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

Baptiste MARCHAND
baptiste.marchand@dusa.io

June 14, 2023
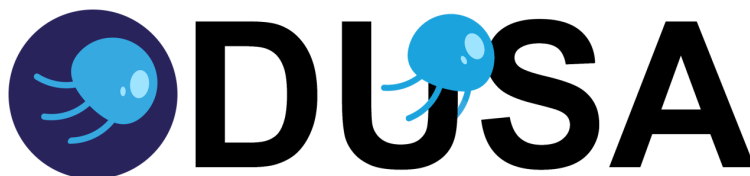
Abstract

Dusa Protocol is a new non-custodial automated market maker. It offers a 100% on-chain experience, thus removing any single point of failure while providing an improved user experience thanks to our automated liquidity technology.

---

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

Contents

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 \$1B of daily volume, rivaling the volumes of centralized exchanges such as Coinbase or Kraken. 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).
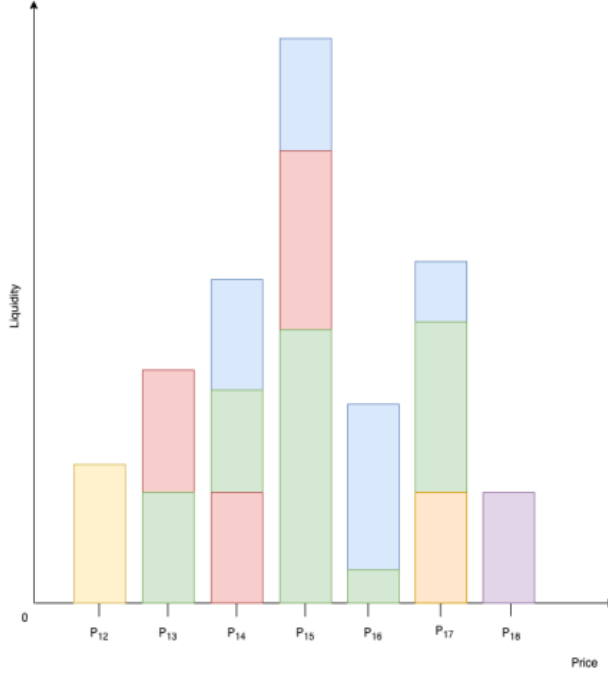

Figure 1: Example of Liquidity Structure color coded [3]

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.

Moreover, the current system lacks decentralization and thus security. Indeed, off-chain initiators are used in different DEX, for example, to execute limit orders. Also, the front end is often hosted on centralized servers which opens the way for front-end attacks. Those failure points have already been exploited multiple times, resulting in user losses. Due to their lack of decentralization, they can also lead to censorship issues on trading pairs and addresses linked to certain DApps.

3　Enter Dusa Protocol

Dusa is a non-custodial automated market maker on the Massa blockchain. Compared to other on-chain liquidity solutions, Dusa Labs has multiple advantages: high fund utilization, low slippage, and reduced impermanent loss (which is made possible by Trader Joe's variable fees mechanism). Indeed, it is based on Trader Joe's Liquidity Book with one key element on top: Autonomous Liquidity (AL), a 100% on-chain liquidity management tool.
AL 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 liquidity management tool, Dusa provides a more sophisticated way to maximize capital efficiency while reducing the time and effort needed to manage these strategies.
Of course, as it is fully on-chain, the computing power is limited. However, this feature can still compete with existing off-chain liquidity managers (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.

4 What does it change?

4.1 Trading

For traders, Autonomous 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.

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. And on top of that, you can access Dusa Labs without the risk of using a fraudulent website as it is stored in chains. 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.

4.2 Providing Liquidity

When depositing liquidity on Dusa Protocol, liquidity providers (LP) can either use the Autonomous Liquidity feature or deactivate it and deposit their concentrated liquidity like on Trader Joe V2 and Uniswap V3. 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.
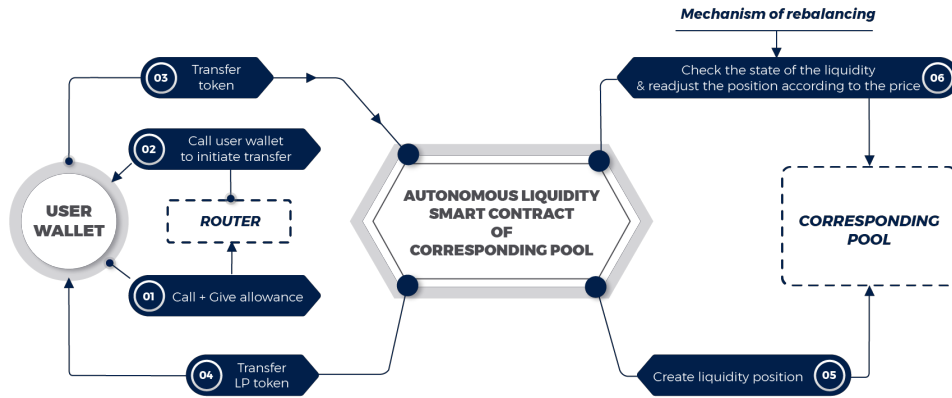

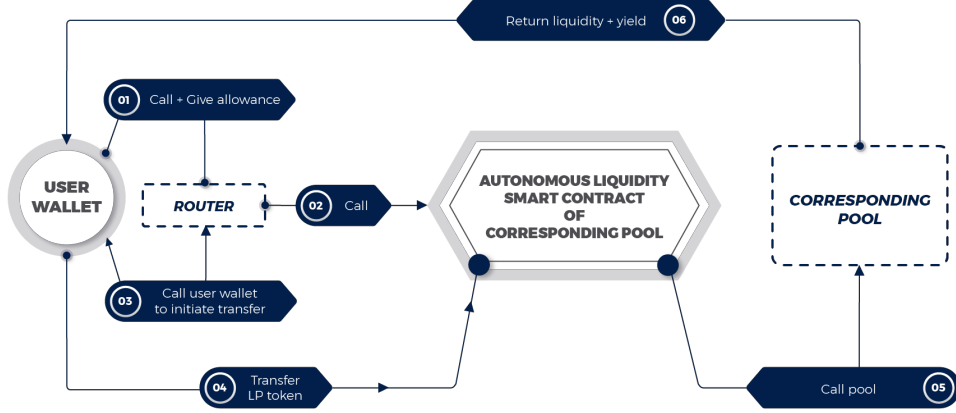Figure 2: adding liquidity to the autonomous liquidity

5

Figure 3: withdrawing liquidity from the autonomous liquidity

When using the AL, the user 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 share of the AL. Then the AL contract adds these funds to its total liquidity under management and starts to place them appropriately in the selected pool. Liquidity ranges are automatically rebalanced when certain rebalance triggers are hit or every few blocks, depending on the volatility of the pair. Liquidity ranges are set according to the current volatility of the pair, the bin containing the price at the time plus a time-weighted average price, the liquidity depth, and the previous position. The mechanism is 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.

The strategy 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.

5 Exceptions

For now, the Autonomous Liquidity tool will not be implemented in the following cases:

- Stable markets: Due to their stability, the AL would be more cost-inefficient than a concentrated position

- Hyper Volatile markets: For such markets, more computing power is required and as our liquidity management tool is on-chain, the computing power is limited.

6 Conclusion

Dusa Protocol is a new non-custodial automated market maker that enables the possibility to have a 100% on-chain experience and thus remove any single point of failure. Dusa also offers a liquidity structure that requires no active management from the LP while also allowing them to handle their liquidity manually.

7 Legal Disclaimer

7.1 Information purposes only

This White Paper is for general information purposes only and may be subject to change without prior notice. Dusa Labs and any current or future affiliated entities, their managers, directors, officers, employees, advisors, consultants, agents, or any other person (the "Dusa Team") do not make or purport to make, and hereby disclaim, any representation, undertaking or warranty in any form whatsoever to any person or entity, including any representation, undertaking or warranty concerning the accuracy and completeness of any of the information set out in this White Paper. Further, circumstances may change, and this White Paper may become outdated. The Dusa Team is under no obligation to update or correct this White Paper in connection therewith. This White Paper may be translated into a language other than English for information purposes only. In such cases, the English language version shall always prevail over the translated versions of this White Paper.

7.2 No contractual relationship

The information herein does not imply any elements of a contractual relationship nor form the basis of or be relied upon in connection with, any investment decision. The information set out in this White Paper is not legally binding and is for community discussion only. It provides an initial overview of certain business and technical essentials underlying the Dusa Protocol.

7.3 Third-party information

The Dusa Team accepts no liability for damages, whether indirect or consequential, of any kind arising from the use, reference, or reliance on the contents of this White Paper. This White Paper may contain references to data, industry publications, and/or third-party research. No warranty is given to the accuracy and completeness of such third-party information. Neither the third-party information, its inferences nor its assumptions have been independently verified.

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).