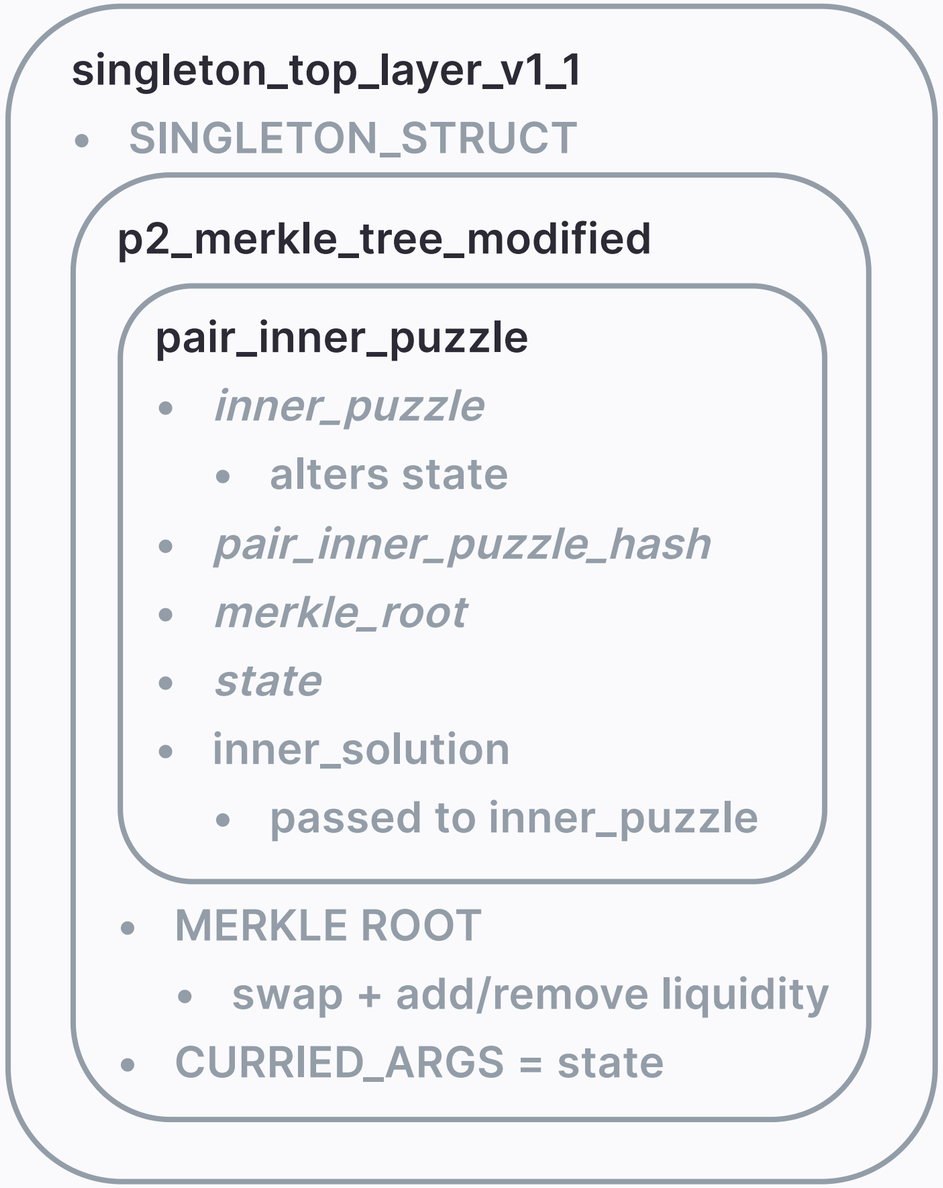
yakuhito

XCH London

The Magic Behind TibetSwap

April 28th, 2023


singleton_top_layer_v1_1
SINGLETON_STRUCT
p2_merkle_tree_modified
pair_inner_puzzle
inner_puzzle
alters state
pair_inner_puzzle_hash
merkle_root
state
inner_solution
passed to inner_puzzle
MERKLE ROOT
swap + add/remove liquidity
CURRIED_ARGS = state

Agenda

Core Concepts

1. CATs
2. Singletons
3. Pay to Singleton
4. Offers
5. Pay to Merkle Tree

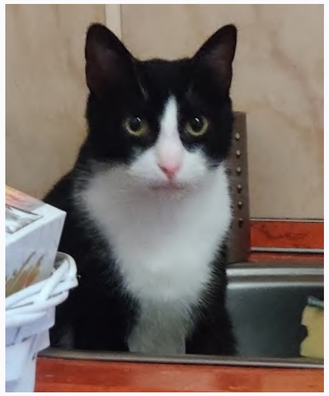
TibetSwap

1. Specs
2. Example: Swap

The End

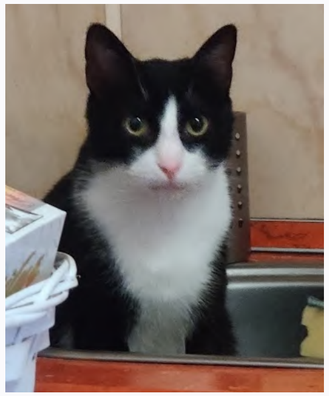
CATs

chialisp.com/cats

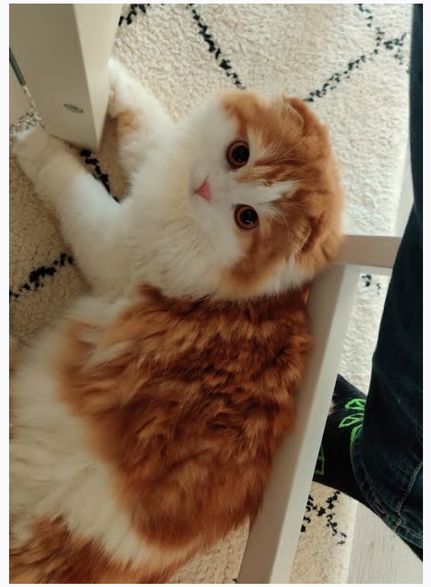


Amount: 500

Amount: 200



Amount: 300

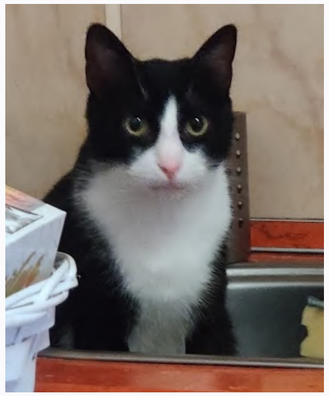


Amount: 1000

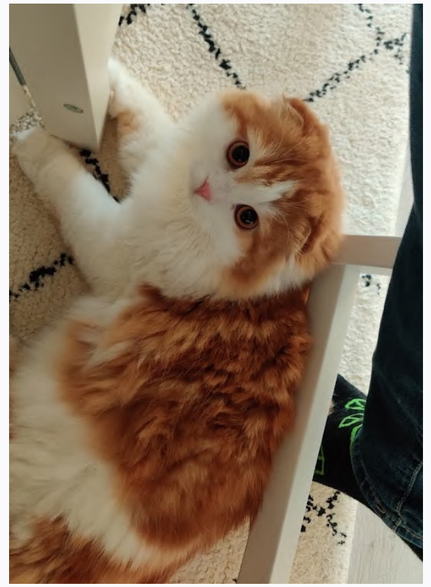
Amount: 500

"Ring"

Amount: 200



Amount: 300



Amount: 1000

But where do CATs come from, really?

TAIL

Token and Asset Issuance Limitations

But where do CATs come from, really?

TAIL

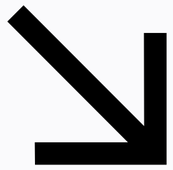
Token and Asset Issuance Limitations

Puzzles:

- genesis_by_coin_id
- everything_with_signature
- delegated_tail
- custom (!)

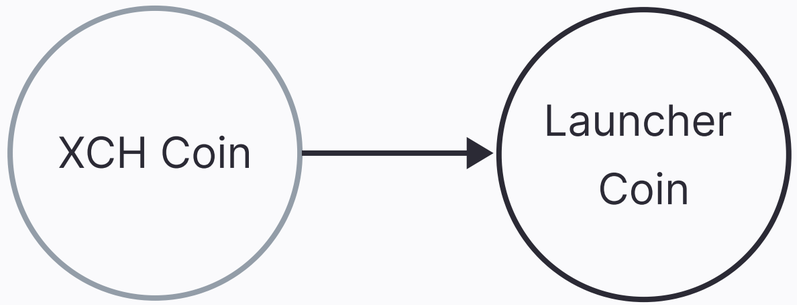
Singletons

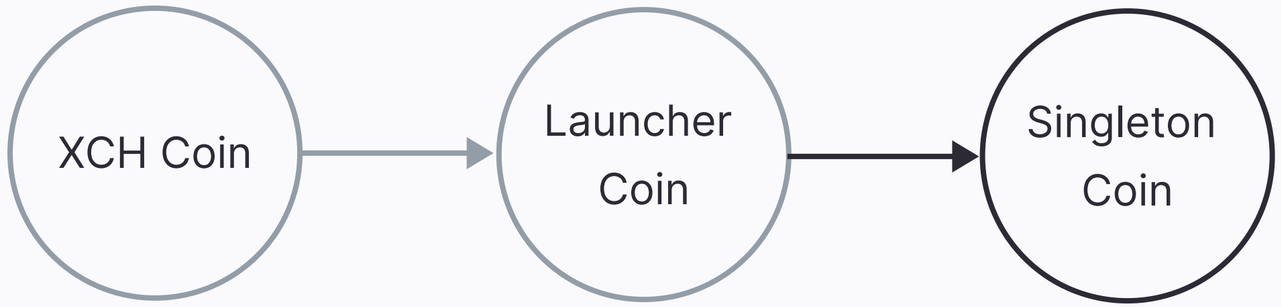
chialisp.com/singletons



Checklist

- ☐ My parent is either the launcher or has the same singleton top layer
- ☐ The inner puzzle produced one odd CREATE_COIN condition



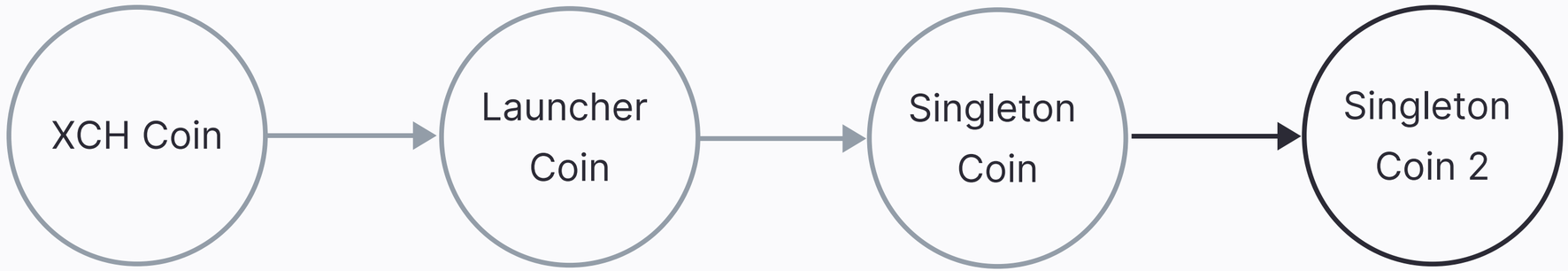


Always creates only one coin

→ launcher id is unique

Wraps odd coin from inner_puzzle

→ ensures 'soul' is passed on



Always creates only one coin

→ launcher id is unique

Wraps odd coin from inner_puzzle
→ ensures 'soul' is passed on

Always creates only one coin
→ launcher id is unique

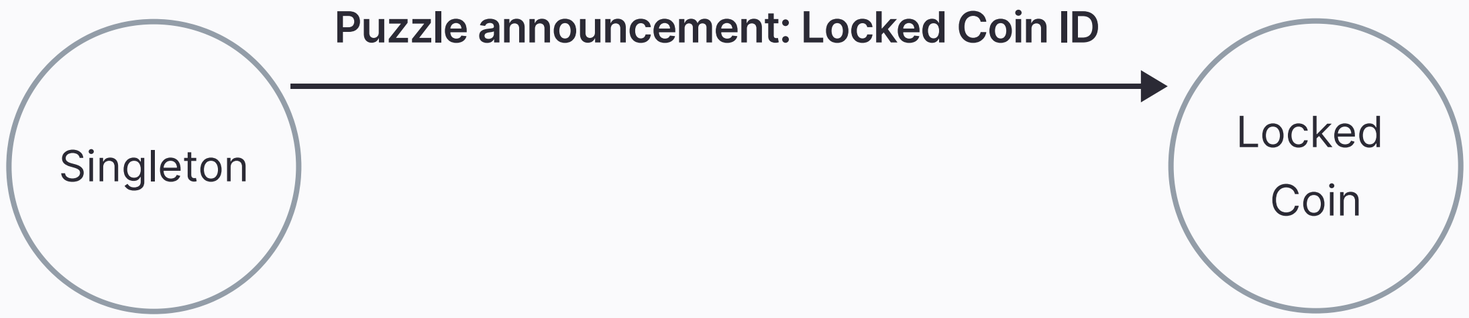
Inner puzzle wants to melt (-113)
→ remove invalid condition, melt

Pay to Singleton

chialisp.com/singletons/#pay-to-singleton

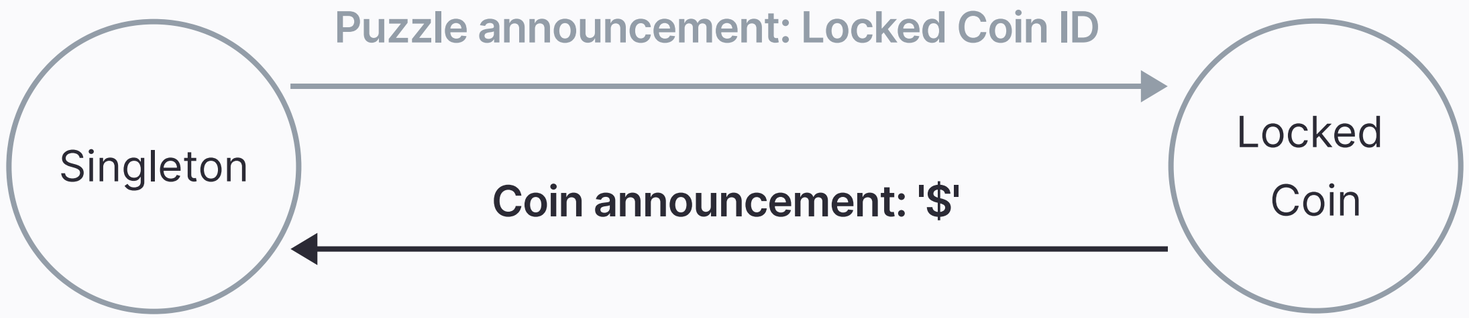
Computing a singleton's puzzle hash requires:

- Singleton module hash
- Launcher puzzle hash
- Launcher ID
- Inner puzzle hash



Computing a singleton's puzzle hash requires:

- Singleton module hash
- Launcher puzzle hash
- Launcher ID
- Inner puzzle hash

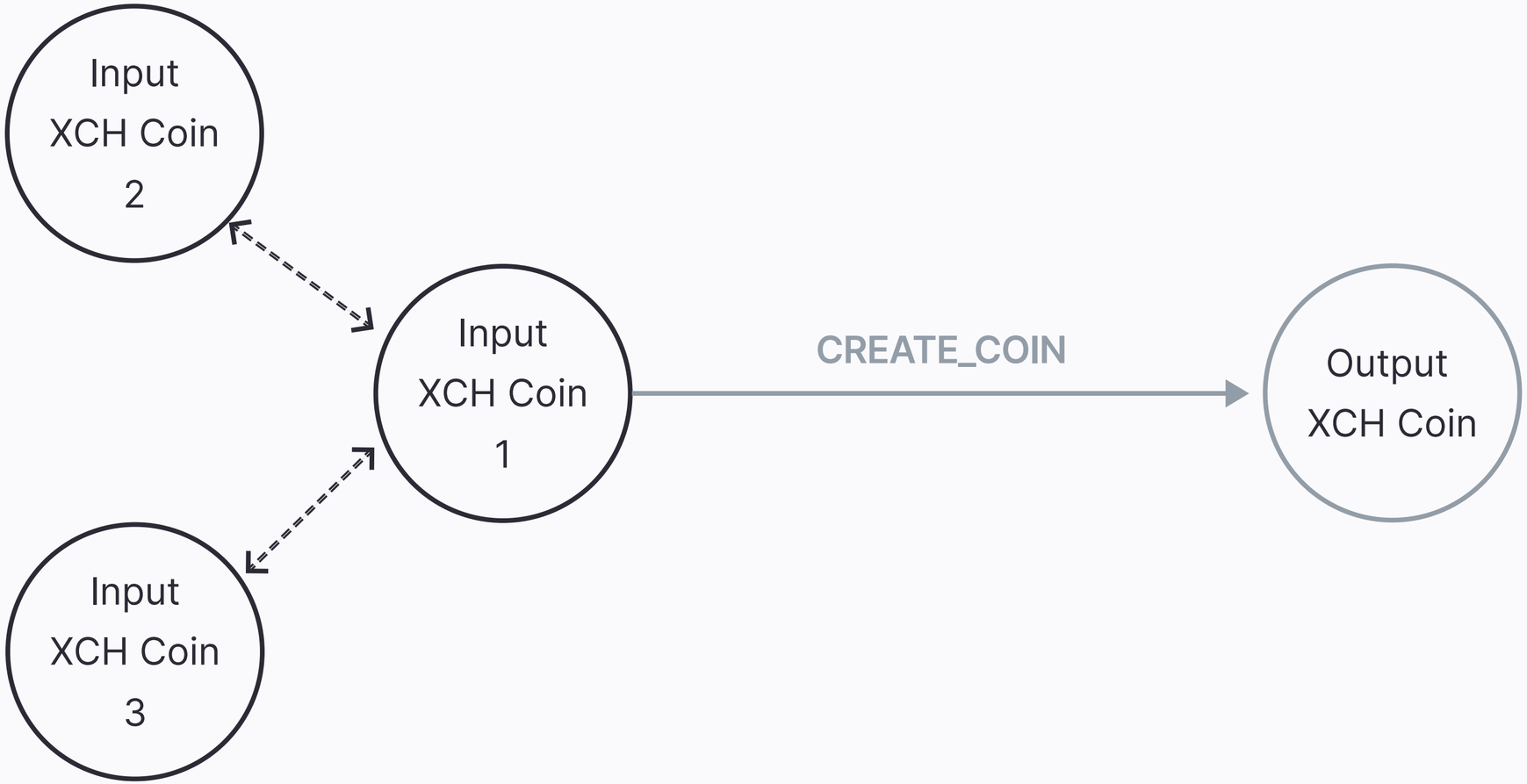


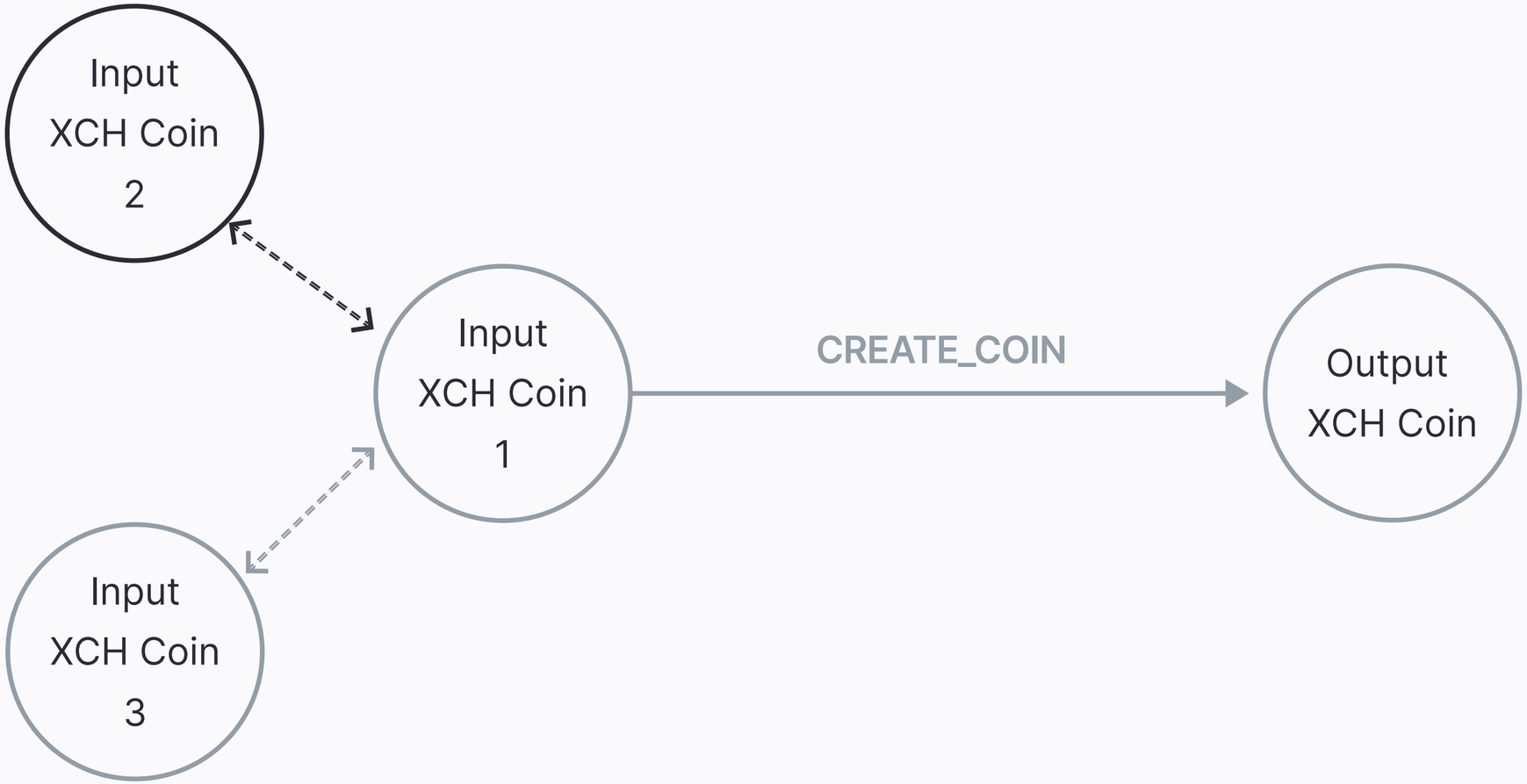
Computing a singleton's puzzle hash requires:

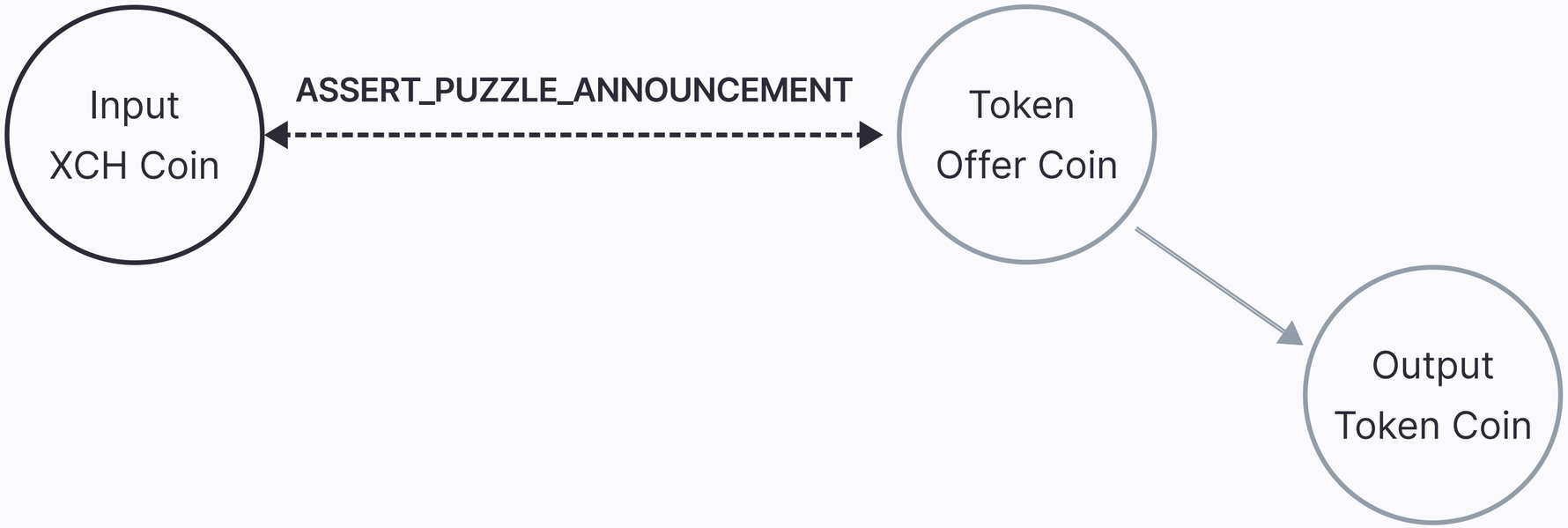
- Singleton module hash
- Launcher puzzle hash
- Launcher ID
- Inner puzzle hash

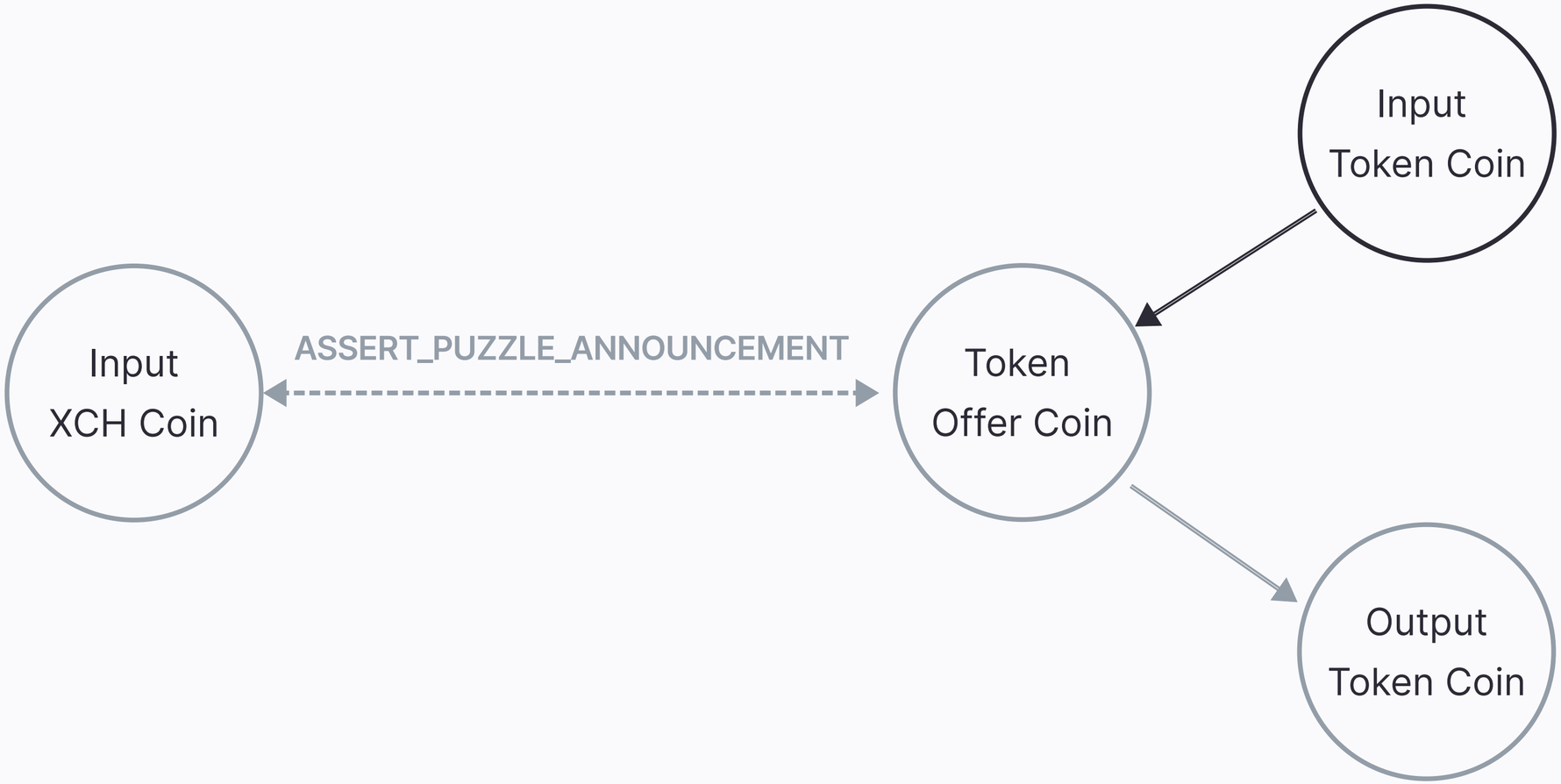
Offers

chialisp.com/offers


Input
XCH Coin
2
Input
XCH Coin
1
Input
XCH Coin
3
CREATE_COIN
Output
XCH Coin

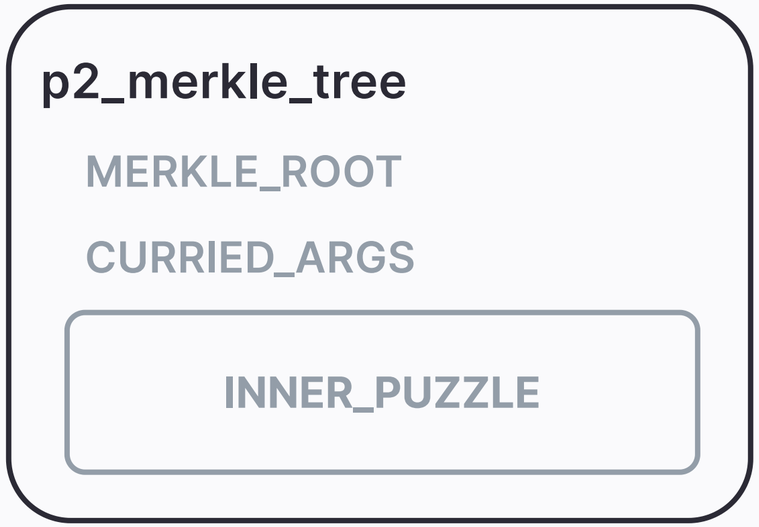

Input
XCH Coin
2
Input
XCH Coin
1
Input
XCH Coin
3
CREATE_COIN
Output
XCH Coin

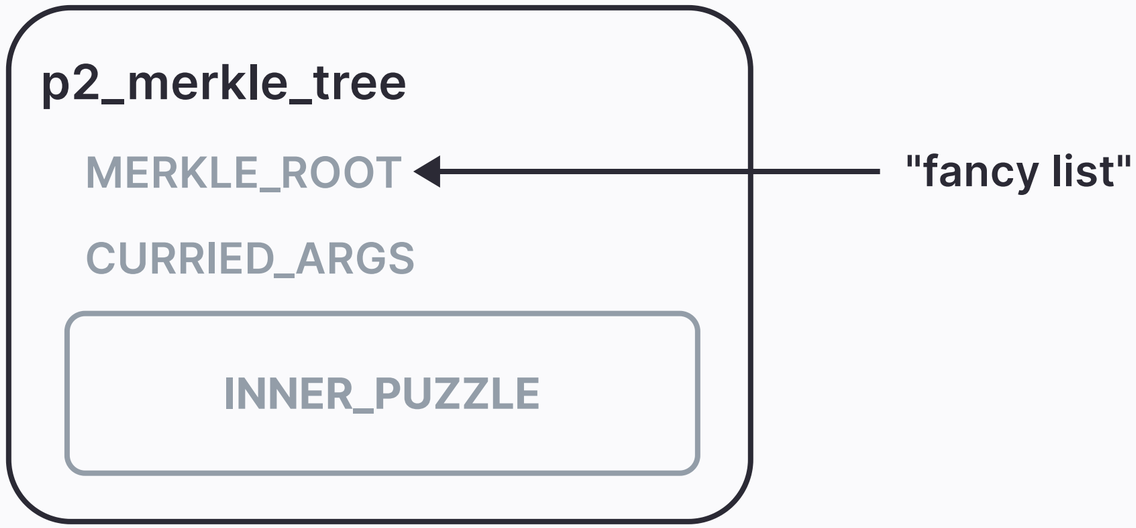

Input
XCH Coin
ASSERT_PUZZLE_ANNOUNCEMENT
Token
Offer Coin
Output
Token Coin

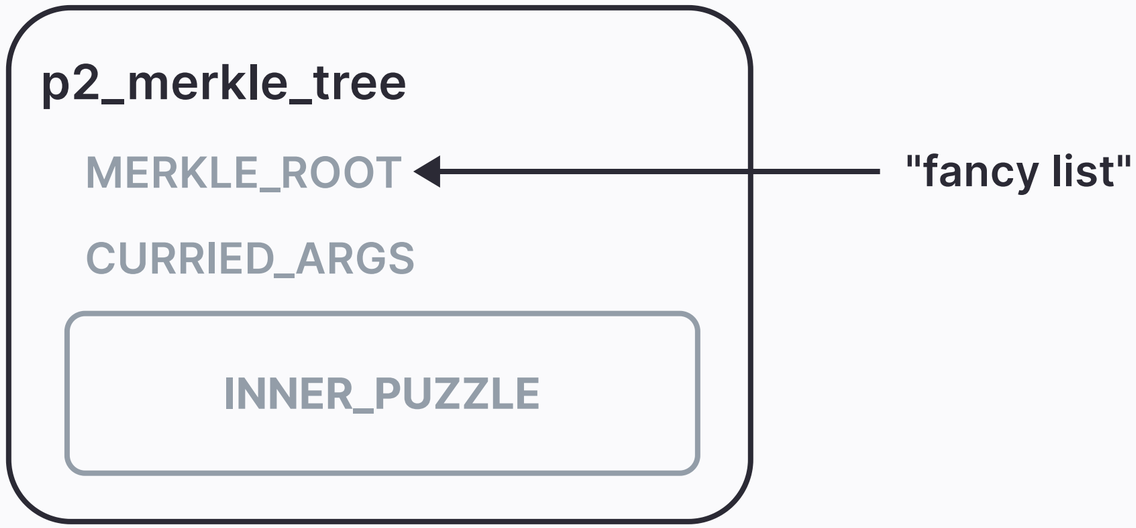

Input
Token Coin
Input
XCH Coin
ASSERT_PUZZLE_ANNOUNCEMENT
Token
Offer Coin
Output
Token Coin

Pay to Merkle Tree

github.com/Chia-Network/internal-custody/blob/main/cic/clsp/drop_coins/p2_merkle_tree.clsp



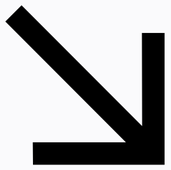

p2_merkle_tree
MERKLE_ROOT
CURRIED_ARGS
INNER_PUZZLE
"fancy list"



Run INNER_PUZZLE with:

- one item from Merkle Tree
- CURRIED_ARGS
- args from solution

Specs



Requirements:

Requirements:

- **Functions:** swap, add liquidity, remove liquidity

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and

to have a simple way of tracking pairs)

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and to have a simple way of tracking pairs)

Solutions:

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and to have a simple way of tracking pairs)

Solutions:

singleton

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and to have a simple way of tracking pairs)

Solutions:

p2_merkle_tree

singleton

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and to have a simple way of tracking pairs)

Solutions:

p2_merkle_tree

singleton = 'brain'

p2_singleton, offers

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and to have a simple way of tracking pairs)

Solutions:

p2_merkle_tree

singleton = 'brain'

p2_singleton, offers custom TAIL

Requirements:

- **Functions:** swap, add liquidity, remove liquidity
- **A state:** liquidity, XCH in reserve, token in reserve
- **Reserves:** XCH and token
- **Liquidity tokens** for each pair
- To be able to **deploy** a pair for any token (and to have a simple way of tracking pairs)

Solutions:

p2_merkle_tree

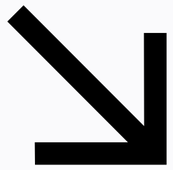
singleton = 'brain'

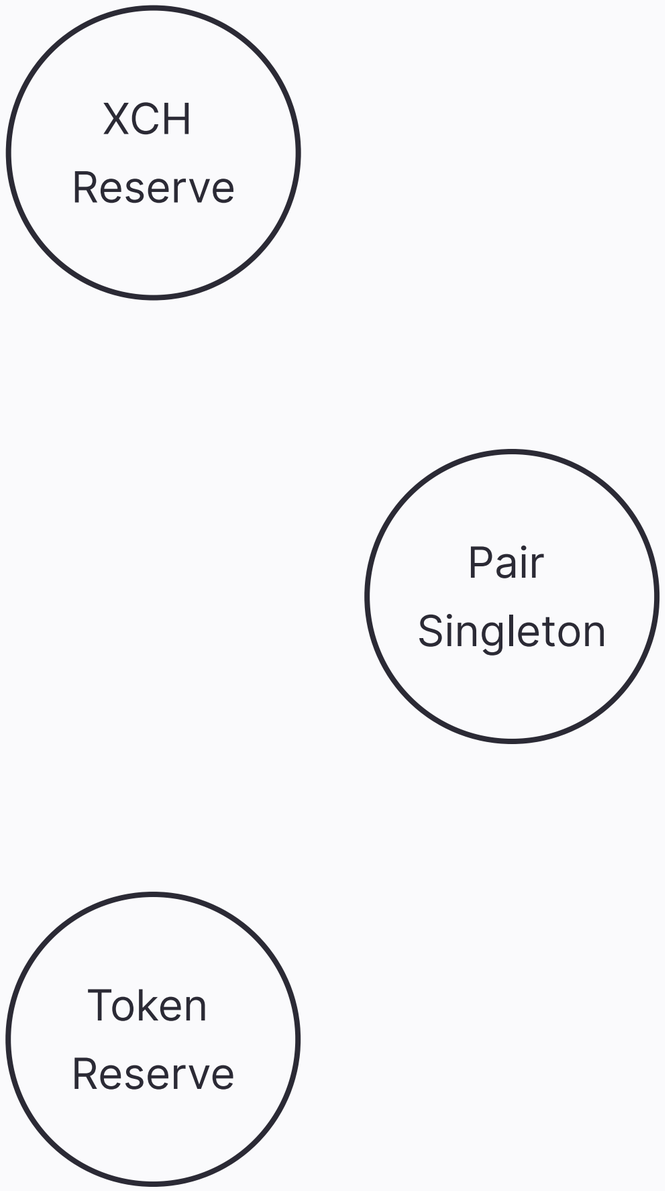
p2_singleton, offers

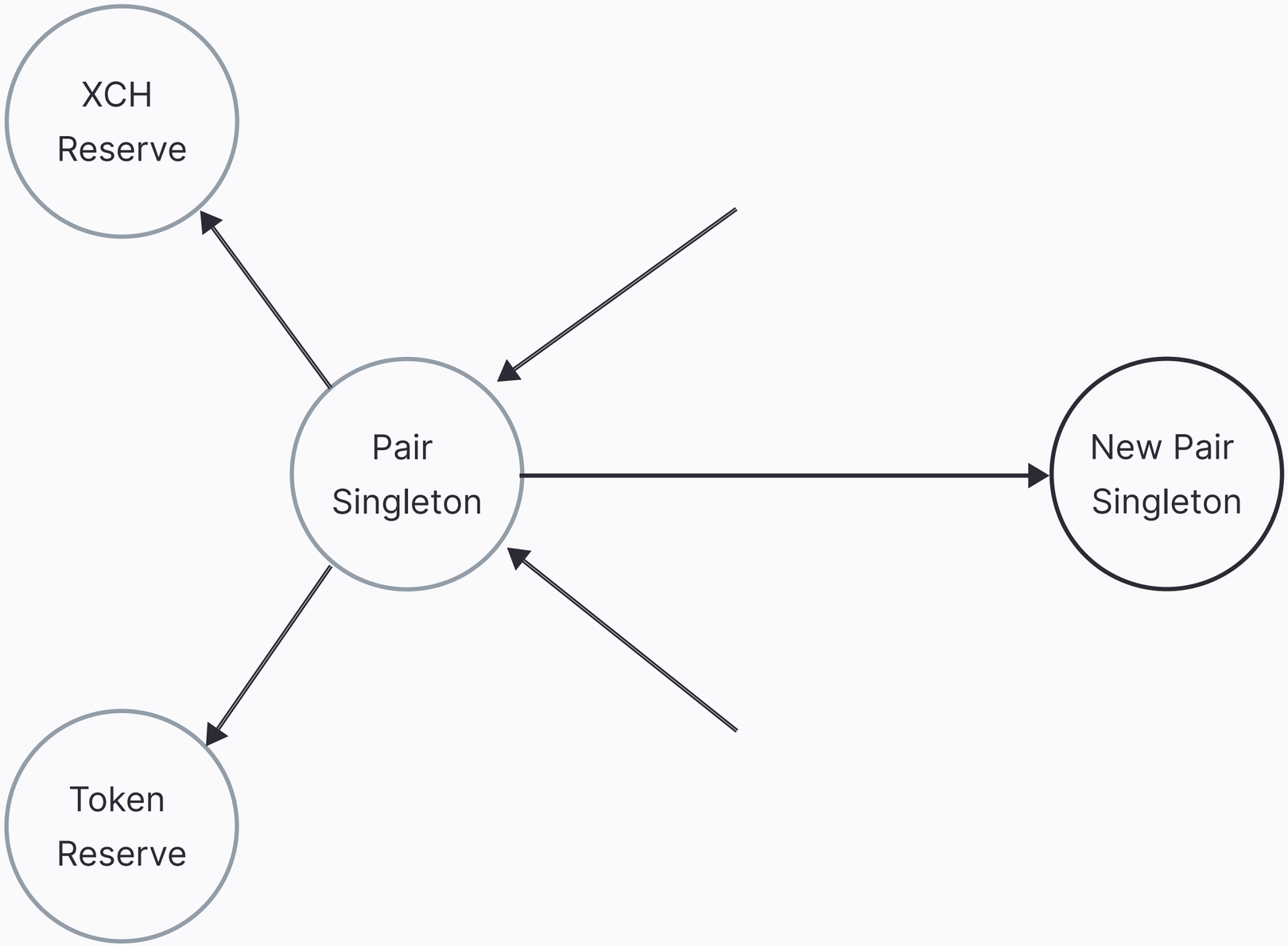
custom TAIL

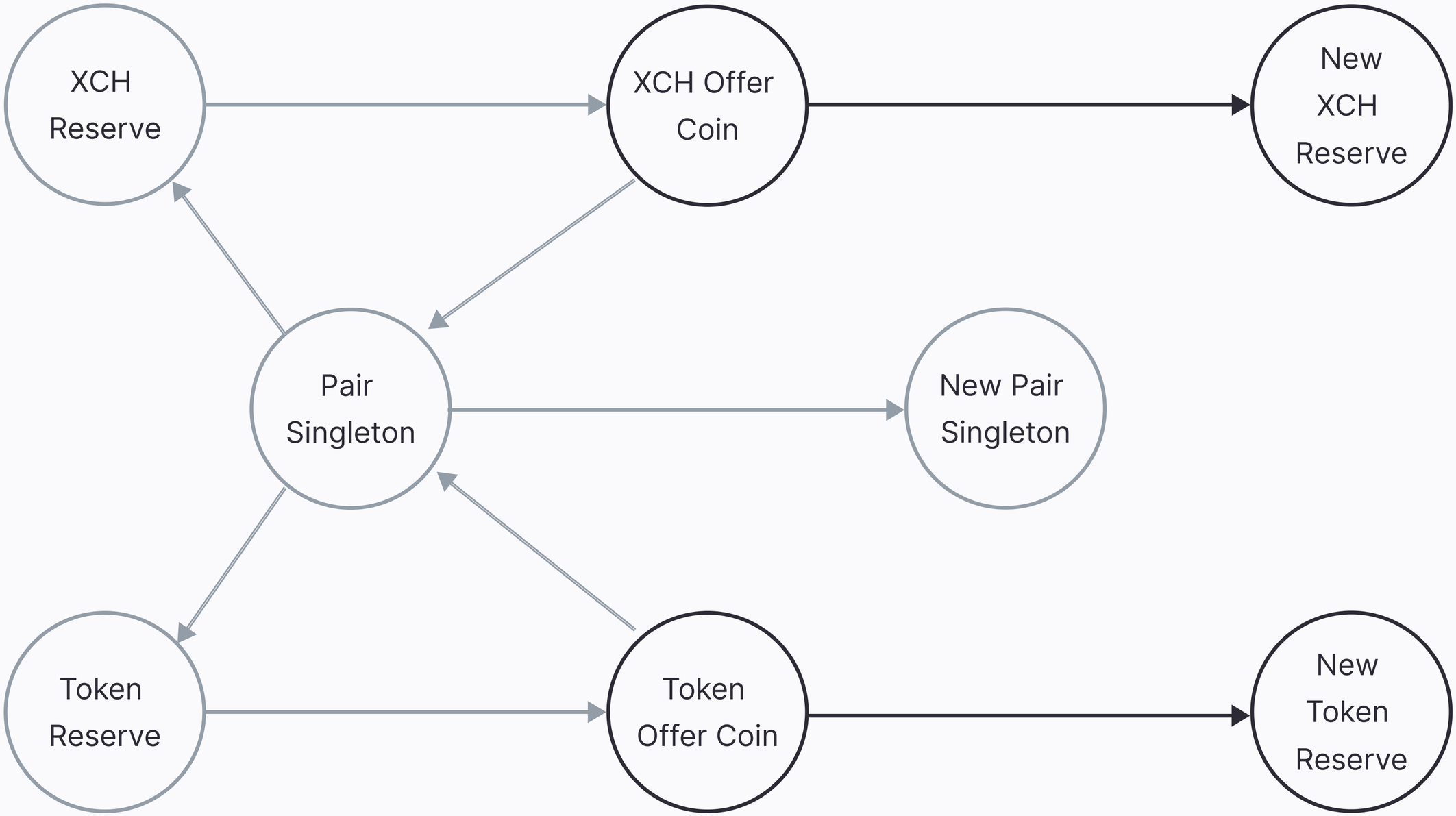
router

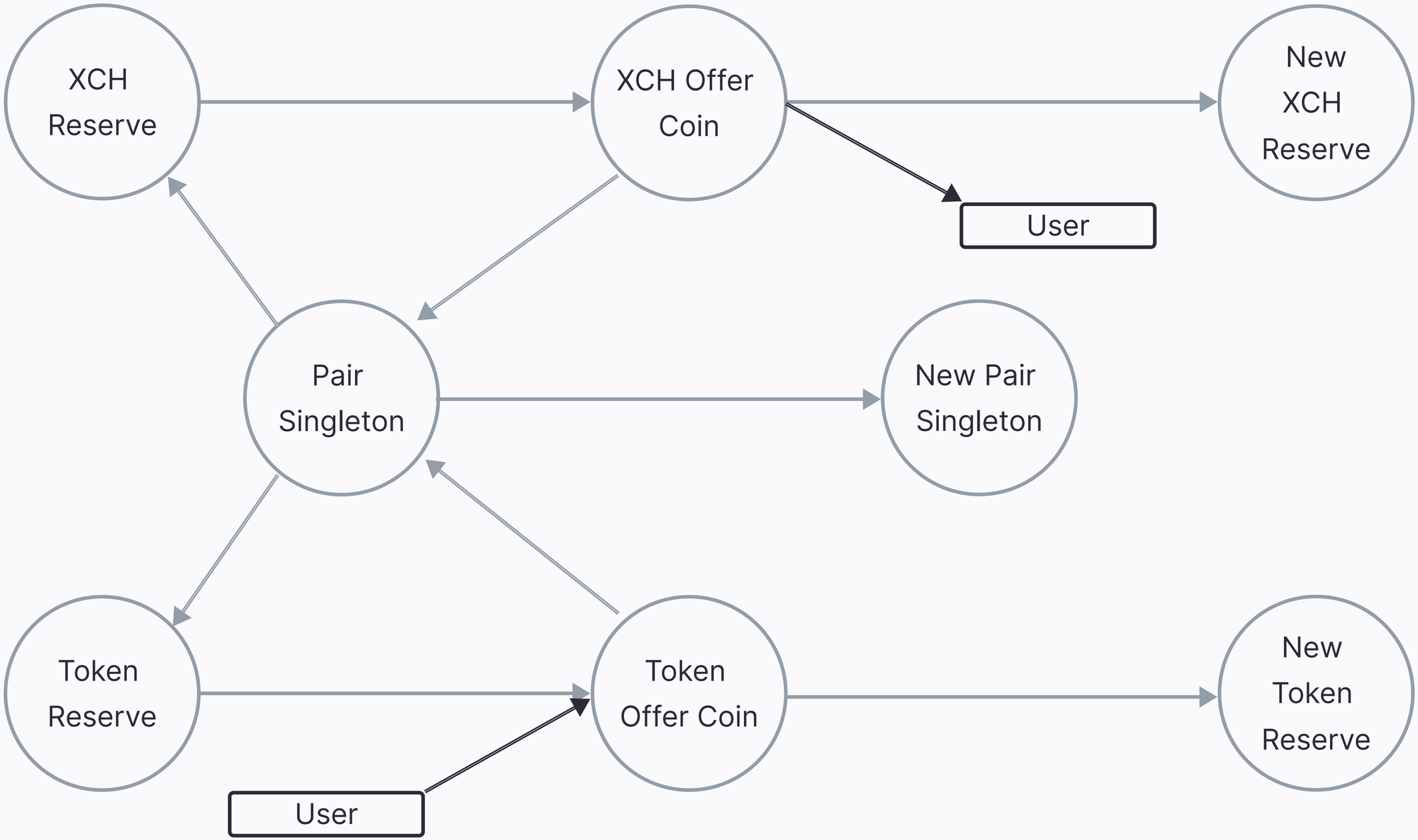
Example: Swap






XCH
Reserve
Pair
Singleton
New Pair
Singleton
Token
Reserve


XCH
Reserve
XCH Offer
Coin
New
XCH
Reserve
Pair
Singleton
New Pair
Singleton
Token
Reserve
Token
Offer Coin
New
Token
Reserve


XCH
Reserve
XCH Offer
Coin
New
XCH
Reserve
User
Pair
Singleton
New Pair
Singleton
Token
Reserve
Token
Offer Coin
New
Token
Reserve
User

Yep, that's it.

Thank you! Questions?

Twitter
TibetSwap
yakuh1t0

Discord
Yakuhito#1838

Keybase
yakuhito_chia

Webistes (Returning Soon!)
TibetSwap.io
github.com/Yakuhito/tibet