Security

Core Security Assumptions

At the core, Wormhole is secured by a network of Guardians nodes that validate and sign messages. If a super majority (e.g. 13 out of 19) Guardians sign the same message, it can be considered valid. A smart contract on the target chain will verify the signatures and format of the message before approving any transaction.

- Wormhole's core security primitive is its signed messages (signed VAAs).
- The Guardian network is currently secured by a collection of 19 of the world's top validator companies listed here
- .
- Guardians produce signed state attestations (signed VAAs), when requested by a Core Contract integrator.
- Every Guardian runs full nodes (rather than light nodes) of every blockchain in the Wormhole network. This means that if a blockchain suffers a consensus attack or hard fork, the blockchain will disconnect from the network, rather than potentially produce invalid signed VAAs.
- Any Signed VAA can be verified as authentic by the Core Contract of any other chain.
- Relayers are considered untrusted in the Wormhole ecosystem.
-

In summary:

- Core integrators aren't exposed to risk from chains and contracts they don't integrate with
- .
- By default, you only trust Wormhole's signing process and the Core Contracts of the chains you're on.
- You can expand your contract and chain dependencies as you see fit.
-

Core assumptions aside, there are many other factors which impact the real-world security of decentralized platforms. Here is more information on additional measures which have been put in place to ensure the security of Wormhole.

Guardian Network

Wormhole is an evolving platform. While the Guardian set currently comprises 19 validators, this is mostly a limitation of current blockchain technology.

Governance

Governance is the process through which contract upgrades happen. Guardians manually vote on governance proposals which originate inside the Guardian Network and are then submitted to ecosystem contracts.

This means thatgovernance actions are held to the same security standard as the rest of the system. A 2/3 super-majority of the Guardians are required to pass any Governance action.

Governance messages can target any of the various wormhole modules, including the core contracts as well as all currently deployed token bridge contracts. When a guardian signs such a message, its signature implies a vote on the action in question. Once more than 2/3 of the guardians have signed, the message and governance action are considered valid.

All governance actions and contract upgrades have been managed via Wormhole'son-chain governance system .

Via governance, the Guardians are able to:

- Change the current Guardian set
- Expand the Guardian set
- Upgrade ecosystem contract implementations
-

The Governance system is fully open source in the core repository. Seethis section for contract source.

Monitoring

A key element of Wormhole's defense-in-depth strategy is that each Guardian is a highly-competent validator company with their own in-house processes for running, monitoring, and securing blockchain operations. This heterogeneous approach to monitoring increases the likelihood that fraudulent activity is detected and reduces the number of single failure points in the system.

Guardians are not just running Wormhole validators, they're running validators forevery blockchain inside of Wormhole as well , which allows them to perform monitoringholistically across decentralized computing , rather than just at a few single points.

Guardians Monitor:

- Block Production & Consensus of each blockchain. If a blockchain's consensus is violated it disconnects from the network until the Guardians resolve the issue.
- Smart Contract level data. Via processes like the Governor, Guardians constantly monitor the circulating supply and token movements across all supported blockchains.
- Guardian Level activity. The Guardian Network functions as an autonomous decentralized computing network, complete with its own blockchain (Gateway
-).
-

Gateway & Asset Layer Protections

One of the most powerful aspects of the Wormhole ecosystem is that Guardians effectively havethe entire state DeFi available to them .

Gateway is a Cosmos based blockchain which runs internally to the Guardian network, whereby the Guardians can effectively execute smart contracts against the current state of all blockchains, rather than just one blockchain.

This enables additional protection for the Wormhole Asset Layer in addition to the core assumptions:

- Global Accountant:
- The accountant tracks the total circulating supply of all Wormhole assets across all chains and prevents any blockchain from bridging assets which would violate the supply invariant.
-

In addition to the Global Accountant, Guardians may only sign transfers that do not violate the requirements of theGovernor . The Governor tracks inflows and outflows of all blockchains and delays suspicious transfers which may be indicative of a exploit.

Open Source

Wormhole builds in the open and is always open source.

- Wormhole Core Repository
- Wormhole Foundation Github Organization
- Wormhole Contract Deployments
-

Audits

Wormhole has been heavily audited, with16 third-party audits completed and a total of25+ started .

Wormhole has had audits performed by the following firms, and continues to seek more:

- Trail of Bits
- Neodyme
- Kudelski
- OtterSec
- Certik
- Hacken
- Zellic
- Coinspect
- Halborn
-

The most up-to-date list of audits, as well as the final reports can be foundhere

Bug Bounties

Wormhole has one of the largest bug bounty programs in all of software development, and has repeatedly shown commitment to engaging with the white hat community.

Wormhole hosts two bug bounty programs:

- AnImmunefi
- program,
- As well as aself-hosted program
-

Both platforms have a top payout of2.5 million dollars .

If you are interested in helping contribute to Wormhole security, please look at this section forGetting started as a White Hat

, and be sure to follow theWormhole Contributor Guidelines .

For more information about submitting to the bug bounty programs, lookhere

Learn More

- TheSECURITY.md
- from the official repository has the latest security policies and updates.
-

Last updated2 months ago

On this page * Core Security Assumptions * Guardian Network * Monitoring * Gateway & Asset Layer Protections * Open Source * Audits * Bug Bounties * Learn More

Was this helpful? Edit on GitHub