FBTC Whitepaper v1.1

An Omnichain BTC With Deep Liquidity and Diverse Yield Opportunities

Abstract

As the digital asset landscape continues to mature, the demand for interoperability and seamless asset flow across various blockchain ecosystems has become increasingly pronounced. FBTC stands out as a pioneering token initiative designed to bridge the liquidity divide between the Bitcoin and non-Bitcoin ecosystems, including their respective layer-2 (L2) networks. Despite the progress made in these networks, achieving frictionless asset transfers across diverse layers remains a significant challenge. FBTC aims to address this challenge by issuing tokens on both EVM-compatible networks and selected non-EVM networks, thereby enhancing asset liquidity and utility. This paper will present an omnichain BTC pegging protocol built on the Threshold Signature Scheme (TSS) network, extending the Bitcoin ecosystem across multiple chains with Turing-complete capabilities.

1. Introduction

Bitcoin, introduced by Satoshi Nakamoto's groundbreaking whitepaper in 2008, revolutionized finance and economy by facilitating trustless cross-border transactions. The growth of Bitcoin has been the precursor of all other blockchains and the cryptocurrency sector, and paved the way for innovations such as the Ordinals protocol and BRC-20, indicating the potential for asset issuance within its ecosystem. However, due to the non-Turing completeness of Bitcoin's script, implementing complex financial products on the Bitcoin main chain presents challenges. Consequently, unlocking the liquidity and application of Bitcoin assets has become a key focus.

1.1 FBTC Overview

FBTC will be deployed through a decentralized framework that involves multiple institutions overseeing the reserves, issuance processes, and a multi-stakeholder governance structure. These institutions will collectively ensure transparency and trust by implementing a proof of reserves system. This system verifies that the underlying Bitcoin assets backing FBTC are publicly disclosed and verifiably held on the Bitcoin network. Such an approach not only strengthens the reliability of FBTC, but also harnesses the strengths of both the Bitcoin and Ethereum networks, maximizing the benefits of blockchain technology.

1.2 FBTC Vision

FBTC aims to augment Bitcoin's existing attributes of security and decentralization by introducing universal liquidity and interoperability. As a beacon for a high-speed, low-friction, and interoperable future, FBTC heralds a new era of Bitcoin utility and velocity. Positioned to become the representative for Bitcoin transactions, FBTC aims to transform all other blockchains into Bitcoin L2 solutions. Beyond merely serving as a store of value, FBTC evolves Bitcoin into a liquid asset that is easily integrated into various yield enhancement strategies.

1.3 FBTC Value Proposition

- **Decentralized and Secure Infrastructure**
    - Decentralized Operations: FBTC employs a TSS network to conduct minting and redemption.
    - Secure Custody: FBTC works with reputable and trusted MPC custody providers to guarantee the security of the BTC principal.
- **Cross-Chain Interoperability and Composability**
    - Omnichain Interoperability: FBTC is minted on Ethereum by default and comes with seamless interoperability to enable a wide range of use cases on a wide range of L1s and L2s.
    - Composable With Blue-Chip DeFi Protocols: FBTC has struck an array of premium partnerships with top DeFi protocols and infrastructure partners.
- **Mass Adoption Readiness**
    - Initial Core Contributors: Antalpha Prime and Mantle.
    - Easy Access: FBTC can be acquired through minting or purchased through qualified users, DEXs and CEXs.

2. Background

Before delving into the overarching architecture of FBTC, this section will elucidate the challenges and development requirements currently facing Bitcoin. Additionally, it will provide an overview and brief analysis of related projects.

2.1 Challenges

The benefits of asset tokenization have been championed by many DeFi pioneers, with ERC20 emerging as the dominant token standard. Its merits in accelerating transactions, reducing intermediaries, and enhancing DeFi composability are evident. However, the adoption of tokenized assets still encounters various challenges. Taking Bitcoin, the top-ranked cryptocurrency, as an example: While initiatives such as wBTC have introduced wrapped BTC tokens to the Ethereum ecosystem, the Total Value Locked (TVL) in BTC-related ecosystems constitutes only 4% of the BTC token market size, which is considerably lower compared to the 75% TVL in ETH ecosystems for the ETH token market size.

BTC-tokenized projects often encounter several common challenges:

- **Centralized Wrapping:** Traditional wrapped BTC solutions grapple with centralization issues, restricted liquidity, and a lack of yield opportunities.
- **Security Vulnerabilities:** Vulnerabilities persist within wallets and exchanges, posing risks to users' assets.
- **Layer 2 Fragmentation:** The proliferation of disparate BTC L2 solutions complicates the ecosystem, and some of them curtail functionalities.
- **Need for Interoperability:** There is a growing demand for cross-chain capabilities to enhance utility and facilitate seamless asset transfers across different blockchains.

2.2 Related Work

Several pioneers have already made exploratory inroads into BTC-wrapped assets on multiple chains. There is compelling evidence that the business models of BTC-wrapped assets can be feasible and sustainable. The primary representatives of such are wBTC and sBTC, whose introductions are below.

wBTC

wBTC is an ERC20 asset pegged 1:1 to Bitcoin and stands as one of the most popular Bitcoin-wrapped assets among users. Its operation relies on centralized custodians for native asset locking and pegged-assets issuance. If a merchant wishes to convert their BTC into wBTC, they initiate the minting process by providing an Ethereum address to the Wrapped

Token contract. Subsequently, the merchant sends the actual Bitcoin to the custodian. The custodian mints wBTC and then transfers it to the merchant's Ethereum address.

sBTC

sBTC is designed as a Bitcoin-pegged asset, leveraging the Stacks Bitcoin layer and interaction with the Bitcoin main chain to achieve its peg mechanism. This approach offers a balance between high performance and decentralized security.

3. Protocol Overview

In the preceding chapters, protocols related to wrapped BTC assets were analyzed. This chapter will provide a detailed introduction to the FBTC protocol and its modules, expounding its design philosophy and technology workflow.

3.1 Overview

FBTC is a wrapped BTC protocol based on the TSS network, leveraging multiple chains' Turing completeness to provide secure Bitcoin scalability. Utilizing a decentralized multi-party computation TSS network enhances the security of the bridges, protecting user assets in various ways. Additionally, it introduces a cross-chain hub that supports multi-chain interoperability, mitigating to some extent the issues caused by the explosive growth of some Bitcoin L2 solutions.

Given the numerous risks associated with transferring BTC assets across different chains, we have partnered with industry leaders to ensure asset safety and minimize risks. Our protocol solutions are tailored for the BTC ecosystem and its stakeholders, and effectively address security concerns when traversing multiple chains.

3.2 Technical Perspectives

3.2.1 System Architecture

The FBTC protocol's architecture is primarily structured around three main components: custodial addresses on the Bitcoin main chain, smart contracts on destination chains, and off-chain modules.

3.2.1.1 Custodial Addresses on the Bitcoin Main Chain

The system will generate a Bitcoin network deposit address for each qualified user, controlled by the MPC nodes. After qualified users deposit Bitcoin to their respective addresses, FBTC will be issued to the corresponding qualified user on the destination chain.

The total amount of Bitcoin locked on the Bitcoin address controlled by the MPC wallet will be consistent with the total supply of FBTC on the destination chain.

3.2.1.2 Smart Contracts in Destination Chains

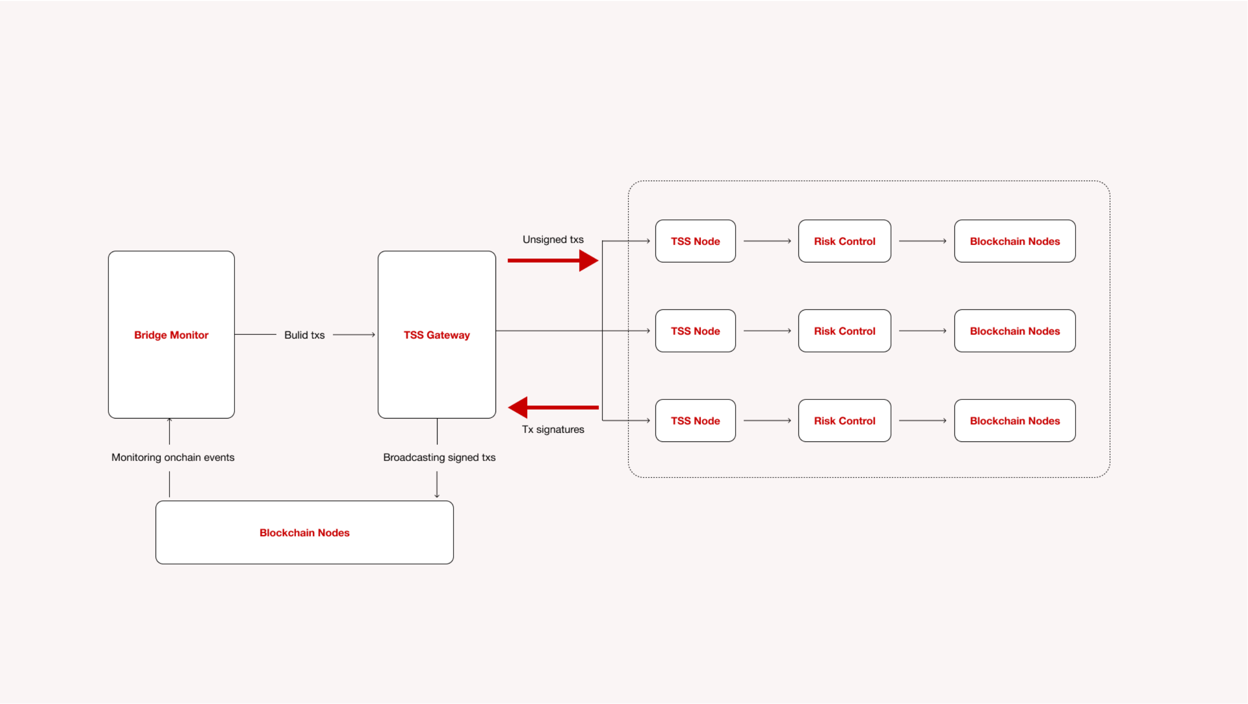
For the Turing-completeness chains, a series of smart contracts are deployed to manage various functionalities:

- **Bridge Contract:** Carry out qualified user management and complete the FBTC issuance, and cross-chain-related operations of FBTC.

- **FBTC Contract:** FBTC will utilize the smart contracts to supply and transfer the tokens, such as ERC20 Token Contract on Ethereum.

3.2.1.3 Off-Chain Modules

In addition to on-chain contracts, several off-chain services play a crucial role in supporting the FBTC ecosystem:



- **Bridge Monitor:** Bridge monitor monitors newly submitted minting, burning, and cross-chain requests and checks whether the request meets the pre-defined requirements. If the request is legitimate, the constructed destination chain transaction will be submitted to the TSS Gateway. Bridge Monitor can only submit unsigned transactions to TSS Gateway. After a transaction is submitted, it will undergo strict scrutiny by the risk control system of every TSS node. After all risk control checks are passed, the transaction will be signed and broadcast to the node.

- **TSS Gateway:** The gateway that coordinates TSS Nodes is used to send signing requests to each TSS Node, collect the final TSS signature results, and broadcast them to the chain.

- **TSS Node:** This is used to generate TSS private key shares and use them for signing. Each party's TSS Node can configure its Risk Control module.

- **Risk Control:** This module can obtain information through trusted blockchain nodes, check each signing request received, and only signing requests that meet all predefined rules will be permitted.

- **Blockchain Nodes:** Standard Bitcoin or other network blockchain nodes. Each MPC participant can run its relevant blockchain node to reduce single-point risks or choose a trusted third-party node.

3.2.2 Key Roles

Qualified Users

An entity or a party that mints FBTC from BTC and burns FBTC into BTC is known as a qualified user. A qualified user can be an institution, an individual or a merchant. Each qualified user will have to fulfill certain requirements and complete Know Your Customer (KYC) or Know Your Business (KYB) before onboarding. Qualified users play a pivotal role in the distribution of FBTC.

Custodians

Custodians manage users' assets in an MPC address whose key shares are held by several trusted institutions. The MPC solution guards the user-deposited BTC and conducts the FBTC issuance under restricted risk control in a decentralized way.

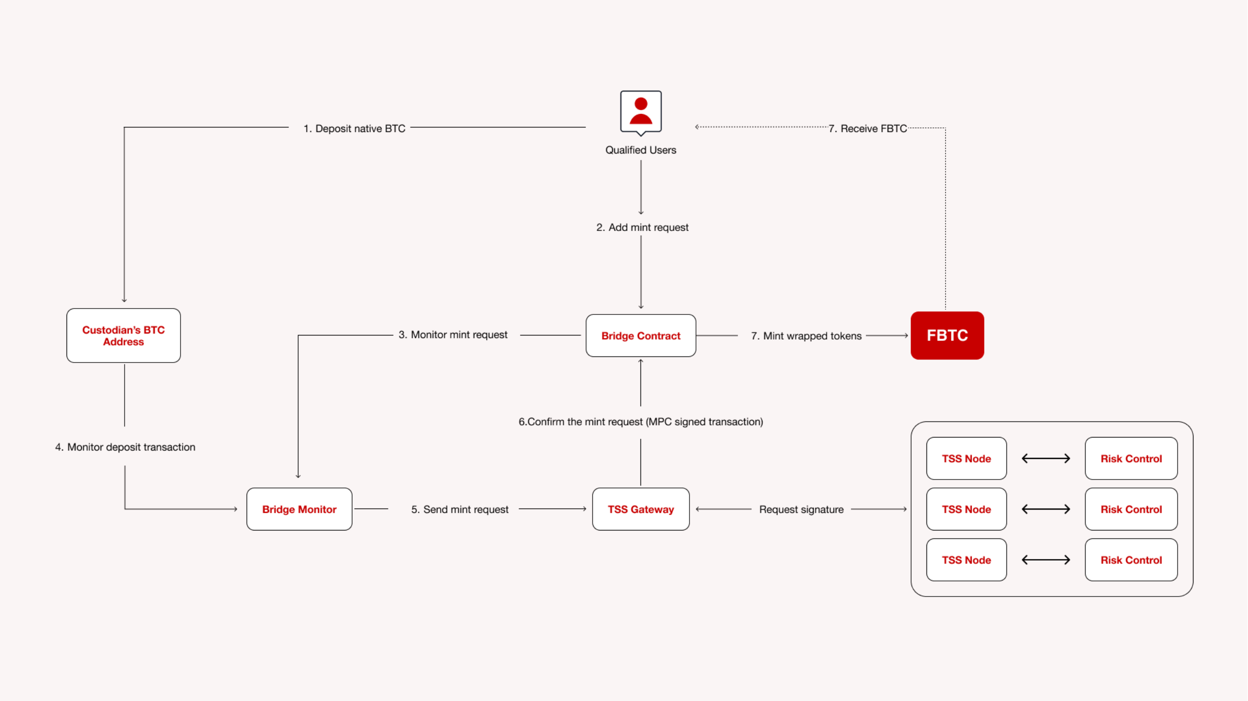
Security Council

FBTC has introduced a Security Council, which is responsible for BTC custodian MPC multi-signature and the bridge's TSS Nodes running. Currently, Mantle, Antalpha Prime, and Cobo serve as the initial council members, with plans to gradually introduce more trusted council members.

3.2.3 Core Process

3.2.3.1 Mint

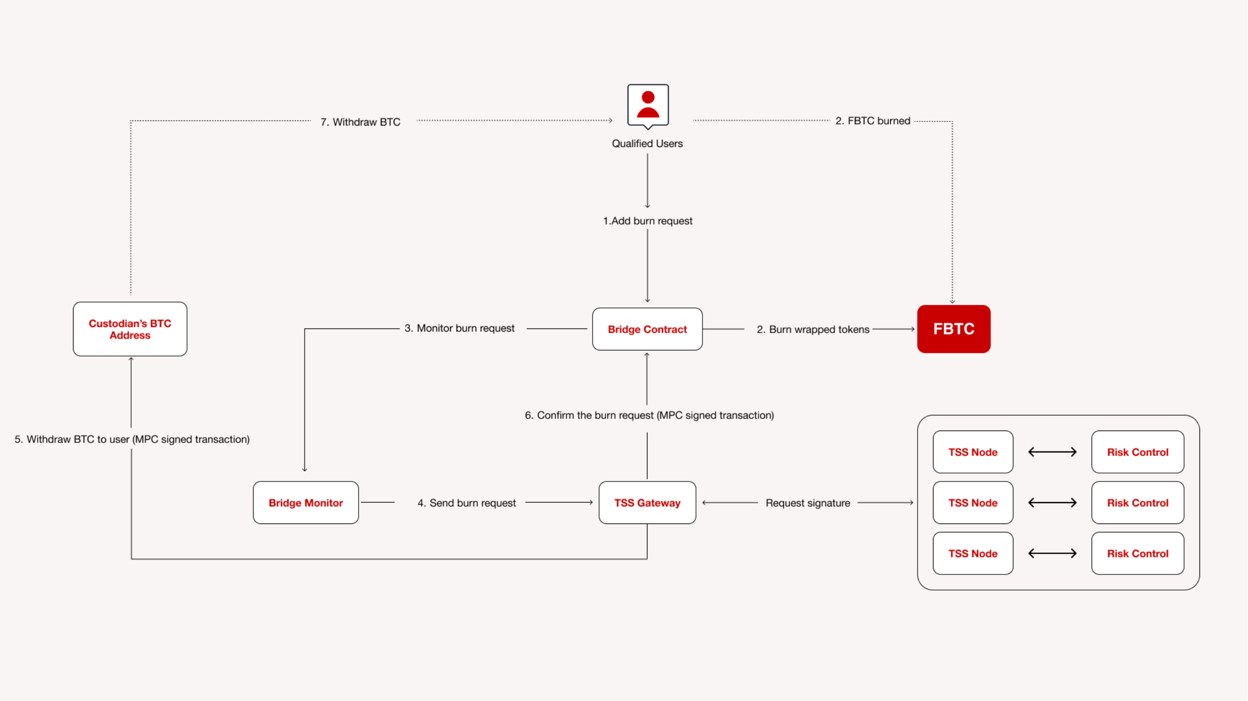
The operation of depositing BTC to the Bitcoin main chain and minting FBTC is only initiated by qualified users. The process is illustrated as follows.



1. Qualified users transfer native BTC to a pre-configured custodial address.
2. Qualified users interact with the Bridge contract and initiate a mint request.
3. The Bridge Monitor that monitors on-chain events in real-time detects the minting request.
4. Bridge Monitor also monitors BTC deposit transactions on the Bitcoin main chain.
5. Bridge Monitor sends the minting request to TSS Gateway.
6. TSS Gateway initiates a contract to confirm the minting of the Bridge contract. Multiple TSS Nodes co-sign through the MPC algorithm construct the transaction signature. Each TSS Node operates an independent risk control system that validates the deposit transactions and minting requests to secure the FBTC minting.
7. After the minting transaction is confirmed on the destination chain, the FBTC token is minted.

3.2.3.2 Burn

The request to burn FBTC and withdraw the underlying BTC can only be initiated by qualified users. The process is illustrated as follows.



1. A qualified user interacts with the Bridge contract and initiates a burn request.

2. The Bridge contract burns the qualified user's FBTC token.

3. The Bridge Monitor monitors the burn request event.

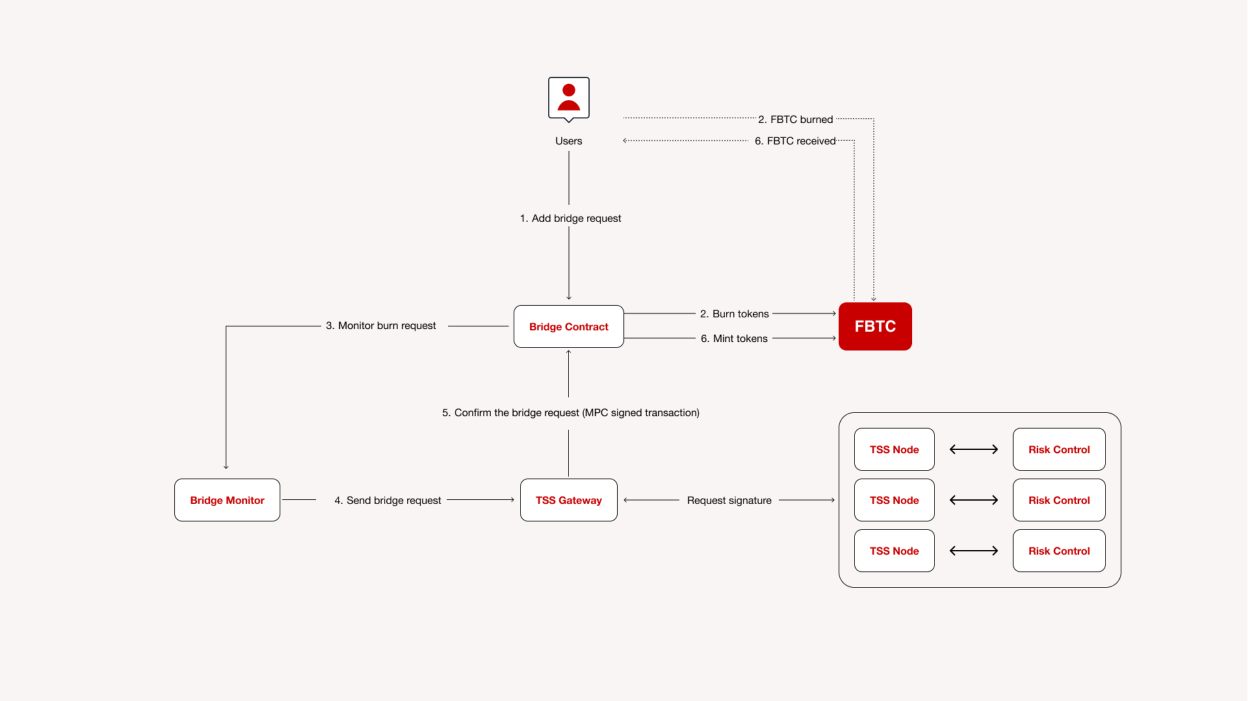
4. Bridge Monitor sends the withdrawal request to TSS Gateway.

5. TSS Gateway initiates a BTC transfer, and transfers the specified amount of BTC to the pre-configured withdrawal address of the qualified user. Multiple TSS Nodes co-sign through the MPC algorithm construct the transaction signature. Each TSS Node operates an independent risk control system that validates the BTC transfer transactions and burning requests to secure the FBTC unwrapping.

6. After the withdrawal transaction is confirmed on the Bitcoin main chain, TSS Gateway calls the Bridge contract to confirm that the withdrawal request has been processed.

3.2.3.3 Cross-Chain

All end users holding FBTC can initiate cross-chain requests to transfer their FBTC assets to other L1/L2 blockchain networks. The process is illustrated as follows.



1. A user interacts with the bridge contract from the source chain and initiates a cross-chain request.

2. The Bridge contract burns the user's FBTC.

3. Bridge Monitor monitors events on the source chain in real-time and detects the cross-chain request immediately.

4. Bridge Monitor sends the cross-chain request to TSS Gateway.

5. TSS Gateway initiates a contract call to the Bridge contract on the destination chain to confirm the FBTC cross-chain operation. Multiple TSS Nodes with individual risk control co-sign the confirmation transaction.

6. After the cross-chain transaction is confirmed on the destination chain, the specified number of FBTC tokens are minted for the users.

FBTC will expand its presence across multiple blockchain networks, enhancing its interoperability and utility. As the digital asset landscape continues to evolve, FBTC aims to explore and integrate with various blockchain ecosystems, unlocking new opportunities and expanding its reach across the broader crypto space.

3.3 Locked FBTC

FBTC possesses versatile applicability across diverse scenarios. This utilizes the tokenization of Bitcoin across multiple chains, facilitating seamless interoperability and accessibility. Additionally, we have introduced locked FBTC to facilitate native BTC based yield strategies in partnership with selected partners.

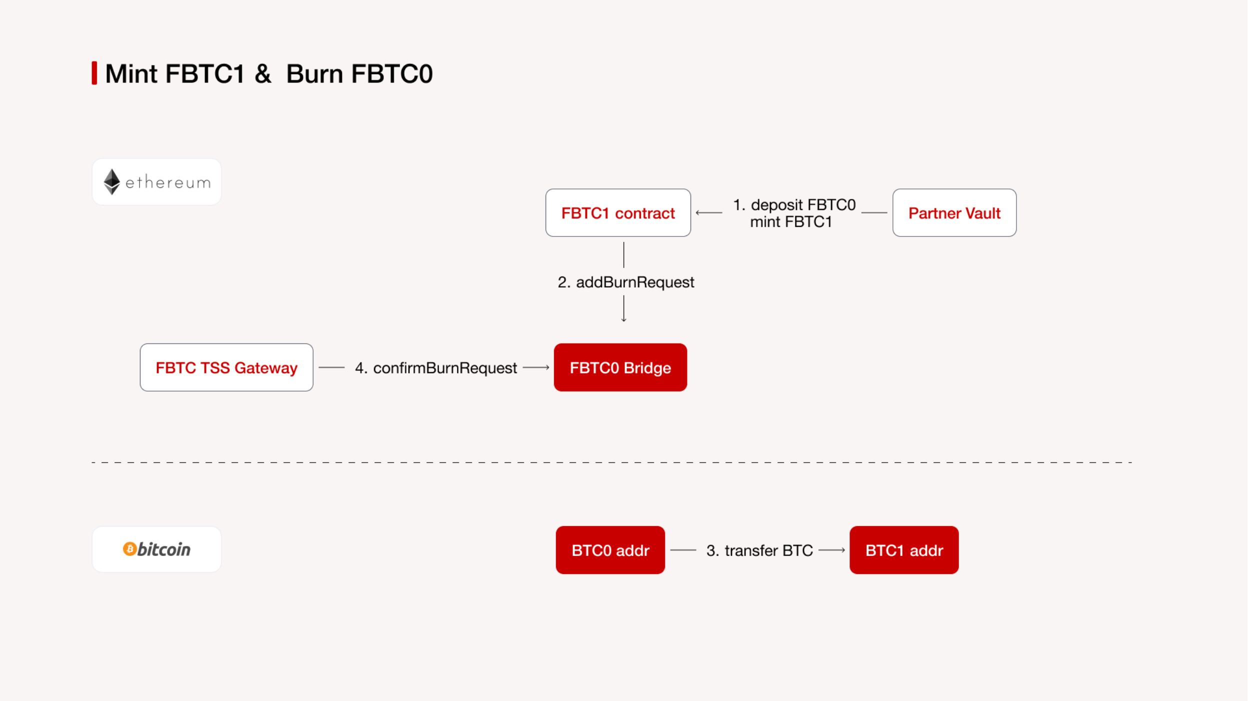
Standard FBTC, namely FBTC0 for easy reference, is 1:1 wrapped BTC, backed by native BTC held in address BTC0. Locked FBTC, namely FBTC1 for easy reference, is locked in partner dApps, backed by native BTC held in a separate address BTC1. Each locked FBTC is created for a dedicated partner protocol.

Type	Bitcoin Host Plan	FBTC Status
Standard FBTC (FBTC0)	MPC address managed by FBTC security council	Free circulation
Locked FBTC (FBTC1)	MPC address managed by FBTC security council and dedicated partner	Restricted: Not transferable

3.3.1 Mint Locked FBTC

When a FBTC0 holder decides to stake FBTC0 with a partner protocol, FBTC0 is staked under Partner Vault. Partner Vault may burn FBTC0 and mint FBTC1 to obtain the underlying native BTC for a dedicated yield strategy.

The process is illustrated as follows.

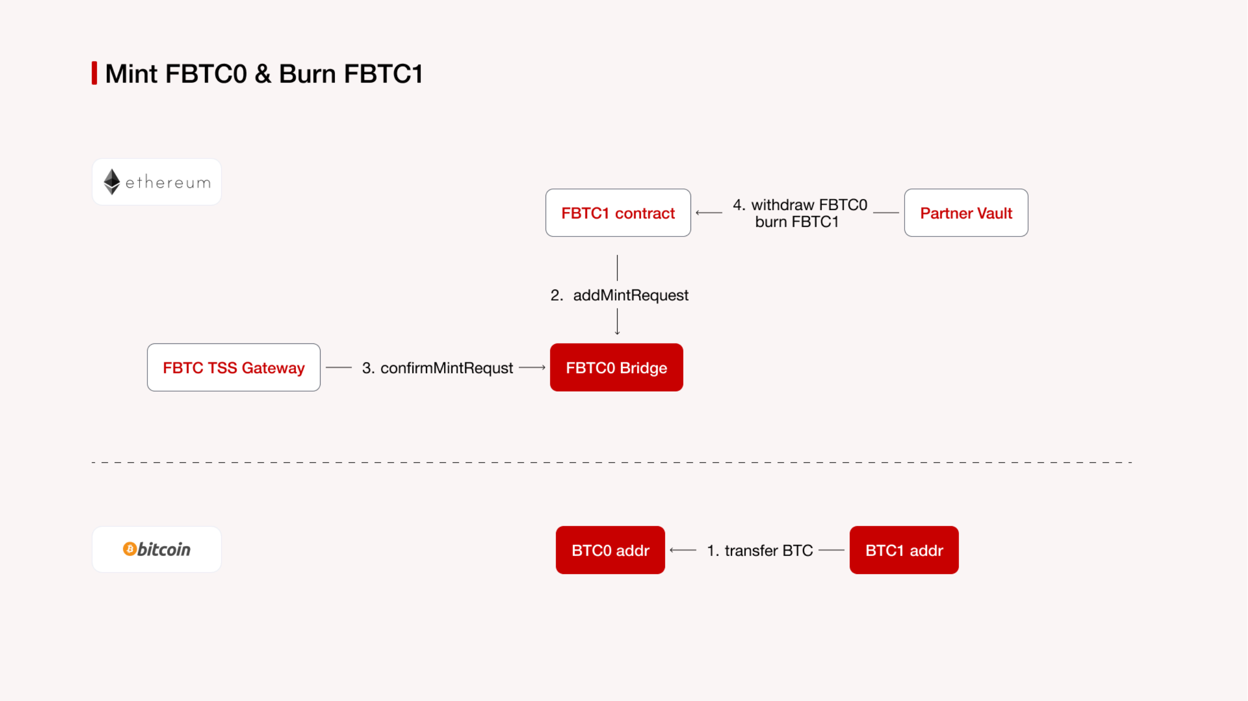


1. A FBTC0 holder transfers his FBTC0 to a partner's vault.
2. Periodically, Partner deposits FBTC0 to FBTC1 contract to initiate a request to mint FBTC1 and burn FBTC0.
3. Bridge Monitor sends the withdrawal request to transfer the corresponding BTC from FBTC0 address to FBTC1 address. FBTC1 address is for Partner's yield strategy use only.
4. FBTC TSS Gateway confirms the FBTC0 is burned properly.

3.3.2 Burn Locked FBTC

When a user decides to redeem FBTC from the partner protocol, Partner may return the underlying BTC, burn FBTC1 and mint FBTC0 to return to the user.

The process is illustrated as follows.



Mint FBTC0 & Burn FBTC1

1. A user initiates a request to redeem FBTC. Partner may collect such requests, and transfers BTC from BTC1 address to standard FBTC's custody address BTC0 periodically.
2. Once BTC is received at FBTC0 address, FBTC1 contract initiates a request to mint FBTC0.
3. FBTC TSS Gateway will confirm FBTC0 is minted.
4. Partner Vault withdraws FBTC0 from FBTC1 contract and burns FBTC1 at the same time.
5. Partner returns FBTC0 to the user from Partner Vault.

4. Security

4.1 Enhanced Ecosystem Back

The realization of FBTC's vision relies heavily on robust ecosystem support. Drawing from the experiences of pioneering projects, FBTC will focus on developing its ecosystem in the following four areas:

- Integrating with Bitcoin's Staking protocols (such as Babylon) to introduce native staking into FBTC.
- Integrating with high-frequency trading profit vaults (such as Solv) to enable FBTC's utilization in CEX funding rate arbitrage.
- Integrating with leading exchanges, custody service providers, and financial service companies in the centralized finance (CeFi) space, FBTC can be adopted as collateral for lending and contract margin.
- Sharing more benefits from on-chain projects, such as pre-mining in Bitcoin L2 ecosystem projects and integration and reward acceleration in leading DeFi projects such as Pendle.

4.2 Trust Model

In cryptocurrency, trust stands as a cornerstone, especially concerning wrapped tokens. Our approach meticulously addresses this vital requirement through key features:

- **1:1 Reserve Assurance:** Ensuring both BTC and FBTC maintain a 1:1 reserve, with stringent constraints preventing any single stakeholder from breaching this ratio.
- **Decentralized Operations:** Prioritizing decentralized operations to foster broad token creation and exchange adoption.
- **Trusted Custodianship:** The implementation requires collaborating with industry-leading custody solution providers. For instance, Cobo provides the underlying MPC technology to protect the BTC principal. Such precautions mitigate risks and bolster user confidence in asset security.
- **Security Council:** The Security Council is responsible for BTC custodian MPC multi-signature and the bridge's TSS Nodes running. Currently, Mantle, Antalpha Prime, and Cobo serve as the initial council members, with plans to gradually introduce more council members.
- **Transparency Initiatives:** Committing to transparency, FBTC will publicly disclose proof of asset reserves on its official website, enhancing overall trust and accountability.

4.3 Regulatory Compliance

We prioritize diligent adherence to financial regulations and compliance as vital components of our operations. Custodians and potential users of FBTC must obtain appropriate licensing based on their respective jurisdictions. Moreover, custodians and market participants involved in the minting, redemption, and transfer of FBTC are required to undergo mandatory Know Your Customer (KYC) and Anti-Money Laundering (AML) processes. Following compliance regulations and implementing regulatory standards, information from the mandatory currency transaction reports and suspicious activity reports will be collected and securely stored.

- **Crypto Anti-Money Laundering (AML)** encompasses the mandates for regulated institutions to thwart criminal transactions, aiming to impede the ingress of illicit funds into the legitimate financial system. Critical steps in this process encompass KYC measures can be including but not limited to:
    - Establishing customer identity.
    - Understanding the nature of clients' financial activities and the legitimacy of the funding sources.
    - Assessing money laundering risks associated with customers.
- **Know Your Customer (KYC)** is integral to AML, entailing the establishment and enforcement of policies, training initiatives, designated responsibilities, and review protocols. Screening accounts against watchlists, monitoring transactions, and employing a flexible, risk-based verification approach are pivotal in ensuring compliance with AML regulations.

In certain situations, crypto businesses are mandated to conduct enhanced due diligence on the customers. EDD necessitates heightened scrutiny of customer identity and behavior. High-risk customers encompass politically exposed persons, individuals engaging in frequent, high-value transactions, and customers hailing from high-risk jurisdictions, among other criteria.

4.4 Decentralized Governance

For asset-packaged programs such as FBTC, governance complexity has been a perennial challenge. Fortunately, many successful projects have led the way with best practices in decentralized governance. By incorporating key stakeholders into the DAO membership list and implementing on-chain voting via governance tokens, a fair and decentralized governance becomes achievable.

5. Tokenomics

The FBTC token is meticulously designed for seamless integration within the multiple chains (Ethereum, EVM-compatible L2s, Alt-L1s, etc.) and Bitcoin ecosystems, offering users a stable and trustworthy medium to capitalize on the strengths of both networks. By facilitating the movement of Bitcoin assets in the broad blockchain infrastructure, FBTC aims to boost liquidity across diverse blockchain layers, paving the way for new opportunities in user engagement and decentralized finance application development.

5.1 Governance

The FBTC token contract operates under the governance of a multi-signature contract, ensuring enhanced security and decentralization. This governance model necessitates the signature of DAO members for adding or removing members, providing a robust framework for membership management.

All custodians and qualified users are inherently recognized as DAO members, but the door remains open for other organizations to join, irrespective of their role as custodians or qualified users. This inclusive approach fosters diversity within the DAO, encouraging broader participation and collaboration across the ecosystem.

Notable multi-signers already committed to the DAO include Mantle, Antalpha Prime, Cobo, and various insurance organizations, each bringing unique expertise and perspectives to the governance table.

The execution of contracts within this DAO framework utilizes an "M of N" signature scheme. Here, “M” signifies the minimum number of required signatures for any multi-signature contract, while “N” represents the total count of DAO members. The DAO members' precise values for “M” and “N” are collaboratively determined, ensuring a balanced approach to decision-making and governance.

This multi-signature governance mechanism reinforces transparency, trust, and accountability within the FBTC ecosystem, aligning with the principles of decentralized finance and community-driven initiatives.

5.2 Fee Mechanism

- **Minting Fees:** Minting fees refer to the costs associated with creating FBTC on the destination chain by depositing BTC on the Bitcoin main chain. When qualified users mint FBTC, they may incur blockchain gas cost, which varies depending on network condition. There is no additional minting fee charged besides gas cost.

- **Redemption Fees:** Redemption fees refer to the costs associated with burning FBTC on the destination chain and redeeming BTC on the Bitcoin main chain. There may be a redemption fee in addition to the gas cost.
- **Merchant Fees:** Merchants may impose a fee when users acquire FBTC through them. These fees serve as compensation for the services rendered by merchants, and play a crucial role in sustaining their operations within the FBTC ecosystem.
- **Bridging Fees:** To optimize cost reduction for users and enrich their experience, the smart contract may apply an extra fee when bridging assets across multiple chains, alongside the gas fee.

6. Conclusion

Within the dynamic realm of blockchain technology, a significant challenge persists in connecting the realms of Bitcoin and applications of decentralized finance (DeFi). The recent surge in BTC L2s and side chains has highlighted the urgent need for a solution that offers seamless connectivity, enhanced interoperability, and widespread adoption. FBTC arrives as a groundbreaking initiative designed to address these challenges head-on.

FBTC serves as a tokenized, decentralized, and universal representation of Bitcoin, aiming to unify Bitcoin outbound liquidity and bolster interoperability across various blockchain ecosystems. By leveraging the robust infrastructure of Mantle initially, FBTC establishes a secure and efficient corridor between the Bitcoin and Ethereum Virtual Machine (EVM) ecosystems. This strategic positioning facilitates permissionless creation and redemption, fosters broader adoption, and unlocks new avenues for yield generation within the DeFi landscape.

In conclusion, FBTC represents a pivotal step towards realizing Bitcoin's full potential, transcending its traditional boundaries, and paving the way for a more interconnected, efficient, and inclusive financial ecosystem.

7. Core Contributors and Partners

MANTLE

ANTALPHA PRIME

Supported by industry-leading core contributors such as Antalpha Prime and Mantle, FBTC benefits from liquidity bootstrapping and additional yield offerings, reinforcing its value proposition and stability. With its commitment to becoming the most widely adopted and fully decentralized tokenized BTC, FBTC aspires to unlock the untapped potential of Bitcoin's true growth power, velocity, and value adoption in the dynamic DeFi world.

Additionally, FBTC has collaborated with various partners to facilitate widespread adoption. Cobo stands out as one of FBTC's early partners. We warmly invite potential partners to join our ecosystem without hesitation. By continuing to invite stakeholders from diverse backgrounds, industries, and perspectives to collaborate, we can harness the full potential of Bitcoin and unlock innovative solutions that benefit individuals and communities worldwide.

Bitcoin embodies invaluable freedom, worldwide consensus, and a robust democracy. As we embark on this journey to make Bitcoin great again, remember that our collective efforts drive its success. Together, we can continue to push the boundaries of what's possible with Bitcoin and create a future where financial freedom is accessible to all.