Begin Wallet - Milestone 4

Bitcoin Compatibility Integration in Begin Wallet

Technical Writer: Francis Luz, CEO

1. Introduction

Begin Wallet is a multi-asset cryptocurrency wallet that supports seamless management of both Cardano and Bitcoin assets. With the release of version 1.21.1, we have introduced Bitcoin compatibility, enabling users to create, sign, and track Bitcoin transactions within the same wallet interface. This enhancement ensures that users can manage both Cardano and Bitcoin under a single seed phrase.

2. Implementation Details

Version 1.21.1 of Begin Wallet introduces Bitcoin wallet management alongside Cardano. Users now have access to:

- A unified seed phrase for managing both Bitcoin and Cardano wallets.
- The ability to create and sign Bitcoin transactions securely.
- An integrated Bitcoin module within Begin Wallet's Open Source Core, ensuring transparency and extensibility.

3. Acceptance Criteria & Features

The integration adheres to the following acceptance criteria:

- Transaction Creation: Users can assemble a Bitcoin transaction by entering the recipient's Bitcoin address, specifying the amount, and reviewing the calculated transaction fee.
- Transaction Signing: Users can sign transactions using their private key and receive confirmation once the transaction is signed and ready for broadcast.
- Transaction Broadcasting: Users can broadcast the signed Bitcoin transaction to the Bitcoin network, including the required fee for miner confirmation.

A demonstration of these features is available in the following video: [Demo](https://youtube.com/shorts/BXALveJ8X1k?feature=share)

An example transaction can be found on Mempool: [Transaction](https://mempool.space/tx/90e1e5760db378aa2101b655af4299193236b930d7850e38b06d96c7993a01c3)

4. Technical Architecture

- The Bitcoin module is implemented within the Open Source Core of Begin Wallet: [GitHub - Begin Core](https://github.com/BeginWallet/begin-core/tree/main/src/core/chain/bitcoin)
- The integration ensures compatibility with standard Bitcoin signing mechanisms while maintaining security and efficiency.
- The wallet uses deterministic key derivation to enable seamless access to both Bitcoin and Cardano accounts from the same seed phrase.
- Supported Bitcoin Address Types:
  - Segwit (p2wpkh): Standard native Segwit addresses for efficient and lower-fee transactions.
  - Taproot (p2tr): Address type enabling Ordinals support and enhanced privacy.
- Base Implementation for Additional Chains: The architecture is designed with flexibility in mind,

allowing for future support of other UTXO-based chains, including Dogecoin (DOGE).

- API Providers for Network Indexing and Transaction Broadcasting:
  - Maestro: Provides transaction history and sending capabilities.
  - Blockstream: Used for balance retrieval.
  - Mempool.space: Utilized for live fee rate estimation.

5. Challenges & Solutions

During development, we encountered the following challenges:

- Transaction Fee Estimation: Ensuring accurate fee calculation required real-time network fee monitoring and adjustment algorithms.
- Seed Phrase Compatibility: Unifying Bitcoin and Cardano under a single seed phrase required careful derivation path management.
- Security Considerations: Implementing secure transaction signing without exposing private keys was a top priority, addressed through hardware and software-based signing solutions.

6. Conclusion & Future Work

The Bitcoin compatibility integration in Begin Wallet marks a significant milestone in multi-asset management. With the ability to create, sign, and track Bitcoin transactions seamlessly, users benefit from enhanced functionality within a unified wallet experience.

Future enhancements may include:

- Lightning Network support for faster Bitcoin transactions.
- Improved fee estimation algorithms based on historical network data.
- Advanced multi-signature wallet support.

For further details, refer to our Catalyst repository: [GitHub - Catalyst](https://github.com/BeginWallet/catalyst-fund-12/)