Cipoal

Elevado Labs
elevado.xyz

Abstract

We propose Cipoal, a Bitcoin Treasury Strategy Protocol (BTSP). Built on Ethereum, the Cipoal protocol issues CIP, a Bitcoin-backed and BTC-denominated reserve currency designed to deterministically preserve or increase the NAV per unit. As a Bitcoin-based central bank, the protocol consolidates all core functions of a financial system – minting, redemption, reserve, accountability, and valuation – into a single autonomous, monolithic smart contract.

1 Introduction

The concept of a central bank – an entity that issues currency, manages reserves, and preserves monetary integrity – is undergoing redefinition in the era of on-chain, programmable finance.

As Bitcoin consolidates its position as the world's neutral reserve asset, it becomes increasingly coherent to conceptualize the emergence of Bitcoin-backed assets that, in addition to being collateralized by Bitcoin and BTC-denominated, are capable of algorithmically compounding their underlying value, ensuring it never declines.

Cipoal is envisioned as a fully on-chain Bitcoin-based central bank – a protocol that (1) holds a bitcoin reserve; (2) issues an Bitcoin-backed asset, and (3) compounds Bitcoin yield to participants.

Built on Ethereum, Cipoal is a Bitcoin Treasury Strategy Protocol (BTSP) that issues CIP, a Bitcoin-backed and BTC-denominated asset whose NAV can only increase over time, not falling below.

By encoding sound monetary principles within deterministic smart contract logic, Cipoal enables participants to gain exposure to Bitcoin value while continuously accumulating more Bitcoin – effectively turning long-term holding into a self-reinforcing treasury strategy.

2 Bitcoin Treasury Strategy Protocol (BTSP)

The Bitcoin Treasury Strategy Protocol (BTSP) is a self-contained system that manages a Bitcoin reserve and issues a Bitcoin-backed, BTC-denominated asset collateralized by that reserve. The protocol is designed so that the asset's underlying value compounds automatically, proportional to protocol activity, all according to predefined, immutable algorithmic rules.

2.1 Functionality

Users deposit Wrapped Bitcoin (WBTC) into a smart contract to mint CIP, based on its current value, which is determined by the total Bitcoin held in the protocol reserve divided by the total number of CIP in circulation, initially set at a 1:0.1 ratio between CIP and WBTC (i.e., 1 CIP equals 0.1 WBTC). To redeem WBTC, users deposit CIP into the contract, which is then burned.

Both minting and redeeming are subject to a 1% entry fee and a 3% exit fee. These fees are retained within the Bitcoin reserve, compounding back into the system and increasing the NAV per CIP for the remaining supply. Fundamentally, every transaction – whether a deposit or redemption – strengthens the protocol's balance sheet and, subsequently, increases the BTC-denominated value per CIP.

3 Protocol Design

Cipoal's protocol design revolves around a reserve of Wrapped Bitcoin (WBTC) and an ERC-20 token, CIP.

Let C denote the total collateral (in WBTC) held by the contract, and S denote the total supply of CIP in circulation.

The net asset value (NAV) per CIP is then defined as:

$$\mathrm{NAV} = \frac{C}{S}$$

Where NAV is expressed in BTC units (through WBTC). The system enforces $\frac{d}{dt}\mathrm{NAV} \geq 0$, guaranteeing that the value of each CIP in BTC terms never decreases over time.

All user interactions – deposits and redemptions – modify C and S in a manner that always increases NAV.

3.1 Fees

Cipoal's internal fee system functions as a 'closed monetary circuit'.

Deposit and redemption fees never exit the system; they remain as retained earnings within the protocol. Over time, this creates an endogenous growth mechanism.

Let F_t denote cumulative fees retained until time t:

$$\mathrm{NAV}_{t+1} = \frac{C_0 + F_t}{S_t}$$

Thus, system activity – both inflows and outflows – increases NAV and subsequently the value per CIP.

Unlike yield from lending or staking, Cipoal's yield is mechanical and riskless, derived from arithmetic redistribution, not counterparty exposure.

4 Asset Design

CIP, the native asset of Cipoal, represents a redeemable claim on the protocol Bitcoin reserve, resembling a non-expiring, non-diluting deposit certificate.

4.1 BTC-Denominated

CIP's denomination in BTC establishes its numéraire neutrality, measuring and storing value in the same unit as its backing.

Denoting value in BTC removes exposure to fiat volatility and establishes a pure Bitcoin monetary system.

Formally, all system variables – C, S, and NAV – are expressed in BTC terms. Fiat valuation becomes an external observer's perspective, not a protocol input.

4.2 Non-Decreasing NAV

The central invariant of Cipoal is non-decreasing NAV.

Because all protocol fees are retained, $\mathrm{NAV}_{t+1} \geq \mathrm{NAV}_t$. The system therefore defines a monotonic NAV trajectory, where each user action contributes to the growth of backing per unit.

Mathematically:

$$\frac{d}{dt}\text{NAV} = \frac{d}{dt}\left(\frac{C}{S}\right) = \frac{S\frac{dC}{dt} - C\frac{dS}{dt}}{S^2} \geq 0$$

This dynamic ensures that even in periods of high redemption, the protocol self-strengthens. Each exit increases the collateral share per remaining CIP, forming a positive feedback loop.

4.2.1 1:>0.1

The Cipoal protocol begins at 1:0.1 – one CIP equals 1/10 WBTC.

However, following the first deposit, the system shifts to 1:>0.1: one CIP becomes backed by more than 1/10 WBTC proportionally.

In equilibrium, the protocol converges toward a perpetual premium over its initial 1:0.1 parity. Every action – minting or redeeming – perpetually reinforces this structural surplus.

4.3 Yield-Bearing

Yield in Cipoal arises from internal compounding of retained fees, not external yield generation.

For a protocol participant, effective yield y_t can be expressed as:

$$y_t = \frac{\text{NAV}_{t+1} - \text{NAV}_t}{\text{NAV}_t}$$

This yield is denominated in BTC terms and represents a deterministic accretion of collateral per share, insulated from market or credit risk. Unlike lending yields, Cipoal's yield does not rely on counterparties – it is a mechanical outcome of user participation and protocol activity.

5 Flywheel

Cipoal's flywheel mechanism represents a self-reinforcing economic cycle.

Fees collected from activity are retained, increasing NAV. Higher NAV theoretically improves the asset's desirability, attracting new deposits, which further raise fees, perpetuating the cycle.

5.1 Mechanism Design

The flywheel mechanism can be modeled as:

$$\mathrm{NAV}_{t+1} = \mathrm{NAV}_t \left(1 + \frac{f_d M_t + f_r R_t}{C_t}\right)$$

Where M_t and R_t represent mint and redemption volumes at time t.

This expresses the reflexivity: system usage → fee accrual → higher NAV → more usage.

5.2 Compounding

In continuous time, the compounding effect of Cipoal follows:

$$\mathrm{NAV}_t = \mathrm{NAV}_0 e^{\lambda t}$$

Where λ is the effective compounding rate determined by aggregate user activity. The longer the system operates with consistent throughput, the greater the exponential divergence from the 1:0.1 initial ratio. This compound dynamic mirrors the behavior of a central bank accumulating reserves via transaction fees rather than taxation or debt issuance.

6 Proof of Reserve (PoR)

Proof of Reserve (PoR) establishes the foundation of Cipoal's transparency and verifiability.

PoR represents the total Reserve Asset Value (RAV) – the complete BTC-denominated balance held within the protocol's custody. RAV is fully observable on-chain, allowing anyone to verify the total reserve at any time.

This continuous, cryptographically enforced verifiability ensures that every unit of issued CIP is backed by verifiable Bitcoin collateral, eliminating reliance on third-party attestations.

Formally:

$$\mathrm{PoR} = \mathrm{RAV} = \text{Total Bitcoin Collateral Held by the Protocol}$$

Because all system variables are public, Proof of Reserve (PoR) is a direct reflection of the protocol's total balance sheet – the digital analogue of a central bank's reserve ledger.

6.1 Insolvency-Proof

Cipoal is structurally insolvency-proof.

No collateral ever leaves the protocol except during CIP redemption operations, and redemptions occur strictly within the limits of available reserves. Each CIP is redeemable at its verifiable Bitcoin-denominated value, i.e., $\mathrm{NAV} = \frac{C}{S}$, preventing any form of undercollateralization.

6.2 Proof of Value (PoV)

Proof of Value (PoV) extends the PoR framework to the level of each CIP unit, linking the protocol's total reserves (RAV) to the per-unit Net Asset Value (NAV).

While PoR validates the existence of the Bitcoin reserve, PoV validates their distributional integrity – ensuring that each unit in circulation maintains a verifiable, non-decreasing claim on the reserve base.

Formally:

$$\mathrm{PoV} = \frac{\mathrm{RAV}}{\text{Total CIP Supply}} = \mathrm{NAV}$$

In this structure, while PoR confirms solvency, PoV confirms value.

7 Risks and Limitations

Cipoal's main dependency is the custodial integrity of WBTC. WBTC is issued by a consortium led by BitGo, holding real BTC in cold storage.

With a multi-billion-dollar market capitalization and years of operational stability, it represents one of the most battle-tested Bitcoin wrappers on Ethereum. Nonetheless, WBTC introduces a mild custodial vector.

8 Conclusion

This initial draft of the Cipoal whitepaper is meant to establish a conceptual understanding of the high-level design and architecture of the proposed protocol. It should not be considered complete or final. The version 1.0 of this paper will be published for public review and community input on https://github.com/elevadoxyz.

A BTC-denominated pricing framework

Let $P_{BTC}(t)$ represent the BTC/USD exchange rate at time t, $C(t)$ the total collateral in WBTC, and $S(t)$ the CIP supply.

The USD-equivalent NAV is:

$$\text{NAV}USD(t) = PBTC(t) \cdot \frac{C(t)}{S(t)}$$

However, within Cipoal, pricing occurs natively in BTC terms:

$$\text{NAV}_{BTC}(t) = \frac{C(t)}{S(t)}$$

This choice of numéraire isolates the asset from fiat volatility, enabling purely bitcoin-based accounting. Traditional portfolio theory assumes USD as the base currency; Cipoal redefines this by using BTC as the unit of account, thereby reconstructing all risk and yield metrics around bitcoin's monetary gravity.

B NAV monotonicity

Let $C(t)$ be total collateral and $S(t)$ total supply.

For every new mint, C increases by $(1 - f_d)D$ while S increases by $(1 - f_d)D/\text{NAV}_t$.

For every redemption, C decreases by $(1 - f_r)R\text{NAV}_t$ and S decreases by R.

Taking the time derivative:

$$\frac{d}{dt}\left(\frac{C}{S}\right) = \frac{S\frac{dC}{dt} - C\frac{dS}{dt}}{S^2}$$

Given both fee parameters $f_d, f_r > 0$, every mint or redemption adds unclaimed residual collateral to C while adjusting S proportionally less. Hence, the numerator is always nonnegative, ensuring $\frac{d}{dt}(\text{NAV}) \geq 0$.

This constitutes a formal proof that NAV can never decrease, regardless of system activity.

C Continuous-time compounding model

Defining $\lambda(t)$ as the instantaneous compounding rate from retained fees:

$$\frac{d(\text{NAV})}{dt} = \lambda(t)\text{NAV}(t)$$

Integration yields:

$$\text{NAV}(t) = \text{NAV}(0)e^{\int_0^t \lambda(\tau)d\tau}$$

Where $\lambda(t) = \frac{f_d\dot{M}(t) + f_r\dot{R}(t)}{C(t)}$.

This describes NAV growth as a function of transactional velocity. The protocol thus resembles a central bank accumulating reserves via transactional friction, compounding value in proportion to activity throughput.

D Fee internalization as monetary seigniorage

In fiat systems, seigniorage arises from monetary issuance. In Cipoal, it arises from fee retention.

The effective ‘seigniorage rate’ per time unit is:

$$\sigma(t) = \frac{f_d M_t + f_r R_t}{S_t}$$

Unlike inflationary seigniorage, this process is anti-inflationary: it increases per-unit collateral rather than diluting supply.

Hence, Cipoal monetizes system participation while remaining deflationary in collateral-per-token terms.

F Immunity to impermanent loss

CIP holders maintain constant collateral exposure.

Since C and S are scalar values, not price-paired liquidity, no relative price exposure exists.

Hence, CIP avoids impermanent loss entirely – unlike AMM LP tokens, for example.

G Anti-dilution mechanics

Each new mint and redemption reinforces per-token collateralization.

The incremental NAV change $\Delta\mathrm{NAV}$ satisfies:

$$\Delta\mathrm{NAV} = \frac{f_d D + f_r R\mathrm{NAV}}{S}$$

Since $f_d, f_r > 0$, $\Delta\mathrm{NAV} > 0$ for any positive system activity.

Cipoal therefore institutionalizes anti-dilution – growth that proportionally benefits existing holders.

H Asymptotic behavior and maturity

As time approaches infinity and activity stabilizes, the system converges to:

$$\lim_{t\to\infty} \mathrm{NAV}(t) = \mathrm{NAV}_0 e^{\lambda^* t}$$

Where λ^* is the steady-state compounding rate.

This creates a predictable NAV trajectory akin to perpetual discount instruments – deterministic and bounded by protocol velocity.

I Dynamic equilibrium and protocol velocity

Let the system's *velocity of participation* be denoted by $v(t) = \frac{M_t + R_t}{S_t}$, where M_t and R_t represent total mint and redemption flows. The growth of NAV can be expressed as:

$$\frac{d(\text{NAV})}{dt} = \text{NAV} \cdot (f_d + f_r) \cdot v(t)$$

At equilibrium, $v(t)$ stabilizes around a long-term mean v^*, producing steady compounding. If $v(t) > v^*$, NAV grows superlinearly; if $v(t) < v^*$, growth remains positive but slows.

This dynamic establishes Cipoal as an activity-sensitive monetary system, where liquidity cycles directly influence reserve expansion – analogous to how GDP velocity affects monetary base expansion in macroeconomics.

J Marginal NAV gain function

Let $G(M, R)$ denote the marginal NAV gain function:

$$G(M, R) = \frac{f_d M + f_r R \text{NAV}}{S}$$

Differentiating with respect to user activity yields:

$$\frac{\partial G}{\partial M} = \frac{f_d}{S}, \quad \frac{\partial G}{\partial R} = \frac{f_r \text{NAV}}{S}$$

This implies that redemptions contribute more to NAV accretion per unit of activity than deposits, since $f_r > f_d$. Consequently, system health is reinforced even under outflows – a countercyclical characteristic unique to Cipoal's design.

K Protocol as closed-loop monetary system

Cipoal functions as a closed-loop monetary economy.

The circuit is defined by four flows: deposit inflow, redemption outflow, fee retention, and NAV adjustment.

Since all value remains on-chain, no leakage occurs; every economic action feeds back into the system's base.

This creates an entropy-negative monetary environment: rather than decaying through inflation or counterparty risk, the system continuously condenses value into fewer, stronger claims – mathematically modeled as:

$$\frac{dE}{dt} = -\eta(f_d M + f_r R)$$

Where E denotes system entropy and $\eta > 0$ a proportional efficiency constant.

L On the predictability of NAV growth

In this appendix, we explore the theoretical predictability of Net Asset Value (NAV) appreciation within the Cipoal protocol, given that its underlying growth mechanism is entirely endogenous – driven by the accumulation of protocol fees that remain within the reserve.

The analysis considers the deterministic relationship between transactional volume, fees, and the resulting incremental increase in Reserve Asset Value (RAV), which in turn determines NAV.

Let:

- R_t: Reserve Asset Value (RAV) at time t, denominated in BTC
- S_t: Total CIP supply at time t
- V_t: Total transaction volume (sum of deposits and redemptions) over period t
- f_d: Deposit fee rate (1%)
- f_r: Redemption fee rate (3%)
- f_{eff}: Effective composite fee rate (average 4%)
- N_t: Net Asset Value (NAV) at time t

The system's NAV at any point in time is defined as:

$$N_t = \frac{R_t}{S_t}$$

Since both R_t and S_t are observable and deterministic on-chain, the NAV is a function of protocol activity rather than speculative market dynamics.

L.1 Reserve growth through fee compounding

Each transaction within the protocol contributes to the reserve via the compounding of fees. Assuming no external yield and a stable total supply (for analytical simplicity), the reserve evolves as:

$$R_{t+1} = R_t + f_{eff} \times V_t$$

This implies that reserve growth is directly proportional to aggregate protocol volume and fee rate. The change in NAV, therefore, can be modeled as:

$$\Delta N_t = \frac{R_{t+1}}{S_t} - \frac{R_t}{S_t} = \frac{f_{eff} \times V_t}{S_t}$$

This relationship demonstrates that the NAV increment is linearly dependent on transaction volume per unit of supply.

L.2 Predictability over a time horizon

Over a time horizon $[0, T]$, if we assume an average transactional volume $\bar{V}$ per unit time and constant supply S, NAV evolution can be expressed as:

$$N_T = N_0 + \frac{f_{eff}}{S} \int_0^T V_t, dt$$

If transactional volume exhibits stable behavior (as expected in mature liquidity environments), the integral term can be approximated as $\bar{V} \times T$, leading to:

$$N_T \approx N_0 + \frac{f_{eff} \times \bar{V} \times T}{S}$$

This provides predictability of NAV growth, allowing participants to estimate the compounding yield of their Bitcoin-denominated holdings over any time window, based on projected protocol activity.