

加密货币搬砖项目介绍书 第一版

前言

币圈是一个入场门槛极低、监管缺失、玩法花样百出的市场。在这个市场具有无数的利差可以赚钱。

本文默认读者已经知道传统市场的期货，如果不明白可以看这个视频

- 海外地址：[期货和你的生活有什么关系？- YouTube https://www.youtube.com/watch?v=EU1E4Rs0BPM](https://www.youtube.com/watch?v=EU1E4Rs0BPM)
- 国内地址：[期货和你的生活有什么关系？- bilibili https://www.bilibili.com/video/av63566148](https://www.bilibili.com/video/av63566148)

前置知识介绍

搬砖常用网站

币圈主要有3大区域，搬砖也往往是在这3大区域里面互相倒腾：

- 中心化交易所：币安、火币、OKEX、抹茶、Coinbase。
- 去中心化交易所（DEX）：uniswap、pancakeswap、sushiswap。
- 流动性挖矿：sushiswap、pancakeswap、quickswap。

注意，以上列举仅仅是举例，也可以视作常用网站。

搬砖基本原理

搬砖需要知道两个基本原理：

- 价差，同一个商品在不同地方的价格差，理论上你只需要在便宜的地方买入，在贵的地方卖出就行。类似以前的倒爷。
- 利差，同一个商品在不同地方的利息差，理论上你只需要在利息低的地方借出，在利息高的地方存入。类似银行吸纳存款和发放贷款挣钱。

公链（区块链）介绍

常用的公链有3个：

1. 比特币链，货币名字是BTC，最原始的比特币链只能转账比特币，后来升级了Omni协议后拥有了承载其他货币和智能合约的能力。
2. 以太坊链（Ethereum），货币名字是ETH，代币协议名字是ERC20。也是目前生态最完善的一个，在上面发行了大量的代币、应用、游戏。但矿工需要消耗大量电力来挖矿，因此手续费高昂。
3. 币安智能链（BSC），货币名字是BNB，代币协议名字是BEP20。不仅密钥和地址与以太坊通用，就连智能合约编写和部署也几乎一样，有点复制以太坊的意思。因为其出块验证被完全把握到币安手里，所以时常被嘲笑为中心化区块链，但优点在于省去挖矿消耗，手续费很低。

还有一些加密货币自己创建了区块链，例如XMR、BEAM、SIA等等，这些链只能供他一种币转账使用。好处是可以用于特殊用途，例如XMR和BEAM这种隐私币的转账就无法追溯。

需要注意的是，各个链之间资产不是相通的，转账不仅需要核对地址，也要核对是否是同一条公链，否则很有可能将钱转到一个无人认领的地址，导致丢失所有资产。

重要金融概念理解

做多、做空、减仓、平仓

做多的意思是买入，如果原本持有0个比特币，做多1个之后就持有了1个比特币。

做空的意思是卖出，如果原本持有0个比特币，做空1个之后就持有了-1个比特币。

减仓的意思是朝着持有0个比特币进行交易，无论持有1个还是-1个，减仓1个之后，持有的数量都是0。

平仓的意思是完全减仓，减仓可以只减一半，平仓就完全直接将仓位变成0。

对冲

对冲，又称套期保值，是市场交易里一个十分重要的操作。

对冲的主要作用是屏蔽掉不必要的风险。我们以A交易所和B交易所举例，假设比特币在A比较便宜，在B比较贵。

那么理论上只需要在A买入，在B卖出，扣除手续费剩下的都是利润。但交易所之间转账往往需要10分钟左右的转账时间，在这10分钟之内，盈亏都会由自己承担。

为了避免承担风险，可以在A买入现货的同时，在B的期货做空，这样就相当于瞬间在A买入，又瞬间在B卖出，利润瞬间锁定。

因为你买了又卖掉，相当于净持仓是0，这时比特币无论怎么波动都对你没影响，你只需要等你的比特币在B到账之后，把比特币在B卖掉，然后在B买入期货（停止做空，比特币已经真正在B的现货卖出了，所以之前在期货的卖出需要买回来）。

现在是真正的把比特币从A搬到了B。全程操作下来，期货承担了一个“提前卖出”的功能，让你避免承受转账期间的价格波动。

“提前卖出”这种操作的作用远不止于此，“提前卖出”是搬砖的基本操作之一，往后会看到更多这个操作的用处。

杠杆

杠杆的作用是放大风险以及利润，如果是10倍杠杆，那么价格每波动1%，都相当于波动了10%。杠杆是非常危险的工具，使用不当可能导致大量损失。

通常有两种杠杆形式：

- 保证金，主要用于期货，如果是2倍杠杆，意味着只需要交50%的保证金，就可以持有100%的仓位。
- 借贷，主要用于现货，通常杠杆不超过2倍，使用1份资产作为抵押，可以借到0.8份左右的其他资产。

交易所会设立爆仓清算线，对于保证金制度来说，如果亏损到保证金不足，就会被强制清算，失去那一份仓位的所有权，也亏损掉所有的保证金。

对于借贷制度来说也是一样，如果抵押资产快要无法偿还借贷的钱，交易所就会启动清算，将抵押资产变卖用于偿还借贷。

爆仓清算是最坏的结果，无论如何都要尽可能避免，在爆仓和放大利润之间权衡。

永续合约

永续合约的概念和传统合约的概念相似，但永续合约永远不会到期，为此我们需要引入一个重要概念：资金费率。

传统合约因为会到期，所以期间无论怎么波动，最终到期交割的时候期货价格一定等于现货价格，依靠交割作为价格锚定的机制。

但永续合约永远都不会到期，应该怎么和现货价格锚定呢？当前普遍采用收取资金费率的方式来锚定。假如期货价格高于现货价格，说明很多人即便期货更贵，也要加杠杆来买期货（行内称之为杠杆赌狗），因此会每8个小时，向所有做多的人收取 $\text{仓位} \times \text{资金费率}$ 这笔钱，然后向所有做空的人按照 $\text{个人仓位占比} \times \text{刚刚收的钱}$ 来瓜分这笔钱。并且期货价格偏离越多，资金费率越高。这样杠杆赌狗们就必须要考虑资金费率的问题，永续合约的价格也就锚定到了现货上。

稳定币

外界嘲笑比特币的时候有一个笑话：

一个男孩找他的爸爸要1个比特币当做生日礼物

他的爸爸说：什么？你要15554美元？14354美元可不是一笔小钱，你要16782美元去做什么？

虽然比特币价格波动没有这个笑话里这么夸张，但是比特币动不动就一天涨跌10%，日内振幅30%也不是稀奇事，有没有价格十分稳定的加密货币呢？

答案是有的，而且有很多，主要分为两类：

- 法币抵押：USDT、BUSD、PAX、TUSD、HUSD
- 加密资产抵押：DAI

法币抵押意味着发行商在美国注册了公司，向银行账户存入美元，并（理论上）发行等额的加密货币。需要注意的是，很多公司并不会向银行存入100%的美元，而是将公司部分资产抵押来当做美元，所以实际上这类币具有发行公司暴雷的风险，使用时需要尽量选择审计结果良好的公司发行的代币。

相比之下，加密资产抵押模式更具有币圈“去中心化”的血统。DAI币的发行完全依赖于运行在区块链上的智能合约，无人可以干预，但是DAI币也并非完美，因为DAI币完全运作在区块链上，曾经就发生过DAI币清算拍卖时因为区块链过于拥堵，导致自动清算机器人出价的交易没有被及时打包，价值450万美元的抵押物以0 DAI的价格被人拍走的事情。最终还是基金会增发MKR币，由爱好者“用爱发电”抹平了这笔缺口。

流动性挖矿

流动性挖矿依靠自己的资金为市场提供流动性来赚钱，属于DeFi的一部分。

例如有的人想将ETH转换为USDT，而有的人想将USDT转为ETH，那么你可以购买ETH和USDT，然后创造或者加入一个ETH/USDT的流动性矿池，依照市场价格为他们提供转换服务并收取一点利差。

去中心化交易所

这里有几个常用缩写需要介绍

- DeFi：全称是Decentralized Finance，去中心化金融，只要是运行在区块链上的金融服务都可以称它属于DeFi
- DEX：全称是Decentralized exchange，去中心化交易所
- CEX：和DEX相对而言，CEX就是中心化交易所

DEX这个词在不太专业的交流论坛里用得比较少，因为绝大多数DEX都提供了几乎所有的金融服务，包括交易、流动性挖矿、抵押借贷等等。所以外界喜欢直接叫DeFi来表示各个DEX，两个词几乎快变成一个意思了。从下图可以看到，1inch在自己的网页标题里直接将DeFi和DEX并列。



在上面我们提到了流动性挖矿，DEX能够提供交易，其根本原理就是对各种流动性矿池进行整合，然后依照算法找到最优的交易路径，将你的货币兑换成想要的货币。就目前而言，算法最为优秀的当属1inch交易所。

加密货币跨链发行

众所周知，比特币是发行在其原生区块链的货币，但是我们在提现比特币的时候，发现竟然可以将比特币提现到以太坊或者BSC上面，这是怎么回事呢？

BTC 提现地址

转账网络 ⓘ

<input type="radio"/> Binance Chain (BNB) BEP2	手续费: 0.0000047 BTC ≈ \$0.173756
<input type="radio"/> Binance Smart Chain BEP20 (BSC)	手续费: 0.0000047 BTC ≈ \$0.173756
<input type="radio"/> Bitcoin(BTC) BTC	手续费: 0.00055 BTC ≈ \$20.33
<input type="radio"/> Ethereum (ETH) ERC20	手续费: 0.00096 BTC ≈ \$35.49

答案在于货币的跨链抵押发行机制。具体来说，发币方在原生链的某个地址上存放足够多的币，而后再在另一条链上发行等量的代币，然后把两个地址公之于众，大家可以看到原生地址存储了多少币，也可以看到在另一条链上发行了多少币。在这里可以看到币安的代币发行情况 <https://www.binance.org/cn/assets-proof>

这个想法十分美好，但实际操作起来具有相当高的风险，风险主要在于以下几个方面：

1. 如何确定用于抵押的币是用户的资产，还是币安自己的资产？要是币安拿用户放在交易所的币去抵押，发行的币再让用户去买，那不是搞笑吗
2. 原则上应该1:1发行，但截至发稿，经过笔者的审计，币安抵押了73601个BTC，却发行了96006个BTC，抵押率仅为76.6%

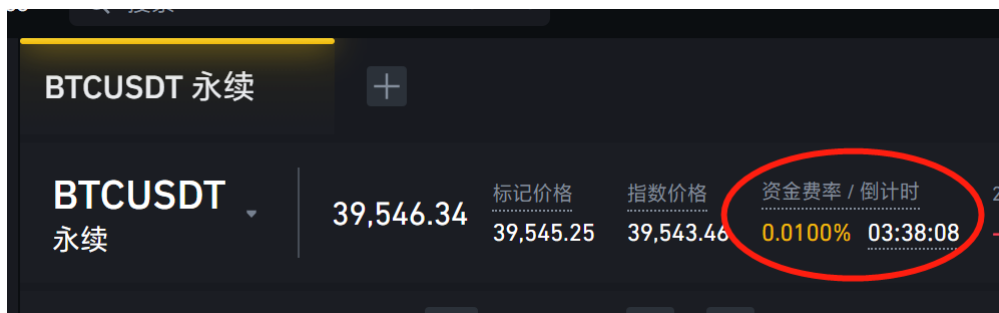
所有的疑惑，在缺乏监管的加密货币市场都无法得到解答，所以尽可能将跨链代币作为交易中介，而不是拿去长期存储。

搬砖项目介绍及操作

永续合约资金费率搬砖法

原理

永续合约资金费率搬砖的原理在于其每8个小时会收取一次资金费率，此方法90%的利润来源都是对手给的资金费率。



在讲解永续合约的时候，我们提到期货可以加很大的杠杆，所以即便期货更贵，他们也会硬冲。如此大量的高杠杆仓位一定会导致期货价格大幅偏离现货。而我们所做的事情，实际上是用我们的真金白银，来压制杠杆赌狗们用杠杆吹出的泡沫，使得期货价格能够更加接近现货价格，让杠杆赌狗能够以更便宜的价格加杠杆，但赌狗的代价就是每8小时，就会向我们支付一笔资金费率。

从另一个意义上来说，我们为期货提供了流动性，而杠杆赌狗则向我们支付利息。

具体操作

在具体操作上非常简单，如果杠杆赌狗在期货拼命做多，那么资金费率就会为正，我们想要吃资金费率，就反向做空期货就行。

但光做空期货还不行，如果价格继续上涨，我们就会亏损，所以为了屏蔽这方面的风险，要使用之前介绍的“对冲”，也就是在现货做多相同的仓位。

一通操作过后，我们在现货做多，在期货做空，两边数量对等，价格波动不会导致亏损，而且还能收到资金费率。

风险点

因为期货要做空，所以价格快速上升的时候会有期货爆仓的风险，如果期货爆仓后没有及时发现，导致一段时间内单方面持有现货，就可能导致亏损。因此价格上升的时候需要适当减仓，将减仓所得资金转账到期货账户来补充保证金。并且需要将资金分散到多个币种上面。一个币可能几个小时内涨50%让你爆仓，5个币全部同时涨50%的概率就非常低，同时需要让系统具有预警机制，即将爆仓的时候自动减仓或者拨打电话警告，尽可能降低爆仓风险。

额外知识

如果价格下降，那么期货账户就会赚钱，因此会多出大量闲置的保证金，此时需要将部分保证金转到现货账户，用于加仓，以此提高收益。

这种搬砖方法，在开仓的时候，期货和现货价格差往往比较大。而我们平仓通常是因为资金费率变少了，这种时候期货和现货价格差往往比较小，所以这时候平仓能够吃到期货和现货的价格差。因此这种搬砖方法不仅赚到了资金费率，也赚到了期现价格差。

上述只介绍了资金费率为正的情况下搬砖的方法。只适用于价格快速上涨的时候使用。在市场价格快速下跌（崩盘）的时候，杠杆赌狗们会转而拼命做空，使得期货价格低于现货价格，也会让资金费率为负，这时候怎么挣钱呢？期货可以直接做多，但现货不能直接做空，那么我们需要从交易所借入相应的币，然后把借入的币卖掉，就达到了给现货做空的效果，类似于传统的股票做空机制。

跨交易所价差搬砖法

原理

各个交易所之间有时候会出现较大的价格差距，这时候如果在便宜的地方买入，在贵的地方卖出，就能直接拿到收益。



通常，跨交易所搬砖是在币安和托管在BSC上的DeFi之间进行。因为对于大多数币来说，在交易所之间转账需要走以太坊的公链，这条链转账费用极其高昂，截至发稿，一笔DeFi交易需要15美元的手续费，转账手续费也要5美元，如果搬砖的本金不大，那么搬砖赚的钱连手续费都填不上。为此，在BSC这条链上面搬砖成了低成本的理想替代品，截至发稿，BSC的DeFi交易手续费为0.6美元，转账手续费仅为0.18美元。

详细操作

本文默认读者会使用区块链的各种操作，如果不明白可以翻到 [附录-DEX使用方法](#) 查看教程。

跨交易所搬砖非常简单，理论上讲，在低价区域购买，在高价区域售出。所以只要学会了DEX的使用方法，就能开始搬砖。

具体而言，如果CEX的币价格比较贵，那么将稳定币提现到区块链钱包，然后在DEX买入，买入的瞬间在CEX期货做空，然后将买入的币充值到CEX，在CEX卖掉，将CEX的期货平仓。就完成了一轮循环。

如果DEX的币价格比较贵，那么在CEX购买货币，购买的同时在期货同等做空，接着将买入的币提现到区块链钱包，然后在DEX卖出，卖出的同时将期货平仓，接着将卖出得到的稳定币充值回CEX，完成一轮循环。

风险点

有一件事情需要注意，那就是大量资金冲击市场的时候造成的滑点问题。

我们可以很方便地在CEX交易所查看当前市场的深度图，估测出自己的交易能造成多大的滑点



在DEX交易所的滑点则更加直观，因为会告诉你本次会接收到多少货币，所以滑点直接就计算出来了

The image shows a trading interface for a swap transaction. The top section has tabs for 'Market' and 'Limit', with 'Market' selected. Below the tabs, there are icons for a refresh, a swap, a plus sign, and a settings icon. The main section is divided into two parts: 'You Pay' and 'You Receive'. Under 'You Pay', the user is paying with 'Tether USD' (USDT) for a balance of 0. The amount being paid is approximately \$48,915.25, which is equivalent to 48437.9 USDT. Under 'You Receive', the user is receiving 'Filecoin' (FIL) for an amount of approximately \$48,135.14, which is equivalent to 725.229 FIL. The percentage change for the received amount is -1.59%, which is circled in red. At the bottom, there is a button labeled 'Insufficient balance'.

滑点有时候多，有时候少。像笔者这次截图的FIL，在DEX仅仅5万美元，就造成了1.59%的滑点，这种滑点很多时候会侵蚀所有的利润甚至造成亏损。

这种滑点也很好规避，设计系统，在搬砖之前自动计算所有数据，如果滑点之后仍然没有亏损，那么就可以开始搬。

额外知识

在本方法的详细交易过程中用到了“对冲”，很多时候没有必要用对冲，对冲会损失两次期货的交易手续费和滑点，是否使用对冲要看币价波动是否剧烈，以及搬砖的差价是否够大。如果搬砖差价很大、价格平稳，就没有必要用对冲。

依据笔者的搬砖经验来说，此方法搬砖的机会，一般出现在两种情况

1. 新币上架：因为存在信息差，很多人不知道这个上架的新币到底值多少钱，所以上架一段时间内，币的价值都和实际价值有较大偏离。所以这段时间搬砖可以获得较大收益。
2. CEX维护升级：通常来说不会期货和现货同时维护，所以即便是在维护，CEX的现货和期货仍然有一个可以交易。但即便有其中一个不能使用，也会让大量的流动性锁死在正在维护的交易所当中，这必然会导致市场流动性大幅下降。流动性下降的后果就是各处都会产生溢价，所以交易所维护升级也是一个搬砖的好时机。

跨交易所利差搬砖法

原理

很多时候我们可以通过抵押来借入某个币，同时，我们可以将这个币放到流动性矿池去赚钱。

借币会被收取利息，而存币能够产生利息，如果产生的利息大于被收取的利息，就可以赚到这利息之差。

详细操作

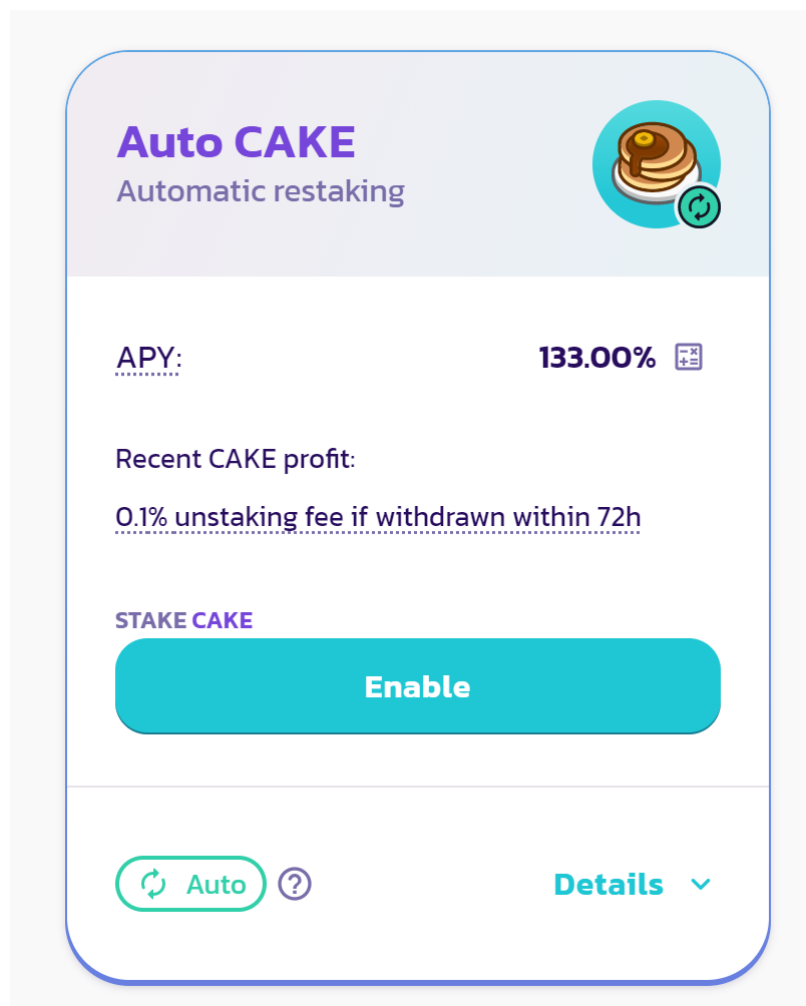
我们以币安和pancake为例，首先查看币安借入cake币会收取的利息，可以看到每小时收取0.00416667%，相当于年利率36%。



The screenshot shows the 'Borrow' (借款) tab selected in the Binance interface. The currency is set to 'CAKE PancakeSwap'. The hourly interest rate is 0.00416667%, the amount borrowed is 0.00000000 CAKE, and the maximum borrowing amount is 0.20672299 CAKE. A link is provided to view more interest and limit information.

借款	还款
币种	
CAKE PancakeSwap	
小时利率:	0.00416667%
已借:	0.00000000 CAKE
最大借款数量:	0.20672299 CAKE
点击 查看更多利率与限额信息。	

我们再到pancake查看抵押cake币的年利率多少，可以看到年利率高达133%。



所以如果从币安借入cake币，放到pancake去抵押，每年就能躺赚97%的利率，这就是利差搬砖法。

风险点

当借入的币快速上涨的时候，如果没有及时给交易所补仓，那么抵押的资产可能会被清算。此时变成了单方面持有cake币，可能导致亏损。所以和上述的资金费率搬砖法一样，需要注意仓位控制，并完善预警系统。

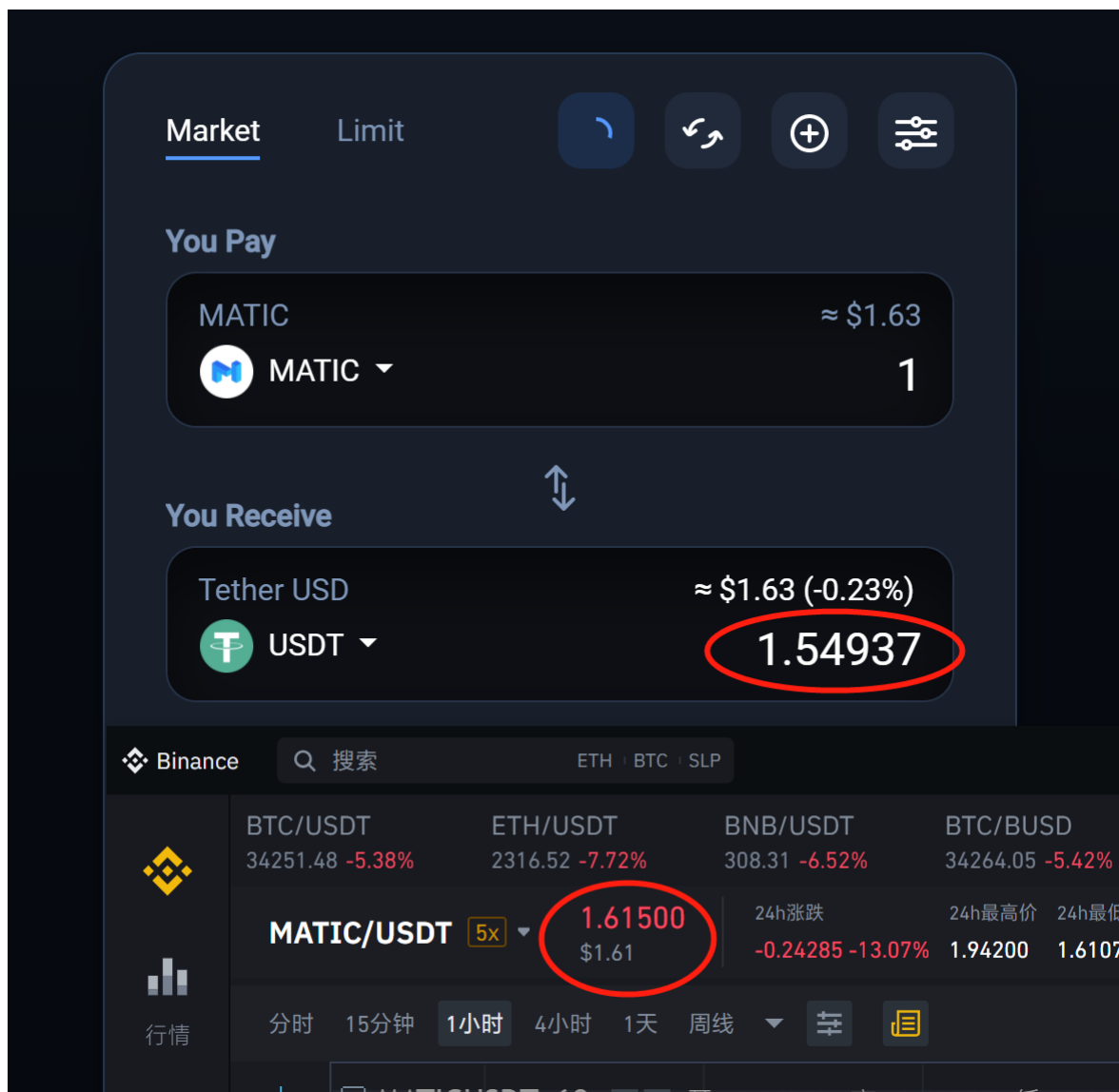
MATIC搬砖法（时效）

前言

此搬砖法具有一定的时效性，并非长久有效，但现在可用。

原理

MATIC币是发行在polygon网络的原生货币，如果要将在polygon网络转移到以太坊主链，需要走Plasma Bridge，这个过程需要7天。这极大地限制了MATIC币的流动性。因此现在MATIC币在polygon网络的DEX当中，价格十分低廉，在下图可以看到，MATIC在DEX的售价是1.54937，在CEX的售价是1.61500。如果将MATIC搬到CEX，利润高达4.2%。



详细操作

因为要和polygon链交互，所以首先要给我们的MetaMask加入polygon网络，参考 [附录-DEX使用方法-前置知识-MetaMask的使用方法](#)，和添加BSC网络一样，我们要添加polygon网络，具体参数如下：

字段	内容
网络名称	Matic 主网络
新增 RPC URL	https://rpc-mainnet.maticvigil.com/
链 ID	137
符号	MATIC
区块链浏览器 URL	https://explorer.matic.network/

polygon链是ETH的一个侧链，因此首先需要将用于买币的资产提现到ETH链上。

提取到ETH链后，打开polygon的钱包 <https://wallet.matic.network/>，进入后先登录，选择MetaMask就行。MetaMask会弹出签名请求，确认即可。



Login



Metamask

Connect using browser wallet



WalletConnect

Connect using mobile wallet



Walletlink

Connect using Coinbase wallet



Don't have wallet? [Download here](#)

然后进入polygon链的钱包页面，在资产中搜索提取出来用来买币的资产（例如USDT），点击Deposit进行充值。

\$0

Receive

Send

You might have some balance in your Ethereum Account. [Move funds to Matic Mainnet](#)

Your tokens on Matic mainnet

Hide zero balances ☐

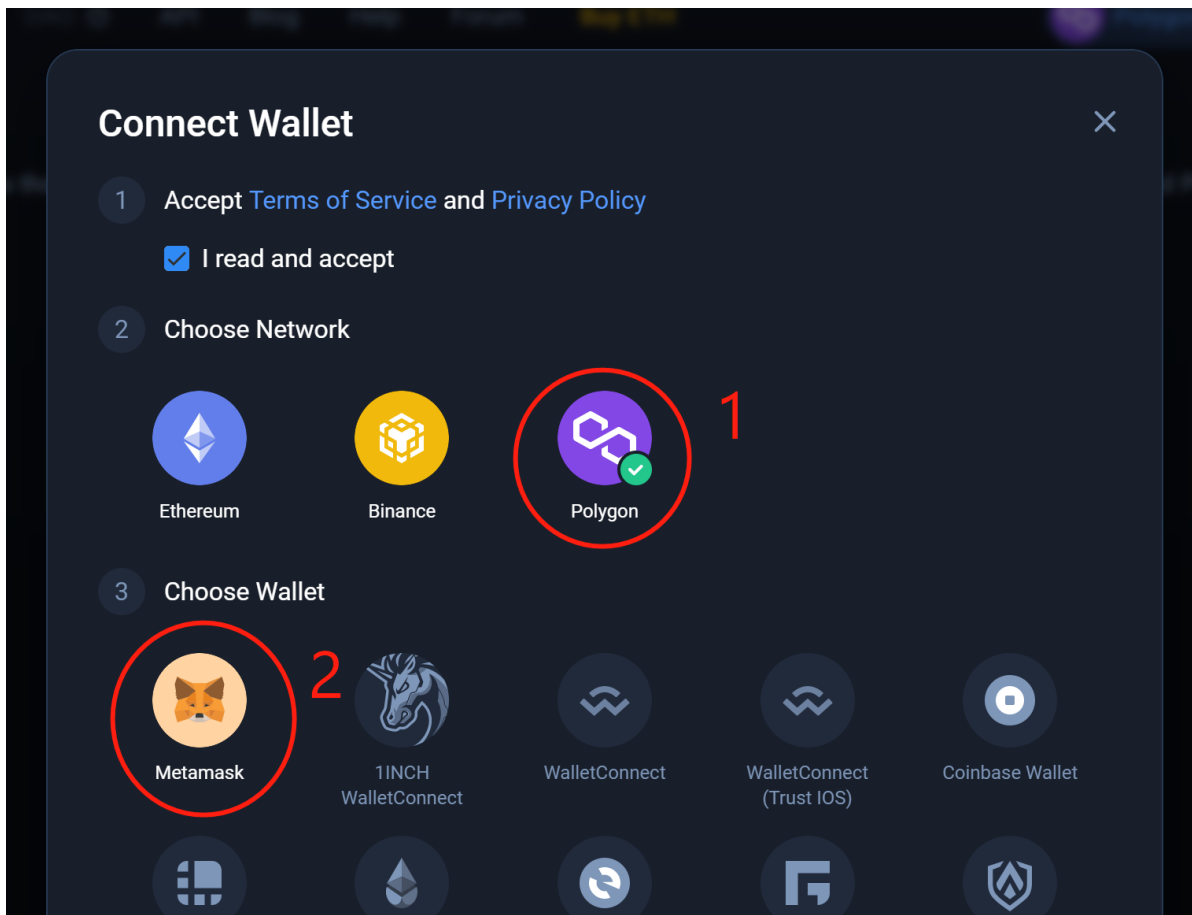
Q USDT

D	Distant Universe Stardust Token	0.00 DUST	\$0	Deposit	Withdraw	Send	:
i	IdleUSDC v4 [Best yield]	0.00 idleUSDCYield	\$0	Deposit	Withdraw	Send	:
i	IdleUSDC v4 [Risk adjusted]	0.00 idleUSDCSafe	\$0	Deposit	Withdraw	Send	:
L	LUSD Stablecoin	0.00 LUSD	\$0	Deposit	Withdraw	Send	:
U	USDT	0.00 USDT	\$0	Deposit	Withdraw	Send	:
Z	Zenfuse Trading Platform Token	0.00 ZEFU	\$0	Deposit	Withdraw	Send	:

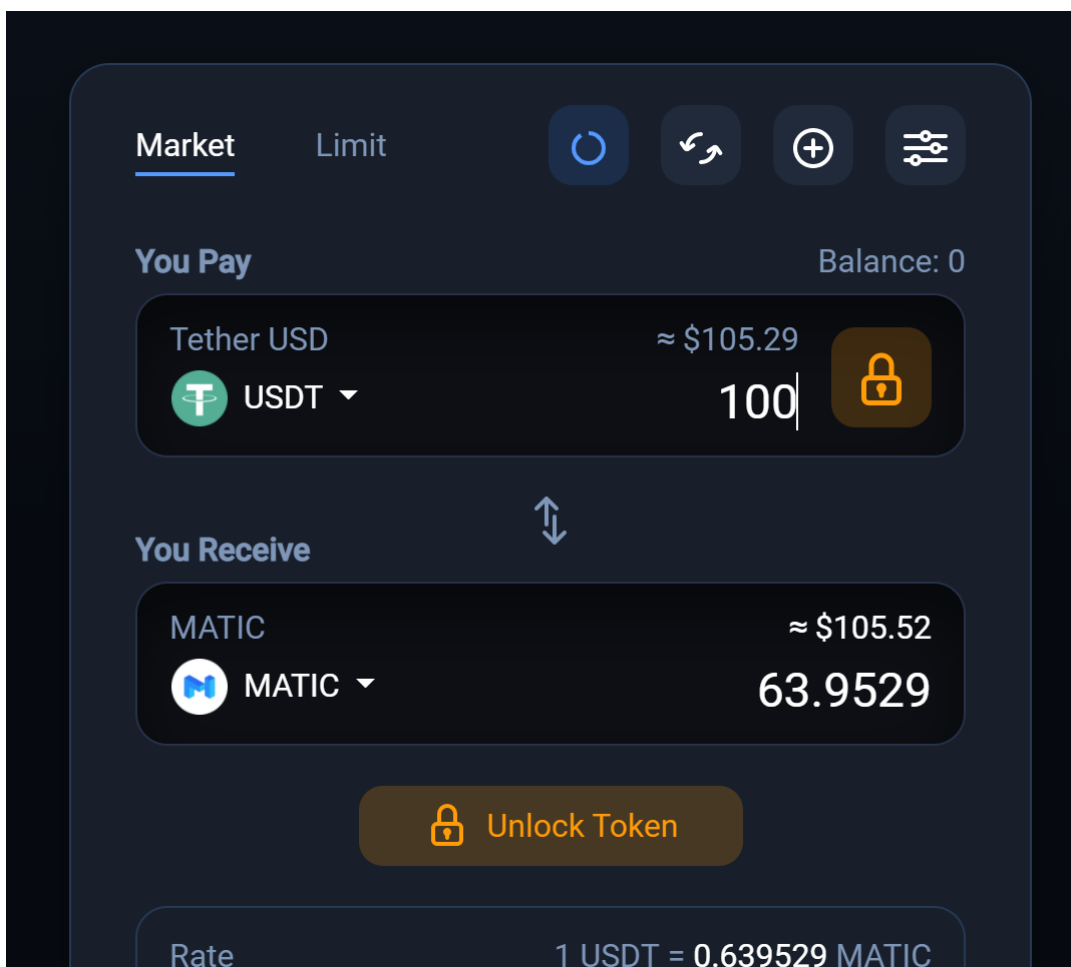
然后在接下里的这个页面里输入要充值的金额，点击Transfer，确认交易，稍等片刻，金额就会从以太坊主链转移到polygon链。

The screenshot displays a transfer interface on a blue background. At the top, a light purple box labeled 'FROM' contains the text 'Ethereum'. Below this, a white input field shows '0' with a 'MAX' button to its right. To the right of the input field is a green circular icon with a white 'T' and the text 'USDT' followed by a dropdown arrow. Below the input field, the text '\$ 0.000' is displayed. To the right of this, the text 'Available Balance: 0.000 USDT' is shown. In the center of the interface is a blue circular button with a white double-headed arrow icon and the text 'Switch' below it. Below the 'Switch' button is a light blue box labeled 'TO' containing the text 'Matic Network'. To the right of 'Matic Network', the text 'Available Balance: 0.000 USDT' is displayed. At the bottom of the interface, the text 'Transfer Mode: PoS Bridge' is shown. Below this is a large black button with the text 'Transfer' in white.

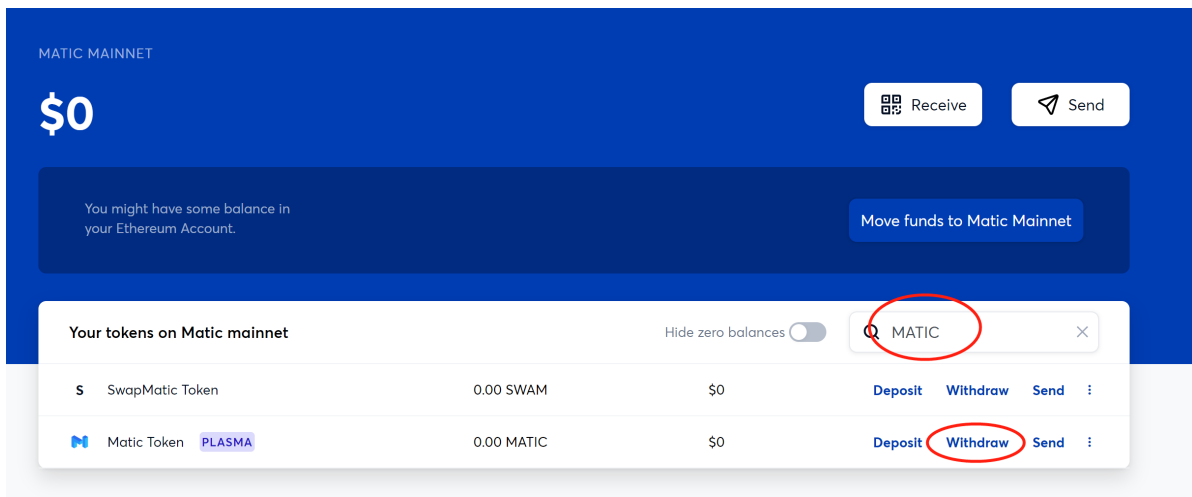
金额转移到polygon链之后，打开1inch交易所，选择polygon网络和MetaMask钱包，连接到交易所。



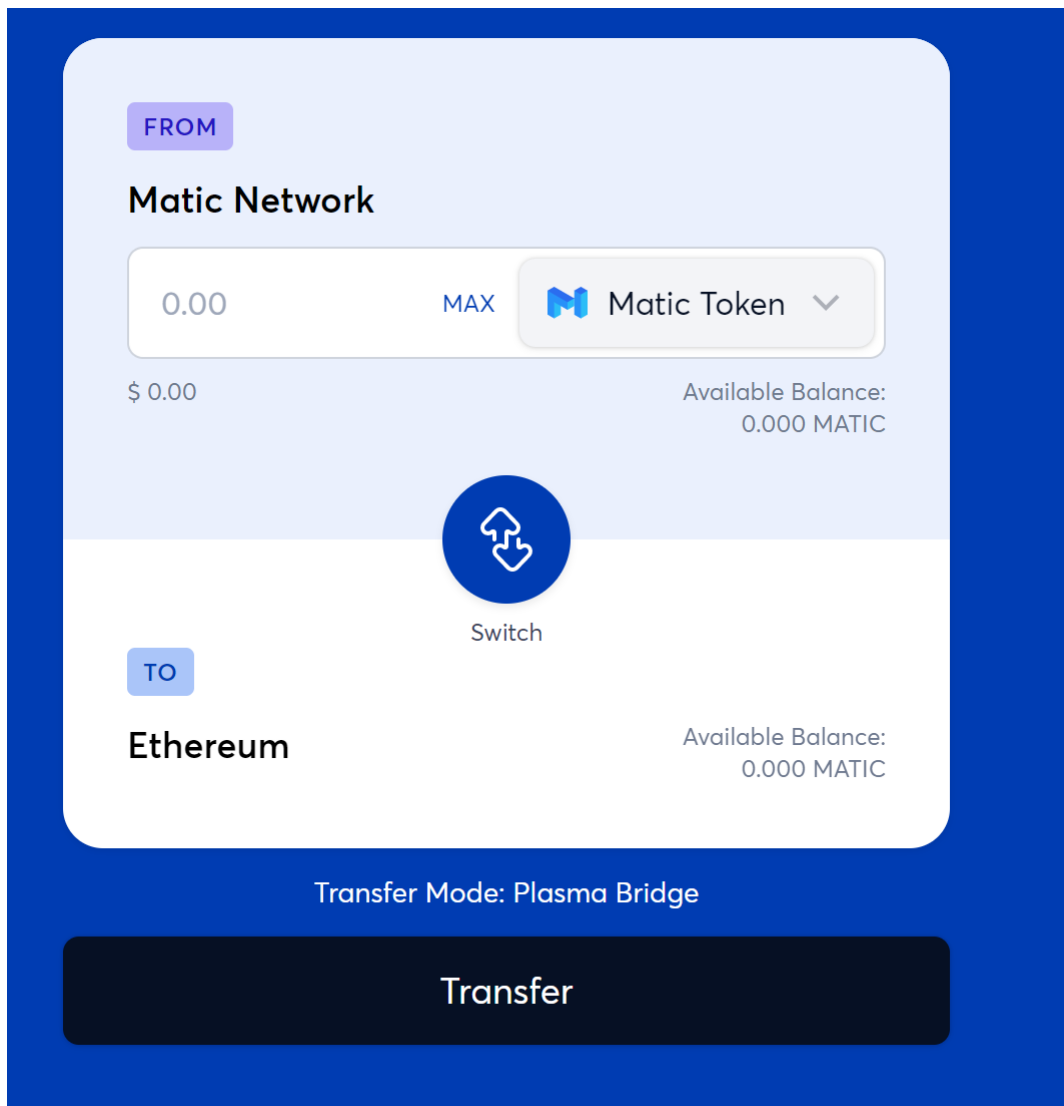
这时已经可以交易了，正常购买MATIC即可，在DEX购买MATIC的同时，不要忘记在CEX期货做空对冲。



购买MATIC之后，返回之前的polygon钱包，搜索找到MATIC币，点击Withdraw。



在提现页面输入要提现的MATIC数量，点击Transfer，确认交易。



现在，等7天之后，MATIC币就会从polygon侧链合并到ETH主网上，这时只需要将MATIC充值到交易所卖掉，再将之前用于对冲的期货平仓，就完成了一轮搬砖。

风险点

MATIC币从polygon网络发送到ETH主网需要7天时间，这7天时间MATIC会被锁仓完全无法交易，而此时期货处于做空状态，如果MATIC涨幅十分厉害，期货有爆仓风险且根本无法补充保证金（除非从外界用人民币补充保证金），所以虽然利润很高（7天4.2%），也只建议小仓位搬砖。

稳定币价差搬砖法（特殊）

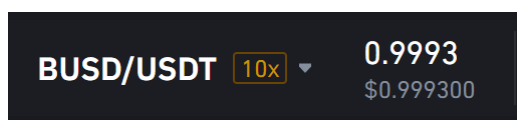
前言

在所有搬砖方法里，稳定币价差搬砖法是最为特殊的一个。

此方法极为稳定，且收益可观，但是对资金要求很高，一般不低于100万人民币。

原理

稳定币虽然与美元1:1挂钩，但是各个稳定币之间总有一丁点溢价，如下图，0.9993个BUSD就可以换到1个USDT。



那么是否存在一条路径，能够USDT->BUSD->????->????->USDT，循环一圈后资金还可以变多呢？

实际上这条路径是存在的，通常需要用脚本监控并实时计算，这就是稳定币价差搬砖法。

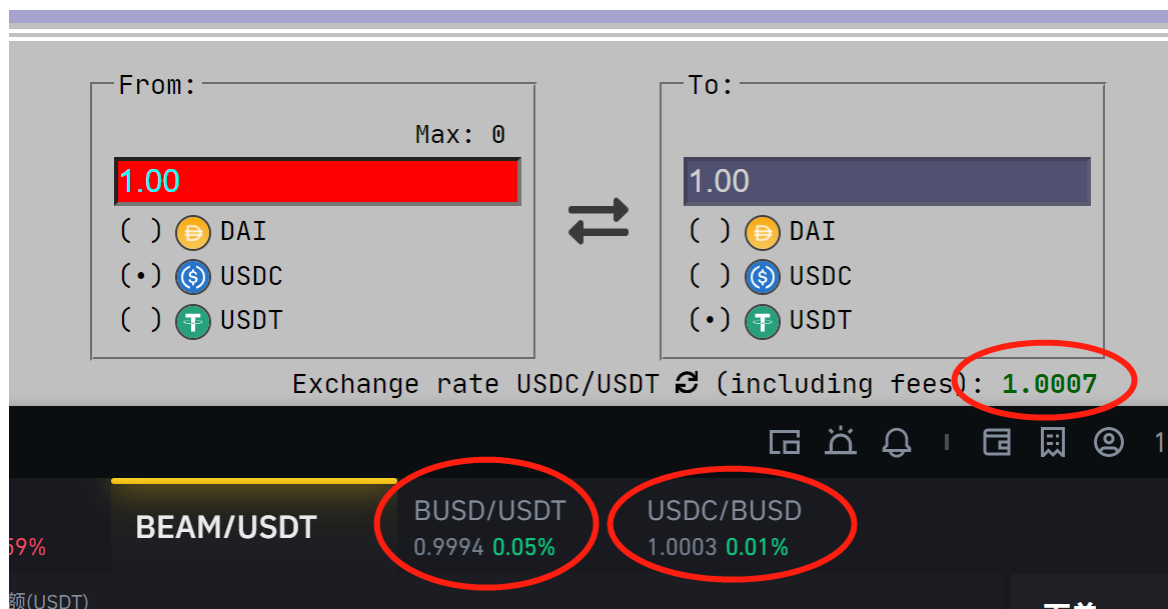
详细操作

因为交易路径的计算较为复杂，人工难以完成，且写稿时并没有搬砖的机会，因此这里由笔者对DEX价格少量修改，以此演示一遍搬砖过程。

需要说明的是，我们要用到这个网站 <https://polygon.curve.fi/aave>，这是一个专注稳定币的DEX。

我们以1USDT作为起始资金，看看沿着路径最终能变成多少。

先截取当前要用到的价格，可以看到当前价格是 0.9994 BUSD/USDT、1.0003 USDC/BUSD、1.0007 USDC/USDT。



那么假设我们现在手里有 1 USDT，交换过程如下：

- 1 USDT 换成 BUSD，得到 0.9994 BUSD
- 0.9994 BUSD 换成 USDC，得到 0.99969982 USDC
- 0.99969982 USDC 换成 USDT，得到 1.000399609874 USDT

一圈下来，我们手里的1 USDT，变成了1.000399609874 USDT，利润0.0399%，如果是1,000,000人民币本金，那么此次收益就有399.6人民币，注意这是十几分钟内赚到的。

风险点

此方法没有任何的市场风险，外部风险就是持有稳定币的时候，发行公司暴雷。或者稳定币在交易所里的时候，交易所暴雷。

后记

搬砖的套路非常简单，只需要懂得一点金融知识就可以做，难点在于机会的寻找、把握和风险控制，这也对系统的开发有比较高的要求。

附录

钱包密钥知识扩展

钱包密钥方面，通常会接触到3样东西，助记词、私钥、地址。

他们之间的关系可以描述为 助记词->私钥->地址。

助记词可以按照特定的算法按照顺序生成私钥，所以掌握一个助记词，相当于掌握N个不同的私钥。而私钥不能反推出助记词，每个私钥都是一个独立的账户。

BSC和以太坊用的是几乎一样的算法，因此在BSC上的私钥，在以太坊上面也能用，地址是一模一样的。

有时候我们会看到地址里面大小写掺杂的情况，例如笔者的账户地址

`0xF55a2c087417Ee99d8cdFeF9BA50d974a09685cf`，但地址实际上是不分大小写的，把地址全部写成大写，或者全部写成小写，都不影响使用。但这种大小写掺杂的写法包含了“校验”信息，遵循EIP55协议，如果大小写出现了问题，就说明这个地址有误，避免了用户将资产发送到错误的地址里面。

DEX使用方法

前置知识

在以太坊或者BSC区块链进行交易首先需要掌握两样东西：

- 钱包的使用，以MetaMask为例
- 区块链浏览器的使用，以BscScan为例

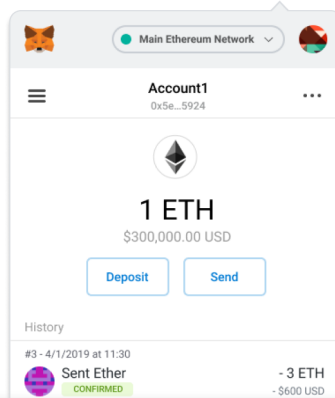
MetaMask的使用方法

使用DeFi需要有钱包来给区块链应用授权，为此你需要创建一个新的钱包，推荐使用圈内公认的MetaMask，他是一个开源钱包，官网是metamask.io，我们需要下载其浏览器插件。

直接点击下方的 `Install MetaMask for Chrome` 就可以跳转到Chrome插件应用商店。Edge浏览器也可以安装。

[Chrome](#)
[iOS](#)
[Android](#)

Install MetaMask for your browser


[Install MetaMask for Chrome](#)

下载安装之后根据提示创建新的账户，一定要将生成的助记词多处备份，助记词丢失意味着账户里所有的资产全部丢失！

助憶詞

助憶詞將可協助您用更簡單的方式備份帳戶資訊。

警告: 絕對不要洩漏您的助憶詞。任何人只要得知助憶詞代表他可以竊取您所有的以太幣和代幣。

island lamp ankle print sun ketchup
winter diamond illegal extra rain
hungry

[稍後提醒我](#)
[下一頁](#)

提示:

您可以用密碼管理系統例如 1Password 等軟體儲存助憶詞。

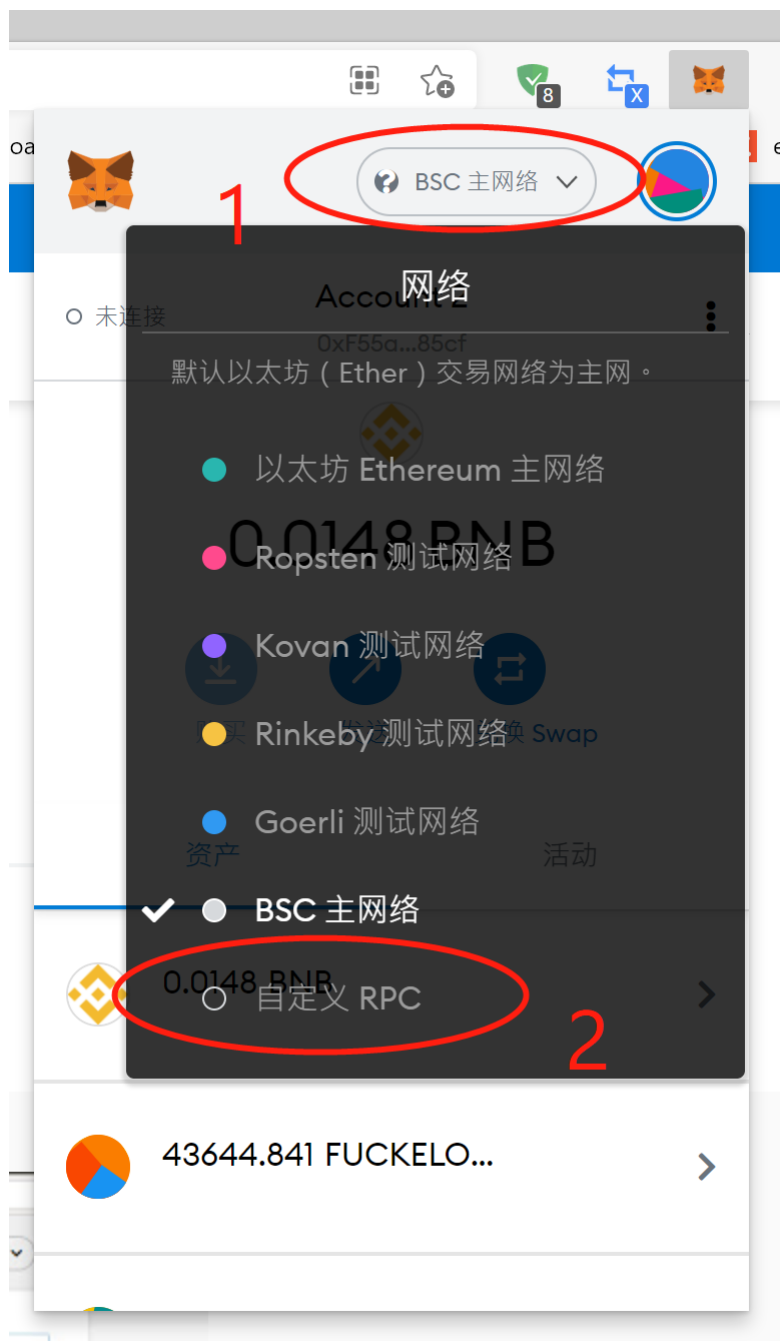
將助憶詞寫在紙上，並保存在安全的場所。若想要更安全，將助憶詞分別寫在不同紙張上並存放在不同的地方。

絕對不要忘記您的助憶詞。

下載助憶詞文字檔案，並安全的保存在有加密功能的外接硬碟或其他儲存裝置。

绝对不要忘记这个

安装好之后已经可以访问正统的以太坊主链以及各个以太坊的测试链了。但是还没法访问BSC，我们需要将BSC的各种信息加入到软件里，才能访问BSC。



直接按照如下内容填写就好

字段	内容
网络名称	BSC 主网络
新增 RPC URL	https://bsc-dataseed1.binance.org
链 ID	56
符号	BNB
区块链浏览器 URL	https://bscscan.com



The image shows a mobile application interface for configuring a blockchain network. At the top, there is a header bar with a fox icon on the left, a dropdown menu labeled "BSC 主网络" in the center, and a circular icon on the right. Below the header, a modal window titled "网络" (Network) is displayed. The modal contains several input fields: "网络名称" (Network Name) with the value "BSC 主网络", "新增 RPC URL" (Add RPC URL) with the value "https://bsc-dataseed1.binance.org", "链 ID" (Chain ID) with the value "56", "符号 (选填)" (Symbol, optional) with the value "BNB", and "区块浏览器 URL (选填)" (Block Explorer URL, optional) with the value "https://bscscan.com". At the bottom of the modal, there are two buttons: "取消" (Cancel) and "保存" (Save).

填写之后保存，就可以随时切换到BSC网络了。

区块浏览器的使用方法

相比MetaMask来说，区块浏览器是一个更加常用的东西，MetaMask在大多数情况都是作为一个浏览器插件，为各种DeFi应用提供交易授权而已，而区块浏览器仅仅是不能授权交易，其他账户余额、交易记录、交易详情等等所有信息都可以在区块浏览器上面查看。

以太坊的区块浏览器是 <https://etherscan.io/>，BSC的区块浏览器是 <https://bscscan.com/>。两个区块浏览器的功能和页面布局非常相似，所以这里以笔者的BSC账户作为演示介绍。

打开 <https://bscscan.com/>，主页直接就有搜索框。

Binance Smart Chain Explorer

All Filters

Search by Address / Txn Hash / Block / Token



BNB PRICE

\$325.58 @ 0.009078 BTC (-13.69%)



LATEST BLOCK

7800860 (3.0s)

569.

搜索笔者的账户地址 `0xF55a2c087417Ee99d8cDfEf9BA50d974a09685cf`，可以查看笔者账户的所有信息。

Address 0xf55a2c087417Ee99d8cDfE9BA50d974a09685cf

BuyExchangeEarnGaming

Overview

Balance:0.014830253957138184 BNB

BNB Value:\$5.02 (@ \$338.78/BNB)

TOKEN: \$71.94

More Info

My Name Tag: Not Available, login to update

TransactionsInternal Txns

Latest 25 from a total of 25 transactions

Search for Token Name

BEP-20 Tokens (3)

Binance-Peg ... (BTCB)\$71.940.0019441 BTCB@37,002.3927

Fuck Elon mu... (FUCKEL...)43,500.00013369 FUCKELON

SHIBA INU (SHIB)302,115 SHIB

Txn Hash	To	Value	[Txn Fee]
0x60ff429d463ecf0879a...	OUT	PancakeSwap: Router v2	0.000498895531204 BNB0.00105255
0xf172fcc200f9d0c3595cf...	OUT	0xc4b65a780c3233245...	0 BNB0.00010908
0x2500514255e082dc50...	OUT	0xf307910a4c7bbc7969...	0 BNB0.000180745
0xcd0cbc35c40e45e1e...	OUT	0xf307910a4c7bbc7969...	0 BNB0.00022203
0x3d8fb7af23e47d88a6c...	OUT	BUSD-T Stablecoin	0 BNB0.000180635
0xecd9f14bd1f0c321d1b...	OUT	BUSD-T Stablecoin	0 BNB0.00022203
0xa69009ca9a352b4f50...	OUT	BUSD-T Stablecoin	0 BNB0.000105695
0xd7033a5a44a0c32598e...	OUT	1inch: Router V3	0 BNB0.001340145
0x2d1a1169601561af44...	OUT	BUSD-T Stablecoin	0 BNB0.000180695

所持代币的余额及市值

交易记录

每笔交易都使用Transaction Hash进行区分，通常简称Txn或者tx id，可以搜索笔者的这笔交易0x97dfd9bbca3e0619494f626d290e7b89a3ec0d279f0703171f4397d88cda31a5。

Transaction Details

Buy

Exchange

Earn

Overview

Comments

Transaction Hash:

0x97dfd9bbca3e0619494f626d290e7b89a3ec0d279f0703171f4397d88cda31a5

交易哈希

Status:

Success

交易状态

Block:

6618375

1185232 Block Confirmations

被打包到了哪个编号的区块里面

Timestamp:

41 days 23 hrs ago (Apr-16-2021 02:31:06 PM +UTC)

交易时间

From:

0xf8b5c45c6388c9ee12546061786026aeea4b682

转账来源

To:

0xf55a2c087417ee99d8cdfef9ba50d974a09685cf

转账目的地址（笔者账户）

Value:

0.03 BNB

(\$10.23)

转账金额

Transaction Fee:

0.000105 BNB

(\$0.04)

这笔交易花掉的手续费

BNB Price:

\$508.96 / BNB

转账当时的BNB价格

Click to see More

Private Note:

To access the Private Note feature, you must be [Logged In](#)

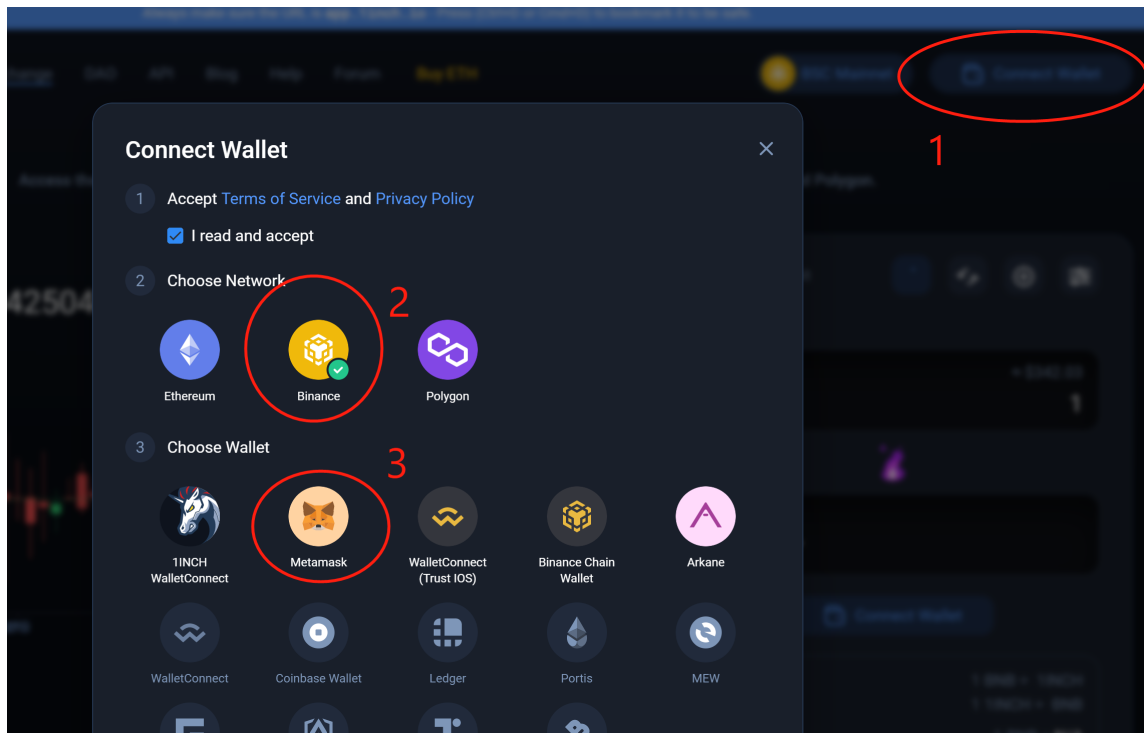
使用方法

知道钱包和区块链浏览器怎么用之后，就可以开始玩DeFi了。

玩DeFi之前起码要让账户里有几美元的BNB作为手续费和交易资金，通常是在中心化交易所入金，然后买BNB，再提现到自己区块链的钱包里。如果暂时还不想到中心化交易所开户，可以找朋友买点。

DeFi的交易所众多，最为出名的当属1inch，地址是 <https://app.1inch.io/>，这里也用1inch交易一次作为教程。

先打开1inch，点击右上角的Connect Wallet，网络选择Binance，钱包选择MetaMask。



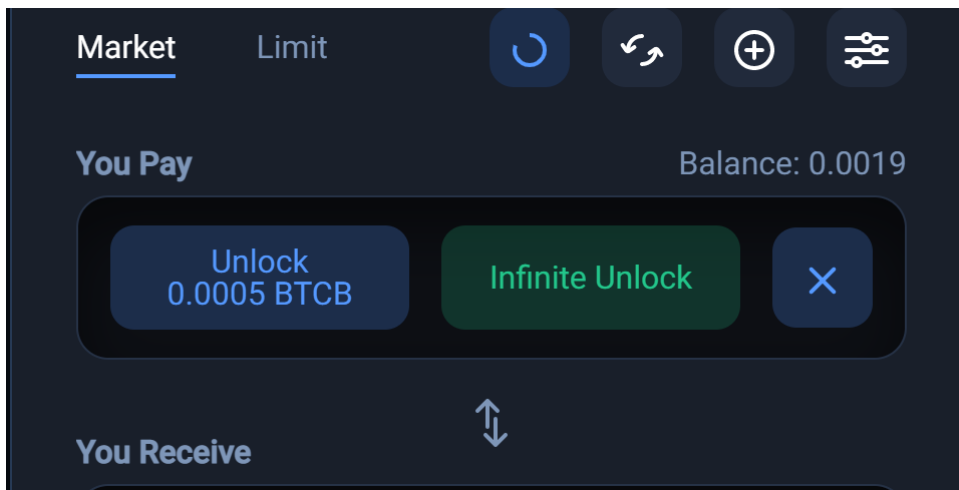
右上角的MetaMask插件会弹出窗口请求授权，选择要授权的账户点击确认即可。

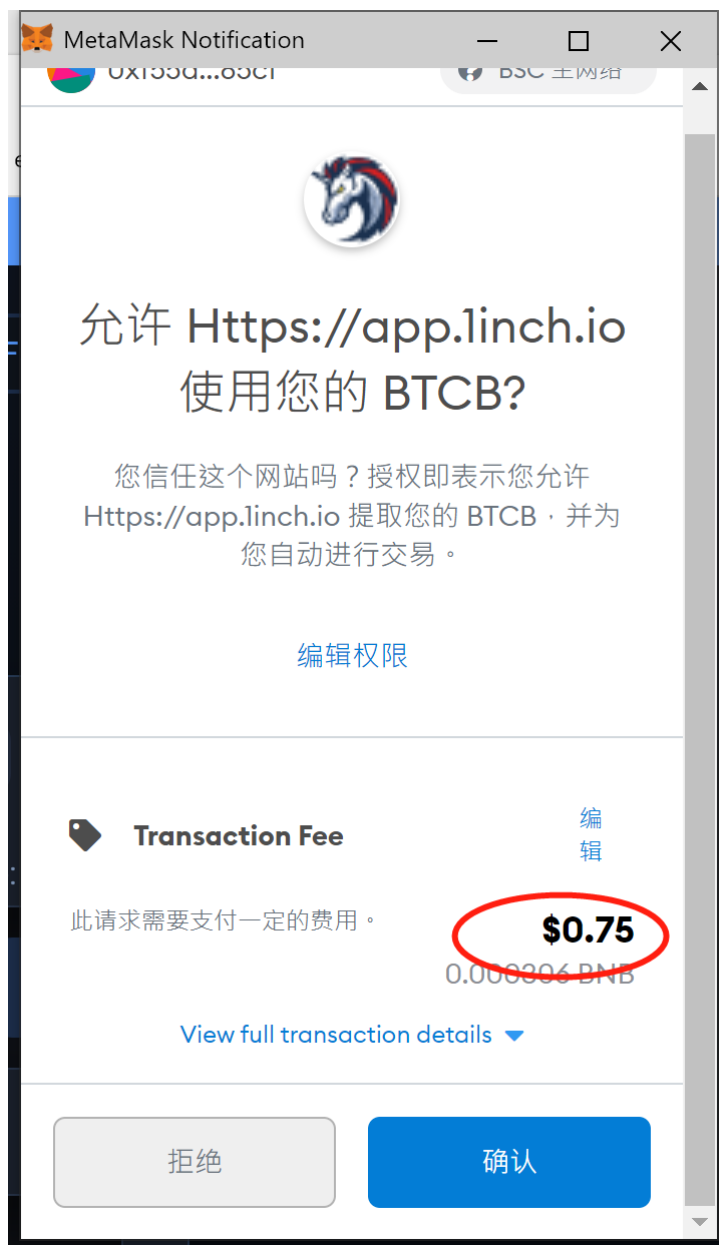
确认授权之后就可以开始交易，1inch的交易界面如下。



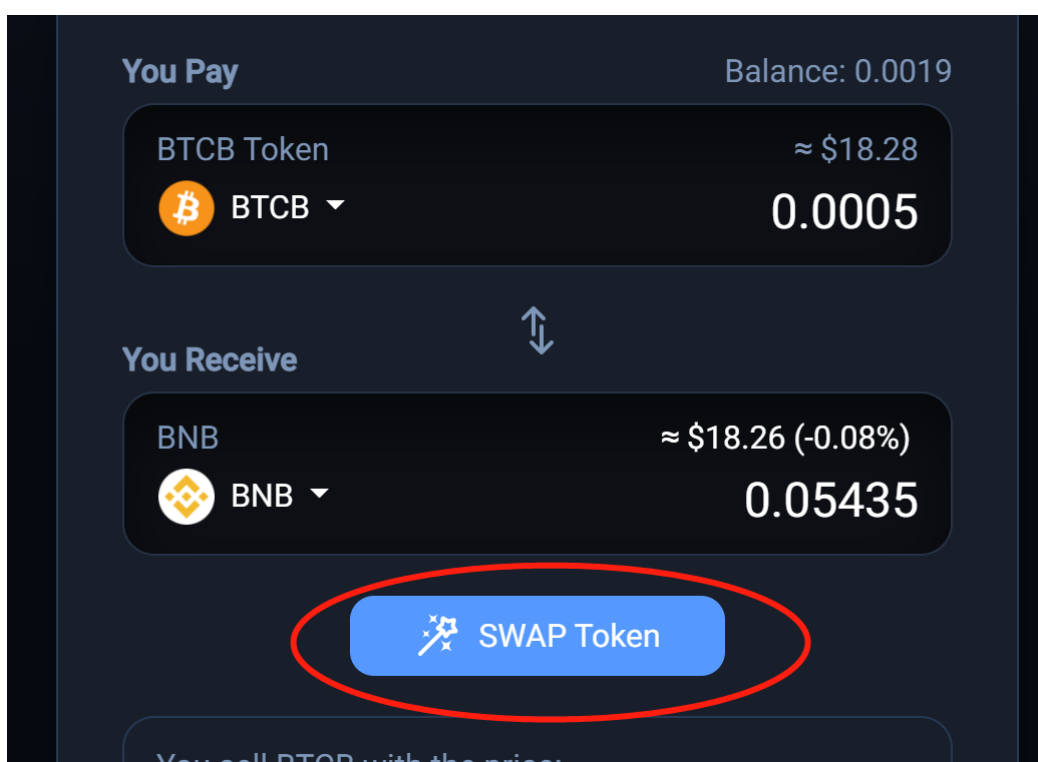
可以看到当前交易按钮显示Unlock Token，说明当前想要支付的货币没有在这个网站上面授权使用额度，我们需要点击解锁按钮。

点击解锁按钮可以看到有两个选项，一个是解锁本次交易要用到的数额，一个是解锁无限数额（实际上是大约 10^{59} 个）。一般来说，只要这个应用足够安全，就推荐解锁所有数额，因为每次解锁都需要消耗交易费。






解锁之后就可以看到交易按钮变成了Swap Token，此时点击这个按钮就可以发起交易。




然后会弹出确认单，上面详细显示了本次交易的所有信息，包括你需要支付的代币数量、可能会收到的代币数量、交易手续费等等。

Confirm Swap

 BTCB ≈ \$18.27
0.0005

↓

 BNB ≈ \$18.26 (-0.08%)
0.054326967859820622


You sell BTCB with the price:
1 BTCB = **108.6539357** BNB (≈\$36,510.98)

You buy BNB with Price:
1 BNB = **0.0092035** BTCB (≈\$336.29)

Minimum received 0.05378 BNB

Price Impact 0.08 %

Transaction cost ≈ \$0.41 (0.001212474 BNB)

 Confirm Swap

和授权额度一样，交易也需要授权，从下图可以看到，交易类型是swap，燃料价格默认为6。这些数据都是交易所计算出来的，一般不需要改，直接点确认就发起交易了。



来看看这次的交易结果，此次交易的tx是

0x89df4ead6687757521fd567e72e8e18e79c16e423fab2d02b11ac968297c3e2，可以从Token Transferred看到，我们用0.0005个BTCB，换到了0.05432个BNB，这和交易确认单上显示的一致。交易手续费是价值0.36美元的BNB，比确认单上估算的手续费略便宜一点。

Overview

Internal Txns

Logs (7)

Comments

Transaction Hash:

0x89df4ead6687757521fd567e72e8e18e79c16e423fabcd02b11ac968297c3e2

Status:

Success

Block:

7805654

32 Block Confirmations

Timestamp:

1 min ago (May-28-2021 03:22:17 PM +UTC)

From:

0xf55a2c087417ee99d8cdfef9ba50d974a09685cf

Interacted With (To):

Contract 0x11111112542d85b3ef69ae05771c2dccc4faa26 (1inch: Router V3)

TRANSFER 0.054326967859820622 BNB From [Binance: WBNB ...](#) To → [1inch v3: R...](#)

TRANSFER 0.054326967859820622 BNB From [1inch v3: Router](#) To → [0xf55a2c087417ee99d8cdfef...](#)

Tokens Transferred: 2

From 0xf55a2c087417e... To 0x1b1675a97b2f6... For 0.0005 (\$18.38)

Binance-Peg ... (BTCB)

From 0x1b1675a97b2f6... To 1inch v3: Router For 0.054326967859820622 (\$18.40)

Wrapped BNB (WBNB)

Value:

0 BNB (\$0.00)

Transaction Fee:

0.001068732 BNB (\$0.36)

Click to see More

Private Note:

To access the Private Note feature, you must be [Logged In](#)

作者信息

- 作者：sukidesuka 联系方式：电报@sukidesuka
- 审校、顾问：花白