Articles

Introduction

1inch Fusion+ (intent-based atomic cross-chain swaps)

> ⓘ **INFO**
>
> For a comprehensive technical overview, refer to the 1inch Fusion+ whitepaper.

The 1inch Fusion+ API is a powerful solution for secure and efficient cross-chain swaps in DeFi that uses a creative architecture of Dutch auctions and automated recovery, all without relying on a single centralized custodian.

Phases of a Fusion+ swap

The process typically involves two main participants: the maker, who initiates the swap, and the resolver, who completes it; and has three phases. However, if any problems arise, there is an optional 4th *recovery phase* that can be used as a last resort.

Phase 1: Announcement

The maker initiates the process by signing a 1inch Fusion+ order and broadcasting it to 1inch. This signals their intent to execute a cross-chain swap and sets the process in motion.

The order is distributed to all resolvers, triggering a Dutch auction. Resolvers compete by offering progressively better prices as the auction continues until a resolver locks in the order by initiating an escrow on the source chain.

Phase 2: Deposit

The winning resolver deposits the maker's assets into an escrow contract on the source chain, and then deposits the corresponding assets into an escrow on the destination chain. Both escrows are linked by a secret hash, ensuring that assets can only be unlocked once the swap is completed. A small

safety deposit is also assigned to each escrow, incentivizing the resolver to successfuly complete the order.

Phase 3: Withdrawal

Once both escrows are verified by the relayer, the secret is revealed, allowing the resolver to unlock the assets on the destination chain for the maker. The resolver then uses the same secret to retrieve their newly acquired assets on the source chain, finalizing the swap.

Optional phase: Recovery

In the event of a failed swap (e.g., if a party becomes unresponsive), the protocol includes a recovery mechanism. After the timelock expires, any resolver or any participating entity can cancel the swap and return the assets to their original owners. The safety deposit in each escrow is transfered to any resolver who steps in to complete the swap during this phase.
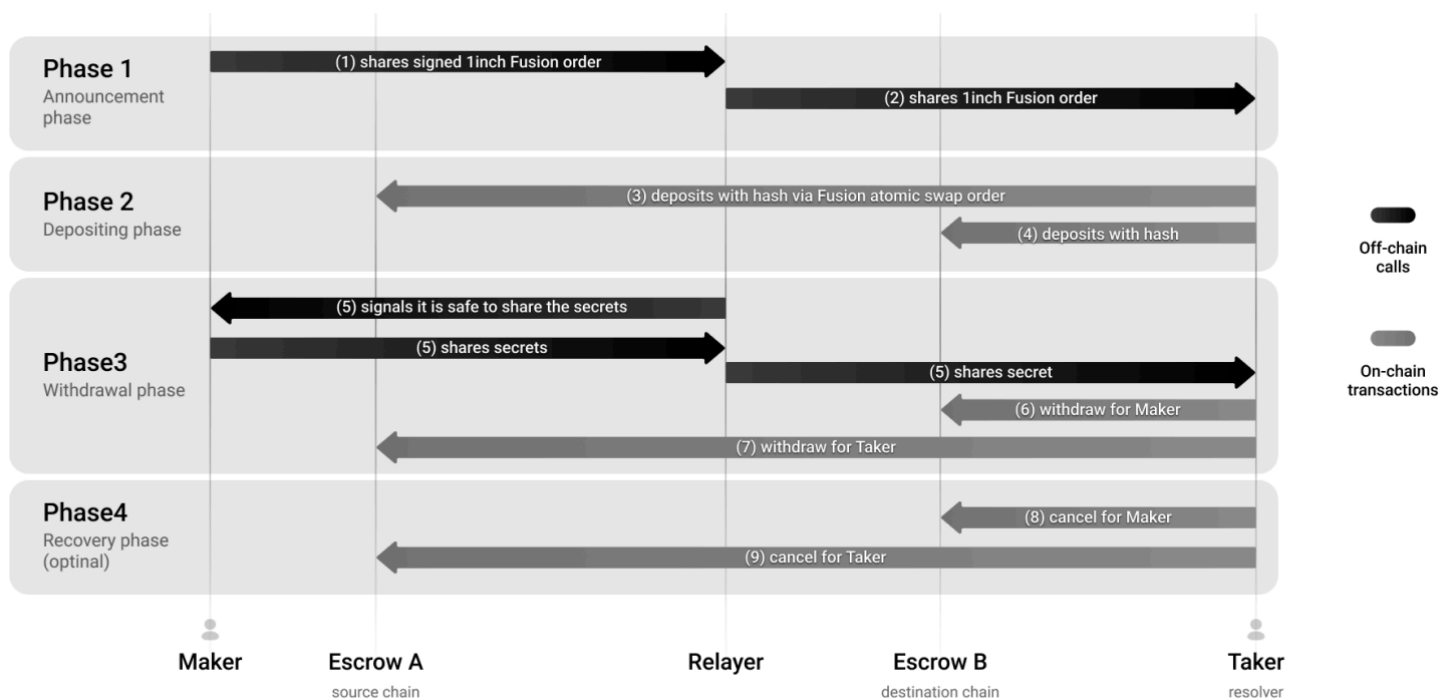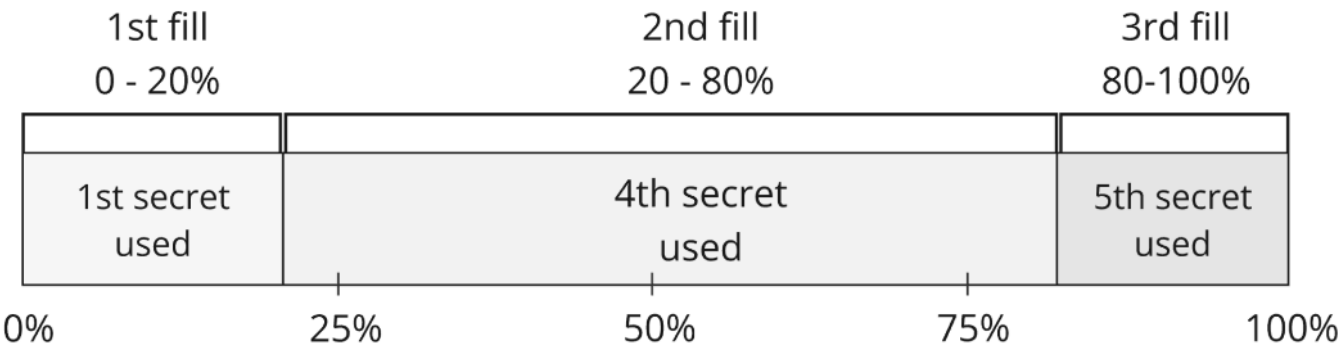

The partial fill feature

When an order is 100% filled, a single secret is used to finalize the transaction between two parties. However, when an order is only partially filled by different resolvers, revealing the secret to the public could let others claim the remainder of the order without completing their part.

To solve this, a Merkle tree of secrets is implemented for partial fills, which splits the order into equal parts and generates dedicated secrets for each portion of swap.

For example, if an order is divided into four parts, the first secret is used for the first 25%, the second for 50%, and so on. If a participant fills a part of the order, the next participant uses the corresponding secret based on the current progress to continue filling the order. This ensures that each participant can only fill their portion without exposing the rest of the order.

In the example image below, the 1st secret is used for the initial 0-20% fill, marking the first stage of the order. Secrets 2 and 3 are not used because the order skips directly from 20% to 80%, bypassing the ranges where these secrets would apply. The 4th secret is then used to fill the order from 20% to 80%, covering this larger portion. Finally, the 5th secret is used to complete the final 80-100% of the order, ensuring that the entire order is securely and progressively filled.

1st fill	2nd fill	3rd fill
0 - 20%	20 - 80%	80-100%
1st secret used	4th secret used	5th secret used

0%　　　　　　25%　　　　　　50%　　　　　　75%　　　　　　100%

API reference

For detailed information about each endpoint, refer to the Fusion+ API Swagger section.