Kommodo: a primitive lending protocol

Kevin Foesenek
kevin@kommodo.org
www.kommodo.org

Abstract. A primitives based fully collateralized lending protocol allows financial parties to lend and borrow assets without the trust of a central party. Blockchains provide part of the solution, but the main benefits are lost if a trusted third party is still required to determine the price between assets. We propose a solution to the pricing problem by requiring concentrated liquidity positions for liquidity and collateral. The use of concentrated liquidity positions can guarantee that the value of the collateral position will always be higher or equal to the borrowed position, removing the need for trusted third parties or liquidation games.

1. Introduction

Lening and borrowing is a large part of the trust based financial system. Within the decentralized finance space there is active research to integrate lending and borrowing without requiring trust. The current decentralized finance based lending protocol implementations require trust in an oracle. Recently there have been made developments that do not require trusting an oracle, however these systems use liquidation games, are complex and require active participation to avoid liquidation. In this paper Kommodo is presented, a novel lending protocol that allows lending and borrowing between any token pair with minimal complexity and without the trust of oracles or liquidation games.

2. Lending protocols

Lending protocols allow depositing funds and receiving a yield in return. In addition a lending protocol allows to borrow these deposited funds against collateral funds while paying interest for these borrow activities. Pooled lending protocols aggregate deposited funds in a pool to borrow from while peer to peer lending protocols match single lenders and borrowers. Pooling the funds allows for efficient matching between lenders and borrowers.

Permissionless lending protocols have no knowledge of the borrower or option to retrieve the borrowed funds and therefore require full collateralization of the loan. To determine the collateral needed between two assets the permissionless lending protocol requires knowledge of the asset prices.

A change in price can require an increase in collateral. Current implementations of blockchain based lending protocols use oracles to input the price and liquidation games to guarantee sufficient collateral on changing prices. There are lending protocols that do not require trusting an oracle for price input, these protocol determine the price algorithmically based on the total lending pool conditions. These protocols are complex and require liquidation games to guarantee sufficient collateral on changing prices.

3. Automated market makers

Trading is the mechanism for price discovery of an asset. The decentralized finance space implemented automated market makers (AMMs) for efficient blockchain based trading, allowing price discovery between assets referred to as tokens. AMMs are agents that pool liquidity and make it available to traders according to an algorithm [1]. AMMs allow for permissionless trading efficiently matching trades.

Initial iterations of AMMs inefficiently distributed liquidity uniformly along a single curve. Concentrated liquidity positions (CLPs) are AMMs liquidity positions (LPs) with the ability to concentrate the liquidity by “bounding" it within an arbitrary price range [2]. This improves the pool’s capital efficiency and allows LPs to approximate their preferred reserves curve, while still being efficiently aggregated with the rest of the pool. For AMMs with two assets (A and B) the CLPs will return A at a price above the bound price range, B below the bound price range and a mix of A and B within the bound price range.

4. Concentraten liquidity lending

For permissionless lending protocols the collateral value is required to be higher than the borrow value at all times. To comply with this requirement the collateral has to increase when price changes increase the collateral needed. When the collateral asset deposited is the same as the borrowed asset there is no active price change, the price is always equal to 1. On initial requirement of full collateralization this guarantees that the deposited collateral value is always higher than the borrowed value, no future increases in collateral are ever required. However borrowing and lending between the same asset has no real use case.

We propose a protocol for lending and borrowing CLPs as the asset. The use op CLPs allows a combination of trading between two assets while having the value guarantee of using one asset. The only requirement for borrowing a CLP is that the price of the borrow CLP is higher than the price of the collateral CLP:

$b =$ CLP borrow
$c =$ CLP collateral
$P =$ price
$V =$ value

$$Pb > Pc$$

CLPs consist of two assets (A and B). For an equal amount of A the collateral CLP will return equal amount of A or a higher amount of B than the borrow CLP:

$$borrowB = \frac{amountA}{Pb}$$
$$collateralB = \frac{amountA}{Pc}$$

Pb is higher than Pc resulting in a collateral B amount greater than borrow B amount or and equal A amount:

$$collateralB > borrowB$$
$$collateralA = borrowA$$

When described as the value of the CLPs:

$$Vc >= Vb$$

As shown the use of CLPs allows to mathematically guarantee the requirement of a permissionless lending protocols. This beautifully simple guarantee allows for the protocol to be permissionless and require no oracle, governance or liquidation games.

5. Interest

The lender and the borrower each take some risk with the CLP position. If the price rises to above the lenders price there will be impairment loss over holding the deposited token. If the price drops below the borrowers price there will be impairment loss over holding the deposited token. Because of this for a lender it is best to choose a high as possible price for the borrow CLP and for the borrower it is best to choose a low as possible price for the collateral CLP.

The amount available to borrow is higher the lower a CLPs price. So the borrower is incentivized to borrow a CLP as close to the current price as possible while providing a collateral CLP with an as low as possible price. To counter this the interest rate is low when Pc is close to Pb and a high when Pc is far from Pb. The safer the position for the borrower, lower Pc, the more interest the lender receives for giving out this loan.

The loans are guaranteed fully collateralized, closing of the loan will therefore only happen when the borrower closes it or by anyone when no interest is available.

6. Conclusion

We proposed a protocol for lending and borrowing without relying on trust. The protocol requires no external governance, price or other input. This is achieved by using CLPs as assets to provide the guarantee that the amount of collateral is always equal to or more then the amount borrowed. This design incentives borrower to provide collateral with an as low as possible CLP price. To mitigate this incentive interest is proportional to the distance between Pb and Pc. Closing a borrow position can only be done by the borrower or by anyone when no interest is no longer payed.

References

[1] Abraham Othman. 2012. Automated Market Making: Theory and Practice. Ph.D. Dissertation. Carnegie Mellon University.

[2] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer and Dan Robinson. 2021. Uniswap v3 Core. Retrieved Okt 9, 2023 from https://uniswap.org/whitepaper-v3.pdf