Vukašin Gostović
https://rainshower.cloud/
17 May 2022

Rainshower Alpha

Permissionless token borrows for Ethereum and its rollups.

Rainshower is a permissionless protocol that allows users to borrow and lend tokens to speculate and earn yield. To achieve this borrow creators (makers) create a borrow, with their token of choice, and anyone can borrow (take) and short tokens as long it's backed by sufficient collateral. Borrow takers pay the makers an upfront fee for their services. Liquidity risks are minimized by ensuring positions are collateralized and kept above a maintenance margin. If the position is under-collateralized, a liquidation event for the position can be engaged. To ensure that borrows aren't indefinitely held and tokens stuck, all borrows have an expiry date set at borrow creation.

Note: This paper is a draft. While the core mechanics will be similar to release, they are not set in stone and will be changed.

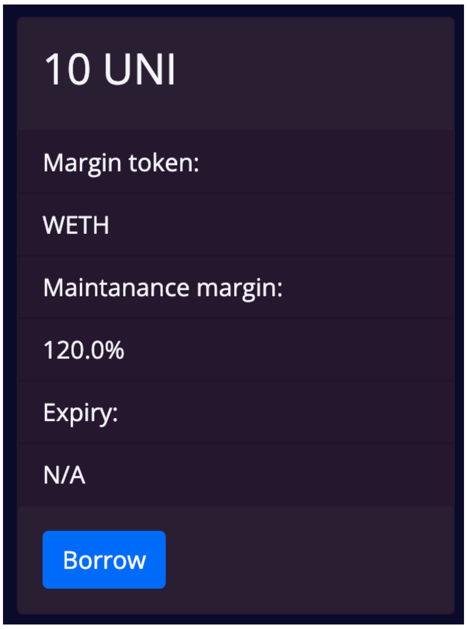
Creating a borrow

Borrows are made by market participants who want to speculate on the price going up. They are rewarded for their market-making services by the takers who pay them interest. Similar to Uniswap liquidity pools, borrow are created by a factory contract. Borrow makers set the initial parameters of the borrow. These parameters include:

- Amount of tokens put up for borrow
- Address of the token being put up for borrow
- Address of the token to be used as margin
- Maintenance margin
- Maker fee (Interest)

- Expiry time
- Uniswap V3 swap router
- Uniswap V3 liquidity pool
- Uniswap V3 TWAP oracle time period
- Uniswap V3 TWAP oracle address

Some of these parameters, like the oracle address, cannot be changed by the maker. These variables are stored in the factory contract and can only be changed by a DAO vote. Once a borrowing contract with the above parameters is created, the borrow maker will need to fund it with tokens being put up for borrow. Once the borrow is funded, it becomes open and can be borrowed by anyone who can fulfill the borrow obligations.



10 UNI

Margin token:

WETH

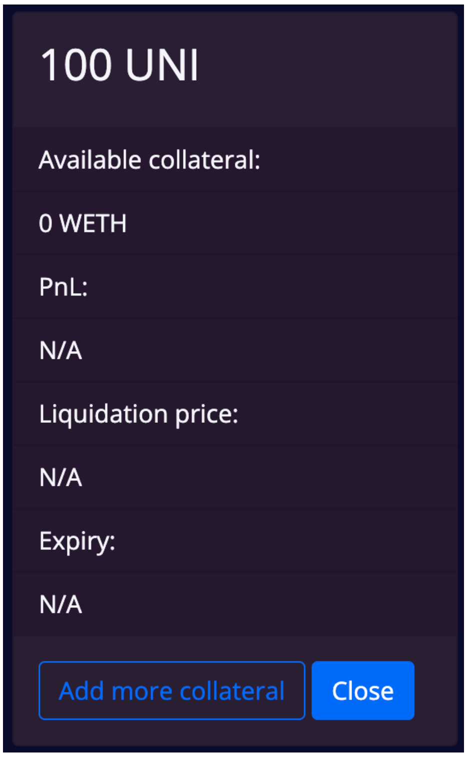
Maintanance margin:

120.0%

Expiry:

N/A

Example of an open borrow



100 UNI

Available collateral:

0 WETH

PnL:

N/A

Liquidation price:

N/A

Expiry:

N/A

Example of an active borrow

Taking a borrow

Borrows are taken by market participants who want to speculate on the price going down. To take a borrow, takers need to ensure that they have enough collateral to cover the maintenance margin and the taker fee. If the taker has enough collateral to cover all the obligations, the margin and the taker fee are transferred to the token contract, and a swap of the borrowed tokens for the margin token is initiated.

First, the market price of the borrowed token denominated in the margin token (also referred to as $baseToken$) is calculated ($baseTokenMinimum$). The oracle used is an on-chain Uniswap V3 TWAP oracle. The period can be adjusted upon borrow creation to strike a balance between price manipulation resistance and convenience.

It is important to note that for illiquid pairs, a higher TWAP period, and maintenance margin, might be required to protect agains manipulation.

The minimal amount of margin needed to open a deposit is:

$$tokensToDeposit = baseTokenMinimum \times maintananceMargin$$

Since liquidations can be triggered when the maintenance margin isn't met, it's recommended to deposit additional collateral upon taking a borrow. After collateral has been deposited,

The borrowed tokens are swapped to the margin token using the Uniswap V3 pool provided upon borrow creation. The maximum slippage for a swap is 1%. If a swap has higher than 1% slippage, the whole function will revert and the process of taking a borrow will need to be repeated.

Closing a position

Borrows are divided into open and active. Open borrows are funded with the token to be borrowed and have not found a counterparty. These borrows can be closed at any time by the maker, or in the case the borrow expired, by anyone. The tokens deposited into these positions are automatically returned to the maker.

Opposite to open borrows, active borrows have found a taker who deposited their collateral. These positions can be closed by the taker at any point before expiry, or in the case the borrow expires by anyone. Takers are incentivized to close their positions before expiry because if an active borrow expires, liquidation can be triggered. All the regular liquidation mechanics apply which means that takers would be giving up a good sum of their collateral if a position expires.

Liquidations

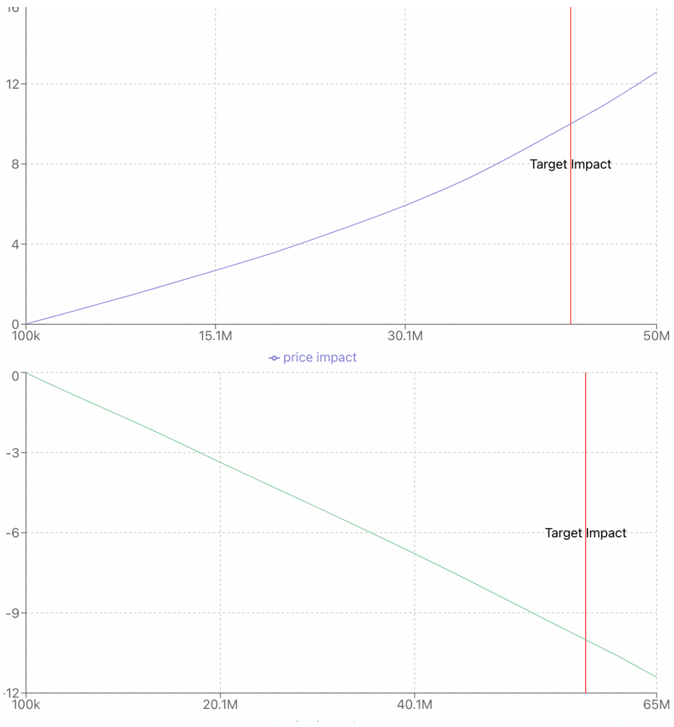
Note: This section is a draft and will be subject to major change before release. Positions cannot be liquidated during the Rainshower Alpha test.

When a position becomes under-collateralised, a liquidation on the position can be triggered. The takers remaining capital is swapped to the borrowed token and returned to the borrow maker, as well as the taker fee. To incentivise healthy liquidation practices 50% of the remaining taker margin after liquidation is returned to the taker, while the rest is given as a reward to the liquidator.

Oracle risks

To keep Rainshower sovereign and decentralized, we use a Uniswap V3 TWAP oracle to determine the mark price of a token pair. While this solution enables any token pair to be used, it also introduces risks to both makers and takers in the form of short-term price manipulation. For example, price manipulation can be used to liquidate open borrows, that wouldn’t have been liquidated otherwise. For liquid pairs, price manipulation poses very small risks to parties engaged in a borrow and huge risks to the manipulator, who risks losing capital due to arbitrage.

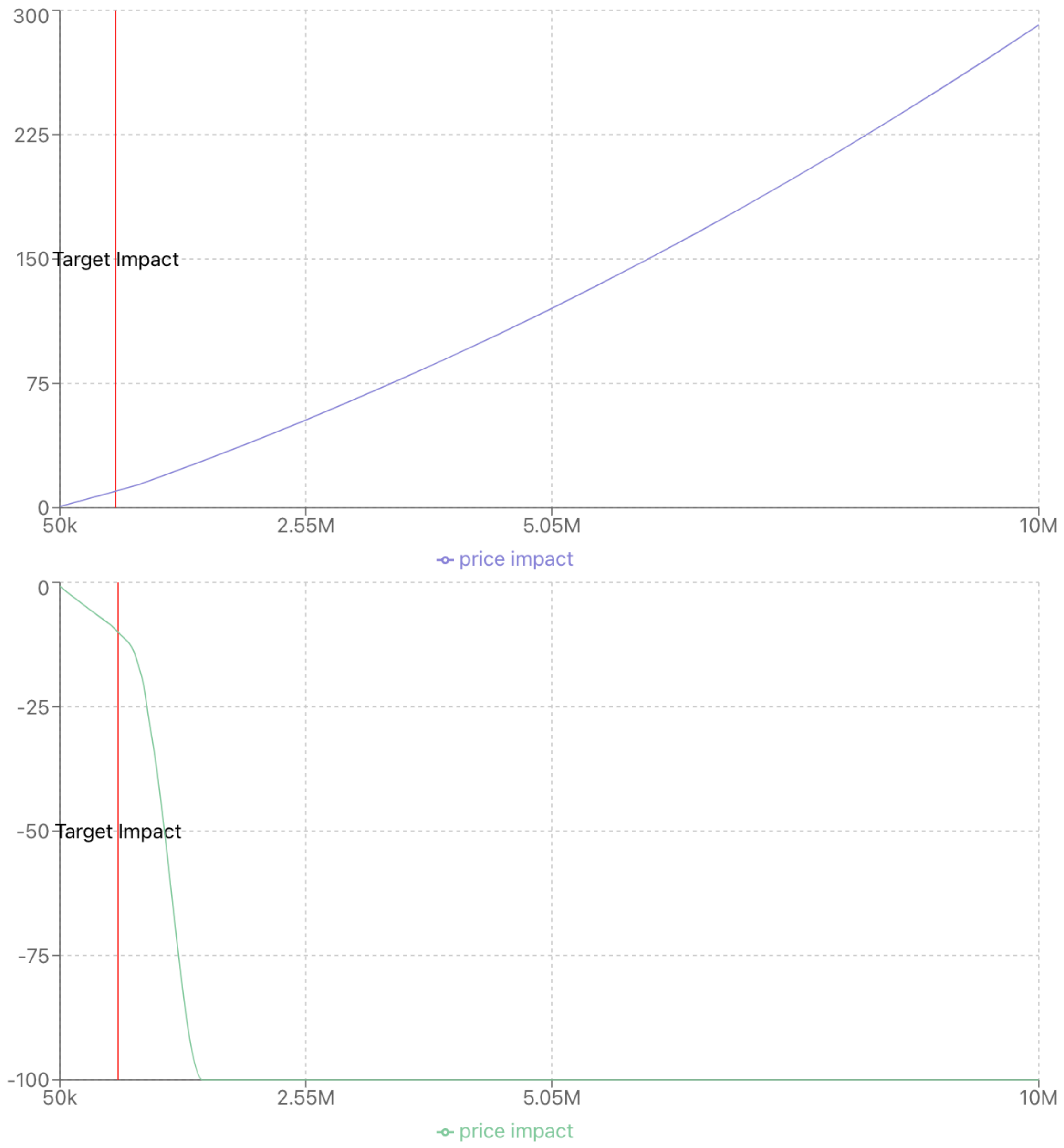
As an example, we can see that manipulating a liquid pair like WBTC/ETH doesn’t make sense, as it requires massive amounts of capital that the attacker risks losing to MEV and arbitrage bots. This makes the risk very high with a very low reward.



Uniswap V3 on chain TWAP attack costs for the WBTC/ETH pair. For a single block, a target impact of 10% would cost $1,879,087.773 on the upside, and $2,989,432.511 on the downside.

However, when we encounter lower liquidity pairs like 1INCH/WETH, we see that our attack would cost much less. Compared to our WBTC/ETH attack, we notice a 98.15% decrease in the cost to manipulate the price upwards, and a 98.74% decrease in the cost to manipulate downwards. This increases the risks for takers, as it can make forcing a liquidation to occur very lucrative.

To protect against this kind of price manipulation, it is recommended to keep enough collateral in the borrow and to use a higher TWAP period to force the attacker to attack for more than a single block, potentially making it unprofitable to do so.



Uniswap V3 on chain TWAP attack costs for the 1INCH/ETH pair. For a single block, a target impact of 10% would cost $34,615.793 on the upside, and $37,656.822 on the downside.

It should also be noted that due to the min and max tick price, there is a hard limit by how much a price can change in a single block, or in the case of rollups, a transaction. Given the spot price *(price)* (which is assumed constant outside of the attacked block), TWAP period *(period)*, and a number of attack blocks *(blocks)*, the attack can move the price up or down no more than:

$$maxTickPrice = 1.0001^{887272}$$

$$minTickPrice = 1.0001^{-887272}$$

$$maxTwapPrice = (p^{(period-blocks)} * maxTickPrice^{blocks})^{(1/period)}$$

$$minTwapPRice = (p^{(period-blocks)} * minTickPrice^{blocks})^{(1/period)}$$

Conclusion

We propose a protocol for trustless borrows between two parties, with rules of the borrow, agreed to by both before execution. We have designed borrows to work in any market conditions with minimal liquidity necessary for them to operate smoothly. All borrows need to have sufficient collateral and those that don't get liquidated. "Bank run" scenarios are prevented by liquidity being locked in the borrow for a certain amount of time, or in the case of liquidation or closure by the borrow taker. This positions Rainshower borrows a useful tool for all kinds of market participants.