ANASTASIA LABS

Trustless P2P On-Ramp Smart Contract Design Specification

Date: July 9, 2024
Project: Money Kit
Version 1.0

1 Introduction

This document provides a detailed technical protocol design specification for a Trustless P2P On-Ramp smart contract application. The system is designed to connect cryptocurrency sellers and buyers in a decentralized manner, ensuring the secure transfer of funds with minimal trust required between parties. The application leverages Money Kit for user registration and transaction validation.

2 Key Components

1. **Money Kit Integration** Ensures that both buyers and sellers are registered and validated
2. **Smart Contract** Manages fund deposits, timelocks, and the release of the funds based on cryptographic proof
3. **Cryptographic Proof** Mechanism for the buyer to prove fiat payment delivery
4. **Timelocked Transactions** Ensures funds are held securely until conditions are met
5. **Non-Compliance Mechanism** Handles cases where buyers do not follow through with the purchase

3 Protocol Design

3.1 Data Structures

```
data Datum = Datum
  { paymentInfoHash :: ByteString
      -- ^ Hashed payment information
  , sellPriceUsd :: Integer
      -- ^ Price in USD for the sale
  , valueSold :: Value
      -- ^ Cryptocurrency value being sold
  , sellerPKH :: PubKeyHash
      -- ^ Seller's PubKeyHash
  , buyerPKH :: Maybe PubKeyHash
      -- ^ Buyer's PubKeyHash
  , timelock :: Maybe POSIXTime
      -- ^ Deadline for buyer to claim
  }

data Redeemer
  = Cancel
  -- ^ Seller cancels the value selling
  | Update
  -- ^ MoneyKit updates the buyer and timelock
  | Claim
  -- ^ Buyer claims the value
```

3.2 Registration

Buyer and Seller Registration

- Both parties must register via MoneyKit.

3.3 Transaction Phases

3.3.1 Submit value to sell

Seller submits transaction to sell the value.

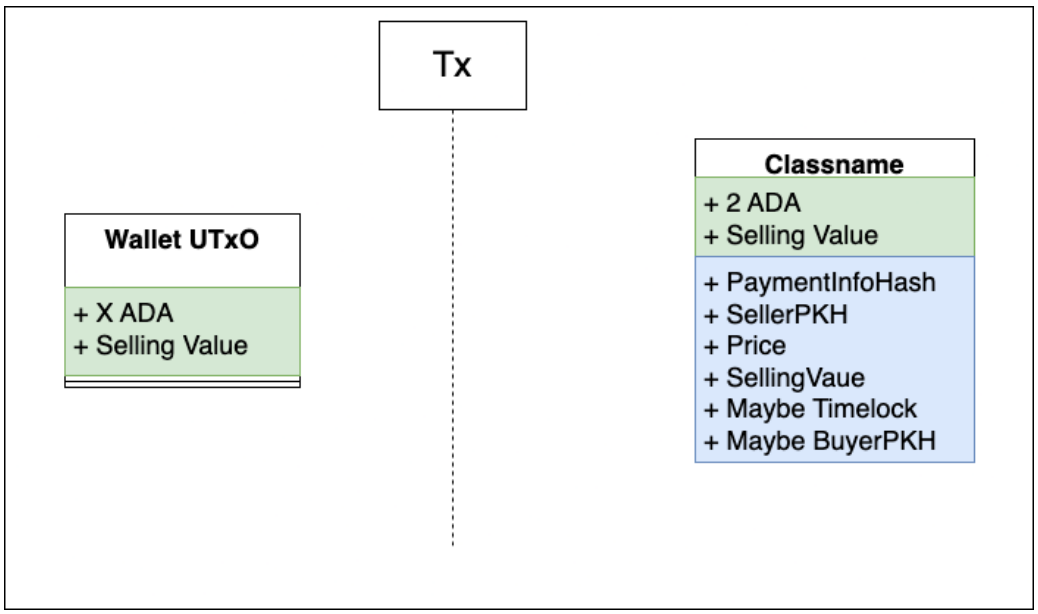

Figure 1: Submitting Value to Sell

3.3.2 Intent to Buy

- Buyer submits an intent to buy.
- MoneyKit make a transaction to update buyer information and timelock of seller's UTxO.

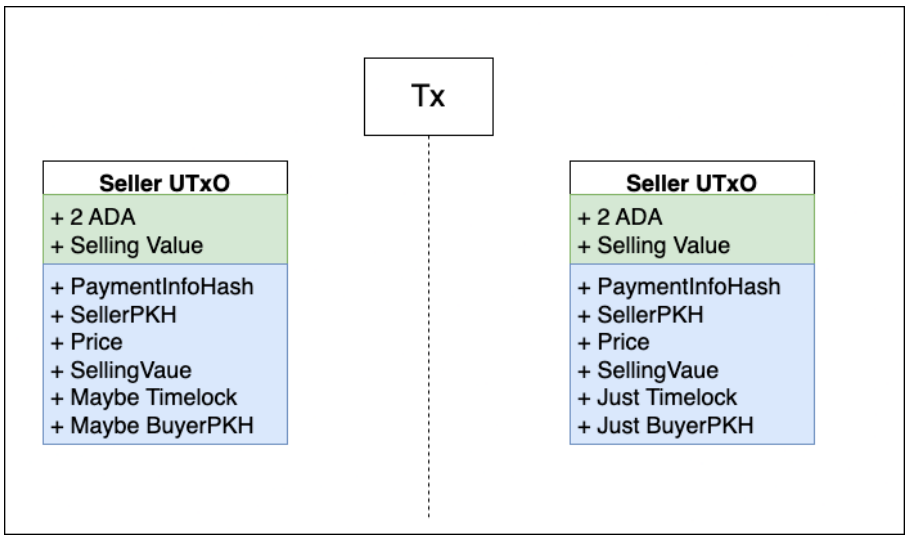

Figure 2: Intent to Buy Process

3.3.3 Cancel the sell

The seller cancels the selling order. This transaction can only be executed if one of the following conditions is met:

- No buyer has submitted an intent to buy.
- Or the timelock has expired.

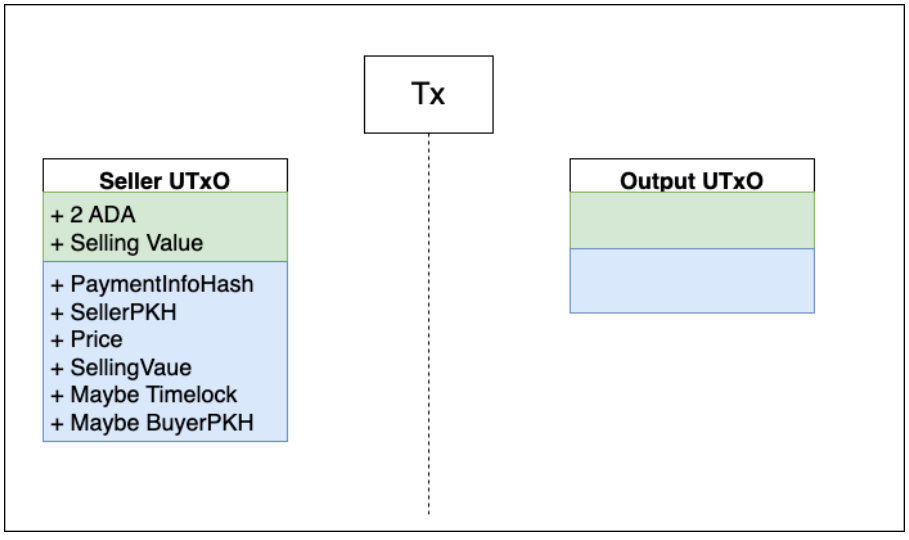

Figure 3: Cancel the sell

3.3.4 Claim

- Buyer claims the value.

- MoneyKit takes the fee.

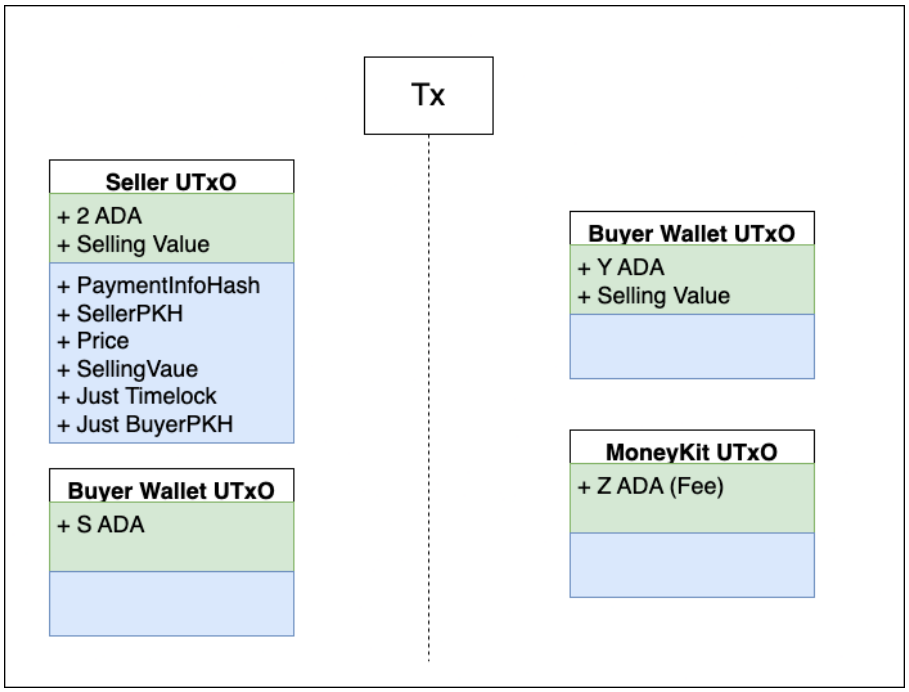

Figure 4: Claim

3.4 MoneyKit flow

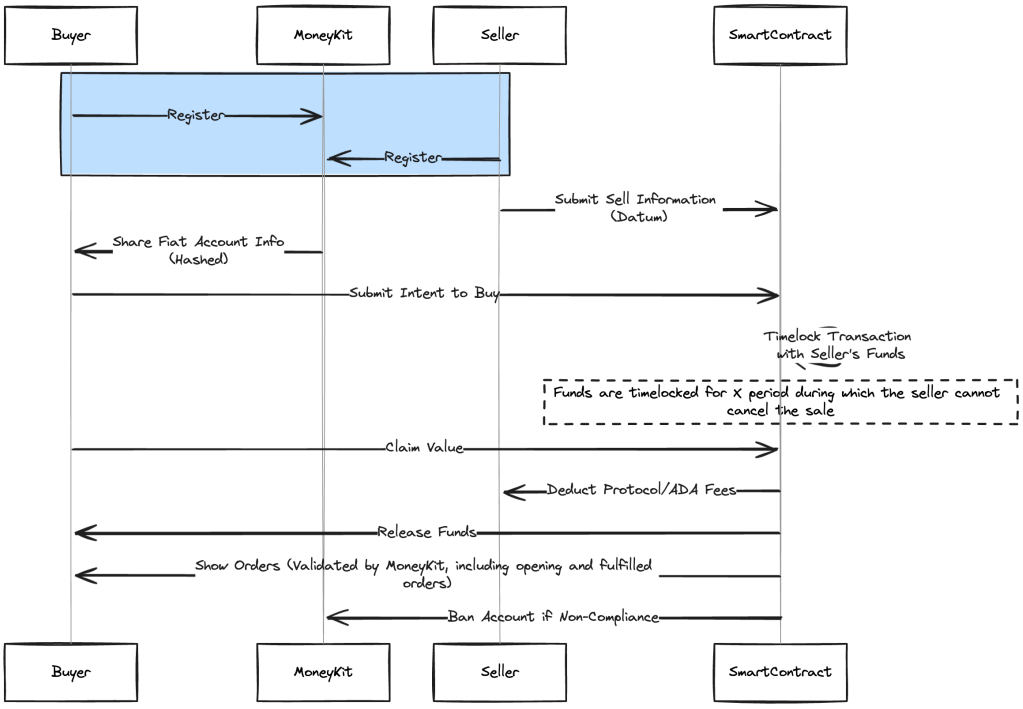

Figure 5: MoneyKit Flow

4 Security Considerations

- **Timelock**:
  - Ensure timelock duration is sufficient for payment confirmation.
  - Protect against replay attacks using unique transaction IDs.
- **Cryptographic Proof**:
  - Use robust cryptographic methods to ensure proof cannot be forged.
- **Non-Compliance**:
  - Implement a reliable mechanism to detect and handle non-compliance by buyers.

5 Conclusion

This specification outlines the design and implementation of a Trustless P2P On-Ramp smart contract application. By leveraging MoneyKit for user validation and implementing secure smart contract logic, the system ensures a trustless and secure environment for cryptocurrency transactions.