Wallet Integration

About CIP-08 and CIP-30

This guide is a walkthrough on how to implement the *message signing* described in CIP-08 in order to authenticate users on the web with just their CIP-30-compatible wallet app:

https://developers.cardano.org/docs/integrate-cardano/user-wallet-authentication/

However while it is useful to study the above, in order to simplify and standardize our platform, we're going to use a multi-chain wrapper library instead (see next section).

Using Weld

We're going to use this library to integrate with Cardano wallets:

https://github.com/Cardano-Forge/weld

Weld lets you manage wallet connections across multiple blockchains using a single intuitive interface.

How Authentication works

In a Web3 app using wallets like **Nami** or **Vespr**, authentication typically works through **wallet-based signature verification**. Here's a simplified flow:

1. **Connect Wallet**: The user connects their wallet to the Web3 app. The wallet extension (like Nami or Vespr) interfaces with the app to allow interactions.
2. **Generate Nonce**: The app generates a unique, random string (nonce) and sends it to the wallet for the user to sign. This ensures that each authentication request is unique and prevents replay attacks.
3. **Sign Nonce**: The user signs the nonce using their private key in the wallet. This signature doesn't expose the private key but proves ownership of the wallet.
4. **Verify Signature**: The app receives the signed nonce and verifies it using the user's public key (derived from their wallet address). If the signature is valid, it confirms the user controls the wallet.
5. **Authenticate User**: Once verified, the app logs in the user and associates their wallet address with their session or profile. The wallet address often serves as the unique user identifier.
6. **Session Management**: The app can use cookies, tokens (like JWTs), or smart contract events to manage sessions while interacting with the blockchain.

This method ensures secure, decentralized authentication without traditional usernames or passwords. Wallets like Nami and Vespr streamline this process by providing user-friendly interfaces for signing and verifying data.

We'll be testing with both those wallets, and the screenshots you're going to see in the documentation will be from one of those two wallets (and especially on mobile phones, with Vespr).

Revision #6
Created 22 November 2024 17:27:12 by Aric Fedida
Updated 7 December 2024 18:46:45 by Aric Fedida