Proposal

Wormhole

is a leading cross-chain interoperability protocol, allowing generic messaging over 22 heterogenousblockchains and soon to be many more.

Since launch on mainnet in August 2021, 160 million messages have been transmitted with2 million messages currently generated a day between asset transfers and messaging. The sheer load of messages that Wormhole processes in a 24 hour period is comparable to an L1 and signals its high reliability.

Wormhole has nineteen guardians comprised of the leading PoS validatorswho jointly attest to messages. Each guardian holds equal weight in governance and consensus. Wormhole requires over two-thirds of the 19 guardians to gain consensus and pass verification, thus we assume that at least one-third of our guardian set is trustworthy.

Hashflow

is a decentralized exchange platform designed for interoperability, zero slippage, and MEV-protected trades. Hashflow works by connecting professional market makers directly to traders using a request-for-quote (RFQ) model.

Hashflow uses DeFi-native RFQs to fetch quotes from market makers who are responsible for managing liquidity in the pools. Market makers are required to cryptographically sign quotes that remain unchanged for the duration of the trade. This ensures that the price is guaranteed and cannot be front-run or sandwich attacked. It also protects traders against slippage if there is significant price movement between the time it takes to validate the transaction on the source chain and relay the payload on to the destination chain.

Hashflow leverages Wormhole's generalized message-passing to communicate between source and destination chains.

We propose a custom protocol utilizing Wormhole's generic messaging for cross-chain communication and Hashflow's cross-chain DEX to facilitate collateral transfers when backing aTokens (detailed below). Generic messaging unlocks Wormhole as a neutral interoperability layer on which protocols can serve users across most chains today. Wormhole has been integrated with Hashflow, which leverages a request-for-quote (RFQ) model for efficient liquidity provision, depth, and order execution quality. Users request a quote to sell some amount of asset X on the source chain and buy some amount of asset Y on the target chain without incurring slippage on the quoted price. Institutional market makers compete on price and depth for order execution and provide a signed quote to the user, which the user includes as calldata when sending the trade transaction on the source chain. With over $11.75B in lifetime trading volume and aggregate average daily volume of $25M from traders directly using the platform and through the aggregators 1inch Network, Open Ocean, Odos, and Zerion, Hashflow has been battle-tested and is a logical starting choice for these cross-chain collateral transfers. Users pay no trading fees for this cross-chain swap but are responsible for the associated gas fees when bridging their aTokens and might incur an implicit fee in any price-differences between the collateral asset on the source and destination chain. Additionally, Wormhole currently does not charge any fees for token bridging.

Pending Aave V3 deployments on the specific L1s/L2s, the protocol can support Aave on Ethereum, Avalanche, Polygon, Arbitrum, Optimism, and BNB. To start, we suggest piloting Portals on Arbitrum as a burgeoning deployment and ecosystem.

Integration

A custom protocol (”Protocol”) utilizing Wormhole and Hashflow for a Portals integration could function as follows for a given source and target chain:

1. User uses the Protocol front-end built on Wormhole to transfer aTokens to the Protocol contract.

2. Protocol front-end will fetch a signed quote from Hashflow which will be used as a payload to perform the cross-chain swap

3. Protocol front-end will allow the user to review the quote before confirming the transaction

4. User's aTokens are then escrowed in the Protocol on the source chain.

5. Protocol front-end will fetch a signed quote from Hashflow which will be used as a payload to perform the cross-chain swap

6. Protocol front-end will allow the user to review the quote before confirming the transaction

7. User's aTokens are then escrowed in the Protocol on the source chain.

8. Following the transfer of aTokens, the source chain Protocol contract calls thewithdraw function in the Aave Pool contract on the source chain, which transfers the user's previously escrowed aTokens from the Protocol contract to the Aave Pool contract and then transfers the user's underlying collateral from the Aave Pool contract to the Protocol contract.

9. The contract then submits the signed quote to Hashflow’s cross-chain router to swap the user’s source-chain native collateral to the target-chain native collateral, sending this collateral to the target chain Protocol contract.
10. Next, the target chain Protocol contract callsmintUnbacked function in the target chain Aave Pool contract followed by the backUnbacked function to atomically mint aTokens to the user on the target chain and back these aTokens.

[

image

1920×1176 38.9 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/1/1ee30a3705443fc408ede7019f2c0bf534956707.jpeg)

To prevent the collateral risk to the Protocol on the source chain and to allow for seamless atomic liquidations on the target chain, we suggest that Aave prevent users from bridging aTokens used as collateral on the source chain and prevent the use of the unbacked aTokens as collateral on the target chain until they’ve been backed by the bridge.

Technical Specifications

- Is the entity a Bridge?
- While users can bridge assets using applications built atop Wormhole, Wormhole is primarily a generic interoperability protocol, enabling users and developers alike to use and build complex, composable applications on top of Wormhole.
- While users can bridge assets using applications built atop Wormhole, Wormhole is primarily a generic interoperability protocol, enabling users and developers alike to use and build complex, composable applications on top of Wormhole.
- Can anyone provide liquidity to the protocol?
- N/A
- N/A
- Is liquidity incentivized?
- No, at this time liquidity is not incentivized.
- No, at this time liquidity is not incentivized.
- Is there a fee model for participants?
- There are currently no fees when participants use Wormhole.
- There are currently no fees when participants use Wormhole.
- Does the entity plan to provide available liquidity into Aave protocol?
- TBD
- TBD
- Link to analytics dashboard of protocol (Liquidity, assets, networks, volume).
- https://wormhole.com/stats/
- https://wormhole.com/explorer/
- https://app.hashflow.com/dashboard
- https://wormhole.com/stats/
- https://wormhole.com/explorer/
- https://app.hashflow.com/dashboard
- If applicable, link to the user-focused dapp of the entity.
- https://www.portalbridge.com/#/transfer
- https://wormhole.com/ecosystem/

- https://app.hashflow.com/
- https://www.portalbridge.com/#/transfer
- https://wormhole.com/ecosystem/
- https://app.hashflow.com/
- Link to technical documentation
- https://book.wormhole.com/
- https://docs.hashflow.com/hashflow/product/bridgeless-cross-chain-swaps
- https://book.wormhole.com/
- https://docs.hashflow.com/hashflow/product/bridgeless-cross-chain-swaps

Proposed Portals Asset Minting Caps

On all networks that Aave V3 is deployed on and Wormhole supports, we propose conservative Portals minting caps of $0.5M, $1M, and 50 ETH respectively for USDC, USDT, and ETH to begin with but aim to increase this over time subject to governance. The protocol will charge users a nominal 3bps fee to bridge over their aTokens, of which the Aave DAO will be entitled to 50%.

[

Screenshot 2023-02-22 at 3.27.46 PM

1436×168 6.53 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/1/1e2d15ce1ccdbe0b798b6069ede56f673f1de8a1.png)

Benefits to AaveDAO

Aave is at an inflection point, with a sizable but closing head-start on its multi-chain deployment and usage. With the launch of V3 on Ethereum, it is timely to pilot Portals, enabling seamless flows of capital from the liquidity hub of Ethereum to the other V3 deployments. For AaveDao’s longterm success, it’s imperative that the DAO fosters these multi-chain deployments while still in the lead as the tight integration of aToken assets into DeFi creates a strong moat. Additionally, with tens to hundreds of millions of TVL and volume in Hashflow and Wormhole, we see Portals as an natural way to onboard Hashflow and Wormhole users into the Aave ecosystem.

Audits & Security

- List of relevant security audits of the Wormhole network
- January 2022 - Neodyme

: Ethereum Contracts

- January 2022 - Neodyme

: Solana Contracts

- January 2022 - Neodyme

: Terra Contracts

- January 2022 - Neodyme

: Guardian

- January 2022 - Neodyme

: Solitaire

- July 2022 - Kudelski

: Ethereum Contracts

- July 2022 - Kudelski

: Solana Contracts

- July 2022 - Kudelski

: Terra Contracts

- July 2022 - Kudelski

: Guardian

- August 2022 - Kudelski

: Algorand Contracts

- September 2022 - OtterSec

: NEAR Contracts

- September 2022 - Trail of Bits

: Solana Contracts

- September 2022 - Trail of Bits

: CosmWasm Contracts

- Underway audits can be found here
- January 2022 - Neodyme

: Ethereum Contracts

- January 2022 - Neodyme

: Solana Contracts

- January 2022 - Neodyme

: Terra Contracts

- January 2022 - Neodyme

: Guardian

- January 2022 - Neodyme

: Solitaire

- July 2022 - Kudelski

: Ethereum Contracts

- July 2022 - Kudelski

: Solana Contracts

- July 2022 - Kudelski

: Terra Contracts

- July 2022 - Kudelski

: Guardian

- August 2022 - Kudelski

: Algorand Contracts

- September 2022 - OtterSec

: NEAR Contracts

- September 2022 - Trail of Bits

: Solana Contracts

- September 2022 - Trail of Bits

: CosmWasm Contracts

- Underway audits can be found here
- List of relevant security audits of Hashflow
- [October 2022 - Quantstamp

](https://drive.google.com/file/d/1a-aBAXF3XuKaP9SBGQk_Zcrc2DiUZ2uG/view)

- October 2022 - Certik
- November 2022 - OpenZeppelin

- [October 2022 - Quantstamp

](https://drive.google.com/file/d/1a-aBAXF3XuKaP9SBGQk_Zcrc2DiUZ2uG/view)

- October 2022 - Certik
- November 2022 - OpenZeppelin

- Security Properties
- The Wormhole dependency in the implementation above is in the core messaging layer, relying on the standard trust assumption of the PoA consensus with 19 guardians where more than two-thirds are required to reach consensus and verify a message. These guardians are made up of some of the largest and most reputable staking providers in crypto. This level of operational security diversity is a useful property in preventing wholesale compromise of the Guardian Set due to operational failures of a single or small number of organizations. More information on Wormhole security practices can be found here.
- Hashflow relies on Market Makers for providing quotes, and Wormhole for ensuring that the cross-chain messages are correctly passed. The former is a transparent process (the user can see these quotes ahead of execution), whereas the latter falls back on Wormhole's security properties.
- The logic of creating new unbacked aTokens on the target chain, withdrawing collateral on behalf of the user on the source chain, and backing users' unbacked aTokens on the target chain lies in the Aave protocol, falling back on Aave's security.

- The Wormhole dependency in the implementation above is in the core messaging layer, relying on the standard trust assumption of the PoA consensus with 19 guardians where more than two-thirds are required to reach consensus and verify a message. These guardians are made up of some of the largest and most reputable staking providers in crypto. This level of operational security diversity is a useful property in preventing wholesale compromise of the Guardian Set due to operational failures of a single or small number of organizations. More information on Wormhole security practices can be found here.
- Hashflow relies on Market Makers for providing quotes, and Wormhole for ensuring that the cross-chain messages are correctly passed. The former is a transparent process (the user can see these quotes ahead of execution), whereas the latter falls back on Wormhole's security properties.
- The logic of creating new unbacked aTokens on the target chain, withdrawing collateral on behalf of the user on the source chain, and backing users' unbacked aTokens on the target chain lies in the Aave protocol, falling back on Aave's security.

- Has the Entity experienced outages, downtime, or exploits/hacks? On which Networks?
- We recognize that Wormhole has earned some press for thehack in February of this year. Since then, Wormhole continues to add multiple security layers to help prevent/mitigate the effects of smart contract bugs like the one responsible for that hack:
- The first of these, Governor, allows each Guardian to set limits on the notional value of any transfer originating on a supported chain within a specified time period. The Governor allows Wormhole Guardians to provide optional value movement protections to token bridges built on Wormhole. This protection allows Wormhole Guardians to govern (or effectively rate-limit) the notional flow of assets from any given token bridge chain. This safety feature allows Guardians to limit the impact of any security issue any given chain may have from affecting other connected chains. The Governor allows the setting of daily limits of notional flow and also has an ability to set a fixed finality delay for transactions over a specific size for each supported chain.

- Further layers of security to prevent incorrect withdrawals of funds is the Cosmos-based Wormhole Chain, which enables Guardians to independently verify if the source chain has sufficient funds to do cross-chain transfers, and an emergency shutdown module, allowing a quorum of Guardians to temporarily pause value movement through Wormhole.

- The first of these, Governor, allows each Guardian to set limits on the notional value of any transfer originating on a supported chain within a specified time period. The Governor allows Wormhole Guardians to provide optional value movement protections to token bridges built on Wormhole. This protection allows Wormhole Guardians to govern (or effectively rate-limit) the notional flow of assets from any given token bridge chain. This safety feature allows Guardians to limit the impact of any security issue any given chain may have from affecting other connected chains. The Governor allows the setting of daily limits of notional flow and also has an ability to set a fixed finality delay for transactions over a specific size for each supported chain.

- Further layers of security to prevent incorrect withdrawals of funds is the Cosmos-based Wormhole Chain, which enables Guardians to independently verify if the source chain has sufficient funds to do cross-chain transfers, and an emergency shutdown module, allowing a quorum of Guardians to temporarily pause value movement through Wormhole.

- Additionally, Wormhole has a $2.5M bounty program on Immunefi.

- We recognize that Wormhole has earned some press for thehack in February of this year. Since then, Wormhole continues to add multiple security layers to help prevent/mitigate the effects of smart contract bugs like the one responsible for that hack:

- The first of these, Governor, allows each Guardian to set limits on the notional value of any transfer originating on a supported chain within a specified time period. The Governor allows Wormhole Guardians to provide optional value movement protections to token bridges built on Wormhole. This protection allows Wormhole Guardians to govern (or effectively rate-limit) the notional flow of assets from any given token bridge chain. This safety feature allows Guardians to limit the impact of any security issue any given chain may have from affecting other connected chains. The Governor allows the setting of daily limits of notional flow and also has an ability to set a fixed finality delay for transactions over a specific size for each supported chain.

- Further layers of security to prevent incorrect withdrawals of funds is the Cosmos-based Wormhole Chain, which enables Guardians to independently verify if the source chain has sufficient funds to do cross-chain transfers, and an emergency shutdown module, allowing a quorum of Guardians to temporarily pause value movement through Wormhole.

- The first of these, Governor, allows each Guardian to set limits on the notional value of any transfer originating on a supported chain within a specified time period. The Governor allows Wormhole Guardians to provide optional value movement protections to token bridges built on Wormhole. This protection allows Wormhole Guardians to govern (or effectively rate-limit) the notional flow of assets from any given token bridge chain. This safety feature allows Guardians to limit the impact of any security issue any given chain may have from affecting other connected chains. The Governor allows the setting of daily limits of notional flow and also has an ability to set a fixed finality delay for transactions over a specific size for each supported chain.

- Further layers of security to prevent incorrect withdrawals of funds is the Cosmos-based Wormhole Chain, which enables Guardians to independently verify if the source chain has sufficient funds to do cross-chain transfers, and an emergency shutdown module, allowing a quorum of Guardians to temporarily pause value movement through Wormhole.

- Additionally, Wormhole has a $2.5M bounty program on Immunefi.