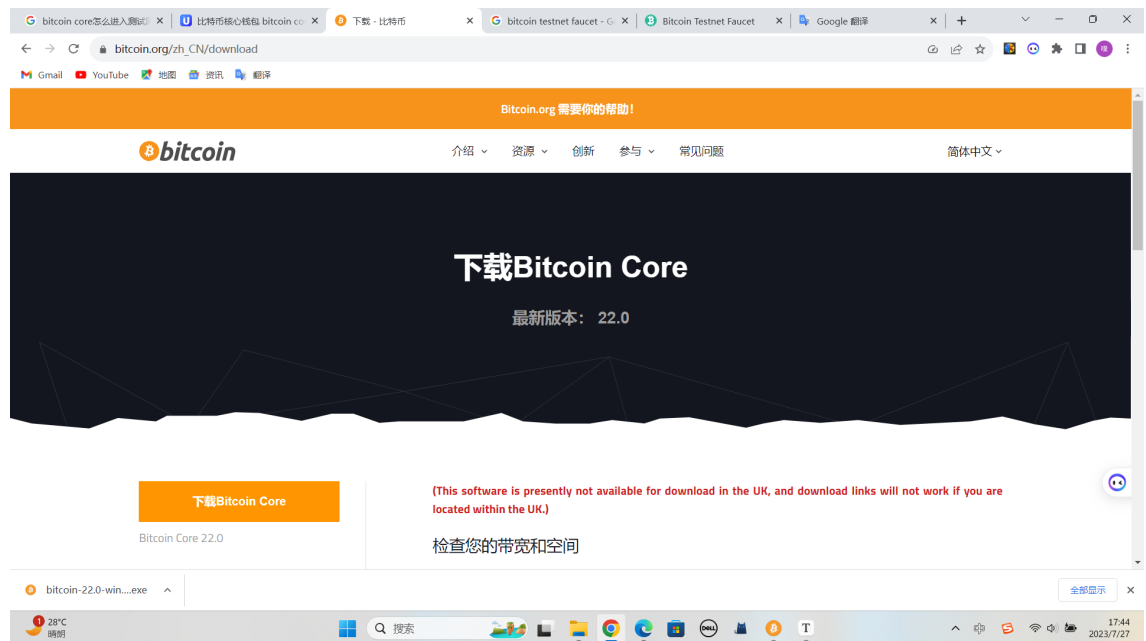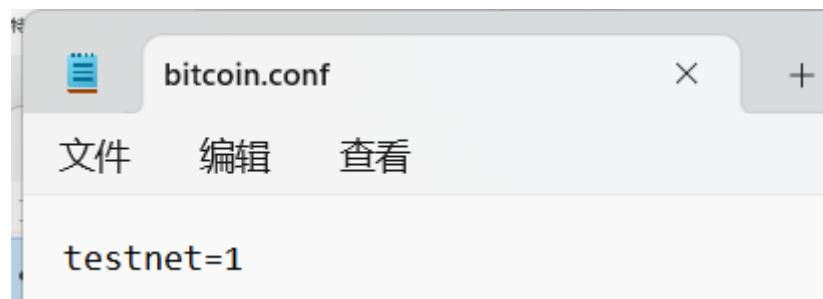## 2.18 - send a tx on Bitcoin testnet, and parse the tx data down to every bit
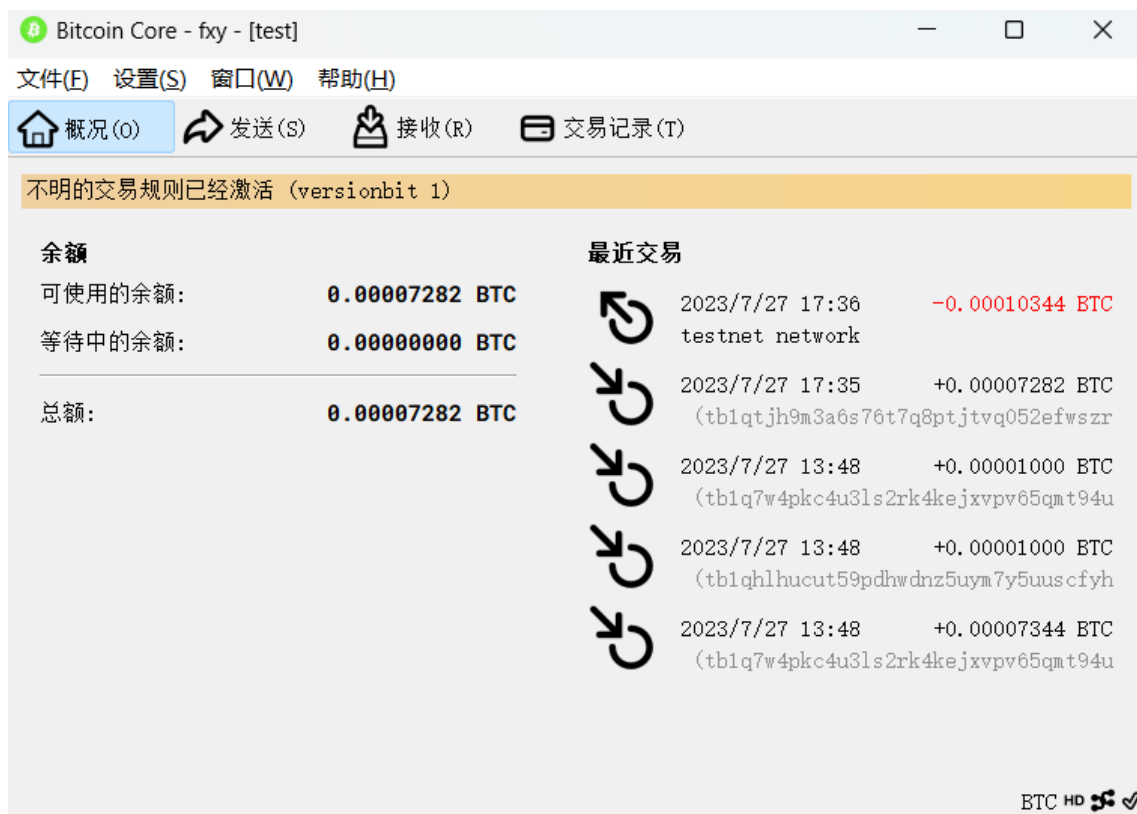
1. 发送交易

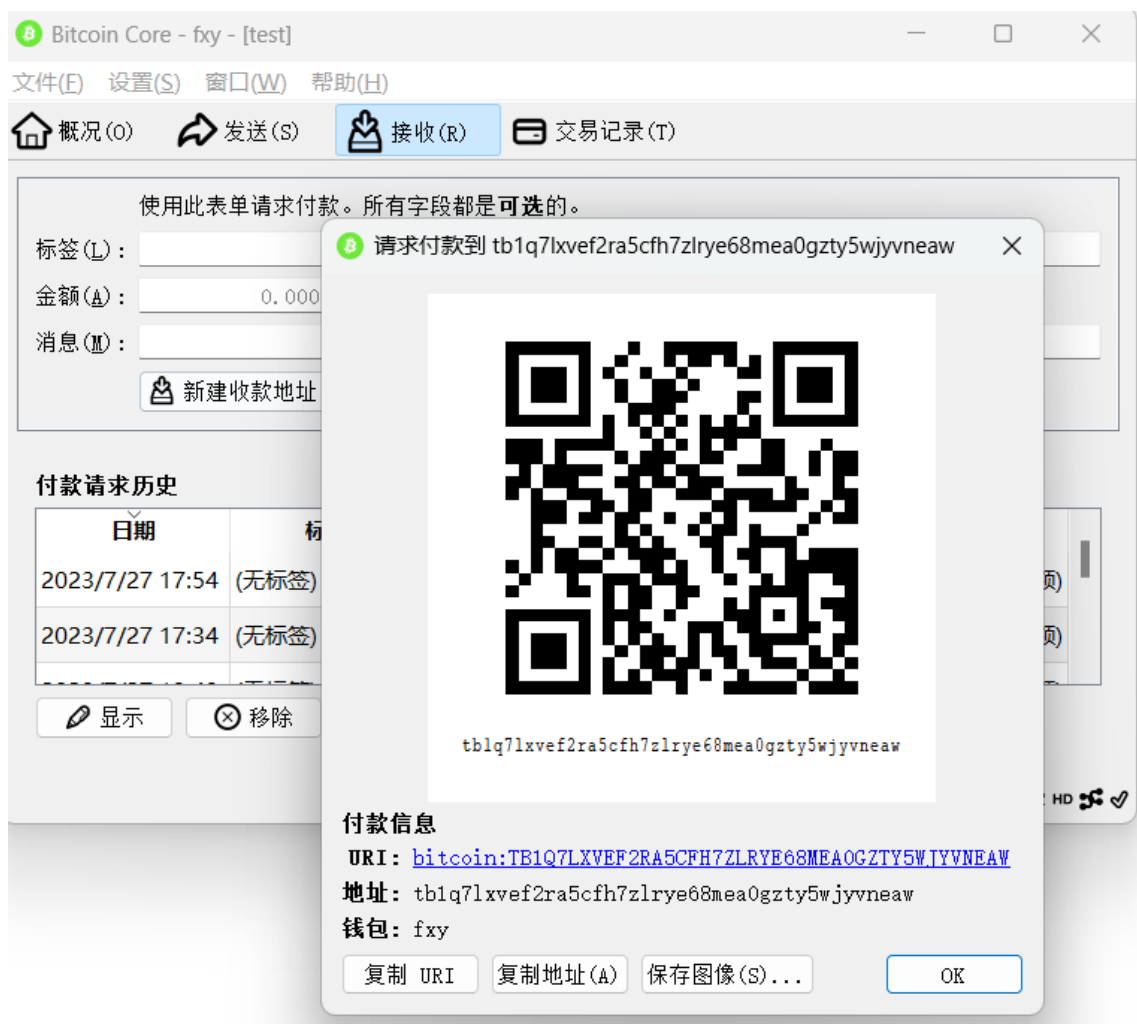我使用的本地搭建Bitcoin Core来进行接收发送交易，首先是下载Bitcoin Core：

之后安装完成后打开会提示会下载从2009开始的完整的区块链，大约是420G，这是真正的Bitcoin的主网络。在这个上面进行交易用的是真正的比特币，大可不必。所以需要先要将主网络修改为Bitcoin的测试网络，修改方法是更改Bitcoin Core的配置文件添加"testnet =1"语句，之后重启Bitcoin Core就切换到测试网络了。切换成功后会自动同步测试网络，整个数据大约为33GB。同步完成后就可以正常使用了。之后为了正常使用需要先创建一个钱包，我这个叫"fxy"。
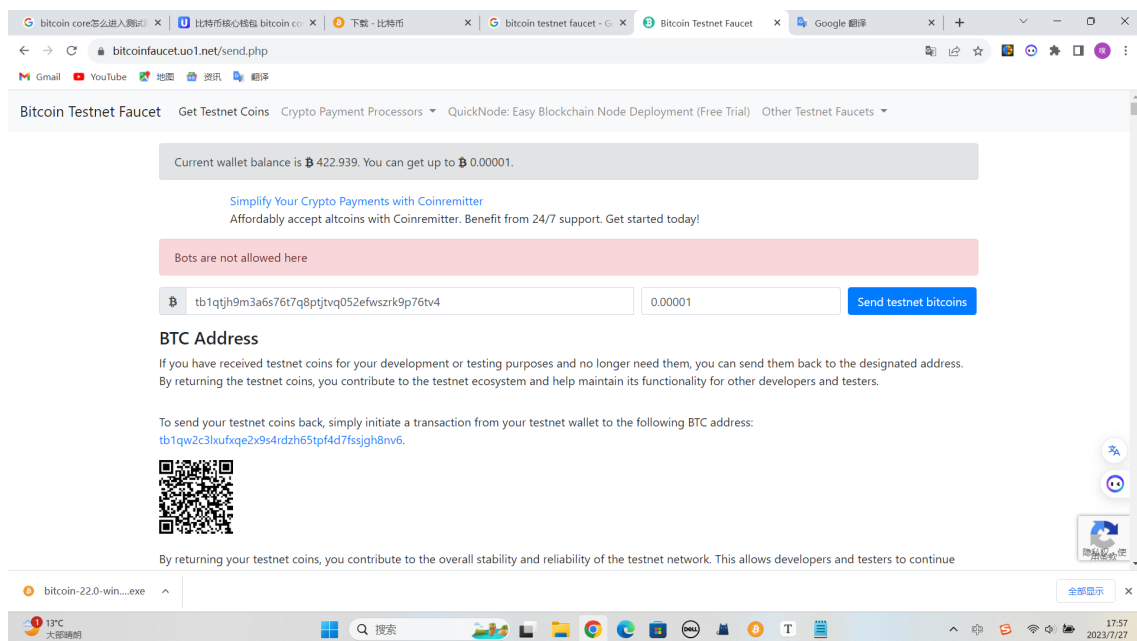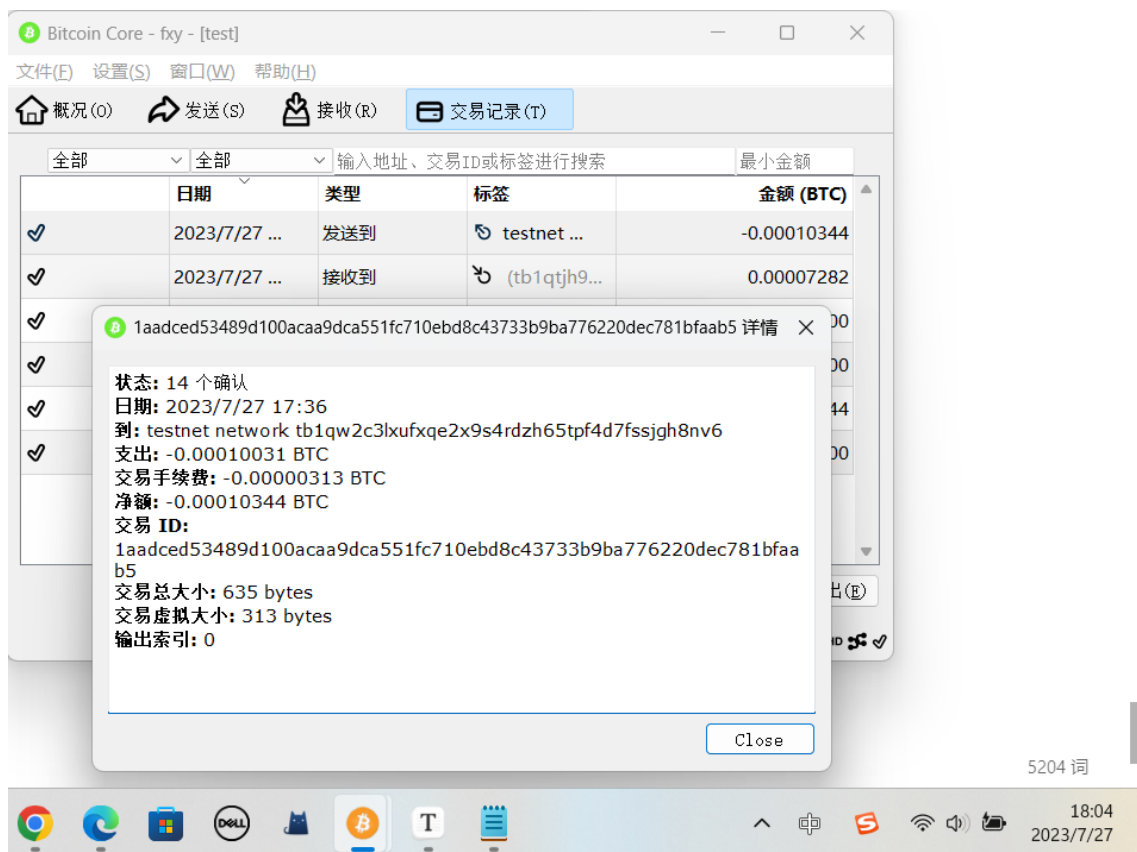
之后为发送一笔交易，先要获得一笔比特币，首先是创建自己的收款地址，在接收中新建收款地址：

然后去网上找一个水龙头网站给这个咱生成的地址发送一些测试比特币：

这样Bitcoin Core就会接收这些测试比特币，测试网络和主网络一样需要经过几次确认才可以正常使用，大约等待十几分钟就行了。之后等已经确认完成后，即可使用余额不为零就可以发送交易了。只需要在发送中输入金额等信息然后确认签名发送就完成了。发送之后点击这笔交易就可以看到详细信息，如下：

之后为了得到更详细的数据可以到特定网站解析交易ID，如下：

2. 解析数据

我这笔交易的ID为
1aadced53489d100acaa9dca551fc710ebd8c43733b9ba776220dec781bfaab5。在上面这个网站可以看到该笔交易的Hex值：

之后该网站下可以直接转换该Hex，结果如下：

```
{
    "addresses": [
        "tb1q5kcnmg78yv7zrvhu7843z8yj9glmv7mz6hlz8d",
        "tb1q7w4pkc4u3ls2rk4kejxvpv65qmt94u8qqwk86j",
        "tb1qw2c3lxufxqe2x9s4rdzh65tpf4d7fssjgh8nv6",
        "tb1qhlhucut59pdhwdnz5uym7y5uuscfyhyh48wegg"
    ],
    "block_height": -1,
    "block_index": -1,
    "confirmations": 0,
    "double_spend": false,
    "fees": 313,
    "hash":
"1aadced53489d100acaa9dca551fc710ebd8c43733b9ba776220dec781bfaab5",
    "inputs": [
        {
            "addresses": [
                "tb1qhlhucut59pdhwdnz5uym7y5uuscfyhyh48wegg"
            ],
            "age": 2468585,
            "output_index": 0,
            "output_value": 1000,
            "prev_hash":
"54c73960d12b4871312fba2c58517defd5a1de396a3dad7c8aac3df7b3ca05d2",
            "script_type": "pay-to-witness-pubkey-hash",
```

            "sequence": 4294967293,
            "witness": [

"304402205214f14fb41dd8bdd824a5b38860d91c772b5d833928c7fd7d251876c539d37b0220
23250c2dcf38205ba71b0f83009a37f5e08bb23b55493e9fd48dd1e85b102a1c01",

"036a66aca48601f3d0161ac59f6f9b54a148d23078ce6157b17fdb3f20ea51bdff"
            ]
        },
        {
            "addresses": [
                "tb1q5kcnmg78yv7zrvhu7843z8yj9glmv7mz6hlz8d"
            ],
            "age": 2468584,
            "output_index": 1,
            "output_value": 1000,
            "prev_hash":
"dc44760815d094cc8a9021d3c69c5d99429f619a1087c6afaf9a1c6916cb8aa0",
            "script_type": "pay-to-witness-pubkey-hash",
            "sequence": 4294967293,
            "witness": [

"304402201c9abae972c64d72e01ba7b6990c1f41d594c8779674e75095620fe82d898b900220
329c8971a2b4ccde602ef1e506d463ce356ec93e17aaf1e791a0988b06b21aaa01",

"032fe79d9839e4cc768f95b60913322bf38ffcf66ef071777ca16b1617ea657aef"
            ]
        },
        {
            "addresses": [
                "tb1q7w4pkc4u3ls2rk4kejxvpv65qmt94u8qqwk86j"
            ],
            "age": 2468585,
            "output_index": 1,
            "output_value": 7344,
            "prev_hash":
"e96dc94bebcb88387bb025c733cdcb46b63e987673e3578937ad041c480bc8f1",
            "script_type": "pay-to-witness-pubkey-hash",
            "sequence": 4294967293,
            "witness": [

"304402204b679b74c1d72a29bcc24aa37e90d59b16cad5c2d3dafe8557766ebb0316e0c30220
746d3c2cfe0d3e3f2088b260c6f73efa0e28928ea08248eee3424172597b15b701",

"03012e16ac21389bb7b8967ff868c2f412818108325d3cab3e3909db692562a12f"
            ]
        },
        {
            "addresses": [
                "tb1q7w4pkc4u3ls2rk4kejxvpv65qmt94u8qqwk86j"
            ],
            "age": 2468585,
            "output_index": 0,
            "output_value": 1000,
            "prev_hash":
"2ad5a8c0cccd1868d74ac3e6f421991920e339db2f96bb80bc5f2b09a5d4a54b",

```
                "script_type": "pay-to-witness-pubkey-hash",
                "sequence": 4294967293,
                "witness": [

  "3044022077e79a69730ffe5e907b104c2c0c837c27a1eeabc1acf42c94c9b561668d71600220
  46ec4088410e38bef2b89e9c5ab05b4c6d2f6d003469b3779d5e1ad32ce16da901",

  "03012e16ac21389bb7b8967ff868c2f412818108325d3cab3e3909db692562a12f"
                ]
            }
        ],
        "lock_time": 2468676,
        "opt_in_rbf": true,
        "outputs": [
            {
                "addresses": [
                    "tb1qw2c3lxufxqe2x9s4rdzh65tpf4d7fssjgh8nv6"
                ],
                "script": "001472b11f9b893032a316151b457d51614d5be4c212",
                "script_type": "pay-to-witness-pubkey-hash",
                "value": 10031
            }
        ],
        "preference": "low",
        "received": "2023-07-27T10:23:11.105990444Z",
        "relayed_by": "54.86.77.44",
        "size": 635,
        "total": 10031,
        "ver": 2,
        "vin_sz": 4,
        "vout_sz": 1,
        "vsize": 313
    }
```

3. 实现环境

CPU:

CPU   11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz

所用网站:

Bitcoin Core:https://bitcoin.org/zh_CN/download

Bitcoin 水龙头:https://bitcoinfaucet.uo1.net/send.php

交易信息:https://live.blockcypher.com/btc-testnet/

交易详细信息:https://live.blockcypher.com/btc-testnet/decodetx/