Bifrost documentation

Architecture overview

Bifrost is an optimistic bridge that leverages Cardano Stake Pools high decentralization level to secure the peg-ins and peg-outs from and to other UTxO blockchains like Bitcoin, Dogecoin and Litecoin. Because of the limited scripting capabilities of these blockchains, in recent years different bridging alternatives have been proposed. The current most known alternatives are FROST signatures of a small set of external nodes (Stacks), BitVM optimistic behaviour with 1-of-n honesty assumption with limited availability (Cardinal, Citrea) and Watchtower multisignature behaviour (Rosen Bridge).

Bifrost takes inspiration from all these solutions, but this time Cardano is used as a core component to guarantee the security and uncensorability of the user's actions.

It then becomes easier to connect Cardano, a UTXO blockchain with smart contracts, to other smart contract blockchains and Layer 2s, making Cardano the central component of a safe bridging process.

The Cardano SPOs collectively become the responsible custodians of bridged assets on the original blockchain. For example, SPOs keep and manage the locked BTC on the Bitcoin side, while its bridged version bBTC circulates freely on Cardano.

Bridge	Stacks Frost bridge	BitVM2	Rosen Bridge	Bifrost
Security assumption	Trust in small set of L2 nodes	At least 1 actor must honestly forget his private key	Trust in a set of nodes from a low marketcap blockchain	Weighted-majority of Cardano SPOs must behave honestly
Peg-in & Peg-out Availability	L2 nodes must be collaborative	Pre-chosen fixed set of operators must be collaborative	Majority of guards must be collaborative	Weighted-majority of Cardano SPOs must be collaborative
Peg-in & Peg-out Granularity	Any amount	Fixed static amounts	Any amount	Any amount
Speed in good case	Minutes	Minutes	Minutes	1 Week
Speed in pessimistic case	Minutes	Weeks	Minutes	Weeks
Costs	Low	Medium	Low	Low

Bifrost has been built to ensure security and availability, not speed or low costs. In fact, Bifrost operations may take up to 1 or more Cardano epochs (an epoch is currently equals to 5 days), as coordination and heavy operations must be executed in the correct order. The peg-ins and peg-outs also have to compensate for the work of all actors involved in Bifrost. Therefore Bifrost should be used to move big amounts of liquidity in and out of Cardano and not for intra-day

retail/small business operations. Once big amounts of liquidity have been bridged to Cardano, for this type of smaller and frequent peg-ins and peg-outs it is possible to safely use services like FluidToken FluidSwaps, cutting costs and execution time without sacrificing security.

The security of Bifrost is guaranteed by SPOs participation: for a strong and reliable bridge, most of the top SPOs by delegation must participate in the protocol.

Components

Bifrost setup is made by the following components:

- **Cardano**: the destination blockchain where bridged assets can safely participate in DeFi activities.
- **Source blockchain**: the original blockchain that contains assets to bridge to Cardano, like Bitcoin, Dogecoin and Litecoin.
- **Depositors**: users that lock their assets on the source blockchain to mint them on Cardano.
- **Withdrawers**: users that burn their bridged assets on Cardano to unlock them on the proper source blockchain.
- **Cardano Stake Pool Operators (SPOs)**: Cardano nodes that have delegated stake by Cardano users and that participate in Cardano consensus, guaranteeing its security.
- **Multisig treasury**: a script address on the source blockchain that holds all the bridged assets and it's protected by a multisignature that only SPOs together can use. Each SPO has a weight equal to its delegation and a specific threshold of SPOs signature must be reached to spend/move the multisig treasury.
- **Watchtowers**: an open and always dynamic set of actors who have visibility on both Cardano and the source blockchain. Their only duty is to compete to post the most truthful source blockchain chain of blocks. This allows Cardano to know what's happening on the source blockchain. Anyone can become a Watchtower at any moment.

Bifrost logic is fully encapsulated in the following solutions:

- **SPOs program**: this code must run along with the usual SPO stack. It gives SPOs the ability to coordinate to sign Bitcoin transactions and the ability to see and interact with the needed Cardano smart contracts.
- **Watchtower program**: watchtowers run this software on top of source blockchain and Cardano nodes to be able to properly post the best chain of blocks to Cardano.
- Cardano smart contracts:
  - **spos_registry.ak**: SPOs that participate in Bifrost need to register here for the next upcoming epoch. The registry is a on-chain linked list ordered by SPOs edcs key and each node also contains the SPO secp key that will be used to sign source blockchain transactions.
  - **watchtower.ak**: The watchtowers (anyone) post the best chain of blocks here, other watchtowers eventually challenge it by posting a better version and the winner gets rewarded by the end of the availability window.
  - **peg_in.ak**: when a depositor wants to bridge his assets, he starts by minting a unique NFT and by locking it here. Burning this NFT plus the proof that the source blockchain locking transaction happened, allow the depositor to mint the bridged assets on Cardano

- **peg_out.ak**: when a withdrawer wants to unlock the bridged assets on the proper source blockchain, he starts the peg-out process sending his bridged assets to this smart contract along with a freshly minted unique NFT in the same eUTxO. A proof that the source blockchain unlocking transaction happened, allows the withdrawer to burn this eUTxO and retrieve the min_utxo locked ADA.
- **bridged_asset.ak**: At the end of peg-ins, it allows to mint the bridged version of the source blockchain assets; at the end of peg-outs it allows to burn these bridged assets.

Components relationships

Watchtowers, who run the watchtower program, challenge each other to be the first to post the best source blockchain chain of valid blocks in the Watchtower smart contract. The winner for each chain is rewarded with some ADA, proportionally for each valid block posted.

Depositors, who want to peg-in, mint the proper NFT in peg_in.ak, send their source blockchain assets to the treasury address and wait for the epoch to end.

Withdrawers, who want to peg-out, mint the proper NFT, send it along their bridged assets to peg_out.ak and wait for the epoch to end.

SPOs, who register with their delegated stake to join the next epoch in spos_registry.ak, own both a unique edcs key and a secp key. The registration is accepted only if the SPO has a delegated stake bigger than a minimum threshold.

At the end of each epoch, the registered SPOs (that normally also include the old group) verify each other's delegated stake to ensure honesty and participate in a ceremony to generate their new shared multisignature address.

The old SPOs group then transfers ownership of the source blockchain treasury to the new SPOs group executing a source blockchain transaction from the old SPOs Treasury address to the new one.

This transaction also aggregates all the peg-in transactions to always keep the treasury in one single UTxO.

This transaction also sends the correct amount of the treasury to the source blockchain addresses that have correctly requested a peg-out.

At this point the depositors can burn their peg_in.ak NFT and mint their bridged assets, while the withdrawers can burn their bridged assets locked and the NFT in the peg_out.ak to earn the min_utxo ADA attached to each eUTxO.

User peg-in flow

Let's use Bitcoin as example. A user who wants to move his BTC from Bitcoin to Cardano is called a depositor. These are the steps to execute a correct peg-in:

- Check the status of Bifrost: if the bridge is correctly operational and we are not too near the end of the current Cardano epoch, the peg-in can be done.
- Retrieve the current Bitcoin Treasury Address that is controlled by the Cardano SPOs.

- On Cardano, mint a unique peg_in.ak NFT and send it to the peg_in.ak spend script, putting in the datum the current Bitcoin Treasury Address.
- On Bitcoin, send to the Bitcoin Treasury Address the amount of BTC to peg-in in a single Output adding in the transaction metadata the asset name of the peg_in.ak NFT.
- Wait for the watchtowers to post on Cardano the Bitcoin block that contains the Bitcoin transaction (at least 100 Bitcoin blocks must have passed, ~12 hours).
- Create a peg-in Bitcoin transaction inclusion proof using Binocular oracle and use it to complete the Cardano peg-in request, minting the correct amount of fBTC and burning the peg-in NFT.

User peg-out flow

Let's use Bitcoin as example. A user who wants to move his BTC from Cardano to Bitcoin is called a withdrawer. These are the steps to execute a correct peg-out:

- Check the status of Bifrost: if the bridge is correctly operational and we are not too near the end of the current Cardano epoch, the peg-in can be done.
- Retrieve the current Bitcoin Treasury Address that is controlled by the Cardano SPOs.
- On Cardano, mint a unique peg_out.ak NFT and send it, along with the correct number of fBTC, to the peg_out.ak spend script, putting in the datum the current Bitcoin Treasury Address.
- Wait for the watchtowers to post the Treasury Movement transaction of the next Epoch, that includes the refunds for the withdrawers (at least 8 Bitcoin blocks must have passed). At this point, you have received your BTC on Bitcoin from the Bitcoin Treasury with a utxo that contains your peg_out.ak NFT AssetName in the transaction metadata.
- Create a peg-out Bitcoin transaction inclusion proof using Binocular oracle and use it to complete the Cardano peg-out request, burning the peg_out.ak NFT and the 30 fBTC.

Guaranteeing censor-resistant peg-ins and peg-outs

The main axiom is: When the user uses any bridge, he is already fully trusting the source (ex. Bitcoin) and the destination (ex. Cardano). Every additional component that the bridge uses and that it can't be under direct control of the user is an additional trust assumption.

Bifrost is truly trustless only if it doesn't necessarily add new trust assumptions. As long as the Cardano SPOs and the watchtowers are collaborative, each peg-in or peg-out is permission-less: no actor exists who can decide if the user is permitted to move his assets between the blockchains.

Therefore, the potential additional trust assumptions in Bifrost are the Cardano SPOs and the watchtowers:

- Even if the user becomes a Cardano SPO, he would be just a small part of the total weight-based set of SPOs. Luckily, the strong majority of the SPOs are always incentivized in behaving correctly and on time, like they do when they participate in block-production consensus on Cardano. In fact, the security of Bifrost directly impacts their revenue model: more assets moved with Bifrost imply more Cardano transactions and an increase of the ADA price caused by the bigger demand to execute these transactions. Cardano SPOs want the bridge to work well because their revenue stream strongly depends on it.

- Watchtowers are an “always open” set of nodes that challenge each other to post on Cardano the best chain of block from the source blockchains (ex. from Bitcoin). While the watchtowers earn rewards for doing this job, they could potentially collude and stop the posting of new blocks, halting the bridge for an unbounded timeframe. In these case the user that wants to peg-in or peg-out can spin up a watchtower himself and posting the source blockchains blocks starting from the latest confirmed ones. Because every user is able to become a watchtower any time, there will be now a safe challenge among them to post the correct chain of blocks, resuming the Bifrost operations even in case of collusion.

Flow of Bitcoin over epochs, cerimonies

todo

Flow of SPOs on Cardano

todo

How to join Bifrost as SPO

todo

Why Mithril is not necessary

todo

Why Frost

todo

WORK FROM ZKFOLD HERE

Watchtowers and Bitcoin State Verification (Lantr)

Watchtower Architecture

Watchtowers are permissionless participants who maintain Bitcoin blockchain state on Cardano. They serve as the critical link between the Bitcoin and Cardano networks, ensuring that BiFrost has accurate, up-to-date information about the Bitcoin blockchain.

Key Design Principles:

- **Permissionless Participation**: Anyone can become a watchtower at any time without registration, bonding, or approval. This ensures the system cannot be censored or controlled by a small group.
- **Competitive Model**: Multiple watchtowers compete to submit the most accurate chain of blocks. If one watchtower submits invalid or stale data, others can immediately challenge with the correct chain.

- **Economic Incentives**: Watchtowers are rewarded for posting valid blocks, creating a natural incentive for honest and timely participation.

Core Watchtower Responsibilities

1. **Monitor Bitcoin Network**: Watchtowers continuously track the Bitcoin blockchain for new blocks as they are mined.
2. **Submit Block Headers**: When new Bitcoin blocks are found, watchtowers submit the 80-byte block headers to the Binocular Oracle smart contract on Cardano. These headers contain all information needed to verify Bitcoin consensus rules.
3. **Compete for Accuracy**: Multiple watchtowers naturally compete to submit the most accurate chain. If a watchtower submits headers from an invalid or weaker fork, other watchtowers can challenge by submitting the correct chain with higher cumulative proof-of-work.
4. **Maintain Oracle Liveness**: Watchtowers ensure the Oracle never becomes stale by continuously updating it with the latest Bitcoin state. This is essential for timely peg-in and peg-out processing.

BiFrost-Specific Watchtower Duties

Beyond maintaining general Bitcoin state, watchtowers perform specialized duties for the BiFrost bridge:

Deposit Detection

- Monitor the Treasury Taproot address for incoming Bitcoin transactions
- Match detected deposits to pending PegInRequest UTxOs on Cardano
- Track transaction confirmations as blocks are added

Proof Submission for Peg-ins

- Once a Bitcoin deposit transaction reaches the required confirmation threshold (100 Bitcoin blocks plus 200 minutes of challenge period), watchtowers construct Merkle proofs
- These proofs demonstrate: (1) the transaction exists in a specific block, and (2) that block is confirmed in the Binocular Oracle
- Submitting valid proofs triggers fBTC minting for the depositor

Peg-out Monitoring

TODO

Anomaly Detection

- Continuously verify that Treasury BTC balance matches or exceeds circulating fBTC supply
- Alert the system if invariants are violated
- Trigger failover mechanisms if SPO signing stalls or quorum is lost
- TODO

Binocular Oracle

The Binocular Oracle is the on-chain component that stores and validates Bitcoin blockchain state on Cardano. It provides trustless verification without requiring trust in any external party. For complete technical details, see the Binocular Whitepaper [1].

Bitcoin Consensus Validation The Oracle validates all Bitcoin consensus rules directly on-chain:

- Proof-of-Work verification (block hash meets difficulty target)
- Difficulty adjustment validation (every 2016 blocks)
- Timestamp constraints (greater than median-time-past, less than 2 hours in future)
- Chain continuity (each block references valid parent)

Fork Management The Oracle maintains a tree of competing Bitcoin forks and automatically selects the canonical chain based on cumulative chainwork (total proof-of-work). This mirrors exactly how Bitcoin Core selects the best chain, ensuring the Oracle always reflects Bitcoin's true state.

Confirmation Tracking Blocks progress through multiple stages:

- Initially added to the forks tree when submitted
- Tracked for confirmation depth (distance from chain tip)
- Only blocks with 100+ confirmations are considered for finality

Transaction Inclusion Proofs For BiFrost operations, the Oracle provides data for Watchtowers to construct proofs that:

- Prove a specific transaction exists within a confirmed block
- Prove the block is part of the confirmed chain
- Enable trustless verification of peg-in deposits and peg-out completions

Challenge Period Mechanism

To prevent pre-computed attacks and ensure security, blocks are not immediately finalized when submitted:

1. **Submission**: A watchtower submits new Bitcoin block headers to the Oracle
2. **Challenge Window**: A 200-minute window opens during which any other watchtower can submit a competing fork with higher chainwork
3. **Resolution**: The Oracle automatically selects the chain with the highest cumulative proof-of-work
4. **Finalization**: After the challenge period expires and the block has 100+ confirmations, it becomes "confirmed" and can be used for peg-in proofs

This mechanism ensures that even if a malicious watchtower pre-computes a short fork, honest watchtowers have ample time to submit the correct chain.

Security: 1-Honest-Watchtower Assumption

BiFrost's watchtower design relies on a minimal trust assumption: only one honest watchtower needs to exist for the system to function correctly.

Why This Works:

- If all active watchtowers collude to censor or submit invalid data, any user can spin up their own watchtower
- The permissionless design means no one can prevent new watchtowers from joining
- Honest watchtowers are economically incentivized to challenge invalid submissions

Censorship Resistance:

- A user wanting to peg-in or peg-out can always become a watchtower themselves
- They can then submit the necessary Bitcoin blocks and proofs for their own transactions
- This ensures BiFrost remains operational even in adversarial conditions

This 1-of-n honesty assumption is significantly weaker than typical bridge trust models that require trusting a majority or specific set of operators.

References

[1] Nemish, Alexander. "Binocular: A Trustless Bitcoin Oracle for Cardano." 2025. https://github.com/lantr-io/binocular/blob/main/pdfs/Whitepaper.pdf

[2] Komlo, C. and Goldberg, I. "FROST: Flexible Round-Optimized Schnorr Threshold Signatures." RFC 9591, IETF, 2024. https://datatracker.ietf.org/doc/rfc9591/

[3] Wuille, P. et al. "BIP340: Schnorr Signatures for secp256k1." Bitcoin Improvement Proposal, 2020. https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

[4] Wuille, P. et al. "BIP341: Taproot: SegWit version 1 spending rules." Bitcoin Improvement Proposal, 2020. https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki