Crosschain Security Considerations for the Degen in All of Us

Layne Haber
Cofounder & Research Lead, Connext
You are collateral damage in the battledome.
Contagion Risk

Bridged Assets
DApps adopt bridged assets, which are 1:1 backed by custodied funds on origin chain.
Contagion Risk

Bridged Assets
DAapps adopt bridged assets, which are 1:1 backed by custodied funds on origin chain.
## Contagion Risk

<table>
<thead>
<tr>
<th>Bridge</th>
<th>Custodied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polygon</td>
<td>$2B</td>
</tr>
<tr>
<td>Optimism</td>
<td>$882M</td>
</tr>
<tr>
<td>Arbitrum</td>
<td>$959M</td>
</tr>
<tr>
<td>Gnosis</td>
<td>$216M</td>
</tr>
<tr>
<td>Avalanche</td>
<td>$1.1B</td>
</tr>
</tbody>
</table>
# How to Lose $2.5B in ~1 yr*

<table>
<thead>
<tr>
<th>Network</th>
<th>Amount</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poly Network</td>
<td>$610M</td>
<td>8/10/21</td>
</tr>
<tr>
<td>Qubit</td>
<td>$80M</td>
<td>1/27/22</td>
</tr>
<tr>
<td>Wormhole</td>
<td>$320M</td>
<td>2/2/22</td>
</tr>
<tr>
<td>Ronin</td>
<td>$625M</td>
<td>3/23/22</td>
</tr>
<tr>
<td>Horizon</td>
<td>$100M</td>
<td>6/23/22</td>
</tr>
<tr>
<td>Nomad</td>
<td>$186M</td>
<td>8/1/22</td>
</tr>
<tr>
<td>BSC</td>
<td>$570M</td>
<td>10/7/22</td>
</tr>
</tbody>
</table>

*not inclusive
Choose your fighter.
Bridge Tradeoffs
Can’t have all the nice things, but can have some
A Taxonomy of Bridges

Natively Verified
Domain's own validators verify txs
Natively Verified
Domain’s own validators verify txs
A Taxonomy of Bridges

Externally Verified
3rd party validators verify txs
Trust-minimized
Generalizable
Extensible
Low-Latency
Trust-minimized
Extensible
Externally Verified
3rd party validators verify txs
A Taxonomy of Bridges

Optimistically Verified
1-of-N watchers prove fraud
Optimistically Verified
1-of-N watchers prove fraud
ZK Bridges: An Aside

Execution of bridge actions are provably correct using validity proofs.
ZK Bridges: An Aside

ZK Bridges
Execution of bridge actions are provably correct using validity proofs.
Enter the Arena.
Types of Security

**Economic**

How much would it cost to corrupt your system?

**Implementation**

How complex is the implementation of your system?

**Environment**

How can your system handle underlying domains with low economic security?
Economic Security
What's your price?

Validator 1

Validator 2

... ...

Validator N

Bridge
Economic Security

Natively Verified
Must corrupt the underlying domain validator set
Economic Security

Externally Verified
Must corrupt the bridge validator set
Economic Security

Optimistically Verified
Must corrupt the entire watcher set
Winner: Economic Security

1st  Native
2nd  Optimistic
3rd  External
Implementation Security

Would it be modeled by a theoretical physicist?
Implementation Security

What are your development processes?
What are the built-in defenses?
Implementation Security

Natively Verified
Unique implementations needed for each domain
Externally Verified
Easily portable between domains, complex off-chain coordination
Implementation Security

Domain A

Domain B

Domain C

Optimistically Verified
Easily portable between domains, minimal off-chain coordination
Winner: Implementation Security

1st Optimistic
2nd External
3rd Native
Environment Security
Can you prevent 51% attacks on underlying domains?
Environment Security

Natively Verified
Verifies underlying consensus
Environment Security

Externally Verified
Delay and off-chain verification easy to add, but not required.
Environment Security

Optimistically Verified
Delay embedded in the protocol
Winner: Environment Security

1st Optimistic

2nd External

3rd Native
YOUR ALL-AROUND CHAMPION IS OPTIMISTIC!!!!
YOUR ALL-AROUND CHAMPION IS OPTIMISTIC!!!!
...but how much does theory really matter tho
Exploit Difficulty

Environment

Economic

Implementation

You are here — Implementation

Difficulty
Security does not exist in a vacuum.
## Common Bridge Shortcuts

<table>
<thead>
<tr>
<th>Whitelists</th>
<th>LPing, watchers, verifiers, assets all commonly exist behind a whitelist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgradeability</td>
<td>Most bridges have some multisig that is able to instantly upgrade parts of their system.</td>
</tr>
<tr>
<td>Centralization</td>
<td>Pausability, centralized supporting components (i.e. not running your own node, centralized messaging)</td>
</tr>
</tbody>
</table>
Practical Considerations

Is this my life now

How long are you exposed to the bridge risk?

Where r ur receipts

How much money has your bridge secured, and for how long? Upgrades reset this.

Who do u kno here

Can you trust the judgment of the team? What is the social signalling?
Thanks, call me

https://jobs.connext.network
discord.gg/connext
@LayneHaber / layne@connext.network