Cadena Bitcoin: A Peer-to-Peer Electronic Credit System

Kevin Bell — kevin@cadenabitcoin.com
Ladanyi Szilard — sziller@cadenabitcoin.com

Overview

A purely peer-to-peer electronic credit system enables borrowing and lending directly between peers, bypassing financial institutions. While digital signatures offer a partial solution, their benefits erode if a trusted third party is still needed for custody. Cadena provides a trust-minimized solution using the Bitcoin network, leveraging discreet log contracts (DLCs), adaptor signatures, and oracles to create a secure, private, and scalable credit market.

1. Introduction

Online credit today depends heavily on financial institutions acting as intermediaries, issuing fiat currency and managing transactions. This trust-based model, while functional, has flaws: transactions are reversible, mediation raises costs, and disputes rely on third-party intervention. Worse, fiat money creation misaligns incentives—fueling debt, currency debasement, and financial instability over time. We propose a cryptographic alternative: an electronic credit system where two parties can lend and borrow directly, free from trusted intermediaries. Transactions are computationally irreversible, protecting both lenders and borrowers from counterparty risk. This paper introduces Cadena — a solution to the custody problem—using Bitcoin's Blockchain, discreet log contracts, adaptor signatures, and an oracle to build a decentralized credit market.

2. What Is a Loan?

A secured loan is more than just a debt—it's a financial instrument blending obligation and options. For the borrower, it's a duty to repay paired with an implicit put option on the collateral. If the collateral (here, Bitcoin) falls below the agreed strike price at maturity, the borrower

defaults, surrendering the collateral instead of paying out-of-pocket. The borrower's downside is capped at the collateral's value. The cost of this put reflects the interest paid plus any equity the borrower contributes.

For the lender, a loan is a right to full repayment at maturity (a call option), offset by the risk of the borrower's put. Higher Bitcoin volatility increases the put's value—and thus the lender's risk—since a price drop could leave them with less-valuable collateral. A higher strike price amplifies this risk further, reducing the collateral's buffer against market swings.

3. Transactions

Cadena's transactions are based on Discreet Log Contracts (DLCs), a Bitcoin-based framework addressing contract-simplicity, privacy, trust minimization and deterministic execution. DLCs obscure contract details on the Blockchain, making them invisible to outsiders. An electronic loan, in this system, consists of pre-signed transactions for each possible outcome at the contract's end. Time locks and oracle attestations ensure only the correct transaction can be broadcast to the Bitcoin network.

Traditional secured lending falters without custody: lenders can't verify collateral without a trusted authority or third party. Centralizing custody reintroduces third-party risks—bank-driven money creation and costly legal enforcement. Cadena avoids this by combining Bitcoin's native security with oracles - cryptographically incentivized, non-interactive, publicly verifiable data injection points, not counterparties. The oracle's role is constrained, auditable, and deliberately ignorant of its downstream use - eliminating the need for intermediaries or custodians.

4. DLC Protocol

In Cadena, contracts are represented by a single on-chain Transaction holding all funds until execution. Here's how it works:

- Alice (lender) and Bob (borrower) agree on a funding transaction ID (txid) and interest rate.
- They pre-create child transactions that spend this (then future) output before it's broadcast and confirmed.
- These transactions represent all possible outcomes, but on execution only the one - unlocked by the oracle's signature - can be published on the Blockchain. Both parties sign and store these options upfront.

The DLC protocol prioritizes privacy and trust minimization. By using an oracle to resolve outcomes — without revealing private keys — it enables smart contracts with conditional, time-locked payments. Bitcoin (the unit) serves as both collateral and unit of account, eliminating settlement risk for both parties.

5. Adaptor Signatures

Adaptor signatures are the cryptographic backbone of Cadena's execution. They allow the parties to pre-commit to every possible contract outcome, with each signature becoming valid only when extended, thus unlocked by a matching oracle attestation.

At contract inception:

- Signatures for every possible outcome are created and shared between borrower and lender.

- When the oracle attests Bitcoin's price at maturity, it effectively "signs" the correct output.
- This enables either party to publish the correct execution-transaction on-chain—without needing further cooperation
- Only two on-chain transactions occur: funding and execution. No separate closing step is needed.

6. Oracle

The Oracle problem — ensuring reliable external data — is one of the core challenges Cadena tackles through careful system design and the use of Discreet Log Contracts. Rather than eliminating the oracle, Cadena constrains and disincentivizes its misuse while keeping it unaware of its own involvement.

- Reliability: mirrored oracles, backups, and redundancy guarantee attestations. The technology is open source. If all fail, funds revert to their owners after a certain period as failsafe.
- Incentives: Oracles are reputationally (and financially) motivated to publish unique and consistent attestations. They are blind to contract details, publish their attestations in the public domain, and provide an impartial and verifiable price feed for all users.

This architecture supports a decentralized credit marketplace where lenders and borrowers connect securely — without relying on centralized control.

7. Example

We show how Cadena works with a loan between Bob (borrower) and Alice (lender). Bob puts up 1 Bitcoin (100,000,000 sats) as collateral. Alice provides the loan's discounted value at the start, with interest and fees deducted upfront.

- Collateral: 1 BTC (100,000,000 sats).
- Loan Size: 80% of the collateral's fiat value, set by an oracle at inception.
- Interest: 9% annual rate, or 0.75% for the 30-day term (simple interest).
- Fee: Cadena charges 250,000 sats, covering network costs and support.

Proceeds: Bob receives the loan minus interest and fees. Calculation:

- Repayment: 80,000,000 sats.
- Discounted for interest: 80,000,000 ÷ 1.0075 = 79,404,467 sats.
- Minus fee: 79,404,467 - 250,000 = 79,154,467 sats.

Bob keeps this amount from his own Bitcoin, avoiding the need to transfer collateral to Alice and back.

Oracle Role: An oracle attests Bitcoin's price in USD at the end of the 30-day term.

- Inception: Bitcoin is $100,000. The loan's fiat value is 80% of 1 BTC, or $80,000. Bob receives 79,154,467 sats (as above).
- Settlement: The oracle's final price determines how the 1 BTC collateral splits. Alice gets $80,000 worth of Bitcoin; Bob gets the rest.

Outcomes:

- Price rises to $120,000:

  Alice gets 66,666,667 sats ($80,000 ÷ $120,000 × 100,000,000).

  Bob gets 33,333,333 sats (100,000,000 - 66,666,667).

- Price stays at $100,000:

  Alice gets 80,000,000 sats ($80,000 ÷ $100,000 × 100,000,000).

  Bob gets 20,000,000 sats.

- Price falls to $90,000:

  Alice gets 88,888,889 sats ($80,000 ÷ $90,000 × 100,000,000).

  Bob gets 11,111,111 sats.

- Price drops to $80,000 or below:

  Alice gets 100,000,000 sats (all collateral).

  Bob gets 0 sats.

In each case, Alice's fiat return is fixed at $80,000 worth of Bitcoin. Bob's outcome depends on Bitcoin's price movement.

8. Conclusion

Bitcoin's secure, verifiable network offers more than value transfer—it's a foundation for decentralized credit. Cadena's use of discreet log contracts, adaptor signatures, and oracles enables peer-to-peer lending without trusted third parties. This system could democratize finance, reduce systemic risk, and provide additional use cases for Bitcoin in global financial markets.