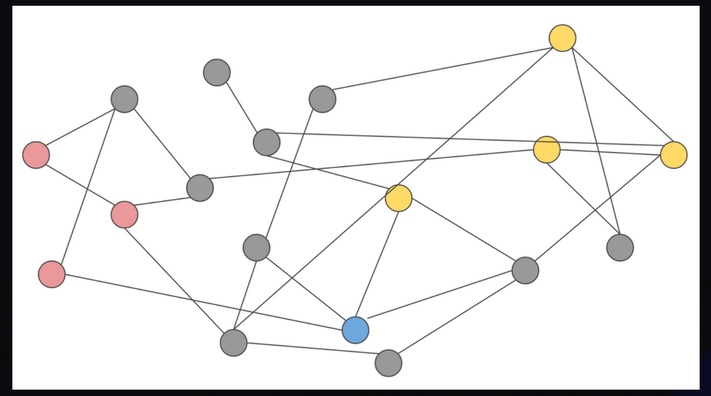


Patterns for Success and Failure in Crosschain Bridge Design

Runtime Verification Security Weekly, 11 January 2024

David Hyland-Wood

Bridge Assessment Report

Search ••• | Try Notion

Bridge Assessment Report

An initiative by UNISWAP FOUNDATION

Bridge Assessment Report

Table of Contents

- Summary
- Introduction
  - Disclaimers
- Current State: How Uniswap Governance Works
- Future State of Uniswap Cross-chain Governance
- Bridge Assessment Methodology
- Bridge Assessment Analysis Overview
- Bridge Assessments
- Architectural Recommendations
- Conclusion
- Bridge Committee Members
- Appendix 1: The Uniswap DAO's Cross-chain Governance Use Case's Requirements and Constraints
- Appendix 2: Multi-bridge Design Considerations
- Appendix 3: Cross-chain Governance Flow
- Appendix 4: Native Bridges Versus Governance Standardization

https://uniswap.notion.site/Bridge-Assessment-Report-0c8477afadce425abac9c0bd175ca382

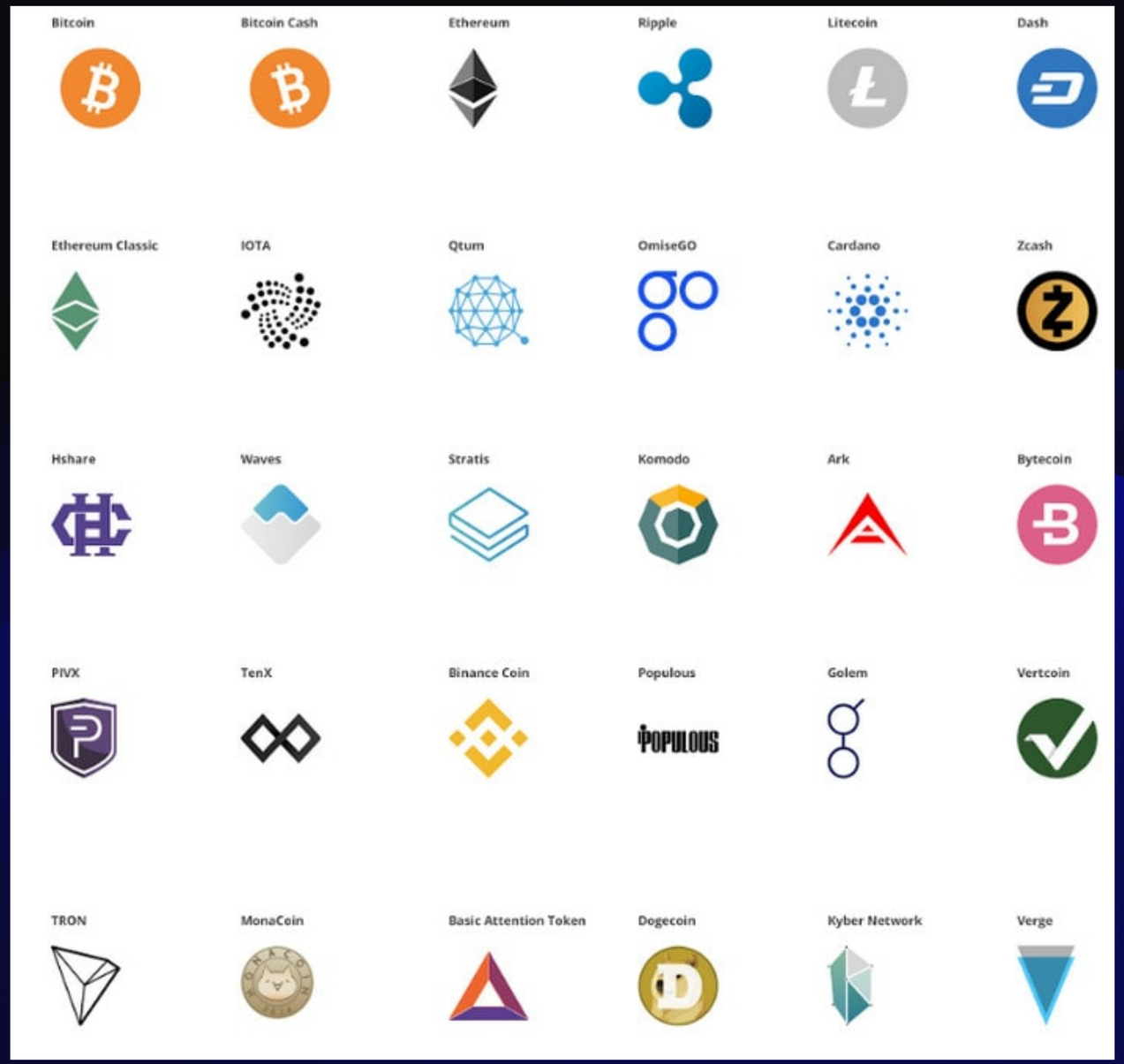
There are *many* blockchains

Quick Answer 🔍

How many blockchains are there in 2023?

There are at least 1,000 blockchains.

https://earthweb.com/how-many-blockchains-are-there/



How can we transfer information and currencies between chains?

- We need some sort of bridge
- These are typically called crosschain (or cross-chain) bridges
- Crosschain bridges may be used to transfer:
  - Cryptocurrencies
  - Messages

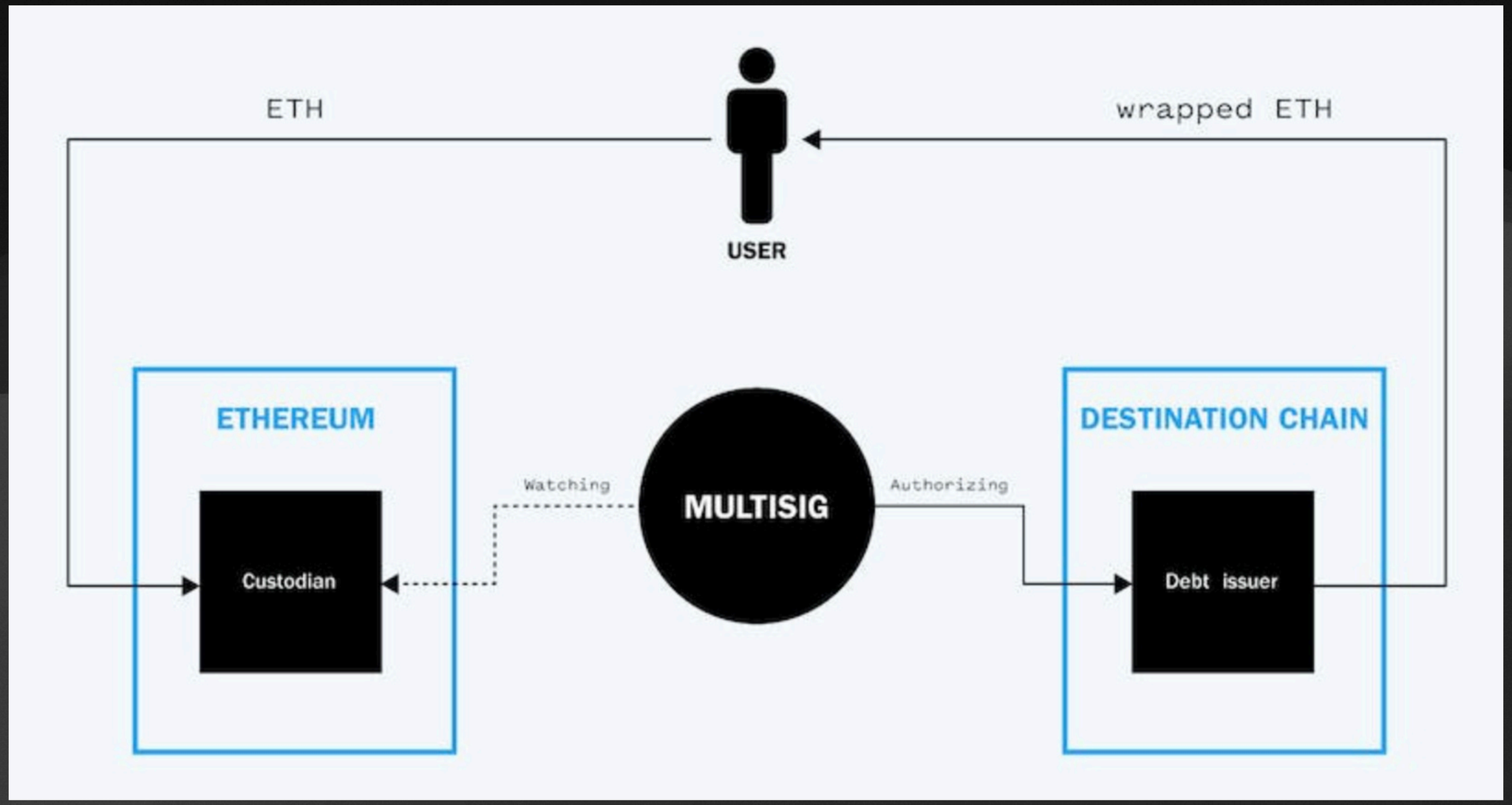
https://www.zeeve.io/blog/what-are-cross-chain-bridges-a-detailed-guide/

How can we transfer information and currencies between chains?

- We need some sort of bridge
- These are typically called crosschain (or cross-chain) bridges
- Crosschain bridges may be used to transfer:
  - Cryptocurrencies
  - Messages

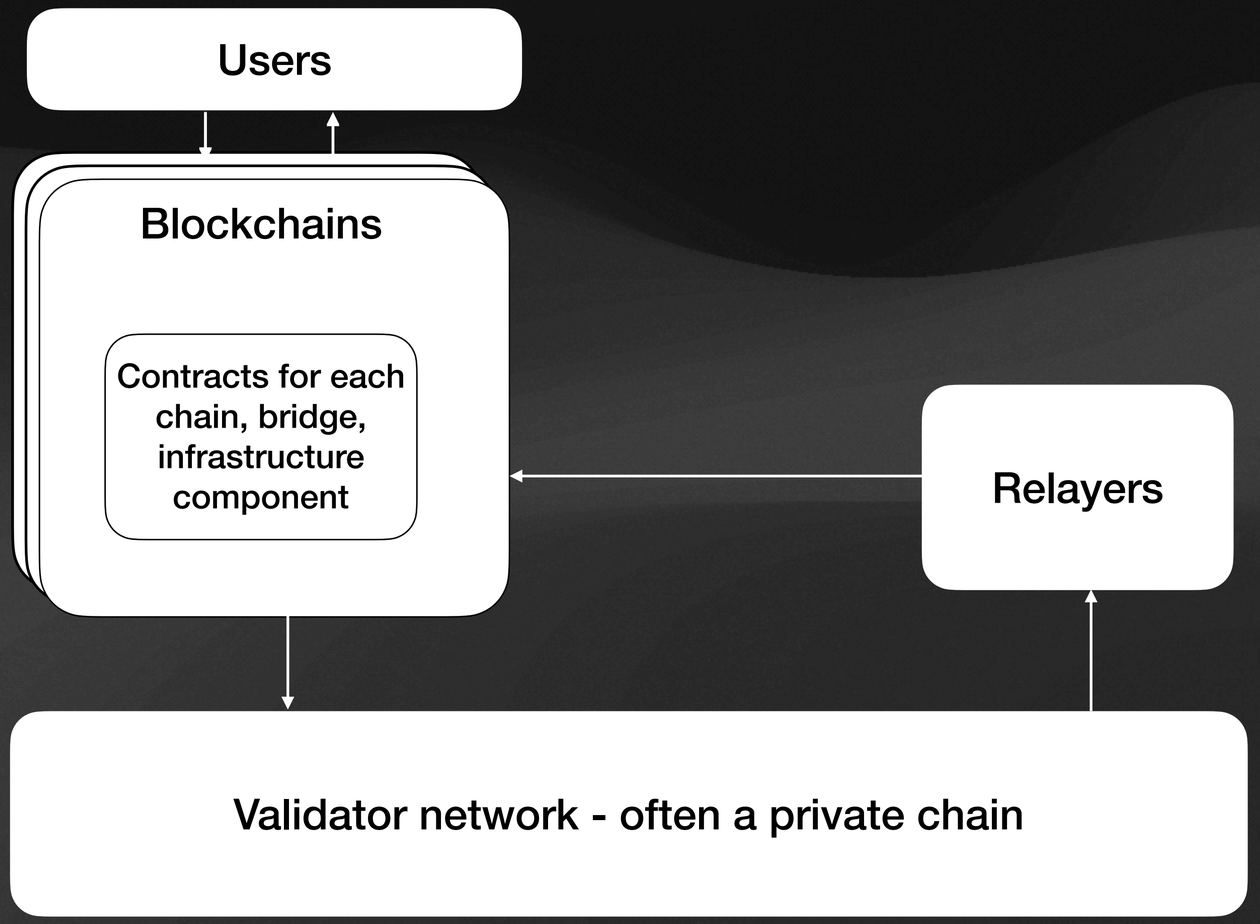
https://www.zeeve.io/blog/what-are-cross-chain-bridges-a-detailed-guide/

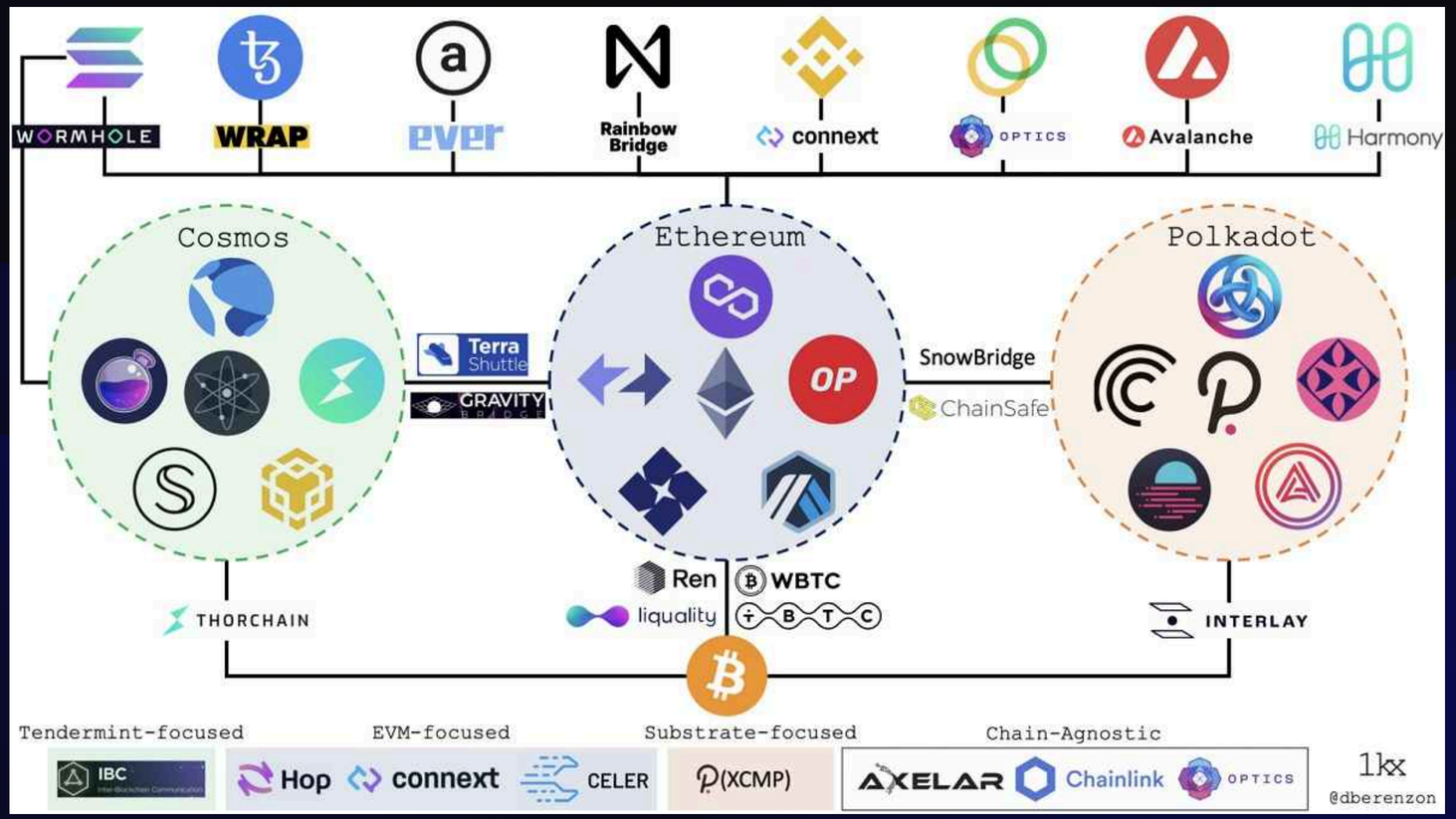
A Generic Bridge - Function



Credit: Axelar

A Generic Bridge - Architecture

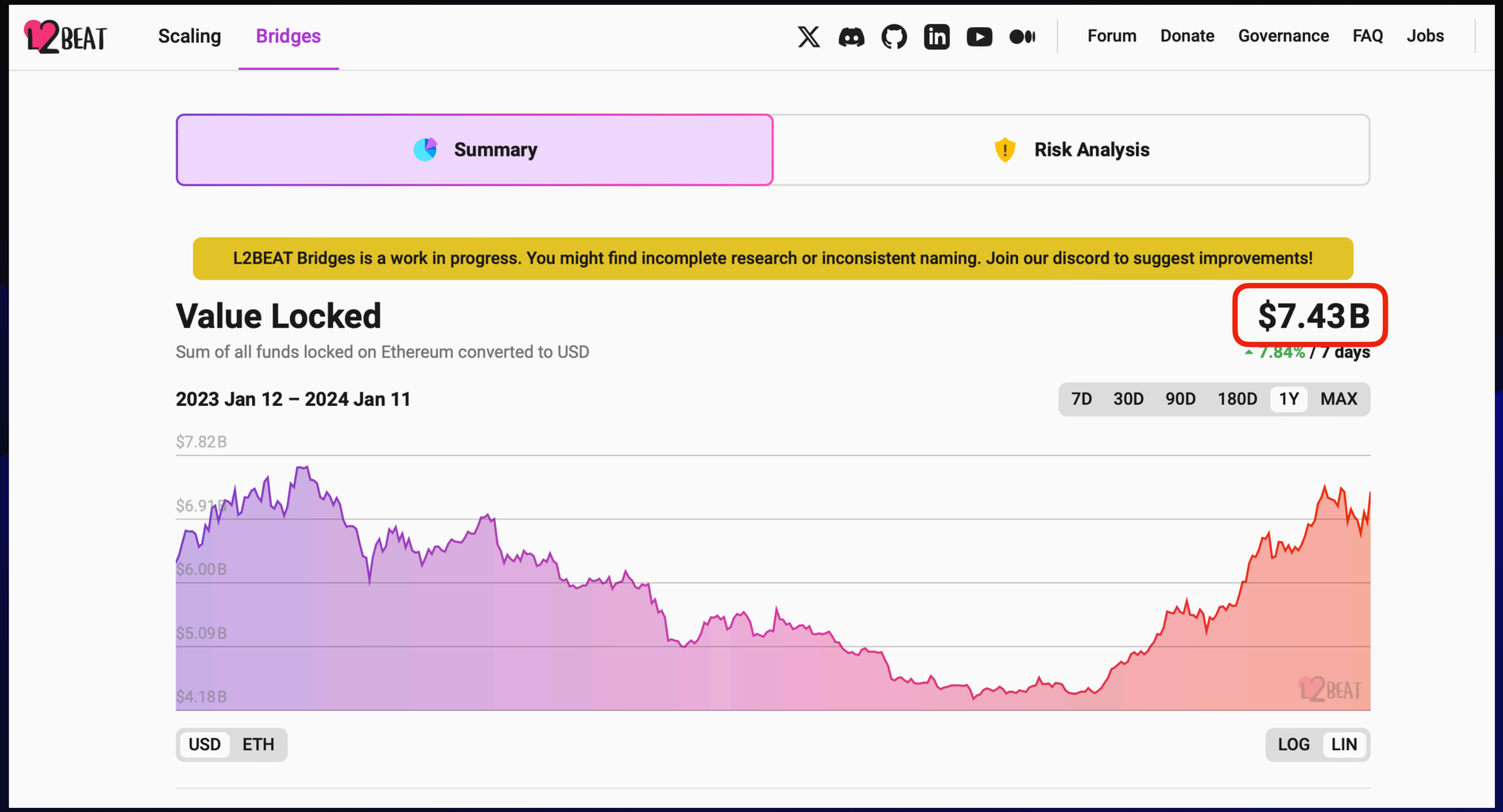




https://news.bitcoin.com/study-shows-cross-chain-bridge-technology-growth-bridges-to-ethereum-exceed-7-billion/

It's never that simple

Now we have *too many* crosschain bridges!



https://l2beat.com/bridges/summary

Crosschain bridges are big business

…so they get hacked. A lot.

2022-3

Organisation	Chains	Lost (USD)	Recovered (USD)
Ronin Bridge	Ronin sidechain	$624M	$30M
Poly Network Bridge	Ethereum, Binance Smart Chain, Polygon and others	$611M	Nearly all (chaotic whitehat)
BSC Bridge	Binance	$566M	~455M
SBF/FTX/Alameda Research	Tether/Ethereum	$477M	$100M frozen
Wormhole Bridge	Solana	$326M	Reportedly all
Mixin Network	Ethereum, Bitcoin	$200M	-

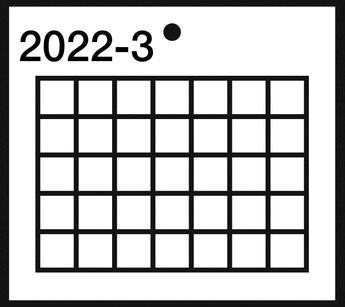
https://rekt.news/leaderboard/

The most common types of bridge hacks

- **Fake Events** (generate a fake deposit or depositing a valueless token) (e.g., Wormhole hack, BSC hack, broadly the Euler hack)
- **Message Verification Bugs** (lack of proper validation) (e.g., Poly hack)
- **Access Control Bugs** (lack of access control validations on critical functions) (e.g., Ronin hack, Poly hack)
- **Validator Takeover** (e.g., Ronin, Mixin hacks)
- **Admin or Users' Private Key Leak** (e.g., Harmony hack, Ronin hack, probably Mixin hack)

https://quillaudits.medium.com/bridge-security-in-blockchain-quillaudits-f4710d1d61d

Top Bridge Hacks by Hack Type



Organisation	Lost (USD)	Hack Type	Category
Ronin Bridge	$624M	Access Control Validator Takeover Admin Key Leakage	Operations
Poly Network Bridge	$611M	Message verification Access Control	Software and Operations
BSC Bridge	$566M	Fake Events	Software
Wormhole Bridge	$326M	Fake Events	Software
Mixin Network	$200M	Access Control Validator Takeover	Operations

https://rekt.news/leaderboard/

Rough Comparison of Top Hack Categories

Category	Organisation	Lost (USD)
Operations	Ronin Bridge Poly Network Bridge Mixin Network	$1,129.5M
Software	BSC Bridge Wormhole	$1,197.5M

So, operations is at least as economically important to secure as software

So, how to architect bridges to avoid the most common hacks?

Secure (and decentralise) your bridge

Big Bridges

- **Continuing to decentralise:**
  - **Axelar**
  - **LayerZero**
  - **Wormhole**
- **Dual-bridging?**
  - **Wormhole, Axelar and Lido DAO**

Additionally:

- Security Audits
- Bug bounty Programs
- Insurance

Standardisation

ERC-5164

Cross-Chain Execution

Defines an interface that supports execution across EVM networks.

Authors: Brendan Asselstine, Pierrick Turelier, Chris Whinfrey

Created 2022-06-14

Ethereum Improvement Proposals

All Core Networking Interface ERC Meta Informational

Review Standards Track: ERC

ERC-5164: Cross-Chain Execution

Defines an interface that supports execution across EVM networks.

Authors Brendan Asselstine (@asselstine), Pierrick Turelier (@PierrickGT), Chris Whinfrey (@cwhinfrey)

Created 2022-06-14

This EIP is in the process of being peer-reviewed. If you are interested in this EIP, please participate using this discussion link.

Table of Contents

- Abstract
- Motivation
- Specification
  - MessageDispatcher
  - MessageExecutor
- Rationale
- Backwards Compatibility
- Security Considerations
- Copyright

Abstract

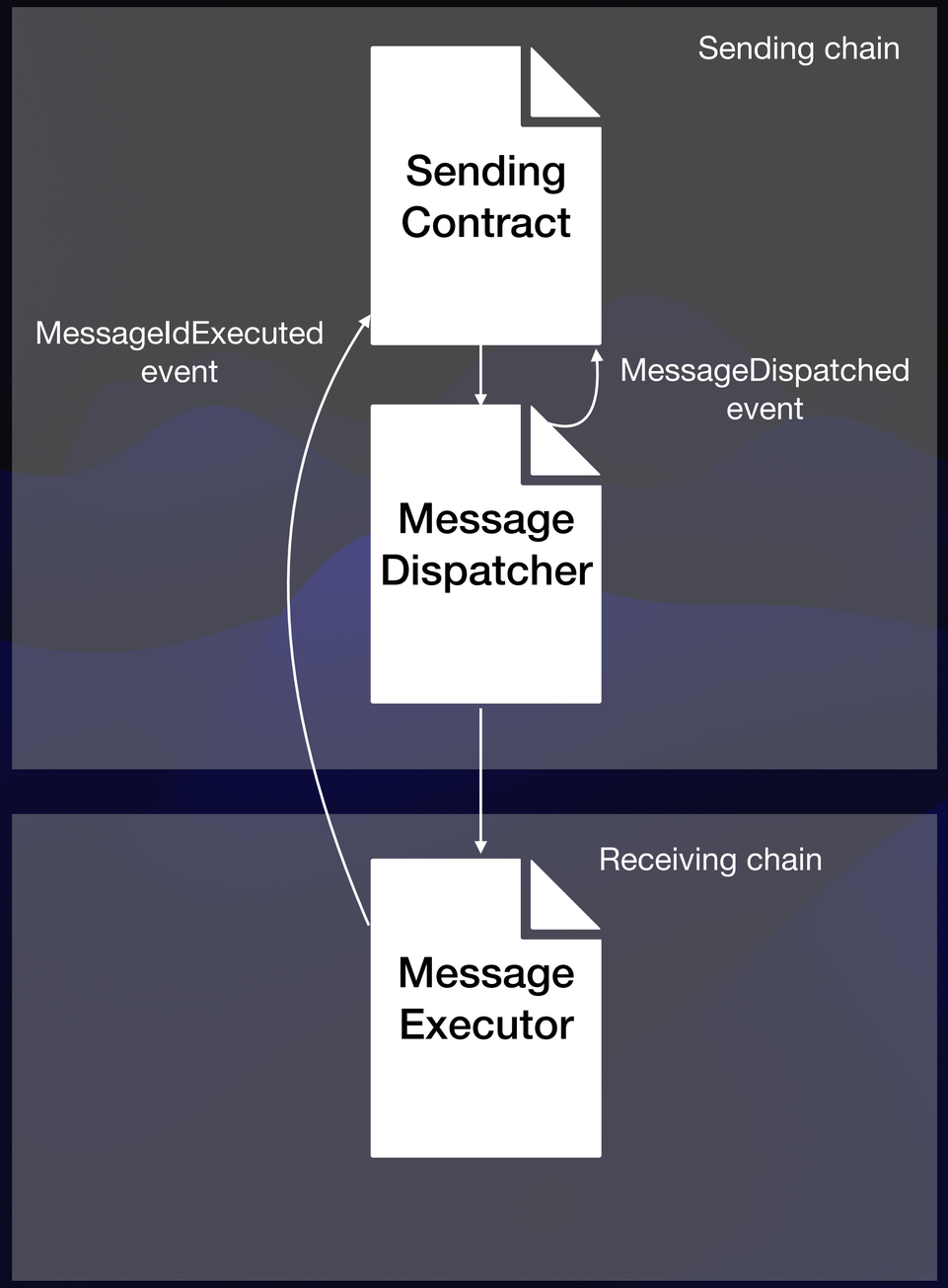
This specification defines a cross-chain execution interface for EVM-based blockchains. Implementations of this specification will allow contracts on one chain to call contracts on another by sending a cross-chain message.

The specification defines two components: the "Message Dispatcher" and the "Message Executor". The Message Dispatcher lives on the calling side, and the executor lives on the receiving side. When a message is sent, a Message Dispatcher will move the message through a transport layer to a Message Executor, where they are executed. Implementations of this specification must implement both components.

Motivation

Many Ethereum protocols need to coordinate state changes across multiple EVM-based blockchains. These chains often have native or third-party bridges that allow Ethereum contracts to execute code. However, bridges have different APIs so bridge integrations are custom. Each one affords different properties; with varying degrees of security, speed, and control. Defining a simple, common

ERC-5164



dispatchMessage(uint256 toChainId, address to, bytes calldata data) external payable returns (bytes32 messageId);

Authentication of the MessageDispatcher is via EIP-2771 (Secure Protocol for Native Meta Transactions)

Messages:
- get executed ***once***
- in any order

Bridge-agnostic solutions

Gnosis Block Header Oracle (Hashi 橋)

Redundant Array of Independent Hash Oracles (RAIHO); Bridges must agree to proceed

https://github.com/gnosis/hashi

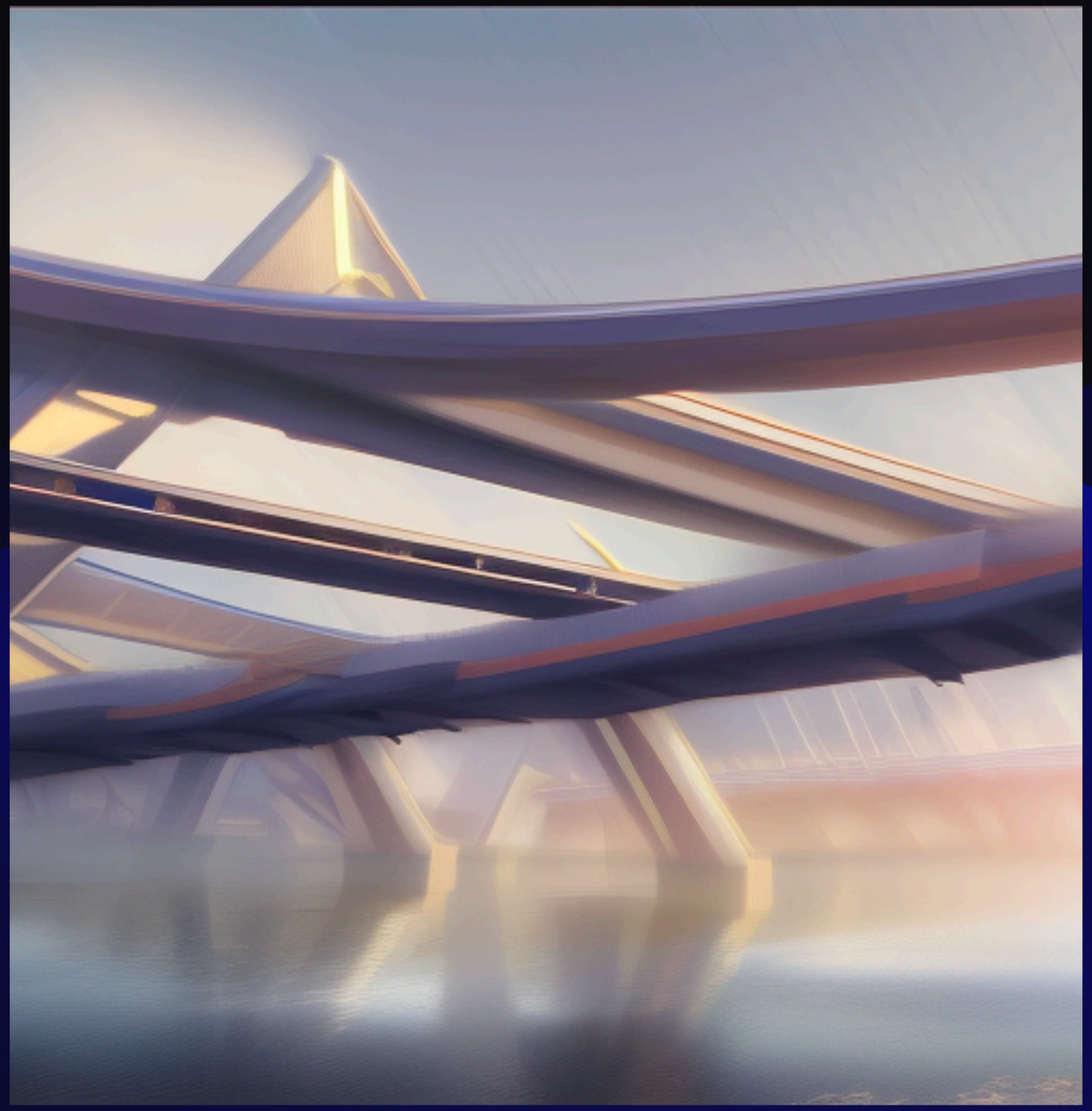
Hashi 橋

- Attempts to provide:
  - “Additive” security: New bridge approaches can ideally increase the security of existing bridges instead of offering new tradeoffs
  - Standardization at least on the lowest level (block header)
- Drawbacks:
  - The main drawback of this approach is higher gas costs and potentially slower bridging times.

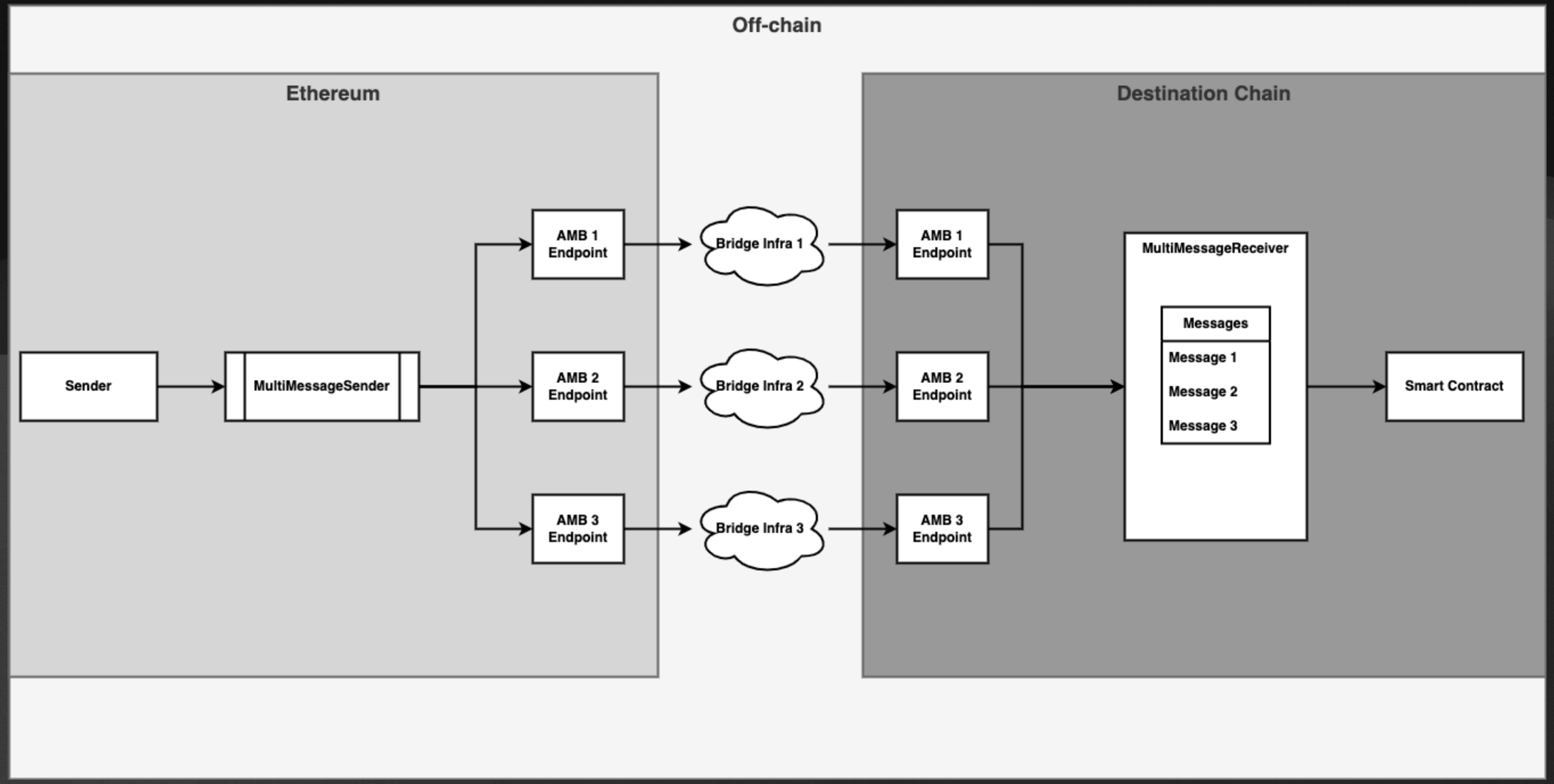
Multi-Message-Aggregation (MMA)

Started January 2023

https://github.com/MultiMessageAggregation/multibridge

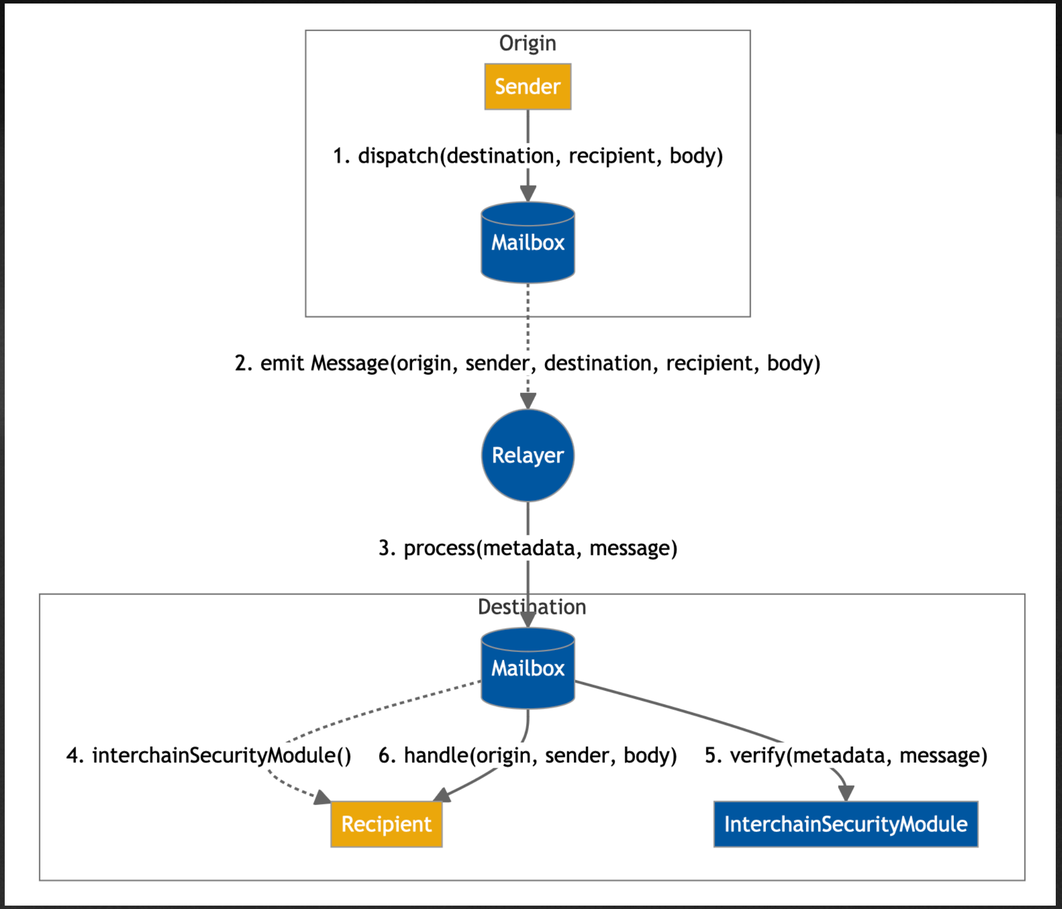


MMA Architecture



MMA-Compliant Implementations

- Celer State Guardian Network (https://celer.network)
- Hyperlane (hyperlane.xyz) in progress



Hyperlane

Conclusions

Critical Lesson

- Hacks related to operations have been roughly as economically impactful as those related to software.
- Securing bridges requires a broader focus on approaches beyond audits:
  - Operational security
  - Incident response
  - Formal verification
  - Architectural approaches
  - Protocol reviews

Currently

- Securing bridges: A failure in concept?
- Bridge-agnostic solutions are immature, yet promising.
  - Even if one is ready, there aren't a sufficient number of bridges ready to participate in multi-bridge solutions.
  - Ideally having 3-5 or even more to guarantee high safety and liveness would be best.
- Standardisation: Premature?
  - A standard approach would be great to minimise complexity and opportunities for new bug injections, but may be too early.
  - Hyperlane and Celer are implementing MMA; they may diverge
  - Gnosis deviated from ERC-5164