TradBTC : Institutional Yield Vaults for BTC

Abstract

The Bitcoin Finance (BTCFi) sector has traditionally been constrained by the illiquidity of staked assets, limiting their utility in dynamic financial ecosystems.

This white paper introduces a novel framework that redefines BTCFi through the creation of derivative primitives built atop these staked assets. By leveraging institutional yield vaults on the Babylon protocol, we enhance baseline yields from 0.5–1% APY to a target range of **7–12%** APY.

This approach integrates synthetic asset creation, strategic partnerships, and robust settlement mechanisms to provide liquidity, yield optimization, and risk-managed exposure for participants.

Core Framework Overview

At the heart of this system is the Institutional Yield Vault with low risk strategic (max Entropic Value at Risk of 3-5%), a structured product designed to aggregate and optimize staked Bitcoin (BTC) holdings.

Each vault is partnered with a dedicated institutional entity that executes Net Asset Value (NAV) based monthly strategies (in options, perps, structured products, etc.), ensuring professional management and performance alignment. To initiate operations, each vault requires a minimum kickoff amount, establishing a threshold for viability and scale.
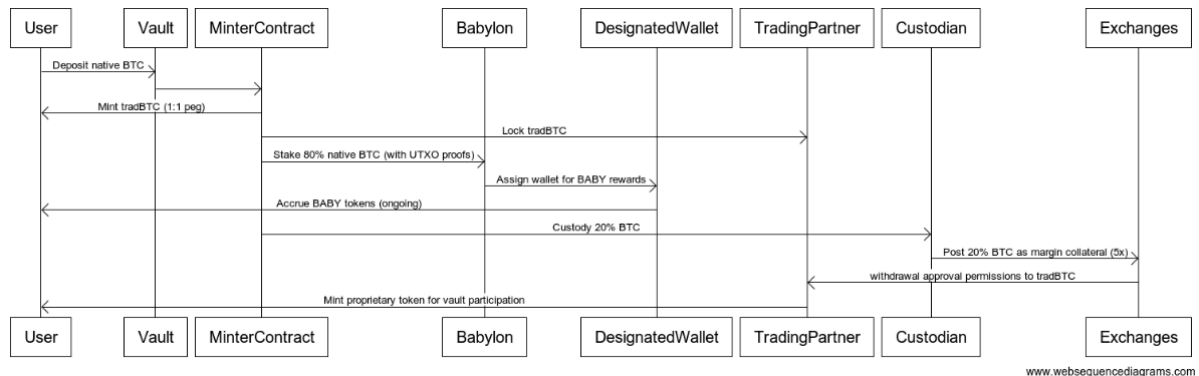
The vault's primary innovation lies in the issuance of a synthetic asset, termed **tradBTC** - a yield-bearing, BTC-backed ERC-20 token.

Minting and Allocation Process

Participants interact with the system via a minter contract, which facilitates the conversion of native BTC into tradBTC at a 1:1 price peg. Upon receipt of native BTC:

- **80% Allocation to Staking**: This portion is directly staked on the Babylon protocol, with on-chain UTXO proofs verifying the commitment (non custodial). This can also be done with existing LST protocols like LBTC, SolvBTC, etc. A designated wallet is assigned to each user to accrue BABY reward tokens.
- **20% Allocation to Custody and Liquidity Provision**: The remaining native BTC is securely custodied with secure custodians such as *Ledger, Anchorage Digital*. The custodied BTC is posted as margin collateral (**5x margin, for the full amount**) for market makers (MMs), trading desks or exchanges (such as Deribit, Binance, Coincall, etc.) executing trades. *These third parties are directly integrated as asset allocators with the custodian*. These entities are granted controlled withdrawal access to the locked tradBTC with the institutional trading partner (*explained below*), to eliminate counterparty risk.

The tradBTC tokens are subsequently locked with the designated trading partner for the vault, who provide us with their LP token to represent participation in the vault's strategy.

Sequence diagram (participants: User, Vault, MinterContract, Babylon, DesignatedWallet, TradingPartner, Custodian, Exchanges):
- User → Vault: Deposit native BTC
- Vault → User: Mint tradBTC (1:1 peg)
- Vault → TradingPartner: Lock tradBTC
- MinterContract → Babylon: Stake 80% native BTC (with UTXO proofs)
- Babylon → DesignatedWallet: Assign wallet for BABY rewards
- Babylon → User: Accrue BABY tokens (ongoing)
- Babylon → Custodian: Custody 20% BTC
- Custodian → Exchanges: Post 20% BTC as margin collateral (5x)
- Exchanges → Custodian: withdrawal approval permissions to tradBTC
- MinterContract → User: Mint proprietary token for vault participation
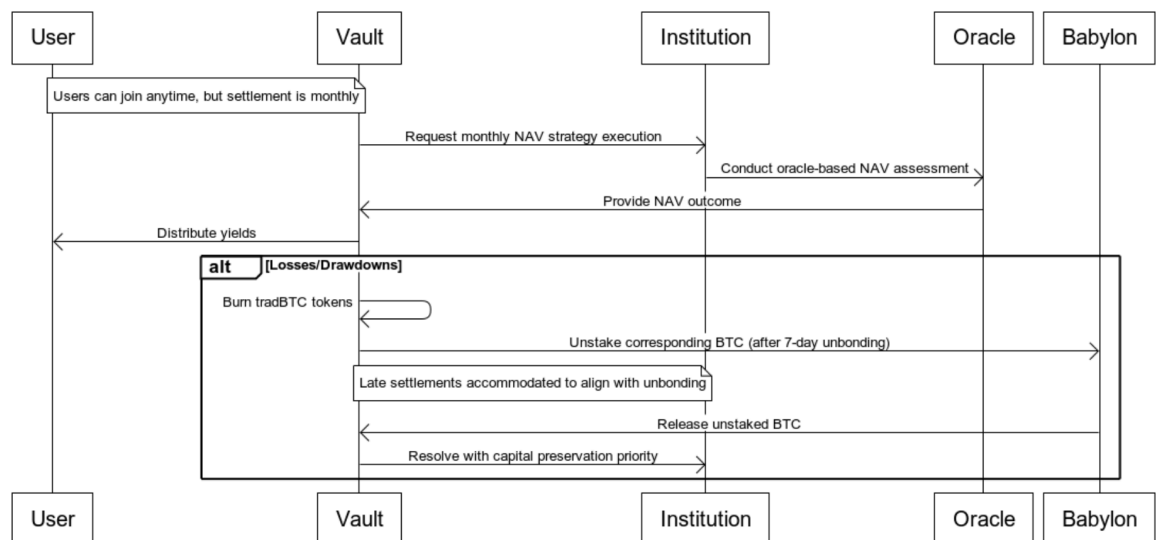
www.websequencediagrams.com

Settlement and Yield Distribution

Vault participation is flexible, allowing users to join at any time. However, all participants adhere to a unified monthly settlement date, promoting synchronized NAV evaluations and equitable distribution.

Settlement occurs at the end of each monthly cycle, utilizing **Pyth Network for Oracle-Based NAV Assessment** to be conducted in collaboration with the institutional yield provider. Outcomes are handled as follows:

- **Profits**: Yields are distributed native BTC/BABY tokens, reflecting the vault's performance and reward accruals.
- **Losses**: In the event of drawdowns, resolution prioritizes capital preservation. tradBTC tokens are burned, and the corresponding BTC is unstaked following Babylon's 7-day unbonding period. Late settlements are accommodated, as the monthly NAV process with institutional partners can extend to align with this timeline.
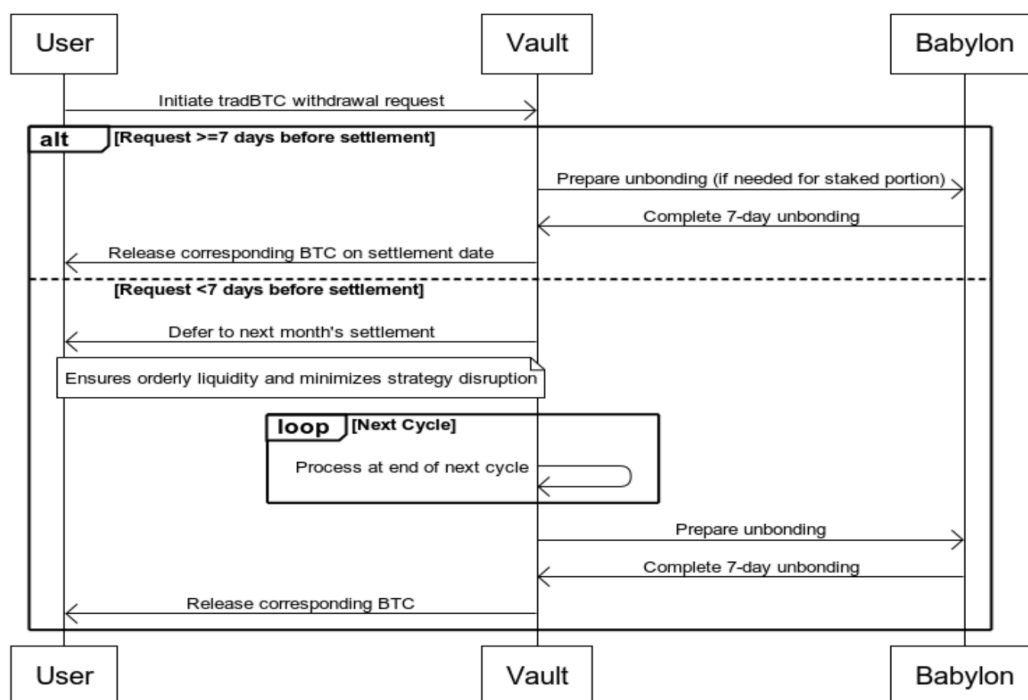
Sequence diagram (participants: User, Vault, Institution, Oracle, Babylon):
- Note over Vault: Users can join anytime, but settlement is monthly
- Vault → Institution: Request monthly NAV strategy execution
- Institution → Oracle: Conduct oracle-based NAV assessment
- Institution → Vault: Provide NAV outcome
- Vault → User: Distribute yields
- alt [Losses/Drawdowns]
  - Vault → Vault: Burn tradBTC tokens
  - Vault → Babylon: Unstake corresponding BTC (after 7-day unbonding)
  - Note over Vault: Late settlements accommodated to align with unbonding
  - Babylon → Vault: Release unstaked BTC
  - Vault → Institution: Resolve with capital preservation priority

Using Pyth Network for Oracle-Based NAV Assessment in TradBTC Vault.

We will use Pyth Network for the monthly NAV settlement of TradBTC Institutional Yield Vaults. At the end of each cycle, the institutional partner runs an off-chain calculation that pulls real-time Pyth price feeds (Deribit BTC-PERP mark price) via the Pyth Benchmark API. The partner then computes the exact NAV per underlying BTC (factoring in Babylon staking value, accrued BABY rewards, and the full PnL of the 20 % derivatives tranche), and signs a message for that vault, cycle number, navPerBTC, and timestamp. Pyth gives us fast, manipulation-resistant, fully verifiable monthly NAV settlement using the same oracle infrastructure that already secures $50B+ across Morpho, Aevo, Synthetix, and most major perp/option venues, no custom oracle, no centralised price server, just institutional-signed math anchored to Pyth's data providers.

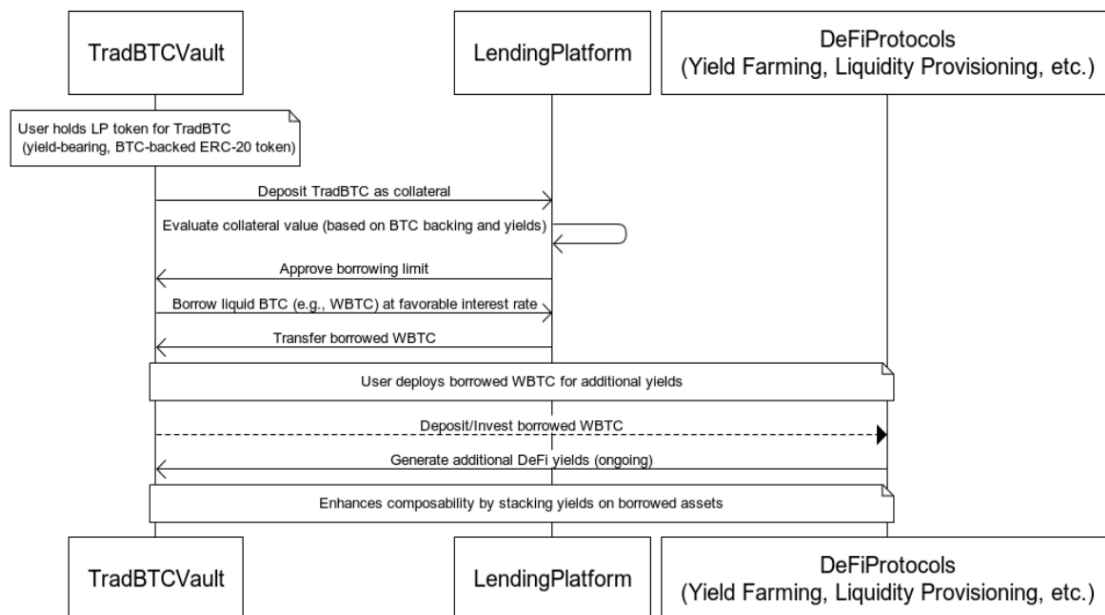**Withdrawal Mechanics and Risk Management**

To maintain vault integrity and accommodate unbonding requirements, all tradBTC withdrawals must be initiated at least 7 days prior to the end of a settlement cycle. Requests submitted after this window are deferred to the subsequent month's settlement date, ensuring orderly liquidity provision and minimizing disruption to ongoing strategies.

This framework mitigates illiquidity risks inherent in staked assets by introducing derivative overlays, while institutional partnerships and custodial integrations provide layers of security and operational resilience.

Additional DeFi Composability on BTC backed LP token

As TradBTC (LP token as it is locked with the trading institution) is an yield bearing asset backed by staked BTC on Babylon,it can be used to borrow more liquid forms of BTC for favourable interest rates (such as WBTC) on platforms such as Morpho and Euler. This opens more doors to generate additional DeFi yields on the borrowed assets on multiple Defi protocols and products.

Economic Value and Scalability

In traditional finance, it is extremely common in Derivative markets that Spot Liquidity and Derivative Liquidity to be in different venues managed by institutional intermediaries.

As Bitcoin provides a trustless mechanism to check reserves, it provides an untapped trillion dollar market opportunity up for grabs for all the staked assets to be used as market collateral in a non custodial manner, without the need of any intermediaries.

Babylon is perfectly positioned to capture this opportunity. Currently BTC derivatives account for ~68% of crypto options/futures volume. Annual projection of BTC settled derivative volumes is over $23–$28 trillion.

Through our solution, no new markets need to be made and we can work with the existing liquidity in different venues (integrating with different DEXs, CEXs and Market Makers) without the need to unstake/move the BTC from the Babylon ecosystem.

At the same time, we are creating a virtuous loop for new Stakers to enter the Babylon ecosystem as the yields are extremely competitive and above the market average.