

Basics

Routers are the active liquidity providers & nodes of the Connex network.

How do routers work?

1. Before becoming active in the network, routers provide liquidity on each chain and for each asset they want to support. This liquidity is denominated in nextAssets
2.
 - a Connex-specific unit-of-account that acts as an IOU of locked funds on Ethereum L1.
3. Routers observe all chains in the network. Forxcall
4. s involving their supported chains & assets, routers simulate the transaction on destination, create a bid
5. (a signed transaction that executes the destination chain interaction), and submit that bid to the Connex sequencer
6. .
7. The sequencer waits a fixed period of time to collect bids from routers and then randomly selects from among them. For every batch of transactions, the sequencer will send a corresponding batch of winning bids to a relayer network (e.g. Gelato) to submit the transaction to the destination chain.
8. For router transactions that are submitted by the sequencer immediately (see fast path), the router effectively fronts
9. the transaction funds and call data on the destination, being repaid by the protocol after the slow path completes if they submitted the transaction with the parameters provided in the origin chain
10. xcall
11. .
12. .

Risks

Routers are largely designed to be as passive and safe for operators as possible. However, there are some risks to be aware of:

1. Hot wallet:
2. Routers are effectively a "hot wallet" of funds owned by the router operator that can unilaterally spend owned funds in the protocol. This means that proper key management practices are a must for routers that want to operate in production.
3. Misconfigured environments:
4. Router operators should also ensure that they are careful to not expose the router's private API as part of setting up their environment.
5. Protocol security
6. : As with any protocol, router operators are ultimately exposed to the risk of Connex's underlying implementation. While this risk is never 0, Connex follows best practices for [auditing](#)
7. , [security bounties](#)
8. , and operational practices to keep routers safe.
9. .

Refer to [security.md](#) and [router community call](#) for best practices to mitigate these risks.

Business Model

The router's primary business model is to earn transaction fees for providing liquidity and relaying data across chains.

Routers earn a fee of 5 basis points (0.05%) on all liquidity that is provided for a user transaction. Router liquidity is then subsequently locked up until it can be claimed against the slow path. In effect, this is as if the router is giving a protocol-level loan to the user for a period of up to 2 hours. In this model, router ROI scales with user demand - routers earn the highest returns if a high percentage of their capital is frequently locked up.

Routers currently do not take a fee for relaying data itself. There are future plans to implement an EIP-1559-style tip, that can supplement router income for data-only transactions.

[Previous Supported Chains](#) [Next Spinning Up](#) Last updated 4 months ago On this page * [How do routers work?](#) * [Risks](#) * [Business Model](#)

[Edit on GitHub](#)