FluidSwaps Whitepaper: Cardano and Bitcoin Cross-Chain Interoperab

Introduction

Swaps between Cardano and Bitcoin are possible through FluidSwaps, which leverages smart contract technology on both chains.

This whitepaper will explain the process and code behind FluidSwaps, allowing permissionless cross-chain trades between Cardano (ADA) and Bitcoin (BTC) without third-party trust.

This system allows users to:

1. Use Cardano smart contracts for permissionless trades.
2. Utilize Bitcoin's custom script logic for unlocking funds.

Process Overview

In FluidSwaps, Alice and Bob want to trade Bitcoin and ADA respectively, in a trustless, permissionless manner. The process works as follows:

1. **Alice** has 1 Bitcoin (BTC), and **Bob** has 100k ADA.
2. Bob shares the hash of a password with Alice and deposits the 100k ADA into the Cardano smart contract.
3. Alice can unlock the ADA by signing with her Bitcoin wallet and providing the password.
4. If Alice doesn't sign within a certain expiration time, Bob can reclaim the ADA.
5. On the Bitcoin side, a script is used to lock 1 Bitcoin. Alice sends the Bitcoin to an address that requires Bob to reveal the password to unlock it.
6. Once Bob claims the Bitcoin, Alice can claim the 100k ADA from the Cardano contract.

This interaction uses the power of smart contracts and Bitcoin's script functionality to ensure secure,

trustless swaps.

Code Explanation

The following explains the key code involved in FluidSwaps.

1. **Cardano Smart Contract (Aiken-based) Code**:
   - Bob shares a hashed password with Alice.
   - Bob sends ADA to the smart contract, which contains the hashed password in the datum.
   - Alice claims the ADA by signing the contract with her Bitcoin wallet and providing the correct password.
   - After expiration, Bob can reclaim the ADA if Alice does not act.

This smart contract is written in Aiken, leveraging Cardano's smart contract functionality.

2. **Bitcoin Script Code**:
   - A Bitcoin address is generated from the public keys of Alice and Bob plus the hashed password.
   - Alice sends 1 Bitcoin to this address.
   - Bob reveals the password to unlock the Bitcoin. If Bob does not reveal it in time, Alice can reclaim it.

The Bitcoin script ensures that funds are locked until Bob reveals the password.

Here is the simplified pseudocode behind both contracts:

Cardano Smart Contract (Aiken):
- Bob shares the hashed password.
- Bob sends 100k ADA to the contract, with the password in the datum.

- Alice can claim the ADA by signing the contract and providing the password.
- If Alice does not sign within the expiration time, Bob can reclaim the ADA.

Bitcoin Script:

- Bitcoin address generated using Alice's and Bob's public keys and the password hash.
- Alice sends 1 Bitcoin to this address.
- Bob must reveal the password to unlock it.
- If Bob does not unlock it in time, Alice can reclaim the Bitcoin.

This combination of technologies ensures a secure, permissionless swap between Bitcoin and Cardano.

Applications of FluidSwaps

FluidSwaps can be used in various decentralized finance (DeFi) applications, such as:

- **NFT Marketplaces**: Enable users to swap Bitcoin and ADA seamlessly for NFTs.
- **Decentralized Exchanges (DEX)**: Swap Bitcoin (BTC) and Cardano native tokens (ADA/CNT) directly.
- **Liquidity Injection**: Allow Bitcoin liquidity into Cardano ecosystems.
- **Smart Contracts for Bitcoin**: Use smart contracts on Cardano to interact with Bitcoin transactions.

These applications demonstrate the real-world utility of cross-chain interoperability between Bitcoin and Cardano.

Conclusion

FluidSwaps empowers decentralized applications by enabling permissionless, trustless swaps

between Bitcoin and Cardano using their respective smart contract and script functionalities. This integration brings the power of cross-chain interoperability, benefiting both ecosystems and fostering a more inclusive DeFi landscape.