Mai Protocol v3:

Permissionless Perpetual Swap Protocol based on an advanced AMM

1. Introduction

Mai Protocol V3 designed by MCDEX is an AMM-based decentralized perpetual swap protocol. Perpetual swap is one of the most popular derivatives that has no expiration date, supports margin trading, and has its price soft pegged to index price.

The goal of this protocol is to allow anyone to create and trade in any perpetual market. To start with, anyone can create their own perpetual market with the price feed of underlying asset and choose any ERC20 as collateral. Secondly, we have designed an AMM for the perpetual market and this AMM also has better capital efficiency. Moreover, AMM solves the liquidity problem - anyone can provide liquidity to AMM by depositing assets in the pool and get reasonable market making profit. At last, anyone can trade perpetual swaps permissionlessly. Traders' assets are in the smart contract in a noncustodial way and the process of trading are conducted on chain completely.

The smart contract of the protocol has been strictly audited by a third party, and there is no admin key of the protocol, maximizing the decentralization and security of this protocol.

We believe that permissionless is the key feature of this protocol, which can empower the whole community to contribute to the MCDEX ecosystem - anyone can create the perpetual market of an on-chain or off-chain synthetic assets. With the evolvement of MCDEX community, more diversified perpetual market will be created, and trading volume will be generated.

2. Perpetual Swaps

2.1. Market Participants

This protocol is completely based on AMM. Please refer to the MAI v3 AMM Design document for detailed information regarding AMM.

There are following roles in the market:

a) AMM: AMM plays the role of a central counterparty, providing liquidity for the perpetual swap. Like a normal trader, AMM has its independent margin account, and is able to hold positions.

b) Operator: An operator is the creator and manager of the perpetual swap.

How to become an Operator:

i. Create a perpetual swap and set the initial parameters (such as margin rate, AMM risk parameters, etc.). The AMM of perpetual swap has a set of risk parameters. By adjusting these parameters, an operator is able to change AMM' s market making risk, market depth, slippage, and spread etc.

ii. Pay for (or provide) Oracle service. The protocol defines an Oracle interface so that the currently available Oracles can be applied in this protocol. An operator can provide their own Oracle data to perpetual swaps as well.

iii. An operator can set a range of the risk parameters and adjust the risk parameters within this range.

iv. The operator can initiate the governance process to change the range of the risk parameters. (see 2.9 AMM parameters and governance)

v. Operator can transfer his role to other addresses and opt out their operator role. The perpetual market without an operator will be governed by LP.

Benefits:

i. profit from every trade by charging management fee set by themselves.

ii. incentives which are distributed to some potential pools that have good performances

iii. initiate AMM governance proposal

Risks: Not applicable

c) Liquidity provider:

How to become a LP:

i. deposit collateral in the AMM pool

Benefits:

i. Trading fee at a fixed ratio
ii. Profit from spread and slippage
iii. Funding payment paid by trader
iv. Liquidation penalty
v. Incentive distributed to some potential AMM pools (see section 3.2 tokenomics)
vi. LP can participate in AMM governance (see section 2.10 The Parameters and Governance of AMM).

Risks: When AMM has position, there is a risk exposure. If the index price changes at this moment, there could be a loss on AMM. This loss will be shared by all LP.

d) Trader: Traders are the major participants in the market. Traders realize PNL by trading against AMM and they are always the taker. In this protocol, all trades must go through AMM, and traders can’ t bypass AMM to trade amongst themselves. For every trade, traders need to pay a certain amount of transaction fee. In addition, trader will pay or receive funding payment according to the funding rate policy.

e) Keeper： Keeper is an auxiliary role. Anyone can be a keeper to liquidate accounts with insufficient margin (see section 2.4 liquidation).

f) Delegator: A delegator is a special role. There could be a delegator for every margin account. A delegator can operate over the account to trade (directly against AMM or through a broker), but they can’ t withdraw fund from the account. The goal of delegator is to separate hot and cold wallets and realize the custody of trading strategies.

2.2. Funding Payment

Similar with the traditional perpetual swap, this protocol utilizes funding payment to anchor the index price.

Since all trades must go through AMM, the market reaches balance when AMM doesn’ t have any position. At this point AMM will provide the best bid and the best ask price around the index, then the current market price is close to the index.

The AMM price shifts according to its position. When AMM longs, the AMM price will be lower than the index price, and vice versa when AMM shorts. In other word, the market is out of balance at this point, so the market price will shift relative to the index. In this case, the protocol will charge funding payment from the positions opposite to AMM and the traders with the same position of AMM will also receive the funding payment. AMM always receives funding payment as long as it holds positions. The funding rate is positively correlated with AMM’ s position size, i.e. the more position AMM holds, the further away the market price deviates, causing a higher funding payment.

On one hand, funding payment can prevent more traders from becoming the counterparty of AMM, which could lead to a further price deviation. On the other hand, a high funding rate will attract more LP to add liquidity or open the same position with AMM. Based on the AMM design, both adding liquidity to AMM and trading against AMM which reduces the AMM’ s position size will decrease price deviation. In such a way, funding payment will push the market price back to the index.

2.3. Margin & PNL

Due to the permissionless nature of this protocol, anyone can create any perpetual swaps of different risk levels. To prevent the spread of risk across different perpetual swaps, the protocol uses isolated margin mechanism - each perpetual swap owned by a trader has its own independent margin account, and the PNL of this account won’ t affect other margin accounts they trade.

When a trader enters long or short position of ΔN contracts at a certain entry price P_{entry}, $\Delta N > 0$ indicates that the trader longs, $\Delta N < 0$ indicates that the trader shorts.

When opening position, the margin balance of the trader' s margin account must be larger than or equal to the Initial Margin:

$$P_{mark}|\Delta N|R_{im}$$

P_{mark} is the mark price provided by Oracle. P_{mark} is usually equal to the index price P_{index} or is a TWAP result of P_{index} when using some decentralized Oracle like Uniswap. $M_{im}$is the Initial Margin Rate of the perpetual contract.

The PNL (Profit and Loss) of the position is calculated as follows:

$$\left(P_{mark} - P_{entry}\right)\Delta N$$

The profit of the MCDEX perpetual position can be withdrawn at any time, i.e. "PNL" always refers to its realized state. And the position loss is deducted from the margin balance in real time.

Trader can close position at an exit price P_{exit}. The PNL after the trader closes the position is:

$$(P_{exit} - P_{entry})\Delta N$$

The trader must ensure that the margin balance of the margin account always be larger than or equal to the Maintenance Margin:

$$P_{mark}\Delta N M_{mm}$$

If the maintenance margin requirement cannot be met, the position will be liquidated.

In the end, every perpetual swap has a "Keeper Gas Reward" parameter. When the position is liquidated, the keeper will receive a set amount of reward to pay for Gas. Therefore, our protocol requires that, as long as the position size of margin account is bigger than 0 (disregarding the position value), the margin balance has to be sufficient for the “Keeper Gas Reward”. Otherwise, the position will be liquidated.

2.4. Liquidation

When the margin balance is less than the maintenance margin, the position will be liquidated. The keeper initiates liquidation against positions with insufficient margin. Anyone could act as a keeper. There are two ways of liquidation:

Liquidation through AMM: Liquidated position will be closed through AMM, meaning that this position is transferred to AMM. Liquidation penalty also goes to AMM’s liquidity pool. The keeper will receive a certain amount of “Keeper Gas Reward”.

Taken over by Keeper: The liquidated position will be transferred to keeper. In this case, the keeper takes the position risk and receives the liquidation penalty.

2.5. Settlement

Although it is a perpetual swap, there could be a liquidity deficiency in extreme situations. If there is a liquidation loss due to AMM liquidity deficiency or delayed liquidation, the insurance fund in AMM will prioritize making up the liquidation loss. If the AMM insurance fund is insufficient, the contract will enter settlement stage. The perpetual swap will settle at the latest index price, and the remaining asset will be distributed to traders according their margin balance. i.e. The liquidation loss is undertaken by all position-holding traders based on their margin balance. For those who doesn’t have any position, they will not be charged with any liquidation loss. We believe that under extreme circumstances, entering settlement promptly and allowing traders to withdraw margin will protect all sides. This mechanism is a form of circuit breaker.

Besides, when Oracle does not provide updates for over 24 hours, the contract will also enter settlement.

There are two stages of settlement. The first one is called "Emergency", in which the Oracle stops updating. At this point, keepers will review all the margin accounts and obtain "Keeper Gas Reward". During the review, the margin balance will be calculated based on the settlement price. When the review is completed, settlement enters a second stage called "Cleared". Traders can then withdraw the remaining margin.

2.6. Insurance Fund

Every perpetual swap comes with one insurance fund to pay for liquidation loss:

Anyone can donate to the insurance fund. We encourage operators to donate to the initial capital and supplement the insurance fund as the contract runs.

When trader's position gets liquidated due to insufficient margin, a certain ratio (based on the AMM parameters) of the charged liquidation penalty goes to the insurance fund. The remaining part goes to the liquidator (AMM or keeper). Every insurance fund has a max fund size. When this maximum size is reached, the newly added fund goes into the liquidity pool of AMM. LP can increase this upper limit through governance, but it can't be decreased.

2.7. Limit & Stop Orders

Trading against AMM is similar to place a market order to the traditional order book. In the case of perpetual swaps, people are usually inclined to look for opportunities and control fill price through limit orders. Besides, Stop order is an important tool for high leveraged trades. Hence, we designed relatively centralized limit and stop orders. The trader can sign a limit or a stop order and send the order to an entrusted "Broker" server. The Broker sever will observe the AMM price on the chain and submit order to the contract when the AMM price meets the order's requirement. When the smart contract receives order from Broker, it will proceed the order after verifying its validity.

Keep in mind that Broker wouldn't match the received orders, so all the orders will be traded against AMM in the first-in-first-service order. Broker will charge traders with the Gas fee.

2.8. Security

We fully understand that security is the key factor of this type of protocols. Before getting published, all contracts and upgrades will go through strict audit. The design of AMM’ s financial structure will be verified as well.

To maximize the decentralized characteristic of this protocol, there is no admin key in the code.

Although operators have limited privileges over the perpetual swaps, which to an extent increase the security, traders need to carefully choose the perpetual swaps they would like to trade and trade at their own risk. We encourage operators to choose decentralized Oracles and limit the risk parameters in a smaller range (or set fixed parameters), so that the credibility can be increased.

2.9. Referral

Referral fee is supported in this protocol. The referrer will receive a certain amount of referral fee from the operator fee and LP fee when their referee trades against AMM or through a broker. The ratio of this referral fee will be set by AMM governance. In such way, institutional investors can profit from referring traders to AMM by running their own frontend.

2.10. The Parameters and Governance of AMM

The AMM parameters have two categories: the alterable ones and the unalterable ones. Operator and LP can adjust alterable parameters by voting. AMM has a group of risk parameters, and each has an effective range. According to the market, operator can freely adjust the risk parameters within the effective range. A voting procedure is required if there is a need to change the range.

An operator can initiate a proposal. If there is no operator in the perpetual swap, LP with a more than 1% share can also initiate the proposal. Each proposal will proceed by vote among LP who owns LP token before the proposal was initiated. The vote quorum must be more than 10% of the total LP share. The voting period lasts 72 hours, and the resolution can become effective after a 24-hour time lock. When voting, LP needs to stake their LP token. If the proposal passes, then the LP token that voted yes will be unlocked after 72 hours since the execution of the proposal; the LP token that voted no will be unlocked immediately. If the proposal fails, then all LP token will be unlocked right after the voting period. When an LP initiates a proposal, the system will automatically record their vote as "yes" and lock their LP token.

AMM Parameters	Definition	Alterable/Unalterable
Underlying Asset	A string that identifies the underlying asset	Unalterable
Collateral Token Address	Collateral ERC20 token address	Unalterable
Operator Address	Operator's address	Alterable by Operator
Oracle Adapter Address	Address of adapter compatible for Mai3 Oracle	Unalterable
Initial Margin Rate	Determines the max leverage when open position	Alterable by LP Governance (only decrements are allowed)
Maintenance Margin Rate	Determines the leverage when position is liquidated; Smaller than the initial margin rate	Alterable by LP Governance (only decrements are allowed)
Vault Fee	The rate of trading fee that enters the DAO Vault	Alterable by MCDEX DAO Governance
Operator Fee	The rate of trading fee that goes to operator; Less than 1%	Alterable by LP Governance
LP Fee	The rate of trading fee that goes to LP; Less than 1%	Alterable by LP Governance

Referral Fee	The rate of referral fee from the Operator Fee and LP Fee	Alterable by LP Governance
Liquidation Penalty Rate	The rate of liquidation penalty. Liquidation Penalty=Position Value* Liquidation Penalty; Smaller than the maintenance margin rate	Alterable by LP Governance
Insurance Fund Rate	The ratio of penalty that goes to the insurance fund	Alterable by LP Governance
Insurance Fund Max	The upper limit of the insurance fund	Alterable by LP Governance (only increments are allowed)
Keeper Gas Reward	When keeper executes liquidation or reviews accounts during settlement, they receive a fixed amount of reward to pay for Gas.	Alterable by LP Governance
AMM Risk Parameters	A set of parameters that helps with the risk management of AMM as the market maker	The Effective Range is Alterable by Governance, and Operator Adjusts within Range.

Please pay attention to the fact that all the risk parameters are effective within a designated range. Operators can adjust the parameters within this range without going through the governance procedures. In such way, LP can authorize the operator adjust the risk parameters according to the market, which is significant at an early stage. After the protocol has been running for a while and the risk parameters gradually stabilize, LP can cut the effective range of the risk parameters through governance (or even fix the parameters) to further strengthen AMM’ s decentralized characteristic.

In addition to the proposals for revising AMM parameters, there are three special proposals that requires a vote quorum no less than 20% of the total LP share.

i. Upgrade the code of AMM smart contract
ii. Make a perpetual swap enter settlement stage
iii. Appoint an operator. LP can initiate this proposal only when there is no operator.

2.11. Multi-chain deployment

MCDEX believes that various public chains have their own users and ecosystems. This protocol stays neutral when choosing public chains. In order to maximize our usability, the smart contracts of this protocol are able to run on various public chains. MCDEX DAO will support the development of this protocol on these public chains, growing the MCDEX ecosystem.

3. MCDEX DAO

3.1 Governance

The MCDEX community has issued its governance token MCB and has done a series of governance work. While launching the Mai3 protocol, we will establish MCDEX DAO based on MCB. MCDEX DAO will be the core of the MCDEX community. The mission of MCDAO is to continuously develop the MCDEX ecosystem.

MCDEX DAO has vault. The asset in this vault comes from:

i. Share from the fee captured by MCDEX ecosystem
ii. Newly issued MCB in the MCB tokenomics
iii. Other payments made to MCDEX DAO

The asset in the vault is used to assist the MCDEX DAO mission. Its specific usage includes but not limited to:

i. Liquidity incentive: Incentives for LP of AMM

ii. Governance incentive: Incentives for MCB holders who participate in community governance

iii. Development incentive: Incentives for community starters and community managers

iv. Audit fee and other required fee

v. Add liquidity to products in the MCDEX ecosystem

vi. Buyback MCB from the secondary market. The MCB will be part of the vault asset

vii. Provide liquidity for MCB (in the MCB liquidity pool on Uniswap)

MCB holders have the governance right of MCDEX DAO. MCDEX DAO applies the "Off-chain discussion, On-chain governance" method. Since the governance is on the chain, every proposal is essentially an executable smart contract. MCDEX DAO should provide a smart contract factory for the ease of initiating proposals.

The MCDEX DAO governance includes:

i. Managing the specific usage of the vault asset;

ii. Running numerous perpetual swaps as operator;

iii. Electing a multi-signature address when necessary. This multi-signature address will complete the routine work representing MCDEX DAO as an operator;

iv. Upgrading MCDEX DAO smart contract

The MCDEX governance proposal needs to be initiated by MCB holders, and the initiator's MCB voting power has to be no less than 1% of the issued total. The voting quorum has to be no less than 10% of the issued total. The proposal initiator is set to vote yes.

A MCB holder can delegate the voting power to another holder.

The voting period lasts 72 hours, and there is a time lock of 48 hours. Participants need to stake MCB. If the proposal passes, the MCB that voted yes will be unlocked after 72 hours since the execution of this proposal, and the MCB that voted no will be unlocked immediately when the voting period terminates. If the proposal fails, all staked MCB will be unlocked immediately when the voting period terminates.

3.2 Tokenomics

The original MCB tokenomics has room for improvement: The rapidly increasing inflation has been overwhelming for MCB holders. Therefore, we will openly discuss the upgraded MCB tokenomics with the community before the launching of Mai 3. The tokenomics include issue size, issue object, and issue speed.

The principles of the new tokenomics as follows:

i. The issued MCB keeps circulating.

ii. MCB has to be captured from the MCDEX ecosystem

iii. Due to the significance of liquidity in derivatives, we still need to issue more MCB as liquidity incentives.

iv. The new tokenomics has to take into account the profit of current MCB holders.