1INCH FUSION+

INTENT-BASED ATOMIC CROSS-CHAIN SWAPS

Anton Bukov
k06aaa@gmail.com

Sergej Kunz
info@deacix.de

Mikhail Melnik
by.zumzoom@gmail.com

Gleb Alekseev
alekseev.gleb@gmail.com

Matt Snow
tradersnow22@gmail.com

Xenia Shape
xenia.shape@gmail.com

ABSTRACT

The widespread adoption of decentralized finance (DeFi) has been hindered by limited interoperability between different blockchain networks, creating a demand for effective cross-chain solutions. Current popular bridging solutions are often centralized, introducing significant security and censorship risks. Decentralized alternatives, such as atomic swaps, suffer from poor user experience (UX). Thus, there remains a critical need in the market for a truly decentralized, operator-free, and governance-free protocol.

To bridge these gaps, 1inch presents Fusion+. Inspired by the concept of atomic swaps, this protocol improves the model with auctions and signature-driven operations to streamline user interactions. Supporting implementation across major L1 and L2 chains, Fusion+ works on top of the 1inch existing intent-based protocols (e.g. Fusion and Limit Order protocol), providing seamless value exchange in a self-custodial manner. This innovation minimizes centralization, boosts efficiency and security (compared to existing bridging methods), and enables direct transactions between users, professional traders and market makers (resolvers) across chains, promoting broader adoption of Web3 technologies.

1 Classic "Atomic Swaps" and Escrow Contract

Atomic swaps enable the decentralized, trustless exchange of digital assets between two parties on different blockchains, requiring no middleman or trusted party. The core innovation behind atomic swaps is the escrow contract powered by Hashed Timelock Contracts (HTLCs), which ensures that the exchange occurs atomically. This means either both parties successfully exchange their assets, or no exchange takes place, maintaining the security and integrity of the operation.

Key components of escrow contract include:

1. **Hashlock:** A cryptographic mechanism in a smart contract where funds are locked using the hash of a secret value. To unlock the funds, the hash preimage (original secret value) must be provided, ensuring the secret is revealed to the recipient. This guarantees that the funds can only be accessed once the correct secret is disclosed, ensuring secure operation.
2. **Timelock:** A condition in a smart contract that sets a specific time frame within which an action must be completed. If the action, such as claiming funds in an atomic swap, is not completed within this predefined period, the contract recognizes the operation was canceled, ensuring the locked funds are returned to the original owner. This prevents the assets from being stuck indefinitely and provides a clear deadline for the transaction's completion.

Steps in an atomic swap operation:

1. **Agreement and secret generation:**
   - Alice and Bob agree to swap digital assets across two different blockchains (Chain A and Chain B).
   - Alice generates a secret value (S) and computes its hash (H).
2. **Initiation of Swap:**
   - Alice creates an escrow on Chain A, locking her assets with hashlock (H) and a timelock (T1) for Bob as receiver.
   - This escrow ensures Bob can only claim the funds if he provides the secret value (S) within the time limit T1.
3. **Verification and Counter-escrow:**
   - Bob verifies Alice's escrow on Chain A.
   - Bob then creates a corresponding escrow on Chain B, locking his assets with the same hashlock (H) and a shorter timelock (T2) to ensure Alice reveals the secret before T1 expires.
4. **Completion:**
   - Alice claims Bob's assets on Chain B by revealing the secret value (S).
   - The revelation of the secret value on Chain B allows Bob to claim Alice's assets on Blockchain A using the same secret value (S).

Security and Efficiency:

The use of hashlocks ensures that the funds can only be released with the correct secret, while timelocks prevent funds from being indefinitely locked if the swap is not completed. This mechanism ensures a trustless and secure method for cross-chain asset exchanges, eliminating the need for intermediaries while increasing decentralization.

2 1inch Fusion+

1inch Fusion+ offers several key benefits over classic atomic swaps.

First, it simplifies the process by allowing the user, referred to as the maker, to sign the 1inch Fusion order, enabling the taker to handle everything. This eliminates the need for the maker's active involvement, thereby improving the overall UX of the exchange.

Second, it consists of a 1inch Fusion order, which inherently uses the Dutch auction mechanism. This allows users to receive the best rates by taking advantage of the competition among 1inch resolvers. This competition incentivises resolvers to provide the most favorable terms, ensuring users receive optimal value for their swaps.

Finally, to address any potential unresponsiveness, 1inch Fusion Atomic Swaps employ 1inch resolvers. These resolvers can step in to complete the transaction if either party becomes unresponsive after a timeout, ensuring the operation is reliably and securely finalized.

2.1 Hashlocks with 1inch Fusion order

At the core of 1inch cross-chain swaps is the 1inch escrow smart contract. It handles escrow and token transfers. To achieve cross-chain functionality, a copy of this contract is deployed on each participating chain.

To simplify the process for the maker, all deposit and withdrawal operations are executed by the taker, known as the "1inch resolver" or "resolver." Resolvers are entities that have passed KYC/KYB procedures and have legally enforced agreements with 1inch Network. Additionally, the protocol enables resolvers to conduct withdrawals from escrow on behalf of the maker, directly to the maker's account, by using the secret (after its revelation). A target withdrawal address defined during the escrow creation makes it possible to limit withdrawals to one specific address.

The protocol workflow is divided into 4 phases, involving two key participants: the maker, who initiates the swap, and the resolver, who executes the process. If any issue arises throughout the process, an alternative 4th “Recovery phase” exists as a precautionary measure. See Figure 1 for details.

Phase 1: Announcement phase

1. The maker signs and issues a 1inch Fusion atomic order and secret hash to the 1inch Network, signaling their intent to make a cross-chain swap.
2. The relayer (1inch service) shares the 1inch Fusion order with all resolvers, and the Dutch auction begins. The price decreases over time until it becomes profitable for a resolver to take the order, at which point it becomes fixed when that resolver creates the source chain escrow.

Phase 2: Deposit phase

3. The resolver deposits the maker's tokens into the source chain escrow contract. The escrow incorporates the secret hash, token type and amount, target address, and timelock specifications for both chains.
4. The resolver deposits the taker amount into the escrow contract on the destination chain, employing the same secret hash and providing relevant escrow details.

Phase 3: Withdrawal Phase:

5. The 1inch relayer service ensures that both escrows, containing the required token and amount, are created, and the finality lock has passed, and then discloses the secret to all resolvers.
6. Utilizing the secret, the resolver unlocks their assets on the source chain, simultaneously revealing the secret to the public.
7. The resolver then uses the same secret to unlock the assets for the maker from the destination chain's escrow, thereby finalizing the swap.

Phase 4: Recovery phase (Optional):

If neither party receives the designated assets on any chain before the timelock expires, any resolver can transfer these assets back to each respective owner.

Additionally, the protocol introduces safety deposit mechanics. When a resolver deposits assets to the escrow, they include an additional amount of the chain's native asset, called a “safety deposit”. The safety deposit goes to the executor of a withdrawal or cancellation transaction. This incentivizes resolvers to perform cancellations on behalf of the maker.

8. The resolver executes cancelation for the source chain escrow to return funds to the maker on the source chain.
9. The resolver executes cancelation for the destination chain escrow, returning their previously deposited assets and safety deposit.

2.2 Secrets handling

Storage: The maker's frontend dApp (or mobile app) stores the secret. This secret is stored on the maker's side

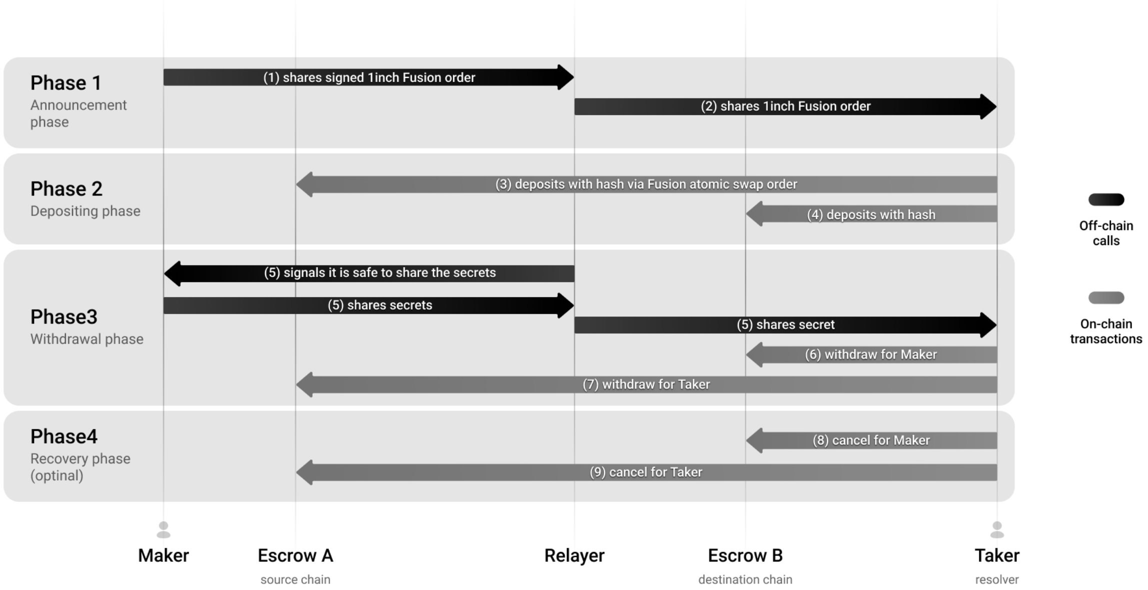

Figure 1: 1inch Fusion+ phases and flows

until resolver signals that escrows are created and then transmitted to the 1inch relayer service to hand it to resolvers.

Conditional transmission: Upon verifying the creation of the escrow on the destination chain, the maker shares the secret with the relayer which then transmits it to all resolvers. Acting as a relay, the service ensures that the resolver receives the secret only after they have fulfilled their part of the transaction.

Trust and convenience: The maker has no need to trust any of the participants since all the data is verifiable on-chain. They receive full automation of the monitoring and transmission process. After initiating the swap, it does not require any additional actions from the maker. The transaction will be completed autonomously once the resolver fulfills their obligations.

Security considerations: The secret is shared after finality locks, which are defined separately for each chain to mitigate potential chain reorganization.

2.3 Dutch Auction

The Fusion+ order price is defined through a competitive Dutch auction. Key parameters for the order configuration include the auction start timestamp, the maximum exchange rate (auction start rate), the minimum return amount (the lowest acceptable exchange rate), and a decrease rate that controls how the exchange rate gradually declines over time. These parameters provide flexibility in configuring the Dutch auction. The parameters description and an example of the current configuration are outlined below.

2.3.1 Auction structure

Each Fusion+ order is executed through a competitive Dutch auction. The auction settings are set by the application built on the protocol and are included in the order when it's created and signed. These key parameters then guide the auction process within Fusion.

Auction start timestamp

This is calculated as the order's signature timestamp plus a waiting period. It determines when the auction officially starts. Any authorized resolver can fill an order with the defined maximum exchange rate before the auction start timestamp.

Waiting period

This delay enables the user to avoid a situation when the auction starts before signing the order, especially for multisig wallets.

Auction start rate

The maximum exchange rate at which a user's order can be filled. Before the Dutch auction process begins, resolvers may fill the order at this rate.

Minimum return amount

This is the lowest threshold of the exchange rate acceptable to the user, below which the order will not be filled. It effectively sets the floor price in the Dutch auction.

Decrease rate

A rate at which the order's exchange rate declines over time once the auction has started. This is a piecewise lin-

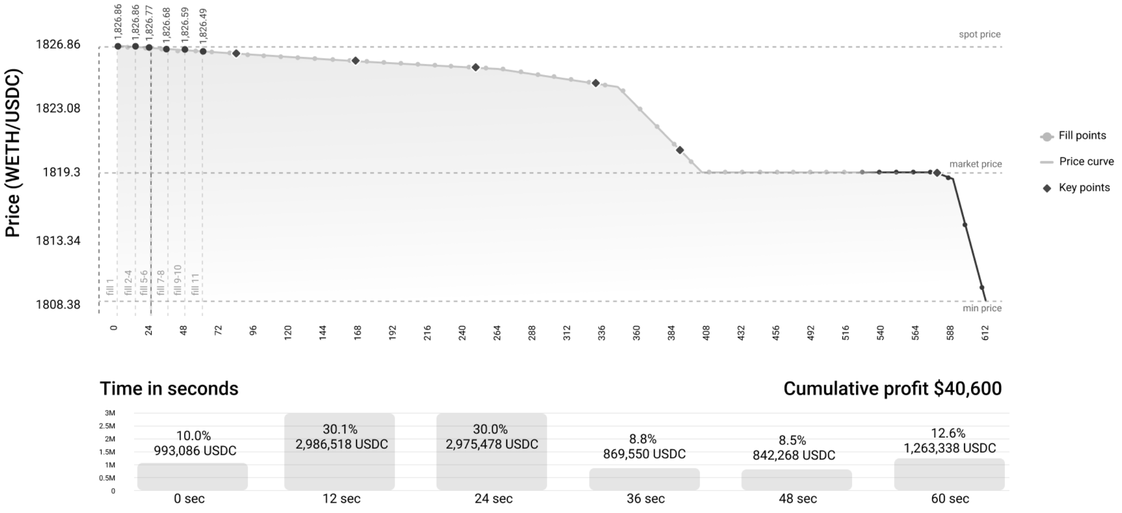

Figure 2: Example of a 5436 WETH to USDC Fusion Swap

ear function, named price curve, included in the order description.

Resolvers compete to fill an order as soon as it becomes profitable for them, otherwise they risk losing the profits to another resolver.

2.3.2 Price curve

The Dutch auction in 1inch Fusion+ orders does not decrease linearly. The auction duration is divided into several segments, each having its own decrease speed, which allows for an increased potential outcome depending on market conditions. The auction configuration is a parameter of the Fusion order. This approach provides flexibility to implement various configuration strategies without making changes to the protocol. Below is an example of an order configuration for 1inch Fusion and Fusion+.

To define the curve for an order, 1inch utilizes a grid approach. Specifically, instead of starting the exchange of X token for Y token at the market price, the auction commences at a market exchange rate of X/6, referred to as the *SpotPrice*.

This methodology involves dividing the outgoing amount into smaller segments and subsequently observing the price at each segment. The outgoing amount X is divided into six equal parts, resulting in the following price points: X/6, 2X/6, 3X/6, 4X/6, 5X/6, and 6X/6.

Throughout approximately two-thirds of the auction duration, the process involves a descending adjustment from the initial *SpotPrice* towards the prevailing market price. This approach, in combination with partial fills, offers more favorable prices and quicker order fulfillment.

2.3.3 Partial fills

The partial fill functionality enables large swaps to be executed even more efficiently, at rates better than current network market, as different resolvers fill different parts of the order. The intent-based approach ensures that the user does not pay any gas fees even if their order expires.

At each point of time the order can become profitable for a resolver, and they can fill it at the price designated by the curve either completely or partially. In case of partial fill, the auction goes on until the fill becomes profitable for the same or another resolver.

Figure 2 illustrates a swap of 5,436 WETH to USDC. Within 1 minute, several resolvers executed 11 partial fills, ranging from 8.5% to 30.1% of the total swap amount in each block. As a result, the user received 40,524 USDC more than if they had swapped the entire amount at once at the current market price.

2.3.4 Price adjustments on gas costs

A change in the gas costs on source chain between signing a transaction and its execution could result in an order expiration due to gas price volatility. In 1inch Fusion+ the price curve is adjusted based on market conditions, if necessary. As a result, orders are executed faster and the probability of an order expiration is lower.

Figure 3 explains how adjusted price influences execution. In a standard auction, if *baseFee* increases, the resolver won't be able to immediately fulfill the order due to the high gas price, and the user might have to wait for a long time for the order to be executed. If *baseFee* declines, the resolver will collect the difference in the gas costs. Possible execution case 1, *baseFee* declined, and the adjusted price curve reacted by increasing the number of tokens the

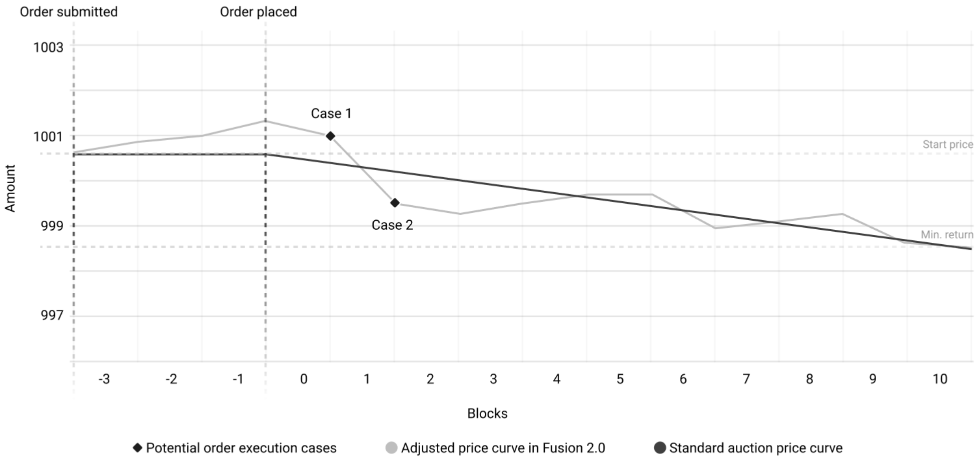

Figure 3: A swap of 1,000 USDT into USDC with gas adjustments

user will receive upon the order execution. In Possible execution case 2, *baseFee* increased, prompting the adjusted price curve to correct the execution costs. As a result, the user won't have to wait until the resolver is interested in fulfilling the order due to a decline in baseFee or a Dutch auction price decline.

2.4 Timelocks

To safeguard all participants from potential asset loss, the protocol incorporates several mechanisms:

- **Finality timelocks** are designed to ensure that chain finality (reorganization attacks) won't affect the swap. The secret is shared at specific points in time and only with the whitelisted/KYCed resolvers.
- **Cancelation timelocks** ensure that all participants can retrieve their funds if a swap cannot be completed. For instance, if the second escrow wasn't created or the secret hasn't been shared for any reason, any participant can withdraw their funds after timelock expiration (known as withdrawal on cancel or cancellation).
- **Swap completion incentives** streamline the withdrawal process and ensure its seamless execution without requiring active involvement of the maker. The protocol implements a safety deposit mechanism that incentivizes resolvers to finalize the swap. A resolver provides a safety deposit when creating an escrow. The party that executes the withdrawal receives this safety deposit which both covers transaction costs and provides an incentive for executing the withdrawal. After sharing the secret, the resolver has a limited time to exclusively complete the swap on the destination chain or execute a cancellation on the source chain.

Refer to Figure 4 for timelocks explanation.

2.4.1 Finality lock

Chain A escrow creation (A1)

A resolver creates an escrow on Chain A (source chain) assuming that the maker has the necessary assets and approvals and adds a safety deposit to the escrow. Upon creation, the Dutch auction price becomes fixed. A finality timelock period is applied to the escrow. At this stage, withdrawals are prohibited, and the secret remains unknown.

Chain B escrow creation (B1)

After or during the finality lock period on chain A, the resolver can create the second escrow on chain B (destination chain) by providing assets and a safety deposit. The lockdown period is applied on chain B as well. The withdrawals are prohibited until finality lock expires.

2.4.2 Hashlock (finality lock expires)

After the lockdown periods on source and destination chains expire, the relayer ensures both escrows were created with the required parameters. It then shares the secret with all resolvers, including the one that sent the proof.

Exclusive withdraw on Chains A and B (A2 and B2)

Upon receiving the secret, the executing resolver has a limited exclusive timeframe to complete the swap and unlock both escrows, transferring the assets to each respective owner and claiming back their security deposits. If the shared secret is invalid for any reason, withdrawal cannot be processed, and both the maker and resolver can retrieve their assets during the cancellation period.

Resolver-exclusive hashlock expires (A3 and B3)

After the resolver's exclusive execution period is over, any resolver can claim the safety deposit on both chains by

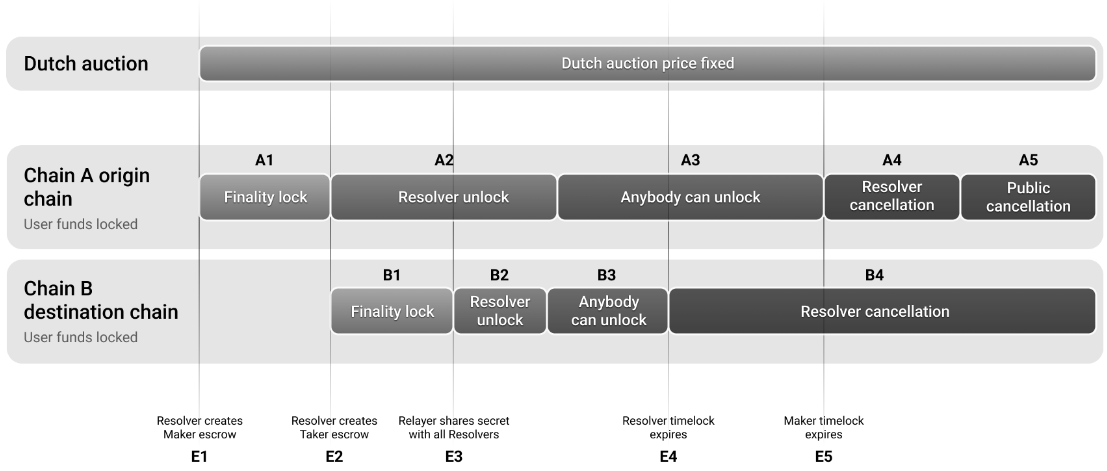

Figure 4: Timelocks sequences

unlocking the escrow and transferring the funds to each respective party.

2.4.3 Cancellation

Chains A and B timelock expires (A4 and B4)

The timelock on the destination chain (chain B) expires, and the resolver can recover their original assets if the key hasn't been shared. The resolver's timelock duration is shorter than the maker's timelock. This arrangement protects the resolver from malicious users, allowing them to recover their assets if the swap has not been completed for any reason.

Chain A exclusive timelock expires (A5)

The timelock on the source chain (chain A) expires, allowing the maker to withdraw their assets. The cancellation period is separated into two parts. At the beginning of the period, only the executing resolver has the ability to cancel the escrow and return the assets to the user, securing their safety deposit. If they don't do that, any of the resolvers can claim the safety deposit, thereby canceling the escrow.

2.5 Partial fills and secret management

When an order is filled completely, a single secret is used to unlock the transaction between the two parties. However, when an order is only partially filled, and multiple participants are involved, revealing the secret to one participant exposes it to all, potentially allowing others to claim the remaining portion of the swap without fulfilling their part.

To overcome this challenge, we've introduced the concept of a Merkle tree of secrets. This method involves splitting the original order into N equal parts. Along with these parts, we generate N+1 secrets. All the secrets are packed into the Merkle tree and the index of the secret in the tree corresponds to the fill percentage. For instance, if the order is divided into four parts (25% each), the 1st secret is required for the first 25% fill, the 2nd secret for 50%, the 3rd for 75%, and the 4th for the full 100% completion. Each part can also be partially filled. In such cases, the next resolver must complete any leftover portion from the previously filled part and at least a portion of one new piece. When secret N has been used and the order hasn't been filled completely, secret N + 1 is used to complete the order.

When a resolver (a participant who fills the order) wants to partially fill an order, they use the appropriate secret based on the current fill percentage and the desired amount of tokens to be filled.

For example, if an order is split into 4 parts (and 5 secrets) and the first resolver intends to fill an order to 20%, they utilize the first secret and fill it up to 20% percent. If another resolver later wishes to increase the order fill by and additional 60% and fill it from 20% to 80%, they would use the 4th secret, and the last resolver to fill the remaining 20% uses the fifth secret.

3 Protocol Settings Governed By DAO

In this protocol, certain key parameters are designed to be controlled by the 1inch Decentralized Autonomous Organization (DAO) to ensure that changes are made in the best interests of the community. The settings controlled by the DAO include:

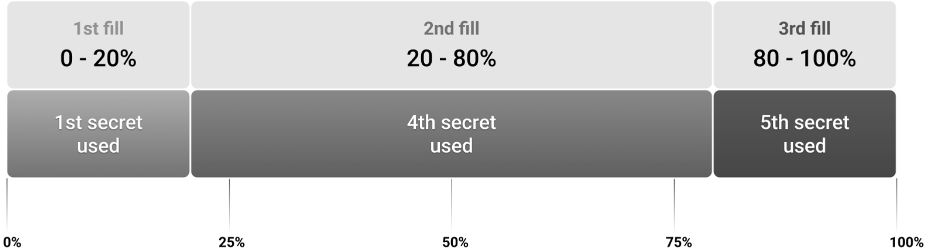

Figure 5: Example of a partial fill

3.1 Maximum swap amount (initial limitation)

Initially, the protocol may set a maximum cap on the swap amounts. This limitation is a risk management strategy designed to protect the ecosystem and its users from potential vulnerabilities or unforeseen market dynamics during the early stages of the protocol's deployment. The ultimate goal is to incrementally ease these restrictions, with the intention of removing them entirely once the protocol has demonstrated its reliability over time.

3.2 Fee structure

Resolver fees: A fee is incurred by resolvers (those who resolve swap orders) in the protocol. The fee is a customizable parameter that can be set to 0 in order to disable fee collection, and can be assigned to any address.

DAO adjustment authority: The specific percentages or amounts of these fees are governed by the DAO. This ensures that fee adjustments can be made in response to changing market conditions, protocol needs or community preferences. This capacity for modification allows for a dynamic and responsive fee structure, aligning with the protocol's long-term objectives and sustainability.

4 Conclusion

The 1inch Fusion+ is an intent-based cross-chain swap protocol that uses Dutch auctions to create a competitive routing marketplace for order resolvers. By utilizing existing 1inch Network products and protocols, it adds flexibility (which classic atomic swap are lacking) and makes the use of the protocol convenient and safe for users.

References

[1] Tier Nolan. Alt chains and atomic transfers. Bitcoin Forum, May 2013. Available: `https://bitcointalk.org/index.php?topic=193281.0`.

[2] Hashed timelock contracts. Bitcoin Wiki. Available: `https://bitcoinwiki.org/wiki/hashed-timelock-contracts`.