[ARFC] Onboard tBTC to Aave v3 on Ethereum, Arbitrum and Optimism.

Author: ACI (Aave Chan Initiative)

Date: 2024-05-13

Summary:

The proposal aims to onboard Threshold Network's tBTC, to the Aave v3 protocol on Ethereum, Arbitrum and Optimism. tBTC is backed one-to-one with Bitcoin.

Motivation/Background:

tBTC is Threshold's decentralized and permissionless bridge to bring BTC to the Ethereum network. tBTC has been designed to allow Bitcoin holders to participate in Ethereum's Decentralized Finance (DeFi) applications. Users wishing to utilize their Bitcoin on Ethereum can use the tBTC decentralized bridge to deposit their Bitcoin into the system and get a minted tBTC token in their Ethereum wallet.

Having recently acquired a Chainlink oracle, tBTC enables Aave users to have access to the only wrapped Bitcoin, which can be permissionlessly minted and redeemed, where the BTC that backs it is not held by a central intermediary, but is instead held by a decentralized network of nodes using threshold cryptography. This implies a fully decentralized and permissionless lending and borrowing experience for BTC (i.e. bridge native BTC to tBTC and borrow via Aave).

tBTC was created by a decentralized effort of contributors at the Threshold Network DAO, and extensively utilizes the Threshold Network's threshold cryptography to create a secure BTC asset. tBTC is a product launched on Threshold Network, on which many other decentralized applications are being built.

Threshold Network DAO was born out of the first on-chain merger between two decentralized protocols, Keep Network and NuCypher early in 2022. The DAO has successfully operated since that time, and supports an active community of contributors that work towards building tBTC liquidity and usability.

Benefits for Aave:

- Further decentralization and trust minimisation in the Aave stack.

- A range of lending options for those who wish to earn yield on their BTC.

- Collaboration with the Threshold Network DAO, opening up the opportunity to incorporate other Threshold products (such as Threshold Access Control and thUSD) into the Aave offering.

- Preferable yields on tBTC through active incentive participation, boosting Aave protocol use, fees and TVL.

- Additional incentive allocation originating from Arbitrium's LTIPP.

Specification

Ticker: TBTC

Contract Addresses:

Ethereum: 0x18084fba666a33d37592fa2633fd49a74dd93a88

Arbitrum: 0x6c84a8f1c29108f47a79964b5fe888d4f4d0de40

Optimism: 0x6c84a8f1c29108F47a79964b5Fe888D4f4D0dE40

Chainlink Oracle:

Ethereum: 0x8350b7De6a6a2C1368E7D4Bd968190e13E354297

Arbitrum: 0xE808488e8627F6531bA79a13A9E0271B39abEb1C

Optimism: 0x5a61374950D4BFa5a3D4f2CA36FC1d23A92b6f21

Risk parameters

Risk Parameters will be provided by Risk Services Providers at the earliest possible and ARFC will be updated with that

feedback.

Emission schedule

tBTC is one-to-one backed with real Bitcoin, meaning that there isn't an emissions schedule, but a mint and redeem function that adjusts the supply of tBTC based on native BTC coming into and out of the system.

Risks

For tBTC, wallets are created periodically based on governance. In order for the wallet to move funds, it produces signatures using a Threshold Elliptic Curve Digital Signature Algorithm, requiring 51-of-100 Signers to cooperate. The 100 signers on each wallet are chosen with our Sortition Pool, and the randomness is provided by the Random Beacon. More can be found here - [Wallet Generation | Threshold Docs 1](#)

The Threshold Council multisig is a 6/9 Gnosis Safe multisig with 9 unique signers that form the Threshold Network Council. The Council has limited upgrade privileges over the smart contracts. However, those privileges do not include any custodial power over deposited BTC:

Council Multisig Ethereum Address: 0x9F6e831c8F8939DC0C830C6e492e7cEf4f9C2F5f

Useful Links:

Project: https://www.threshold.network/

Minting dashboard: https://dashboard.threshold.network/tBTC/mint

GitHub: [GitHub - keep-network/tbtc-v2: Trustlessly tokenized Bitcoin everywhere, version 2](#)

Docs: [tBTC Bitcoin Bridge | Threshold Docs](#)

Audit: [About](#)

Immunfi Bug Bounty: [Threshold Network Bug Bounties | Immunefi | Immunefi](#)

Llama Risk Report: [Collateral Risk Assessment: Threshold BTC (tBTC) - HackMD](#)

Twitter: https://twitter.com/thetnetwork

Discord: [Threshold Network ✛](#)

Dune: https://dune.com/threshold/tbtc & https://dune.com/sensecapital/tbtc-liquidity

Disclaimer:

This proposal is powered by Skywards. The Aave Chan Initiative is not directly affiliated with Threshold Network and did not receive compensation for creation this proposal.

Next Steps:

1. Publication of a standard ARFC, collect community and service providers feedback before escalating the proposal to the ARFC Snapshot stage.

2. If the ARFC Snapshot outcome is positive, publish an AIP vote for final confirmation and enforcement of the proposal.

Copyright: