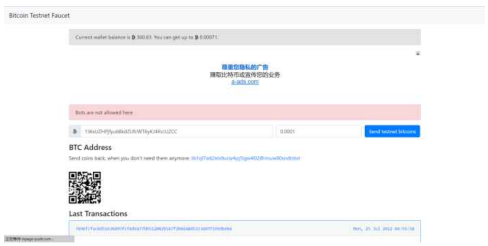
分析比特币交易

一.在测试网站中发起一笔交易

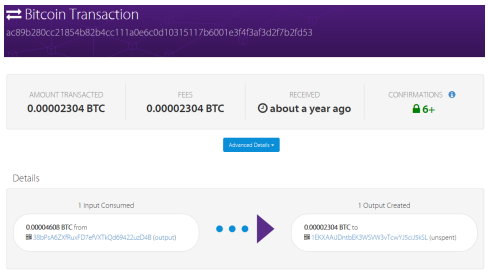
获取公私钥对

获取测试币



创建一笔交易并查看（由于无法注册比特币账户，后续所选资料为网上资料）

通过blockcypher的API接口可以拿到更加详细的JSON数据



二.得到的交易原始数据

**0100000001f744bec7dd6c33cf384c8a4cb33269ca48c940e5852410d395807f6e56f673430100
0000fd5e0100483045022100bd16b2ffa11293785671690916 2c00a66e7c5e6cccd0093ec9aece
127632f8dc02205a567c53161e5fb62ac8d202acf8f8cc2f5a6496f47a878555dae7ffde85a41d0
1483045022100ac3c0365e103d97d3cc935755d5177e8f383993a558998200f8537e64f6b5200
02202216716f7fa54adc69095c4127ff6f97d42e28517a103f7691808db3cde6ee5b014cc95241
04a7ada7c84ae36e98735597ee770a7cfd2d5d9398154b088ee352d3a83b21bbf537c0b8e4ea
0acc172285b37571a9b1e36c0da387d6d1f361f0b65cad5c3f659e4104fe411f77e5aa50b54e0f
2be0204b26cd1d2bf77bf95f2108a6b012e34637289121cd351c696c8a519b4b58674a87e7907
385b4a5e7c0cfa5019346c1b04040914104eeffa9bbfe6dd2c99a9747ca5d1c1ebd15fe0344f52
ff2915e3c11b3be9be11236895e5514b085c1f8a1bd8ef9c3db0cf1095aaf442cae11d88c3af02
6fabd1653aeffffffff0100090000000000001976a914921a4c141746bbd7beb8e81b05ba93d84
b076a0088ac00000000**

三.分析

01000000 版本号

01 交易数量

f744bec7dd6c33cf384c8a4cb33269ca48c940e5852410d395807f6e56f
67343 UTXO

01000000 UTXO的index

fd5e01 需要解锁的Input长度

0048304502210 0bd16b2ffa1129378567169091 62c00a66e7c5e6cccd0093ec9aece127632f8dc02205a567c53161e5fb62ac8d202acf8f8cc2f5a6496f47a878555dae7ffde85a41d014830450221 00ac3c0365e103d97d3cc935755d5177e8f383993a558998200f8537e64f6b5200022022167 16f7fa54adc69095c4127ff6f97d42e28517a103f7691808db3cde6ee5b014cc9524104a7ada7c84ae36e98735597ee770a7cfd2d5d9398154b088ee352d3a83b21bbf537c0b8e4ea0acc172285b37571a9b1e36c0da387d6d1f361f0b65cad5c3f659e4104fe411f77e5aa50b54e0f2be0204b26cd1d2bf77bf95f2108a6b012e34637289121cd351c696c8a519b4b58674a87e7907385b4a5e7c0cfa5019346c1b04040914104eeffa9bbfe6dd2c99a9747ca5d1c1ebd15fe0344f52ff2915e3c11b3be9be11236895e5514b085c1f8a1bd8ef9c3db0cf1095aaf442cae11d88c3af026fabd1653ae 需要解锁的Input

01 交易输出的数量

0009000000000000 交易的金额

19 给Ouput加锁的长度

76a914921a4c141746bbd7beb8e81b05ba93d84b076a0088ac 给Ouput加锁

00000000 时间戳

四.补充

一个用户想要使用比特币时，需要解锁上一次交易时加锁的内容并付款给矿工。

时间戳影响用户可以在多久后使用此比特币