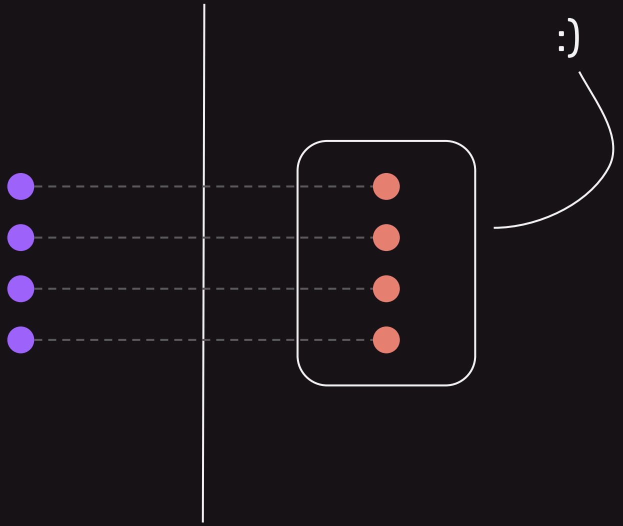
Crosschain Security Considerations for the Degen in All of Us

Layne Haber
Cofounder & Research Lead, Connext

connext

You are collateral damage in the battledome.

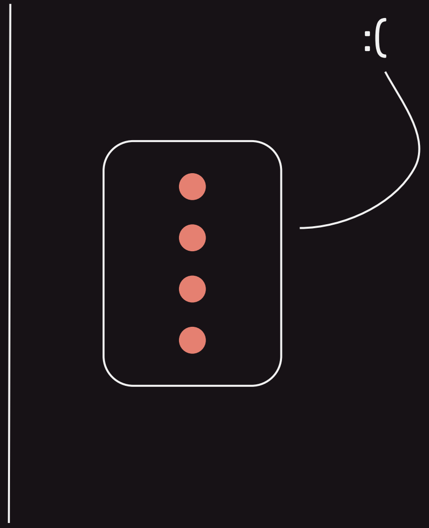
Contagion Risk



Bridged Assets

DApps adopt bridged assets, which are 1:1 backed by custodied funds on origin chain

Contagion Risk



Bridged Assets

DApps adopt bridged assets, which are 1:1 backed by custodied funds on origin chain

Contagion Risk

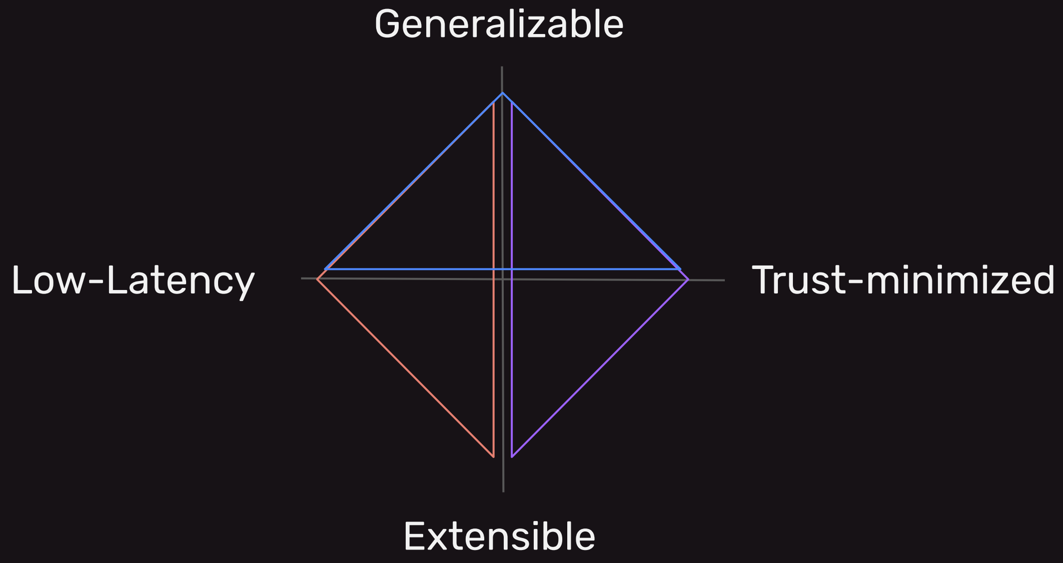
Bridge	Custodied
Polygon	$2B
Optimism	$882M
Arbitrum	$959M
Gnosis	$216M
Avalanche	$1.1B

How to Lose $2.5B in ~1 yr*

Poly Network	$610M	8/10/21
Qubit	$80M	1/27/22
Wormhole	$320M	2/2/22
Ronin	$625M	3/23/22
Horizon	$100M	6/23/22
Nomad	$186M	8/1/22
BSC	$570M	10/7/22

*not inclusive

Choose your fighter.

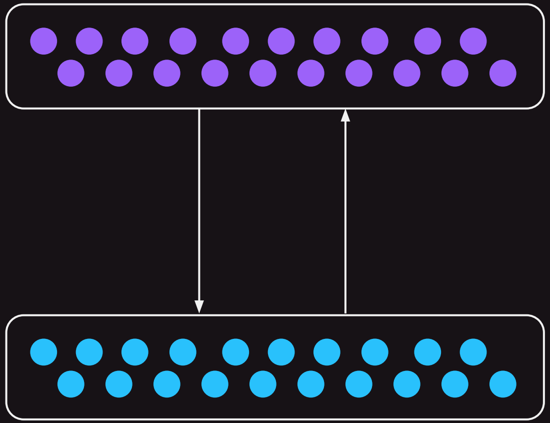


Bridge Tradeoffs

Can’t have all the nice things, but can have some

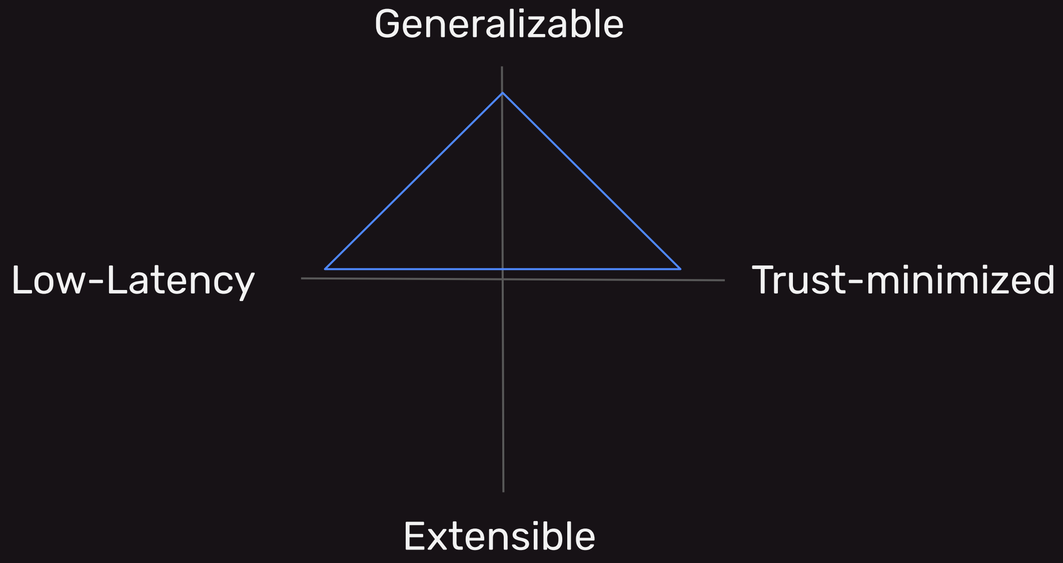
connext

A Taxonomy of Bridges



Natively Verified

Domain’s own validators verify txs

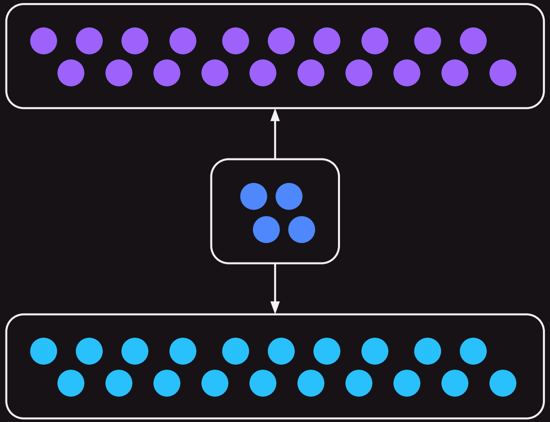


Natively Verified

Domain's own validators verify txs

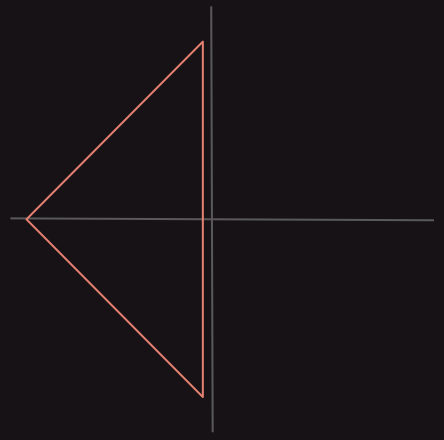
connext

A Taxonomy of Bridges



Externally Verified

3rd party validators verify txs



Generalizable

Low-Latency

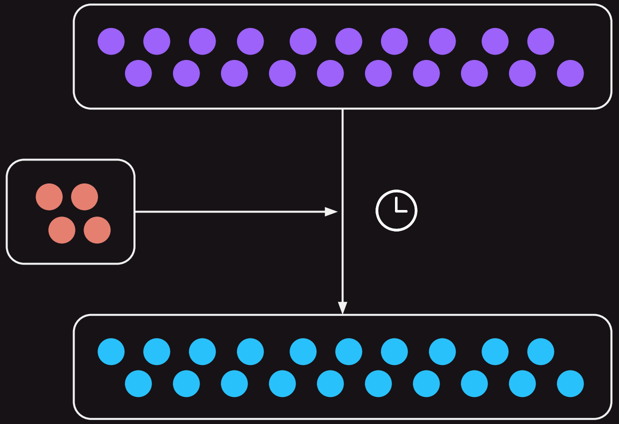
Trust-minimized

Extensible

Externally Verified

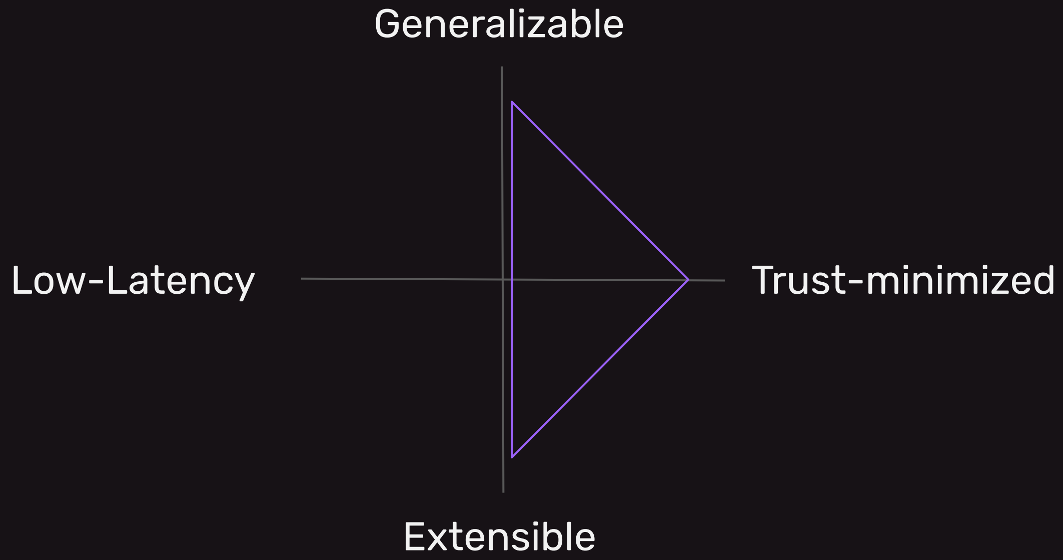
3rd party validators verify txs

A Taxonomy of Bridges



Optimistically Verified

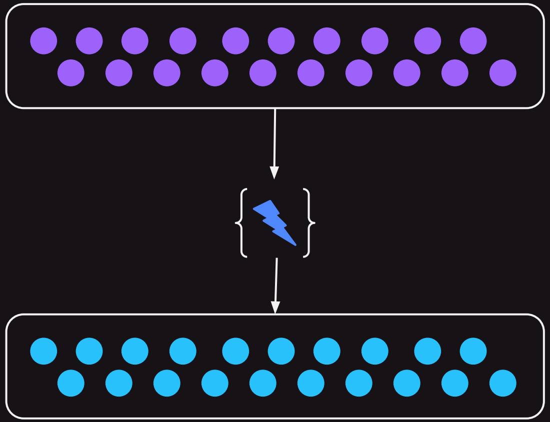
1-of-N watchers prove fraud



Optimistically Verified

1-of-N watchers prove fraud

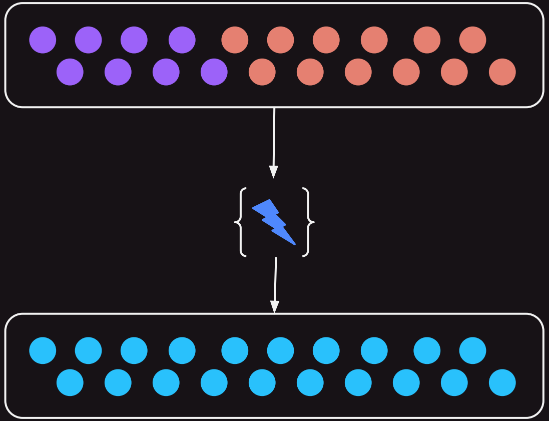
ZK Bridges: An Aside



ZK Bridges

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

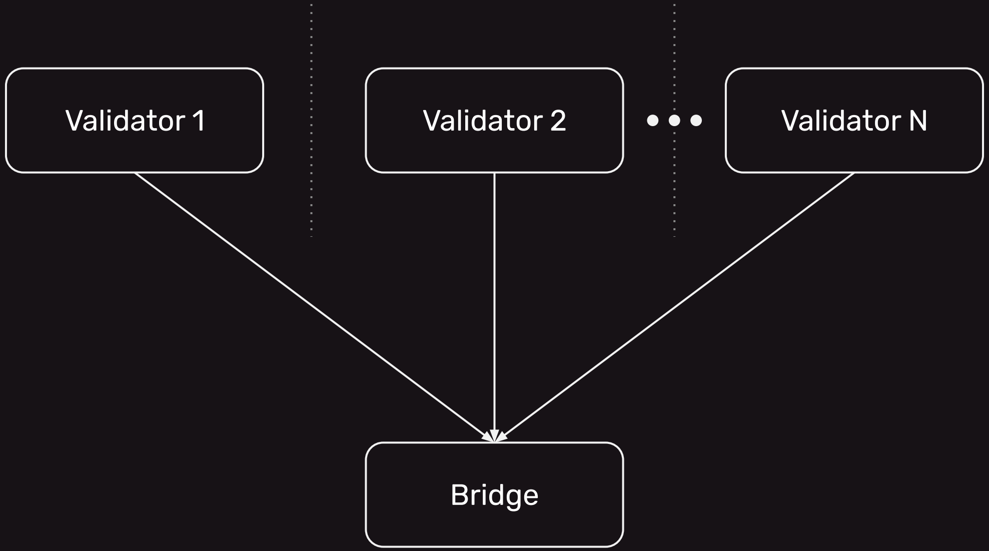
Economic How much would it cost to corrupt your system?

Implementation How complex is the implementation of your system?

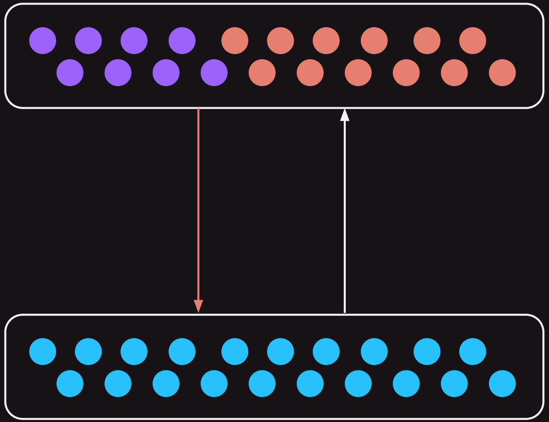
Environment How can your system handle underlying domains with low economic security?

Economic Security

What’s your price?



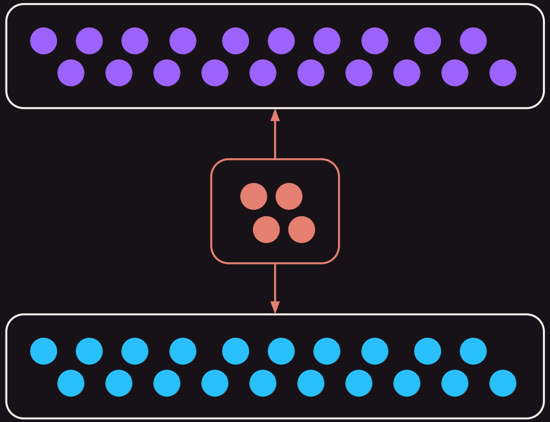
Economic Security



Natively Verified

Must corrupt the underlying domain validator set

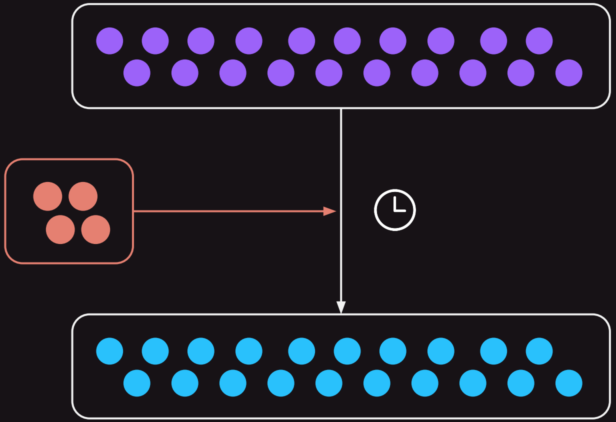
Economic Security



Externally Verified

Must corrupt the bridge validator set

Economic Security



Optimistically Verified

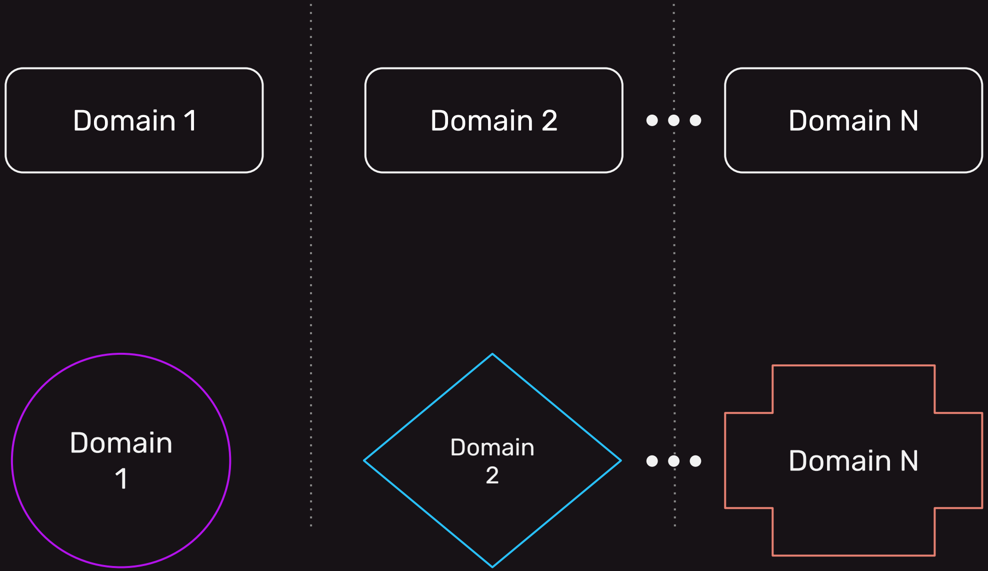
Must corrupt the entire watcher set

Winner: Economic Security

1st	Native
2nd	Optimistic
3rd	External

Implementation Security

Would it be modeled by a theoretical physicist?



Domain 1

Domain 2

Domain N

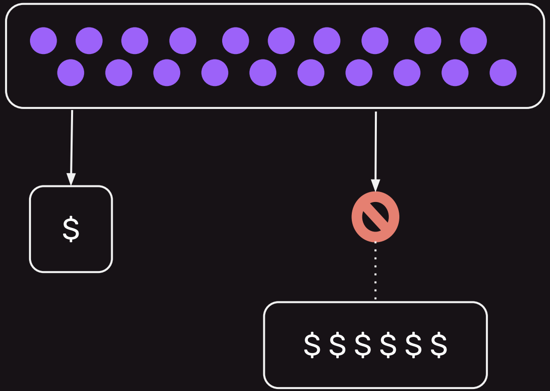
Domain 1

Domain 2

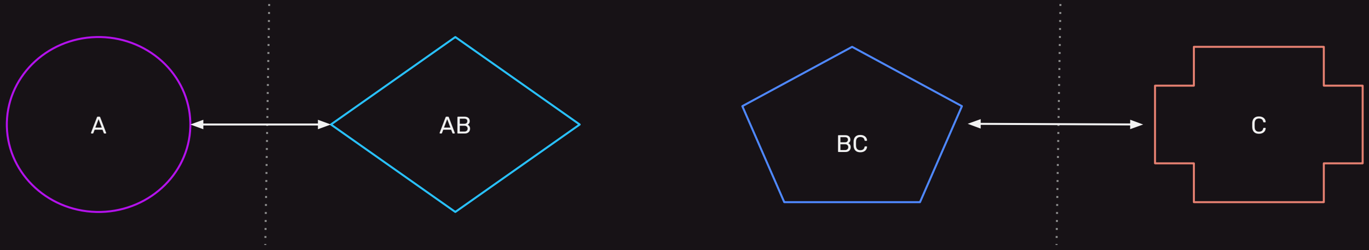
Domain N

Implementation Security

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



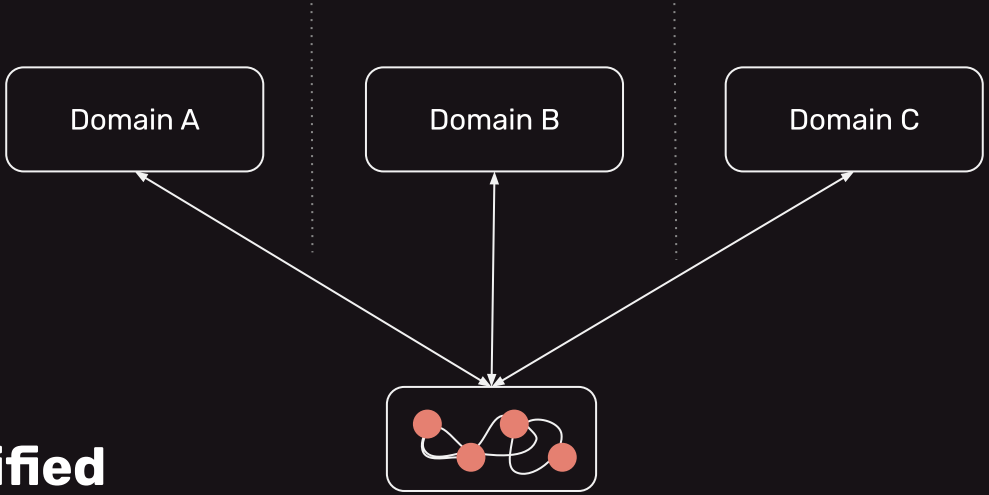
Implementation Security



Natively Verified

Unique implementations needed for each domain

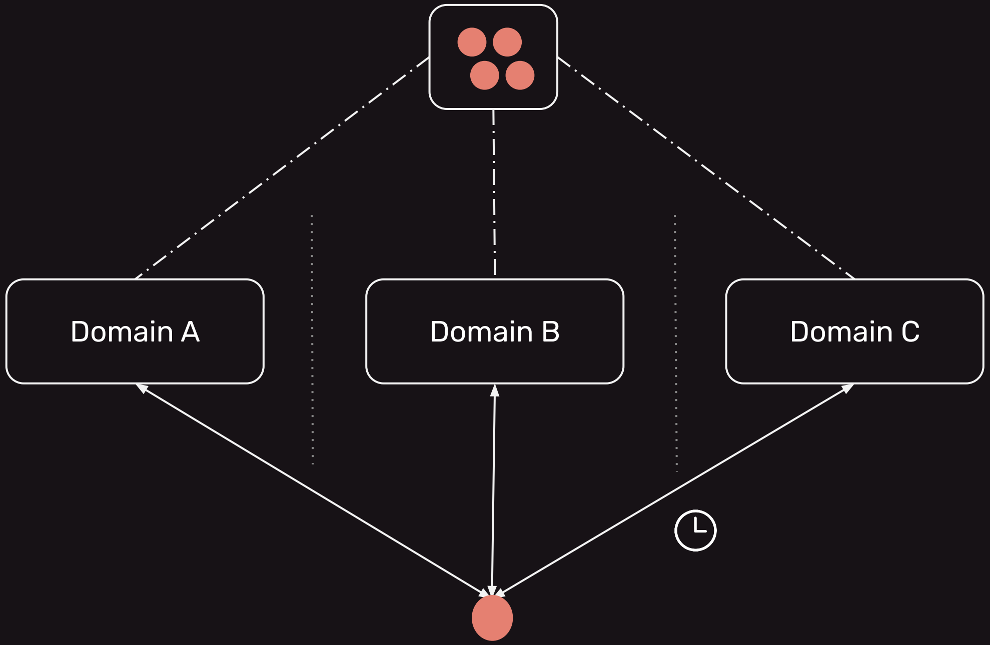
Implementation Security



Externally Verified

Easily portable between domains,
complex off-chain coordination

Implementation Security

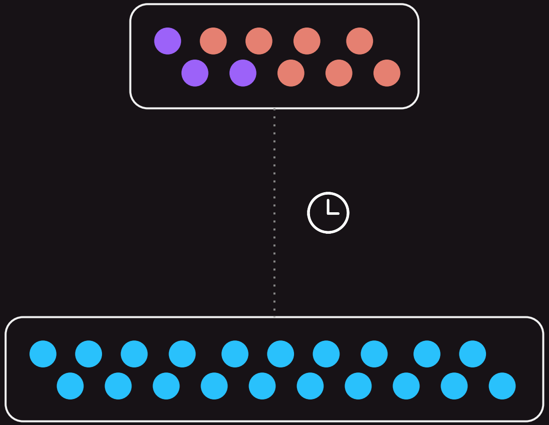


Optimistically Verified

Easily portable between domains, minimal off-chain coordination

Winner: Implementation Security

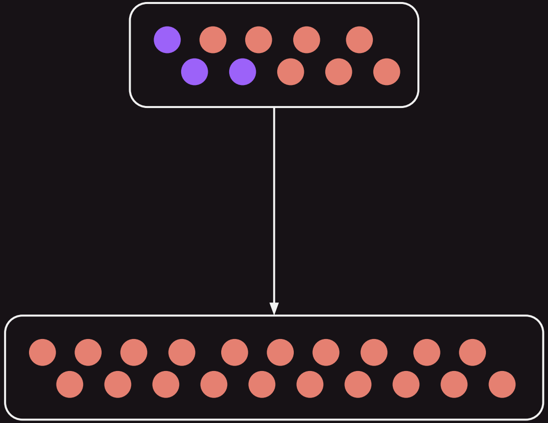
1st	Optimistic
2nd	External
3rd	Native



Environment Security

Can you prevent 51% attacks on underlying domains?

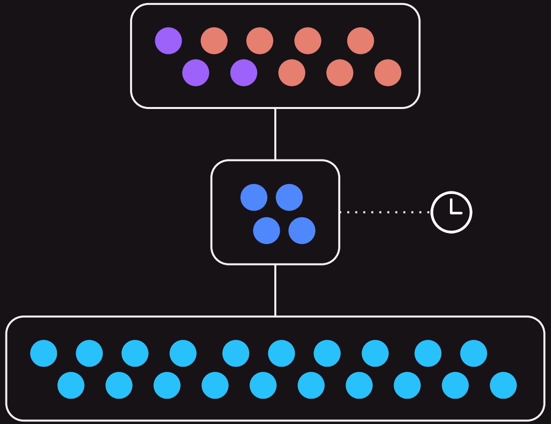
Environment Security



Natively Verified

Verifies underlying consensus

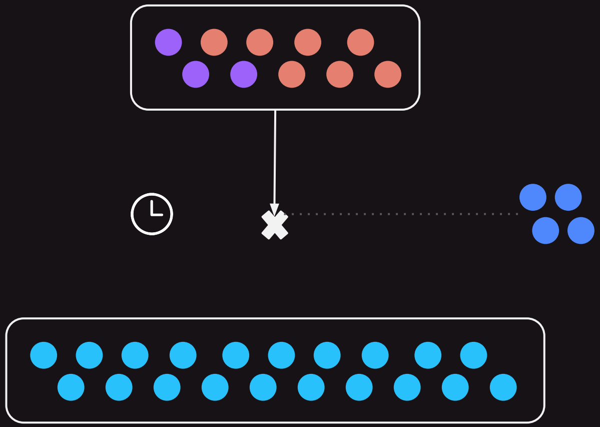
Environment Security



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

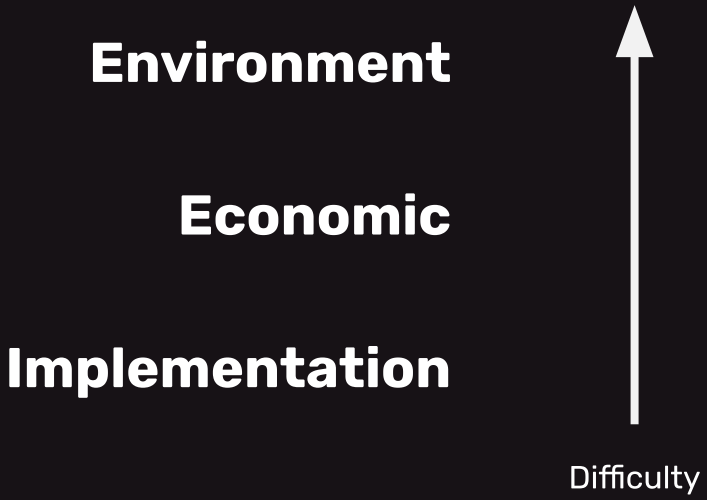
1st	Optimistic
2nd	External
3rd	Native

YOUR ALL-AROUND CHAMPION IS OPTIMISTIC!!!!

YOUR ALL-AROUND CHAMPION IS OPTIMISTIC!!!!

…but how much does theory really matter tho

Exploit Difficulty



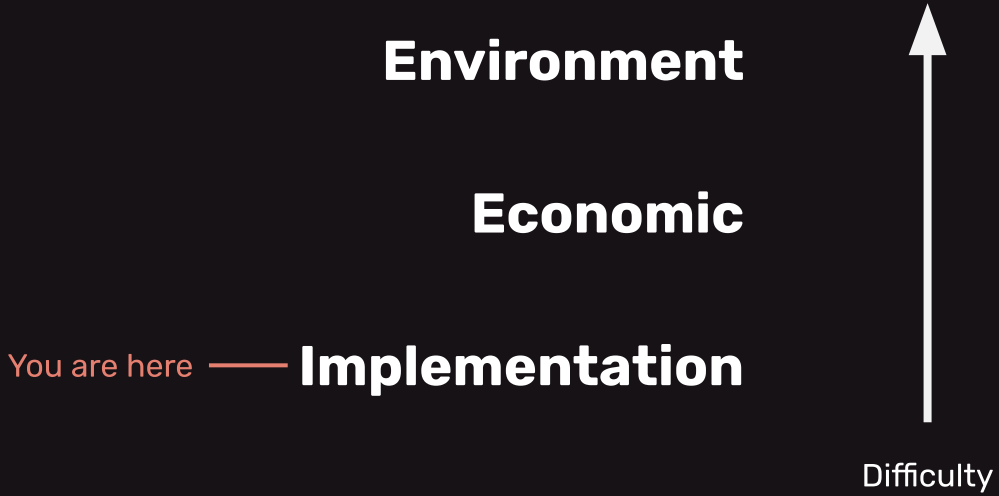
Environment

Economic

Implementation

Difficulty

Exploit Difficulty



Environment

Economic

You are here — Implementation

Difficulty

Security does not exist in a vacuum.

Common Bridge Shortcuts

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

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

connext