tBTC

https://threshold.network/

https://docs.threshold.network/

GitHub

ChatGPT

Grok

Gemini,

Threshold Networkについて

会社名ではなく、2つのプロジェクトが合併して誕生した名前。

Keep Network : 分散型カストディ tBTC v1を開発

NuCypher : 暗号関係の開発

運営は Threshold DAO がになっていて、基盤トークンは T(Threshold Token)

tBTCとは

Grok

2025/09現在は tBTC v2

2025/10/07現在でmainnet運用していない

Bitcoin – Ethereum 間のブリッジプロトコル

ERC-20 の wrapped token

つまり BTC を EVMチェーンに持ち込むためのもの

1tBTC = 1BTC という完全裏付け型

主要コンポーネント

Threshold Networkのノード（キーパー）

tBTCのブリッジは、Threshold Networkの分散型ノード群（キーパーと呼ばれる）によって運営されます。これらのノードは、ビットコインの預け入れ（デポジット）や引き出し（リデンプション）を監視し、tBTCの発行や焼却を管理します。

BTC Vault

ビットコインをロックするためのビットコインネットワーク上のマルチシグウォレット。ユーザーがBTCを預けると、このウォレットに資金が保管されます。

TBTC Vault（イーサリアム側）

イーサリアム上のスマートコントラクトで、tBTCの発行と管理を担当。BTC Vaultに預けられたBTCに応じてtBTCをミント（発行）します。

Bank Contract

ブリッジの財務管理を行うコントラクトで、tBTCのリデンプションフィーやその他の資産を管理。例として、Bank Contractでは残高確認や手数料管理が行われます。

Governor Bravo Timelock Controller

ガバナンス提案の実行を管理するコントラクト。リデンプションフィーの引き出しや送金などの操作は、このコントラクトを通じて承認されます

鍵は 3つある

Keep署名者グループの鍵

通常使いの鍵で、デポジットでユーザはこの鍵だけのアドレスに送金する

これが GG18ベースの TSSによって多数のノードに分散している

tBTCコントラクトの緊急停止用鍵

Threshold DAOの鍵

ブリッジのプロセス

デポジット

ユーザは Threshold Network のブリッジインターフェースを通じて指定されたデポジット用アドレスに BTC送金

BTC Vault は 2-of-3 マルチシグだが、デポジット用アドレスは Keep署名者グループ鍵のアドレスを使う

Threshold Networkのキーパーがビットコインネットワーク上でトランザクションを確認し、預け入れが正当であることを検証

検証後、TBTC Vaultスマートコントラクトが同量のtBTCをユーザーのイーサリアムウォレットに発行

スマコンの呼び出しはキーパーが出してくれる

リデンプション

tBTCの提出

ユーザーがtBTCをTBTC Vaultに送り、リデンプションをリクエスト。

リクエストはユーザがスマコンを呼び出す必要があるそうだ。

手数料の徴収

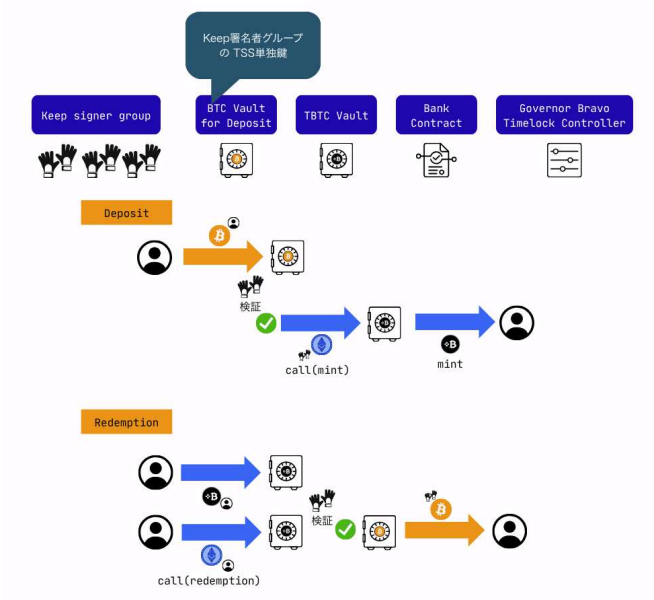
リデンプションには少額の手数料（Redemption Fees）がかかり、これがThreshold DAOの収益の一部となる（例: TIP-105で約10.5 tBTCの手数料が蓄積）。

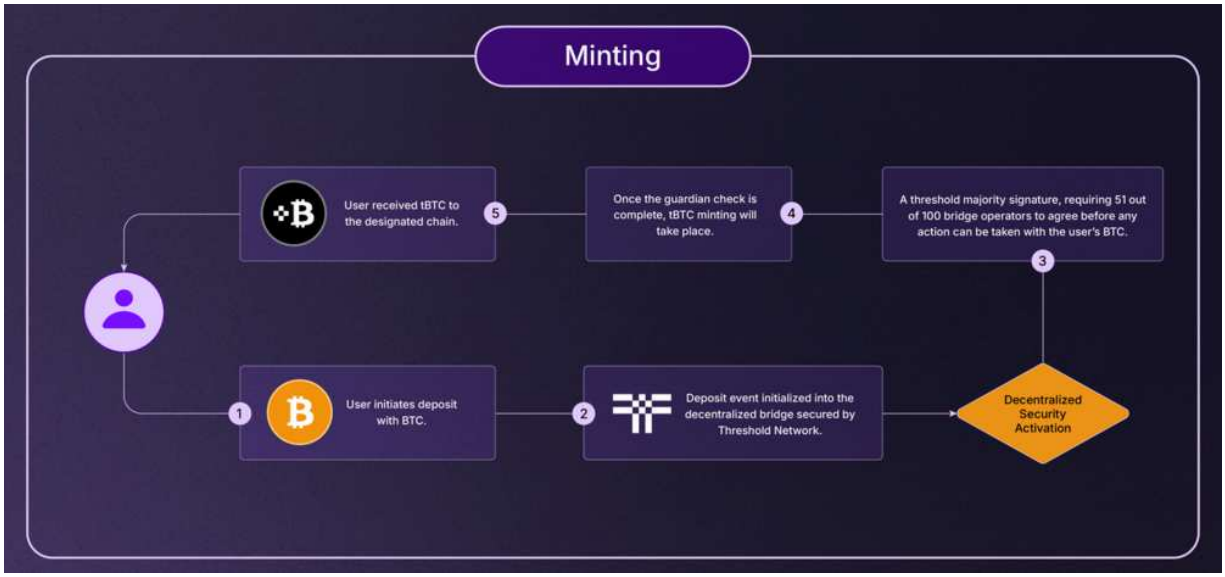
BTCの解放

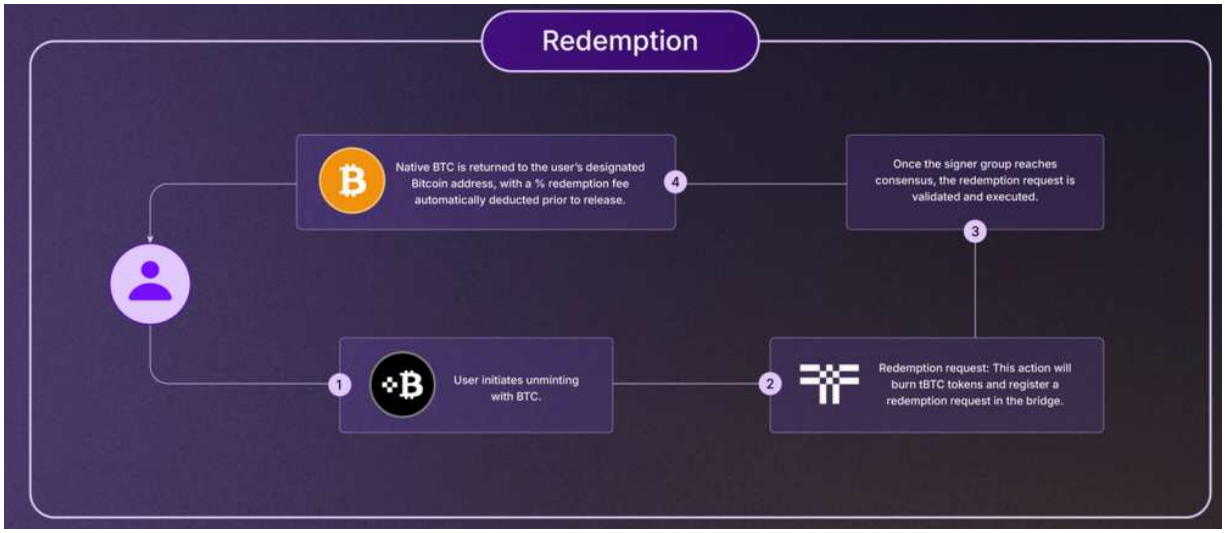
キーパーがリクエストを確認し、BTC Vaultから対応するBTCをユーザーのビットコインアドレスに送金。

tBTCの焼却

リデンプションが完了すると、提出されたtBTCは焼却され、総供給量が調整される。







自称「permissionless bridge」

だが、もちろんそんなことはない。せいぜい trust-minimized bridge。

~~FROST + ROAST で分散している~~ 現在は GG18 というアルゴリズムを使っている(ECDSA)

署名ノードは誰でも参加できる設計を検討している

ユーザは登録など無しで tBTC の mint を依頼できる

が、現状(2025/09)では署名ノードは許可したノードしか参加していない **permissioned**

The Path to Permissionlessness - Threshold Docs

BitVMや FROSTなどで 1-of-N ができるまではこのままらしい