Cadena Bitcoin — Lender Security & Operations Memo

For balance-sheet providers evaluating institutional Bitcoin-collateralized credit Issued by Cadena Bitcoin S.A. de C.V. · May 17, 2026

Executive summary

In the current rate environment, **on-chain non-custodial Bitcoin credit is the only structure that delivers institutional lenders double-digit USD-denominated yields without the failure modes of the 2022 lending collapse.** This memo addresses the security and operational concerns balance-sheet providers raise when sizing positions in this asset class: collateral safety, oracle architecture, settlement mechanics, failure-mode coverage, and gap risk.

The structural answer at a glance:

Concern	Cadena's structural answer
Where does the lender's principal sit?	On-chain Discreet Log Contract collateral pool. Cadena holds no key at any point.
How is liquidation handled?	**There is no in-term liquidation.** Settlement is a single event at maturity via pre-signed Contract Execution Transaction (CET).
What if the oracle fails?	Pre-signed CETs cover every BTC/USD attestation the oracle could publish. If the oracle fails to publish, the refund timelock path returns Bitcoin to both parties.
What if Cadena disappears?	The contract is enforced by Bitcoin script, not by Cadena. The pre-signed CETs broadcast automatically; Cadena's operational continuity is not required for settlement.
What is the lender's gap risk?	The contract pool covers the lender's full USD target down to a 50% BTC drop between funding and maturity. Below that, the lender

Concern	Cadena's structural answer
	absorbs the shortfall — hedgeable separately with a put position struck near the 50% LTV mark.
How is collateral protected from rehypothecation?	Each contract sits in a unique on-chain UTXO. No commingling, no pooling, no reuse.

Every claim in this memo is verifiable on-chain or in open-source code. A Cadena contract settled on Bitcoin's mainnet on **May 9, 2026**, executing exactly per the pre-signed structure: mempool.space/tx/95bf1377…9e5aab7d.

---

1. Collateral security architecture

1.1 Where the lender's Bitcoin actually sits

When an institutional lender funds a Cadena contract, the Bitcoin is committed to a Discreet Log Contract (DLC) on Bitcoin's base layer. **Both the lender's principal and the borrower's collateral are committed to the same on-chain DLC pool in a single funding transaction.**

Cadena, in its role as Structuring Agent and matching counterparty:

- Does not hold the lender's Bitcoin at any point
- Does not hold the borrower's collateral at any point
- Does not hold any key required for settlement
- Does not have any administrative control over the DLC pool during the term

The DLC pool is enforced by Bitcoin script. The keys are held by the lender and borrower respectively, with all settlement outcomes pre-signed at funding.

1.2 The pre-signed Contract Execution Transactions (CETs)

Before any Bitcoin moves to fund the DLC, both parties sign every possible Contract Execution Transaction — one for every BTC/USD price the oracle could attest to at maturity. If the oracle has 1,000 possible outcomes in its range, then 1,000 pre-signed CETs exist before the funding transaction is broadcast.

This is the structural guarantee: **the contract's lifecycle is mathematically determined before it begins.** Neither party can refuse to settle. Neither party can alter the outcome. The oracle does not authorize — it selects which of the pre-signed CETs broadcasts.

1.3 No commingling, no rehypothecation, no fractional reserves

Each Cadena contract is an independent on-chain UTXO. The lender's Bitcoin is never pooled with other lenders' Bitcoin. It is never lent to a third party. It is never used as collateral for any other obligation.

Compare to CeFi lenders (BlockFi, Celsius, Voyager) where customer Bitcoin was commingled in operational accounts and used to fund the platform's own positions — the structural cause of the 2022 collapses. **Cadena's architecture makes that failure mode impossible** because the Bitcoin never leaves a script-enforced contract.

1.4 Open-source verification

The Cadena Signer App is open-source and available for code review:

github.com/CadenaWizard/cryptlib

Risk teams can read the code, reproduce builds, audit key generation, and verify that the signing flow does what we describe. No claim in this memo depends on trust in Cadena's word.

---

2. Oracle architecture & redundancy

2.1 The DLCP Oracle

Cadena contracts use the **DLCP Oracle** for BTC/USD price attestation at maturity. The DLCP Oracle is independent of Cadena (separate operating entity, separate key infrastructure) and has been operating production-grade attestations across multiple DLC-based platforms.

Key properties:

- **Cryptographic pre-commitment.** The oracle publishes its public key at contract funding. Any future attestation is verifiable against that pre-committed key — the oracle cannot retroactively manipulate the published price without the manipulation being detectable on-chain.
- **Multiple aggregated feeds.** The oracle aggregates BTC/USD prices from multiple independent exchanges. Methodology is publicly documented. This protects against any single-exchange manipulation.

- **Single-attestation event.** The oracle publishes a single, signed attestation at the contract's maturity timestamp. There is no settlement-period flexibility — the attestation is a single discrete event.

2.2 What happens if the oracle fails to publish

This is the operational question risk officers ask first. The structural answer: **a refund timelock path returns Bitcoin to both parties if the oracle fails to publish at the contract maturity.**

Mechanically:

- Each Cadena contract is funded with both the maturity-settlement CETs **and** a refund transaction with a timelock
- The refund timelock activates if the oracle has not published its attestation within a defined window after maturity
- The refund transaction returns the lender's principal and the borrower's collateral to their respective parties — no settlement claim attaches if the oracle is silent

This is a script-enforced fallback. It does not require Cadena's cooperation; the borrower or lender can broadcast the refund transaction unilaterally once the timelock activates.

2.3 Oracle redundancy roadmap

For institutional-scale contracts, Cadena's roadmap includes a multi-oracle attestation requirement — settlement is contingent on attestations from 2-of-3 or 3-of-5 independent oracles, with the median or aggregated value selected. This further reduces single-oracle attack surface for larger contract sizes.

Today's product uses single-oracle DLCP attestation with the refund timelock fallback. Multi-oracle support is on the 2026 roadmap; we can prioritize for institutional anchor contracts.

---

3. Settlement mechanics — what actually happens at maturity

3.1 The single-event model

There are no margin calls in a Cadena contract. There are no in-term liquidations. There is no settlement-period grace window or partial liquidation logic.

Settlement is a single event at the contract's maturity timestamp.

1. The DLCP Oracle attests to BTC/USD at the settlement timestamp.

2. The pre-signed CET corresponding to that attested price broadcasts on Bitcoin's mainnet.
3. The lender's USD-denominated target is paid in Bitcoin at the maturity price.
4. The borrower receives the residual back to self-custody.

This entire process executes automatically once the oracle attests. Cadena's operational continuity is not required.

3.2 What this means for the lender's risk profile

For a balance-sheet provider, the structural implications are:

- **No path risk during the term.** The lender's outcome at maturity depends only on the BTC/USD price at maturity — not on whether BTC swung wildly during the term, whether the borrower's behavior changed, or whether Cadena did anything during the term.
- **No need for monitoring infrastructure.** The lender does not need to monitor margin levels, trigger margin calls, or manage collateral top-ups. The contract is locked.
- **Predictable settlement timing.** The lender knows the exact date of settlement and the exact USD target. The only variable is the BTC price at maturity, which determines how many sats the dollar target translates to.

3.3 What happens if the borrower's collateral is insufficient

The contract pool is sized so the lender's full USD target is paid down to a 50% BTC drop between funding and maturity. If BTC drops more than 50%, the pool is fully consumed paying the lender's dollar target — the borrower receives zero residual. **The lender's target is met as long as the pool covers it.**

If BTC drops more than 100% of the LTV cushion (i.e., below ~$40K from an $80K funding spot), the pool is no longer sufficient to cover the full target. This is the gap-risk regime, covered in Section 5.

---

4. Failure mode coverage

Risk teams should ask: *"For every operational failure mode I can imagine, what does the lender experience?"* This section addresses each.

4.1 What if Cadena disappears overnight

Outcome: settlement still executes. The pre-signed CETs are held by both parties at funding. The DLCP Oracle publishes its attestation. The CET broadcasts automatically. Cadena's operational existence is not required for the contract to settle.

If Cadena disappears mid-onboarding (before funding), the lender's Bitcoin is in the lender's wallet — nothing has been committed yet.

4.2 What if the oracle disappears or fails to attest

Outcome: refund timelock activates. Bitcoin returns to both parties at the timelock expiry. The lender does not lose principal; the borrower does not lose collateral. The interest is forfeit (no settlement, no interest paid), but the principal is preserved.

4.3 What if the borrower behaves badly during the term

Outcome: irrelevant to the lender. The borrower has no operational role during the term. The collateral is locked. The borrower cannot withdraw, cannot recall, cannot trigger any action. Settlement is automatic at maturity.

4.4 What if Bitcoin's price moves dramatically intra-term

Outcome: irrelevant to the lender until maturity. The contract has no in-term sensitivity. The lender's outcome depends only on the BTC/USD price at the maturity timestamp.

4.5 What if a force-majeure event disrupts Bitcoin's network

Outcome: settlement waits. Bitcoin transactions confirm when the network operates. If the network experiences extended downtime, settlement is delayed. The contract terms do not expire — the pre-signed CETs remain valid indefinitely until they're broadcast.

This is theoretical (Bitcoin has not had a multi-day outage since 2013), but the contract architecture is robust to it.

4.6 What if the lender or borrower loses their key

Outcome: matters for the residual, not for settlement. The pre-signed CETs broadcast automatically; settlement happens regardless. But the recipient of the pre-signed outputs needs their key to spend those outputs after settlement.

- **Lender loses key:** lender cannot spend the BTC paid out at settlement. This is standard self-custody risk; the lender should use institutional-grade key management (multisig, HSMs).
- **Borrower loses key:** same — they cannot spend the residual back to a new wallet.

Cadena cannot recover lost keys. We strongly recommend institutional lenders use 2-of-3 or 3-of-5 multisig for the funding key.

4.7 What if Cadena's matching service is compromised

Outcome: pre-funding only. A compromise of Cadena's matching service could affect pre-funding match logic (e.g., showing wrong terms during onboarding), but cannot affect a funded contract. Once both parties have signed the funding transaction and the CETs, the contract is committed and Cadena's operational systems are out of the loop.

---

5. Gap risk and hedging

This is the only structural risk the lender cannot eliminate through contract architecture alone. We frame it honestly.

5.1 The gap-risk regime

The contract pool covers the lender's full USD target down to a 50% BTC drop between funding and maturity. Below that threshold, the pool is no longer sufficient.

The shortfall in deep-drop scenarios is the gap-risk component of the lender's position.

5.2 Hedge construction

The gap risk is hedgeable with a put option struck near the 50% LTV threshold:

- **Construction:** purchase a BTC put option with strike at ~50% of the funding spot, expiring at or near the contract maturity
- **Cost:** depends on volatility regime; typically 2-3% of notional for a 12-month put at 50% strike in 2026 market conditions
- **Effect:** the put's intrinsic value at maturity offsets the contract pool's shortfall, capping the lender's downside exposure

For a $1M position at 12% annualized, hedge cost of 2-3% reduces net yield from 12% to 9-10%. **The hedged position effectively delivers double-digit USD yield with full downside protection.** This is the structural answer to "double-digit yield without the corresponding tail risk" — a category that does not exist in any other contemporary Bitcoin-credit product.

5.3 Lenders who don't hedge

Some institutional lenders may choose not to hedge:

- The unhedged position retains the full 12% USD yield

- Downside is capped at the borrower's collateral commitment (lender never loses principal beyond the gap-risk component)
- Historical Bitcoin drawdowns of >50% from peak have occurred but resolved over multi-month windows — sophisticated lenders may view this as an acceptable tail risk for the yield premium

This is a risk-tolerance decision, not a structural flaw. Both hedged and unhedged positions are valid.

---

6. Regulatory posture

6.1 Cadena's regulatory standing

Cadena Bitcoin S.A. de C.V. is a registered Bitcoin Service Provider in El Salvador under the country's BSP framework. El Salvador's framework specifically licenses Bitcoin-related financial services and provides a stable operational jurisdiction.

6.2 KYC and identity verification

KYC is mandatory for all contract participants. The identity verification flow:

- Runs **on-device** via the open-sourced Cadena Signer App
- Routes identity data to **Sumsub** (the third-party identity-verification provider) directly
- **Does not retain identity data at Cadena.** The customer's identity flows from their device to Sumsub; Cadena holds no centralized KYC trove

This architecture is materially better for institutional lenders concerned about counterparty diligence (the borrower is KYC'd) and for institutional lenders concerned about their own data privacy (their identity is held by Sumsub, not by a counterparty).

6.3 What this means for the lender's compliance team

The lender can verify:

- Cadena's BSP registration (publicly verifiable in El Salvador's regulatory registry)
- Sumsub's identity-verification SOC-2 / ISO 27001 standing (Sumsub's own compliance posture, separable from Cadena)
- The Signer App's open-source code (publicly verifiable, reproducible by the lender's technical team)
- The on-chain contracts (publicly verifiable on mempool.space)

Every claim in this section is independently verifiable. The lender's compliance team does not need to trust Cadena's word on any of it.

---

7. The proof artifact

7.1 The May 9, 2026 mainnet settlement

On **November 10, 2025**, two parties committed Bitcoin to a Cadena DLC. The contract:

- 6-month term
- 50% LTV
- DLCP Oracle for BTC/USD settlement

On **May 9, 2026**, the pre-signed CET broadcast on Bitcoin's mainnet. The lender's USD-denominated target was paid in BTC at the maturity price. The borrower received the residual back to self-custody.

The architecture executed exactly per the pre-signed structure.

Verify directly:
mempool.space/tx/95bf1377f4709235656bbaafa4afe454f91e905f8bb2dfe3e2bd1b619e5aab7d

7.2 Why this matters for institutional diligence

For a balance-sheet provider, the difference between *claimed* and *demonstrated* is structural. The May 9 settlement is the demonstration — Cadena's architecture executed correctly with real money on Bitcoin's mainnet. Every operational claim in this memo can be referenced against that transaction.

This is the diligence artifact that matters. Not a deck. Not a testnet demo. Not a screenshot. A real contract, with real money, on Bitcoin's base layer, fully verifiable.

---

8. Diligence checklist for the lender's risk team

Item	**Verification path**
Cadena's regulatory standing	El Salvador BSP registry (public)

Item	Verification path
Open-source Signer App	github.com/CadenaWizard/cryptlib
DLC architecture verification	Independent code review or third-party audit (we'll fund formal audit for institutional anchor commitments)
Oracle independence	DLCP Oracle public methodology + key infrastructure
Mainnet settlement record	mempool.space/tx/95bf1377…9e5aab7d
KYC framework	Sumsub SOC-2 / ISO 27001 documentation (provided on request)
Settlement mechanics	Pre-signed CET structure — code review + on-chain reference
Gap-risk hedge construction	Standard put option through the lender's existing derivatives counterparty
Contract terms in writing	Indicative term sheet (provided per institutional engagement)

Kevin Bell, CFA Founder & CEO, Cadena Bitcoin S.A. de C.V. kevin@cadenabitcoin.com · cadenabitcoin.com Calendar: calendly.com/cadenabitcoin-info/30min

---

This memo is for institutional diligence purposes. Rates shown reflect current market indicative pricing — actual rates clear at the marketplace at time of match. Past contract performance does not guarantee future outcomes. Bitcoin-collateralized credit involves real risks including gap risk below the 50% LTV threshold and operational risks of new financial infrastructure. Always conduct your own diligence and consult qualified professionals before deploying capital.

Source: Cadena_Knowledge_Base_v0.4.md · Code repository: github.com/CadenaWizard/cryptlib · Mainnet reference: mempool.space/tx/95bf1377…9e5aab7d · Last updated: May 17, 2026