Project Document: PropFi — Real World Asset Tokenization on Cardano

Hackathon Track: General Stablecoin Application

Date: October 26, 2023

---

1. Executive Summary

PropFi is a decentralized application (DApp) built on the Cardano blockchain designed to solve the twin challenges of the global real estate market: **high entry barriers** and **illiquidity**.

By leveraging Cardano's secure eUTxO architecture and native asset standards, PropFi enables asset owners to fractionalize real-world properties into digital tokens. These tokens represent legal ownership shares and can be traded instantly for stablecoins (like USDM or iUSD). This process democratizes access to real estate investment and unlocks liquidity for asset owners, all through a seamless, mobile-first experience without reliance on traditional financial middlemen.

Key Value Proposition

- **For Investors:** Access high-yield global real estate with low capital (e.g., buy $100 of a New York apartment) directly from a mobile device.
- **For Asset Owners:** Unlock property value instantly by selling fractional shares to a global pool of investors, bypassing slow traditional sales processes.
- **For the Ecosystem:** Demonstrates a powerful, real-world use case for Cardano stablecoins, driving transaction volume and utility.

---

2. Problem & Solution Statement

The Problem

Traditional real estate suffers from significant inefficiencies:

1. **High Capital Barrier:** Prime real estate is unaffordable for most individual investors.
2. **Severe Illiquidity:** Buying or selling property is a slow, bureaucratic process taking months, trapping capital.
3. **Geographical Limits:** Investing in foreign markets involves complex legal and financial hurdles.
4. **Middleman Tax:** Brokers, lawyers, and banks extract significant fees at every step.

The PropFi Solution

PropFi utilizes blockchain technology to create a trustless bridge between physical assets and digital liquidity:

1. **Fractionalization:** A $1M property is represented by 1,000,000 tokens, making entry affordable for anyone.
2. **Instant Liquidity:** Tokens can be bought or sold 24/7 against stablecoin liquidity pools via smart contracts.
3. **Global Access:** A permissionless platform allows anyone with a Cardano wallet to invest globally.
4. **Automated Trust:** Smart contracts handle escrow, ownership transfers, and payment distribution, removing costly intermediaries.

---

3. Technical Architecture

The platform is built as a unified Single-Page Application (SPA) using Flutter, interacting with the Cardano blockchain via a robust backend infrastructure.

High-Level Tech Stack

Component	Technology Choice	Purpose
Frontend	Flutter (Dart)	Cross-platform mobile & web app with a single codebase.
Blockchain	Cardano (Preprod Testnet)	Secure, scalable settlement layer.
Smart Contracts	Aiken	Modern, functional language for secure on-chain logic.
Tx Building	MeshJS / Lucid (TS)	SDKs to construct complex transactions for wallet signing.

Blockchain Data	Blockfrost / Koios	API provider to query on-chain data (UTxOs, assets).
Storage	IPFS (via Pinata)	Decentralized storage for high-res images and legal documents.
Wallets	Eternl, Flint (CIP-30)	Browser and mobile extension wallets for user interaction.

System Workflow

The workflow is split into two primary user roles within the single application: the **Admin/Seller** and the **Investor**.

A. The Asset Tokenization Flow (Admin/Seller Role)

1. **Data Input:** Admin logs into the DApp and provides property details (title, valuation, location) and uploads legal title deeds (PDF) and high-quality images.
2. **Off-Chain Storage:** The Flutter app uploads files to IPFS via Pinata, retrieving unique content hashes (CIDs).
3. **Metadata Construction:** The app constructs a CIP-25 compliant metadata JSON object containing property details and IPFS hashes representing legal proof.
4. **Minting Transaction:** The app uses the MeshJS SDK to build a minting transaction. This transaction:
    - Mints a defined supply of fractional tokens (Native Assets) under a unique Policy ID representing the property.
    - Attaches the constructed metadata to the transaction.
    - Sends the newly minted supply to the **PropFi Sales Smart Contract**.
5. **On-Chain Confirmation:** The Admin signs the transaction with their wallet. The tokens are created and locked in the sales contract, ready for purchase.

B. The Investment Flow (Investor Role)

1. **Marketplace Discovery:** The Investor opens the app. The app queries Blockfrost to find assets currently held at the Sales Smart Contract address and fetches their metadata to populate the marketplace feed.
2. **Purchase Action:** The Investor selects a property and specifies a stablecoin amount to invest (e.g., 500 USDM).
3. **Atomic Swap Transaction:** The app builds a smart contract transaction that performs an atomic swap:
    - **Input 1:** Investor's wallet sends 500 USDM to the Sales Contract.

    - **Output 1:** Sales Contract sends the equivalent value of Property Tokens to the Investor's wallet.
    - *Crucially, the Aiken smart contract validates that the correct amount of stablecoin is received based on the set token price before releasing assets.*
4. **Execution:** The Investor signs the transaction. The swap happens instantly and trustlessly on-chain. The investor's portfolio dashboard is updated to reflect their new ownership.

---

4. Smart Contract Design (Aiken)

The core logic resides in two primary Aiken contracts:

1. Minting Policy Contract

This contract controls the creation of property tokens.

- **Logic:** It enforces that only a designated "Admin" or "Issuer" wallet signature can mint tokens under a specific Policy ID. This prevents unauthorized creation of fake property tokens.

2. Sales / Marketplace Validator

This contract holds the minted tokens and manages sales.

- **Datum (State):** Stores essential data like the token price (in stablecoin), the seller's payout address, and the Policy ID of the accepted stablecoin.
- **Redeemer (Action):** Handles the Buy action.
- **Validation Logic:** When a Buy is attempted, the contract checks:
    - Is the incoming payment made in the correct, whitelisted stablecoin?
    - Does the amount of stablecoin match the number of property tokens being requested, based on the price in the Datum?
    - If both are true, the transaction is approved, and the atomic swap executes.

---

5. Hackathon Implementation Roadmap

This roadmap outlines a 4-week sprint to deliver a functional MVP representing the primary sales cycle.

Phase	Duration	Key Deliverables

Week 1: Foundation & Core Logic	7 Days	• Setup Aiken, Flutter, and Blockfrost environments. • **Aiken:** Draft initial Minting Policy and Sales Validator contracts. • **Flutter:** Scaffold app UI with fake data for Marketplace and Detail 6screens. • **Integration:** Create scripts to mint test stablecoins on Preprod network.
Week 2: Connecting the Pipes	7 Days	• **Aiken:** Finalize Sales Validator logic with unit tests for atomic swaps. Deploy to testnet. • **Flutter:** Build wallet connection UI (CIP-30 integration). • **Integration:** Implement IPFS upload service via Pinata API. Set up transaction building framework using MeshJS within the Flutter project.

Week 3: The Core Loop (Heavy Lift)	7 Days	• **Admin Feature:** Wire "Mint" button in UI to trigger real on-chain minting transaction with metadata. • **Investor Feature:** Replace fake marketplace data with real on-chain data fetched via Blockfrost. • **Investor Feature:** Wire "Buy" button to trigger the atomic swap smart contract transaction.
Week 4: Polish & Presentation	7 Days	• **Testing:** End-to-end testing of the buy cycle on Testnet. Fix bugs. • **UI/UX:** Apply final branding, loading states, and error handling. • **Demo Prep:** Record a clean, live demonstration video of the purchase flow. Finalize submission documentation.

---

6. Future Outlook & Scalability (Post-Hackathon)

While the hackathon MVP focuses on the primary sale, the platform is designed for future expansion:

1. **Secondary Market:** Implement a peer-to-peer order book design, allowing investors to trade fractional shares among themselves.

2. **Yield Distribution:** Create a mechanism to airdrop rental income (in stablecoins) periodically to holders of property tokens.
3. **DAO Governance:** Transition admin control to a DAO, allowing token holders to vote on which new properties to acquire or list.
4. **Legal Framework Integration:** Partner with legal firms to establish the real-world Special Purpose Vehicle (SPV) structure that legally binds the on-chain tokens to the physical deed.