CoinSwap: A platform for Stable Coin trading and ICOs

CoinSwap Team

March 3, 2021

Abstract

This document describes the CoinSwap system. CoinSwap is designed as a coin trading platform with maximally allowed price fluctuation and as a platform for Initial Coin Offers (ICO) without centralized organizations.

1 Warning

As an academic security research team, the team has tried its best to ensure the security of the system. Specifically, the team has carried out extensive code review and testing of the CoinSwap smart contracts. The team has considered an extensive list of candidate attacking scenarios on the smart contracts and integrated security mechanisms against these attacks. Though the team has reasonable confidence on the security of the system, we do not provide any kind of warranty. The users should use this system at their own risk.

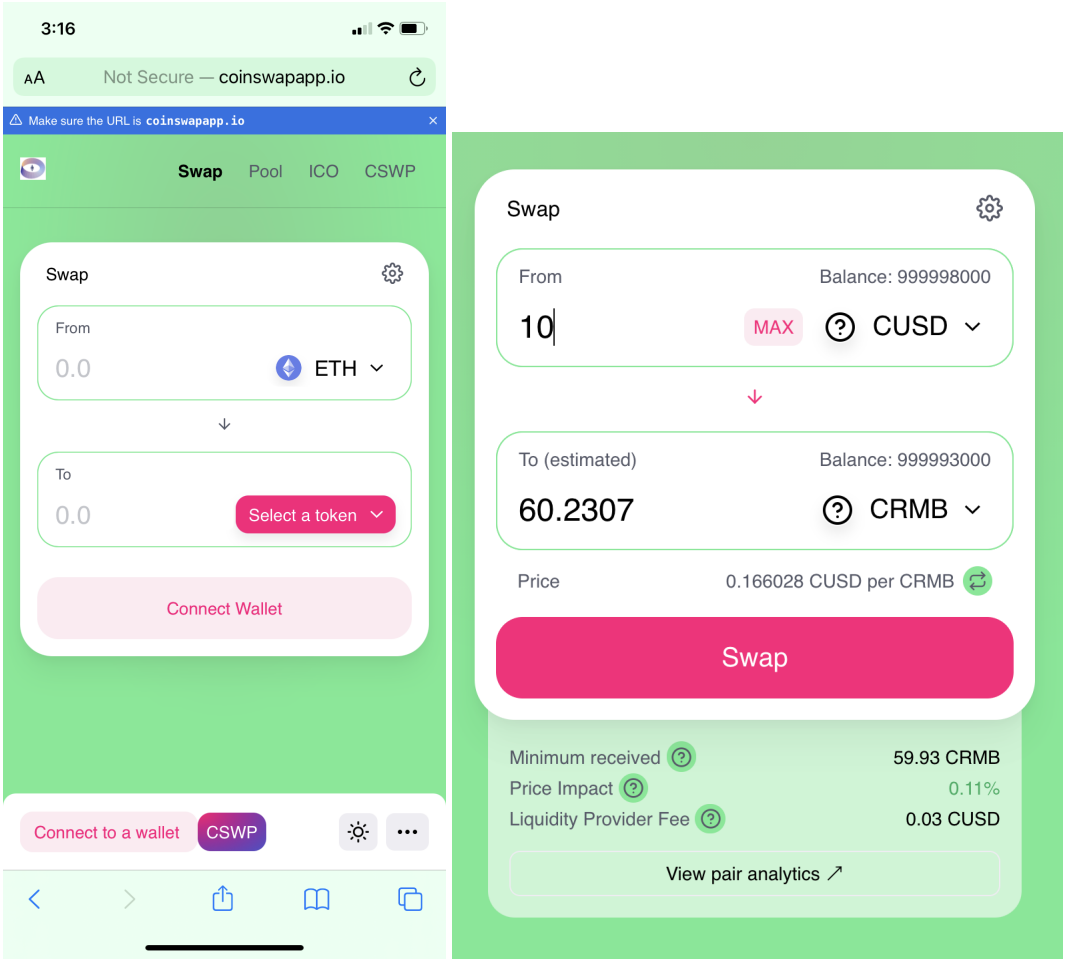
The team is aware of the fact that the core technologies of this system is protected under US patent application 63073890. Though the team provides the source code for free and users can use this system for free. It may not be allowed for third parties to copy the smart contracts and re-deploy them.

The team adapted Uniswap web front user interface for CoinSwap. Due to limited resource, the team has not carried out extensive testing and code-review on the UI source codes. Thus the UI may be buggy at some application scenario. These bugs will have only impact on the user experience and will not break the security of the underlying smart contract security. When resources are available, the team will redevelop the user interfaces.

The system has been tested on Desktop Computer with Chrome browser and MetaMask wallet. It may not be fully compatible with other browsers.

2 User Interface

The reader is referred to Wang [2] and Wang [3] for technical details of the constant circle based automated market makers. The purpose of this document is to show how to use the CoinSwap user interface. The CoinSwap system could be accessed at `http://coinswapapp.io/` and the related source codes could be retrieved from `https://github.com/coinswapapp/`. After you are at the web portal, please click the "Connect Wallet" button to connect your MetaMask wallet. If you do not have MetaMask wallet extension installed to your browser, please install it first (follow instructions at `https://metamask.io`).



At the top level, there are four buttons that one can click

- Swap: this is the default page that one sees at `http://coinswapapp.io/`
- Pool
- ICO
- CSWP: this is reserved for the development of a CoinSwap governance system and is not functional yet.

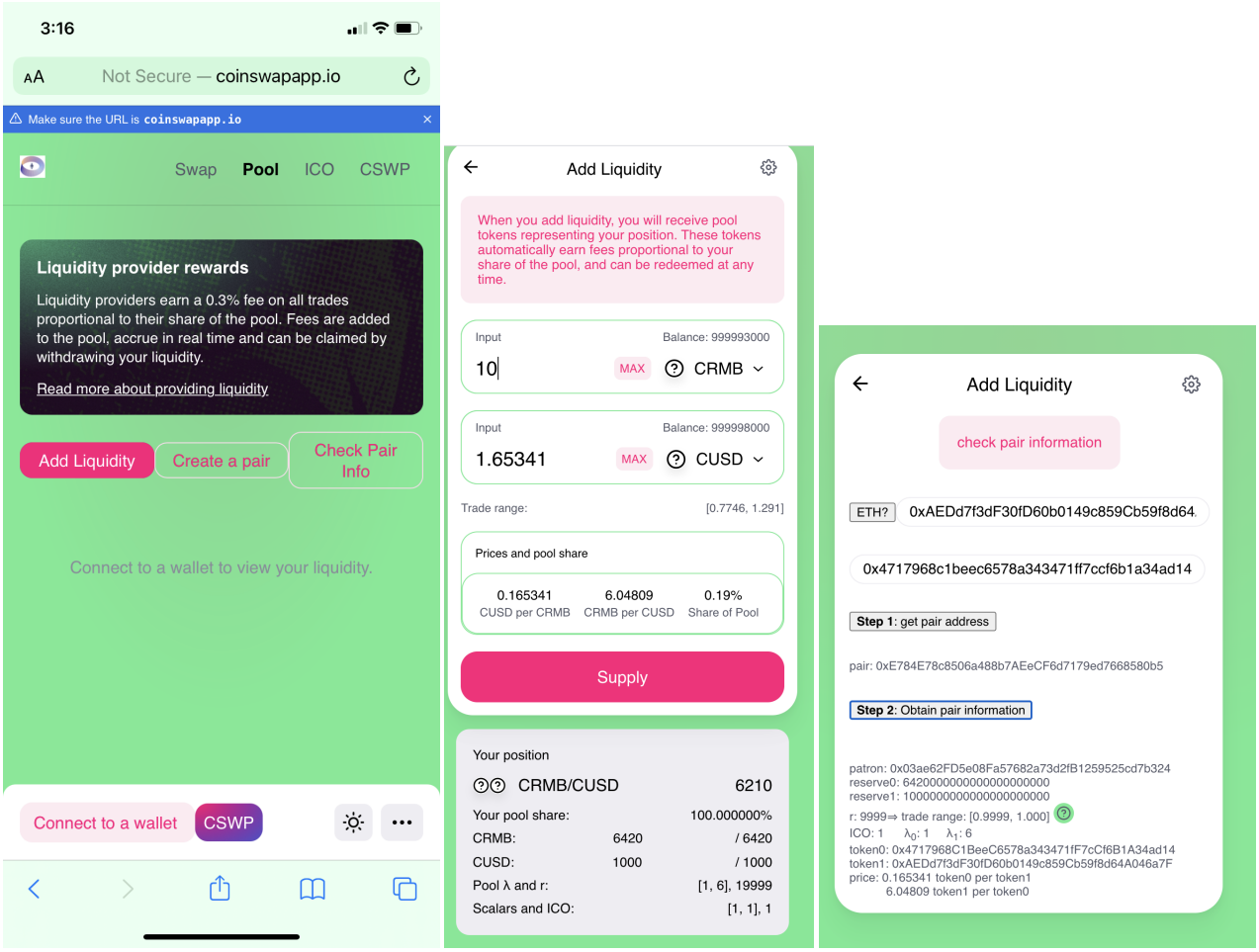
2.1 Swap

After you click the "Swap" button, you will land to the Swap page. Use the drop-down button to select the tokens that you want to swap. Then you can input the amount either in the top input box or the bottom output box. If the swap is possible, the other box should be filled automatically (right picture above). Then you can follow the instructions to complete the swapping.

2.2 Pool

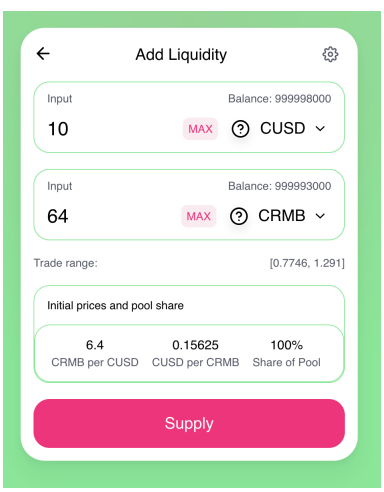
If you click the "Pool" button, you will land to the pool page with three choices

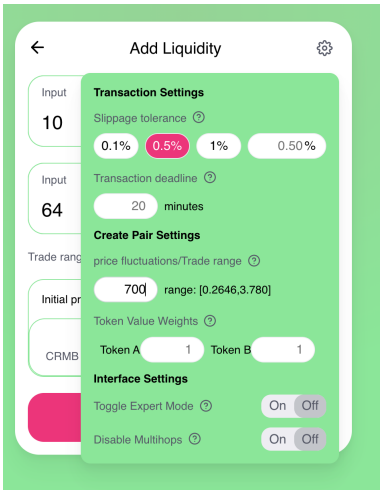
- Check Pair Info
- Create Pair
- Add Liquidity



For an existing pair, you can add liquidity to the pool by clicking the "'add liquidity" button. Use the drop-down button to select the two tokens of the pair. Then input amount in one of the input boxes and follow the steps to complete providing liquidity to the pool (see the second picture above). You may check the parameters for an existing pair by clicking the "Check Pair Info" and follow the steps there (the third picture above). To check a pair information, you need to input the addresses of the two tokens for that pair.

You can create a new pair by clicking the "Create a pair" button and follows the instructions. For a new pair, you should provide the same value tokens as liquidity. That is, if one USD token is equivalent to 6.4 RMB token, you should provide liquidity like this: 10 USD tokens and 64 RMB tokens (see the first picture below). Furthermore, you may click the setting button at top right to adjust the pair parameters. The parameter that one can configure is the "price fluctuation/trade range" value in the "Create Pair Settings" section (the second picture below). You can input a value from 1 to 9999. This controls the maximally allowed price fluctuation. The smaller the value, the larger the fluctuation. The third picture below shows the price ranges for several parameters. For example, if one input $r = 5000$, then the price fluctuation corresponds to the row 15000, which means the weighted token price could change from 0.70 to 1.41. As an example for our above tokens of USD and RMB with a current price of 1USD=6.4RMB. Based on the market situation, one USD token could be traded from $6.4 \times 0.70 = 4.48$ RMB tokens to $6.4 \times 1.41 = 9.02$ RMB tokens.



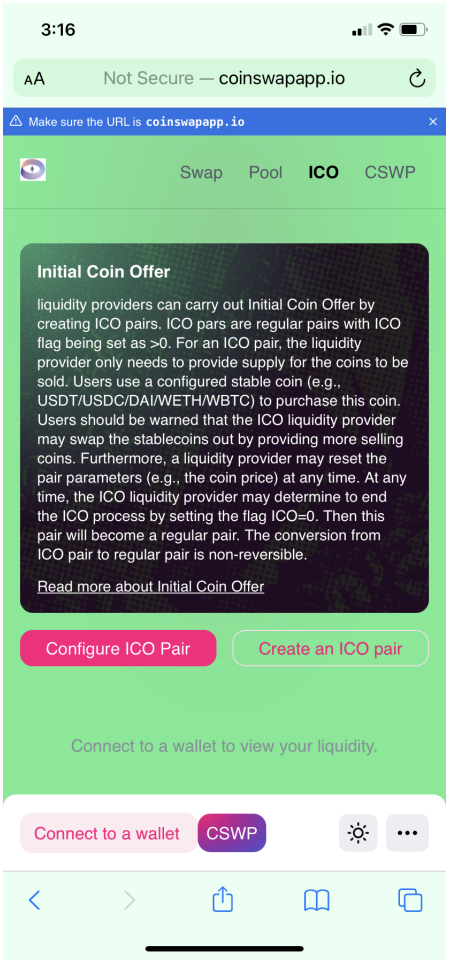


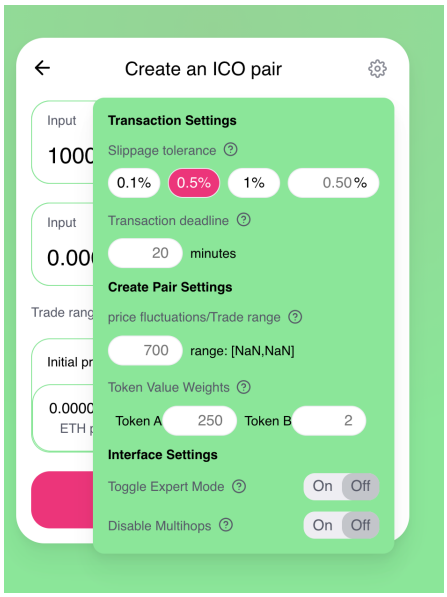
value r	minimal price	maximum price
10001	0.01000000000	100.0000000
10010	0.03162277660	31.62277660
10100	0.1000000000	10.00000000
10500	0.2236067977	4.472135956
11000	0.3162277660	3.162277660
15000	0.7071067814	1.414213562
17000	0.8366600265	1.195228609
19000	0.9486832980	1.054092553
19900	0.9949874374	1.005037815
19990	0.9994998752	1.000500375
19999	0.9999499985	1.000050004

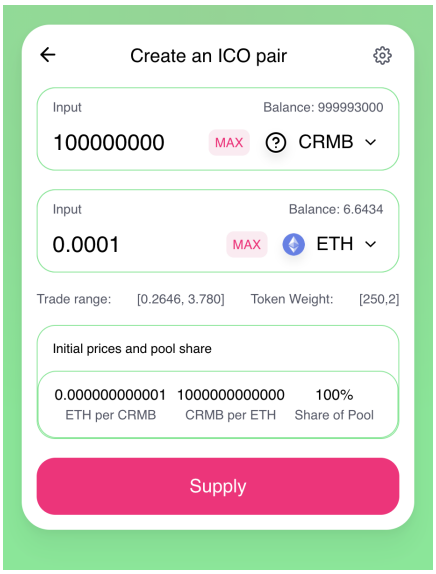
2.3 ICO

If you click the "ICO" button, you will land to the ICO page with two choices (the first picture below)

- Create an ICO pair
- Configure ICO Pair

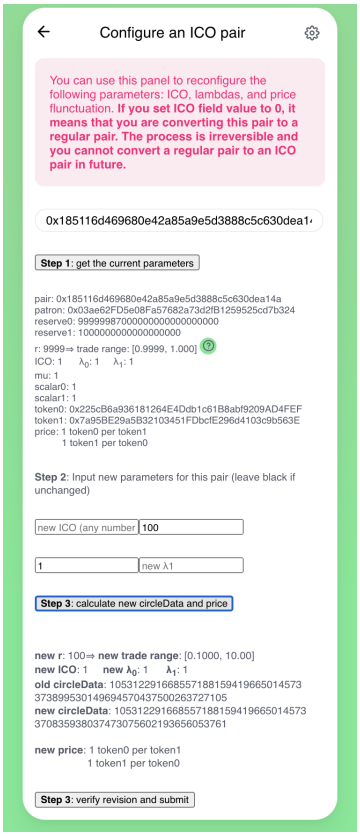






An ICO pair is distinguished from a regular pair with the following two properties

- For an ICO pair, one does not need to provide the same values of token as liquidity for the pool. Essentially, one only needs to provide the tokens that one wants to sell and zero amount of other tokens. However, the current UI needs the two boxes are non-zero. Thus one still needs to provide a tiny amount (e.g., 0.1US$) in the other box. As an example, if one develop a token called CRMB and wants to sell 100000000 CRMB tokens to the market, one may create the ICO pair by providing 100000000 CRMB tokens and 0.0001 ETH (or any amount of other tokens such as USDT) as in the third picture above. To set up the market price for these CRMB tokens, one needs to click the top-right setting button and change the Token Value Weights. Assume that one, wants to sell one 125 CRMB tokens for one ETH, then one can input 250 in the Token A field and 2 in the Token B field. If you make mistakes, do not worry about this, you will be able to change these values later (the second picture above). Similar to a regular pair, one can change the value of price fluctuation/trade range to control the maximally allowed price changes.
- For an ICO pair, one may be able to change the price of tokens when market changes. One can do this by clicking the "Configure ICO Pair" button. On the "Configure an ICO pair" page, you can input the ICO pair address and then follow the steps to revise the values of token weights and price fluctuation range. At the same time, one may just convert the ICO pair to a regular pair by setting the ICO flag to 0. It should be noted that, after you convert the pair to a regular pair, you will not be able to change any parameters any more and the pair stays as a regular pair forever. See the following picture for details.



References

[1] E.W. Mayer. Efficient long division via montgomery multiply. *arXiv preprint arXiv:1303.0328*, 2013.

[2] Yongge Wang. Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*, 2020.

[3] Yongge Wang. Implementing automated market makers with constant ellipse. *Technical Report*, 2021.