cBTC Whitepaper:
A Bitcoin-Backed Monetary Protocol

James Tector

jamestector@gmail.com

Abstract

cBTC proposes a Bitcoin-native monetary system that bridges Bitcoin's role as a store of value with its use as a medium of exchange.The protocol enables Liquidity Providers (LPs) to lock BTC as collateral and mint **cBTC**, a Bitcoin-denominated token that floats freely on the market. cBTC is designed for daily transactions, powered by a **self-balancing, non-custodial protocol** that expands Bitcoin's monetary utility without compromising decentralization or self-custody. cBTC is **not a stablecoin — it is Bitcoin made liquid.**

---

1. Introduction

Bitcoin is the most secure and decentralized store of value ever created, but it lacks a *native, capital-efficient monetary layer* capable of enabling yield, liquidity, and programmability without introducing fiat or custodial risk.

Stablecoins provide transactional convenience but rely on banks and off-chain collateral—reintroducing the very trust Bitcoin was designed to remove.

cBTC introduces a **Bitcoin-backed floating-rate asset** that operates entirely within Bitcoin's economic domain.

Collateral, yield, redemption, and governance are all denominated in BTC.

Every mint, redemption, and liquidity cycle reinforces solvency, creating a protocol that strengthens as it grows.

---

2. System Overview & Initial Bootstrapping

cBTC operates through a set of on-chain contracts and participants that together form a **closed Bitcoin economy**—no fiat, no stablecoins, no synthetic assets.

Actors

- **Liquidity Providers (LPs):** Deposit BTC for 1–12 months to enable cBTC minting and earn 15 % annual BTC yield.
- **cBTC Users:** Acquire and use cBTC as a transactional token; freely swap between cBTC and BTC at market rates.
- **Protocol Treasury (Redemption Pool):** Holds BTC reserves for redemptions, funded by 0.2 % swap fees and unvested BTC yield.
- **Governance (LP Collective):** One LP contract = one vote; decides LTV, yield, fees, and reserve redistribution.

Core Contracts

Contract	Function
LP Vault	Locks BTC deposits, tracks vesting schedules, allows unilateral withdrawal after one month.
Yield Pool	Prefunds 0.15 BTC per 1 BTC deposit to pay yield.
Redemption Pool	Holds BTC reserves; collects 0.2 % swap/redemption fees.
Mint Swap Contract	Mints new cBTC against incoming BTC at oracle-derived BTC/cBTC rates.
Governance Registry	Stores LP votes, parameters, and approved updates.

Initial Liquidity Bootstrapping: A Native bootstrapping Cycle
The system bootstraps its own liquidity reserves through a direct Bitcoin-to-cBTC market making process:

1. LP Deposit → Alice locks 1 BTC into the Vault.
2. Minting → Protocol mints 30 000 cBTC (30 % LTV).
3. Market Offering → 30 000 cBTC listed for BTC directly.
4. Exchange → Buyers pay 0.30 BTC (1 cBTC = 0.00001 BTC).
5. Reserve Allocation → 0.15 BTC → Yield Pool; 0.15 BTC → Redemption Pool.

Component	BTC Flow	Purpose
LP Deposit	1.00 BTC	Locked collateral
cBTC Sale	+0.30 BTC	Market proceeds
Yield Pool	+0.15 BTC	Prefunds yield
Redemption Pool	+0.15 BTC	Initial liquidity

Benefits of Bitcoin-Native Bootstrapping:

- **Pure Bitcoin Economy:** No fiat conversion required at any stage
- **Immediate Utility:** Early buyers can immediately use cBTC for transactions or provide liquidity
- **Price Discovery:** The initial exchange rate establishes natural market valuation
- **Transparency:** Automatic liquidity recycling
- **Regulatory Simplicity:** Avoids banking relationships and fiat compliance overhead

This process creates a partially-backed system from inception, with 0.15 BTC in reserves backing 30,000 cBTC. Early cBTC buyers become the foundation of the ecosystem, able to immediately use their cBTC for payments or provide additional liquidity on decentralized exchanges.

---

3. Tokenomics & Monetary Policy

3.1 Floating Price & Oracle

A decentralized oracle reports the time-weighted BTC/cBTC rate (PBTC/cBTCP_{BTC/cBTC}PBTC/cBTC) for minting and redemption.

Only BTC/cBTC markets are used — no fiat feeds.

3.2 Redemption

BTC_out = cBTC_amount × P_BTC/cBTC × (1 – 0.002)

- 0.2 % fee goes to the Redemption Pool.
- Redeemed cBTC is burned, reducing supply and raising coverage.

3.3 Elastic Supply via Mint Swap

When cBTC > intrinsic value, users mint new tokens:

cBTC_minted = BTC_deposited / P_BTC/cBTC

Deposited BTC → Redemption Pool.

When price < intrinsic value, redemptions burn supply.

→ Self-balancing loop.

3.4 Yield Mechanism

Each 1 BTC deposit prefunds 0.15 BTC into the Yield Pool.

Yield vests over 12 months:

Y_t = 0.15 × (t / 12)

Unvested yield from early exit → Redemption Pool.

All yield paid in real BTC.

3.5 Reserve Growth & Coverage Ratio

R_{t+1} = R_t + F_t + U_t

F_t = fees; U_t = unvested yield.

Coverage ratio:

C = (RedemptionPool + YieldPool) / (cBTC_Supply × P_BTC/cBTC)

Activity → Higher coverage → Over-collateralization.

3.6 Summary

- 100 % BTC-denominated collateral and reserves.
- Elastic supply via market forces.
- Prefunded, non-inflationary yield.
- System solvency grows with usage.

cBTC = Bitcoin liquidity in motion.

---

4. Risk & Stability Analysis

Structural Design

cBTC uses a **two-tier system**:

- LPs = Senior creditors (first claim on collateral, Yield)
- cBTC holders = Junior creditors (claim on reserve pool, liquidity)

This hierarchy isolates yield obligations from transactional liquidity risk.

Market Risk:

BTC crash does not impair BTC-denominated solvency.

Mitigations → 30 % LTV, dynamic adjustments, deflationary burns.

Liquidity Risk:

Risk	Mitigation
Bank run	0.2 % fee + redemption throttle
Token scarcity	Mint Swap expands supply
Exchange illiquidity	On-chain AMM fallback

Mitigations:

1. Conservative 30% LTV for initial minting

2. Dynamic LTV adjustment during high volatility (governance-controlled)

3. Deflationary burn mechanism that raises per-token backing during redemptions

Liquidity Risk:

- **Bank run:** Mitigated by 0.2% redemption fee (increasing cost of mass exits) and throttled redemption rates if reserve drawdowns exceed daily thresholds.
- **Token scarcity:** Mitigated by Mint Swap mechanism (elastic supply).
- **Exchange illiquidity:** On-chain Mint/Redemption contracts act as AMM of last resort.

Black Swan Scenario:

In a worst-case scenario of simultaneous BTC price crash and cBTC bank run:

1. Redemption fees increase with volume, slowing reserve depletion
2. As cBTC is burned, coverage ratio for remaining holders increases
3. The system can temporarily increase redemption fees or pause minting via governance to stabilize
4. The prefunded yield pool provides an additional buffer

Operational Risk:

Dual oracles, proof-of-reserve multi-sig, audits, 48 h timelock.

---

5. Economic Model & Projections

Under base parameters:

- 1 BTC LP deposit
- 30% early LP exits
- 30% monthly transaction turnover
- 0.2% swap/redemption fee

Projected Reserve Growth

Timeline	Redemption Pool	Coverage Ratio	Notes
Initial	0.15 BTC	50%	Bootstrapping
Year 1	0.22 BTC	73%	Early equilibrium
Year 3	0.30 BTC	100%	Full coverage
Year 5	0.38 BTC	126%	Over-collateralized

The model demonstrates **endogenous solvency**: activity → fees → higher reserves → greater trust → more LPs → more usage → still higher reserves.

---

6. Governance & Legal Framework

Governance Model

Governance rests entirely with Liquidity Providers.

Voting Rules:

- One LP contract = one vote
- Any LP can propose one change every 30 days
- Quorum: 60% of active LPs; Approval: ⅔ majority
- Execution delay: 48-hour timelock

Adjustable Parameters:

- LTV ratio for new mints
- LP annual yield rate
- Redemption fee (0.2% baseline)
- Mint spread for new issuance
- Reserve redistribution policies

Reserve Redistribution:

When Redemption Pool coverage (C) exceeds 100%, LPs can vote to:

1. Redistribute surplus BTC to LPs pro-rata
2. Allocate part to a protocol treasury fund
3. Temporarily raise LTV to expand cBTC supply

Legal Standing:

- LPs **retain full ownership** of their BTC; smart contracts only enforce time-locks
- After one month, LPs can unilaterally withdraw BTC and accrued yield directly from contract
- cBTC is a **BTC-denominated digital commodity**, not a fiat-pegged stablecoin
- BTC-denominated yield = service reward, not interest
- No governance or utility token = no securities risk
- Variable BTC redemption value = avoids e-money classification

---

7. Implementation Architecture

Core Modules:

- **LP Vault:** Receives BTC, enforces 1-month minimum lock, releases vested yield
- **Yield Pool:** Prefunds and distributes yield; unvested yield auto-transfers to Redemption Pool
- **Redemption Pool:** Executes redemptions (0.2% fee), burns cBTC, collects unvested yield and mint inflows
- **Mint Swap Contract:** Mints new cBTC against BTC inflows
- **Governance Registry:** Stores parameters and voting states

BTC Custody & Security

- Preferably through a Bitcoin Layer-2 or multi-sig bridge with on-chain proof-of-reserves
- LPs maintain private ownership; only time-lock enforced
- Public dashboard displays all BTC addresses and total balances
- 3-of-5 multi-sig for bridge operations
- Formal contract audits and 48-hour governance timelock

Roadmap

Phase	Objective	Duration
1. Testnet	Prototype contracts, oracles, and dashboard	3 months
2. Mainnet Beta	Live bridge, limited LP participation	6 months
3. Full Launch	Governance activation, audits complete	12 months
4. Expansion	BTC L2 integration, corporate APIs	Year 2

---

8. Liquidity Incentive & Anti-Looping Mechanism

8.1 Purpose

Prevent repeated short-term withdrawals and redeposits that could compound yield faster than intended, while keeping full non-custodial flexibility.

8.2 Mechanism

Each LP deposit is treated as an **independent position** with its own vesting curve. Yield remains **prefunded (0.15 BTC per 1 BTC)** but **vests non-linearly**—slower at first, faster toward maturity.

$Y(t) = Ymax \times (t / T)^p$

where T = 12 months, Ymax = 0.15 BTC, p > 1 (typically 1.5–2.0).

8.3 Example Vesting

Month	Linear (p = 1)	p = 1.5	p = 2.0
3	0.0375	0.0188	0.0094
6	0.0750	0.0530	0.0375
9	0.1125	0.0974	0.0844
12	0.1500	0.1500	0.1500

Early withdrawals earn far less than the linear schedule, removing any advantage from cycling.

8.4 Withdrawal & Forfeiture

On withdrawal at time t:

- LP receives vested yield Y(t).
- Unvested portion Ymax – Y(t) returns to the Redemption Pool.
- Any new deposit starts a fresh curve (t = 0).

Partial withdrawals are handled pro-rata without resetting the age of remaining funds.

8.5 Optional Smooth Floor

Governance may define a small early-period floor (10–20 % of linear) for friendlier UX:

$Y(t) = Ymax \times \max\{ \lambda (t/T),\ (t/T)^p \},\ \lambda \in [0.1, 0.2]$

8.6 Governance Control

- Parameter p and T set by governance; changes apply only to new positions.
- Ensures predictability and fair treatment across epochs.

8.7 Rationale

- No identity tracking needed; each new deposit always starts from slow yield.
- Encourages continuous liquidity and long-term LP commitment.
- All unvested yield recycles into the Redemption Pool, strengthening reserves.

cBTC discourages yield-looping through back-loaded non-linear vesting. Short cycles underperform holding; all unvested yield reinforces system stability.

---

9. Competitive Landscape

- Unlike wrapped Bitcoin (WBTC, tBTC), cBTC is non-custodial and capital-efficient.
- Unlike synthetic Bitcoin (sBTC), cBTC is directly backed by Bitcoin collateral.

- Unlike algorithmic stablecoins (UST), cBTC maintains exogenous Bitcoin reserves.
- Our closest analogue is Money on Chain, but with a simpler single-token model
- Unlike other Bitcoin-backed assets that often rely on fiat gateways, cBTC operates in a pure Bitcoin economic environment from day one.

Protocol	Custody	Collateral	Peg	Yield	Governance
WBTC	Custodial	1:1 BTC	USD	None	Centralized
tBTC	Federated	1:1 BTC	USD	None	DAO
sBTC	Synthetic	Algorithmic	USD	None	DAO
cBTC	**Non-custodial**	≤ 30 % BTC	**Floating BTC rate**	**15 % BTC yield**	**LP Voting**

Advantages: Pure BTC economy, floating rate, prefunded yield, self-balancing reserves.

---

10. Conclusion & Future Outlook

cBTC represents a fundamental advancement in Bitcoin-native finance—a **self-funding monetary layer** that combines the stability of collateral with the efficiency of market-based price discovery.

Every mint, redemption, and LP action reinforces—not weakens—the system. Through conservative LTV ratios, prefunded yields, and automatic reserve recapitalization, cBTC creates an endogenous stability mechanism that trends toward over-collateralization.

Vision

cBTC will become:

- The preferred **medium of exchange** for companies holding Bitcoin treasuries
- The first **non-fiat liquidity standard** for decentralized commerce
- cBTC establishes a complete **Bitcoin-native financial loop**—from collateralization to transaction to redemption—without ever requiring fiat conversion.
- A **bridge between Bitcoin's value storage and daily use**
- The **unit of account** for Bitcoin-native finance

Global Monetary Standard

As Bitcoin establishes itself as the global reserve asset, cBTC is positioned to become the natural unit of account for Bitcoin-denominated commerce. While Bitcoin serves as the bedrock store of value, cBTC enables the daily transactions, smart contracts, and financial applications that require a more fluid, stable, transaction-optimized representation of Bitcoin's value.

Just as the US dollar became the global unit of account for trade in the Bretton Woods system, cBTC can become the standard unit of account for the Bitcoin monetary network—the native measurement for prices, salaries, and contracts in a Bitcoin-centric economy.

cBTC is not another stablecoin—it is Bitcoin's native monetary expansion and the foundation for a new global financial standard.

cBTC is Bitcoin made liquid.

Annex I — cBTC FAQ

1. What does cBTC offer that Bitcoin itself does not?

Bitcoin is the ultimate store of value — but it is passive capital.

It cannot generate yield, adjust to liquidity demand, or plug directly into programmable finance.

cBTC makes Bitcoin dynamic:

- LPs earn **15% BTC yield** by locking BTC.
- The same BTC supports cBTC liquidity for payments and applications.
- Supply expands or contracts automatically with real market demand.

Bitcoin stores value — cBTC moves it.

---

2. How is cBTC different from stablecoins?

Stablecoins replicate **fiat currency** on blockchains. They depend on banks, off-chain collateral, and a USD peg.

cBTC has no fiat component:

- Backed only by Bitcoin.
- Floating BTC/cBTC market price — no dollar peg.
- All collateral, yield, and governance denominated in BTC.
- No custodians, no banks, no fiat exposure.

Stablecoins mirror the dollar; cBTC amplifies Bitcoin.

---

3. What happens if Bitcoin's market price drops?

Even if BTC's external fiat price falls, **cBTC's solvency remains unchanged in BTC terms.**

All assets and liabilities exist inside the same unit — Bitcoin.

Stabilizing factors:

- Conservative **30% LTV** ratio for minting.
- **Prefunded BTC yield pool** ensures liquidity.
- Early LP exits add unvested BTC to reserves.
- **Redemptions burn cBTC**, increasing per-token collateralization.

In a downturn, cBTC automatically deleverages — not collapses.

---

4. Who governs the cBTC protocol?

Governance rests solely with Liquidity Providers.

Each LP contract carries **one vote**, independent of BTC size.

Key rules:

- Quorum: 60% of LPs; Approval: ⅔ majority.
- 48-hour timelock before execution.
- LPs can modify collateral ratios, yields, fees, and redistribution policies.

Governed by Bitcoin holders, for Bitcoin holders.

---

5. How is cBTC created and redeemed?

Minting (BTC → cBTC):

- LPs deposit BTC → protocol mints new cBTC at **30% LTV**.
- Users can also mint by sending BTC to the **Mint Swap Contract** when demand is high.
- Deposited BTC strengthens the **Redemption Pool**.

Redemption (cBTC → BTC):

BTCout=cBTC×PBTC/cBTC×(1−0.002) BTC_{out} = cBTC × P_{BTC/cBTC} × (1 - 0.002)BTCout=cBTC×PBTC/cBTC×(1−0.002)

- 0.2% fee retained in the Redemption Pool.
- Redeemed cBTC is burned, tightening supply.

Minting expands liquidity; redemptions contract it.

---

6. How is cBTC different from other Bitcoin-backed assets?

Asset	Custody	Collateral	Pricing	Yield	Governance
WBTC	Centralized	1:1 BTC	USD peg	None	Custodial
tBTC	Federated	1:1 BTC	USD peg	None	Token DAO
cBTC	Non-custodial	≤30% BTC	Floating BTC rate	**15% BTC yield**	**LP-only voting**

Key distinction:
cBTC never leaves the Bitcoin economy — it's Bitcoin liquidity expressed in tokenized form.

---

7. What prevents cBTC from becoming another "algorithmic stablecoin"?

Algorithmic stablecoins failed because they used **self-referential collateral** and fiat pegs. cBTC uses **exogenous Bitcoin collateral** and market-based pricing.

Safeguards:

- Backed 100% by real BTC deposits.
- No synthetic or dual-token peg mechanisms.
- Yield and reserves fully prefunded in BTC.
- Elastic supply adjusts naturally with market behavior.

No algorithmic peg — just Bitcoin backing Bitcoin.

---

8. What is the long-term vision for cBTC?

To serve as the **Bitcoin-denominated liquidity layer** for global commerce.

In this model:

- Bitcoin = Reserve asset (store of value).
- cBTC = Circulating medium of exchange (working capital).

As adoption grows, cBTC can become the **unit of account** for Bitcoin-based trade, contracts, and payroll.

If Bitcoin is the vault, cBTC is the bloodstream.

---

9. How is the 15% BTC yield sustainable?

Each LP deposit of 1 BTC triggers a market sale of 30% LTV in cBTC, which returns **0.30 BTC** to the protocol.

That BTC is split:

- **0.15 BTC → Yield Pool** (to pay LP yield)
- **0.15 BTC → Redemption Pool** (collateral reserves)

No new tokens are created; yield is paid from Bitcoin liquidity already within the system. Early LP withdrawals recycle unvested yield back into the reserve.

Yield paid in Bitcoin, from Bitcoin, using Bitcoin liquidity.

---

10. What risks do Liquidity Providers face?

1. **Lock-up period:** Minimum 1-month term.
2. **Vesting:** Yield accrues over 12 months; early exit forfeits part of it.
3. **Smart-contract risk:** Contracts are audited but not risk-free.
4. **Governance:** LPs collectively manage parameters; changes apply globally.

Mitigations:

- LPs can unilaterally withdraw BTC after one month.
- Conservative 30% LTV ensures reserve protection.
- All assets remain Bitcoin — no fiat or counterparty risk.

LPs lend to the network, not to an institution — and keep control of their BTC.

---

11. Can cBTC be integrated into DeFi and exchanges?

Yes. cBTC is designed for **BTC-based interoperability**.

Integration avenues:

- Deployed as ERC-20-compatible token on Bitcoin-connected smart-contract layers.
- Traded in **BTC/cBTC pairs** on exchanges and DEXs.
- Used as collateral or settlement currency in BTC-denominated DeFi.
- Integrated into business treasuries and payment processors using Bitcoin rails.

Each integration increases fee volume, enlarging the Redemption Pool and strengthening coverage.

cBTC is the Bitcoin liquidity bridge between self-custody and programmability.