Binocular: A Decentralized Optimistic Bitcoin Oracle on Cardano

Alexander Nemish @ Lantr

Draft v0.1

Abstract

Binocular is a decentralized, optimistic, trustless and permissionless Bitcoin oracle built on the Cardano blockchain. It enables Cardano smart contracts to access and verify Bitcoin state, opening up exciting possibilities like two-way bridges between the Cardano and Bitcoin ecosystems, providing a source of entropy, and allowing derivation of Bitcoin transaction inclusion proofs.

Introduction

Cross-chain interoperability is critical for decentralized ecosystems. By providing a trust-minimized oracle for Bitcoin state, Binocular extends Cardano's capabilities, enabling smart contracts to respond to Bitcoin events (block headers, proof of work).

Binocular follows an optimistic model where honest participants update the oracle, while users are incentivized to detect and report fraud.

Overview

Key Concepts

- **Miners:** Participants who update the oracle with valid block headers.
- **Fraud Proofs:** Evidence showing a submitted block header is invalid.
- **Chainwork:** Measures cumulative proof of work for chain validation.
- Anyone can become a Miner by committing a deposit into a Fraud Bond contract and minting a Miner token.
- Miners can create and update Oracle TxOuts with a Bitcoin block header in the Datum.
- Block header hash, block height and block chainwork are verified by the Binocular contract.
- Miners can withdraw the Fraud Bond by buring the Miner token after the deposit timeout.
- Anyone can challenge the Datum by submitting a Fraud Proof and take the Fraud Bond.

Fraud is when a published Bitcoin block header is not in the longest chain.

Fraud Proof is a Bitcoin block header of the same height or a timestamp within a same time range as the disputed block but with a higher chainwork.

- Mint a Miner token by depositing Fraud Bond into the contract.
- Minted Token name contains the deposit timeout.
- Miner token holders can submit Bitcoin a block header to the contract Datum.
- Miners can withdraw the Fraud Bond after the deposit timeout.
- Anyone can challenge the Datum by submitting a Fraud Proof and take the Fraud Bond.

Design

Fraud Bond

Fraud Bond is a UTXO locked by a validator script that can be spend if:

1. if timeout passed and the creator signature is valid
2. fraud proof is provided

Miner Token

Minting a Miner token checks:

1. Fraud Bond is valid
    1. is unspent: the TxOut of `Bond` validator hash is referenced in the transaction
    2. has > `minDeposit` ADA locked
    3. has timeout > `minTimeout` in the future
2. Oracle TxOut is created
    1. it's a first TxOut
    2. TxOut contains the Miner token as a proof this Oracle TxOut was checked by the Miner contract
    3. Datum has a predefined valid `initial Block header`
    4. Datum has a `ownerPubKeyHash` and the transaction is signed by the owner

Burning a Miner token checks:

1. Oracle TxOut:
    1. is spent
    2. has a valid signature of the owner

Updating the Oracle

Updating the Oracle checks:

1. Miner token is preserved

2. New TxOut Datum is updated
    1. Datum has a valid `block header hash`
    2. Datum has a valid `block height`
        1. is higher than the previous block height
        2. checks the Coinbase tx hash inclusion proof against the block header merkle root hash
    3. Datum has a valid `chainwork`
        1. block header hash is $<$ `target` according to the block header
    4. Block `timestamp` is in the past
    5. Datum has a valid `ownerPubKeyHash`
    6. Datum is signed by the owner

Fraud Proof

Lets anyone challenge invalid updates by submitting a conflicting block header.

Security Assumptions

- Mining a Bitcoin block for block height in (initialBlockHight, currentBlock-Hight) is more expensive than the Fraud Bond deposit value
- SHA256 is a secure hash function
- Ed25519 is a secure signature scheme

Limitations & Future Work

In this initial design, the frequency at which the Oracle is updated depends on the incentives and activity level of the Miner participants. An area for future exploration is incentive design to ensure frequent, consistent Oracle updates.

The Miner and Fraud Proof roles also require archival Bitcoin node access, introducing external dependencies. Future work could explore ways to further decentralize and trustlessly-bootstrap the system.

Conclusion

Binocular presents a trust-minimized approach to cross-chain interoperability by serving as a decentralized Bitcoin Oracle for Cardano. Its optimistic design and robust economic incentives ensure accuracy while empowering developers to build innovative cross-chain DApps.

References

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf
2. Scalus: https://scalus.org

3. NIPoPoW Paper: "Non-Interactive Proofs of Proof-of-Work," https://eprint.iacr.org/2017/963.pdf
4. Learn Me a Bitcoin: https://learnmeabitcoin.com/
5. Cardano Documentation: https://docs.cardano.org/
6. Bitcoin Developer Guide: https://developer.bitcoin.org/