ANASTASIA LABS

Trustless P2P On-Ramp Smart Contract Design Specification

Date: June 18, 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
  }
```

3.2 Registration

Buyer and Seller Registration

- Both parties must register via MoneyKit.

3.3 Transaction Phases

3.3.1 Intent to Buy

- Buyer submits an intent to buy.
- Fiat account information (hashed) is shared with the seller.

- Transaction is created and timelocked with the seller’s funds in the UTxO.

3.3.2 Timelock Phase

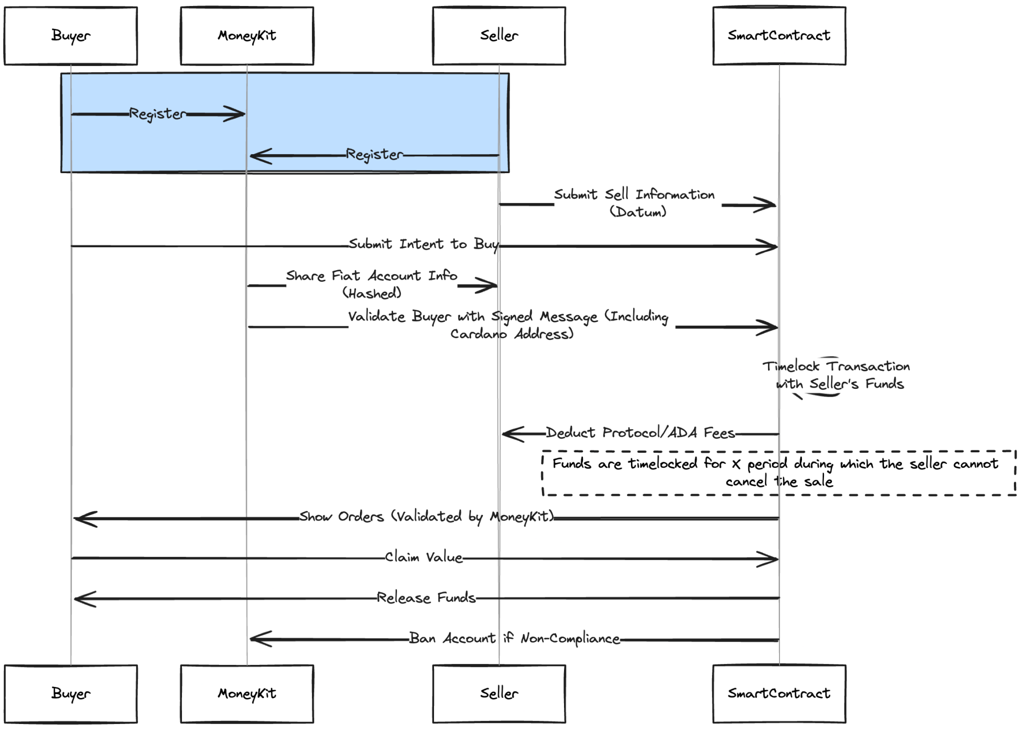
- Transition to the timelock phase requires a signed message from MoneyKit, validating the buyer’s registration.
- MoneyKit provides a signed message validating the user’s registration and Cardano address.
- Only validated orders are shown in the UI.

3.3.3 Payment and Fund Release

- Funds are timelocked for a specified period (e.g., 15 blocks after payment is made).
- The buyer generates a cryptographic proof of payment and submits it to the smart contract.
- Upon successful verification, the funds are released to the buyer.

3.3.4 Non-Compliance Handling

- If the buyer submits an intent to buy and does not follow through, the associated MoneyKit account is banned.


Buyer
MoneyKit
Seller
SmartContract
Register
Register
Submit Sell Information (Datum)
Submit Intent to Buy
Share Fiat Account Info (Hashed)
Validate Buyer with Signed Message (Including Cardano Address)
Timelock Transaction with Seller's Funds
Deduct Protocol/ADA Fees
Funds are timelocked for X period during which the seller cannot cancel the sale
Show Orders (Validated by MoneyKit)
Claim Value
Release Funds
Ban Account if Non-Compliance
Buyer
MoneyKit
Seller
SmartContract

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.