

# **cBTC Whitepaper:**

## **A Bitcoin-Backed Monetary Protocol**

James Tector

jamestector@gmail.com

### **Abstract**

cBTC is a Bitcoin-native working capital protocol that enables the issuance of credit-like instruments fully backed by Bitcoin, without fiat pegs, price oracles, liquidations, or custodial risk. The protocol extends Bitcoin's utility beyond passive holding by allowing Bitcoin to be used as productive capital under deterministic and auditable rules.

cBTC is issued through Minting Channels, where participants lock Bitcoin at a maximum loan-to-value of 30%. Deposited Bitcoin is programmatically allocated between time-locked principal, a dedicated redemption reserve, and a non-linear yield allocation. This structure ensures over-collateralization, pre-funded yield, and strict solvency guarantees.

cBTC functions as a bearer asset secured by Bitcoin private keys and may exist both as on-chain bearer notes for settlement and redemption, and as a Lightning-based asset for low-cost, high-frequency transfers. Redemption is always available through a global Redemption Pool and follows transparent, rule-based haircut tiers during periods of reserve depletion, without liquidations or forced collateral seizure.

By combining conservative collateralization, layered asset representation, and deterministic redemption, cBTC introduces a native Bitcoin credit layer designed for real-world working capital use while preserving Bitcoin's core principles of self-custody, transparency, and monetary discipline.

---

## **1. Introduction**

Bitcoin has established itself as a robust form of digital money and a secure store of value. Its monetary properties—fixed supply, censorship resistance, and self-custody—have made it uniquely suited for long-term savings. However, Bitcoin's design prioritizes monetary finality over capital productivity. As a result, Bitcoin is often

treated as inert collateral: valuable, but difficult to deploy as working capital without relinquishing custody or accepting significant systemic risk.

Most existing attempts to extract utility from Bitcoin collateral rely on trusted intermediaries, fiat-pegged instruments, or liquidation-based lending models. Wrapped Bitcoin, custodial lending platforms, and synthetic stablecoins all introduce external dependencies that undermine Bitcoin’s trust model. These systems typically require price oracles, margin calls, discretionary liquidation, or custodial control of collateral—features that are incompatible with Bitcoin’s ethos of self-sovereignty and monetary discipline.

cBTC is designed as a native alternative. Rather than importing financial abstractions from fiat or DeFi systems, cBTC treats Bitcoin itself as productive capital and builds a conservative credit layer directly on top of it. The protocol allows Bitcoin holders to generate liquidity and yield without surrendering ownership, without relying on external price feeds, and without exposing collateral to liquidation risk. Credit issuance is bounded by deterministic rules and anchored entirely in Bitcoin-denominated constraints.

At its core, cBTC introduces the concept of “**Minting Channels**”: Bitcoin-secured contracts that lock collateral under predefined conditions and authorize the issuance of a fixed quantity of cBTC. These channels define explicit limits on leverage, yield, and redemption, ensuring that every unit of cBTC in circulation is backed by locked Bitcoin and governed by transparent solvency rules. Unlike account-based credit systems, cBTC does not rely on discretionary risk management or dynamic collateral valuation; all economic behavior is expressed in advance through protocol invariants.

cBTC is intended to function as working capital rather than settlement money. To fulfill this role, the protocol separates custody and finality from circulation. While Bitcoin remains the ultimate settlement layer, cBTC can circulate off-chain as a bearer asset over Bitcoin-secured payment channels, enabling low-cost and high-frequency transfers without compromising self-custody. On-chain representations of cBTC are reserved for settlement, redemption, and final state transitions.

By combining conservative collateralization, layered asset representation, and deterministic redemption mechanics, cBTC seeks to expand Bitcoin’s economic surface area without weakening its foundations. The protocol does not aim to replace Bitcoin as money, but to complement it by enabling a native, transparent, and non-custodial form of Bitcoin-backed working capital.

---

## 2. Protocol Overview and Actors

The cBTC protocol defines a deterministic system for issuing, circulating, and redeeming Bitcoin-backed working capital. It is structured around a small number of clearly defined actors and a limited set of state transitions, each governed by explicit Bitcoin-denominated rules. The protocol avoids discretionary decision-making and external dependencies by encoding economic behavior directly into issuance, custody, and redemption constraints.

---

## 2.1 Core Actors

### **Collateral Providers (CPs)**

Collateral Providers are Bitcoin holders who choose to open Minting Channels in order to issue cBTC. By depositing Bitcoin into the protocol, a Collateral Provider authorizes the minting of a fixed quantity of cBTC under predefined rules.

A Collateral Provider:

- deposits Bitcoin into a Minting Channel,
- receives newly issued cBTC,
- retains ownership of the underlying collateral subject to time-lock conditions,
- may earn yield as long as the Minting Channel remains open.

Collateral Providers are not borrowers in the traditional sense. They do not face margin calls, liquidations, or price-based collateral adjustments. Their obligations and benefits are fixed at the moment a Minting Channel is opened.

---

### **cBTC Holders**

cBTC holders are any entities that possess cBTC, regardless of whether they originally minted it. Holders may acquire cBTC through issuance, exchange, or payment, and may transfer it freely within the constraints of the protocol's asset representation.

cBTC holders:

- control cBTC via Bitcoin private keys,
- may hold cBTC on-chain or off-chain,
- may redeem cBTC for Bitcoin according to the protocol's redemption rules,
- are exposed to redemption haircuts during periods of reserve depletion.

Holding cBTC does not confer any claim on principal collateral or yield allocations. The only enforceable claim associated with cBTC is the right to redeem against the Redemption Pool under the current protocol conditions.

---

### **Coordinators**

Coordinators are protocol participants that facilitate minting, redemption, and state tracking. They are responsible for assembling transactions, validating protocol rules, and publishing publicly auditable system state.

In the real-world protocol design:

- coordinators do not custody Bitcoin,
- coordinators cannot unilaterally modify protocol rules,
- coordinator actions are fully observable and verifiable.

The protocol is designed so that coordination can be performed by multiple independent parties over time. No single coordinator is essential to the long-term integrity of the system.

---

## 2.2 Minting Channels

Minting Channels are the fundamental issuance mechanism of the cBTC protocol. A Minting Channel is created when a Collateral Provider deposits Bitcoin into a set of predefined locking conditions. Once opened, a Minting Channel authorizes the minting of a fixed quantity of cBTC and defines the collateral structure that backs it.

Each Minting Channel:

- is opened with a single Bitcoin transaction,
- locks Bitcoin under deterministic allocation rules,
- has a defined lifecycle from opening to closure,
- operates independently of all other Minting Channels.

Minting Channels do not interact with market prices or external data feeds. All parameters governing issuance, yield, and redemption are fixed at channel creation.

---

## 2.3 Issuance Constraints

cBTC issuance is governed by strict loan-to-value limits expressed exclusively in Bitcoin terms. For each unit of Bitcoin deposited into a Minting Channel, a fixed quantity of cBTC is minted at a maximum loan-to-value of 30%.

The deposited Bitcoin is allocated as follows:

- a time-locked principal portion,
- a dedicated contribution to the global Redemption Pool,
- a yield allocation subject to time-based vesting.

These allocations are immutable once the Minting Channel is opened and cannot be modified off-chain.

---

## 2.4 Asset Representation and Circulation

The protocol treats cBTC as a bearer asset secured by Bitcoin private keys. cBTC may exist in two complementary representations:

- **On-chain bearer form**, used for settlement, redemption, and final state transitions.
- **Off-chain form**, carried over Bitcoin-secured payment channels, enabling low-cost and high-frequency transfers suitable for working capital use.

Ownership of cBTC is always defined by control of Bitcoin keys. No account-based ledger, centralized registry, or custodial balance system exists within the protocol.

Circulation of cBTC is expected to occur primarily off-chain, while on-chain representation serves as a settlement and redemption layer.

---

## 2.5 Redemption Pool

The Redemption Pool is a global Bitcoin reserve dedicated exclusively to the redemption of cBTC. Bitcoin enters the Redemption Pool through predefined protocol events, including the opening of Minting Channels and the forfeiture of unvested yield.

The Redemption Pool:

- holds Bitcoin only,
- performs no function other than cBTC redemption,
- cannot be used for yield generation or discretionary spending.

Bitcoin can leave the Redemption Pool only in exchange for provably burned cBTC and according to the protocol's redemption rules.

---

## 2.6 System-Level Invariants

The protocol enforces a set of global invariants that apply across all Minting Channels:

- cBTC issuance is capped per channel and constrained by Bitcoin collateral.
- A minimum global solvency threshold must be maintained between outstanding cBTC and Redemption Pool reserves.
- New Minting Channels cannot be opened when solvency thresholds are violated.
- Redemption never touches principal or yield collateral.

These invariants are essential to the protocol's stability and are enforced through deterministic rules rather than discretionary intervention.

---

## 3. Minting, Issuance Math, and Collateral Allocation

This section defines the deterministic rules governing cBTC issuance. All cBTC in circulation originates from Minting Channels and is backed by Bitcoin locked under predefined conditions. No other issuance mechanism exists.

---

### 3.1 Minting Channel Creation

A Minting Channel is created when a Collateral Provider deposits Bitcoin into the protocol under a single on-chain transaction. This transaction establishes the full collateral structure of the channel and authorizes the minting of cBTC.

Let:

- **D** = total Bitcoin deposited by the Collateral Provider (in BTC)

Minting Channels are subject to a per-channel deposit cap to limit risk concentration. The protocol does not impose a global supply cap on cBTC; total supply is constrained by collateral availability and global solvency rules.

Once a Minting Channel is opened, its parameters are immutable.

---

### 3.2 Issuance Rate and Loan-to-Value Constraint

cBTC issuance is governed by a fixed, Bitcoin-denominated loan-to-value constraint.

- **Maximum LTV:** 30%
- **Issuance rate:**

$$\text{Minted cBTC} = 30,000 \times P$$

This issuance rate corresponds to a redemption floor of:

$$1 \text{ cBTC} = 0.00001 \text{ BTC}$$

The issuance rate is fixed at channel creation and does not depend on market prices, volatility, or external data.

---

### 3.3 Collateral Allocation

The Bitcoin deposited into a Minting Channel is programmatically allocated into three distinct portions at the moment of channel creation:

#### ***Principal (70%)***

$$\text{Principal} = 0.70 \times D$$

The principal portion represents the core collateral backing the Minting Channel. It is time-locked for a minimum duration and cannot be accessed, pledged, or redeemed while the channel remains open.

Principal collateral is never used for cBTC redemptions and is not exposed to liquidation under any circumstances.

---

#### ***Redemption Reserve Contribution (15%)***

$$\text{Redemption Contribution} = 0.15 \times D$$

This portion is transferred to the global Redemption Pool at channel creation. It serves as immediate backing for cBTC redemptions and contributes to system-wide solvency.

Once transferred, this Bitcoin is no longer associated with the individual Minting Channel and cannot be reclaimed by the Collateral Provider.

---

#### ***Yield Allocation (15%)***

$$\text{Yield Allocation} = 0.15 \times D$$

The yield allocation represents prefunded yield associated with the Minting Channel. This Bitcoin is locked under time-based conditions and is released to the Collateral Provider only as long as the Minting Channel remains open.

Yield allocation:

- is not pooled globally,
- does not participate in redemptions,
- is forfeited in whole or in part if the channel is closed early.

Unvested yield is redirected to the Redemption Pool upon early channel closure.

---

## 3.4 Immutability of Channel Parameters

Once a Minting Channel is opened:

- the deposited amount **D**,
- the minted cBTC quantity,
- the collateral split between principal, redemption, and yield,
- and the time-lock conditions

are fixed and cannot be altered.

There is no mechanism for:

- increasing issuance against the same collateral,
- refinancing a channel,
- adjusting collateral ratios,
- or rolling over positions.

To increase cBTC exposure, a new Minting Channel must be opened under current protocol conditions.

---

## 3.5 Channel Lifecycle

Each Minting Channel follows a simple lifecycle:

1. **Opening**
  - Bitcoin is deposited.
  - Collateral is allocated.
  - cBTC is minted and credited to the Collateral Provider.
2. **Active Period**
  - Principal and yield remain locked.
  - cBTC circulates independently of the channel.
  - Yield vests progressively over time.
3. **Closure**
  - Principal is released to the Collateral Provider.
  - Vested yield is paid out.
  - Unvested yield, if any, is transferred to the Redemption Pool.

Channel closure does not depend on the outstanding amount of cBTC in circulation. cBTC remains redeemable independently of the channel lifecycle.

---



## 3.6 Minting Channel Duration and Time Constraints

Minting Channels are time-bound contracts with predefined minimum and maximum durations. These time constraints are enforced at channel creation and define both yield eligibility and early-closure conditions.

---

### *Minimum Lock Period*

Each Minting Channel is subject to a minimum lock period during which principal collateral cannot be released and the channel cannot be closed without forfeiting yield.

- **Minimum duration:**

**1 month**, defined as approximately **4,320 Bitcoin blocks**

This minimum lock period serves several purposes:

- prevents rapid mint-and-close behavior,
- ensures that cBTC issuance represents committed capital rather than transient leverage,
- aligns yield incentives with meaningful time commitment.

Channels closed before the minimum lock period forfeit **all** associated yield, which is redirected to the Redemption Pool.

---

### *Maximum Channel Duration*

Minting Channels are not perpetual. Each channel has a defined maximum duration after which it must be closed or settled.

- **Maximum duration:**

**1 year**, defined as approximately **52,560 Bitcoin blocks**

At maximum duration:

- the Minting Channel reaches full maturity,
- the entire yield allocation becomes fully vested,
- principal collateral is eligible for release upon closure.

Channels cannot be extended, rolled over, or renewed automatically. To continue participation, a new Minting Channel must be opened under the protocol rules in effect at that time.

---

## ***Yield Accrual Within the Duration Window***

Yield accrues only while the Minting Channel remains open and locked within the defined duration window.

- Yield is:
  - non-linear,
  - back-loaded,
  - distributed across predefined vesting tranches.
- Yield accrual stops immediately upon channel closure, regardless of duration reached.

Early closure results in partial or total forfeiture of unvested yield, which is transferred to the Redemption Pool.

---

## ***Duration Invariants***

The following duration-related invariants apply to all Minting Channels:

- Channels cannot be closed before the minimum lock period without yield forfeiture.
- Channels cannot remain open beyond the maximum duration.
- Duration parameters are fixed at channel creation and cannot be altered.
- Duration constraints apply independently to each Minting Channel.

These constraints ensure predictable capital commitment, prevent abuse, and support the protocol's global solvency mechanisms.

---

## **3.7 Independence of Minting Channels**

Minting Channels are isolated from one another:

- Failure or closure of one channel does not affect others.
- Yield is calculated and distributed per channel.
- Principal collateral is not cross-linked or rehypothecated.

System-wide solvency is managed exclusively through the Redemption Pool and global issuance constraints, not through inter-channel dependency.

---

## **3.8 Summary of Issuance Invariants**

The following issuance invariants hold at all times within the cBTC protocol:

- All cBTC originates exclusively from Minting Channels.
- Issuance is fixed at **30,000 cBTC per BTC deposited**, corresponding to a maximum loan-to-value of 30%.
- Bitcoin deposited into a Minting Channel is immutably allocated between:
  - time-locked principal collateral,
  - a global Redemption Pool contribution,
  - and a prefunded yield allocation.
- Principal collateral is never liquidated and is never used for redemptions.
- Redemption collateral is prefunded, global, and can only be used to redeem burned cBTC.
- Yield is prefunded, non-linear, time-based, and forfeitable upon early channel closure.
- Minting Channels are time-bound contracts with a fixed minimum lock period and a fixed maximum duration.
- Full yield eligibility requires the Minting Channel to remain open for the entire maximum duration.
- Minting Channels cannot be modified, extended, refinanced, or rolled over once opened.
- Minting Channels are isolated from one another and do not share principal or yield collateral.

These invariants define the economic and temporal structure of cBTC issuance and ensure predictable behavior across all Minting Channels regardless of market conditions.

---

## 4. Yield Mechanics and Time-Based Incentives

The cBTC protocol incorporates yield as a deterministic, prefunded incentive for locking Bitcoin capital over time. Yield is not generated through lending, rehypothecation, or market activity. Instead, yield is allocated at Minting Channel creation and distributed according to explicit time-based rules.

This design ensures that yield is earned through commitment and patience rather than through leverage, risk-taking, or discretionary management.

---

### 4.1 Prefunded Yield Allocation

For each Minting Channel, a fixed portion of the deposited Bitcoin is reserved as yield at channel creation:

$$\text{Yield Allocation} = 0.15 \times D$$

where **D** is the total Bitcoin deposited into the Minting Channel.

This yield allocation:

- is locked under Bitcoin-enforced conditions,
- is associated exclusively with a single Minting Channel,
- does not interact with or depend on other channels,
- is never pooled or rehypothecated.

Because yield is prefunded, the protocol does not promise future returns based on uncertain revenue or system growth. All yield obligations are fully collateralized from the outset.

---

## 4.2 Non-Linear Yield Distribution

Yield within a Minting Channel is distributed according to a **non-linear, back-loaded schedule**. This means that yield accrues slowly during the early stages of the channel and accelerates as the channel approaches full maturity.

The purpose of non-linear distribution is to:

- discourage short-term channel openings,
- reward long-term capital commitment,
- align yield incentives with system stability.

Yield is divided into **six discrete vesting tranches**, each becoming available only after specific time thresholds are reached.

---

## 4.3 Vesting Tranches

The yield allocation of a Minting Channel is divided into six tranches, each representing a portion of the total yield. Tranches vest sequentially over the lifetime of the channel.

While the exact tranche schedule may evolve over time, the following principles apply:

- Tranches vest only while the Minting Channel remains open.
- Tranches vest at predefined block-height milestones between the minimum and maximum channel duration.
- Unvested tranches are forfeited upon early channel closure.

The final tranche vests only if the channel remains open for the full maximum duration.

---

## 4.4 Early Closure and Yield Forfeiture

If a Minting Channel is closed before reaching full maturity:

- only vested yield tranches are paid out to the Collateral Provider,
- all unvested yield is forfeited,
- forfeited yield is transferred to the global Redemption Pool.

This mechanism serves two critical purposes:

1. It penalizes early exits without threatening principal collateral.
2. It strengthens system solvency by replenishing redemption reserves during periods of reduced commitment.

There is no mechanism to reclaim forfeited yield or retroactively vest yield after channel closure.

---

## 4.5 Yield Independence and Isolation

Yield is calculated, vested, and distributed **per Minting Channel**. There is no global yield pool and no shared yield exposure between channels.

As a result:

- yield earned by one Collateral Provider does not depend on the behavior of others,
- yield risk is fully localized to the channel that generated it,
- failure or early closure of one channel does not affect yield outcomes elsewhere.

This isolation eliminates systemic yield risk and prevents the formation of centralized yield “honeypots”.

---

## 4.6 Yield and Redemption Separation

Yield allocations are strictly separated from redemption mechanics:

- Yield Bitcoin is never used to redeem cBTC.
- Yield Bitcoin cannot be accessed by cBTC holders.
- Yield Bitcoin becomes redemption collateral **only if forfeited** due to early channel closure.

This separation ensures that yield incentives do not weaken redemption guarantees and that redemption behavior remains predictable and transparent.

---

## 4.7 Yield Invariants

The following yield-related invariants apply at all times:

- Yield is prefunded at Minting Channel creation.
- Yield accrues only while the channel remains open.
- Yield distribution is non-linear and time-based.
- Yield is isolated per channel and never pooled.
- Early channel closure results in forfeiture of unvested yield.
- Forfeited yield strengthens the Redemption Pool.

These invariants ensure that yield serves as an incentive for long-term participation without introducing leverage, rehypothecation, or systemic risk.

---

## 5. Redemption Pool and Redemption Mechanics

Redemption is the mechanism through which cBTC is converted back into native Bitcoin. The cBTC protocol is designed so that redemption is always rule-based, transparent, and independent of discretionary intervention. Rather than relying on liquidations or price oracles, redemption is governed by a dedicated Bitcoin reserve and deterministic payout rules.

---

### 5.1 The Redemption Pool

The Redemption Pool is a global Bitcoin reserve whose sole purpose is to redeem cBTC. Bitcoin enters the Redemption Pool through predefined protocol events and cannot be used for any other function.

Bitcoin flows into the Redemption Pool from:

- the redemption allocation of newly opened Minting Channels,
- unvested yield forfeited upon early channel closure.

The Redemption Pool:

- holds Bitcoin only,
- does not generate yield,
- does not participate in governance,
- does not interact with principal collateral,
- cannot be accessed for any purpose other than cBTC redemption.

This design ensures that the Redemption Pool remains structurally simple and resistant to misuse.

---

## 5.2 Redemption Invariant

A fundamental invariant of the protocol is:

**Bitcoin can leave the Redemption Pool only in exchange for provably burned cBTC.**

For every redemption:

1. cBTC is destroyed and removed from circulation.
2. Bitcoin is released from the Redemption Pool according to the current redemption rules.

There is no mechanism to redeem cBTC by accessing principal or yield collateral. All redemptions are settled exclusively from the Redemption Pool.

---

## 5.3 Maximum Redemption Liability

Let:

- **O** = total outstanding cBTC supply,
- **P** = Bitcoin balance of the Redemption Pool.

At the redemption floor price of:

$$1 \text{ cBTC} = 0.00001 \text{ BTC}$$

the maximum Bitcoin liability implied by outstanding cBTC is:

$$L = O \times 0.00001 \text{ BTC}$$

The protocol tracks the **coverage ratio**:

$$R = P \setminus L$$

This ratio determines the effective redemption rate.

---

## 5.4 Redemption Coverage Tiers and Haircuts

Redemption is always available but is subject to coverage-based payout tiers designed to preserve system solvency under stress.

### ***Tier 1: High Coverage***

If:

$$R \geq 0.70$$

then redemptions are paid at the full floor rate:

$$1 \text{ cBTC} = 0.00001 \text{ BTC}$$

---

### ***Tier 2: Medium Coverage***

If:

$$0.35 \leq R < 0.70$$

then redemptions are paid at a discounted rate:

$$1 \text{ cBTC} = 0.000005 \text{ BTC}$$

This haircut reduces outflows while preserving redemption availability.

---

### ***Tier 3: Low Coverage***

If:

$$R < 0.35$$

then the Redemption Pool is distributed **pro-rata** across all cBTC presented for redemption:

$$\text{Redemption Price} = P/O \text{ BTC per cBTC}$$

In this regime, all redeemers receive the same proportional share of the remaining Bitcoin reserves.

---

## **5.5 Redemption Ordering**

Redemption requests are processed on a **first-in-first-out (FIFO)** basis within each coverage tier.



Because the coverage ratio and effective redemption price are publicly observable, cBTC holders can make informed decisions about when to redeem based on current system conditions.

---

## 5.6 No Liquidations, No Forced Actions

The redemption mechanism does not involve:

- margin calls,
- liquidations,
- forced seizure of collateral,
- or dynamic collateral valuation.

Redemption haircuts apply uniformly based on global coverage, not individual behavior. Collateral Providers are not penalized through principal loss, and cBTC holders accept redemption outcomes according to transparent protocol rules.

---

## 5.7 Interaction with Global Solvency Controls

Redemption mechanics operate alongside global issuance constraints.

If the Redemption Pool coverage falls below required thresholds:

- new Minting Channels are halted,
- no additional cBTC can be issued,
- redemption continues under the applicable coverage tier.

This separation ensures that redemption remains functional even during periods of issuance suspension.

---

## 5.8 Redemption Invariants

The following invariants apply to redemption at all times:

- Redemption is always possible.
- Redemption never touches principal collateral.
- Redemption never touches yield allocations.
- Bitcoin leaves the Redemption Pool only against burned cBTC.
- Redemption payouts follow deterministic coverage tiers.
- Redemption does not depend on price oracles or external markets.

These invariants ensure orderly behavior under both normal and stressed conditions while preserving the protocol's conservative economic design.

---

## 6. Global Solvency Controls and Issuance Limits

The cBTC protocol enforces global solvency through explicit Bitcoin-denominated constraints that apply across all Minting Channels. These controls ensure that the aggregate supply of cBTC remains bounded by available redemption reserves and that systemic risk cannot accumulate through unchecked issuance.

Global solvency is enforced deterministically and does not rely on discretionary risk management, price feeds, or reactive intervention.

---

### 6.1 System-Wide Solvency Objective

The primary solvency objective of the protocol is to ensure that a meaningful portion of outstanding cBTC liabilities is always backed by immediately available Bitcoin reserves.

This objective is expressed through the following invariant:

**The Bitcoin balance of the Redemption Pool must be at least 50% of the maximum redemption liability implied by outstanding cBTC supply.**

This threshold is designed to:

- provide credible redemption backing,
  - absorb redemption demand under stress,
  - prevent dilution of cBTC holders through excessive issuance.
- 

### 6.2 Measurement of Solvency

Let:

- **O** = total outstanding cBTC supply,
- **P** = Bitcoin balance of the Redemption Pool,
- **L** = maximum redemption liability at the floor price.

Then:

$$L = O \times 0.00001 \text{ BTC}$$

The system-wide solvency ratio is defined as:

$$S = P \setminus L$$

This ratio is continuously observable and forms the basis for issuance controls.

---

## 6.3 Hard Issuance Halt

The protocol enforces solvency through a **hard halt on new issuance**.

If:

$$S < 0.50$$

then:

- no new Minting Channels may be opened,
- no additional cBTC may be issued,
- issuance remains suspended until solvency is restored.

There is no mechanism to override this halt, scale issuance dynamically, or permit partial issuance. The issuance rate is either fully enabled or fully disabled based on the solvency threshold.

This design prioritizes simplicity, predictability, and resistance to discretionary abuse.

---

## 6.4 Solvency Restoration Mechanisms

Solvency may be restored through the following protocol-native mechanisms:

- Opening of new Minting Channels once issuance resumes, contributing additional Bitcoin to the Redemption Pool.
- Forfeiture of unvested yield from early channel closures.
- Reduction of outstanding cBTC supply through redemptions and burns.

No emergency recapitalization, governance intervention, or external funding mechanism exists within the protocol.

---

## 6.5 Issuance Caps and Risk Containment

To limit concentration risk, the protocol enforces a maximum deposit size per Minting Channel.

- **Maximum deposit per Minting Channel:** 5 BTC

This cap:

- limits the impact of individual participants,
- reduces systemic exposure to single-channel behavior,
- encourages distributed issuance.

The protocol does not impose a fixed global supply cap on cBTC. Aggregate supply is constrained by:

- available Bitcoin collateral,
  - Redemption Pool solvency,
  - and the hard issuance halt mechanism.
- 

## 6.6 Independence from Market Prices

All solvency calculations and issuance controls are expressed exclusively in Bitcoin terms.

The protocol does not consider:

- fiat prices,
- exchange rates,
- volatility metrics,
- or market capitalization.

As a result, solvency behavior is deterministic and independent of external market conditions.

---

## 6.7 Solvency Invariants

The following solvency-related invariants apply at all times:

- cBTC issuance is constrained by Bitcoin collateral, not market prices.
- A minimum Redemption Pool coverage threshold must be maintained.
- Issuance halts automatically when solvency thresholds are violated.
- Solvency is restored only through protocol-native mechanisms.
- No discretionary authority can override issuance constraints.

These invariants ensure that cBTC remains a conservative, Bitcoin-backed working capital instrument even under adverse conditions.

---

## 7. Asset Representation and Circulation

cBTC is designed as a bearer asset secured by Bitcoin itself. Ownership, transfer, and redemption of cBTC are always defined by control of Bitcoin private keys rather than

by accounts, balances, or custodial ledgers. The protocol separates **settlement and finality** from **circulation**, allowing cBTC to function efficiently as working capital without compromising self-custody.

---

## 7.1 Bearer Asset Model

cBTC does not exist as an account-based token or as a separate blockchain asset. Instead, cBTC is a bearer claim whose control is derived from Bitcoin cryptographic keys.

In all representations:

- there is no concept of an account balance maintained by the protocol,
- there is no centralized registry of ownership,
- possession of cBTC is equivalent to possession of the corresponding Bitcoin private keys.

This model ensures that cBTC inherits Bitcoin's core custody guarantees and censorship resistance.

---

## 7.2 Dual Representation

To balance security, finality, and cost-efficient circulation, cBTC may exist in two complementary representations:

- **On-chain bearer representation**, used for settlement, redemption, and final state transitions.
- **Off-chain representation**, carried over Bitcoin-secured payment channels, used for high-frequency, low-cost transfers.

Both representations correspond to the same global cBTC supply. Moving cBTC between representations does not change total supply and does not affect redemption rights.

---

## 7.3 On-Chain Bearer Representation

In its on-chain form, cBTC is represented by Bitcoin UTXOs that are associated with a defined quantity of cBTC. Control over these UTXOs is enforced by standard Bitcoin scripts and private keys.

On-chain cBTC:

- is self-custodied via Bitcoin keys,

- can be transferred using standard Bitcoin transactions,
- can be provably burned to authorize redemption,
- is intended primarily for settlement, escrow, and redemption.

Because on-chain transfers incur Bitcoin transaction fees, this representation is not intended for frequent movement and does not serve as the primary circulation layer.

---

## 7.4 Off-Chain Circulation Layer

To fulfill its role as working capital, cBTC is designed to circulate primarily off-chain. Off-chain circulation allows cBTC to be transferred at low cost and high frequency without requiring on-chain Bitcoin transactions for each transfer.

Off-chain cBTC:

- remains secured by Bitcoin cryptography,
- is controlled by the same private keys used for Bitcoin payment channels,
- can be transferred instantly and with minimal fees,
- does not require custodial intermediaries.

The protocol does not mandate a specific off-chain implementation but is compatible with Bitcoin-native payment channel systems that support asset transfer.

---

## 7.5 Supply Neutrality Across Layers

Let:

- $S_{on}$  be the on-chain cBTC supply,
- $S_{off}$  be the off-chain cBTC supply.

At all times:

$$S_{total} = S_{on} + S_{off}$$

Transitions between on-chain and off-chain representations:

- require a provable destruction of cBTC in one layer,
- result in the creation of an equivalent amount in the other,
- do not affect total supply.

Minting increases total supply. Redemption decreases total supply. Circulation between layers is supply-neutral.

---

## 7.6 Self-Custody and Transfer Guarantees

In both representations:

- users retain exclusive control over their cBTC,
- no party can freeze, seize, or reassign cBTC without the owner's signature,
- transfers require cryptographic authorization by the holder.

There is no administrative control over cBTC balances, and no protocol component has the ability to arbitrarily move user funds.

---

## 7.7 Circulation Invariants

The following invariants apply to cBTC representation and circulation:

- cBTC is always a bearer asset secured by Bitcoin private keys.
- No account-based or custodial ledger exists within the protocol.
- On-chain representation provides settlement and redemption finality.
- Off-chain representation provides low-cost, high-frequency transfers.
- Movement between representations does not affect total supply.
- Ownership of cBTC is independent of Minting Channel lifecycle.

These properties ensure that cBTC can function as efficient working capital while remaining fully aligned with Bitcoin's custody and security model.

---

# 8. Security Model and Trust Assumptions

The cBTC protocol is designed to minimize trust while remaining practical to deploy in the real world. Its security model is based on a clear separation between **custody-critical guarantees**, which are enforced by Bitcoin itself, and **coordination functions**, which may be performed by protocol participants without granting them control over funds.

This section explicitly defines what the protocol guarantees, what it assumes, and how failures are handled.

---

## 8.1 Bitcoin-Enforced Security Guarantees

The following properties are enforced directly by Bitcoin and do not depend on trusted intermediaries:

## ***Custody of Collateral***

- Principal collateral is locked under Bitcoin time-lock conditions.
- Yield allocations are locked under deterministic, time-based conditions.
- Redemption Pool Bitcoin is held in restricted outputs dedicated exclusively to redemption.

No protocol participant can unilaterally move, seize, or reassign these funds.

---

## ***Immutability of Minting Channels***

Once a Minting Channel is opened:

- the deposited amount,
- the issued cBTC quantity,
- the collateral allocation,
- and the channel duration

are immutable on-chain facts. They cannot be altered by off-chain processes or discretionary decisions.

---

## ***Bearer Ownership of cBTC***

In all representations, ownership of cBTC is defined by control of Bitcoin private keys. No account system, administrator, or registry can override cryptographic ownership.

---

## ***Provable Burn for Redemption***

Redemption of cBTC requires provable destruction of cBTC supply. Bitcoin can leave the Redemption Pool only after a corresponding burn event has occurred.

---

## **8.2 Protocol-Level Coordination**

Some protocol functions require coordination and state tracking beyond what Bitcoin alone can express. These functions do not involve custody of funds and do not grant discretionary control over protocol assets.

Coordination functions include:

- assembling Minting Channel transactions,
- tracking total outstanding cBTC supply,
- tracking Redemption Pool balances,



- computing redemption coverage ratios,
- enforcing issuance halts,
- processing redemptions according to protocol rules.

These functions are deterministic and auditable. Multiple independent parties may perform them using publicly observable data.

---

## 8.3 Role of Coordinators

Coordinators are protocol participants that perform coordination functions.

A coordinator:

- does not custody Bitcoin,
- does not control user funds,
- cannot modify protocol rules,
- cannot access principal or yield collateral,
- cannot redeem cBTC without burn.

Coordinator behavior is transparent and verifiable. Incorrect or malicious behavior can be detected by any observer using public blockchain data.

The protocol is designed so that coordination roles are replaceable and non-exclusive.

---

## 8.4 Failure Scenarios and System Behavior

The protocol is designed to fail safely.

### ***Coordinator Failure***

If coordinators become unavailable:

- no new Minting Channels can be opened,
- redemptions may be delayed.

However:

- no Bitcoin collateral is lost,
- no cBTC balances are altered,
- no protocol rules are violated.

Alternative coordinators may resume operation using public state.

---

## ***Redemption Stress***

If redemption demand exceeds available reserves:

- redemption continues under coverage-based haircut rules,
- no liquidations occur,
- principal collateral remains untouched.

The system degrades predictably rather than catastrophically.

---

## ***Adversarial Behavior***

Attempts to:

- mint cBTC without collateral,
- withdraw Redemption Pool funds without burning cBTC,
- seize principal or yield collateral

are prevented by Bitcoin-enforced conditions.

---

## **8.5 Trust Assumptions**

The protocol makes the following explicit assumptions:

- Bitcoin functions as specified and maintains consensus.
- Participants can verify blockchain state independently.
- Coordinators may exist but are not trusted with custody.
- Users retain responsibility for their private keys.

No assumption is made about:

- market prices,
  - external liquidity,
  - discretionary governance intervention.
- 

## **8.6 Security Invariants**

The following security invariants apply at all times:

- Custody of Bitcoin collateral is enforced by Bitcoin.
- cBTC ownership is defined solely by cryptographic keys.
- No liquidation mechanism exists.
- No administrator can override protocol rules.

- Coordination does not imply custody.

These invariants ensure that cBTC extends Bitcoin's economic functionality without introducing custodial or discretionary risk.

---

## 9. Lifecycle, Failure Modes, and System Behavior

This section describes how the cBTC protocol evolves over time and how it behaves under normal operation, stress, and partial failure. The protocol is designed to be conservative and predictable, favoring safe degradation over dynamic intervention.

---

### 9.1 System Lifecycle

The cBTC protocol progresses through a series of well-defined lifecycle phases driven by Minting Channel activity and redemption behavior.

---

#### ***Issuance Phase***

During normal operation:

- Collateral Providers open Minting Channels.
- Bitcoin is locked and allocated according to protocol rules.
- New cBTC is minted and enters circulation.
- Redemption Pool reserves increase through issuance and forfeited yield.

Issuance remains enabled as long as global solvency thresholds are maintained.

---

#### ***Circulation Phase***

Once issued:

- cBTC circulates independently of its originating Minting Channel.
- Transfers occur primarily off-chain to minimize costs.
- cBTC holders may exchange, hold, or redeem cBTC at any time.

Circulation does not affect channel collateral or yield accrual.

---

## ***Maturity and Closure Phase***

As Minting Channels reach maturity:

- Yield tranches vest progressively.
- Upon closure, principal collateral is released to the Collateral Provider.
- Vested yield is paid out.
- Unvested yield is forfeited to the Redemption Pool.

Channel closure does not alter outstanding cBTC supply.

---

## ***Contraction Phase***

System contraction occurs when:

- redemption demand exceeds issuance,
- cBTC is burned through redemptions,
- issuance halts due to solvency constraints.

In contraction, the system reduces outstanding cBTC supply without liquidations or forced collateral actions.

---

## **9.2 Failure Modes and Safe Degradation**

The cBTC protocol is designed to fail safely rather than dynamically intervene under stress.

---

### ***Issuance Suspension***

If global solvency thresholds are breached:

- new Minting Channels are halted,
- no new cBTC is issued.

Existing channels continue to operate normally. Redemption remains available under the applicable coverage tier.

---

### ***Redemption Stress***

Under heavy redemption demand:

- redemption payouts follow deterministic haircut tiers,

- redemption continues even under reserve depletion,
- no participant is prioritized beyond FIFO ordering.

The system degrades proportionally rather than catastrophically.

---

### ***Coordinator Failure***

If coordinators cease operation:

- issuance pauses,
- redemption processing may be delayed.

No Bitcoin collateral is endangered. The protocol can resume operation once coordination is restored by any party capable of reconstructing public state.

---

### ***Participant Exit***

If Collateral Providers exit early:

- principal collateral remains protected,
- unvested yield is forfeited,
- redemption reserves are strengthened.

There is no contagion effect between Minting Channels.

---

## **9.3 Absence of Liquidations and Forced Actions**

At no point does the protocol:

- liquidate collateral,
- seize principal,
- revalue positions,
- or compel participant behavior.

All protocol outcomes result from predefined rules triggered by explicit actions or time-based conditions.

---

## **9.4 Predictability and Transparency**

All protocol behavior is:

- deterministic,

- based on publicly observable data,
- verifiable by any participant.

No discretionary intervention, emergency governance, or opaque risk management exists within the system.

---

## 9.5 System-Level Invariants

Throughout its lifecycle, the cBTC protocol maintains the following invariants:

- Bitcoin collateral is never rehypothecated.
- Issuance is bounded by explicit solvency constraints.
- Redemption operates independently of Minting Channel lifecycle.
- Yield incentives reinforce long-term participation.
- Failure modes preserve custody and system integrity.

These properties ensure that cBTC behaves as a conservative, Bitcoin-native working capital instrument across all operational conditions.

# ANNEX I — Philosophical Foundations of cBTC

## Bitcoin as Money and Bitcoin as Capital

Bitcoin is most commonly understood as money: a scarce, bearer asset optimized for settlement, savings, and censorship-resistant transfer. Its fixed supply, verifiability, and resistance to discretionary control make it uniquely suited as a store of value and a unit of final settlement.

However, throughout economic history, money has also functioned as capital. Capital is money deployed with time preference, risk constraints, and contractual discipline. When money becomes capital, it does not lose its monetary properties; instead, it acquires temporal structure.

Bitcoin today excels as money but remains underdeveloped as capital. Most attempts to deploy Bitcoin productively either remove custody, introduce price dependency on fiat currencies, or rely on liquidation-based risk management. These approaches treat Bitcoin as collateral to be managed rather than as capital to be respected.

cBTC is built on the premise that Bitcoin can function as capital *without* sacrificing its monetary integrity.

---

## Credit Without Fiat Abstractions

Modern credit systems are deeply intertwined with fiat assumptions: elastic supply, central price discovery, discretionary intervention, and liquidation-based enforcement. When these abstractions are applied to Bitcoin, they introduce fragility rather than utility.

cBTC rejects these abstractions entirely. It does not:

- peg to fiat currencies,
- depend on external price feeds,
- adjust leverage dynamically,
- liquidate collateral in response to market movements.

Instead, cBTC expresses credit purely in Bitcoin terms. Credit issuance is bounded by fixed loan-to-value constraints. Obligations are defined at inception and do not change in response to price volatility. Risk is managed through conservative collateralization, time commitment, and deterministic redemption—not through reactive intervention.

This approach treats credit not as a speculative instrument, but as a contractual transformation of time-locked capital into liquidity.

---

## **Time Preference as the Core Risk Variable**

In the cBTC protocol, time—not price—is the dominant variable.

Yield is not generated by trading, lending, or rehypothecation. It is prefunded and earned exclusively through sustained capital commitment. Participants are rewarded for locking Bitcoin over meaningful time horizons, and penalized for early exit through yield forfeiture rather than collateral seizure.

This structure reflects a fundamental economic insight: capital formation requires time preference alignment. Short-term leverage introduces systemic fragility; long-term commitment produces stability.

By embedding time directly into issuance, yield, and redemption mechanics, cBTC internalizes this principle at the protocol level.

---

## **Bearer Assets and Monetary Discipline**

Both Bitcoin and cBTC are bearer assets. Ownership is defined by cryptographic control rather than by accounts or permissions. There is no concept of identity, reputation, or administrative override within the protocol.

Bearer systems impose discipline. Losses are not socialized. Gains are not subsidized. Participants must evaluate risk based on transparent rules rather than discretionary assurances.

cBTC extends this bearer model to credit. Holders of cBTC accept redemption outcomes according to publicly known solvency conditions. There are no guarantees beyond what the protocol explicitly provides. This transparency replaces trust with verifiability.

---

## **Solvency Over Liquidity**

Traditional financial systems prioritize liquidity, often at the expense of solvency. When liquidity disappears, systems rely on emergency intervention, balance sheet expansion, or forced liquidation.

cBTC inverts this priority. Solvency is preserved even if liquidity contracts. Issuance halts when reserves fall below defined thresholds. Redemption continues under deterministic haircuts rather than being suspended or selectively honored.

This ensures that the system remains coherent under stress. Participants may face losses, but the rules do not change.

---



## Bitcoin-Native, Not Bitcoin-Derived

cBTC is not an overlay that abstracts away Bitcoin's constraints. It is built by embracing them.

All custody-critical guarantees are enforced by Bitcoin. All economic limits are expressed in Bitcoin terms. All transfers preserve self-custody. The protocol does not attempt to make Bitcoin behave like fiat or like a general-purpose smart contract platform.

Instead, it accepts Bitcoin's limitations and builds a conservative credit layer that operates *because* of them, not despite them.

---

## Capital Formation Without Centralization

Historically, capital formation has required trusted intermediaries. cBTC explores a different path: capital formation through deterministic rules enforced by a neutral settlement layer.

The protocol does not assume perfect decentralization from the outset. It acknowledges the role of coordination while rejecting custody and discretion. Over time, coordination can be distributed, replaced, or automated—but the underlying economic invariants remain unchanged.

This separation between protocol rules and implementation allows cBTC to evolve without compromising its foundational principles.

---

## Conclusion

cBTC is not an attempt to replace Bitcoin, nor to optimize it for every possible use case. It is a focused exploration of one question:

*Can Bitcoin function as productive capital  
without ceasing to be sound money?*

The protocol answers this question by constraining credit, privileging solvency, embedding time preference, and preserving self-custody. In doing so, cBTC seeks to expand Bitcoin's economic role while remaining faithful to the principles that made Bitcoin valuable in the first place.

## Annex II — cBTC Frequently Asked Questions (FAQ)

---

### What is cBTC in simple terms?

cBTC is a Bitcoin-native working capital instrument. It allows Bitcoin holders to lock BTC under deterministic rules and receive a transferable, Bitcoin-backed asset that can be used for payments, liquidity, or exchange—without selling their Bitcoin, without fiat pegs, and without liquidation risk.

---

### Is cBTC a stablecoin?

No.

cBTC is not pegged to any fiat currency and does not attempt to maintain a stable fiat price. It is denominated entirely in Bitcoin terms and represents a fixed claim against Bitcoin redemption reserves under predefined rules.

---

### How is cBTC issued?

cBTC is issued through **Minting Channels**. A Collateral Provider deposits Bitcoin into a Minting Channel and receives cBTC according to a fixed issuance rate:

- **30,000 cBTC per BTC deposited**
- Maximum loan-to-value: **30%**

All cBTC in circulation originates from Minting Channels.

---

### What happens to the Bitcoin deposited in a Minting Channel?

The deposited Bitcoin is immutably allocated at channel creation:

- **70%** is locked as principal collateral
- **15%** is contributed to the global Redemption Pool
- **15%** is reserved as prefunded yield

These allocations cannot be modified after the channel is opened.

---

## Can the protocol liquidate my Bitcoin?

No.

There are no liquidations, margin calls, or price-based collateral adjustments in cBTC. Principal collateral is never seized or sold, regardless of market conditions.

---

## How long is Bitcoin locked in a Minting Channel?

Minting Channels are time-bound:

- **Minimum lock period:** approximately 1 month ( $\approx 4,320$  blocks)
- **Maximum duration:** approximately 1 year ( $\approx 52,560$  blocks)

Full yield eligibility requires the channel to remain open for the entire maximum duration.

---

## How does yield work?

Yield is prefunded at channel creation and distributed over time:

- Yield is **non-linear and back-loaded**
- It is divided into **six vesting tranches**
- Yield accrues only while the channel remains open
- Closing a channel early forfeits unvested yield

Forfeited yield is transferred to the Redemption Pool.

---

## Where does the yield come from?

Yield does not come from lending, trading, or rehypothecation. It is prefunded by the Collateral Provider at channel creation. The protocol does not promise returns generated by system activity or growth.

---

## How can cBTC be transferred?

cBTC can be transferred in two ways:

- **Off-chain**, using Bitcoin-secured payment channels, enabling low-cost and high-frequency transfers
- **On-chain**, using Bitcoin transactions for settlement and redemption

Most circulation is expected to occur off-chain to minimize transaction costs.

---

## Is cBTC self-custodial?

Yes.

In all representations, control of cBTC is defined by Bitcoin private keys. There are no accounts, balances, or custodians controlling cBTC on behalf of users.

---

## Does cBTC have its own blockchain or address format?

No.

cBTC does not have a separate blockchain or address system. On-chain cBTC is represented by Bitcoin UTXOs, and off-chain cBTC is carried over Bitcoin-secured payment channels.

---

## How does redemption work?

cBTC can be redeemed for Bitcoin through the global Redemption Pool. Remember:

- cBTC is **burned** during redemption
  - Bitcoin is paid out from the Redemption Pool only
  - Principal and yield collateral are never touched
- 

## Is redemption always available?

Yes, but the redemption rate depends on system-wide reserve coverage.

Redemption follows three deterministic tiers based on the Redemption Pool's coverage ratio:

- **High coverage ( $\geq 70\%$ )**

1 cBTC = 0.00001 BTC

- **Medium coverage (35%–70%)**

1 cBTC = 0.000005 BTC

- **Low coverage ( $< 35\%$ )**

Redemption is pro-rata across remaining reserves

The current redemption rate is publicly observable.

---

## What happens if many users redeem at once?

Redemptions are processed on a FIFO basis and follow the applicable coverage tier. There are no liquidation cascades or emergency interventions. The system degrades predictably under stress.

---

## Can the Redemption Pool be drained or misused?

No.

Bitcoin can leave the Redemption Pool only in exchange for provably burned cBTC and only according to protocol rules. The pool cannot be used for yield, governance, or discretionary spending.

---

## What happens if the Redemption Pool becomes underfunded?

If Redemption Pool reserves fall below required solvency thresholds:

- new Minting Channels are halted,
- no new cBTC can be issued,
- redemption continues under the applicable haircut tier.

Solvency can be restored through redemptions, yield forfeiture, or renewed issuance once thresholds are met.

---

## Is there a maximum supply of cBTC?

There is no fixed global supply cap. Supply is constrained by:

- available Bitcoin collateral,
- Redemption Pool solvency,
- and issuance halts when thresholds are breached.

Each Minting Channel is capped at **5 BTC**.

---

## Who controls the protocol?

There is no central controller. Some coordination is required to assemble transactions and track state, but coordinators do not custody funds and cannot override protocol rules. All actions are publicly auditable.

---

## What happens if coordinators disappear?

Issuance may pause and redemption processing may be delayed, but no funds are lost. The system can resume operation once coordination is restored by any party using publicly observable state.

---

## Is cBTC permissionless?

The protocol is designed to become increasingly permissionless over time. Early deployments may rely on coordination services, but custody and economic rules do not depend on trust in those services.

---

## What problem does cBTC solve?

cBTC allows Bitcoin to function as productive capital without sacrificing self-custody, monetary discipline, or solvency. It enables liquidity and yield without fiat pegs, liquidations, or custodial risk.

---

## How does cBTC affect privacy and transaction traceability?

cBTC is designed to **improve transactional privacy relative to on-chain Bitcoin transfers**, particularly when used as working capital.

Key privacy properties include:

- **Reduced on-chain footprint**

cBTC is intended to circulate primarily off-chain using Bitcoin-secured payment channels. This allows transfers without publishing every transaction to the Bitcoin blockchain.

- **Separation from original UTXOs**

Once Bitcoin is deposited into a Minting Channel, subsequent cBTC transfers are no longer directly linked to the original Bitcoin UTXOs. This reduces address reuse and historical traceability for day-to-day payments.

- **No account-based identity layer**

The protocol does not maintain user accounts, identity records, or transaction histories outside of Bitcoin itself. Ownership and transfers are defined solely by cryptographic keys.

- **Public but minimal settlement layer**

On-chain activity is limited to:

- Minting Channel creation and closure
- Settlement and redemption events

These events are publicly visible but occur far less frequently than typical payment flows.

---

## Is cBTC anonymous?

No.

Like Bitcoin, cBTC does not provide absolute anonymity.

- On-chain actions remain publicly visible.
- Off-chain transfers inherit the privacy properties of the underlying payment channel system.
- There is no protocol-level mixing or obfuscation.

However, cBTC **significantly reduces transactional exposure** by minimizing the need for repeated on-chain movements of Bitcoin.

---

## Does redemption affect privacy?

Redemption requires an on-chain interaction and is therefore publicly observable. This is intentional and necessary to preserve auditability and solvency guarantees.

Importantly:

- redemption does not reveal the history of off-chain cBTC transfers,
  - only the final redemption event is visible on-chain.
-

## **Can users improve privacy further?**

Yes.

As with Bitcoin, users may enhance privacy by:

- managing keys carefully,
- avoiding address reuse,
- choosing when to settle or redeem,
- and using off-chain circulation for routine transfers.

The protocol does not restrict or prevent the use of additional privacy-preserving techniques that are compatible with Bitcoin.

---

## **How is cBTC different from wrapped Bitcoin or Bitcoin-backed stablecoins?**

Wrapped Bitcoin and stablecoins rely on custodians, fiat pegs, or discretionary liquidation. cBTC relies exclusively on Bitcoin-enforced rules, prefunded collateral, and deterministic redemption mechanics.

---

## **Is cBTC meant to replace Bitcoin?**

No.

Bitcoin remains the base money and settlement layer. cBTC is a complementary instrument designed for working capital use cases.

---

## **Final clarification**

cBTC is not designed to be everything.

It is a narrow, conservative attempt to allow Bitcoin-native credit to exist without recreating the failures of fiat finance.

Participation is voluntary. Risk is explicit. Rules are transparent.



## Annex III — cBTC Innovations Overview

---

cBTC does not introduce a single new mechanism, but rather a coherent set of design choices that together form a conservative, Bitcoin-native credit layer. This annex summarizes the protocol's primary innovations and explains why they matter.

---

### 1. Bitcoin-Native Credit Without Fiat Pegs

Most Bitcoin-backed instruments derive their stability or utility from fiat references. cBTC rejects this model entirely.

- All values are expressed in Bitcoin terms.
- No fiat price targets exist.
- No price feeds or exchange rates are required.

This makes cBTC resilient to oracle failure and removes dependency on external monetary systems.

---

### 2. Deterministic Issuance via Minting Channels

cBTC introduces **Minting Channels** as a new issuance primitive:

- Issuance occurs only at channel creation.
- Loan-to-value is fixed and known in advance.
- No dynamic leverage, refinancing, or rollover exists.

This replaces discretionary credit issuance with contractual, time-bound capital commitment.

---

### 3. Prefunded, Non-Linear Yield

Unlike lending-based yield systems, cBTC yield is:

- prefunded at channel creation,
- isolated per Minting Channel,
- distributed non-linearly over time,
- forfeitable upon early exit.

This eliminates rehypothecation risk and aligns incentives with long-term participation rather than volume or churn.

---

## 4. Global Redemption Pool with Deterministic Haircuts

cBTC introduces a **global Redemption Pool** governed by explicit coverage thresholds:

- Redemption is always available.
- Payouts follow transparent, tiered haircuts.
- No participant is liquidated or prioritized by discretion.

This replaces liquidation cascades with predictable degradation under stress.

---

## 5. Separation of Principal, Yield, and Redemption Collateral

Collateral roles are strictly separated:

- Principal is never touched.
- Yield is isolated and conditional.
- Redemption reserves are global and exclusive.

This structural separation prevents hidden risk coupling and simplifies auditing.

---

## 6. Time as a First-Class Risk Variable

In cBTC, **time replaces price** as the dominant risk dimension.

- Yield accrues through time commitment.
- Early exit is penalized through yield forfeiture.
- No collateral revaluation occurs.

This design avoids reflexive price dynamics and liquidation spirals.

---

## 7. Dual-Layer Asset Representation

cBTC introduces a layered asset model:

- On-chain representation for settlement and redemption.
- Off-chain representation for working capital circulation.

This allows efficient transfers without sacrificing self-custody or auditability.

---

## **8. No Liquidations, No Margin Calls**

At no point does the protocol:

- seize collateral,
- force position closure,
- or reprice risk dynamically.

All outcomes are determined at channel creation and through time-based rules.

---

## **9. Hard Solvency Enforcement**

cBTC enforces solvency through:

- a minimum global redemption coverage threshold,
- automatic issuance halts,
- supply contraction via redemption and burn.

There is no emergency governance, bailout mechanism, or discretionary override.

---

## **10. Separation of Protocol and Implementation**

The protocol explicitly distinguishes:

- economic invariants (unchanging),
- from coordination and implementation (evolvable).

This allows gradual decentralization without altering core guarantees.

---

## **11. Bitcoin-Enforced Custody**

All custody-critical guarantees rely on Bitcoin itself:

- time locks,
- script conditions,
- cryptographic ownership.

No external ledger, multisig custodian, or trust committee is required.

---

## 12. Conservative by Design

cBTC prioritizes:

- solvency over liquidity,
- predictability over optimization,
- discipline over flexibility.

This makes it suitable for long-term capital use rather than speculative leverage.

---

### Conclusion

cBTC's primary innovation is not technical complexity, but **restraint**. By limiting leverage, eliminating discretion, and embedding time preference into credit issuance, the protocol demonstrates how Bitcoin can support productive capital formation without inheriting the fragility of traditional financial systems.