

Dusa Protocol Whitepaper

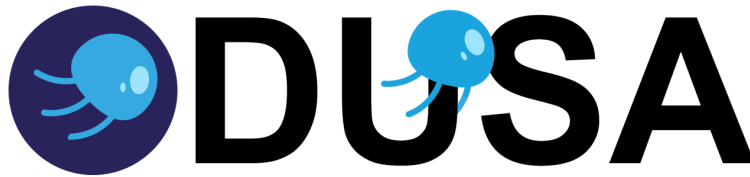
Leo JOUANNY
leo.jouanny@dusa.io

Pierre-Louis HABOURY *
pierre-louis.haboury@dusa.io

Solene DAVIAUD
solene.daviaud@dusa.io

Alexandre DUPIN
alexandre.dupin@dusa.io

March 15, 2024



Abstract

Dusa Protocol is a new non-custodial automated market maker that provides a fully on-chain experience, eliminating single points of failure and enhancing user experience through its advanced automated liquidity technology. This protocol is designed to simplify liquidity management by offering liquidity providers (LPs) the tools to create dynamic, decentralized strategies,

*Corresponding author, please direct any enquiry to contact@dusa.io

Contents

1	Introduction	3
2	The Current State	4
3	Enter Dusa Protocol	4
4	What does it change?	5
4.1	Trading	5
4.2	Providing Liquidity	6
5	Exceptions	8
6	Conclusion	8

1 Introduction

Automated Market Makers (AMMs) are one of the most widely used decentralized crypto products. Even in the current times, these market makers facilitate over \$10B of daily volume, rivaling the volumes of centralized exchanges such as Coinbase or OKX. AMMs connect liquidity from liquidity providers (LPs) looking for yields on their assets to traders wanting to swap them.

The Constant Product Market Maker $x * y = k$, a type of AMM that supports simple, gas-efficient swaps on-chain, popularized AMMs in DeFi. While swaps on Constant Product Market Makers are gas efficient, they are subject to high price impact. To mitigate this, a new wave of AMMs introduced innovations to increase capital efficiency, thereby limiting the price impact of trading, like Uniswap V3's concept of concentrated liquidity [1].

Uniswap V3's concentrated liquidity however has a flaw, research from November 2021 [2] shows that liquidity providers in 17 different Uniswap V3 pools have lost 260 million dollars due to Impermanent Loss whereas the total fees earned were 199 million dollars, resulting in a net loss for LP of more than 60 million dollars. Other protocols began researching a way to limit the Impermanent Loss, like Trader Joe V2. They introduced the concept of Liquidity Book (LB) [3], a novel design for structuring the liquidity of a decentralized exchange combined with a dynamic fee mechanism. It allows liquidity to be discretized into fixed-price bins, improving slippage and swap pricing. And unlike prior concentrated liquidity protocols, LB avoids high impermanent loss to liquidity providers. For example, the figure below could represent a market liquidity structure supplied by different market participants (color-coded).

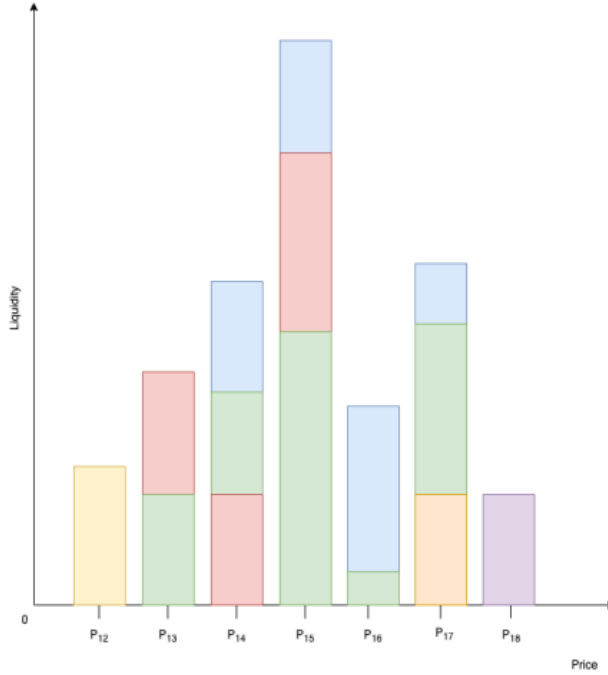


Figure 1: Example of Liquidity Structure color coded [3]

2 The Current State

There is now a protocol that is efficient for traders and liquidity providers. However, liquidity providers have two choices:

- The easy, less efficient way of managing their liquidity, passively, by setting a large range for their liquidity so that they can essentially ‘set and forget’. This approach is much less capital-efficient, but it is popular because it requires less time and effort to manage.
- The hard, more efficient way of managing their liquidity, actively, by rearranging the liquidity when the market moves. This approach is much more capital-efficient but is less popular due to the effort and time needed. Large wallets mainly use it with off-chain bots and wallet management applications.

That’s why we introduced an innovative approach to liquidity management, empowering liquidity providers with the ability to craft their own strategies in a decentralized manner, through customizable autonomous liquidity. This advancement enables users to tailor their risk parameters and impermanent loss (IL) exposure according to their preferences.

Furthermore, the current protocol’s limited automation capabilities also disadvantage another group of users: traders. At present, they lack access to the diverse array of products available on centralized exchanges, which are not found on various decentralized exchanges. Additionally, the front end frequently relies on centralized servers, creating vulnerabilities for front-end attacks.

These vulnerabilities have been exploited on numerous occasions, leading to losses for users. The absence of decentralization also poses a risk of censorship for trading pairs and addresses associated with certain decentralized applications.

3 Enter Dusa Protocol

Dusa operates as a non-custodial automated market maker on the Massa blockchain. Unlike other on-chain liquidity solutions, Dusa Labs boasts several benefits, including high fund utilization, minimal slippage, and a decrease in impermanent loss, thanks to the Liquidity books’ variable fees mechanism. It is fundamentally built on the Trader Joe’s Liquidity Book, but with a crucial addition: decentralized automation capabilities that set the stage for a trading experience similar to a centralized exchange, while maintaining full decentralization.

This trading experience is made possible by Massa’s autonomous smart contract [4], a smart contract that can wake up by itself and execute specific operations autonomously. Moreover, by allowing the concentrated liquidity to be fungible, LB structures allow for further composability and better liquidity management.

By combining these two technologies with our automated strategies possibilities, Dusa provides a more sophisticated way to maximize capital efficiency while reducing the time and effort needed to manage these strategies and providing an advanced trading experience.

Naturally, being entirely on-chain limits the computing power available, which is why we’re initially launching with a limited set of parameters. Yet, this capability, for the first time, allows every liquidity provider the opportunity to create their own management strategy without introducing any off-chain dependencies (like Arrakis Finance [5]) by having more flexibility with the liquidity. Thus,

it improves the Profit & Loss (P&L) for liquidity providers and reduces the percentage of passive liquidity while staying 100% on-chain, decentralized, and requiring no active management from the LP.

Moreover, Dusa Protocol offers the first fully decentralized DeFi protocol with a true 100% on-chain experience. This is made possible by the use of two major innovations:

- Hosting the front-end (web interface) [6] directly on the blockchain to avoid hacks such as with Badger DAO in 2020 or more recently with Curve. This works by stocking the zip file of the platform on the blockchain and extracting it each time the user wants to access Dusa Protocol, just by viewing the blockchain.
- The use of autonomous smart contracts eliminates the need for off-chain functionality that can be a source of human error and hacks. Thus, the asynchronicity and self-wake-up capabilities of smart contracts on Massa allow Dusa Labs to implement autonomous decentralized trading features and more complex strategies to optimize liquidity.

4 What does it change?

4.1 Trading

For traders, better management of liquidity reduces the slippage as the liquidity usage is better than on other AMMs at equal volumes as it reduces passive liquidity. On top of that, on-chain hosting combined with autonomous trading features increases security and user experience.

Currently, to execute a limit order on a DEX, users often have to rely on third-party solutions or off-chain initiators (such as Chainlink) that monitor the price of an asset and execute the trade when the target price is reached. This approach requires external interaction with the blockchain, which can lead to delays and additional transaction costs, without guaranteeing the order's execution due to off-chain dependency.

Dusa's primitives introduce a significant innovation in this area by directly integrating automation features, like limit orders, into the core of the protocol. This allows for more efficient execution of trading strategies without relying on external services or active market monitoring. Additionally, Dusa offers decentralized automation capabilities that reduce latency and costs, while increasing the security and transparency of operations.

For traders, this means a significant improvement in the trading experience with orders executed in a more predictable manner and at lower costs. They also benefit from advanced features such as generating yields on their orders while waiting for execution, a first in the DeFi ecosystem, thus opening new avenues for optimizing their capital.

By leveraging these integrated automation capabilities, builders can design products that better meet the end-users' needs, with more complex and automated trading and liquidity management strategies, without the hassle of third-party solutions.

As an example, if you have some Massa and want to sell them when the price is \$100. You can place an autonomous limit order without the risk of the platform failing to execute it due to certain problems such as a network issue. At the same time, you can keep your Massa staked while

waiting for your order to execute. And on top of that, you can access Dusa Labs without the risk of using a fraudulent website as it is stored on-chain. Thus, it removes two of the failure points of the current system.

Or with the On-Chain DCA, one could build a position over time while hedging against market risk without needing a centralized entity's partial or total intervention.

The possible trading features on Dusa are limit orders, DCA, stop limit, trailing stop, expiring order, and OCO.

This framework empowers traders to leverage our unique primitives to craft strategies that not only wait for the optimal execution moment but can also generate yields in alternative ways (such as staking, restacking, lending,...)

4.2 Providing Liquidity

When depositing liquidity on Dusa Protocol, liquidity providers (LP) can either create their own Autonomous Liquidity strategy or deposit their concentrated liquidity like on a traditional AMM. In both cases, the LP will receive fees to reward them for providing liquidity.

Thus Dusa offers a liquidity structure that requires no active management from the LP while also allowing them to handle their liquidity manually. To implement, for example, a strategy that involves a form of betting on price variations.

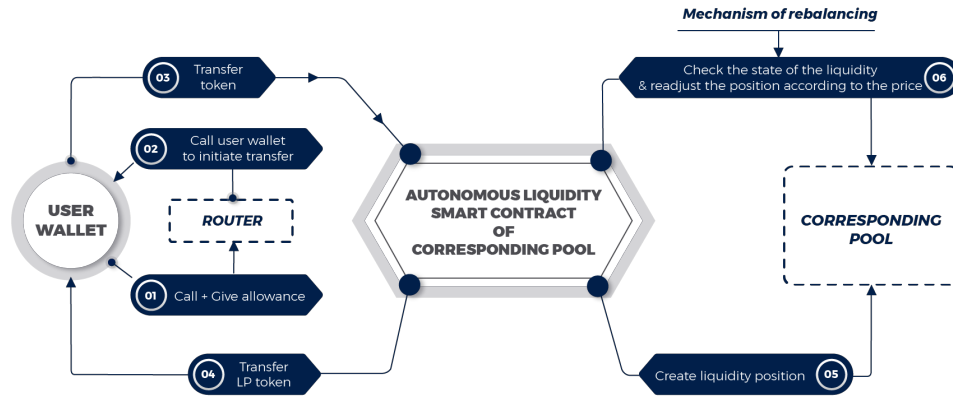


Figure 2: adding liquidity to the autonomous liquidity

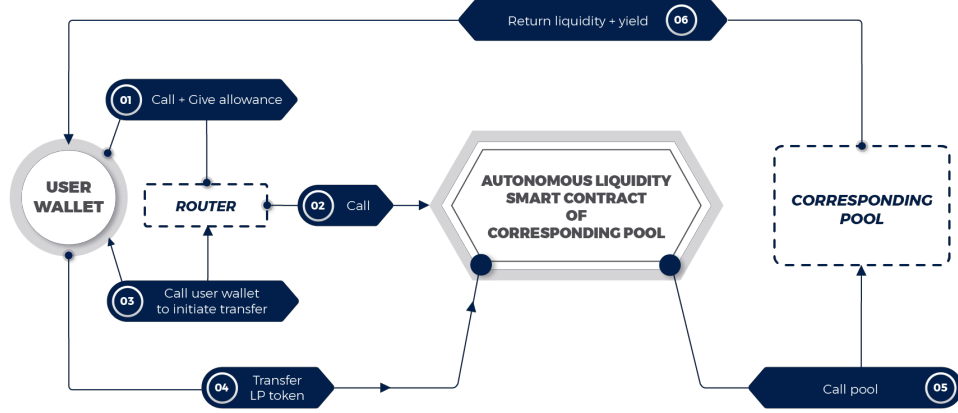


Figure 3: withdrawing liquidity from the autonomous liquidity

When creating a autonomous liquidity position, the user can adapt to the market trend and adapt the parameters of their strategies, such as position width, automation frequencies, rebalancing threshold, liquidity replacement position and shape. Then, they deposits their two tokens into a contract in an equivalent amount, as if they were depositing in a Vault, and receives in return an AL token corresponding to their liquidity position. A mechanism possible can be one based on the passive rebalancing of Charm Finance [7]. It works by passively rebalancing using range orders, which significantly improves its performance.

Rebalancing is necessary when providing concentrated liquidity. For example, if you initially deposit 50% MAS and 50% USDC, but the price moves a lot one way, you might be left with 80% MAS and 20% USDC. Then you'd need to rebalance back to 50/50 somehow so that you don't run out of inventory on either side and can continue providing two-sided liquidity.

One way to rebalance would be to aggressively rebalance by swapping MAS to USDC on Dusa to get back to 50/50, but this incurs the 0.3% trading fee and price impact.

Instead, the rebalance is done passively, placing a narrow range order on one side of the current price. This avoids the need to swap tokens and incur the fee and price impact.

For example, a implementation possible of our autonomous liquidity mechanism is a strategy that always maintains three active range orders:

- Base concentrated position centered around current price x , in the range $[x - \lambda, x + \lambda]$ with λ the base parameter. If λ is lower, it will earn a higher yield from trading fees but can result in a riskier position.
- Rebalancing orders just above or below the current price. It will be in the range $[x - R, x]$, or $[x, x + R]$ with R the rebalance parameters, depending on which token it holds more of after the base order is placed. This order helps the strategy rebalance and get closer to 50/50 to reduce risk.
- A large liquidity position to avoid big liquidity movements leading to an increasing slippage. Thus, only 30% of the total liquidity under management is concentrated and the other 70% is in a larger liquidity position. This also limits the losses in the case of a quick market crash.



Figure 4: Example of the rebalancing mechanism of the autonomous liquidity.

Thus, this solution brings multiple advantages:

- **Improve returns:** Increase the capital efficiency of your liquidity by concentrating liquidity smartly across different ranges and pricing the pools to maximize P&L.
- **Simplicity:** Save time determining the right price ranges, actively monitoring them, or trading in and out to appropriately lock in profits or initiate new positions.
- **Gas Costs:** Share alongside others in the gas costs incurred through actively managing strategies.
- **Transparency:** 100% on-chain.

Using our autonomous liquidity mechanism, LPs can construct a variety of strategies tailored to different market scenarios, thereby introducing an entirely new primitive for LPs to explore.

5 Exceptions

For now, the Autonomous Liquidity strategies will not be available in stable markets. Indeed, due to their stability, the AL would be more cost-inefficient than a concentrated position

6 Conclusion

In conclusion, Dusa Protocol marks a significant advancement in the AMM space by offering a completely on-chain, non-custodial trading and liquidity management solution. It addresses the limitations of existing decentralized exchanges by bringing users more control over their trading strategies and liquidity provision. By providing a framework for LPs to actively engage with their liquidity in a highly customizable and efficient manner, Dusa Protocol offers a compelling vision for the future of DEXes.

References

- [1] Hayden Adams et al. Uniswap v3 Core. en. <https://uniswap.org/whitepaper-v3.pdf>. 2021. (Visited on 01/31/2023).
- [2] Stefan Loesch et al. Impermanent Loss in Uniswap v3. en. <https://arxiv.org/ftp/arxiv/papers/2111/2111.09192.pdf>. 2021.
- [3] MountainFarmer et al. Trader Joe Whitepaper. <https://github.com/traderjoe-xyz/LB-Whitepaper/blob/9d259d99f904b231850e113dbeb13696ee9004c7/Joe%20v2%20Liquidity%20Book%20Whitepaper.pdf>. Nov. 2022. (Visited on 01/31/2023).
- [4] Massa. Massa | Autonomous Smart Contracts. en. <https://massa.net/autonomous-sc>. (Visited on 01/31/2023).
- [5] Arrakis. Arrakis Finance - Web3's Liquidity Layer. en. <https://www.arrakis.finance/>. (Visited on 01/31/2023).
- [6] Massa. Massa's Decentralized web — Massa documentation. <https://docs.massa.net/en/latest/general-doc/decentralized-web.html>. (Visited on 01/31/2023).
- [7] Max. Introducing Alpha Vaults — an LP strategy for Uniswap V3. en. <https://medium.com/charmfinance/introducing-alpha-vaults-an-lp-strategy-for-uniswap-v3-ebf500b67796>. Nov. 2021. (Visited on 01/31/2023).