Cross-chain bridges and associated risks

When working with Chainlink on layer-2 chains and sidechains, you must export your LINK tokens from Ethereum to the target chain using a cross-chain bridge. Follow thisvideo for an example of moving LINK tokens from Ethereum to Polygon.

Cross-chain bridges come with their own risks. In fact, bridge attacks constitute some of thelargest cryptocurrency hacks by value. When moving your LINK tokens or any asset across chains, understand the risks that you are taking with your assets. Chainlink Labs does not endorse any bridge. Ultimately, you are responsible for assessing the bridge that you use to move your assets.

Read theWhat is a cross-chain bridge ,Trade-offs , andRisks sections to learn more about bridges and trust assumptions in their designs. After you read these sections, you will have a better understanding of bridge risks and which aspects you should evaluate when using a bridge.

What is a Cross-chain bridge

With theproliferation of layer-1 blockchains and layer-2 scaling solutions, the web3 ecosystem has become multi-chain. Each blockchain comes with its own approach to scalability, security, and trust.

However, blockchains are not natively capable of communicating with each other, which makesblockchain interoperability protocols critical for allowing dApps to interact with any onchain network and tap into each blockchain's unique assets and features.

Abridge is a core element of cross-chain interoperability. Bridges exist to connect blockchain networks and enable connectivity between them.

Bridges enable the following:

- Cross-chain transfer of assets and information
- dApps can leverage the strengths and benefits of different chains
- Collaboration between developers from different blockchain ecosystems to build new platforms and products for users

As an analogy, you can usethe blockchains as cities mental model :

- Layer-1 blockchains are like cities.
- Layer-2 solutions are equivalent to skyscrapers. As described in the mental model, “Each rollup is like a vertical blockchain that extends from the ground L1”.
- Bridges are like roads and streets that connect different cities and skyscrapers.

Trade-offs

With the growing number of layer-1 and layer-2 chains, the number of bridges has also grownsurpassing one hundred . So, how do you choose the correct bridge?

When choosing a bridge, there is no perfect solution, only trade-offs. As explained in theinteroperability trilemma andEthereum foundation docs , bridge designs must compromise between the following characteristics:

- Trust-minimization:The system does not introduce new trust or security assumptions beyond those of the underlying blockchains. Readtrust-minimization for more details .
- Generalizability:The system enables the transfer of complex arbitrary data. Data could be messages or assets/funds.
- Extensibility:How hard is it to integrate a new blockchain?
- Latency:How long does it take to complete a transaction?
- Costs:How much does it cost to transfer data across chains via a bridge?

Risks

When choosing a bridge, be aware of the following risks.

Smart contract risks

Bugs and vulnerabilities can expose users' assets to different kinds of exploits. Read thisdetailed analysis for an example of a bridge exploit where the attacker could leverage a logical error in the bridge’s smart contract.

Systemic financial risks

To transfer tokens cross-chain, many bridges lock tokens on the source chain and mint derivative or wrapped tokens on the destination chain representing the locked tokens. A hack of the locked tokens or an infinite mint attack on the wrapped

tokens can make all wrapped tokens worthless and expose entire blockchains to risk.

Early stage

Given that bridges are relatively new, there are many unanswered questions related to how bridges will perform in different market conditions.

Trust-minimization (Counterparty risk)

To overcome cross-chain interoperability challenges, some bridges use offchain actors or validators. These actors introduce new trust assumptions in addition to the underlying blockchain trust assumptions. These bridges act as a custodian and are, therefore, trust-based. In contrast, some bridge designs rely on underlying blockchains' validators and, therefore, do not add any trust assumptions. To summarize:

- Trusted (custodial) bridges require a third party to validate movements over the bridge. Users are required to give up control of their crypto assets, so trust is involved as they rely on the bridge operator's reputation.
- Trustless (non-custodial) bridges leverage smart contracts to store and release funds on either side of the bridge. These bridges are trust-minimized because they don't make new trust assumptions beyond the underlying blockchains.

Trustlessness in bridges does not exist in an absolute form (trusted vs. trustless). As explained in the blockchain-interoperabilityblog , there are four general interoperability solutions for validating the state of a source blockchain and relaying the subsequent transaction to the destination blockchain:

Web2 Verification

Web2 verification is when someone uses a web2 service to execute a cross-chain transaction. The most common example in practice is when users leverage centralized exchanges to swap or bridge their own tokens. The user simply deposits their assets into an address on the source chain that's under the control of the exchange and then withdraws the same tokens or different tokens (via a swap on the exchange) to an address on a destination chain controlled by the user.

Web2 verification can be fairly convenient for personal transactions and requires less technical expertise. However, it is limited only to swapping and bridging tokens which requires trust in a centralized custodian.

External verification

External verification is where a group of validator nodes are responsible for verifying transactions. These validators do not belong to either of the two blockchains' validator sets and they also have their trust assumptions irrespective of the underlying blockchains.

External verification typically requires an honest majority assumption, where a majority of the external validator nodes must behave honestly for the integrity of the cross-chain interaction to be upheld. However, additional techniques can be used to increase trust-minimization, such as:

- Optimistic bridge verification
- Risk management networks
- Cryptoeconomic staking

Despite an additional trust assumption, external verification is currently the only practical way to perform cross-chain contract calls between certain types of blockchains while still providing trust-minimized guarantees. It's also a highly generalized and extensible form of cross-chain computation that is capable of supporting more complex cross-chain applications.

Cryptography risk

Some externally verified bridges are secured by multisig walletsRonin is one example. Multisig wallets are also referred to as m-of-n multisigs, with M being the required number of signatures or keys and N being the total number of signatures or keys (m≤n). This means that an attacker only needs to exploit M keys to be able to hack the whole system. In this case, users must trust that the third party is decentralized enough, signers are independent of each other, and that each signer has proper key management in place. Read thisdetailed analysis for an example of a bridge exploit where the attacker could compromise M keys.

Optimistic bridges

Optimistic bridges rely on honest watchers to monitor the bridges' operations and report any risks. Because the watchers of an optimistic system are permissionless, there is no way to know if there is not at least one single watcher monitoring the system. Therefore, the cost of a successful attack is limitless as it requires an attacker to know who the watchers are and hack all of them.

Here are some examples of externally verified bridges that use different techniques to increase trust-minimization :

- Binance bridge is a trusted bridge using the security standards of Binance.
- Polygon POS bridge uses a proof of stake (PoS) consensus algorithm for network security.
- Nomad is an optimistic bridge. It usesoptimistic verification where messages are optimistically signed on the origin chain and a timeout period is enforced on the destination. During this period, a set of actors called watchers can inspect the messages and flag any detected risks.

Local verification

Local verification is when the counterparties in a cross-chain interaction verify the state of one another. If both deem the other valid, the cross-chain transaction is executed, resulting in peer-to-peer cross-chain transactions. Cross-chain swaps using local verification are often referred to as atomic swaps.

This model has a high level of trust-minimization given reasonable blockchain assumptions, as the swap either happens or both transactions fail. Furthermore, the model works so long as both parties are economically adversarial: they cannot collude to steal funds during atomic swaps.

Note that local verification is not very generalizable to a variety of cross-chain contract calls, and comes with tradeoffs like theinadvertent call option problem — a situation where the second party in an atomic swap can either act or not act on the swap, giving them an inadvertent call option for a certain period of time. Thus, local verification is mostly used in cross-chain liquidity protocols involving liquidity pools that exist independently on each chain.

Hop or Connext Legacy are examples of locally verified bridges.

Native verification

In this design, the validators of the destination blockchains are responsible for verifying the state of the source blockchain to confirm a given transaction. This is typically done by running a light client of the source chain in the virtual machine of the destination chain or running them both side-by-side. Native verification is the most trust-minimized form of cross-chain communication, but it is more expensive, offers less development flexibility, and is more suited to blockchains with similar state machines, such as between Ethereum and EVM-based layer-2 networks or only among Cosmos SDK-based blockchains.

TheNEAR Rainbow Bridge is an example of a natively verified bridge. A smart contract with Ethereum light client functionality is deployed on the NEAR blockchain and a smart contract with NEAR protocol light client functionality is deployed on Ethereum. These light clients hold the latest block headers and verify that cross-chain transactions are done across both chains. The trust model relies only on Ethereum and Near validators.