ANASTASIA LABS

# Project Design Specification

| | |
|---|---|
| **Project Number** | 1000013 |
| **Project manager** | Philip DiSarro |
| **Date Started** | February 24, 2024 |
| **Date Completed** | ... |

# Contents

# Payment Subscription Smart Contract

## 1. Overview

This Payment Subscription Smart Contract is developed using Aiken to facilitate automated recurring payments between Subscribers and Merchants on the Cardano blockchain. This smart contract enables users to set up, manage, and cancel subscriptions directly from their wallets.

## 2. Architecture

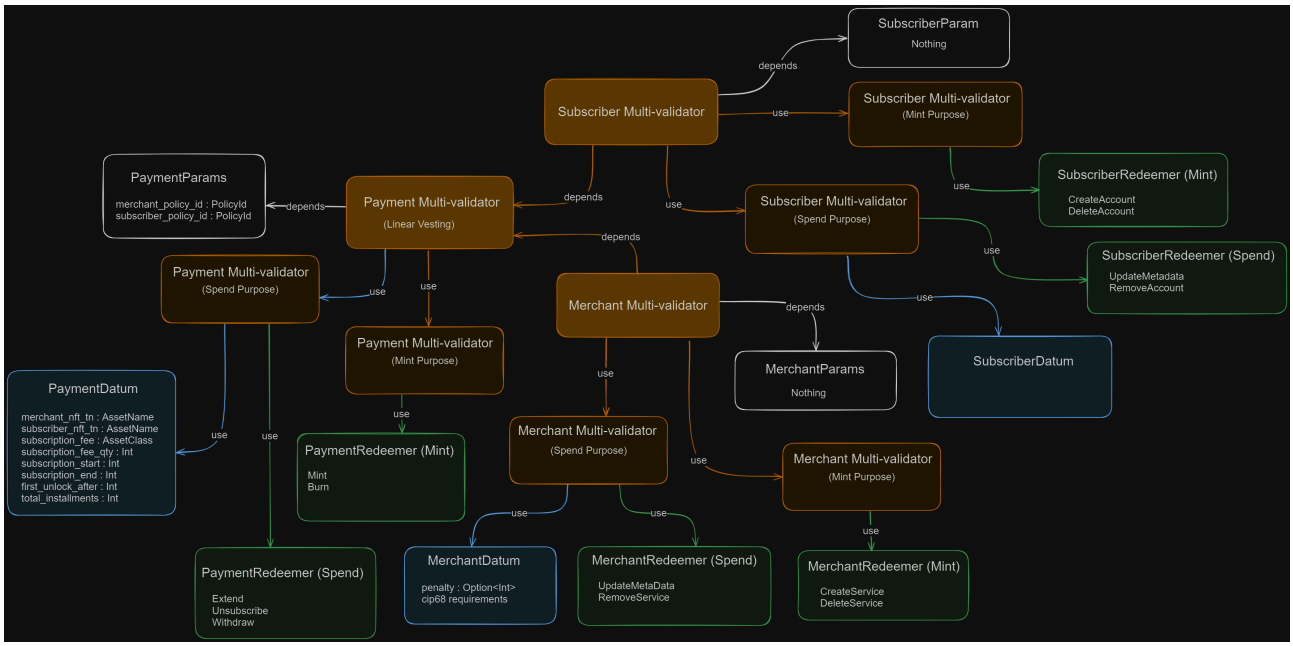


Figure 1: Payment Subscription Architecture

There are three contracts in this subscription system.

- **Merchant Contract:** A multi-validator responsible for creating an initial service by minting a single CIP-68 compliant MerchantNFT and sending it to the merchant while sending the reference NFT to the spending end point. It also updates the metadata for the merchant and deletes the service by burning the MerchantNFT.
- **Subscriber Contract:** A multi-validator responsible for creating the initial subscription to a service by minting a SubscriberNFT and sending it to the user, while sending the reference NFT to the spending endpoint. It also updates the metadata for the subscriber and deletes the user account by burning a SubscriberNFT.

- **Payments Contract:** Responsible for holding the prepaid subscription fees for a service, renewing a subscription to a service, unsubscribing from a service and withdrawing subscription fees. The contract incorporates a linear vesting mechanism to gradually release subscription fees to the merchant over the subscription period. This could also be a multi-validator to authenticate the UTxO.

# 3. Specification

## 3.1. System Actors

- **Merchant:** An entity who interacts with the Merchant Contract in order to create a service and receives subscription payments for the respective service or services. A user becomes a merchant when they mint a Merchant NFT.
- **Subscriber:** An entity who interacts with the Subscriber Contract in order to create an account and deposit prepaid subscription fees to the Payments Contract. A user becomes a subscriber when they mint a Subscribe NFT.

## 3.2. Tokens

- **Merchant NFT:** Can only be minted by a merchant when creating a subscription service and burned when merchant removes their service/services from the system. Datum is updated when a subscription is paid or the merchant withdraws from the Payments Contract.
  - TokenName: Defined in Merchant Multi-validator parameters with the hash of the Merchant Policy Id
- **Subscriber NFT:** Can only be minted when a subscription fee is paid to Payments Contract and burned when subscriber exits the system. Datum is updated when fees are deposited and withdrawn from Payments Contract.
  - TokenName: Defined in Subscriber Multi-validator parameters with hash of the Subscriber Policy Id

## 3.3. Smart Contracts

### 3.3.1. Payments Validator

The Payments Contract is responsible for managing the prepaid subscription fees, validating subscriptions, and ensuring the proper distribution of these fees over the subscription period. It facilitates the creation, extension, and cancellation of subscriptions, allowing both subscribers and merchants to interact with the contract in a secure and automated manner. This contract ensures that subscription payments are correctly handled and that any penalties for early cancellation are appropriately enforced.

#### 3.3.1.1. Parameters

- **`merchant_policy_id`** : Hash of the PolicyId
- **`subscriber_policy_id`** : Hash of the PolicyId

#### 3.3.1.2. Datum

This is a Sum type datum where one represents the main datum and the other one represents a penalty datum.

##### 3.3.1.2.1. Main datum

- **`merchant_nft_tn`:** Merchant's token name encoding UTxO to be consumed when minting the NFT.
- **`subscriber_nft_tn`:** Subscriber's token name encoding UTxO to be consumed when minting the NFT.
- **`subscription_fee`:** AssetClass type for the subscription fee.
- **`subscription_fee_qty`:** Amount of the subscription fee.
- **`subscription_start`:** Start of the subscription.
- **`subscription_end`:** Expiry time of the subscription.
- **`total_installments`:** The number of periodic intervals over which to release subscription fees.

##### 3.3.1.2.2. Penalty datum

- **`merchant_nft_tn`:** Merchant's token name encoding UTxO to be consumed when minting the NFT.

#### 3.3.1.3. Redeemer

- Extend
- Unsubscribe
- Withdraw

#### 3.3.1.4. Validation

- **Extend:** The redeemer will allow anyone to increase the subscription funds.
  - validate that the value of the UTxO is increased as long as the Datum is updated with the Merchant Token Name.
- **Unsubscribe:** The redeemer will allow anyone with a subscriberNFT to spend Subscribe UTxO to unlock funds back to their address.
  - validate the subscriberNFT is being spent.
  - validate that the penalty UTxO is being produced with the merchants Token Name.

- **Withdraw:** The redeemer will allow anyone with a merchantNFT to withdraw funds from the Payments contract
  - validate merchantNFT is being spent
  - validate whether the transaction contains a penalty datum or a normal datum.

#### 3.3.2. Merchant Multi-validator

Merchant Multi-validator is responsible for registering a service creating, updating and removing a service for a merchant.

##### 3.3.2.1. Parameter

Nothing

##### 3.3.2.2. Minting Purpose

###### 3.3.2.2.1. Redeemer

- CreateService
- RemoveAccount

###### 3.3.2.2.2. Validation

- **CreateService:** The redeemer allows creating of a new subscription sevice by minting only one unique Token.
  - validate that out_ref must be present in the Transaction Inputs
  - validate that the redeemer only mints a single CIP68 compliant merchant Token
- **RemoveAccount:**
  - validate that the redeemer only burns a single CIP68 compliant merchant NFT Token.

##### 3.3.2.3. Spend Purpose

###### 3.3.2.3.1. Datum

- `penalty_fee`: AssetClass type for the amount of fees to be deducted when subscriber cancels the subscription.
- `penalty_fee_qty`: Amount of the penalty fees.
- cip-68 requirements

#### 3.3.2.3.2. Redeemer

- UpdateMetaData
- RemoveService

##### 3.3.2.3.2.1. Validation

- **UpdateMetaData:** The redeemer allows for updating the metadata attached to the UTxO sitting at the script address.
  - validate that merchantNFT is being spent.
  - updates the metadata of the Reference NFT token and sends the token to the spending end point
- **RemoveService:** The redeemer allows the removal of a service by a merchant from the subscription system.
  - validate merchentNFT is being spent.
  - Removes all the Reference NFT tokens to another external address.

### 3.3.3. Subscriber Multi-validator

#### 3.3.3.1. Parameter

Nothing

#### 3.3.3.2. Minting Purpose

#### 3.3.3.2.1. Redeemer

- CreateAccount
- DeleteAccount

##### 3.3.3.2.1.1. Validation

- **CreateAccount:** The redeemer allows creating of a new subscription service account by minting only one unique Token.
  - validate that out_ref must be present in the Transaction Inputs
  - validate that the redeemer only mints a single CIP68 compliant SubscriberNFT Token
- **DeleteAccount:**
  - validate that the redeemer only burns a single CIP68 compliant SubscriberNFT Token

#### 3.3.3.3. Spend Purpose

##### 3.3.3.3.1. Datum

- cip-68 requirements

##### 3.3.3.3.2. Redeemer

- UpdateMetaData
- RemoveAccount

###### 3.3.3.3.2.1. Validation

- **UpdateMetaData:** The redeemer allows for updating the metadata attached to the UTxO sitting at the script address.
  - validate that SubscriberNFT is being spent.
  - updates the metadata of the Reference NFT token and sends the token to the spending end point.
- **RemoveAccount:** The redeemer allows the removal of an account by a subscriber from the subscription system.
  - validate that SubscriberNFT is being spent.
  - validate that unlocked funds are sent back to the subscriber address
  - validate that penalty is calculated accurately and fees are in the penalty UTxO
  - Removes all the Reference NFT tokens to athe spending endpoint.

# 4. Transactions

This section outlines the various transactions involved in the Payment Subscription Smart Contract on the Cardano blockchain.

## 4.1. Merchant Multi-validator

### 4.1.1. Mint :: CreateService

This transaction creates a new service by minting a Merchant NFT. This transaction is performed by the merchant to indicate that a new service is available.

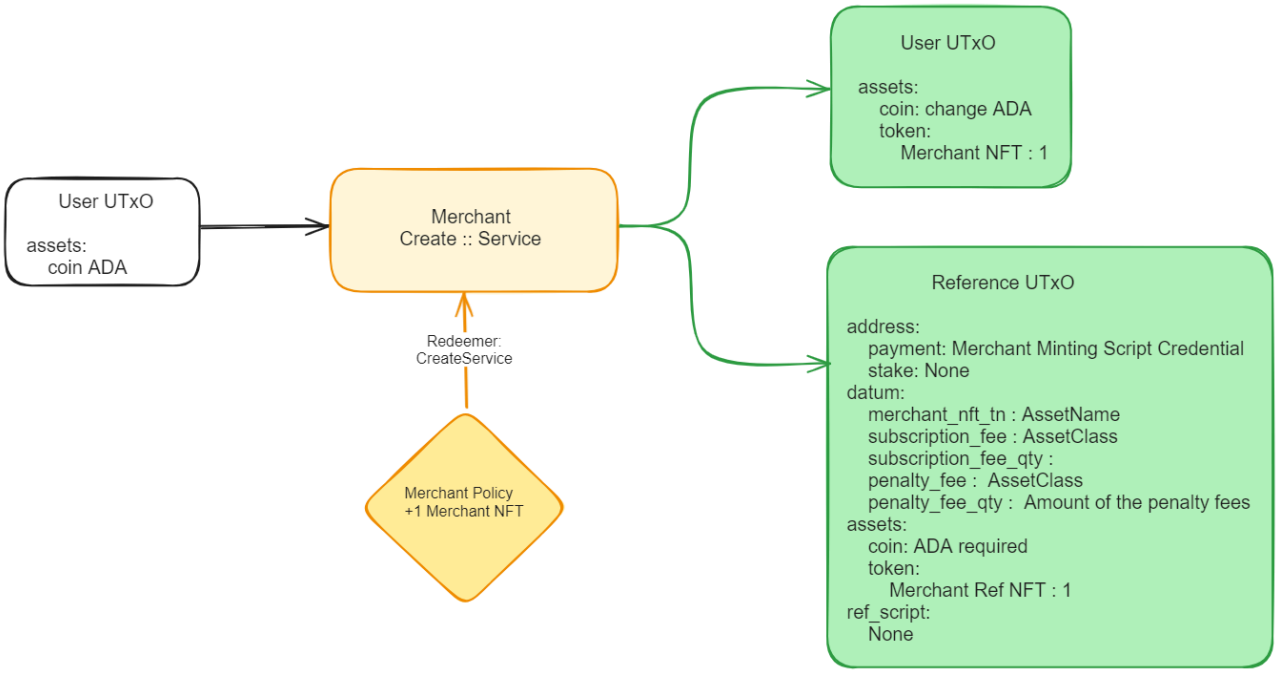


Figure 2: Create Service UTxO diagram

#### 4.1.1.1. Inputs

1. **Merchant Wallet UTxO.**
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA
     - Any additional ADA required for the transaction

#### 4.1.1.2. Outputs

1. **Merchant Wallet UTxO:**
   - Address: Merchant wallet address
   - Datum:
     - **`merchant_nft_tn`:** Merchant's token name encoding UTxO to be consumed when minting the NFT.
     - **`subscription_fee`:** AssetClass type for the subscription fee.
     - **`subscription_fee_qty`:** Amount of the subscription fee.
     - **`penalty_fee`**: AssetClass type for the amount of funds to be deducted when subscriber cancels the subscription.
     - **`penalty_fee_qty`**: Amount of the penalty fees.

- Value:
  - minimum ADA
  - 1 Merchant NFT Asset

2. **Merchant Validator UTxO:**
   - Address: Merchant Multi-validator Address (Mint)
   - Datum:
     - **`merchant_nft_tn`:** Merchant's token name encoding UTxO to be consumed when minting the NFT.
     - **`subscription_fee`:** AssetClass type for the subscription fee.
     - **`subscription_fee_qty`:** Amount of the subscription fee.
     - **`penalty_fee`**: AssetClass type for the amount of funds to be deducted when subscriber cancels the subscription.
     - **`penalty_fee_qty`**: Amount of the penalty fees.
   - Value:
     - 1 Reference NFT Asset

### 4.1.2. Mint :: DeleteService

This transaction deletes an existing service by burning the associated Merchant NFT by the merchant.

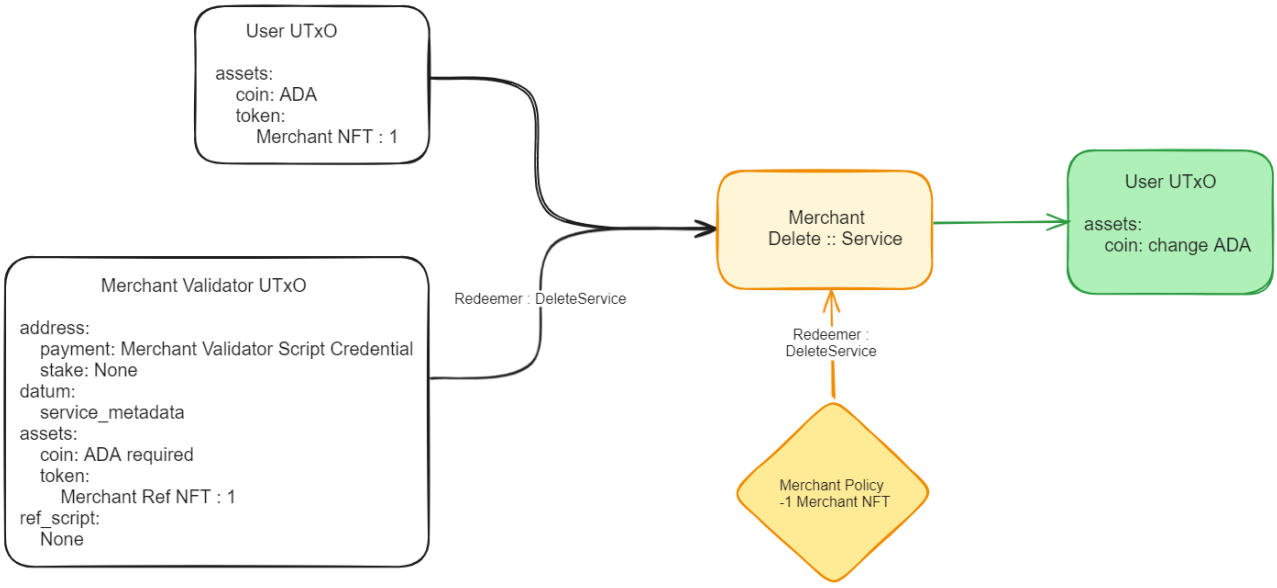


Figure 3: Delete Service UTxO diagram

#### 4.1.2.1. Inputs

1. **Merchant Wallet UTxO**
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA
     - 1 Merchant NFT Asset
2. **Merchant Validator UTxO**
   - Address: Merchant validator script address
   - Value:
     - Minimum ADA
     - 1 Reference NFT Asset

#### 4.1.2.2. Outputs

1. **Merchant Wallet UTxO**
   - Address: Merchant wallet address
   - Value:
     - Minimum ADA (remaining after burning the NFT)

### 4.1.3. Spend :: UpdateMetaData

This transaction updates the metadata attached to the UTxO at the script address, in accordance with CIP-68 standards. It consumes both the Merchant NFT and the Reference NFT, then sends the updated Merchant NFT to the user's wallet and the updated Reference NFT to the spending endpoint.

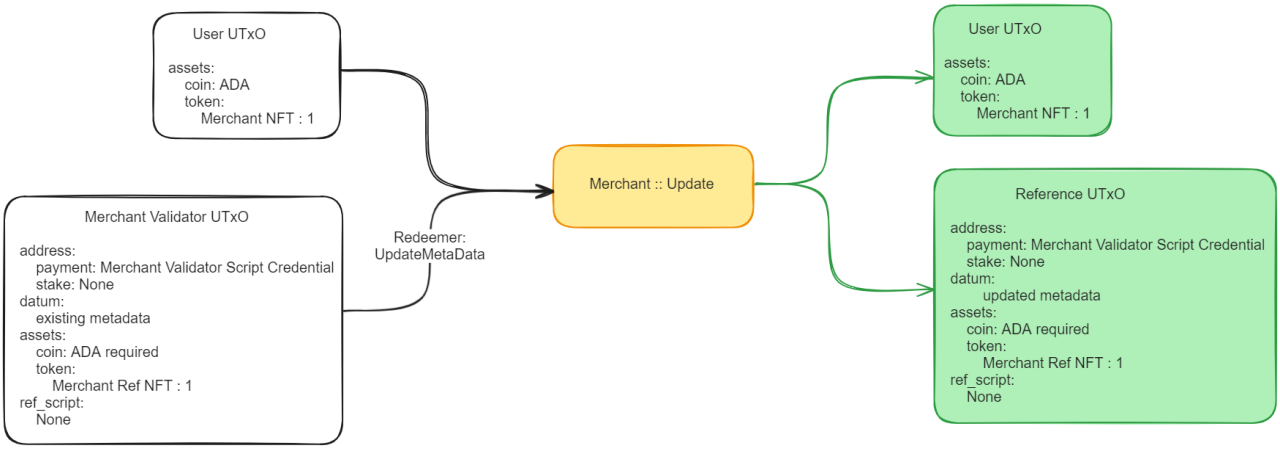


Figure 4: Update Merchant MetaData UTxO diagram

#### 4.1.3.1. Inputs

1. **Merchant Wallet UTxO**
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA
     - Merchant NFT Asset
2. **Merchant Validator UTxO**
   - Address: Merchant validator script address
   - Datum:
     - existing_metadata: Current metadata for the service.
   - Value:
     - Minimum ADA
     - Reference NFT Asset

#### 4.1.3.2. Outputs

1. **Merchant Wallet UTxO**
   - Address: Merchant wallet address
   - Datum:
     - updated_metadata: New metadata for the subscription.
   - Value:
     - Minimum ADA
     - Updated Merchant NFT Asset
2. **Merchant Validator UTxO:**
   - Address: Spending endpoint address
   - Datum:
     - updated_metadata: New metadata for the subscription.
   - Value:
     - Minimum ADA
     - 1 Updated Reference Merchant NFT Asset

#### 4.1.4. Spend :: RemoveService

This transaction spends the Reference UTxO with the Merchant NFT to remove the service.

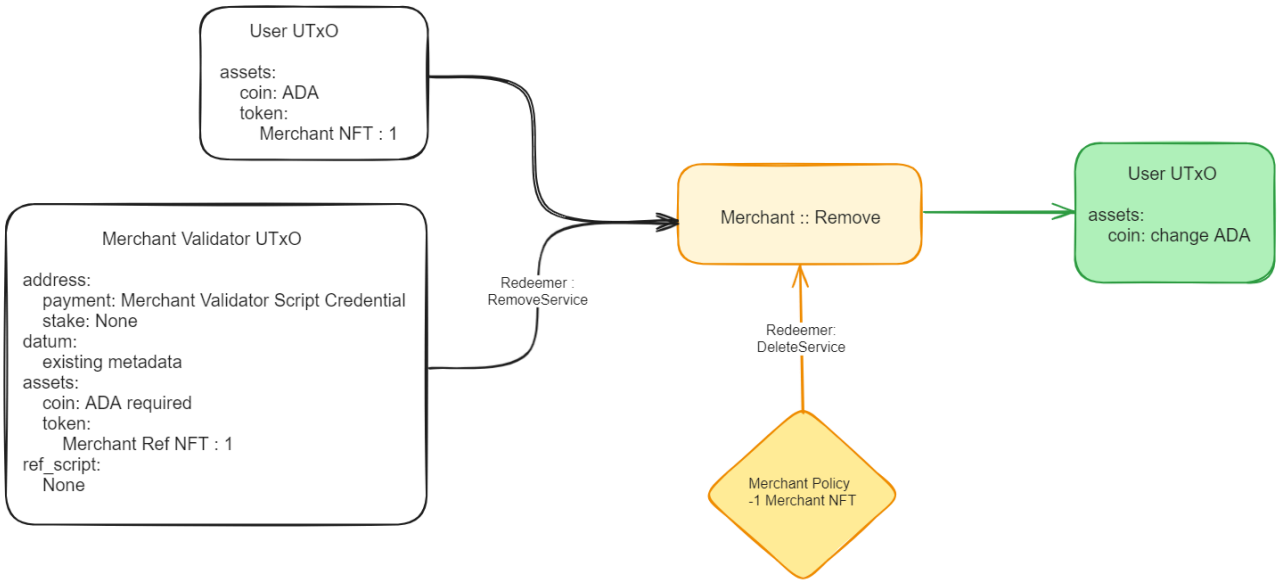


Figure 5: Remove Service UTxO diagram

##### 4.1.4.1. Inputs

1. **Merchant Wallet UTxO**
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA
     - Merchant NFT Asset
2. **Merchant Validator UTxO**
   - Address: Merchant validator script address
   - Datum:
     - service_metadata: Current metadata for the service.
   - Value:
     - Minimum ADA
     - Reference NFT Asset

##### 4.1.4.2. Mints

- Merchant Multi-validator
  - Redeemer: DeleteService
  - Value:
    - −1 Merchant NFT Asset
    - −1 Reference NFT Asset

#### 4.1.4.3. Outputs

1. **Merchant Wallet UTxO**
   - Address: Merchant wallet address
   - Value:
     - Minimum ADA (remaining after burning the NFT)

## 4.2. Subscriber Multi-validator

### 4.2.1. Mint :: CreateAccount

This endpoint mints a new subscription NFT for a subscriber, establishing a new subscription account. It transfers the subscription fee to the Payments Contract and provides the subscriber with a unique subscription token.

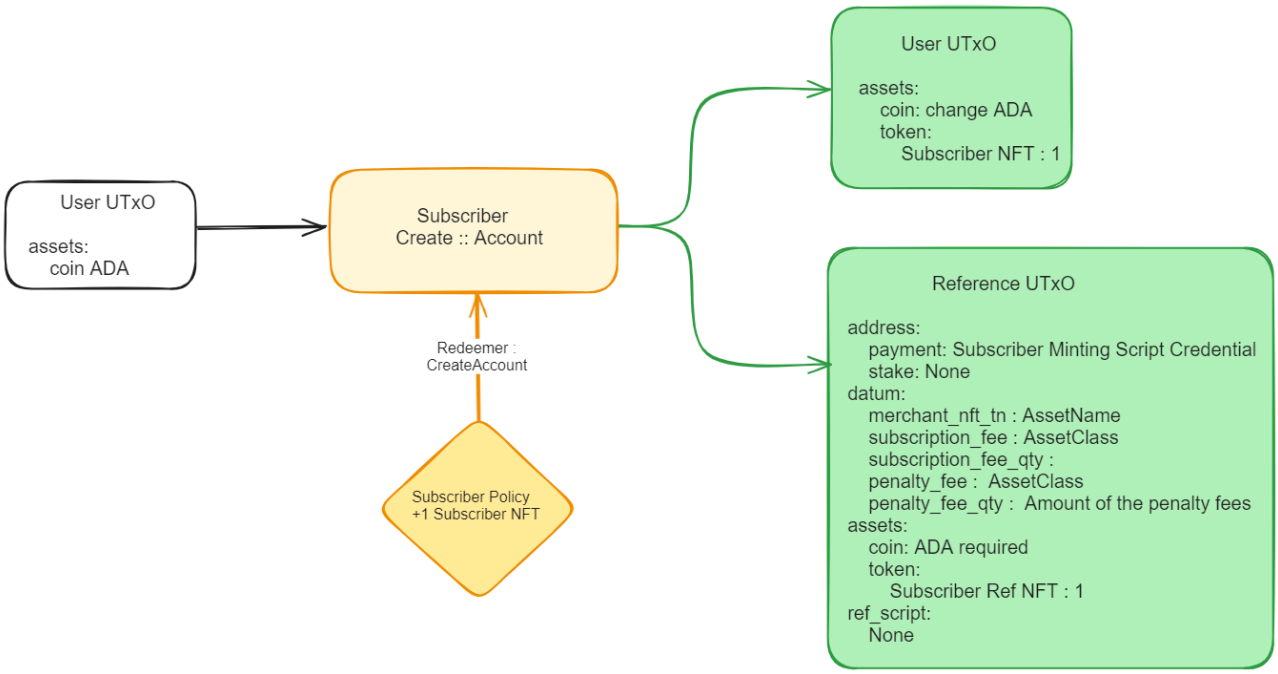


Figure 6: Create Account UTxO diagram

#### 4.2.1.1. Inputs

1. **Subscriber Wallet UTxO.**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Any additional ADA required for the transaction

#### 4.2.1.2. Outputs

1. **Subscriber Wallet UTxO:**
   - Address: Subscriber wallet address
   - Value:
     - minimum ADA
     - 1 Subscriber NFT Asset
2. **Subscriber Validator UTxO:**
   - Address: Merchant Multi-validator Address (Mint)
   - Datum:
     - **`subscription_token_name`:** Subscriber's token name encoding UTxO to be consumed when minting the NFT.
     - **`subscription_fee`:** AssetClass type for the subscription fee.
     - **`subscription_fee_qty`:** Amount of the subscription fee.
     - **`start_date`:** Subscription start date
     - **`end_date`:** Subscription end date
   - Value:
     - 1 Reference NFT Asset

### 4.2.2. Mint :: DeleteAccount

This endpoint burns the subscription NFT, effectively canceling the subscription. It deducts a penalty fee from the subscriber's balance and transfers it to the merchant.

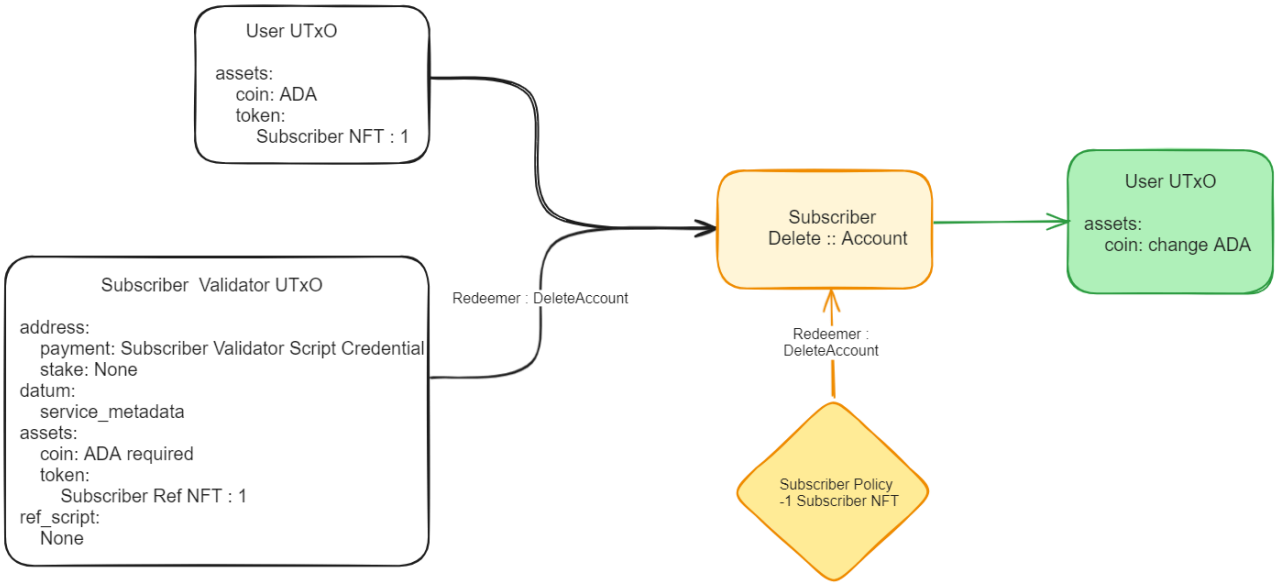


Figure 7: Delete Account UTxO diagram

#### 4.2.2.1. Inputs

1. **Subscriber UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - 1 Subscriber NFT Asset
2. **Subscriber Validator UTxO**
   - Address: Subscriber Multi-validator Address (Mint)
   - Datum:
     - subscriber_nft_tn: Subscriber's token name encoding UTxO to be consumed when burning the NFT.
     - subscription_fee: AssetClass type for the subscription fee.
     - subscription_fee_qty: Amount of the subscription fee.
     - penalty_fee: AssetClass type for the amount of funds to be deducted when - subscriber cancels the subscription.
     - penalty_fee_qty: Amount of the penalty fees.
   - Value:
     - 1 Reference NFT Asset

#### 4.2.2.2. Outputs

1. Subscriber Wallet UTxO:
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
2. Change UTxO:

   Any remaining ADA or other tokens from the transaction inputs that are not used in the transaction are returned to the subscriber's address as change.

### 4.2.3. Spend :: UpdateMetaData

This transaction updates the metadata attached to the subscriber UTxO at the script address. It consumes both the Subscriber NFT and the Reference NFT, then sends the updated Subscriber NFT to the user's wallet and the updated Reference NFT to the spending endpoint.

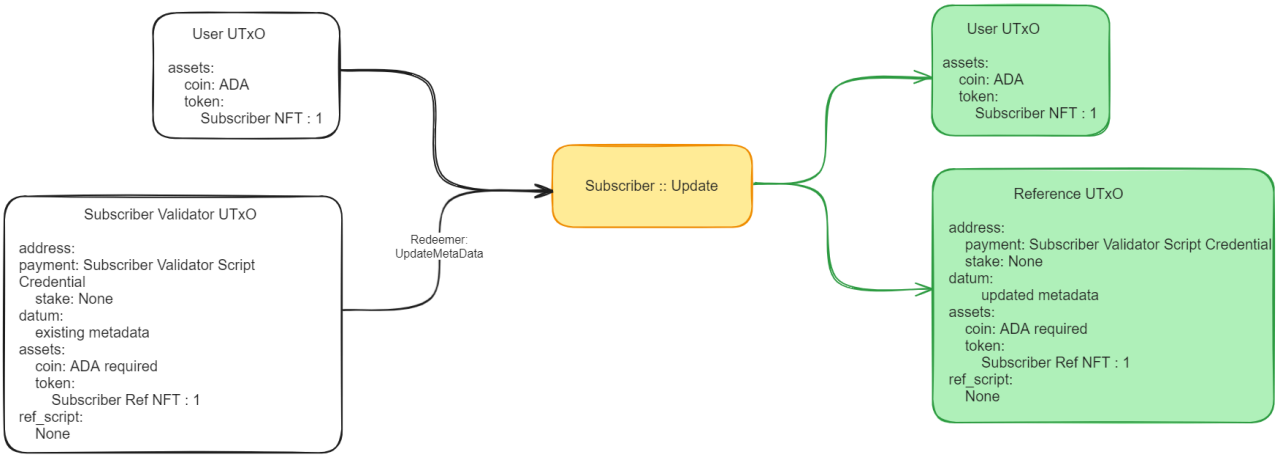


Figure 8: Update Subscriber Metadata UTxO diagram

#### 4.2.3.1. Inputs

1. **Subscriber UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Subscriber NFT Asset

2. **Subscriber Validator UTxO**
   - Address: Subscriber validator script addres
   - Datum:
     - existing_metadata: Current metadata for the Subscriber.
   - Value:
     - Minimum ADA
     - 1 Reference NFT Asset

#### 4.2.3.2. Outputs

1. **Subscriber UTxO**
   - Address: Subscriber's wallet address
   - Datum:
     - updated_metadata: New metadata for the subscriber
   - Value:
     - Minimum ADA
     - Updated Subscriber NFT Asset
2. **Subscriber Validator UTxO**
   - Address: Subscriber validator script address
   - Datum:
     - updated_metadata: New metadata for the subscriber
   - Value:
     - Minimum ADA
     - Updated Reference NFT Asset

### 4.2.4. Spend :: RemoveAccount

This transaction effectively terminates the subscription and removes the subscriber's account from the system by consuming the Subscriber NFT and the Reference NFT. The inputs include a UTxO from the subscriber's wallet containing the Subscriber NFT and a UTxO from the Merchant Multi-validator containing the Reference NFT and relevant metadata. The outputs return the minimum ADA to the merchant's wallet and any remaining ADA or other tokens to the subscriber's wallet.

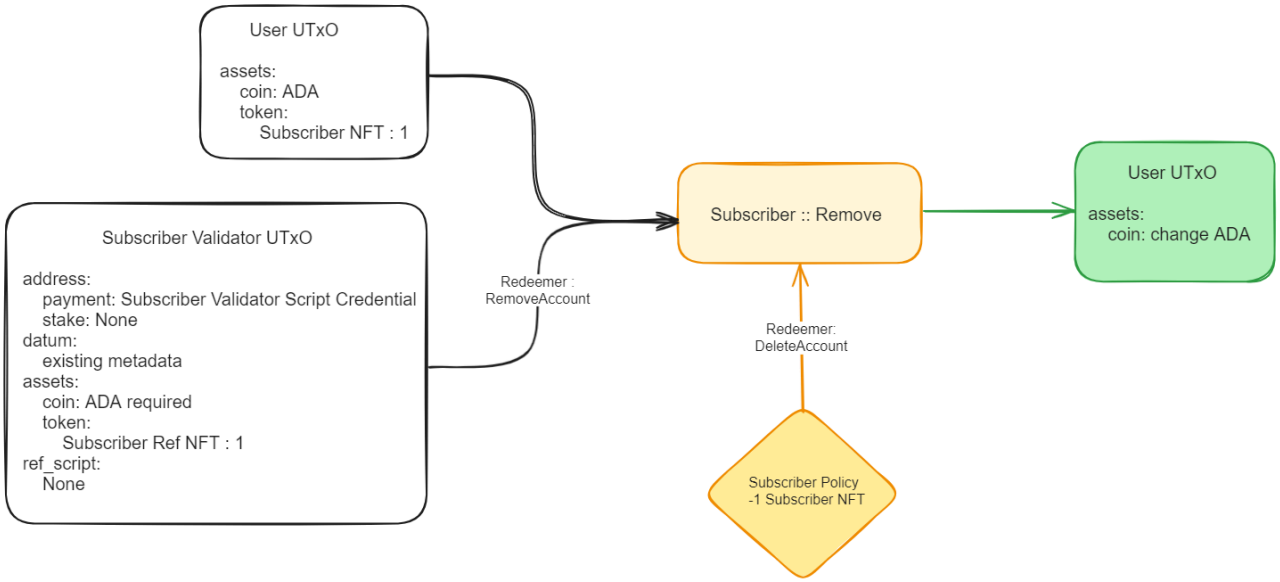


Figure 9: Remove Account Metadata UTxO diagram

#### 4.2.4.1. Inputs

1. **Subscriber Wallet UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Subscriber NFT Asset
2. **Subscriber Policy UTxO**

- Address: Merchant Multi-validator Address (Spend)
- Datum:
  - merchant_nft_tn: Merchant's token name encoding UTxO to be consumed when spending the NFT.
  - subscription_fee: AssetClass type for the subscription fee.
  - subscription_fee_qty: Amount of the subscription fee.
  - penalty_fee: AssetClass type for the amount of funds to be deducted when subscriber - cancels the subscription.
  - penalty_fee_qty: Amount of the penalty fees.
- Value:
  - Minimum ADA
  - 1 Reference NFT Asset

#### 4.2.4.2. Outputs

1. **Merchant UTxO**
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA (remaining after burning the NFT)
2. **Subscriber Validator UTxO**
   - Address: Subscriber Validator address
   - Datum: None
   - Value:None
3. **Change UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Remaining ADA and other tokens, if any

## 4.3. Payments Validator

### 4.3.1. Spend :: Extend

This transaction allows subscribers to extend their subscription period by adding more funds to cover additional time.

#### 4.3.1.1. Inputs

1. **Subscriber Wallet UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Subscription Token Asset (if any additional ADA is required)
2. **Payments Validator UTxO**
   - Address: Payments validator script address
   - Datum:
     - current_datum: Current metadata for the subscription
   - Value:

- Minimum ADA
- Reference NFT Asset

#### 4.3.1.2. Outputs

1. **Subscriber Wallet UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Subscription Token Asset (if applicable)
2. **Payments Validator UTxO**
   - Address: Payments validator script address
   - Datum:
     - updated_datum: Updated metadata with extended subscription details
   - Value:
     - Increased ADA to cover the extended subscription period
     - Reference NFT Asset

### 4.3.2. Spend :: Unsubscribe

#### 4.3.2.1. Inputs

1. **Subscriber Wallet UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Subscriber NFT Asset
2. **Payments Validator UTxO**
   - Address: Payments validator script address
   - Datum:
     - current_datum: Current metadata for the subscription
   - Value:
     - Minimum ADA
     - Reference NFT Asset

#### 4.3.2.2. Outputs

1. **Subscriber Wallet UTxO**
   - Address: Subscriber's wallet address
   - Value:
     - Minimum ADA
     - Unspent portion of the subscription fee (minus any penalties)
     - Subscription Token Asset (if applicable)
2. **Payments Validator UTxO**
   - Address: Payments validator script address
   - Datum:
     - penalty_datum: Metadata indicating the penalty for early unsubscription
   - Value:
     - Minimum ADA
     - Penalty Reference NFT Asset (if applicable)

#### 4.3.3. Spend :: Withdraw

The Withdraw endpoint allows merchants to withdraw accumulated subscription fees from the contract.

##### 4.3.3.1. Inputs:

1. Merchant Wallet UTxO
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA
     - Merchant NFT Asset
2. Payments Validator UTxO
   - Address: Payments validator script address
   - Datum:
     - current_datum: Current metadata for the subscription
   - Value:
     - Minimum ADA
     - Reference NFT Asset

##### 4.3.3.2. Outputs:

1. Merchant Wallet UTxO
   - Address: Merchant's wallet address
   - Value:
     - Minimum ADA
     - Withdrawn subscription fee portion
     - Merchant NFT Asset
2. Payments Validator UTxO
   - Address: Payments validator script address
   - Datum:
     - updated_datum: Metadata reflecting the withdrawal
   - Value:
     - Remaining ADA after withdrawal
     - Reference NFT Asset