ANASTASIA LABS

Upgradable Multi-Signature Contract

Project Design Specification

Contents

1. Overview

This Upgradable Multi-Signature Smart Contract is developed using Aiken for the Cardano blockchain. It is designed to facilitate secure asset transactions by authorized members within predefined thresholds. The contract allows for seamless adjustment of signer thresholds and dynamic addition or removal of signers, ensuring long-term usability and adaptability.

2. Architecture

There are one main contracts in this multi-sig system.

1. **Multisig Validator**

   This is the core contract responsible for handling the logic for:

   - Managing authorized signers
   - Validating and executing transactions
   - Handling contract upgrades
   - Verifying signatures and authenticating transactions

3. Specification

3.1. System Actors

- **Signers**

  Entities who are authorized to sign transactions, participate in the management of the multi-sig wallet, and approve changes to the signer list or thresholds.

- **Initiator**

  The entity who creates the initial multi-sig wallet setup, defining the initial set of signers and thresholds.

3.2. Tokens

- None

3.3. Smart Contracts

3.3.1. Multi-sig validator

The Multi-sig Contract is the primary contract responsible for managing the list of authorized signers, validating transactions, and ensuring the proper execution of multi-sig operations. It facilitates the initialization of the multi-sig wallet, updating of signers, execution of transactions, and upgrading of the contract.

3.3.1.1. Parameters

- None

3.3.1.2. Spend Purpose

3.3.1.3. Datum

- **`signers`:** List of public key hashes of authorized signers.
- **`threshold`:** Minimum number of required signatures.
- **`funds`:** AssetClass of the funds to be withdrawn.
- **`funds_qty`:** The total amount of funds controlled by the contract
- **`spending_limit`:** Max Amount of funds to be withdrawn per transaction.

3.3.1.4. Redeemer

- Sign
- Update

3.3.1.5. Validation

1. **Common Checks (for both Sign and Update)**
   - Ensure the transaction is signed by at least the required number of authorized signers
   - Verify that the output value contains at least the input value (no unauthorized spending)

2. **Sign**

   The redeemer allows a majority of the authorized signers to collectively approve and execute transactions using the funds controlled by the multi-signature contract

   - Ensure the spent amount is within the spending_limit
   - Verify that the exact amount specified in the redeemer is being spent
   - Ensure the output datum matches the input datum (no changes to the multisig configuration)

3. **Update**

   The redeemer enables the modification of the multi-signature arrangement itself.

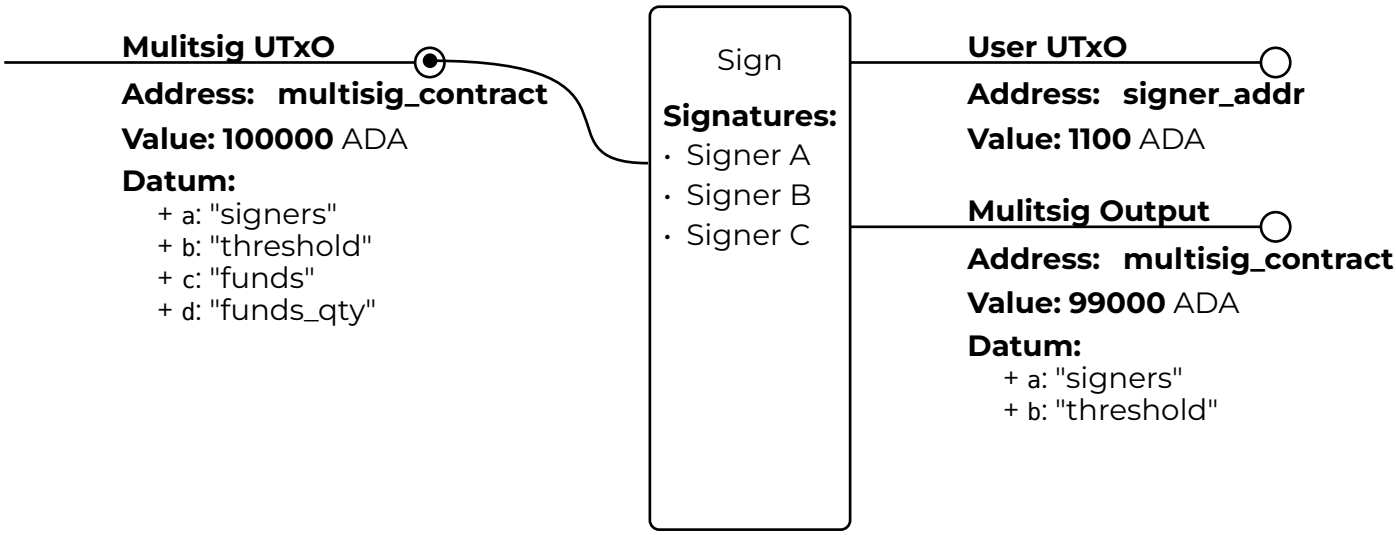
   - Enforce bounds on new signers list and threshold:
     - New signer count > 0
     - 0 < New threshold ≤ New signer count
     - New funds_qty ≥ 0
     - 0 ≤ New spending_limit ≤ New funds_qty
   - Ensure there are no duplicate keys in the new list of signers
   - Verify that input value equals output value (no spending during update)
   - Ensure the new configuration is stored in the output datum

4. Transactions

This section outlines the various transactions involved in the Upgradable Multi-Signature Contract on the Cardano blockchain.

4.1.1. Spend :: Sign

This action ensures that the number of signers meets or exceeds the specified threshold and The datum of the Multisig remains the same.



Note: Sign UTxO Diagram

4.1.1.1. Inputs

1. **Multisig Validator UTxO**
   - Address: Multisig validator script address
   - Datum:
     - `signers`
     - `threshold`
     - `funds`
     - `funds_qty`

.

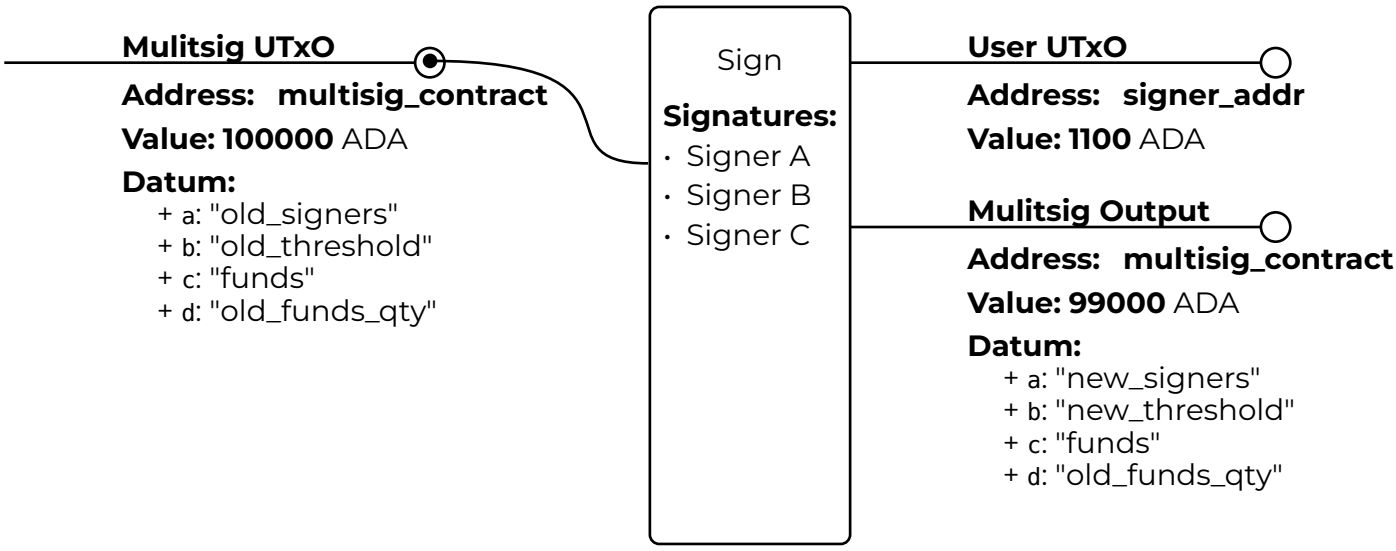
- Value:
  - ADA + Any tokens
  - Locked Value

4.1.1.2. Outputs

1. **Recipient Wallet UTxO**
   - Address: Recipient wallet address
     - Transferred ADA/tokens
2. **Multisig Validator UTxO:**
   - Address: Multisig validator script address
   - Datum:
     - `signers`
     - `threshold`
     - `funds`
     - `funds_qty`
   - Value:
     - Remaining ADA + Remaining tokens

4.1.2. Spend :: Update

Allows for the addition or removal of members from the Multisig arrangement, and updates the required signers threshold.



Note: Update UTxO Diagram

4.1.2.1. Inputs

1. **Multisig Validator UTxO**
   - Address: Multisig validator script address
   - Datum:
     - `old_signers`
     - `old_threshold`
     - `funds`
     - `old_funds_qty`
   - Value:
     - X ADA + Any tokens

4.1.2.2. Outputs

1. **Multisig Wallet UTxO**
   - Address: Merchant wallet address

- Datum:
  - `new_signers`
  - `new_threshold`
  - `funds`
  - `new_funds_qty`
- Value:
  - X ADA + Any tokens (unchanged)