6] OPENZEPPELIN SECURITY, MCDEX Mai Protocol Audit.

[7] MCDEX documents.