ARC: Add support for BTC.b (Native Bitcoin bridged to Avalanche)

Snapshot vote: Snapshot

References

- Project: https://www.avax.network/
- Document portal: https://docs.avax.network
- Contract addresses: Bitcoin (BTC.b) Token Tracker | SnowTrace
- Twitter: https://twitter.com/avalancheavax?s=20&t=PSU83btgvaI0pwbkwO8vCA
- Telegram: Telegram: Contact @avalancheavax
- Technical Documentation: Bridging Bitcoin To Avalanche: A Technical Overview | by Michael Kaplan | Avalanche | Jun, 2022 | Medium
- Support Documentation: Avalanche Bridge | Avalanche Support

Summary

This is a proposal to list BTC.b as a collateral asset. BTC.b is the bridged version of Bitcoin from the Avalanche Bitcoin bridge.

Motivation

The Avalanche Bridge has become a cornerstone piece of infrastructure for the Avalanche community, introducing an innovative security model that uses Intel SGX technology to usher in a new era of bridge technology. The Bitcoin bridge will allow users to directly on and off-ramp from the Bitcoin network and enable Bitcoin users the chance to participate in DeFi. It is a seamless, easy and secure process.

Driving Factors

- Secure: the bridge must be audited and built with security-first technologies.
- Cost-Effective: the cost of bridging assets should be low.
- Fast: the transaction should take the least amount of time possible.
- Transparent: users should be informed of the transfer status at every step of the process.
- Intuitive: users new to crypto asset transfers can easily understand the steps to use the bridge.

Specifications

1. What is the link between the author of the AIP and the Asset?

The author of the AIP is a representative of the Ava Labs team.

1. Provide a high-level overview of the project and the token

Ava Labs is the servicing firm behind the Avalanche blockchain. Avalanche is a network that is EVM compatible and can scale both vertically and horizontally through the subnet architecture and rollups. Avalanche subnets can also support custom virtual machines and many programming languages.

BTC.b is the Avalanche bridged version of native Bitcoin and is non-custodial and permissionless allowing for one of the best and easiest on/off ramps to the Bitcoin network.

1. Explain the positioning of the token in the AAVE ecosystem. Why would it be a good asset to borrow or use as collateral?

BTC.b is redeemable for the native version of BTC and might be the quickest, easiest and safest way to get BTC on-chain. As we have seen in recent times CeFi carries its own risks and BTC.b allows another avenue to get BTC on-chain.

BTC.b is already integrated into multiple DeFi protocols within the Avalanche ecosystem such as Trader Joe, Platypus Finance, Pangolin, Benqi, and Paraswap.

1. Provide a brief history of the project and the different components: DAO (is it live?), products (are they live?). How did it overcome some of the challenges it faced?

Avalanche’s primary network consisting of its X-Chain, P-Chain, and C-Chain went live a little over a year ago with on-chain

protocols launching around that time and since then has not had any downtime. C-Chain is an EVM-compatible contract chain and Avalanche subnets allow for horizontal scaling into a variety of virtual machines and languages.

The Avalanche Ethereum Bridge is the most popular Ethereum bridge in terms of TVL and the network has become very popular for DeFi, peaking at 2nd or 3rd in terms of TVL only behind Ethereum. Avalanche initially struggled to gain liquidity and traction but Avalanche Rush, Avalanche's liquidity mining program that took place in the Autumn of 2021, attracted both Ethereum bluechip protocols and thousands of new users. Avalanche also has native stablecoins ensuring some of the bridge risks are taken away.

1. How is the asset currently used?

Currently, there is about $28M worth of BTC.b bridged to Avalanche C-Chain. Some of the top protocols with BTC.b integrated include $25M of liquidity deposited in Platypus Finance, the Avalanche native stableswap, $600k of liquidity within the Benqi lending protocol, and $12M of liquidity for the AVAX-BTC.b pair within the AMM Trader Joe.

1. Emission schedule

No emission schedule

1. Token (& Protocol) permissions (minting) and upgradability. Is there a multisig? What can it do? Who are the signers?

The bridge uses Intel SGX with a total of 8 wardens and the approval structure of 6 of 8. The wardens include Ankr, Blockdaemon, Chainstack, Protofire, Avascan, Ava Labs, Bware Labs, and Halborn. BTC bridging with Avalanche Bridge is not supported with Metamask or any other wallet other than the Avalanche Core Wallet. This is because the Core Wallet Extension was custom built to support Bitcoin and the Avalanche Bridge and to handle the technical problems of linking Bitcoin and EVM chains within a wallet.

1. Market data (Market Cap, 24h Volume, Volatility, Exchanges, Maturity)
2. Market Cap: $28M
3. 24 Hr Volume: $501k
4. Exchanges: Trader Joe, Platypus Finance, and Pangolin
5. CoinGecko: Bitcoin Avalanche Bridged (BTC.b) Price in USD: BTC.B Live Price Chart & News | CoinGecko
6. Social channels data (Size of communities, activity on Github)
7. Twitter: 715k followers (https://twitter.com/avalancheavax)
8. Telegram: 48k member (Telegram: Contact @avalancheavax)
9. Contracts date of deployments, number of transactions, number of holders for tokens
10. Date of deployment: June 21, 2022
11. The number of transactions: 14,440
12. The number of holders: 408

How It Works/Technical Specifications

The Bridge can be broken down into two main parts: the SGX application and a set of third-party indexers and verifiers called "Wardens." The Wardens are responsible for indexing the Avalanche and Bitcoin blockchains and submitting eligible transactions to the enclave for processing. The SGX application requires 3 of 4 Wardens to submit the same transaction before generating the signed transaction to process the Bridge transfer on the other network. For security reasons, neither the enclave nor the Wardens are directly accessible to bridge users. Instead, they'll explicitly whitelist each other's IP addresses for direct communication. In addition, all communication between the Enclave and Wardens will be encrypted and verified using TLS and include an HMAC signature. For relaying information to the Bridge user base, each warden hosts a JSON file containing the current bridge settings, assets requirements, and attestation report. The front end is set to disable itself if there's any discrepancy within the critical information.

Proposed Technical Parameters

BTC.b is proposed to start with a 70 percent max LTV, a 75 percent liquidation threshold, and a 6.5 percent liquidation penalty. With the level of on-chain liquidity and the ability to bridge from BTC.b back to native BTC quickly and exchange on centralized exchanges for native Avalanche stablecoins, these parameters are safe.