cBTC Whitepaper:
A Bitcoin-Backed Monetary Protocol

James Tector

jamestector@gmail.com

Abstract

cBTC introduces a Bitcoin-native monetary layer that transforms Bitcoin from a passive store of value into a productive and liquid transactional asset. The protocol enables Collateral Providers (CPs) to lock BTC as collateral to mint cBTC, a freely floating Bitcoin-denominated token backed by BTC reserves. Unlike conventional stablecoins, cBTC has no fiat peg and no reliance on USD or external banking systems.

cBTC is redeemable exclusively for BTC at a market-based BTC/cBTC exchange rate, ensuring decentralization, transparency, and resistance to arbitrage attacks.

The system uses prefunded BTC yield, non-linear vesting, Taproot-secured custody, and Lightning Network liquidity deployment to create a fully Bitcoin-aligned monetary engine.

cBTC is not a stablecoin — it is Bitcoin made liquid.

---

1. Introduction

Bitcoin is the world's most secure and decentralized monetary base layer but remains underutilized as a daily medium of exchange. Most Bitcoin holders treat BTC as long-term savings, while stablecoins—anchored to fiat currencies—dominate transactional activity.

However, fiat-pegged assets:

- reintroduce counterparty risk,
- depend on banks and regulators,
- rely on custodians or centralized issuers,

- and weaken Bitcoin's monetary sovereignty.

What Bitcoin lacks is a **purely Bitcoin-denominated**, elastic, liquid, and yield-efficient transactional asset that can operate without relying on fiat infrastructure.

cBTC solves this problem by establishing a **Bitcoin-first monetary system** where:

- Collateral is BTC
- Yield is prefunded in BTC
- Redemption pays BTC
- Governance is BTC-based
- Pricing is BTC/cBTC
- Liquidity flows through Bitcoin rails
- No USD, no stablecoin mechanics, no external peg

The protocol introduces:

- A floating Bitcoin-native token (currency) (cBTC)
- A prefunded yield mechanism
- Taproot-based time-locked custody
- An internal AMM for BTC/cBTC price discovery
- A redemption pool with BTC reserves
- Dynamic, incentive-aligned CP participation
- Lightning Network liquidity deployment

cBTC creates a Bitcoin equivalent of a "Layer-2 monetary supply/M2," enabling:

- commerce
- payroll
- settlement
- treasury operations
- liquidity routing
- decentralized finance

— all denominated in Bitcoin.

---

2. System Overview & Initial Bootstrapping

cBTC is a Bitcoin-native monetary protocol composed of several coordinated components that operate together to provide liquidity, yield, and redemption guarantees without relying on fiat systems. All key actors—Collateral Providers, cBTC users, and governance participants—interact entirely within Bitcoin rails.

cBTC's design includes:

- **CP Vault**: Holds BTC collateral under Taproot-enforced time locks.
- **Minting Engine**: Creates new cBTC at a fixed Loan-to-Value ratio.

- **Marketplace Pool**: Issues cBTC to users in exchange for BTC.
- **Redemption Pool**: Holds BTC reserves to redeem cBTC from users.
- **Yield Pool**: Holds prefunded CP yield and deploys unvested yield as LN liquidity.
- **Pricing Module (Internal AMM)**: Determines cBTC/BTC redemption and minting rates.
- **Governance Registry**: Records CP votes and parameter changes.

The system is fully decentralized, open source and Bitcoin-denominated. No stablecoins, no fiat references, no external custodial bridges are required.

2.1 Actors

Collateral Providers (CPs)

CPs supply BTC collateral to the protocol. In return, they receive:

- A prefunded 15% APY BTC initial yield
- Control via CP-only governance
- Ability to withdraw principal + vested yield after 1 month

CPs keep full ownership of all deposited BTC and yield, enforced by Taproot timelocks.

cBTC Users

Users interact with the protocol by:

- Exchanging BTC for cBTC via the Marketplace Pool
- Redeeming cBTC for BTC via the Redemption Pool
- Using cBTC as a fast, liquid unit for payments or DeFi
- May hold cBTC on Lightning (as a Taproot Asset / L2 representation) or on-chain

They do not need to be CPs and bear no direct responsibility for system governance.

Protocol Reserves

The system maintains two Bitcoin-denominated reserves:

1. **Redemption Reserves**

- BTC specifically allocated to back cBTC redemptions
- Funded by user BTC spent in the Marketplace and by fees/unvested yield
- Always verifiable on-chain

2. Yield Reserves (CP Yield Tranches)

- BTC prefunded to pay CP yield (0.15 BTC per 1 BTC deposited)
- Split into **time-locked tranches** governed by Taproot scripts
- While unvested, can be deployed as **Lightning Network liquidity**, but always under CP ownership and with strict timelocks

Both are fully visible on-chain.

Governance (CP Collective)

Governance is controlled entirely by CPs.

Key features:

- **One CP vault (or CP contract) = one vote**
- CPs can vote on:
  - LTV ratio for new minting
  - Base yield rate
  - Redemption fee
  - Use of fees and surplus reserves
  - LN liquidity policies for unvested yield
- All changes are subject to:
  - Quorum requirements
  - Supermajority approval
  - A 48-hour timelock before enforcement

There is **no governance token**. Governance power is tied directly to economic contribution (BTC liquidity).

2.2 Core Contracts / Modules

CP Vault

- Receives BTC deposits from CPs (0.05–1 BTC per vault instance)
- Enforces a **minimum 1-month lock (4320 Bitcoin blocks)** on principal
- Coordinates the creation of **yield tranches** (Taproot outputs) representing prefunded yield
- Tracks vesting schedules and supports partial or full withdrawal after timelocks expire
- On early exit, ensures that only **vested yield** is withdrawable and that unvested yield is redirected according to protocol rules (e.g., toward Redemption Reserves)

The Vault is a logical controller; actual custody is enforced on Bitcoin via Taproot scripts.

Minting Module

- Mints new cBTC at a fixed LTV ratio (default: 30%)

- Sends minted cBTC directly to Marketplace Pool
- Cannot mint to CPs directly (avoids distortions)

Marketplace Pool

The Marketplace Pool:

- Receives newly minted cBTC from the Minting Module
- Exchanges BTC ↔ cBTC with users at prices set by the internal AMM
- Sends received BTC into
    - **Redemption Reserves** (50%)
    - **Yield Infrastructure** (50%) for CP yield prefunding

This is the main entry point for users acquiring cBTC with BTC.

Redemption Pool

The Redemption Pool:

- Holds BTC reserves backing cBTC
- Burns cBTC when users redeem
- Uses the internal AMM price (BTC/cBTC) to determine how much BTC to pay out
- Collects redemption fees (e.g. 0.2%) that increase reserves and coverage
- May receive unvested yield from early CP exits, further strengthening solvency

This pool is the core of the system's solvency and redemption guarantees.

Yield Infrastructure (Yield Pool)

The Yield "Pool" is a logical module responsible for:

- Receiving BTC allocated to CP yield from Marketplace inflows
- Structuring this BTC into **Taproot-based yield tranches** per CP position
- Applying non-linear vesting schedules
- Coordinating the use of **unvested yield tranches as Lightning Network liquidity**, under:
    - joint CP + protocol spending conditions before vesting, and
    - CP-only control after vesting

Importantly, the Yield Pool does not own the yield; it **coordinates** how prefunded CP-owned yield is locked, vested, and optionally deployed as LN liquidity.

Internal AMM (Automated Market Maker)

Rather than relying on external oracles for pricing, cBTC uses an **internal Automated Market Maker (AMM)** that:

- Sets BTC/cBTC exchange rates based on the ratio of BTC and cBTC in protocol pools
- Quotes prices for both:
    - BTC → cBTC (mint-like buys via Marketplace)
    - cBTC → BTC (redemptions via Redemption Pool)

External markets (DEXs, centralized exchanges, LN swap markets) arbitrage against this AMM, keeping cBTC pricing aligned with global markets without requiring USD oracles.

Oracles may optionally be used **only as guardrails** to pause operations if internal prices diverge too far from external BTC/cBTC markets.

Governance Registry

The Governance Registry:

- Stores all configurable parameters (LTV, yield rate, fees, vesting curve parameters, LN usage rules)
- Records CP votes and proposals
- Applies an **execution timelock** to all accepted changes
- Controls which scripts and keysets are authorized to operate Redemption and Yield tranches

2.3 Initial Bootstrapping

The bootstrap process establishes the first cBTC supply, initial reserves, and CP yield tranches in a Bitcoin-native way.

1. **CP deposits BTC into CP Vault**
    - Example: 1 BTC
    - CP principal is locked under Taproot with a 1-month minimum lock.
2. **Protocol mints cBTC at 30% LTV**
    - 1 BTC deposit → 30,000 cBTC minted
    - Newly minted cBTC is sent **entirely to the Marketplace Pool**
3. **Users acquire cBTC with BTC**
    - Users send BTC to the Marketplace Pool
    - The internal AMM quotes a BTC/cBTC rate (e.g., 0.00001 BTC per cBTC initially)
    - Example: user sends 0.10 BTC and receives ~10,000 cBTC
4. **BTC from users is split between reserves**
    - 50% → **Redemption Reserves**
    - 50% → **Yield Infrastructure**, which:
        - allocates per-CP yield tranches
        - structures them as Taproot outputs with non-linear vesting schedules
        - optionally deploys unvested tranches as LN liquidity
5. **cBTC is delivered to users**
    - Either directly to an on-chain cBTC address

- Or to a Lightning-compatible representation (Taproot Asset / L2 token)

At the end of bootstrapping:

- CPs have locked BTC and are entitled to time-locked yield
- Users hold cBTC acquired with BTC
- The Redemption Pool has initial BTC reserves
- The Yield tranches are structured and (optionally) partially active as LN liquidity

No fiat enters the system at any point. All value flows are BTC ↔ cBTC.

---

3. Tokenomics & Monetary Policy

cBTC is a Bitcoin-denominated liquidity token backed by BTC reserves and governed by predictable, transparent monetary rules. Its design ensures that cBTC remains elastic, market-priced, and fully anchored to BTC without relying on fiat systems.

The monetary model rests on four pillars:

1. **BTC collateralization through CP vaults**
2. **Elastic cBTC supply through minting/redemption**
3. **Prefunded, non-leveraged BTC yield for CPs**
4. **Market-based BTC/cBTC pricing through internal AMMs**

These create a Bitcoin-native monetary loop that is stable, solvent, and responsive to supply and demand.

3.1 Collateral Model

Collateral Providers (CPs) deposit BTC that underpins the entire system.

Key characteristics:

- Deposits range from **0.05 to 1 BTC** per vault.
- CP always retains **full ownership** of principal + yield via Taproot timelocks.
- Minimum lock time is **1 month (4320 Bitcoin blocks)**.
- Yield vests over **12 months** using a **non-linear vesting curve**.

Each CP deposit enables the protocol to mint cBTC at a fixed Loan-to-Value (LTV) ratio.

Default LTV Ratio: 30%

1 BTC deposit → 30,000 cBTC minted

This design maintains conservative leverage, ensuring that:

- CP yield is prefunded entirely in BTC
- Redemption reserves are always BTC-backed
- The system trends toward increasing over-collateralization as usage grows

3.2 Elastic Supply (Minting and Redeeming)

cBTC is not a stablecoin.

Its supply **expands or contracts** based on market demand.

Minting (Expansion)

Minting occurs when:

- CPs deposit BTC, OR
- Users send BTC to the Marketplace Pool to buy cBTC at market price.

In both cases:

- New cBTC enters circulation
- BTC enters system reserves
- AMM reprices cBTC based on pool ratios

Redemption (Contraction)

Redemption occurs when users send cBTC to the Redemption Pool in exchange for BTC.

During redemption:

- cBTC is burned
- BTC exits the reserve
- Remaining cBTC becomes **better collateralized**
- Redemption fee (0.2%) strengthens reserves

This creates a powerful stabilizing mechanism.

3.3 BTC/cBTC Market-Based Redemption Price

cBTC does **not** use USD or fixed-rate redemption.

It uses a **purely Bitcoin-native AMM price**:

$$BTC\_out = cBTC\_in \times AMM\_price \times (1 - 0.002)$$

Where **AMM_price** is derived from:

- BTC/cBTC ratios in protocol pools
- Arbitrage against external markets

This mechanism:

- Eliminates infinite arbitrage loops
- Preserves reserve solvency
- Avoids reliance on USD oracles
- Keeps the system decentralized

The protocol never assumes a “peg” or fixed cBTC value.

3.4 Prefunded BTC Yield

Each 1 BTC CP deposit triggers a prefunding of 0.15 BTC into the Yield Pool.

This yield:

- Is vested over 12 months
- Is fully owned by the CP
- Cannot fully be withdrawn early
- Is deployed as Lightning Network liquidity while unvested
- Earns additional routing yield
- Redirects unvested yield to reserves if CP exits early

Non-Linear Vesting Curve

A non-linear model discourages rapid cycling:

- Small vesting early
- Accelerated vesting after several months
- Full yield only for CPs who commit longer

This strengthens liquidity stability and reserve growth.

3.5 Reserve Structure

The system maintains two separate reserves:

(A) Redemption Pool

- Funds user redemptions
- Receives 50% of all BTC spent by users buying cBTC
- Receives redemption fees
- Receives unvested CP yield from early exits

- Pays out BTC during redemptions

(B) Yield Pool

- Holds prefunded CP yield
- Deploys unvested yield to LN channels
- Releases vested yield to CPs after timelocks expire
- Transfers expired unvested yield to Redemption Pool

3.6 Coverage Ratio

Coverage Ratio (C) measures the system's solvency:

$$C = Redemption\_Pool\_BTC / Total\_cBTC\_Outstanding$$

Because redemption occurs at market price via AMM, this ratio:

- Increases automatically during redemptions
- Benefits from LN routing fees
- Strengthens when CPs exit early
- Gradually rises as activity increases

The system naturally trends toward over-collateralization during periods of healthy usage.

3.7 Summary of Monetary Properties

- **Floating BTC-native asset**
- **Supply adjusts to demand**
- **Redemptions burn supply**
- **Fees strengthen reserves**
- **Yield prefunded and risk-free**
- **Market-based price discovery**
- **No USD or external fiat anchors**
- **No reliance on lending or leverage**

cBTC's monetary model is inspired by historical free banking systems but built on Bitcoin's cryptographic guarantees.

---

4. Risk & Stability Analysis

The cBTC protocol is designed to operate as a Bitcoin-native monetary system capable of expanding and contracting supply dynamically while maintaining long-term solvency and predictable redemption guarantees. This section provides a critical evaluation of the system's structural risks, economic protections, and stability mechanisms.

cBTC's stability is rooted in:

- **BTC collateralization through CP deposits**
- **Elastic supply via mint and redemption flows**
- **Internal AMM-based pricing**
- **Prefunded yield mechanisms**
- **Reserve accumulation via fees and unvested yield**
- **Non-linear CP vesting**
- **Lightning Network routing yield**
- **CP-governed parameters**

These mechanisms together ensure that cBTC behaves as a responsibly expanding monetary layer rather than a fixed-peg asset susceptible to runs or arbitrage collapses.

4.1 Structural Design

The system distinguishes between two economic classes:

(1) Collateral Providers (CPs) – Senior Creditors

CPs deposit BTC and are entitled to:

- Full principal
- Prefunded yield
- A guaranteed ability to withdraw vested amounts after timelocks

CPs always retain ultimate ownership of their funds through Taproot-enforced spending paths. cBTC holders cannot claim CP collateral under any condition.

(2) cBTC Holders – Junior Creditors

cBTC users hold redeemable claims backed by:

- The Redemption Pool
- AMM pricing
- Fee-reinforced reserves
- Burning of redeemed cBTC

Because they occupy a junior position, the system protects CP solvency first, then cBTC stability.

This economic hierarchy is intentional and foundational to solvency.

4.2 Market Risk

Bitcoin Price Volatility

Because all reserves and obligations are denominated in BTC, the system is inherently insulated from fiat volatility. A drop in BTC/USD does not create insolvency pressure because:

- CP obligations are denominated in BTC.
- cBTC redemptions pay BTC.
- System reserves are BTC.
- cBTC price floats relative to BTC.

Thus, cBTC operates as a **closed Bitcoin-based economy** with no USD debt.

Mitigations

- Conservative 30% LTV
- Dynamic LTV (CP governance-controlled)
- Fees that strengthen reserves
- Burning of redeemed cBTC increases backing per remaining token

4.3 Liquidity Risk

Risk: Rapid Increase in Redemptions ("Bank Run")

If many users redeem cBTC simultaneously:

- Redemption Pool reserves may come under pressure
- The AMM price will adjust automatically (cBTC becomes cheaper in BTC terms)
- Redemptions become less profitable as pool ratios shift
- Arbitrageurs buy discounted cBTC to resell later

The system uses **market pricing, not fixed pricing**, to avoid catastrophic arbitrage drains.

Mitigations

- Redemption fee (0.2%)
- AMM-based pricing (prevents fixed-price drains)
- Non-linear slippage protects the pool
- Burning reduces supply and increases backing for remaining tokens
- Adjustable fee parameters via governance
- Optional redemption throttling for extreme cases

Unlike stablecoins, cBTC does not promise a fixed-value redemption, and therefore cannot collapse under a peg break scenario.

4.4 Economic Protection Mechanisms

(1) Prefunded CP Yield

Because yield is funded upfront, the system does not require:

- borrowing
- leverage
- lending activity
- or continuous demand for loans

This removes the circular-risk feedback loop that caused failures like Celsius, BlockFi, and FTX.

(2) Non-Linear Vesting Curve

This discourages CPs from depositing and withdrawing rapidly to extract repeated yields.

The longer an CP stays locked:

- the more yield becomes vested
- the less remains exposed to liquidation or reallocation

(3) LN Routing Yield

Unvested yield tranches deployed as Lightning liquidity:

- earn routing fees
- increase reserve surplus
- tighten spread between minting and redemption prices

This provides a real economic source of revenue that strengthens the system over time.

(4) Unvested Yield Migration

If an CP withdraws early:

- only vested yield is withdrawable
- unvested yield tranches migrate toward the Redemption Pool
- reserves strengthen automatically

This increases solvency during stress events.

4.5 Pricing Risk

cBTC uses an **internal AMM as the pricing oracle** for BTC/cBTC. This eliminates the dependency on external BTC/USD or cBTC/USD price feeds.

Mitigations

- AMM pricing is endogenous and verifiable
- External market arbitrage ensures alignment
- USD oracles are optional guardrails only
- No redemption at fixed intrinsic rates (avoids infinite arbitrage)

This is a major stability innovation.

4.6 Operational & Technical Risk

(1) Bitcoin Layer-2 Interoperability

Using Lightning Network to deploy unvested yield introduces:

- channel management complexity
- rebalancing risks
- key management requirements
- potential downtime risks

Mitigation:

- Taproot-based scripts ensure CP ownership
- MuSig2 multisig for LN spending paths
- Channel opening/closing restrictions based on CSV
- Watchtower protection for channel states
- Governance-defined operational parameters

(2) Smart Contract Logic

Errors in multisig or Taproot script construction could affect custody.

Mitigation:

- Open-source code
- Multiple independent audits
- Formal verification of vesting and spending paths
- Operational simulation on Testnet and Signet
- Mandatory governance timelock
- Strict separation of CP funds vs protocol funds

4.7 Black Swan Scenario

Consider:

- A sudden BTC price crash
- A rapid spike in cBTC redemptions

- CP mass withdrawals
- External market attack on AMM pricing

System response:

1. **Redemption price adjusts downward** via AMM, slowing reserve drain
2. **cBTC supply contracts** as tokens are burned
3. **Backing ratio increases** for remaining tokens
4. **Redemption fees accumulate**, strengthening reserves
5. **Unvested CP yield flows to Redemption Pool** reinforcing solvency
6. **CP redemption rights remain protected** (senior claims)
7. **Governance may temporarily increase redemption fees** or pause minting

Even under extreme stress, CP funds remain safe, and cBTC stabilizes around its market-clearing BTC value.

4.8 Summary of Stability Features

cBTC stability is achieved through:

- **AMM-based BTC/cBTC redemption pricing**
- **Prefunded and time-locked CP yield**
- **Unvested-yield reserve migration**
- **Redemption fees**
- **CP seniority**
- **Market-driven supply and demand**
- **LN routing yield**
- **Full transparency of reserves**
- **No fiat exposure**
- **No fixed redemption promises**

Together these produce a resilient, Bitcoin-native monetary system capable of weathering volatility and liquidity shocks.

---

5. Economic Model & Projections

The cBTC protocol forms a Bitcoin-native monetary system with predictable monetary dynamics. This section models the economic flows, reserve behavior, long-term solvency trends, and expected system growth under reasonable assumptions.

The cBTC economy is powered by:

1. **CP deposits (BTC collateral)**
2. **Minting cBTC (elastic supply expansion)**
3. **User purchases of cBTC (BTC inflow)**
4. **Redemptions (elastic supply contraction)**
5. **Prefunded CP yield (0.15 BTC per 1 BTC deposit)**
6. **Unvested yield migration to reserves**
7. **LN routing revenue**
8. **Redemption fees (0.2%)**
9. **AMM-based pricing that adjusts automatically to pool balances**

Together, these create a self-reinforcing monetary loop that improves solvency over time.

5.1 Base Assumptions for Modeling

To provide a concrete model, we assume:

- CP deposit = **1 BTC**
- LTV = **30%**
- Minted cBTC = **30,000**
- User purchases of minted cBTC = **0.30 BTC total**
- Split = **0.15 BTC to Yield Tranches**, **0.15 BTC to Redemption Pool**
- CP yield = **15% annually** (0.15 BTC prefunded)
- Early CP exit rate = **30%**
- Monthly transaction turnover = **25–35% of supply**
- Redemption fee = **0.2%**
- Unvested yield used as LN liquidity earns **0.2–3.0% annually** (variable)
- Unvested yield from early exits flows to Redemption Pool

This is not a projection of token price; it is a model of reserve dynamics and solvency.

5.2 Reserve Dynamics

cBTC maintains two reserves:

(1) Redemption Pool (RP)

Provides BTC for redemptions.

Growth factors:

- 50% of user BTC purchases
- Redemption fees (0.2%)
- Unvested yield from early CP exits
- Optional LN routing yield allocation

Drain factors:

- User redemptions
- Governance-approved redistribution

(2) Yield Tranches

Prefunded CP yield, structured as Taproot outputs.

Growth factors:

- BTC inflow from Marketplace purchases
- Routing fees (when unvested and deployed as LN liquidity)

Drain factors:

- Vesting (CP withdrawal)
- Yield tranches from early exits shifted to Redemption Pool

5.3 Coverage Ratio Dynamics

Coverage Ratio (C) is a key solvency indicator:

C = Redemption_Pool_BTC / Total_cBTC_Outstanding

Because redemption uses **market-based AMM pricing**, the system cannot be drained through arbitrage at fixed rates.

What increases Coverage Ratio?

- Redemptions (burning reduces denominator)
- Redemption fees
- Unvested yield migration
- LN routing revenue
- User purchases (BTC inflow)
- Price declines in cBTC relative to BTC (more burns)

What decreases Coverage Ratio?

- Redemptions draining BTC
- Governance-approved surplus redistributions

Overall, the system **naturally trends toward greater solvency** as long as economic activity is non-zero.

5.4 Projected Reserve Growth Over Time

Based on conservative activity assumptions:

Time	Redemption Pool	Coverage Ratio	Notes
Initial	0.15 BTC	50%	After cBTC minted & sold
Year 1	~0.22 BTC	73%	Includes redemption fees + unvested yield
Year 3	~0.30 BTC	100%	System reaches equilibrium
Year 5	~0.38 BTC	126%	Overcollateralization phase

Interpretation:

- Even with modest transaction activity, reserves rise.
- The system tends toward partial overcollateralization, increasing user confidence.
- Governance may decide to redistribute surplus BTC only after hitting safety thresholds.

5.5 Elastic Supply & Market Pricing

cBTC is not pegged.

Its value floats based on BTC/cBTC AMM pricing.

This means:

- If cBTC trades at a premium → users mint (expand supply)
- If cBTC trades at a discount → users redeem (contract supply)
- Arbitrage stabilizes price
- cBTC always finds a market-clearing BTC value

This avoids the fatal fixed-peg dynamics that caused collapses (UST, IRON, etc.).

5.6 Incentive Alignments

The system's economics align incentives to enforce stability:

CP incentives:

- Earn BTC yield (prefunded)
- Benefit from LN routing revenue
- Govern the system
- Prefer long-term locking (boost vesting)
- Have no incentive to run on the system

cBTC holder incentives:

- Redeem when cBTC trades at a discount
- Sell or provide liquidity when cBTC trades at a premium
- Use cBTC for payments (fast, cheap, BTC-denominated)

Arbitrageur incentives:

- Maintain price parity across markets
- Keep AMM pool aligned with external BTC/cBTC price

Protocol incentives:

- Grow activity → grow reserves
- Maintain solvency > maintain trust > increase adoption
- Drive LN usage → increase routing yield → strengthen reserves

5.7 Systemic Resilience

The system benefits from:

- BTC-denominated liabilities
- BTC-denominated reserves
- No fiat exposure
- No lending
- No rehypothecation
- Elastic supply
- Continuous arbitrage-based stabilization
- Burn-and-strengthen redemption mechanics

This combination is unique among crypto monetary systems.

5.8 Long-Term Outlook

The model suggests:

1. **Stability increases with usage**
2. **Reserve coverage naturally approaches 100%**
3. **LN routing revenue enhances sustainability**
4. **cBTC becomes a Bitcoin-native M2 monetary layer**
5. **CP participation grows as trust and returns are proven**
6. **Corporate adoption grows as BTC treasuries seek liquidity solutions**
7. **cBTC eventually becomes the preferred medium of exchange and unit of account.**

cBTC has the potential to evolve into the dominant Bitcoin-denominated liquidity token and the backbone of a broader Bitcoin-native financial ecosystem.

---

6. Governance & Legal Framework

The cBTC protocol operates under a governance framework designed to be simple, transparent, Bitcoin-native, and resistant to capture. Governance responsibilities are strictly limited to parameter adjustments and economic stewardship; the protocol avoids governance tokens, complex DAOs, or centralized administrators.

All decisions are made by **Collateral Providers (CPs)**, whose economic contributions and long-term alignment make them the natural stewards of the system.

6.1 Governance Philosophy

The design principles guiding cBTC governance are:

Bitcoin-First

No fiat exposure, no stablecoin dependencies, no centralized custody.

Minimalist

Governance controls only what is necessary:

- LTV ratio
- Yield rate
- Redemption fee
- Vesting parameters
- LN liquidity allocation policy
- Reserve distribution thresholds

Governance cannot:

- Seize funds
- Alter CP-owned timelocks
- Force or block user redemptions
- Freeze cBTC

One CP = One Vote

Each CP vault is a governance seat.

The size of the deposit does not increase voting weight.

Timelocked Decisions

All approved changes are delayed by **48 hours** before going into effect.

Transparency

All proposals, votes, and enacted changes are recorded publicly.

6.2 Governance Model

Governance is controlled entirely by CPs through on-chain vote signaling.

Voting Rules

- **One CP contract = one vote**
- CPs can submit **one proposal every 30 days**
- Voting window = **7 days**
- Quorum = **60% of active CPs**
- Approval threshold = **⅔ majority**
- Execution timelock = **48 hours**

This ensures:

- No governance token speculation
- No plutocracy
- No governance capture by whales
- Slow, deliberate changes

6.3 Adjustable Parameters

Governance may adjust:

(1) Loan-to-Value (LTV) Ratio for Minting

Default: 30%

Governance may adjust between 20–40%.

(2) CP Annual Yield Rate

Default: 15% BTC-denominated, prefunded.

Changes affect future deposits only.

(3) Redemption Fee

Default: 0.2%

Used to strengthen reserves.

(4) Vesting Curve Parameters

- Steepness
- Duration
- Non-linear weighting

Used to discourage short-term CP cycling.

(5) LN Liquidity Allocation

Percentage of unvested yield that may be deployed as LN liquidity (e.g., 0–80%).

(6) Surplus Reserve Distribution

If Redemption Pool coverage surpasses 100%, CPs may vote to:

- Redistribute surplus BTC pro-rata
- Allocate to development grants
- Increase global redemption backing
- Fund marketing or adoption incentives

The system allows flexibility while maintaining strict Bitcoin-based discipline.

6.4 Legal Structure & Regulatory Positioning

cBTC is designed to align with Bitcoin's regulatory strengths.

Not a Stablecoin

- No USD peg
- No fiat-denominated liabilities
- No promise to maintain parity with fiat

- Redemptions are BTC-based

This avoids stablecoin-specific regulatory categories.

Not a Security

There is:

- No governance token
- No expectation of profit from others' work (yield is prefunded)
- No equity rights
- No dividend flows
- No managerial entity distributing profits

CP rewards are **service rewards**, not financial returns.

Not an Interest-Bearing Product

- Yield is prefunded, not lent or borrowed
- No risk of loss from lending activity
- No centralized entity owes obligations

This differentiates cBTC from lending platforms (Celsius, BlockFi) and prevents classification as a loan product.

Non-Custodial Bitcoin Layer

- CPs retain ownership of all BTC (principal + yield)
- Protocol cannot seize funds
- Users redeem BTC trustlessly
- Taproot timelocks enforce custody rules

This removes custodial licensing risks.

6.5 Custody Model

The custody model is **one of cBTC's most important innovations**.

CPs Own 100% of Their BTC

- Principal
- Vested yield
- Unvested yield (under spending constraints)
- All Taproot outputs securing their yield tranches

Protocol Only Has Enforcement Rights

Not spending rights.

Via Taproot:

- For unvested yield, LN channel operations require **MuSig2 (CP + Protocol)** before vesting
- After vesting, CP has an **exclusive spending path**
- Protocol cannot move CP funds without CP consent
- CP cannot prematurely withdraw yield due to CSV timelocks

This is a fully non-custodial model.

6.6 Redemption Rights

cBTC holders:

- Can always redeem cBTC for BTC at the **AMM-determined BTC/cBTC rate**
- Are not dependent on USD prices
- Cannot force liquidations of CP positions
- Cannot claim CP principal
- Bear price risk only, not custodial risk

This is aligned with Bitcoin-native ethics:

users always receive BTC, not IOUs.

6.7 Summary of Governance & Legal Design

cBTC governance is:

- Simple
- Bitcoin-native
- Non-custodial
- CP-directed
- Transparent
- Minimally adjustable
- Resistant to regulatory exposure
- Free from fiat influences

The legal structure reinforces the protocol's decentralization and ensures the system operates as a Bitcoin-based monetary layer, not a financial intermediary.

---

7. Implementation Architecture

The cBTC protocol is engineered to operate natively on Bitcoin infrastructure, using Taproot, MuSig2 multisignatures, timelocks, and optionally Lightning Network channels. The system is designed for decentralization, transparency, and verifiable solvency without relying on smart-contract chains that attempt to replicate Ethereum-like behavior.

This section outlines the architectural components and how they interact at the Bitcoin protocol level.

7.1 Design Principles

The implementation follows these core principles:

Bitcoin-First Engineering

- All value is denominated in BTC
- CP custody enforced at UTXO level
- Timelocks and spending paths defined via Taproot trees
- Lightning integration optional but native
- No external stablecoins or custodians

Modular Architecture

Each module is independent:

- Vault module
- Minting module
- Marketplace pools
- Redemption module
- Governance registry
- LN liquidity manager

Non-Custodial Logic

Protocol scripts enforce:

- Lock durations
- Vesting schedules
- Vesting cliffs
- Authorized spending paths

...without ever taking full custody of CP funds.

Verifiable Solvency

Redemption Pool reserves are:

- Public
- On-chain
- Auditable by anyone
- Backed by deterministic UTXO sets

This is a radical departure from centralized stablecoins or custodial bridges.

7.2 Core Modules

Below is the structure of each component.

7.2.1 CP Vault (Taproot Vault)

The CP Vault is the heart of the system's custody model.

Deposit Process

- CP deposits BTC into a Taproot UTXO
- UTXO contains multiple spending paths:
    - **Path A (CP-only):** Spendable after timelock expires (principal + vested yield)
    - **Path B (Protocol+CP):** For LN deployment of *unvested* yield
    - **Path C (Fallback/Emergency):** Multi-sig recovery path requiring governance approval

Timelocks

- Principal is subject to a **1-month minimum lock**
- Yield tranches use **non-linear vesting** with staged CSV (relative timelock) or CLTV (absolute timelock)

Security Guarantees

CP always maintains:

- One key to sign vesting withdrawals
- One key for LN channel operations
- Exclusive withdrawal rights after vesting

The protocol can never unilaterally withdraw CP funds.

7.2.2 Minting Module

This module performs:

- Validation of CP deposits
- Calculation of mintable cBTC using LTV ratio
- Issuance of newly minted cBTC to the Marketplace Pool

- Updates to governance registry regarding new CP seat

Minting does **not** mint directly to CPs, preventing CPs from immediately dumping cBTC and causing instability.

7.2.3 Marketplace Pool (BTC → cBTC)

Where users acquire cBTC:

- Users send BTC to a pool address controlled by a Taproot script
- The internal AMM determines the BTC/cBTC rate
- Users receive cBTC to a Bitcoin address or L2 channel
- Incoming BTC is automatically split:
  - **50% to Redemption Reserve** (on-chain UTXOs)
  - **50% to Yield Tranches** (Taproot outputs created for CPs)

The Marketplace Pool is trust-minimized and transparent.

7.2.4 Redemption Pool (cBTC → BTC)

When a user redeems cBTC:

1. cBTC is burned
2. AMM calculates BTC equivalent at the current price
3. BTC is sent from Redemption Reserve
4. A 0.2% fee stays in the Redemption Reserve

Redemption is entirely market-based, preventing attack vectors such as:

- Peg-based draining
- Infinite arbitrage loops
- Oracle manipulation

Because cBTC floats freely, the system cannot collapse from peg breaks.

7.2.5 Internal AMM (Pricing Engine)

Unlike Ethereum-style AMMs, cBTC uses:

- Ratio of BTC to cBTC in protocol pools
- Market pressures from external BTC/cBTC venues
- Optional oracle guardrails for sanity checks

This determines:

(A) Price for BTC→cBTC (mint-like buys)

More BTC in pool → cBTC price increases.

(B) Price for cBTC→BTC (redemptions)

More cBTC in pool → cBTC price decreases.

This dynamic ensures continuous price discovery without fixed ratios.

7.2.6 Governance Registry

Tracks:

- CP vaults
- Votes and proposals
- Parameter states (LTV, yield rate, LN allocation)
- Execution timelocks
- Emergency pause states (if governed parameters exceed thresholds)

Governance interacts only with parameters, never with funds.

7.2.7 Lightning Network Liquidity Engine

This module deploys **unvested CP yield tranches** as LN liquidity.

Key Features

- Only *unvested* yield is used
- Deployed under **MuSig2 spending rules**
- Channels cannot spend CP yield outside custodial paths
- Routing fees flow back to:
  - Redemption Pool
  - Yield Tranches
  - Development Fund (governance controlled)

Advantages

- Adds yield to the system without leverage
- Increases usefulness of CP capital
- Boosts overall Bitcoin liquidity

This is an industry-first mechanism: unvested yield as productive LN liquidity.

7.3 UTXO-Level Architecture (Summary)

Each CP position consists of:

- One principal UTXO
- Multiple yield-tranche UTXOs
- Each with multi-path Taproot spending rules
- All visible and auditable on-chain

The Redemption Pool consists of:

- A set of BTC UTXOs
- Controlled by governance-defined multi-sig
- Used only for redemptions

7.4 Protocol Deployment and Roadmap

Phase 1 — Testnet

Duration: 3 months

Includes:

- CP vault simulation
- Taproot yield tranches
- Basic AMM pricing
- Redemption logic
- LN integration test channels
- Public dashboard for UTXO transparency

Phase 2 — Mainnet Beta

Duration: 6 months

- Limited CP participation
- Smaller maximum vault sizes
- External audits
- Signet LN stress tests

Phase 3 — Full Launch

Duration: 12 months

- All modules active
- Governance system live
- Public launch of documentation and SDK

Phase 4 — Expansion

Duration: Year 2

- Corporate API gateway
- Native cBTC wallets
- Multi-LN integration
- Inclusion in L2 swap markets

7.5 Operational Considerations

- Governance timelock ensures slow, deliberate execution

- Vault migrations require majority CP approval
- Emergency pause only stops *minting*, never redemptions
- Recovery paths are multi-party, never unilateral
- LN channel balancing is handled by pre-approved operators

7.6 Summary

The implementation architecture is:

- Entirely Bitcoin-native
- Fully transparent
- Non-custodial by design
- Modular and upgradeable under governance
- Resistant to regulatory pressure
- Grounded in UTXO-level security

This architecture makes cBTC possible without compromising Bitcoin's core values: decentralization, self-custody, and cryptographic guarantees.

---

8. Liquidity Incentive & Anti-Looping Mechanism

The cBTC protocol enters a landscape where several projects attempt to bring Bitcoin liquidity, synthetic assets, or stablecoins to market. However, none fully achieve what cBTC is designed to do: create a **Bitcoin-native, non-custodial, market-floating, yield-producing monetary layer** without relying on fiat, centralized custody, or external collateral.

This section compares cBTC to existing categories and highlights why the design fills a critical gap in the Bitcoin ecosystem.

8.1 Category Comparison

1. Wrapped Bitcoin (WBTC, RENBTC, tBTC, etc.)

Model: Custodial or semi-custodial BTC-on-EVM representations

Weaknesses:

- Centralized custodians
- Regulatory risk
- Smart contract dependencies
- Historically failed bridges
- No inherent yield
- Not Bitcoin-native

How cBTC differs:

- No custodian
- No tokenized IOU on EVM
- No reliance on wrapped assets
- Full UTXO-level ownership under CP keys
- Bitcoin-only reserves, Bitcoin-only redemption
- Native yield from prefunding + LN liquidity

---

2. Bitcoin-backed stablecoins (e.g., Stably, USD-pegged schemes)

Model: Peg to USD or other fiat

Weaknesses:

- Fiat custodial exposure
- Banking risk
- Requires USD-based oracles
- Falls under stablecoin regulations
- Peg fragility
- Not Bitcoin-denominated

How cBTC differs:

- No USD peg
- No fiat custody
- No USD oracles
- No banking relationships
- Redemption purely BTC→cBTC
- Fully Bitcoin-priced

cBTC is **not a stablecoin** in any form.

---

3. Synthetic Bitcoin (sBTC, synthetic derivatives on L2s)

Model: Smart contract-based BTC exposure on other chains

Weaknesses:

- Collateral backing issues
- High oracle reliance
- Liquidation cascades
- Exposure to chain risk
- Complexity and fragmentation

How cBTC differs:

- No synthetic exposure
- No oracles for core pricing (AMM-driven)
- No liquidation events
- Single-chain Bitcoin-native implementation

---

4. Algorithmic Stablecoins (UST, FRAX v1, IRON)

Model: Supply elasticity, arbitrage, external peg maintenance

Weaknesses:

- Prone to death spirals
- Peg breaks lead to collapses
- Reliant on external demand for minting and burning
- High reflexivity risk
- Not BTC-backed

How cBTC differs:

- No peg
- No stable value guarantee
- No artificial arbitrage incentives
- Always redeemable via market-based BTC price
- Reserves in actual BTC, not IOUs
- No death spirals possible (no peg to break)

---

5. Bitcoin DeFi on Ethereum/Altchains (Badger, Sovryn, Stacks-based BTCs)

Model: Protocols recreate DeFi using wrapped Bitcoin or L2 synthetic representations

Weaknesses:

- Not Bitcoin-native
- Smart contract chain security assumptions
- Variable liquidity
- Oracle dependencies
- Centralized bridge points

How cBTC differs:

- Operates purely on Bitcoin and optional Lightning
- No cross-chain bridge
- Guaranteed CP custody of BTC

- No reliance on wrapped Bitcoin

---

6. Money-on-Chain and Collateralized Bitcoin Stablecoins

Closest analogue to cBTC in concept, but major differences remain.

Money-on-Chain weaknesses:

- PEG to USD
- Multitoken complexity
- Requires external stability guarantees
- Uses additional collateral types

How cBTC differs:

- No peg
- Single-token system
- Pure Bitcoin collateral
- Uses AMM pricing, not oracle-pegged redemption

8.2 Unique Advantages of cBTC

1. Pure Bitcoin Monetary Loop

No fiat, no external tokens, no synthetic exposure.

2. Non-Custodial CP Model

CPs always retain ownership of all deposited BTC and yield through Taproot timelocks.

3. Elastic Bitcoin-Native Money Supply

The supply expands and contracts based on:

- BTC inflows
- cBTC redemptions
- Market pricing pressures

4. Internal AMM-Based Price Discovery

No reliance on USD or stablecoin oracles.

5. Prefunded Yield + LN Yield

CPs earn:

- Guaranteed prefunded yield
- Optional LN routing yield

…with no lending risk.

6. Reserve Growth Mechanisms

Redemption fees, unvested yield migration, routing fees.

7. Anti-Cycling Vesting Curve

Discourages quick CP exit/re-entry to extract repeated yield.

8. Governance Without Tokens

One CP = one vote.

No governance token risk.

9. Adaptable and Upgradeable

Governance can adjust key parameters to stabilize the system.

8.3 Strategic Positioning

cBTC's value proposition places it in a unique position:

- For **Bitcoiners**:

  A liquidity layer without sacrificing self-custody or decentralization.

- For **corporate BTC treasuries**:

  A way to use BTC as working capital without selling it.

- For **Lightning Network routing**:

  New liquidity sources from unvested yield deployed productively.

- For **global payments**:

  A stable, purely Bitcoin-denominated medium of exchange.

- For **exchanges and swap services**:

A BTC-native alternative to stablecoins and wrapped assets.

8.4 Summary of Competitive Edge

Category	Others	cBTC
Custody	Often custodial	Fully non-custodial Taproot model
Peg	USD/Fiat	Floating BTC-native
Reserves	Sometimes opaque	100% on-chain BTC
Yield	Risk-based	Prefunded BTC + LN routing
Oracles	Critical	Optional guardrails only
Redemptions	Often fixed	Market-based AMM
Risk	Peg breaks, custodial risk	No peg, CP seniority, burn mechanics
Governance	Token-based, plutocratic	CP-based, 1 seat per vault

cBTC stands alone as a **Bitcoin-native, self-balancing monetary system** that delivers liquidity without sacrificing Bitcoin's ethos.

---

9. Conclusion & Future Outlook

cBTC introduces a fundamentally new model for Bitcoin-native liquidity: an elastic, market-priced, non-custodial, yield-enabled monetary asset that increases Bitcoin's usefulness without weakening its monetary principles. This system is not a stablecoin, not synthetic, not custodial, and not dependent on fiat infrastructure. It is a **Bitcoin-only monetary expansion layer** aligned with Bitcoin's core philosophy of self-sovereignty, transparency, and decentralization.

Throughout this whitepaper, we outlined the economic logic, incentive design, implementation architecture, and governance mechanisms that position cBTC as a foundational component in the emerging Bitcoin-native financial landscape.

9.1 Summary of the cBTC Model

cBTC achieves:

1. Bitcoin-denominated liquidity

cBTC serves as a medium of exchange that:

- uses BTC as its sole backing

- is redeemable only for BTC
- floats freely relative to BTC through AMM pricing

2. Non-custodial CP ownership

CPs retain full ownership of:

- principal BTC
- vesting yield
- unvested yield tranches (with controlled spending paths)

Custody is enforced via Taproot scripts, not trust.

3. Elastic monetary supply

Supply expands and contracts based on:

- user demand
- BTC inflows
- redemptions
- arbitrage flows
- AMM pricing

4. Built-in solvency protections

The system strengthens over time through:

- redemption burning
- fee revenue
- migration of unvested yield
- non-linear vesting to reduce CP cycling
- Lightning routing yield generation

5. Bitcoin-native implementation

No bridges, no wrapped tokens, no fiat, no alternative chains. Everything happens on:

- Bitcoin L1 (Taproot-based)
- Lightning Network (optional use of unvested yield)

9.2 Why cBTC Matters

Bitcoin is the world's strongest base layer money, but it lacks native monetary instruments that allow:

- capital-efficient liquidity
- scalable payments

- working capital usage for treasuries
- self-custodial yield
- non-fiat denominated commerce

Stablecoins solved liquidity for the crypto world—but at the cost of fiat reliance and custodial risk.

cBTC solves this in a Bitcoin-native manner:

- No fiat peg
- No USD collateral
- No external banks
- No custodial IOUs
- No off-chain liabilities

cBTC is a monetary expansion layer that enhances Bitcoin **without compromising it.**

9.3 Economic Role of cBTC

If Bitcoin is the base layer (Layer 1) of money:

- cBTC acts as **Layer 2 monetary liquidity (M2)**
- Lightning provides **Layer 2 payment rails**
- Taproot controls enable **Layer 2 custodial guarantees**

Together, they create:

- A complete Bitcoin-native financial stack
- A self-contained Bitcoin economy
- A monetary system that scales without leaving Bitcoin

cBTC becomes a natural choice for:

- Payments
- Settlements
- Payroll
- Treasury liquidity
- Merchant operations
- Cross-border transfers
- Programmatic financial logic

9.4 Path to Becoming a Global Bitcoin Unit of Account

As Bitcoin adoption grows globally, cBTC could become:

- The day-to-day transacting unit
- The medium of exchange
- The liquidity reference asset across Bitcoin-native markets
- A natural pricing unit for wages, goods, and services in BTC economies

This does **not** replace Bitcoin.

Instead, it **complements** it:

- BTC remains the store of value (M0 / M1)
- cBTC becomes the transactional medium (M2)

This is similar to how:

- Gold was the base store of value
- Banknotes were the medium of exchange

But **without the custodial risks** of traditional banking.

9.5 Long-Term Vision

In a mature Bitcoin economy, cBTC could form the backbone of:

1. Bitcoin-native commerce

Frictionless payments priced directly in BTC, but without spending unvested long-term savings.

2. Bitcoin treasury liquidity

Companies can operate working capital without selling BTC.

3. New rails for DeFi on Bitcoin

No altchains, no wrapped assets.

4. Lightning Network deep liquidity

Unvested yield tranches act as routing capital—making Lightning more efficient.

5. Institutional adoption

cBTC enables:

- predictable yield
- liquidity management
- transparent backing

- no fiat exposure
- regulatory simplicity

6. Global financial independence

A system built purely on Bitcoin rails can:

- operate across borders
- remain censorship-resistant
- avoid fiat inflation
- provide stable liquidity during global crises

9.6 Final Thoughts

cBTC represents a major innovation in Bitcoin-native finance:

- It is **not a stablecoin**
- It is **not synthetic Bitcoin**
- It is **not wrapped Bitcoin**
- It is **not an interest-bearing loan product**
- It is **not a centralized financial layer**

It is a *new category*:

Bitcoin-Denominated Elastic Liquidity

Powered by:

- Transparent reserves
- Non-custodial CP-controlled BTC
- Market-based redemption pricing
- Prefunded yield
- Lightning-native liquidity
- Simple CP governance

cBTC is Bitcoin—made liquid, scalable, and usable for the real economy.

---

10. Anti-Cycling Yield Mechanism

One of the most important economic safeguards in the cBTC system is the **Anti-Cycling Yield Mechanism**. This mechanism prevents Collateral Providers (CPs) from repeatedly depositing and withdrawing BTC to capture multiple rounds of prefunded yield. Without such a mechanism, an CP could:

1. Deposit 1 BTC

2. Receive 0.15 BTC prefunded yield
3. Withdraw after 1 month
4. Deposit again
5. Receive another 0.15 BTC
6. Repeat indefinitely

This would create an **extractive loop**, funneling value away from the system and weakening reserves.

To solve this, cBTC introduces a **non-linear vesting mechanism** that makes long-term CP participation meaningfully more profitable while heavily disincentivizing short-term cycling.

10.1 The Problem: Yield Cycling Attack

Without protection, the system could be abused via:

Short-Term Yield Farming

CP deposits to mint yield, then immediately exits and re-deposits to mint yield again.

Capital Churn

CPs try to maximize APY by rapid cycles, harming reserve stability.

Reserve Leakage

Repeated prefunded yield drains the Redemption Pool over time.

Incentives Misaligned

Small depositors could repeatedly extract yield without providing long-term liquidity to cBTC users.

To prevent this, we introduce a carefully designed **Vesting Function**.

10.2 Solution: Non-Linear Vesting Curve

The cBTC system uses a **non-linear yield vesting curve**, which determines how much yield an CP can withdraw based on time. Instead of vesting linearly (constant monthly unlocks), the curve is designed such that:

- **Very little yield vests early**
- Vesting increases significantly after several months
- Full vesting occurs only near the end of the 12-month period

This dramatically disincentivizes cycling.

Conceptual Vesting Curve (Example)

Lock Duration	% of Yield Vested	Notes
1 month	~3%	Almost no yield for short stay
2 months	~7%	Still minimal
3 months	~12%	CP can withdraw, but yield small
6 months	~40%	Steep increase
9 months	~70%	Strong incentive to stay longer
12 months	100%	Full yield vesting

CPs that exit after 1–3 months receive only a *small fraction* of the 0.15 BTC yield.

The remaining **unvested yield** automatically migrates to the **Redemption Reserves**, strengthening the solvency of the system.

10.3 Why Non-Linear Vesting Works

1. Discourages Short-Term CP Behavior

Fast exits are no longer profitable.

2. Strengthens Reserves

Unvested yield migrating to the Redemption Pool:

- increases backing
- increases system solvency
- reduces redemption risk

3. Rewards Long-Term CPs

The vesting curve makes long-term locking vastly more profitable than short-term cycles.

4. Simple, Transparent, Predictable

The vesting schedule is:

- published
- verifiable
- enforced via Taproot timelocks
- consistent across all CPs

5. Aligns Incentives

CPs become committed stakeholders:

- long-term liquidity
- governance participation
- sustainable yield

10.4 Taproot Enforcement of Vesting

Vesting is not managed by an off-chain server or protocol administrator. Instead, vesting is embedded **directly into Bitcoin UTXOs**:

- Each yield tranche is represented as a Taproot output.
- Each output contains its own time-based spending path.
- CPs can only spend yield that has reached the correct vesting timelock.
- The protocol cannot accelerate or cancel vesting.

Spending Conditions

Each yield UTXO contains paths:

1. **CP-only Path**
   - Activated after the vesting timelock expires
   - CP can spend without protocol approval
2. **Joint CP + Protocol Path**
   - Active before vesting
   - Used only for LN liquidity deployment
   - Cannot be used to give CP access to funds early
3. **Early Exit Migration Path**
   - If CP exits before vesting completes
   - Protocol-directed path migrates unvested yield to Redemption Pool

This architecture eliminates the possibility of CP extraction attacks.

10.5 Optional Complementary Mechanisms

Governance may optionally implement:

- **CP Commitment Multipliers**
- **Staggered Yield Tranche Release**
- **Reputation Scores for CP Reliability**
- **Dynamic Adjustments to Vesting Curves**
- **Cooldown Periods** (optional, though not necessary)

These are extensions, not core requirements.

10.6 Summary

The Anti-Cycling Yield Mechanism ensures:

- **Sustainable CP participation**
- **Protection against yield extraction attacks**

- **Strengthening of Redemption Reserves via unvested yield**
- **Alignment of long-term incentives**
- **Non-custodial enforcement using Taproot**

By preventing repeated yield farming, the protocol preserves solvency while maintaining a predictable, transparent, and Bitcoin-native economic model.

---

11. Major Risks & Critical Evaluation

Every monetary system—whether fiat, crypto, or Bitcoin-native—carries inherent risks. The purpose of this section is to critically analyze cBTC's design, identify potential weaknesses, and clearly articulate areas requiring careful management, further research, or conservative assumptions.

This section is intentionally critical. Its purpose is not to market cBTC, but to ensure the protocol is approached realistically, responsibly, and transparently.

11.1 Overview of Categories of Risk

We evaluate risks across:

1. **Economic Risks**
2. **Market Dynamics Risks**
3. **Liquidity Risks**
4. **User Behavior Risks**
5. **Technical / Implementation Risks**
6. **Governance Risks**
7. **Regulatory Risks**
8. **Adoption Risks**

11.2 Economic Risks

1. Large CP exits could temporarily reduce confidence

If many CPs exit around the same time:

- Redemption Reserves may temporarily outpace Yield Tranches
- cBTC users may fear slower reserve growth
- Market liquidity may thin

Mitigation:
Non-linear vesting ensures early exit penalizes CPs, boosting Redemption Reserves.

2. Excessive concentration of CPs

If a few CPs control too much collateral:

- Governance effectiveness could decrease
- Governance could be biased
- LN liquidity may be centrally controlled

Mitigation:
1 Vault = 1 Vote.

Deposit size does not influence voting weight.

3. Insufficient economic activity

cBTC stability improves with:

- redemptions
- minting
- trading volume
- LN routing revenue

Low usage means reserve growth slows.

Mitigation:
Protocol remains solvent even with low usage due to prefunded yield and conservative LTV.

4. High transaction fees on Bitcoin

Bitcoin base layer fees could reduce:

- user access to cBTC
- redemption efficiency

Mitigation:
Lightning-native cBTC and LN-based redemptions minimize L1 reliance.

11.3 Market Dynamics Risks

1. Volatile BTC/cBTC exchange rates

Because cBTC floats, rapid swings can:

- confuse users
- invite speculative trading
- impact arbitrage operations

Mitigation:
AMM design + arbitrage stabilizes price.

---

2. Liquidity fragmentation

If cBTC liquidity spreads across too many venues:

- arbitrage efficiency may slow
- AMM pools may become imbalanced

Mitigation:
Concentrated liquidity incentives + CP governance.

---

3. Price discovery challenges

Since cBTC is novel:

- initial market pricing may be inefficient
- early volatility expected

Mitigation:
Bootstrap via Marketplace Pool ensures initial liquidity.

11.4 Liquidity Risks

1. Sudden redemption surges ("bank run")

If many users redeem simultaneously:

- Redemption Pool could be strained
- AMM price swings become significant

Mitigation:

- No fixed peg eliminates death spiral risk
- Burning reduces supply and increases backing
- Redemption fee slows drains
- Unvested yield flows into reserves
- CP seniority ensures solvency

2. CP exit clustering

If many CPs exit within the same period:

- Long-term liquidity may temporarily reduce

Mitigation:
Non-linear vesting punishes short-term CPs.

Governance can slow new CP exits during extreme conditions.

11.5 User Behavior Risks

1. Misunderstanding cBTC as stablecoin

Users may mistakenly treat cBTC as pegged or "stable."

Mitigation:
Communication must emphasize:

- Floating BTC/cBTC rate
- No peg
- Natural price discovery

2. Yield-chasing without long-term commitment

Despite vesting, some CPs may seek short-term returns.

Mitigation:
Non-linear vesting makes early exits unprofitable.

3. Inexperienced LN operators

Using unvested yield as LN liquidity requires careful channel management.

Mitigation:
Protocol-run LN nodes can manage liquidity while CP retains ownership via Taproot paths.

11.6 Technical Risks

1. Taproot script complexity

Complex Tapscripts may introduce bugs.

Mitigation:

- Multiple independent audits

- Formal verification
- Public Taproot trees
- Minimalistic script design philosophy

2. LN routing policy complexity

Deploying unvested yield into LN channels is technically advanced.

Mitigation:
The protocol may:

- operate shared LN nodes
- use automated liquidity management tools
- limit LN deployment to conservative amounts

3. AMM implementation risks

AMM must be carefully designed to:

- adapt to liquidity levels
- avoid toxic arbitrage

Mitigation:
Use well-tested AMM math and external audits.

4. Multisig key compromise

A compromised key could disrupt operational modules.

Mitigation:

- MuSig2 reduces attack surface
- Hardware multisig
- Governance-based rotation

11.7 Governance Risks

1. CP collusion

If many CPs collude, they could adjust parameters unfavorably.

Mitigation:
1 CP = 1 vote prevents large CPs from dominating. 48-hour timelocks allow community monitoring.

2. Governance apathy

If CPs do not participate:

- parameter adjustments may be delayed
- system may not react quickly to market changes

Mitigation:
Automatic triggers (e.g., LTV floors) can act as guardrails.

Timelocks may slow reaction times.

Mitigation:
Emergency pause function can freeze minting (Not redemptions—those must always remain available.)

11.8 Regulatory Risks

1. Misclassification as a stablecoin

Some regulators may incorrectly treat cBTC as a stablecoin.

Mitigation:
Clear documentation:

- no USD peg
- floating BTC rate
- no fiat reserves
- no interest-bearing deposits

2. Misclassification as a security

CP yield could be misinterpreted as a security return.

Mitigation:

- Yield is prefunded, not promised
- CP retains full custody

- No expectation of profit from managerial efforts
- Non-custodial design

3. LN liquidity misunderstood as lending

Some jurisdictions may incorrectly view routing as lending.

Mitigation:
Routing fees are payments for providing channel liquidity, not interest.

11.9 Adoption Risks

1. Lack of early liquidity

Users may hesitate to adopt early due to low volume.

Mitigation:
Bootstrap Marketplace Pools + incentivized first-year CP program.

2. UX complexity

Bitcoin-native systems require:

- Lightning
- Tapscripts
- AMM interactions

Mitigation:
User-friendly wallets, SDKs, and simplified interfaces.

3. Learning curve

Users unfamiliar with cBTC may hesitate.

Mitigation:
Clear communications and educational resources.

11.10 Final Risk Assessment Summary

Risk Type	Severity	Mitigation Strength
Economic	Medium	Strong
Market	Medium	Moderate
Liquidity	Medium–High	Strong
Technical	Medium–High	Strong (Taproot + audits)
Governance	Low–Medium	Strong
Regulatory	Medium	Strong (Bitcoin-native design)
Adoption	Medium	Moderate

Overall, the cBTC system exhibits:

- **High solvency resilience**
- **Strong custody guarantees**
- **Strong alignment with Bitcoin incentives**
- **No exposure to fiat, stablecoin, or synthetic risks**
- **No liquidation cascades, no peg breaks, no rehypothecation**

It is a robust monetary architecture with manageable risks and clear mitigations.

---

12. Critical Evaluation Summary

The cBTC protocol represents a novel approach to Bitcoin-native monetary design, combining elements of free-banking theory, modern automated market making, Lightning Network liquidity, and Taproot-enforced custody. This section consolidates the strengths and weaknesses of the system into a clear, balanced assessment. The intention is to provide a realistic understanding of where cBTC excels and where it must be carefully managed.

12.1 Strengths of the cBTC System

1. Pure Bitcoin-Native Monetary Layer

cBTC avoids:

- fiat exposure
- centralized custodians
- wrapped tokens
- synthetic assets
- USD oracles

Everything occurs on Bitcoin rails.
This significantly reduces regulatory and systemic risk.

---

2. Fully Non-Custodial CP Model

CPs retain 100% ownership of:

- principal BTC
- all vested yield
- unvested yield (under constrained paths)

No entity, governance group, or protocol wallet can seize CP assets.

This is one of the strongest custody models in any crypto system.

---

3. Elastic, Market-Priced Supply

cBTC does not depend on:

- fixed pegs
- USD price feeds
- lending markets
- liquidations
- artificial arbitrage incentives

Instead:

- supply expands via minting when cBTC appreciates
- supply contracts via burning when cBTC depreciates
- AMM pricing ensures consistent market discovery
- arbitrage keeps markets aligned

This eliminates peg-collapse scenarios like UST.

---

4. Prefunded BTC Yield

Unlike lending-based protocols:

- yield is never borrowed from anyone
- yield is never rehypothecated
- yield is known and capped upfront
- there is no credit risk

The system cannot fail from:

- loan defaults
- cascading liquidations
- collateral mispricing

This makes cBTC yield fundamentally safer.

5. Reserve Strengthening Mechanisms

Reserves grow from:

- 0.2% redemption fees
- Unvested yield from early CP exits
- LN routing fees
- cBTC burns
- Increasing demand for cBTC

This creates a **positive feedback loop**:

more use → more fees → more reserves → stronger solvency.

6. Protection Against Yield Cycling

The non-linear vesting curve ensures:

- short-term CPs gain almost no yield
- long-term CPs receive most of the reward
- early exit strengthens reserves

Prevents extraction attacks and aligns incentives.

---

7. Optional Lightning Network Yield

Deploying unvested yield as LN liquidity:

- increases LN efficiency
- generates routing revenue
- supports Bitcoin's broader infrastructure
- increases effective returns for CPs
- deepens liquidity for cBTC transactions

This creates utility beyond simple monetary issuance.

---

8. Transparent Governance

- One CP vault = one vote
- No governance token speculation
- 48-hour timelocked changes

- Minimal set of adjustable parameters
- Public record of all decisions

Makes governance simple, fair, and tamper-resistant.

---

1. Complexity of Implementation

Bitcoin-native Taproot logic, LN channels, AMM pricing, and vesting tranches create:

- significant engineering challenges
- a large attack surface for bugs

This complexity requires:

- extensive audits
- simulation
- cautious rollout

---

2. Initial Liquidity Bootstrapping

Early phases may suffer from:

- thin markets
- price volatility
- slow adoption
- CP hesitancy

User trust must be earned gradually.

3. LN Channel Operational Risk

Using unvested yield as LN liquidity introduces:

- channel downtime risk
- routing optimization issues
- channel exhaustion during volatility

LN operation must be carefully managed.

---

4. Risk of Misunderstanding

Users may mistakenly think:

- cBTC is pegged to BTC or USD
- cBTC is a stablecoin
- CP yield is interest

Incorrect assumptions could harm user experience.

Clear communication is essential.

---

5. AMM Vulnerability to Low Liquidity

If AMM pools are small:

- slippage increases
- arbitrage inefficiency rises
- cBTC price becomes more volatile

Early liquidity incentives may be needed.

---

6. Governance Dependence

CP voting is simple but could face:

- low participation
- factional differences
- slow reaction times

Parameter mismanagement is possible if governance weakens.

---

7. Regulatory Uncertainty

Although Bitcoin-native design mitigates many risks, regulators may still misclassify:

- CP yield as interest
- cBTC as a security or stablecoin
- LN routing yield as lending income

Education, documentation, and transparency will be essential.

12.3 Systemic Risks That Are NOT Present

Unlike most crypto monetary systems, cBTC **does not** have the following failure vectors:

- No stablecoin peg to collapse
- No synthetic asset exposure
- No collateral liquidation cascades
- No leverage
- No rehypothecation
- No custodial risk
- No lending-based insolvency
- No cross-chain bridge risk
- No reliance on DeFi tokenomics
- No mint-at-fixed-price arbitrage attack vector

This dramatically improves long-term survivability.

12.4 Overall Assessment

cBTC is a **strong, well-structured, Bitcoin-native monetary protocol** that introduces several innovations:

Strengths:

- Fully non-custodial
- BTC-only economy
- Floating market-based pricing
- Elastic supply
- Prefunded yield
- Taproot-enforced vesting
- LN liquidity deployment
- Simple governance
- Systemic solvency protections

Weaknesses:

- Technically complex
- Requires high-quality engineering
- Relies on gradual adoption
- LN operations may be difficult early on
- Communication must prevent misunderstandings

Final Evaluation:

cBTC is **sound, sustainable, and aligned with Bitcoin principles**, but must be:

- implemented carefully
- audited rigorously
- explained clearly
- deployed incrementally

If executed well, cBTC could become the most important native monetary layer built on Bitcoin—enhancing liquidity, enabling commerce, and expanding Bitcoin's role in the global economy.

ANNEX I — Philosophical Foundations of cBTC

1. Introduction

The cBTC protocol is not merely a technical invention.

It is an answer to a deeper monetary question that Bitcoin has re-opened:

Is Bitcoin money, or is Bitcoin digital capital?

The distinction is essential.

If Bitcoin is simply "money," then there should be no need to build representations or liquidity layers on top of it.

But the market tells a different story: custody-based derivatives like wBTC, tBTC, and Liquid BTC continue to grow. This demand exists because Bitcoin—while the best store of value humanity has ever created—faces natural limitations as a medium of exchange.

Bitcoin's settlement properties (10-minute blocks, limited block space, high fees during congestion) make BTC a perfect **base asset**, but a challenging **working currency**.

This annex explains the philosophical reasoning behind cBTC: why such a system is needed, how it respects Bitcoin's ethos, and how it builds on the monetary insights of Mises, Hayek, Rothbard, Saifedean Ammous, Gigi, Foss, and other thinkers who shaped modern sound-money theory.

---

2. Bitcoin's Nature: Capital or Money?

In classical and Austrian economics, a distinction exists between:

- **Money proper** (the base settlement asset, like gold)
- **Fiduciary media / credit money** (liquid instruments circulating above the base asset)

Bitcoin today overwhelmingly behaves as **digital capital**:

- People accumulate it
- People hoard it
- People avoid spending it
- People build generational savings with it
- People prefer to borrow against it rather than dispose of it

This mirrors gold historically.

Gold was the hardest monetary asset—yet it failed as everyday money because individuals naturally avoid spending the scarcest thing they own.

As Saifedean Ammous wrote:

"People spend the easy money and save the hard money."

This is the essence of **Gresham's Law** applied to Bitcoin.

Thus, Bitcoin may be a perfect **store of value**, but the market still needs:

- a medium of exchange
- flexible working capital
- liquidity that does not sacrifice sovereignty
- low-fee transactional instruments
- a unit of account for daily usage

cBTC exists to fill this gap in a way consistent with Bitcoin's ethos.

---

3. The Monetary Trilemma: Why Bitcoin Cannot Be All Three Layers

Money ideally serves three purposes:

1. **Store of Value**
2. **Medium of Exchange**
3. **Unit of Account**

But as every Austrian economist from Mises to Rothbard observed, no monetary asset can excel at all three simultaneously.

This is analogous to the blockchain trilemma*: improving one dimension degrades the others*.

Gold solved the Store of Value dimension, but required **silver**, bills of exchange, and banknotes as the medium of exchange.

Bitcoin solves the digital Store of Value dimension more perfectly than gold ever could. But the medium of exchange layer must be built *on top*, not *within*, Bitcoin's base layer if we want:

- scalable payments
- low fees
- rapid finality
- privacy
- programmable liquidity
- flexibility for commerce

This is not a failure of Bitcoin.

It is the natural structure of all sound monetary systems.

---

4. Austrian Economics: Bitcoin as the New Gold Standard

Mises described fiduciary media (credit-based currency) as an unavoidable component of advanced economies—**provided it is transparently collateralized** and **not issued arbitrarily**.

Historically this required banks, vaults, and trust.

But Bitcoin changes the possibilities:

- 21M BTC
- perfect divisibility
- cryptographic enforcement
- programmable scripts (Taproot)
- transparent on-chain reserves
- no need for human issuers

cBTC is the first attempt to build a fiduciary-media layer aligned with Austrian principles **without custodians**, following Mises' foundational ideas but removing the institutional trust element.

Hayek imagined a world where currencies compete freely.

Bitcoin achieved the first part: a free-market base money.

cBTC creates the second part: a **Bitcoin-native competitive liquidity layer**, without banks or states.

Gigi and Saifedean note that:

"Bitcoin is the base layer. Commerce will happen on layers above it."

cBTC is precisely such a layer.

---

5. Why cBTC Is Needed: Market Demand for Bitcoin Liquidity

The market clearly demands:

- wrapped BTC

- tokenized BTC
- synthetic BTC
- Bitcoin-backed credit

But all existing systems introduce:

- custodial risk
- oracle risk
- rehypothecation
- centralized trust
- exposure to foreign blockchain security models

This is the very scenario Austrian economists warned about: monetary centralization driven by the need for liquidity. Gold was centralized not by philosophy but by *economic necessity*.

If the Bitcoin ecosystem does not create a self-custodial liquidity system, banks and institutions will.

They will custody BTC, leverage it, and reintroduce fiat credit expansion on top of Bitcoin— replicating the exact problems Bitcoin was designed to escape.

cBTC is a philosophical and strategic response to prevent Bitcoin from becoming "gold 2.0"— stored in institutional vaults, inaccessible to individuals.

---

6. Bitcoin as Productive Capital: Why cBTC Unlocks the Next Stage

Bitcoin today is **passive capital**.

It appreciates but does not produce.

In every mature economy, capital must become **productive**:

- land produces rent
- factories produce goods
- gold historically produced credit
- Bitcoin can produce **liquidity, yield, and working capital** without leaving self-custody

cBTC enables exactly this:

BTC holders become decentralized collateral providers for a global currency, without giving up control of their Bitcoin.

This transforms BTC from a static store of value into:

- generative capital

- collateral for liquidity
- a backbone for payments
- a mechanism to maintain sovereignty
- the reserve asset of a decentralized monetary layer

This is the world that Austrian economics envisioned:

a monetary system governed by market forces, collateral, and individual sovereignty—not by states or banks.

---

7. cBTC as a Decentralized Credit Expansion Layer

Unlike stablecoins or wrapped BTC, cBTC is **not**:

- pegged 1:1
- custodial
- fiat-denominated
- reliant on a bank
- dependent on market makers
- vulnerable to liquidation cascades

It is a **transparent, algorithmic redemption system** governed by:

- real BTC reserves
- predictable minting conditions
- an anti-liquidation design
- market supply and demand
- self-custodied collateral

This is the first implementation of fiduciary media *without* fractional-reserve banking.

It achieves what Mises described—liquidity emerging from collateral—but replaces banks with **cryptographic enforcement**.

---

8. The Alternative Future: Centralized Bitcoin Credit (The Threat)

If Bitcoin does not develop a natively decentralized credit system, the future is predictable:

- banks custody BTC
- institutions issue credit on top of BTC
- individuals lose sovereignty
- Bitcoin becomes the new institutional reserve asset
- the monetary layer becomes fiat again

In other words:

Bitcoin wins the asset layer but loses the monetary layer.

cBTC is a philosophical countermeasure to that outcome.

It ensures that:

- Bitcoin holders retain monetary power
- liquidity is not monopolized
- credit is not centralized
- sovereignty remains with the user
- decentralization continues into the higher layers

---

9. Conclusion: The Philosophical Essence of cBTC

cBTC is not just a financial protocol.

It is an attempt to realize the full potential of Bitcoin as sound money by building—

A decentralized, permissionless, Austrian-style liquidity and credit layer anchored in self-custodied Bitcoin.

It resolves the tension between Bitcoin as capital and Bitcoin as money.

It enables:

- Bitcoin as the base settlement asset
- cBTC as the circulating medium
- a transparent unit of account emerging naturally
- a sovereign, distributed, global monetary system

This is the monetary architecture Bitcoin deserves—and the one Austrian economists would likely have envisioned if they had access to cryptography.

📚 References

Austrian Economics

Menger, C. (1871). *Principles of Economics*. Vienna: Wilhelm Braumüller.
— Foundational work on the origin of money and spontaneous order.

Mises, L. von. (1912). *The Theory of Money and Credit*. Vienna: Duncker & Humblot.
— Explains the nature of money, fiduciary media, and monetary layers.

Mises, L. von. (1949). *Human Action: A Treatise on Economics*. New Haven: Yale University Press.
— Comprehensive exposition of Austrian capital theory and monetary structure.

Rothbard, M. N. (1963). *What Has Government Done to Our Money?* Auburn, AL: Ludwig von Mises Institute.
— A concise explanation of sound money and the centralization of gold.

Rothbard, M. N. (1983). *The Mystery of Banking*. New York: Richardson & Snyder.
— Detailed analysis of fractional-reserve banking and credit expansion.

Hayek, F. A. (1931). *Prices and Production*. London: Routledge.
— Discusses capital structure, liquidity needs, and economic coordination.

Hayek, F. A. (1976). *Denationalisation of Money: The Argument Refined*. London: Institute of Economic Affairs.
— Advocates free-market, competing currencies—philosophical precursor to layered Bitcoin money.

Modern Bitcoin Authors

Ammous, S. (2018). *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Hoboken: Wiley.
— Explains Bitcoin as hard money and why users do not spend the hardest monetary asset.

Ammous, S. (2021). *The Fiat Standard*. Self-published.
— Describes fiat as a credit system and contrasts it with Bitcoin's potential for decentralized collateral.

Gigi. (2019). *21 Lessons: What I Learned Falling Down the Bitcoin Rabbit Hole*. Self-published.
— Philosophical reflections on Bitcoin as a base layer and the emergence of higher monetary layers.

Gigi. (n.d.). "Essays on Bitcoin." dergigi.com.
— Articles on sovereignty, privacy, layers, and Bitcoin as a protocol for global commerce.

Annex II — cBTC FAQ

This FAQ is designed to answer the key questions users, Collateral Providers, exchanges, developers, and institutions may have about cBTC. All answers use the updated BTC-native model, with **no USD references**, **no fiat peg**, and **AMM-driven BTC/cBTC pricing**.

---

1. What is cBTC?

cBTC is a **Bitcoin-denominated liquidity token** backed by BTC reserves and redeemable for BTC using a **market-based BTC/cBTC exchange rate**. It is not pegged to USD, not synthetic, not wrapped, and not custodial.

cBTC expands Bitcoin's usefulness by acting as a **liquid, spendable medium of exchange** fully anchored to Bitcoin.

---

2. Why would anyone use cBTC instead of simply using BTC?

Most Bitcoin holders prefer to **never move or expose their cold-storage BTC**, because using BTC directly leaks:

- UTXO history
- wallet clusters
- ownership patterns
- transaction linkages
- net worth estimates
- taint/traceability
- security risk

cBTC solves this by letting users mobilize only the small portion of their BTC they want to use operationally, while keeping the rest untouched, private, offline, and out of risk.

In addition:

- cBTC can be used in programmable environments (Lightning, Layer 2 apps, cross-chain liquidity)
- cBTC is easier for repeated payments, contracts, and microtransactions
- cBTC can function as working capital without exposing or moving your long-term BTC holdings

BTC remains your "vault asset," while cBTC becomes your "operational asset."

---

3. Does cBTC replace BTC as money?

No.

BTC remains:

- the monetary base
- the savings asset
- the long-term store of value

cBTC simply provides a **risk-isolated layer for liquidity, payments, and programmability**, without touching your real BTC.

---

4. Isn't this similar to wBTC, tBTC, or other wrapped/tokenized BTC?

No.
This is the biggest misconception.

Wrapped or tokenized BTC:

- require a custodian or federation (BitGo, multisig, bridge operators)
- move your BTC off Bitcoin
- issue IOUs or tokens on other chains
- depend on third-party redemption
- are not Bitcoin-native
- are vulnerable to regulatory capture and custodian failure

cBTC never leaves Bitcoin rails, and your underlying BTC is never held by any custodian.

Redemption happens entirely on Bitcoin.

This is a **categorically different trust model** from all wrapped assets.

---

5. How is cBTC different from synthetic BTC (sBTC, mBTC, DLN synthetic BTC, etc.)?

Synthetic BTC products:

- do **not** hold real BTC
- rely on price oracles
- depend on collateral managers
- require liquidation systems
- operate entirely off Bitcoin
- are not redeemable for actual BTC
- expose users to smart contract and oracle risk

cBTC is fully backed by real BTC, verifiable on-chain, and always redeemable in native BTC.

There are no oracles required for price stabilization, no liquidation engines, and no synthetic exposure.

---

6. Why is privacy such an important reason to use cBTC?

Whenever you spend BTC:

- the receiver can study your UTXO
- they can approximate your BTC wealth
- they can follow the chain backward and forward
- your cold storage becomes linked to your spending behavior

Over time, this creates a **permanent forensic footprint**.

With cBTC:

- you only expose one UTXO when acquiring cBTC
- all subsequent activity happens with cBTC, not your treasury BTC
- Lightning/Taproot layers add extra privacy
- your long-term BTC savings remain unlinked and invisible

cBTC isolates your operational activity from your savings, protecting your privacy and security.

---

7. Does cBTC allow me to use my BTC without exposing my cold storage?

Yes.
This is one of its main design goals.

Users can:

- keep 95–99% of their BTC untouched

- “activate” only a chosen portion into cBTC for operational use
- perform payments, Lightning routing, contracts, and liquidity operations using cBTC
- never touch or reveal their cold-storage addresses again

This is impossible with BTC alone.

---

8. Is cBTC designed to compete with stablecoins like USDT or USDC?

No.

Stablecoins are **fiat-pegged**.

cBTC is **Bitcoin-denominated**.

cBTC is designed for:

- Bitcoin-native economies
- Bitcoin-denominated contracts
- Bitcoin liquidity markets
- Lightning-native commerce
- people who live in a BTC unit of account

It could be seen as an alternative to wrapped BTC, not stablecoins.

---

9. Is cBTC useful for Lightning Network liquidity?

Yes — and this is a major use case.

cBTC can be:

- routed
- pooled
- used as channel collateral
- integrated into Collateral Providers
- bridged between layers
- used in automated market makers

—all without revealing your main BTC holdings.

BTC can be used on LN too, but **every movement exposes your main UTXOs.** cBTC isolates this risk.

---

10. Why is it useful that cBTC is always redeemable for real BTC?

Because **no wrapped/tokenized BTC can provide this without trusting a custodian.**

With cBTC:

- redemption is on-chain
- fully self-custodial
- verifiable
- trustless
- not dependent on any federation

The holder of cBTC always has a direct path back to Bitcoin, not an IOU issuer.

This is the key property that synthetic BTC on Ethereum and other chains *cannot* match.

---

11. Why is cBTC needed at all if Bitcoin already exists?

Because Bitcoin is:

- an incredible savings asset
- extremely secure
- extremely robust
- but intentionally *not* designed as a programmable, high-frequency, operational liquidity system

BTC is “vault money.”

It's perfect for savings and long-term custody.

But it is **not** ideal for:

- business payments
- scalable LN routing
- programmable contracts
- multi-chain liquidity
- repeated microtransactions
- interacting with apps
- hedging
- capital-efficient liquidity allocation

cBTC fills this role **without ever compromising Bitcoin’s trust model**.

---

12. Isn’t using BTC directly simpler? Why add another layer?

BTC is simple — but using it operationally exposes:

- your privacy
- your treasury
- your keys
- your UTXOs
- your identity
- your net worth
- your risk surface

Businesses do not want to expose their vault every time they make a payment.

cBTC provides a safe, private, flexible working layer while BTC stays untouched as the savings layer.

---

12. Can cBTC be used without trusting exchanges or custodians?

Yes.

Buying, holding, transferring, and redeeming cBTC:

- does **not** require exchanges
- does **not** require custodians
- does **not** require multisig federations
- does **not** require wrapped IOUs

Only Bitcoin’s trust model.

---

13. Is cBTC a stablecoin?

No.

- It has no fiat peg
- It has no USD-denominated liabilities
- Its price floats relative to BTC
- It is redeemable for BTC, not dollars

cBTC behaves like a **Bitcoin-native monetary layer** similar to free-banking models—not like a stablecoin.

---

14. How does cBTC maintain fairness in minting and redemption?

Using an **internal AMM (Automated Market Maker)** that calculates the BTC/cBTC price based on pool ratios.

The AMM ensures:

- No fixed-price arbitrage
- No peg-collapse scenarios
- Market-driven supply expansion and contraction

This keeps cBTC's redemption rate always aligned with global market pricing.

---

15. What backs cBTC?

Only **BTC**, stored in two types of reserves:

1. **Redemption Reserves**

   Fund BTC redemptions.

2. **Yield Tranche Reserves**

   Prefunded CP yield, time-locked via Taproot. Unvested portions may be deployed as LN liquidity.

There is **no synthetic collateral** and **no wrapped Bitcoin**.

---

16. How is new cBTC created?

Two ways:

1. **(CP) Collateral Deposits** (Minting via LTV Ratio)

   CP deposits BTC → protocol mints cBTC at 30% LTV → cBTC moves to Marketplace Pool.

2. **BTC Purchases by Users** (Elastic Supply)

User sends BTC → Marketplace Pool mints/dispenses cBTC → BTC goes to reserves.

Both are driven **entirely by BTC inflows**.

---

17. How are redemptions executed?

Users send cBTC to the Redemption Pool and receive BTC based on:

- The AMM BTC/cBTC rate
- A 0.2% redemption fee

Redeemed cBTC is **burned**, increasing backing for remaining tokens.

---

18. Does cBTC rely on oracles?

No, not for core operations.

Pricing is determined by:

- internal AMM
- arbitrage with external markets

Oracles may be used only as **safety guardrails**, not for pricing.

---

19. What is the role of Collateral Providers (CPs)?

CPs deposit BTC to:

- enable cBTC minting
- earn prefunded BTC yield
- participate in governance
- provide long-term liquidity

CPs own all BTC they deposit and all yield they vest.

---

20. How does CP yield work?

CPs receive **15% BTC yield (initially)**, prefunded at the moment they deposit.

The yield:

- is split into time-locked Taproot tranches
- vests using a non-linear curve
- can be deployed as LN liquidity while unvested
- is fully non-custodial

Early CP exits unlock only **vested yield**, and unvested yield migrates to reserves.

---

21. What is the Anti-Cycling Yield Mechanism?

A **non-linear vesting curve** that:

- prevents CPs from repeatedly entering/exiting to claim multiple yields
- heavily penalizes early exits
- pushes unvested yield to reserves
- rewards long-term CP commitments

---

22. What happens if many users redeem cBTC at once?

The system remains stable because:

- AMM pricing lowers BTC returned per cBTC
- cBTC is burned during redemption
- Redemption fee increases reserve strength
- Coverage ratio increases for remaining cBTC
- CP collateral is never touched
- Unvested yield boosts reserves during CP exits

No peg = no death spiral.

---

23. Can cBTC collapse like UST or other algorithmic coins?

No, because:

- There is **no peg**
- There is **no synthetic collateral**
- There is **no debt relationship**
- There are **no liquidations**
- Redemptions always pay BTC at **market value**
- The system cannot be drained at fixed prices

cBTC avoids every known collapse mechanism in previous stablecoin failures.

---

24. What determines the price of cBTC?

A combination of:

- Internal AMM-based BTC/cBTC pricing
- External exchange arbitrage
- Supply and demand

No USD pricing is used.

---

25. How can users get cBTC?

Three ways:

1. Buy with BTC via Marketplace Pool
2. Acquire on exchanges (centralized or decentralized)
3. Receive payments from other users

---

26. Can cBTC be used on Lightning?

Yes.

cBTC can be:

- issued as a Taproot Asset (or equivalent)
- routed through LN channels
- funded through unvested yield-derived channels

This makes cBTC a **Bitcoin-native payments asset**.

---

27. What makes cBTC different from wrapped Bitcoin?

Everything.

- No custodian
- No Ethereum
- No bridge
- No redemption delays
- No synthetic representation

- UTXO-level ownership
- Taproot timelock enforcement

This is a **Bitcoin-only system**, not a wrapped asset.

---

28. What happens if the BTC price changes dramatically?

Nothing special.

cBTC is denominated in BTC, not USD.

All obligations and reserves are BTC-denominated, so BTC/USD volatility does not matter.

---

29. Why is cBTC useful to companies with Bitcoin treasuries?

Companies can:

- hold BTC as a treasury asset
- convert part of it to cBTC
- use it as working capital
- retain exposure to BTC
- avoid selling BTC
- use cBTC for payroll, expenses, and operations

cBTC is ideal for Bitcoin-based treasury management.

---

30. Is cBTC legal?

cBTC is:

- not a stablecoin
- not a security
- not a custodial product
- not an interest-bearing loan

Its Bitcoin-native model reduces regulatory exposure.

---

31. How can cBTC fail?

Potential failure vectors:

- incorrect Taproot scripts
- low early liquidity
- LN operational failures
- governance mismanagement

These risks are manageable but require caution.

---

32. Summary of Why cBTC Exists

Bitcoin needs:

- a liquid spendable unit
- without relying on fiat
- without wrapped assets
- without synthetic credit systems

cBTC is the first system to achieve this through:

- elastic supply
- BTC-only reserves
- AMM pricing
- non-custodial yield
- Lightning integration

cBTC is the **monetary glue** that enables a full Bitcoin-native economic ecosystem.

cBTC is the only Bitcoin-native, self-custodied, private, programmable synthetic BTC that is always redeemable for real Bitcoin without any third-party custody.

Annex III — cBTC Innovations Overview

This annex summarizes the core innovations introduced by the cBTC protocol. These innovations distinguish cBTC from stablecoins, synthetic assets, wrapped Bitcoin, and previous attempts at Bitcoin-native money markets. Together, they form a coherent and highly resilient monetary architecture that is fully anchored to Bitcoin.

---

1. Pure Bitcoin-Native Monetary System

Unlike stablecoins or wrapped assets, cBTC is:

- **denominated in BTC**
- **redeemable in BTC**
- **priced in BTC**
- **collateralized by BTC**
- **settled on Bitcoin**
- **optionally operable on Lightning**

No fiat exposure.
No bridges.
No alternative chains.
cBTC is the first functional **Bitcoin-only liquidity token**.

---

2. AMM-Based BTC/cBTC Pricing (No Peg, No Oracle Dependence)

cBTC introduces a **Bitcoin-native Automated Market Maker (AMM)** to determine the BTC/cBTC exchange rate for minting and redemption.

Innovations:

- Redemptions use **pool ratios**, not USD oracles
- Minting happens automatically when BTC flows into the system
- Arbitrage ensures convergence with external markets
- Avoids all fixed-price arbitrage attack vectors

This makes cBTC fundamentally different from:

- stablecoins
- synthetic assets
- wrapped assets
- bridged Bitcoin

---

3. Taproot-Enforced Non-Custodial CP Custody

Traditional crypto protocols take custody of user funds. cBTC does not.

CP funds remain under:

- **their own private keys**
- with **Taproot timelocks**
- and **MuSig2 multi-party constraints**

Innovations:

- Protocol can **coordinate** but never unilaterally spend CP funds
- Vesting enforced through Bitcoin timelocks
- Unvested yield has restricted spending paths (LN-only)

This is one of the strongest custody guarantees in crypto.

---

4. Prefunded BTC Yield (No Lending, No Leverage)

cBTC introduces a yield mechanism fundamentally different from CeFi or DeFi systems.

What it is:

- Yield paid in BTC
- Fully prefunded at deposit time
- Hard-capped
- Enforced by Taproot
- Non-custodial

What it is NOT:

- Not interest
- Not lending
- Not dependent on borrowers
- Not rehypothecated
- Not credit-based

This eliminates the insolvency risks seen in:

- Celsius
- Voyager
- BlockFi
- Terra
- Synthetic stablecoins

---

5. Non-Linear Anti-Cycling Vesting Curve

A major innovation is the **defense against yield cycling attacks**, where CPs repeatedly deposit and withdraw to extract multiple yields.

cBTC's solution:

- Vesting curve starts slow
- Accelerates later
- Penalties for early withdrawal
- Unvested yield flows to reserves

Result:

- Long-term CP incentives
- Protection against extractive behavior
- Strengthening of Redemption Pool

---

6. Unvested Yield as Lightning Network Liquidity

This is a groundbreaking feature:

Unvested yield tranches:

- are owned by the CP
- cannot be withdrawn early
- can be used as **Lightning liquidity collateral**
- earn LN routing fees
- reinforce system reserves

Benefits:

- Strengthens Lightning
- Generates additional non-inflationary yield
- Aligns incentives between CPs and LN operators
- Provides real economic activity, not speculative yield

This ties cBTC into the broader Bitcoin payments ecosystem.

---

7. Elastic Supply Controlled Entirely by BTC Flows

cBTC expands and contracts supply via:

- CP minting
- User purchases
- Redemptions
- AMM-driven pricing

There is **no peg** and **no fixed value**.

Benefits:

- No peg break risk
- No liquidation cascades
- No oracle-based failures
- No obligation to maintain parity to an external asset

The system is reflexive but internally self-correcting.

---

8. BTC-Only Reserve Structure

Two separate Bitcoin reserves:

1. **Redemption Pool** (for redemptions)
2. **Yield Tranches** (for CP yield)

Both are:

- visible on-chain
- controlled through cryptographic scripts
- independent of fiat or other tokens

cBTC is one of the few systems with:

- truly transparent reserves
- no hidden liabilities
- no off-chain claims

---

9. Governance Without Tokens

Most crypto protocols use governance tokens prone to:

- speculation
- plutocracy
- centralization
- regulatory risk

cBTC uses:

- **1 CP vault = 1 vote**
- No token issuance
- No token inflation
- No governance token capture

This creates:

- simple governance
- stable decision-making
- direct representation of economic participants

---

10. Built-In Reserve Accretion Mechanisms

cBTC reserves grow over time due to:

- redemption fees
- unvested yield migration
- arbitrage gains
- LN routing yield
- BTC inflows from user purchases

This creates a **self-reinforcing solvency engine**.

In contrast, many protocols rely on:

- inflationary token issuance
- external subsidies
- yield farming bribes

cBTC is sustainable without these mechanisms.

---

11. Novel Monetary Architecture for Bitcoin

cBTC introduces a new category in monetary design:

Bitcoin-Denominated Elastic Liquidity (BDEL)

Key characteristics:

- Non-custodial savings base (BTC)
- Elastic liquidity token (cBTC)
- Market-based redemption
- Prefunded yield

- Lightning-activated unvested yield
- Complete Bitcoin-native accounting system

This is conceptually similar to:

- Free banking
- Gold-backed banknotes

  But with:

- cryptographic certainty and transparency
- no custodians
- immutable redemption rules

---

12. Integration Across Bitcoin Layers

cBTC unifies several layers of Bitcoin:

Layer	Role
Bitcoin L1	Custody, minting, redemption, vesting, reserve tracking
Taproot	Timelocks, vesting curves, spending-path control
Lightning Network	Yield deployment, liquidity provisioning, payments
cBTC Token Layer	Medium of exchange, unit of liquidity

This is one of the few systems to:

- use LN liquidity as a *yield engine*
- deploy prefunded yield non-custodially
- allow full round-trip redemption in BTC

---

13. Comparison to Existing Projects

Feature	Stablecoins	Wrapped BTC	Synthetic BTC	cBTC
Peg	Fiat	BTC	Synthetic	None
Custody	Custodial	Custodial	Smart contracts	Non-custodial Taproot
Yield	Lending	None	Variable	Prefunded BTC + LN Routing
Redemptions	Fiat	BTC	Synthetic	BTC via AMM
Liquidation Risk	High	Low	High	None
Oracle Dependence	High	Low	High	Optional (guardrails only)
Bitcoin-Native	No	Partial	No	Yes

cBTC is the only model that:

- requires no fiat
- requires no synthetic collateral
- requires no wrapped BTC
- avoids peg-death dynamics
- provides BTC-only yield
- can act natively on Lightning

---

14. Selective Activation of BTC (Partial Mobilization Model)

Traditional wrapped or synthetic BTC models require users to deposit **their entire BTC collateral** into a custodial or federated system.

cBTC introduces an innovation whereby users **activate only the portion of their BTC they need as operational liquidity**, while leaving the remainder:

- in cold storage,
- unmoved,
- unexposed,
- and fully private.

This allows BTC holders to maintain long-term savings in secure custody, while deploying cBTC as a **separated working-capital layer** for payments, contracts, liquidity operations, or Lightning usage.

This "partial activation" model does not exist in wrapped BTC or synthetic models and mirrors real-world treasury management:

vault asset (BTC) vs operational asset (cBTC).

---

15. Native Bitcoin Redeemability Without Custodians or Federations

All existing synthetic or wrapped BTC solutions—wBTC, tBTC, renBTC, Liquid L-BTC, exchange IOUs—require:

- custodians,
- multisig federations,
- bridge operators,
- smart contract custodians, or
- third-party redemption agents.

cBTC is the first system where:

- collateral BTC never leaves Bitcoin's base layer,
- no federation or custodian holds user funds,
- redemption occurs entirely on-chain,
- users maintain direct, final on-chain custody of the underlying BTC.

This creates a **trust-minimized synthetic Bitcoin** with backing and redeemability fully anchored in Bitcoin without external dependencies.

---

16. UTXO Isolation and Operational Privacy Layer

Spending BTC directly exposes a user's UTXO history, revealing:

- transaction ancestry,
- previous counterparties,
- potential wallet clusters,
- balance inference,
- patterns of holdings,
- and risk of forensic linkage.

cBTC introduces a formal **UTXO isolation layer**:

- Users expose only the UTXO used to acquire cBTC.
- All subsequent activity—payments, routing, contracts, settlement—occurs with cBTC.
- Underlying BTC holdings remain permanently unlinked and unexposed.
- Lightning and Taproot-based representations add further privacy guarantees.

This provides substantial privacy, security, and operational protection, especially for businesses, institutions, and high-value holders.

---

17. Off-Chain Transport Privacy Through Lightning and Taproot Assets

Once BTC is converted into cBTC, the asset can be moved using:

- Lightning Network
- Taproot Assets
- onion-routed multi-hop payment paths
- private channel rebalancing
- non-chain-visible settlement flows

This achieves:

- no on-chain footprint for cBTC transfers
- sender–receiver unlinkability

- elimination of address reuse
- transaction metadata privacy
- resistance to chain surveillance heuristics
- optional asynchronous, off-chain settlement

This privacy model **cannot be achieved using on-chain BTC alone**, especially for repeated operational transactions or business activity.

---

18. Fungibility Restoration and Non-Propagation of On-Chain "Taint"

Bitcoin transactions carry historical traces that may be misclassified as "taint" or risk flags by exchanges or blockchain analytics systems.

Because cBTC transfers occur **off-chain** and do not propagate UTXO ancestry:

- historical taint does not follow cBTC users
- cBTC gains **greater fungibility** than on-chain BTC
- counterparties cannot link operational flows to prior BTC history
- cBTC enables clean, uniform units for everyday use
- businesses avoid forensic exposure of treasury assets

This effectively creates a **fungibility restoration mechanism** at the working-capital layer, while maintaining the integrity of the user's original BTC holdings.

---

19. Bitcoin-Native Yield and Liquidity Incentives Without Rehypothecation

Existing BTC yield systems rely on:

- custodial lending,
- rehypothecation,
- exchange risk,
- smart contract custodians,
- or oracle-driven liquidation markets.

cBTC introduces a **Bitcoin-native liquidity mechanism** in which:

- CPs never hold or rehypothecate user BTC,
- yield comes from protocol mechanics (cBTC/BTC spreads, redemption fees),
- the system operates without leverage, custodial lending, or fractionalization.

This creates a completely new category of **risk-transparent, Bitcoin-backed yield** that preserves Bitcoin's custody guarantees.

20. Cross-Layer and Cross-Chain Representation Without Wrapped Custody

All existing cross-chain BTC representations require custody via:

- BitGo (wBTC),
- federations (tBTC, Liquid),
- multisig bridges,
- smart contract custody (WBTC on EVM chains),
- oracle-managed synthetics.

cBTC, however:

- originates natively on Bitcoin,
- can be represented on Lightning, Taproot Assets, or other layers,
- can be bridged trust-minimized via commitment proofs,
- without ever transferring or locking underlying BTC into a custodial structure.

This makes cBTC the only multi-layer Bitcoin asset that **does not require leaving Bitcoin's trust model**.

---

21. BTC Unit-of-Account Stability (Bitcoin-Denominated Financial Layer)

Most crypto assets used in commerce or financial systems are USD-pegged, forcing users into a fiat-denominated mental model.

cBTC creates a Bitcoin-denominated financial layer enabling:

- BTC-priced contracts,
- BTC-native liquidity markets,
- BTC-denominated yield,
- and an internal floating BTC/cBTC exchange rate.

This supports economic activity in a **true Bitcoin unit-of-account**, independent of fiat systems.

---

22. Economic Separation Between Savings Layer and Working Layer

Bitcoin itself excels as a **savings technology**, but directly using BTC for:

- business payments,
- repeated transactions,
- liquidity provision,
- contract automation,
- cross-layer mobility

exposes treasury UTXOs, increases operational risk, and reduces privacy.

cBTC introduces an explicit economic model:

- **BTC = savings layer**
- **cBTC = operational layer**

This separation enables institutions and individuals to safely use Bitcoin in productive contexts without compromising long-term security or privacy.

---

23. No Oracle Dependence for Collateral Integrity

Synthetic BTC systems outside Bitcoin depend on:

- external price oracles,
- liquidation engines,
- collateral debt positions,
- smart contract failure modes.

These create systemic risk, dependency, and complexity.

cBTC avoids these requirements entirely:

- backing is simple and on-chain,
- no oracle is needed for collateral integrity,
- no liquidation risk exists,
- the model remains deterministic and audit-friendly.

This simplifies the security model and ensures robustness under adversarial conditions.

---

24. Programmability Without Trust Trade-Offs

Other programmable BTC wrappers require:

- EVM smart contracts,
- custodial minting keys,
- trusted bridges,
- multisig governance.

cBTC achieves programmability through:

- Taproot commitments,
- Lightning-native representation,
- cross-layer interoperability,
- deterministic redemption mechanisms.

This allows developers to build **BTC-native financial and operational applications** without trusting external custodial systems.

---

25. Guaranteed, Permissionless Redeemability

Redemption is a core guarantee:

- every cBTC is redeemable for BTC,
- redemption does not require permission or approval,
- no entity can freeze, halt, or block redemption,
- redeemability is guaranteed by protocol rules, not institutions.

This stands in stark contrast to:

- centralized wrapped tokens,
- federated peg systems,
- synthetic derivatives dependent on external collateral managers.

Conclusion

cBTC represents a fundamentally new category of Bitcoin-native synthetic asset defined by:

- **Bitcoin-native AMM for BTC/cBTC pricing**
- **Taproot-enforced custodianless CP vaults**
- **Prefunded BTC yield**
- **Non-linear vesting to prevent yield cycling**
- **Unvested yield as LN liquidity**
- **Self-growing BTC reserves**
- **Elastic supply without pegs or fiat**
- **Governance without tokens**
- **Full transparency of reserves and tranches**
- **A new monetary layer for Bitcoin**
- **no custodial dependency**,
- **no off-chain trust**,
- **no federation control**,
- **privacy through UTXO isolation**,
- **partial activation of BTC**,
- **DAO-free, deterministic mechanisms**,

- **native Bitcoin redeemability**,
- **programmability without leaving Bitcoin**,
- **cross-layer mobility**,
- **and Bitcoin-denominated financial operations**.

This architecture enables cBTC to function as a **secure, private, programmable Bitcoin working capital layer**, while leaving the user's core BTC savings untouched, unmoved, and fully self-custodied.