MAYZ Trustless OTC Protocol Close-Out Report

🧾 Project Overview

Project Name: MAYZ Trustless OTC Protocol
Project Number: 1200222
IdeaScale Link: https://cardano.ideascale.com/c/cardano/idea/120544
Project Manager: Agustín Franchella
Team Members: Diego Torres Borda, Federico Ledesma Calatayud, Diego Macchi, Manuel Padilla, Alfred Vilsmeier, Luis Restrepo
Start Date: July 15, 2024
Completion Date: May 9, 2025

🎯 Challenge KPIs and Outcomes

Challenge Area: Products & Integrations That Drive Adoption

- **✔ Full OTC DApp deployed on Cardano Mainnet**
- **✔ All smart contracts and UI repos released open source**
- **✔ Demo video, onboarding guides, public documentation**

✅ Project KPIs by Milestone

1. **Research Liquidity Challenges: Explored pain points within the Cardano DeFi landscape (Milestone 1).**
2. **Architecture & Docs: Delivered architecture diagrams, flowcharts, and a complete technical README (Milestone 2).**
3. **Smart Contracts in Aiken: Built and fully tested smart contract suite using Aiken (Milestone 3).**
4. **Testnet Deployment: Successfully deployed contracts and DApp to Cardano Testnet (Milestone 4).**
5. **Final Delivery: Deployed Mainnet version with demo video and open-source documentation.**

📌 **Proof of Achievement:** [View on Milestones Tracker]

🌟 Highlights & Achievements

- **Created the first trustless OTC protocol on Cardano using NFT-bound trade offers.**
- **Adopted Aiken and Plutus V3, contributing to modern smart contract development.**
- **Engaged the Cardano community in testing and validating the protocol.**
- **Delivered everything open-source, from smart contracts to onboarding tools.**

🧠 Key Learnings

- **Aiken enables faster iteration and smoother testing compared to legacy Plutus.**
- **Starting with a clear architecture minimized rework and errors later.**
- **Phased deployment—testnet to Mainnet—gave us valuable feedback loops.**
- **Strong documentation played a key role in developer and user adoption.**

🔭 Next Steps

- **Perform a comprehensive security audit.**
- **Continue planning for Mainnet expansion based on user demand.**
- **Add integrations with popular wallets (Lace, Eternl) and Cardano DEXs.**
- **Seek partners and funding to expand liquidity support and extend use cases.**

💬 Final Thoughts

The MAYZ Trustless OTC Protocol represents a modular, reusable system for off-chain liquidity matching. By combining NFTs and validator logic into a seamless user experience, we've created a new way to perform OTC trades transparently and securely. Thanks to Project Catalyst and the Cardano community for making this possible.

📂 Project Assets

- **Smart Contracts Repository:** https://github.com/MAYZGitHub/mayz-otc-contracts
- **Frontend Application:** https://github.com/MAYZGitHub/mayz-otc-dapp
- **Milestone Reports:** Available in `catalyst-reports/` directory in the repo
- **Documentation:** See README and `docs/` folder
- **Demo Video:** https://youtu.be/nWqTrBFGd-4

🧩 Functional Documentation

1. Smart Contract Functionality Explained

`create_offer`

- **Purpose:** Starts a new OTC deal by locking the user's tokens and minting a unique NFT.
- **How it works:** The user defines what they are offering and what they want in return. This data is stored in a smart contract UTxO. The use of the `$MAYZ` token is required to authorize order creation.
- **Result:** The offer is now visible and active on-chain.

`accept_offer`

- **Purpose:** A counterparty accepts the offer by providing the required tokens.
- **How it works:** The taker sends the ask tokens and receives the offered tokens in return. The offer NFT is burned.
- **Result:** The deal is settled and closed.

`cancel_offer`

- **Purpose:** Allows the original offer creator to cancel and reclaim their tokens.
- **How it works:** The user must prove ownership via signature and the offer NFT.

- **Result: The offer is closed and funds returned.**

`redeem_after_timeout`

- **Purpose: Acts as a safety net to recover funds if the offer expires.**
- **How it works: After the deadline, the original offerer can retrieve their tokens.**

NFT Minting Logic:

- **Minted NFT uniquely represents the offer.**
- **Enforced to be one per offer.**
- **Token name = `Original Token Name + Amount represented. eg. MAYZ-100, SNEK-1000`.**

2. Security and Error Handling

- **Authorized Actions: Only the offer creator can cancel. Acceptors must own the NFT.**
- **Value Checks: Asset amounts must exactly match offer terms.**
- **Failure Handling: Invalid or actions automatically revert and preserve funds.**
- **Off-Chain Checks: Wallet interface checks validity before transactions are submitted.**

3. Contract Dependencies

- **The OTC contract logic is self-contained, with no technical dependencies on other MAYZ smart contracts.**
- **However, creating OTC offers requires holding and using the `$MAYZ` token, which acts as a utility token.**
- **This dependency is set during protocol creation and could theoretically be replaced by another token if reconfigured.**
- **Admin and Emergency tokens are used to allow protocol upgrades or edits, but they cannot override individual user transactions or seize funds.**

4. Wallet & Ecosystem Integration

- **Wallet Support: Lace, Eternl, Nami, Gero (via Lucid & CIP-30).**
- **Endpoints:**
    - **`/api/otc/create`, `/claim`, `/close`, `/cancel`**
    - **Support full trade lifecycle: create, fulfill, close, cancel**
- **Token Compatibility:**
    - **Uses CIP-20 for tokens, CIP-25 for NFT metadata**
    - **CIP-47 inline datums and CIP-68 reference scripts improve cost-efficiency and indexing**
- **Marketplace Ready: NFTs can be displayed and traded on Cardano NFT platforms.**

5. Upgrade Path & Versioning

- **Approach: Each OTC offer is handled individually through its own UTxO and NFT, which simplifies upgrade logic and avoids central dependencies.**
- **Current Version: Validator logic is exposed via `validatorV1` in the Aiken source code.**
- **How Updates Work:**
    - **New validator versions (e.g., `validatorV2`) can be introduced and selected via the off-chain configuration.**
    - **Offers already created under `validatorV1` remain valid and unaffected.**
- **Protocol Governance Tokens:**
    - **The `EMERGENCY` and `ADMIN` tokens are used to authorize protocol edits or upgrades.**
    - **These tokens do not allow the team to interfere with user funds or override trade logic.**

📣 Documentation & Community Links

- **Final Report:** MAYZ-OTC-CloseOut.md on GitHub

Connect with Us

- Instagram
- Discord
- Medium
- X / Twitter
- Website