Hashi - Additive security for cross-chain bridging

GNOSIS

I. Brief intro to Hashi

II. Why do bridges get hacked?

III. Hashi design principles and goals

IV. Hashi architecture

V. Your challenge

Introducing Hashi

- Hashi is a protocol for cross-chain communication based on additive security; multiple inputs (oracles)
- At its core it's a **Hash Oracle Aggregator**, allowing one to implement a **RAIHO** (Redundant Array of Hash Oracles)
- Goal: **Distribute trust** for bridges on the mechanism level

Why Hashi?

All bridge designs have **trade-offs**

Why trust the security of just one bridge mechanism?

$2B

Lost in 2022

To token bridge exploits

4/5

Rekt.news on leader

Are bridge related exploits

100%

Secure bridge

Does not exist

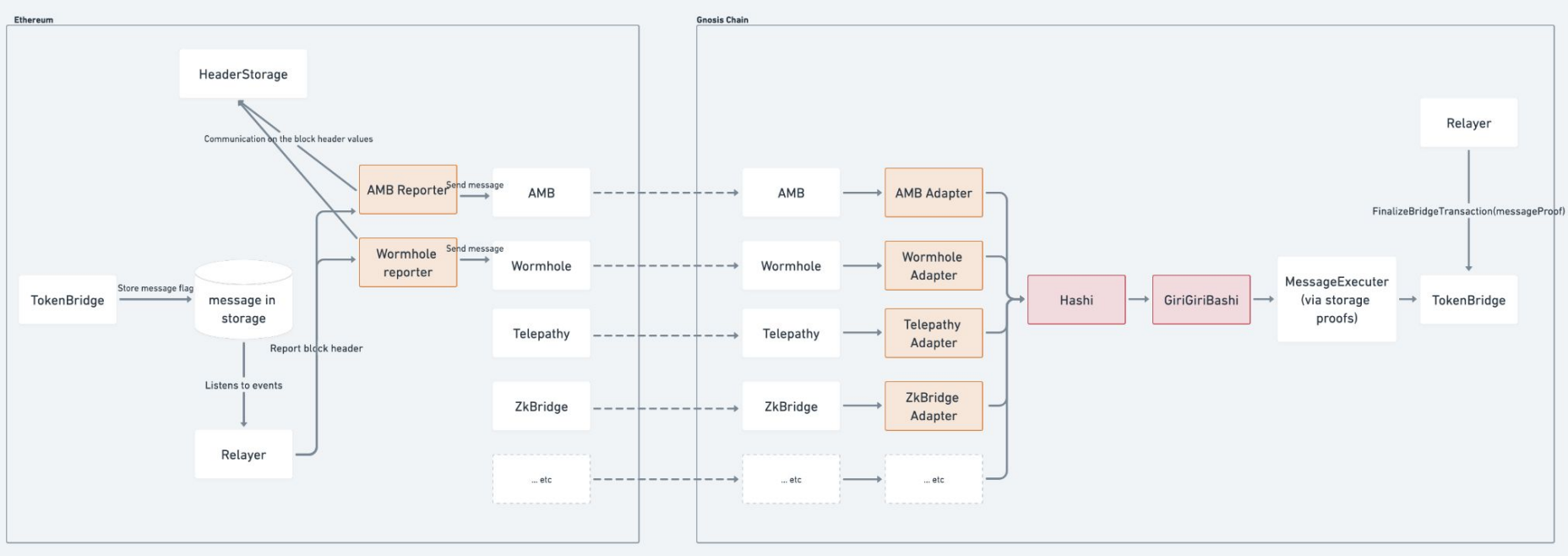
Design principles

- Standardization at the lowest level (hash)
- Modular and agnostic to underlying mechanisms
- **RAIHO**
  (Redundant Array of Independent Hash Oracles)
  - Analogous to RAID
    (Redundant array of Independent Drives)
  - Security over latency and cost
  - Moves as fast as the slowest oracle used
  - Robust and secure, but more costly

Goals

- Diversification on the cross-chain protocol implementations
- Integrations with multiple header oracles (Telepathy, zkBridge, etc)
- Integrations with multiple message passing mechanisms (AMB, Wormhole, etc)
- User choice in which combination of mechanisms to trust to secure their systems

Architecture Overview



Main components

- **Applications** (Token Bridge, Governance Bridge, NFT Bridge)
- **Hash Oracles** (bridges)
- **Core contracts**:
  - Hashi (Oracle aggregator)
  - GiriGiBashi (Governance - Oracle & thresholds management)
- **Storage proofs**: E.g Axiom
- **Reporter contracts**: Initiating a msg transfer in a specific bridge
- **Relayers**: (Permissionless) Listen to events on origin chains and report hashes / trigger transactions on corresponding destination chains

What you can build with Hashi

- Write an **adapter** for another bridge:, preferably a ZK light client one:
    - SuccintLabs, Dendreth, ZKCollective.
- Write a contract that checks **merkle proof** of some event / storage slot
- Alternate implementations of GiriGiriBashi:
  Aggregation/Governance rules in case oracles disagree
- Build an end-to-end application on top of Hashi
  (Token bridge, NFT bridge, Governance bridge, etc)

The Challenge

Category 5: Applications leveraging RAIHO
RAIHO has various use cases, including cross-chain token transfers, NFT bridging, governance bridging, etc.

Participants are encouraged to develop innovative applications on top of a Hashi-based RAIHO.

Category 6: Defense in Depth
As mentioned earlier, it is important to develop a defense-in-depth solution, leveraging different, independent implementations and proof diversity, to achieve even stronger security even if each implementation may have bugs.

Participants are encouraged to build additional header oracle adapters (See the Telepathy adapter or AMB adapter as examples.), adapt and improve on GiriGiriBashi to allow for different control mechanisms.

Deliverables

- Open source code
- Tests and documentation
- PR to the Hashi repo, if your project improves Hashi
- A short presentation explaining your project

Resources

- Repo: github.com/gnosis/hashi
- Intro discussion: ethresear.ch/t/hashi-a-principled-approach-to-bridges
- Intro thread: twitter.com/auryn_macmillan/status/1632696493525323778
- Ask questions on the Gnosis Chain discord - #hashi channel
- Already implemented adapters for:
  - Gnosis AMB, Telepathy, Wormhole, Connext
- Deployed contracts:
  - 0x471c90d7802E438F54c4638f9FF3b96223Fd91d7 -- Hashi on goerli
  - 0xC303dD953928ef4218F0AB8729049bf33Bdc84C8 -- GiriGiriBashi on goerli
  - 0xeFeb149bEAeF362406eC4964AD891C8661396864 -- HeaderStorage on chiado
  - 0xf2c4b937EEd174Ae08A84d568144E8B29B852F57 -- AMBHeaderReporter on chiado
  - 0x871ee6f5DF413E83427Cab46E588F8B3E59474F7 -- AMBAdapter on goerli

Thank you

GNOSIS

GNOSIS CHAIN

Want To Find Out More?

Gnosis DAO forum	https://forum.gnosis.io/
Docs:	https://developers.gnosischain.com/
Ecosystem:	https://gnosischain.world/
Chain stats:	https://beacon.gnosischain.com/
Become a validator:	https://docs.gnosischain.com/validator-info/get-started-node-setup

Find us on telegram, twitter, discord etc