As layer 2s and alternative chains gain traction, we have seen a number of new bridging projects. Some examples are nxtp, Hop, Thorchain, Across and Multichain. Considering the high fees users pay to use these systems, we at Magmo wondered how low we could drive down the cost of cross-chain swaps.

The output of our research is SAFE, the Secure Asymmetric Frugal Exchange. SAFE is a simple and efficient technique for batching cross-chain swaps with the following desirable properties:

- Secure — the protocol is as secure as the weakest chain in the swap.
- Frugal — the protocol attempts to minimize the cost of an individual swap.
- Asymmetric — frugality is achieved by batching swaps. Many swap requests on the From Chain are batched and redeemed in one transaction on the To Chain.

While SAFE is a generalized cross-chain swap protocol, the protocol is especially cost-effective in an environment where the transaction fees on the From Chain are lower than the fees on the To Chain. An example of this scenario is a swap from a rollup to L1 Ethereum.

Cost comparison

We used the SAFE prototype to compare SAFE to nxtp, which we chose as it also uses HTLCs. Our comparison focuses on 2 benchmarks. In the first benchmark, 100 unique addresses each swap an asset from Optimism to mainnet. In the second benchmark, the swap is from Optimism to an Optimism clone. Note we assume L1 gas cost of 150 gwei.

nxtp total cost for 100 swaps

SAFE total cost for 100 swaps

Optimism to mainnet

3.78 ETH

0.266 ETH

Optimism to OP clone

1.07 ETH

0.111 ETH

It should also be noted that nxtp is a more feature rich implementation than SAFE. In addition, nxtp contracts are production code whereas SAFE is a prototype. As a result, we expect SAFE costs to increase as feature are added and contracts are hardened. Nevertheless, the initial benchmarks are very promising! Full benchmark data can be found here.

SAFE in a nutshell

Hashed Timelock Contracts are a proven technique for atomic swaps.

[

htlc

1345×781 56 KB

](https://ethresear.ch/uploads/default/original/2X/4/4534be2ea4b34634cdae47a516513cf81583827b.png)

HTLC sequence of calls

SAFE expands on HTLCs by introducing batching. Batching groups many swap requests on the From Chain into one transaction on the To Chain, making SAFE particularly cost effective in asymmetric cost environments. There are 2 roles in SAFE:

1. A customer — the customer wishes to swap assets from the From Chain to the To Chain.
2. A liquidity provider (LP) — the LP holds assets on the To Chain and is willing to trade those assets for From Chain assets (for a fee).

During normal operation, customers continually submit withdrawal tickets to the From Chain. Periodically, a batch of tickets is created and authorized by the LP. The authorized batch is then used to:

1. Distribute batch funds to customers on the To Chain.

2. Transfer batch funds to the LP on the From Chain.

[

safe

2694×789 157 KB

](https://ethresear.ch/uploads/default/original/2X/6/6e05311eb0e9013be51d66048e3404f3727507ae.png)

SAFE sequence of calls

Cost model

In SAFE, the following transactions must take place:

1. The customer submits a single transaction to the From Chain.
2. To service a swap for a customer, the LP must submit two From Chain transactions plus one To Chain transaction. However, the LP may service a batch of n

swaps with this triplet of transactions, amortizing the bulk of the cost across many swaps.

1. In addition, the LP would periodically move funds from the From Chain to the To Chain. We expect these transactions to be infrequent relative to (1) and (2), so these are ignored.

Thus, the customer's swap is serviced with 1 + 2/n

transactions on the From Chain and 1/n

transactions on the To Chain, where n

is the number of swaps serviced per batch.

Safety

SAFE protects customers against a malicious liquidity provider. The customer must have the ability to monitor and submit transactions to both the From and To Chains. The customer is guaranteed that either:

- Their swap is completed, and they receive assets on the To Chain.
- The swap is abandoned, and they reclaim assets on the From Chain.

Details and an informal security analysis are found inthe SAFE spec. Obvious extensions to SAFE can include logic on the From Chain to incentivize good behaviour.

Limitations of SAFE

As described in the spec, SAFE focuses on asset swaps where one asset on the From Chain maps to one asset on the To Chain. Other projects like Thorchain combine AMM and swaps to allow, for example, swapping native Bitcoin to native Ethereum. We have not explored in detail how to add features like this to SAFE.

In addition, our current contracts do not include the necessary checks to prevent common blockchain attacks. This choice is intentional, aiming for clarity and understanding of the core protocol at the prototype stage.