Stellar

Starbridge

A trust-minimized bridge between Stellar and other blockchains.

Leigh McCulloch

Hi everyone,

I'm going to give you a look into the design of Starbridge.

Starbridge is a trust-minimized bridge between Stellar and other blockchains, initially Ethereum.

Now, I'm giving this talk today, but this design is the result of the ideas of a few folks here at SDF.

Stellar

Starbridge

A trust-minimized bridge from Stellar to other blockchains.

Leigh McCulloch • Nikhil Sariff • Tomer Weller • Nicolas Barry • Siddharth Suresh

So I want to acknowledge them:

- Nikhil
- Tomer
- Nicolas
- And Siddharth

Stellar

Why bridge?

Why would we build a bridge?

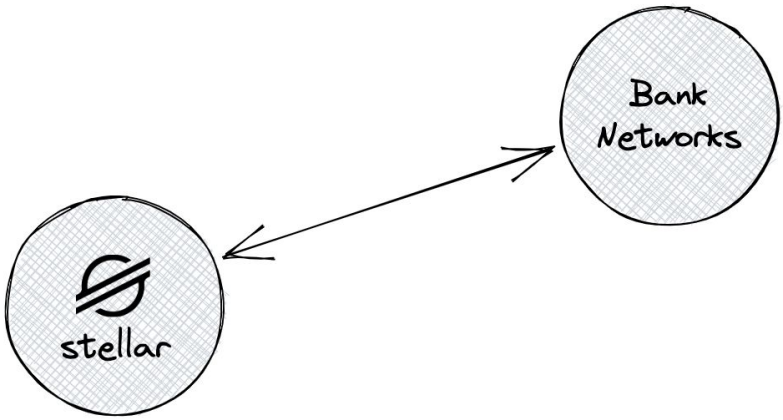
Stellar doesn't exist in isolation.

For Stellar to continue to be successful it needs to have ways to onboard value. Onboarding value requires there being a way to take assets, like USD, from the existing payment networks and getting it on to Stellar.

TRANSITION: Stellar has a great story for this when it comes to non-blockchain networks, like … banking networks, through the anchor network that is growing.

Stellar

Why bridge?

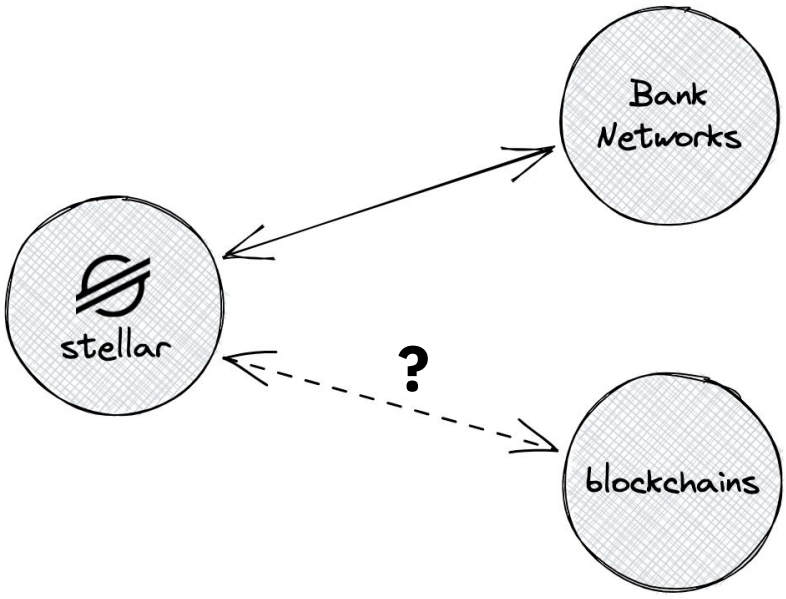


TRANSITION: Stellar has a great story for this when it comes to non-blockchain networks, like … banking networks, through the anchor network that is growing.

TRANSITION: But over the last few years … blockchains have become a part of global financial networks.

Stellar

Why bridge?



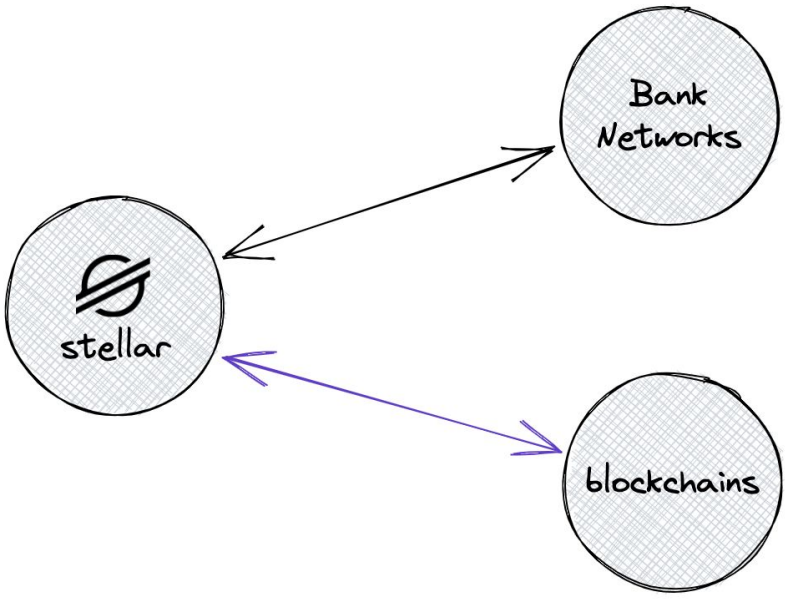
But over the last few years … blockchains have become a part of global financial networks.

And Stellar doesn't have a trust-minimized story for how it connects to blockchains.

Today the story we have is the anchor network, which means a centralized trusted entity custodying assets on Stellar and on the blockchain, and issuing a corresponding wrapped token on the other.

Stellar

Why bridge?



6

STELLAR DEVELOPMENT FOUNDATION

And we hope this will have a couple affects:

1. A usable bridge.
2. That will fill the gap between now and when Stellar has smart contracts and might be more attractive to other bridges.
3. Upskill us on what's required to bridge a network like Stellar, so that we at SDF know what we're talking about when it comes to connecting with other blockchains.

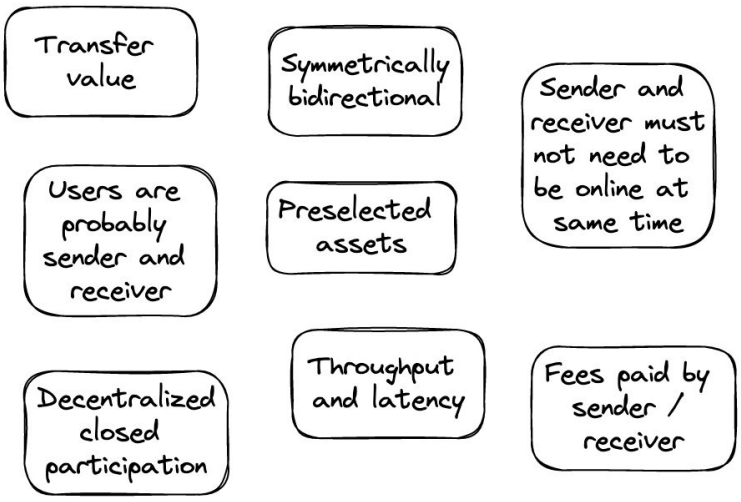
Stellar

Requirements

These are a rough high-level of the requirements we set to satisfy.

Stellar

Requirements



These are a rough high-level of the requirements we set to satisfy.

Stellar

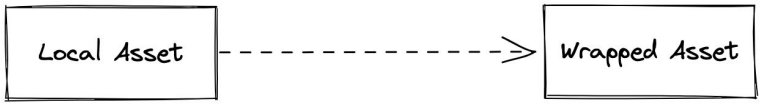
Design

Let’s talk about the design we’re heading towards so far.

We’re going to start with some concepts.

Stellar

Design



The bridge controls local assets and wrapped assets.

Local assets are the assets you'll find on a blockchain that people are using already. Like the Lumen on Stellar.

Wrapped assets are created by the bridge to represent a local asset on a different blockchain.

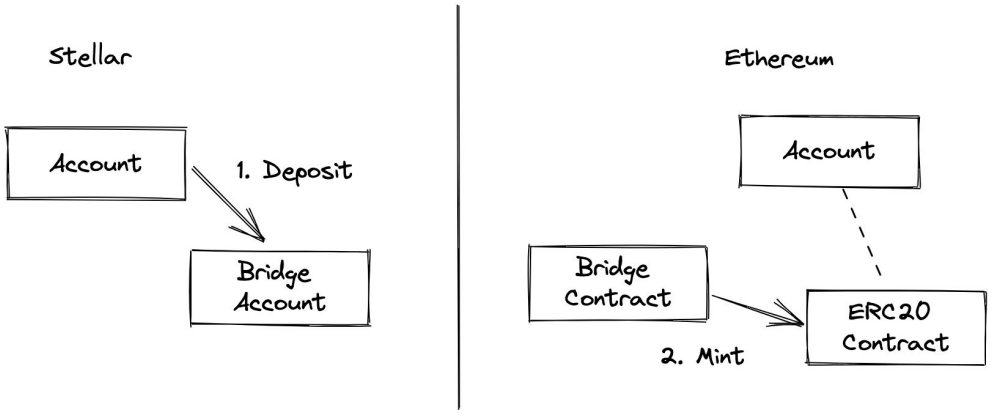
Starbridge uses these assets to perform two different types of transfers.

TRANSITION: The first type of transfer is … a send of a local asset that will be used as a wrapped assets.

Stellar

Sending a local asset that may be used as a wrapped asset

Design



TRANSITION: The first type of transfer is … a send of a local asset that will be used as a wrapped assets.

In this transfer an account will deposit into the bridge a local asset, and the bridge will hold onto that asset.

It's common to say in this situation that the deposited amount is locked up in the bridge.

If you look at stats for bridges TVL is a common measurement for success, and stands for total-value-locked. The more deposits, the higher the TVL.

The result of a deposit will be a mint of a wrapped asset on the other side.

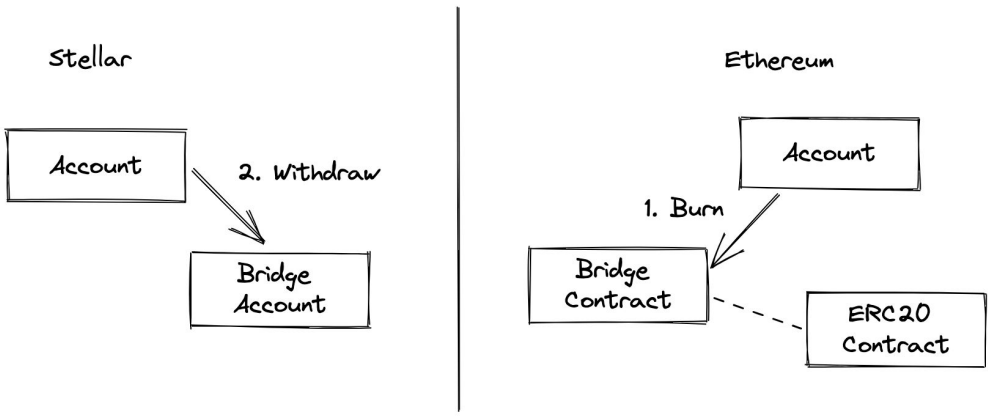
In all these diagrams it doesn't matter which chain is the sender or receiver, so you can imagine them in reverse as well.

TRANSITION: The second type of transfer is … a return of a wrapped asset that unlocks a local asset.

Stellar

Returning a wrapped asset that unlocks a local asset

Design



TRANSITION: The second type of transfer is … a return of a wrapped asset that unlocks a local asset.

The account holding the wrapped asset will burn the wrapped asset.

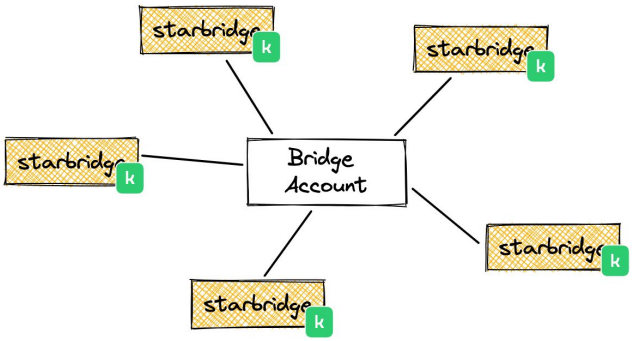
And the account on the other chain can withdraw, or unlock, the local asset.

TRANSITION: When local assets are deposited into the bridge, they're … locked up in an account.

Stellar

Design

Bridge account with m-of-n signers



TRANSITION: When local assets are deposited into the bridge, they're … locked up in an account.

The bridge account is controlled by a group of starbridge operators.

Each starbridge operator holds their own unique key, and together they control the bridge account.

They control the account together using an m-of-n signer setup.

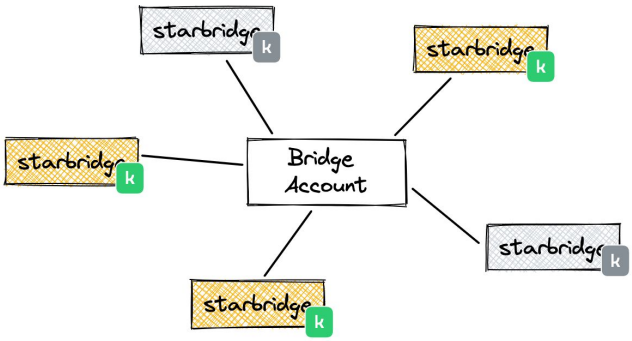
When we say m-of-n we mean there is some number of signers, n, who can authorize transactions.
And for a transaction to be authorized a subset of those signers, m, must sign.

TRANSITION: For example, if the signer configuration is 3-of-5 … any 3-of-the-5 signers need to sign to authorize.

Stellar

Bridge account with m-of-n signers

Design



TRANSITION: For example, if the signer configuration is 3-of-5 … any 3-of-the-5 signers need to sign to authorize.

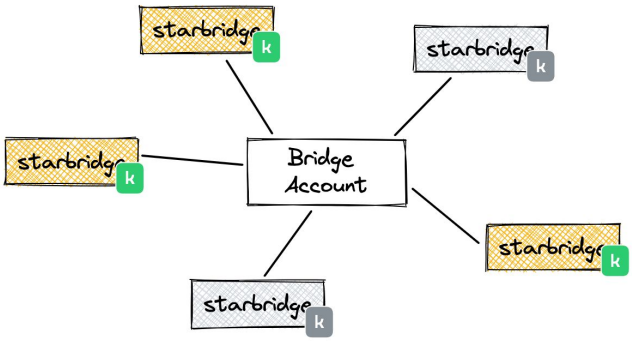
<next slide animation>

This means there's some tolerance to failure. And tolerance to bad behavior.

Stellar

Bridge account with m-of-n signers

Design



TRANSITION: For example, if the signer configuration is 3-of-5 … any 3-of-the-5 signers need to sign to authorize.

<next slide animation>

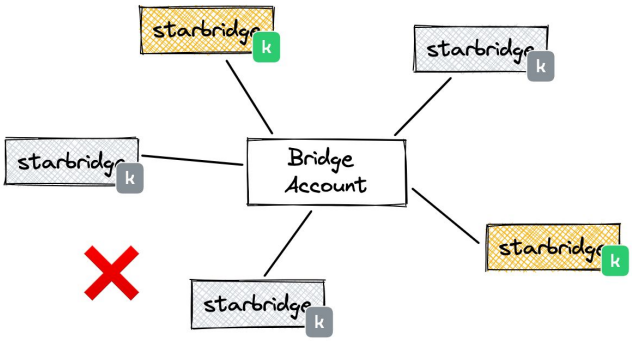
This means there's some tolerance to failure. And tolerance to bad behavior.

TRANSITION: In this configuration if only … 2 sign, the transaction is not authorized.

Stellar

Bridge account with m-of-n signers

Design

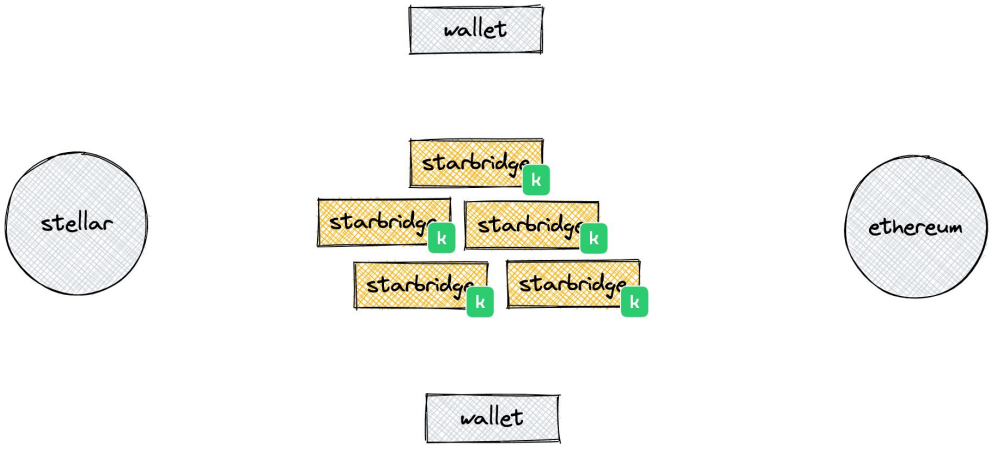


TRANSITION: In this configuration if only … 2 sign, the transaction is not authorized.

TRANSITION: Let's zoom out and walk through how starbridge will make this happen …

Stellar

Design



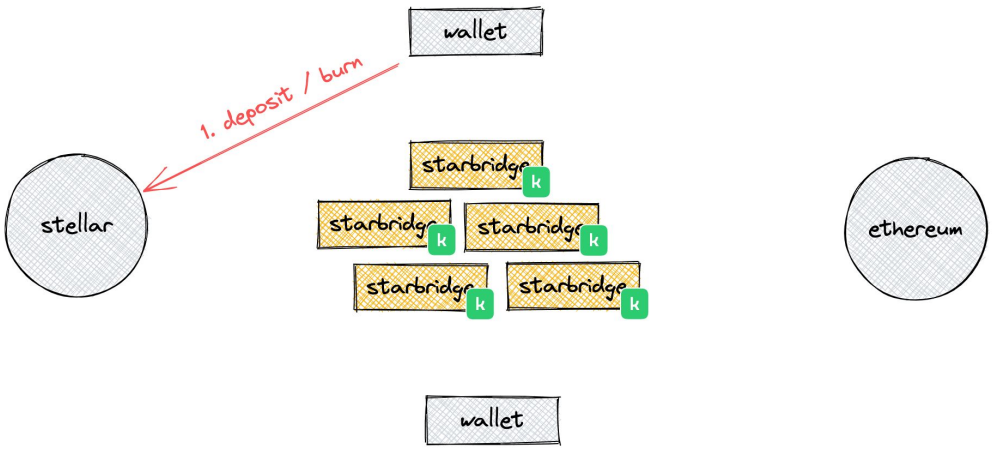
TRANSITION: Let's talk about the components of the system that will make this happen …

In all these diagram we're going to assume there's five entities participating in running starbridge, which is why we have five entities each with a key in the middle of this diagram.

Stellar

Design

Transfer with send and receive

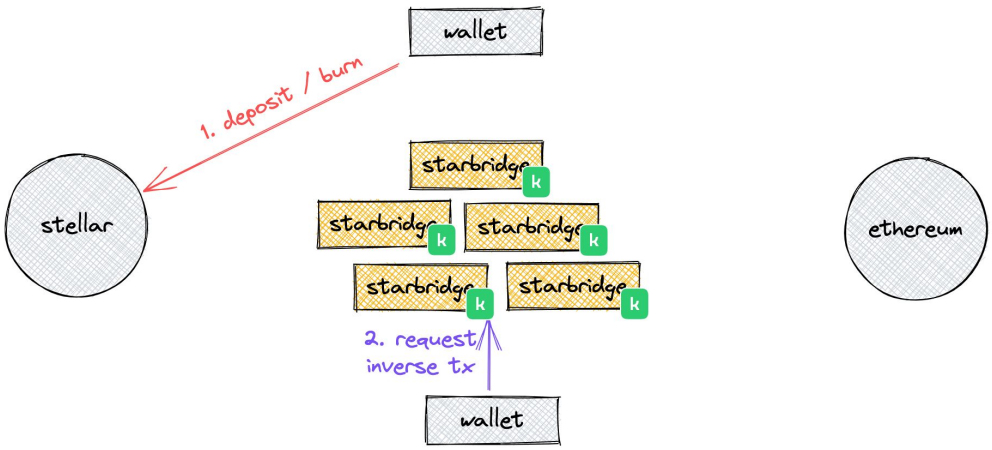


To start a transfer a wallet deposits a local asset into one chain, or if they are returning a wrapped asset, they burn the asset.

Stellar

Design

Transfer with send and receive

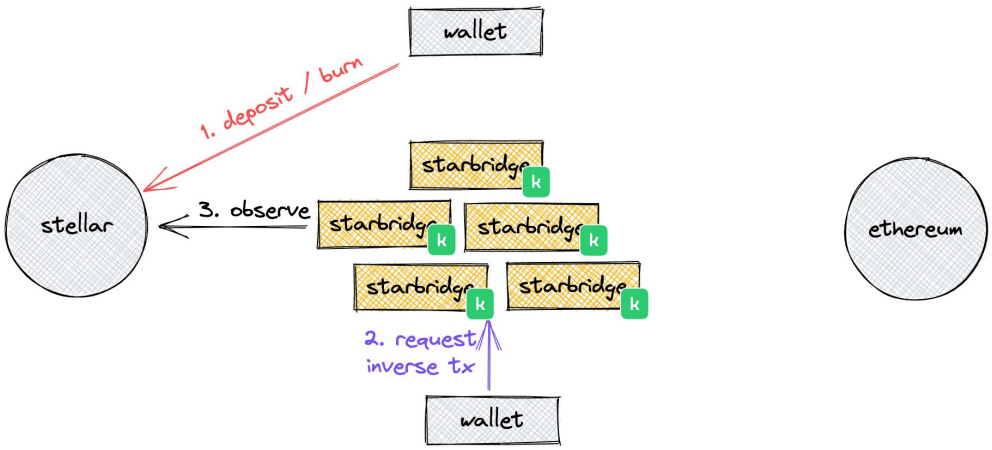


The receiving wallet requests the starbridge network replicate the deposit onto the other chain.

Stellar

Design

Transfer with send and receive

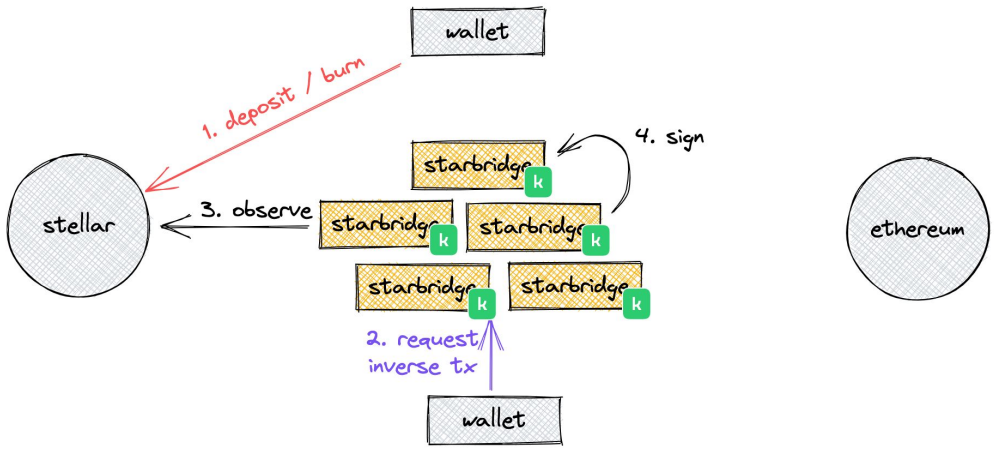


The starbridge nodes all independently observe the deposit on the sending chain.

Stellar

Design

Transfer with send and receive



Once they've observed the event with confidence, they sign the inverse transaction for the destination chain.

Something that might be standing out to you right now is that starbridge hasn't done anything on its own.

A wallet has requested the starbridge nodes to validate a specific operation that occurred on one chain. The starbridge nodes have only acted as a result of that request, and that interaction from the receiving wallet. What we'll see as we continue is that the starbridge nodes do not actually cause replication to occur, they just observe and output signatures when they've been asked to.

This means they require some interaction, which is different to some bridges work. So some bridges work by having the observation and replication occurring naturally without interacting with anyone else. Those bridge design are very elegant.

The reason we have this interaction in the design really comes back to the fact that Stellar is bespoke. We want the receiver to pay the transaction fees, and provide their sequence number on the Stellar network, and to do that we need the starbridge nodes to sign an inverse transaction at the time the transaction is to be submitted, and not earlier.

Technically we don't need this for transactions that flow the other way, to Ethereum. But the overall design is simpler if transfers work the same way in both directions.

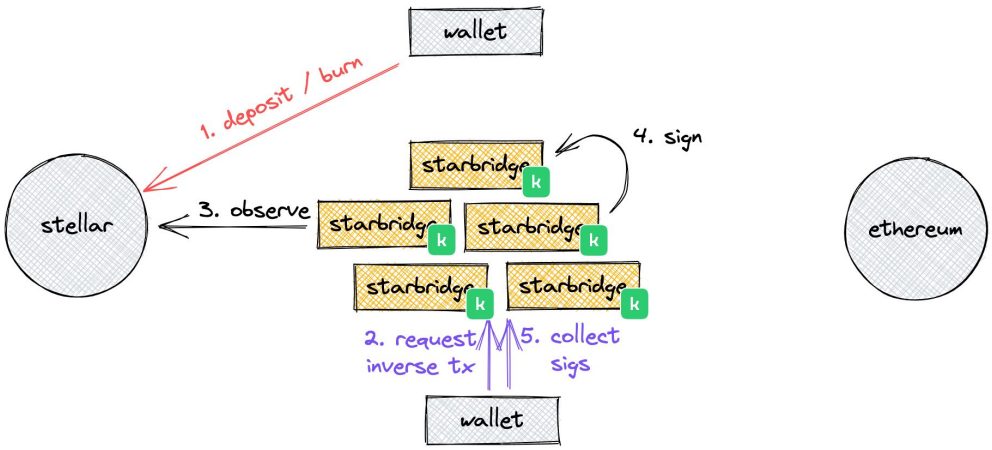
And as a result of this design where we lean into it being an interactive, we can get some additional benefits, like the ability to offer reversals or refunds. Which is a feature that some bridges struggle to implement.

So let’s continue… The starbridge nodes have signed.

Stellar

Design

Transfer with send and receive

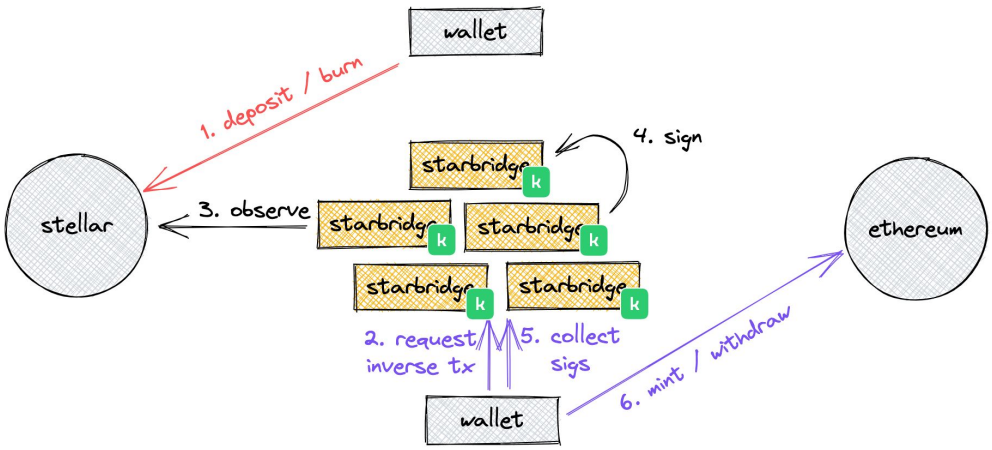


And now the receiving wallet collects those signatures until it has enough signatures to meet the m-of-n requirement of the bridge.

Stellar

Design

Transfer with send and receive



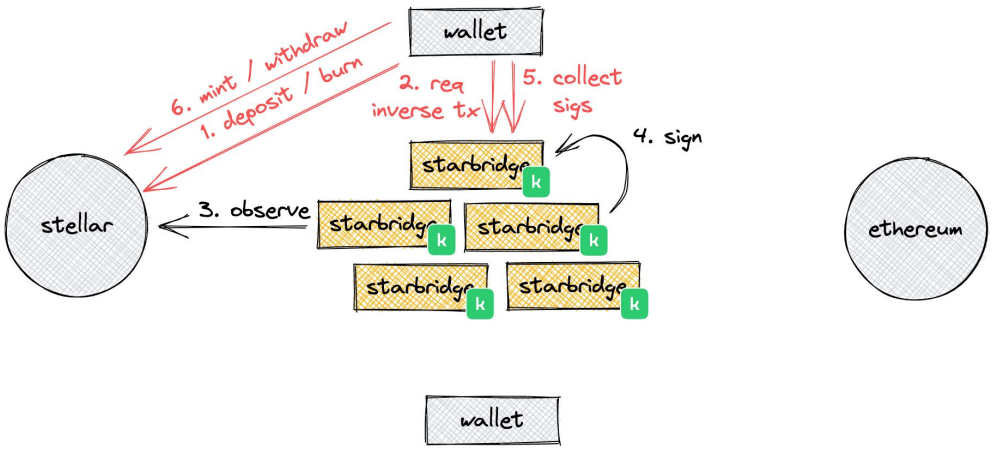
The wallet uses those signatures to submit a transaction or call a contract on the destination chain.

TRANSITION: Starbridge's design will also come with the capability to reverse transfers that can't be completed …

Stellar

Design

Transfer with send and reverse / refund

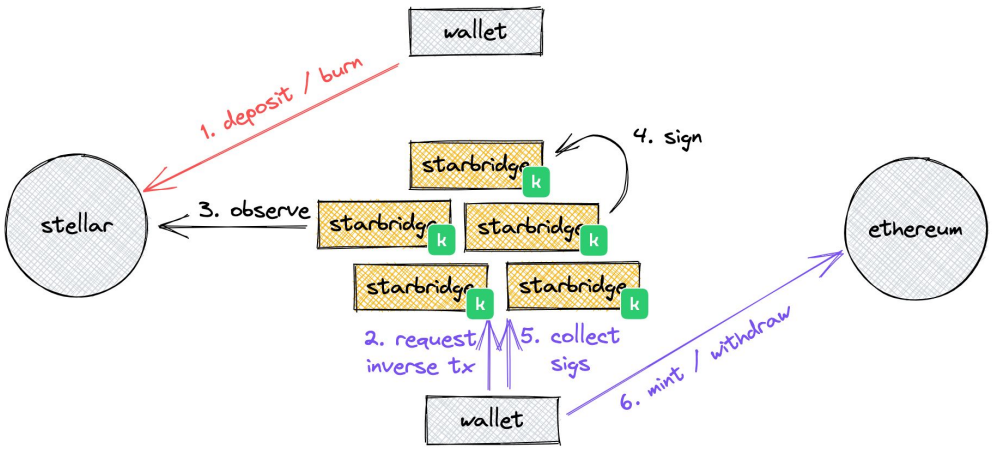


TRANSITION: Starbridge's design will also come with the capability to reverse transfers that can't be completed …

It works much the same like a send would, except the sender becomes the receiver on the same chain.

Stellar

Design



That’s the design we have for how Starbridge is going to work.

Stellar

Find out more at https://github.com/stellar/starbridge/blob/main/doc

Read the design documents at this link.

The docs are relatively lightweight and high-level at this stage, and should be less than 10 minute to read them all.

Questions?