# UniswapX

July 2023

Hayden Adams
hayden@uniswap.org

Noah Zinsmeister
noah@uniswap.org

Mark Toda
mark@uniswap.org

Emily Williams
emily@uniswap.org

Xin Wan
xin@uniswap.org

Matteo Leibowitz
teo@uniswap.org

Will Pote
pote@uniswap.org

Allen Lin
allen.lin@uniswap.org

Eric Zhong
eric.zhong@uniswap.org

Zhiyuan Yang
zach.yang@uniswap.org

Riley Campbell
riley.campbell@uniswap.org

Alex Karys
alex.karys@uniswap.org

Dan Robinson
dan@paradigm.xyz

## ABSTRACT

UniswapX Protocol is a non-custodial Dutch auction-based trading protocol implemented for the Ethereum Virtual Machine.

UniswapX aggregates both onchain and offchain liquidity, internalizes MEV in the form of price improvement, offers gas-free swaps, and can be extended to support cross-chain trading.

## 1 INTRODUCTION

We present a design for a Dutch auction-based decentralized trading protocol using signed offchain orders that are executed and settled onchain.

The UniswapX Protocol offers several benefits:

- UniswapX outsources routing and batching to a permissionless set of *Fillers*. These fillers can route orders to a combination of onchain and offchain liquidity, ensuring that *Swappers* always receive best possible execution on their orders.
- UniswapX trades use Permit2 executable offchain signatures, allowing swappers to pay transaction fees implicitly as part of their swap and avoid maintaining a balance of the chain's native token.
- Swappers never pay gas costs for failed swaps, and orders that are batch settled and/or filled directly from fillers' inventory are more gas efficient than swaps on the core Uniswap Protocol.
- Unlike AMMs, UniswapX internalizes MEV [9], reducing value lost by returning any surplus generated by an order back to the swappers in the form of price improvement. Additionally, UniswapX orders are far less vulnerable to frontrunning.
- UniswapX can be extended to support cross-chain trading, allowing swappers to seamlessly trade assets on an *origin* chain for desired assets on a *destination* chain.

The following sections provide in-depth explanations of these changes and the architectural changes that help make them possible.

## 2 SIGNED ORDERS

When swappers trade through the Uniswap Protocol (v1, v2, v3, and v4 [3–6]), they create and sign transactions. These transactions specify an input token, an output token, a particular execution route, and a minimum output amount. Swappers then submit their transactions to a mempool (whether public or private), where they are then picked up by block builders and included in blocks.

UniswapX leverages Permit2 [19], a token approval contract that introduces signature-based approvals and transfers for any ERC20 token. In addition, UniswapX settles onchain using a *Reactor Contract*, which is responsible for checking that the execution of a trade matches the parameters users expect, and reverting trades that do not. Swappers must first approve the Permit2 contract. Then, rather than creating and submitting transactions themselves, swappers trading through the UniswapX protocol sign orders specifying:

(1) An input token
(2) An output token
(3) An input (output) amount
(4) A starting output (input) amount
(5) A minimum output (input) amount
(6) A decay function
(7) A claim deadline
(8) Authorization for the UniswapX reactor contract to spend tokens on their behalf

These orders are picked up by a combination of MEV searchers, market makers, and/or other onchain agents — collectively known as fillers — who send them to the reactor contract. By submitting swappers' orders onchain, fillers pay gas fees on their behalf. These costs are then recouped by factoring gas fees into the execution price.

The reactor contract then calls the filler's *Executor Contract*, specifying the fill logic. Once assets have been sourced, the executor contract sends assets to the swapper, and the executor pulls funds from the swapper's address. Finally, the Reactor checks that the order's conditions have been met.

UniswapX does not specify how fillers fill swappers' orders: liquidity can be sourced from a combination of onchain liquidity venues like Uniswap or other DEXs, offchain liquidity, or from other UniswapX orders. Multiple orders can be bundled into the same transaction, which can also execute other actions atomically onchain.

## 3 DUTCH ORDERS

In order to provide swappers with best execution, UniswapX uses an order type we call a Dutch order, which closely resembles a Dutch auction. The decaying nature of Dutch orders creates a competitive market among fillers to find the best possible price for swappers as soon as possible while keeping some small profit margin for themselves.

Unlike ordinary limit orders, which always execute at their limit price, Dutch orders execute at a price that depends on the time of its inclusion in a block. The order starts at a price that is estimated to be better for the swapper than the current estimated market price — for example, if the current market price is 1,000 USDC per ETH, a sell order may start at a price of 1,050 USDC per ETH. The order's price then decays over time until it hits the worst price the swapper would be willing to accept (e.g. 995 USDC per ETH).

Fillers are incentivized to fill an order as soon as it is profitable for them to do so. If they wait too long, they risk losing the order to another filler willing to take a smaller profit.

## 4 CROSS-CHAIN ORDERS

The UniswapX Protocol can be extended to support cross-chain trading, where a swapper trades assets they hold on an origin chain for desired assets on a destination chain.

Cross-chain UniswapX offers several benefits:

- UniswapX can offer fast swaps between any two chains, as long as there is a message passing bridge between the two.
- Swapping and bridging are combined into a single action, removing the need for swappers to interface directly with bridges, maintain gas tokens on either chain, or wait for settlement delays.
- UniswapX can offer near-instant exits from an L2 to its parent L1.
- Swappers can specify that they receive native or canonical assets on the destination chain, rather than a bridged asset. For example, ETH on mainnet can be swapped directly for AVAX on Avalanche.
- Passive bridge risk is minimized. Swappers do not assume any exposure to a bridge when swapping native assets, and fillers only take on bridge risk while rebalancing between chains through bridges.

### 4.1 Simplified Cross-Chain Orders

First we will explain a simplified version of the cross-chain UniswapX Protocol, before extending it to the more efficient optimistic protocol.

In order to initiate a cross-chain order, the swapper signs an offchain order that includes the same parameters as a single-chain order, alongside the following additional parameters:

(1) A settlement oracle — a one-way oracle that can attest to events occurring on some destination chain. This could be a canonical bridge between a rollup and its parent chain, a light client bridge, or a third party bridge
(2) A fill deadline — the time before which the order must be filled on the destination chain
(3) A filler bond amount and filler bond asset — the bond that the filler must deposit on the origin chain
(4) A proof deadline — the time before which the filler must prove their fill on the origin chain

Parameterization of the filler bond amount, the fill deadline and the proof deadline are outside the scope of this paper.

As with the single chain implementation of the UniswapX Protocol, the swapper's order is disseminated to a network of fillers, who compete to execute it by submitting the order, alongside the swapper's funds and a filler bond, to the origin chain's reactor contract.

The filler fills an order by transferring the swapper's desired assets on the destination chain. They first send the assets to the reactor contract which then forwards them on to the swapper's address. The reactor contract on the destination chain records that the order was filled before the specified deadline, and relays a message through the settlement oracle back to the reactor contract on the origin chain confirming fulfillment of swapper's order.

The swapper's assets, alongside the bond, are then released to the filler on the origin chain. In the event that the filler does not execute the order before the proof deadline, the swapper receives both their input assets and the filler's bond from the reactor contract on the origin chain.

### 4.2 Optimistic Cross-Chain Orders

Some settlement oracles may be prohibitively slow or expensive to use. For example, executing swaps from one rollup to another may be prohibitively expensive for fillers, taking over seven days and involving at least one transaction on the L1 before they are allowed to take custody of the swapper's input tokens and their initial bond.

An optimistic cross-chain protocol can alleviate these settlement delay issues, effectively constructing a fast and cheap bridge on top of any slow bridge.

The optimistic protocol includes the same parameters as the simplified protocol, plus the following additional parameters:

(1) Challenge bond amount and challenge bond asset — the amount that a challenger must post as a bond on the origin chain.
(2) Challenge deadline — the deadline before which a challenger can challenge a fill. This must be before the proof deadline.

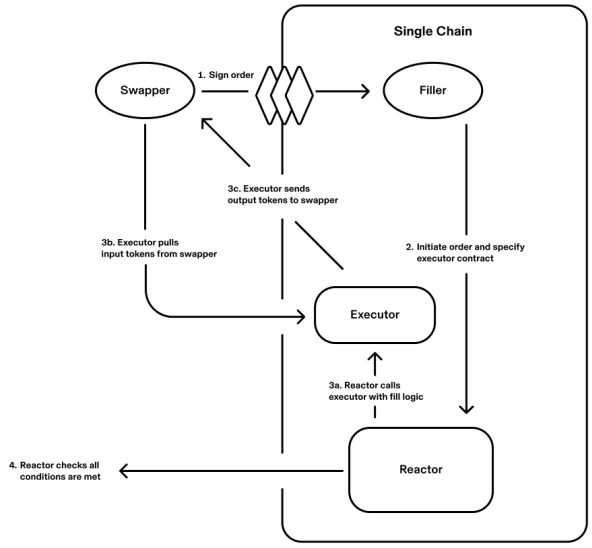


**Figure 1: Single Chain Swap Diagram**

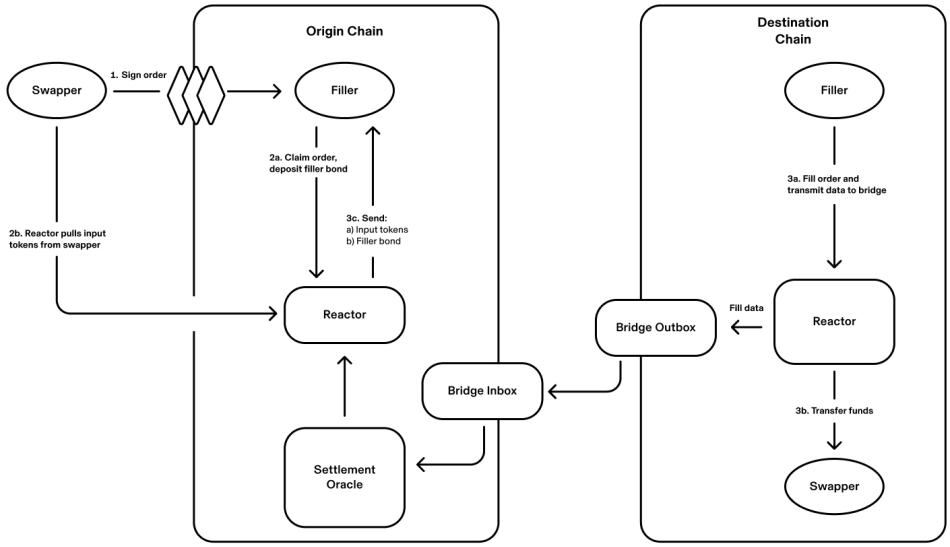


**Figure 2: Simplified Cross Chain Swap Diagram**

As in the simplified protocol, the filler executes an order by claiming the swapper's order and submitting the filler bond to the origin chain reactor contract, and then by transferring assets to the swapper's address on the destination chain via the destination chain reactor contract. The reactor contract records that the order was filled before the fill deadline.

In the optimistic case, the filler fills the swapper's order on the destination chain before the fill deadline, no one challenges the fill before the end of the challenge period and the filler receives the swapper's funds, alongside their filler bond, on the origin chain.

In order to keep the filler honest, anyone can challenge the filler after the fill deadline has passed and before the challenge deadline has expired using the reactor contract on the origin chain. In the event the fill is challenged, the filler has to provide a proof before the proof deadline using the settlement oracle. If the filler can prove that they filled the order before the proof deadline then they

receive the challenger's bond. If instead the filler fails to provide a valid proof, the filler's bond is split between the challenger and the swapper and the swapper's funds are returned to them on the origin chain.

## 5 ORDER PARAMETERIZATION

The UniswapX Protocol does not enforce a specific decay function. Similarly, the protocol does not prescribe a method for setting the initial Dutch order price, but it does include some optional functionalities to enable different mechanisms.

One way of parameterizing the Dutch order starting price is to poll a selection of fillers through an offchain Request For Quote (RFQ) system. In order to incentivize this network of fillers to offer their best possible price, UniswapX allows orders to specify a filler that receives the exclusive right to fill the order for a brief duration, after which the Dutch auction begins and any filler is able to execute the order.[1]

An RFQ system may benefit from using an accompanying reputation or penalty system to limit abuse of the free option that this exclusivity provides fillers and to ensure that swapper user experience does not suffer. As with the order parameterization design, any such system is outside the scope of the core protocol and this paper.[2]

## 6 FEES

Uniswap Governance has the ability to charge a fee of up to 0.05%, the same max fee as Uniswap v2, on the output of each UniswapX swap. Governance must specify fees on a per pair basis, and the fee must be an integer value in basis points. Governance must also activate fees on a per-chain basis.

Interfaces and wallets can choose to charge an additional uncapped fee on swaps submitted through their platforms.

## 7 PRIOR WORK

The UniswapX Protocol draws inspiration from numerous protocols, both past and present. This is not an exhaustive list.

### 7.1 Signed Orders

Many protocols have recognized the utility of having swappers sign orders rather than transactions, including 0x [20] and Wyvern [21]. Several protocols, including CoW Swap [8] and dYdX [13], support batching offchain signed orders. Seaport [17] specifically supports offchain signed orders with a decay function.

### 7.2 Dutch Auctions

Dutch auctions have found numerous applications in DeFi, including for NFT sales in Seaport, for liquidations in MakerDAO [14] and Euler Protocol [11], and for trading in protocols like DutchX [15]. Stephane Gosselin has also previously proposed using Dutch auctions as a method for setting transaction fees in EIP 2593 [10]. More recently, 1inch has explored the combination of signed orders and Dutch auctions in their Fusion Protocol [1].

### 7.3 DEX Aggregators

Projects including 1inch, 0x API, and Paraswap [18] offer swappers smart order routing functionality across a variety of onchain liquidity venues. Some of these projects also allow offchain market makers to provide order improvement through an RFQ system.

### 7.4 Cross-Chain Dutch Auctions

Summa [12] pioneered the idea of Dutch Auction-based cross-chain trades via a one-way message-passing oracle.

### 7.5 Optimistic Bridges

Optics [7], Nomad [16], and Across [2] all use fraud-proof enabled settlement designs to offer trustless and fast token bridging.

## 8 CONCLUSION

UniswapX is a non-custodial and permissionless trading protocol that uses Dutch auctions to create a competitive routing marketplace among fillers and tap into a combination of onchain and offchain liquidity. By structuring orders as Permit2 executable offchain signatures, the protocol provides swappers with a gas-free trading experience. UniswapX can also be extended to support cross-chain swaps, allowing swappers to bridge assets from an L2 to its parent L1 near-instantaneously.

[1] There is an exception to this exclusivity window if another filler is able to provide further price improvement relative to the winning filler's quote, above a minimum bid increment set by the order constructor.

[2] Uniswap Labs is actively working with the research community, including Maryam Bahrani and Tim Roughgarden, to explore possible implementations of a fully permissionless RFQ / reputation system.

## REFERENCES


[1] 1inch Labs. 2022. The 1inch Network releases a major upgrade, Fusion. https://blog.1inch.io/the-1inch-network-releases-a-major-upgrade-fusion/

[2] Across. 2023. Across Overview. https://docs.across.to/how-across-works/overview

[3] Hayden Adams. 2018. *Uniswap v1 Core.* Retrieved Jun 12, 2023 from https://hackmd.io/@HaydenAdams/HJ9jLsfTz

[4] Hayden Adams, Moody Salem, Noah Zinsmeister, Sara Reynolds, Austin Adams, Will Pote, Mark Toda, Alice Henshaw, Emily Williams, and Dan Robinson. 2023. Uniswap v4 Core [Draft]. (2023).

[5] Hayden Adams, Noah Zinsmeister, and Dan Robinson. 2020. *Uniswap v2 Core.* Retrieved Jun 12, 2023 from https://uniswap.org/whitepaper.pdf

[6] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. 2021. *Uniswap v3 Core.* Retrieved Jun 12, 2023 from https://uniswap.org/whitepaper-v3.pdf

[7] Celo. [n. d.]. Optics Bridge FAQs. https://docs.celo.org/protocol/bridge/optics-faq

[8] CoW Protocol. 2019. CoW Protocol Overview. https://docs.cow.fi/?&utm_content=footer-link&utm_medium=web&utm_source=cow.fi

[9] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP).* IEEE, 910–927.

[10] Dan Finlay. 2020. EIP-2593: Escalator fee market change for ETH 1.0 chain. https://eips.ethereum.org/EIPS/eip-2593

[11] Euler Finance. 2022. Euler Finance White Paper. https://docs.euler.finance/getting-started/white-paper

[12] James Prestwich. 2018. Cross-chain Auctions via Bitcoin Double Spends. https://medium.com/summa-technology/summa-auction-bitcoin-technical-7344096498f2

[13] Antonio Juliano. 2018. dydx: A standard for decentralized margin trading and derivatives. *URl: https://whitepaper. dydx. exchange* (2018).

[14] MakerDAO. 2020. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. https://makerdao.com/en/whitepaper#notes

[15] Martin Köppelmann. 2018. DutchX - fully decentralized auction based exchange. https://ethresear.ch/t/dutchx-fully-decentralized-auction-based-exchange/2443

[16] Nomad. 2022. Nomad Protocol Overview. https://docs.nomad.xyz/the-nomad-protocol/overview

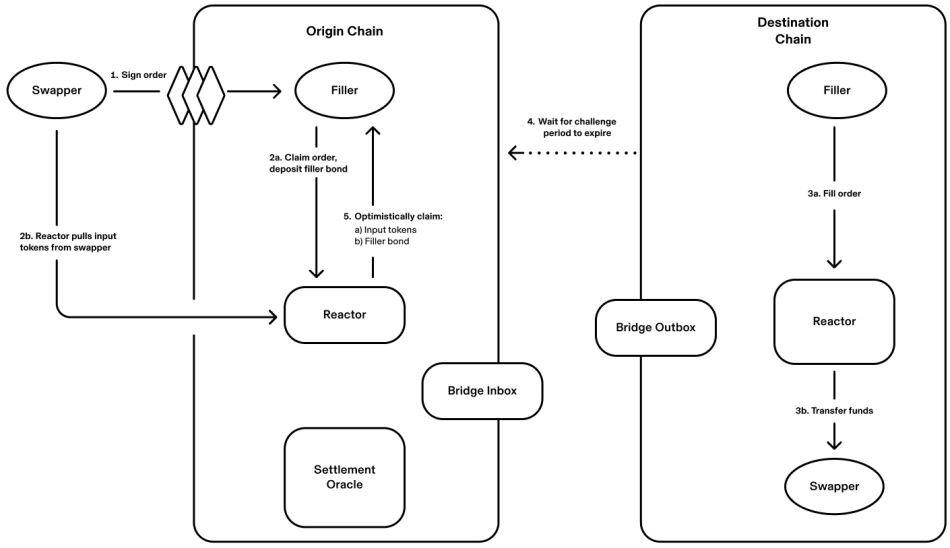


**Figure 3: Optimistic Cross Chain Swap With No Challenge**

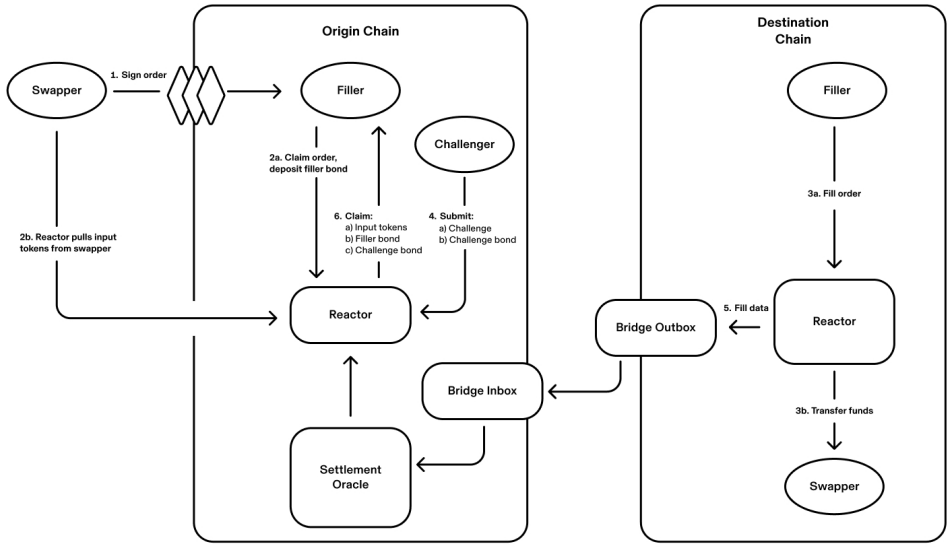


**Figure 4: Optimistic Cross Chain Swap With Unsuccessful Challenge**

[17] Opensea. 2022. Seaport Overview. https://docs.opensea.io/reference/seaport-overview
[18] ParaSwap. 2020. Welcome. https://doc.paraswap.network/
[19] Uniswap Labs. 2022. Introducing Permit2 Universal Router. https://blog.uniswap.org/permit2-and-universal-router
[20] Will Warren and Amir Bandeali. 2017. *0x: An open protocol for decentralized exchange on the Ethereum blockchain.*
[21] Wyvern Protocol. 2020. Wyvern Protocol Documentation. https://wyvernprotocol.com/docs

## DISCLAIMER

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of Uniswap Labs, Paradigm, or their

affiliates and does not necessarily reflect the opinions of Uniswap Labs, Paradigm, their affiliates or individuals associated with them. The opinions reflected herein are subject to change without being updated.