

CoinSwap: 稳定币交易及其首次公开募币(ICO)平台

CoinSwap 团队

March 3, 2021

Abstract

本文是 CoinSwap 平台的使用手册。CoinSwap 主要适合于价格可控的密码数字资产的交易。比如稳定币的交易。此外 CoinSwap 也可以作为不需要交易所的首次公开募币(ICO)平台。

1 警示

作为一个具有20多年网络信息安全研究的学术团队，CoinSwap 团队尽最大的努力来保证CoinSwap系统的安全设计。特别的，我们对CoinSwap 系统的智能合约做了最广泛的安全强度测试并且对每一行代码都经过了无数遍的分析与测试。虽然我们对CoinSwap 系统的安全性能有足够的信心，但是我们无法对系统的安全性做任何承诺。用户在使用本系统前，需要评估自己可以承担的风险。对于您通过CoinSwap 平台交易而引发的损失，CoinSwap 团队不承担任何法律责任。

CoinSwap 系统的核心技术受到美国专利 63073890 的保护。CoinSwap 团队获得了该专利的使用权。所以用户可以放心的使用本系统。我们开放所有源代码供读者做安全分析。但是我们并没获得 第三方 redistribute 该技术的权利。所以在获得授权前使用本系统的技术是非法的。

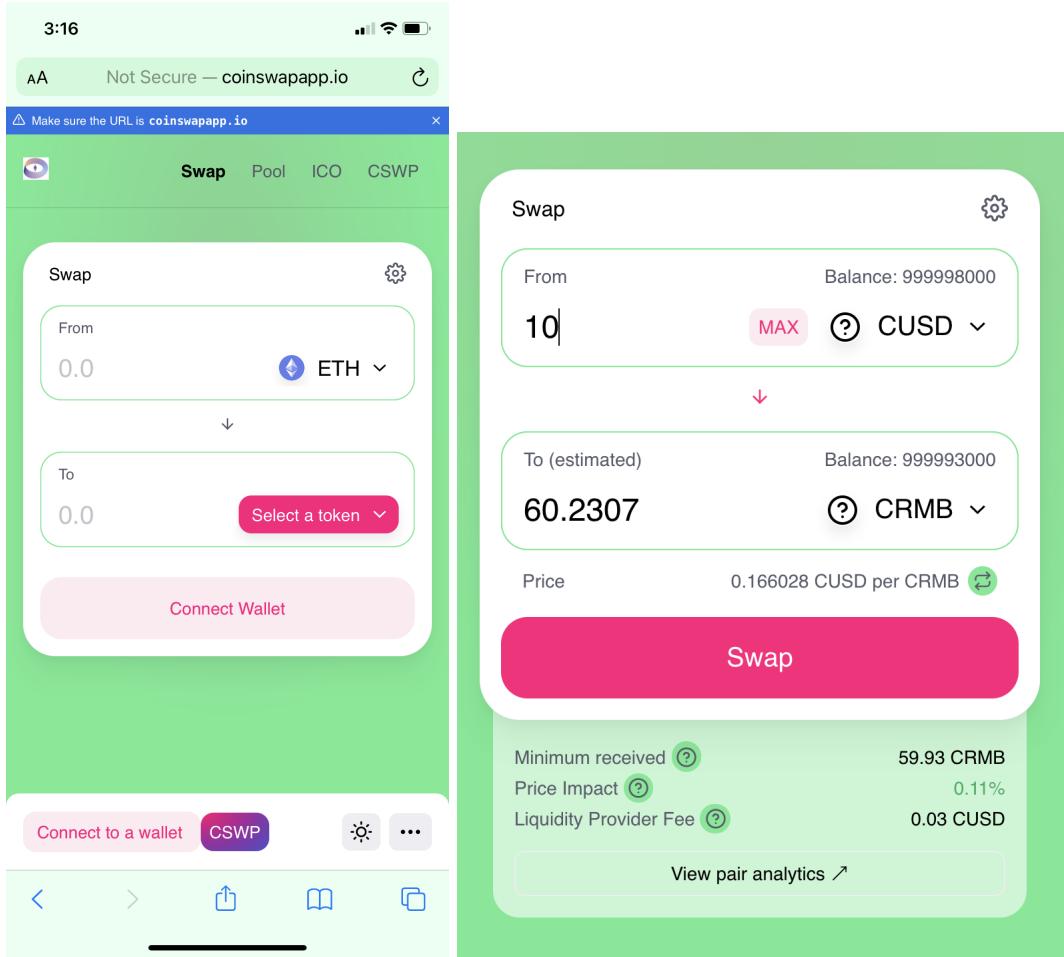
由于CoinSwap 团队是一个很小的学术团队，可获得的资源有限。所有我们修改了 Uniswap 的网页代码，用来访问CoinSwap 的智能合约。修改过的网页代码也许还有不少bug。这些bug也许会影响到您 使用本系统的用户体验。但是不会导致任何的安全问题。所以您可以放心使用。我们在电脑上用 Chrome浏览器和 MetaMask 钱包对本系统做了测试。在手机或别的浏览器里，有些功能也许并不工作。如果有机会得到更多的资源，CoinSwap 团队将会重新开发CoinSwap 的网页代码。

2 用户界面

关于CoinSwap 的核心技术，请您参阅王教授的如下文章： Wang [1] 和 Wang [2]。本手册主要描述如何使用CoinSwap的用户界面。您可以通过网页 <http://coinswapapp.io/> 来使用本系统。CoinSwap 系统的所有代码可以在 <https://github.com/coinswapapp/> 获得。当您登陆CoinSwap 网页后，请按“Connect Wallet”按钮来连接您的钱包。我们对所有的功能通过 MetaMask 钱包做了测试。如果您的Chrome浏览器没有安装 MetaMask 钱包，您可以通过如下网页安装： <https://metamask.io>)。

在CoinSwap网站的主页，用户有如下选择

- Swap/交易：这也是<http://coinswapapp.io/>的首页
- Pool/资金池
- ICO/首次公开募币
- CSWP/CoinSwap 管理系统（正在开发）。CoinSwap团队目前在对CoinSwap的管理方式做出研究和规划。该功能在不久的将来开放。



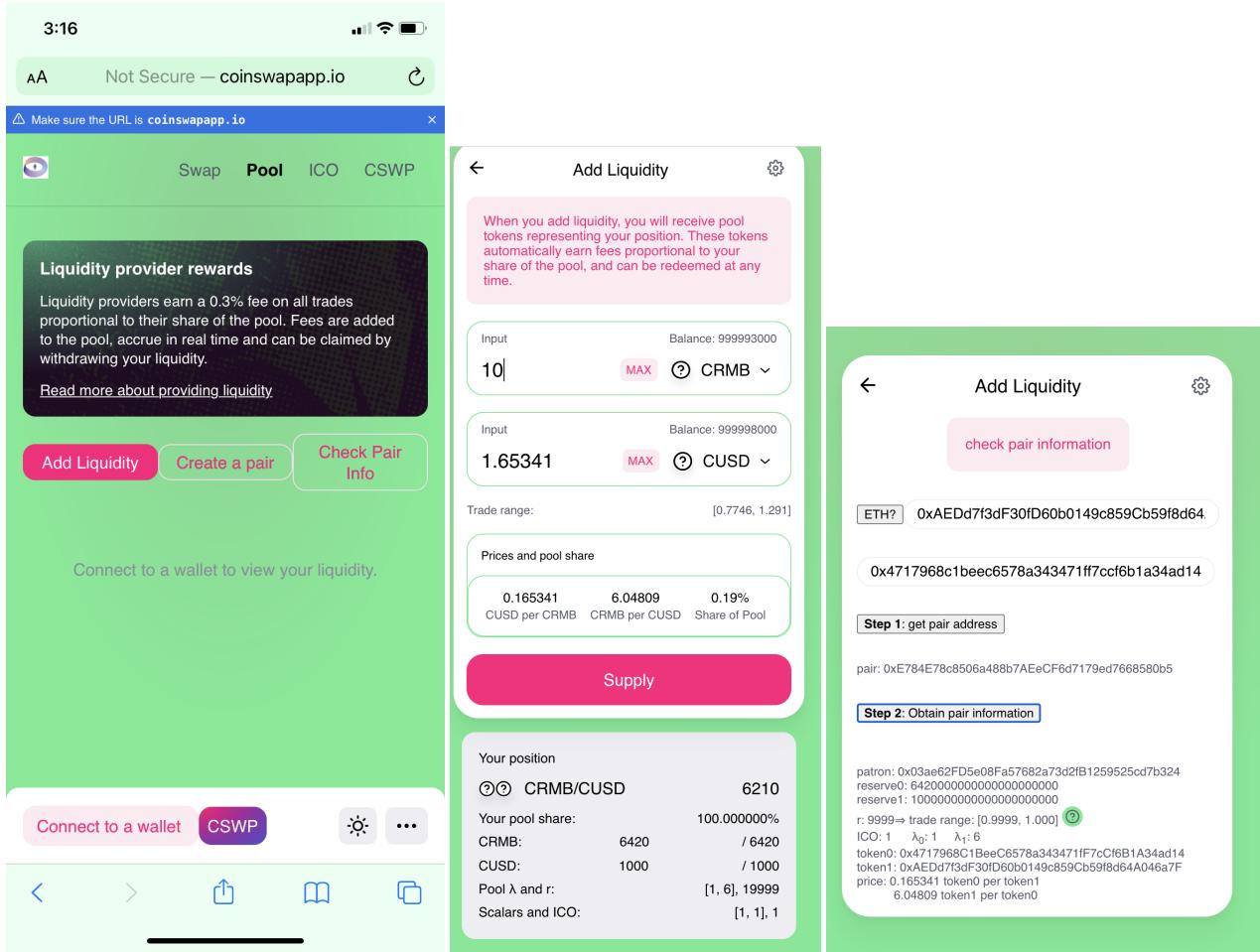
2.1 交易

当您点击“Swap”按钮进入交易网页后，您可以通过货币选择按钮如上图所示选择要交易的货币对。您可以选择任何一种交易货币的数量。系统会自动算出您大概所需要的另一种货币的数量。比如上图中，我决定用10个CUSD货币兑换相应的CRMB货币。系统显示在目前的市场里，我大约可以获得60多个CRMB货币。然后您可以点击“Swap”并遵循步骤完成交易。

2.2 资金池

当您点击“Pool”按钮进入资金池网页后，将出现以下三个选择（如下图所示）：

- Check Pair Info/查阅货币对的信息
- Create Pair/建立一个新的货币对
- Add Liquidity/给一个已经存在的货币对注入资金



如果您要对一个已经存在的货币对注入资金，您可以通过按钮“add liquidity”进入。然后您可以选取货币对的货币并输入您所要注入的资金。您所注入的资金必须要和货币对里现有的资金成正比。所以当您填写一个货币的数量后，系统会自动填入您所需注入的另一个货币的数量（如上图所示）。您也可以通过“Check Pair Info”按钮来调阅目前一个资金对的状况（比如价格，库存等等）。上边的第三个图显示的是一个资金对的目前状况。

如果您要建立一个新的货币对，您可以通过按钮“Create a pair”进入该界面。在建立一个新的货币对的时候，您需要注入价值相同的货币量。比如目前一个USD货币单元可以换取6.4 RMB货币单元。那么如果您在建立(USD, RMB)货币对的时候，就需要注入（比如）10个USD货币单元和64个RMB货币单元（如下图所示）。此外，您可以通过右上方的设置按钮来调节本货币对的参数。在货币对里，您可调节的参数是价格幅度“price fluctuation/trade range”的范围。该参数在“Create Pair Settings”章节里（如下图所示）。在该参数里，你可以输入1到9999之间的任何数字。该参数控制着价格可以变化的最大幅度。该参数越小，允许的价格波动越大。比如，参数 $r = 5000$ 对应的价格幅度行是15000。也就是说价格可以在0.70到1.41之间变化。对于我们上边的RMB和USD的例子，如果目前的价格是1USD=6.4RMB，那么将来在市场波动的时候，一个USD货币单元可以在 $6.4 \times 0.70 = 4.48$ RMB货币单元到 $6.4 \times 1.41 = 9.02$ RMB货币单元之间波动。

value r	minimal price	maximum price
10001	0.01000000000	100.0000000
10010	0.03162277660	31.62277660
10100	0.10000000000	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

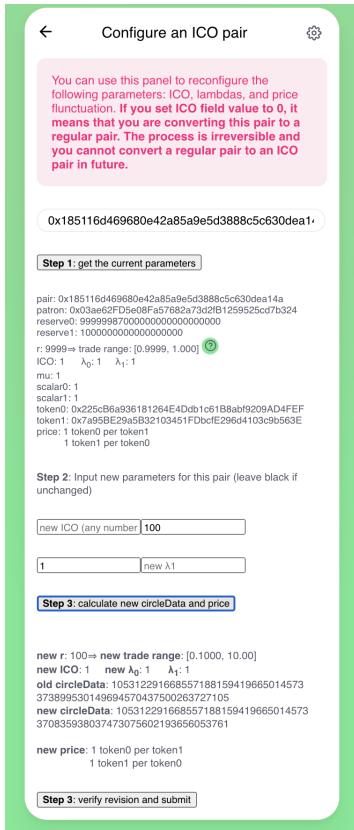
2.3 ICO / 首次公开募币

如果您点击“ICO”按钮进入ICO界面，您会看到如下两个选择：

- Create an ICO pair/建立一个ICO货币对
- Configure ICO Pair/重新设置ICO货币对参数

ICO 货币对和普通货币对的主要区别有以下两点

- 建立一个 ICO 货币对的时候，用户不需要提供等量的货币对。在 CoinSwap 智能合约里，一个用户只需要提供足够数量的待销售tokens。但在目前的用户界面里，每个货币的数量不能为零。所以用户还是需要提供微量的另一种货币（比如0.1美元）。比如，如果您想售卖CRMB货币（token）。您的客户需要用以太币（ETH）来购买您的CRMB。您可以建立一个（CRMB, ETH）的 ICO 货币对。然后注入1000000000 个CRMB货币单元和 0.0001 个以太币ETH（如上图所示）。在您点击“Supply”按钮之前，您需要（也可以不需要）点击右上角的设置按钮来调节 CRMB 的初始价格。在您进入设置页面后（如上中间图），您可以通过调节 Token Value Weights 来调节 CRMB 的价格。比如您需要客户可以用一个以太币购买您 125 个CRMB 货币单元。那么您就需要将 Token A 的权重设置为250，把 Token B 的权重设置为 2 。如果您不小心设置错了。不要惊慌，后边您有机会调整。和普通的货币对设置一样，您可以通过调节 price fluctuation/trade range 的值来控制 价格的浮动范围。
- 随着市场的变化，作为 ICO 货币拥有者的您，如果需要调节待售token 的价格，您可以点击“Configure ICO Pair”按钮来实现该操作。进入“Configure an ICO pair”页面后，您可以输入 ICO 货币对的地址 来获取目前的参数。然后可以输入新的 Token Value Weights 来调整价格。此外，如果您的 ICO 市场活动结束，您可以 把 ICO 货币对的参数 ICO 设置为零。从此该 ICO 货币对就变成了一个普通的货币对。需要特别强调的是，一旦您将 ICO货币对转换为普通货币对，这个货币对将永远是普通货币对。以后无法变回 ICO 货币对。其界面如下图所示。



References

- [1] Yongge Wang. Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*, 2020.
- [2] Yongge Wang. Implementing automated market makers with constant ellipse. *Technical Report*, 2021.