比特币冷热分离

基于 NextBTC 的离线签名实验教程

@BTCDAGE

2026-03-21

Nostr: npub17ahz4xa3hvkvvhh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

目录

一、 实验环境与准备 2

二、 在线准备阶段：资金注入 5

三、【实验一】单输入 (Single UTXO) 离线签名 7

四、【实验二】多输入 (Multi-UTXO) 合并转账签名 15

五、常见问题解答 (Q&A) 21

一、 实验环境与准备

1. 实验环境：

网络环境：

NextBTC 平行链（完全兼容 Bitcoin Core 29.0 / Knots），官网地址：https://nextbtc.rf.gd。该环境能够完美模拟比特币主网的交易逻辑，非常适合开发者和资深玩家进行网络测试。隔离策略： 签名过程在物理断网的离线电脑（或禁用网卡的虚拟机）中进行，确保私钥永不触网。

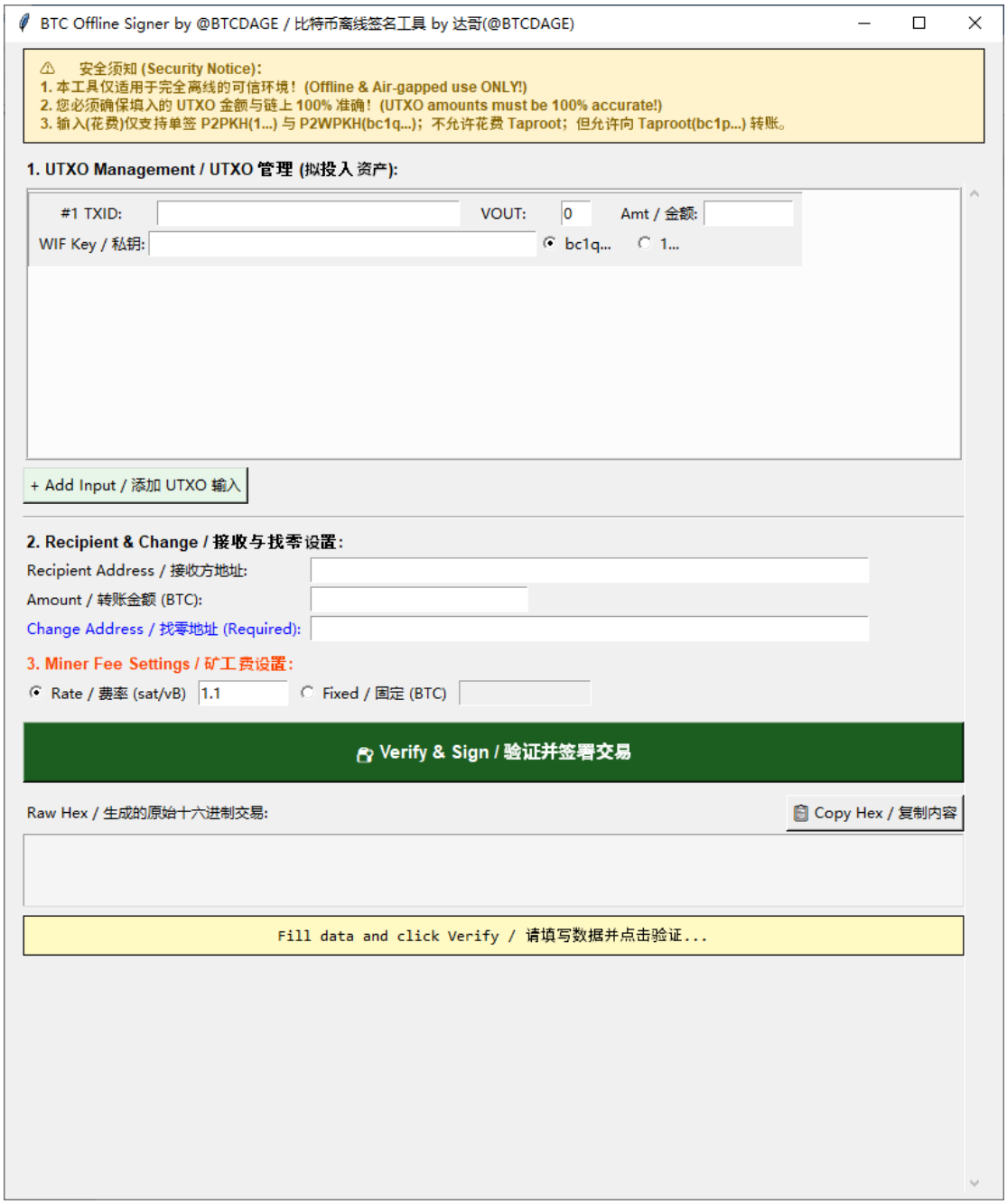
离线工具：

高级脑钱包生成器



开源地址：https://github.com/btcdage2000/BrainWalletGenerator
下载地址：https://github.com/btcdage2000/BrainWalletGenerator/releases/

比特币离线签名工具



开源地址：https://github.com/btcdage2000/BrainWalletSigner

下载地址：https://github.com/btcdage2000/BrainWalletSigner/releases/

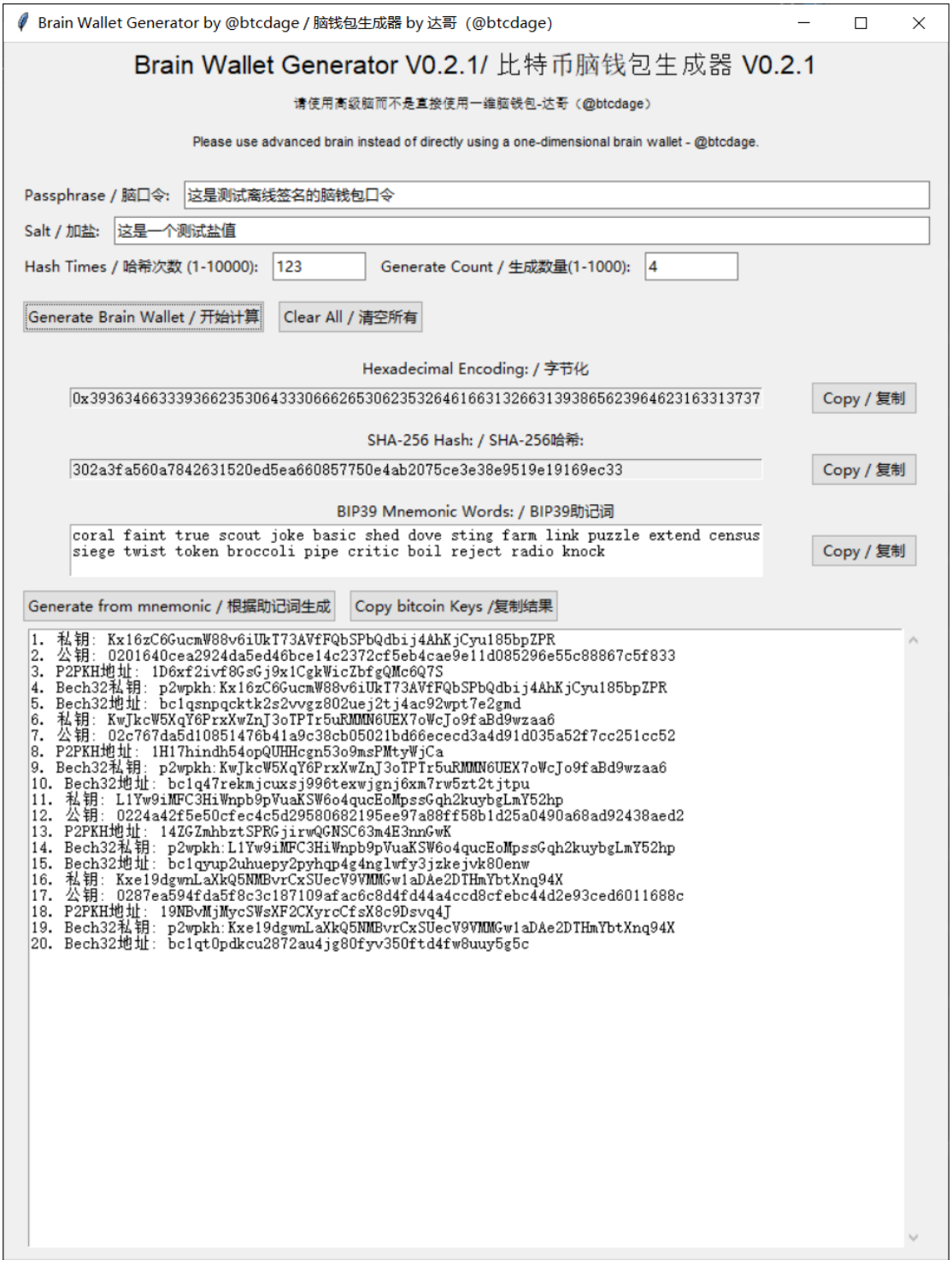
这两个离线工具永远断网运行

2. 实验准备：

使用高级脑钱包工具生成 4 组密钥对（对应地址 A、B、C、D）。

★安全警示： 在实际生产环境中，务必在离线设备上生成地址，且必须使用 20 字符以上

的高熵脑口令/盐值以防碰撞攻击。本实验仅为教学演示，故使用简易口令。
地址生成结果：



每个私钥都对应一个 Legacy 地址（1 开头）和一个 Bech32 地址（bc1 开头）。
A： 私钥 A、地址 A1 (Legacy)、地址 A2 (Bech32)。
B： 私钥 B、地址 B1 (Legacy)、地址 B2 (Bech32)。
C： 私钥 C、地址 C1 (Legacy)、地址 C2 (Bech32)。

D： 私钥 D、地址 D1 (Legacy)、地址 D2 (Bech32)。

A：

私钥 A: Kx16zC6GucmW88v6iUkT73AVfFQbSPbQdbij4AhKjCyu185bpZPR

地址 A1： 1D6xf2ivf8GsGj9x1CgkWicZbfgQMc6Q7S

地址 A2: bc1qsnpqcktk2s2vvgz802uej2tj4ac92wpt7e2gmd

B：

私钥 B: KwJkcW5XqY6PrxXwZnJ3oTPTr5uRMMN6UEX7oWcJo9faBd9wzaa6

公钥 B: 02c767da5d10851476b41a9c38cb05021bd66ececd3a4d91d035a52f7cc251cc52

地址 B1: 1H17hindh54opQUHHcgn53o9msPMtyWjCa

地址 B2: bc1q47rekmjcuxsj996texwjgnj6xm7rw5zt2tjtpu

C：

私钥 C: L1Yw9iMFC3HiWnpb9pVuaKSW6o4qucEoMpssGqh2kuybgLmY52hp

地址 C1： 14ZGZmhbztSPRGjirwQGNSC63m4E3nnGwK

地址 C2： bc1qyup2uhuepy2pyhqp4g4nglwfy3jzkejvk80enw

D:

私钥 D: Kxe19dgwnLaXkQ5NMBvrCxSUecV9VMMGw1aDAe2DTHmYbtXnq94X

公钥 D: 0287ea594fda5f8c3c187109afac6c8d4fd44a4ccd8cfebc44d2e93ced6011688c

地址 D1: 19NBvMjMycSWsXF2CXyrcCfsX8c9Dsvq4J

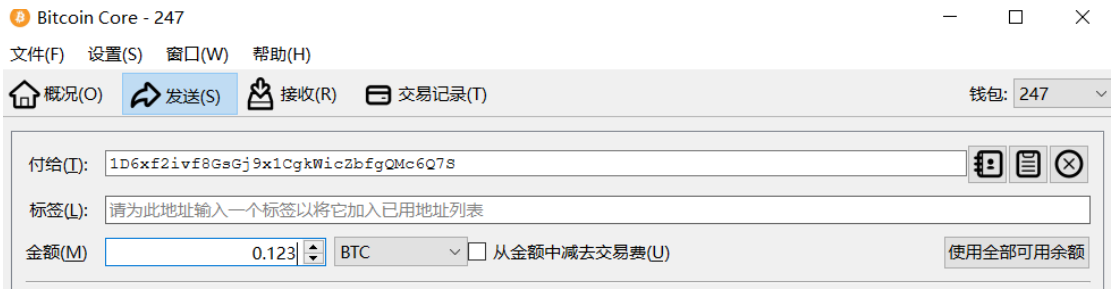
地址 D2: bc1qt0pdkcu2872au4jg80fyv350ftd4fw8uuy5g5c

二、 在线准备阶段：资金注入

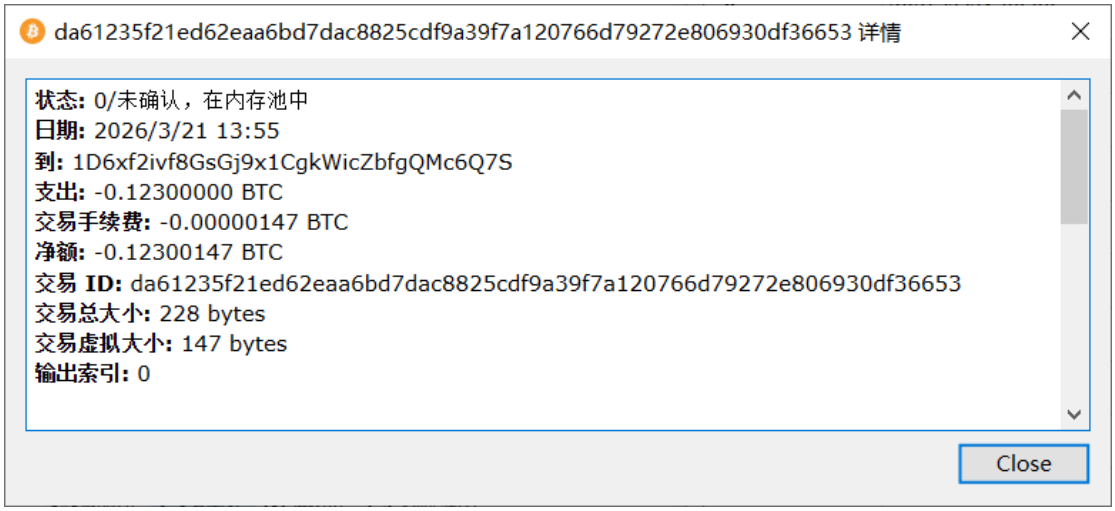
在联网环境下，向地址 A1 转入 0.123 BTC。此步骤模拟从交易所提币到高级脑地址“囤饼”的动作。

地址 A1：

1D6xf2ivf8GsGj9x1CgkWicZbfgQMc6Q7S

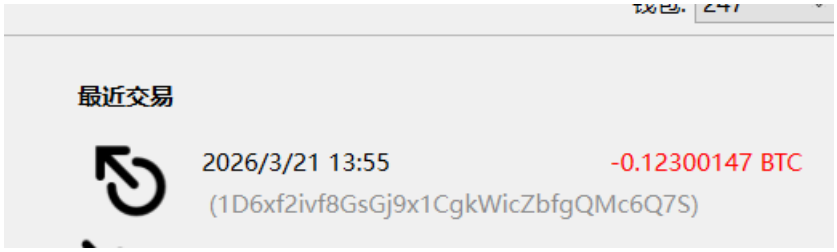


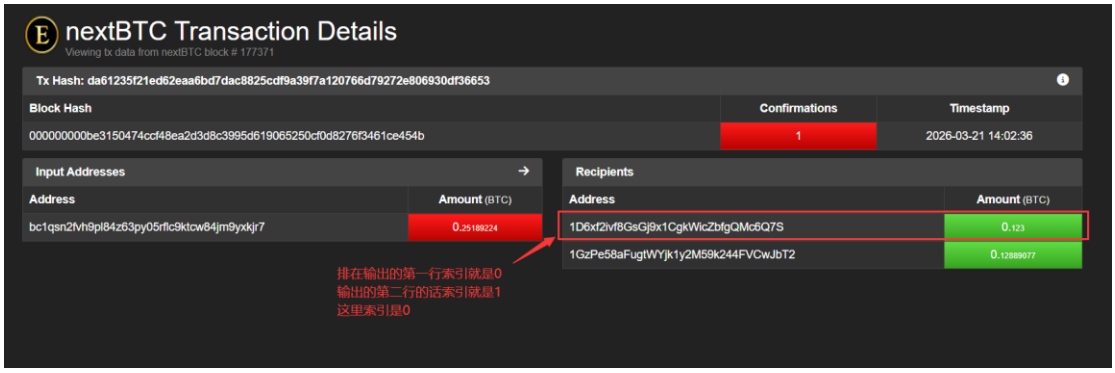


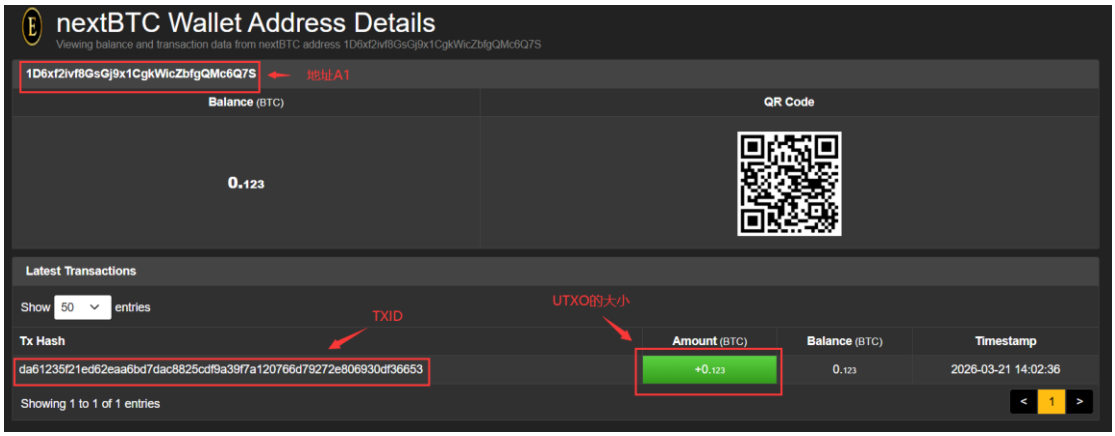


（注意，其实这里就可以看到移动一个 UXTO 所需的关键信息：“交易 ID (TXID)” 和 “输出索引 (VOUT)”）

等待区块打包后，转账就成功了。







三、【实验一】单输入（Single UTXO）离线签名

实验目的：

将地址 A1 中的这笔 UTXO（0.123 BTC）进行拆分：其中 0.1 BTC 转账到地址 B2，余款找零至地址 C2。

操作步骤：

整理信息：

地址 A1：

1D6xf2ivf8GsGj9x1CgkWicZbfgQMc6Q7S

私钥：Kx16zC6GucmW88v6iUkT73AVfFQbSPbQdbij4AhKjCyu185bpZPR

地址 B2：

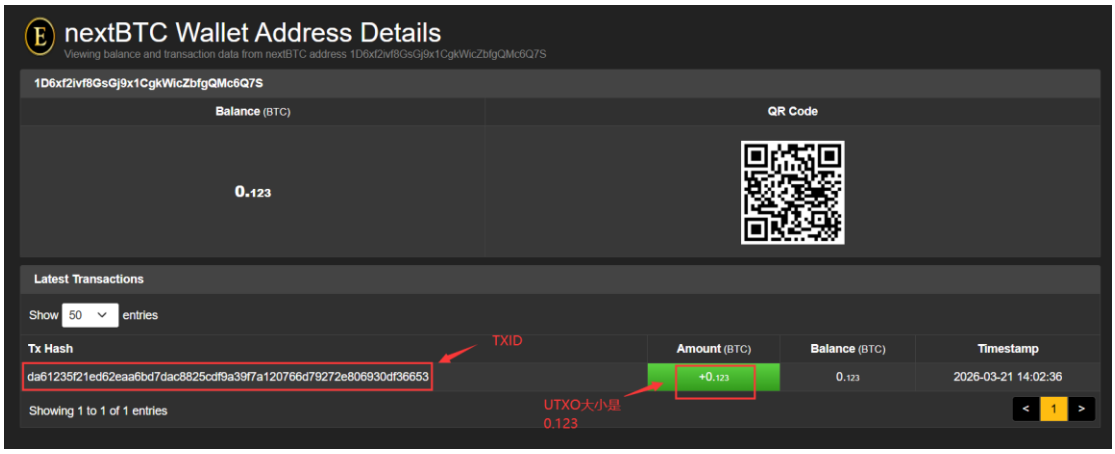
bc1q47rekmjcuxsj996texwjgnj6xm7rw5zt2tjtpu

私钥：接收方不需要私钥

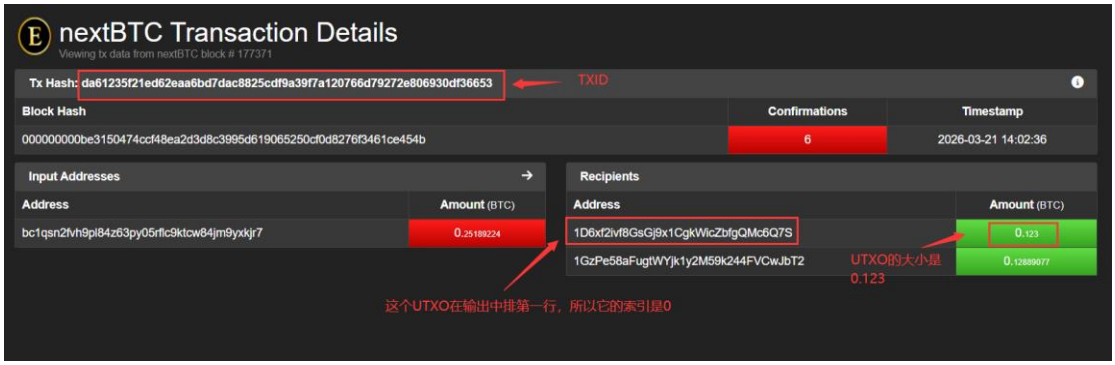
地址 C2：

bc1qyup2uhuepy2pyhqp4g4nglwfy3jzkejvk80enw

私钥：找零接收方不需要私钥



在区块浏览器里查看地址 A1 后我们得到，这个 UTXO 数量为 **0.123**，TX 哈希为：
da61235f21ed62eaa6bd7dac8825cdf9a39f7a120766d79272e806930df36653
点击这个 TXID：

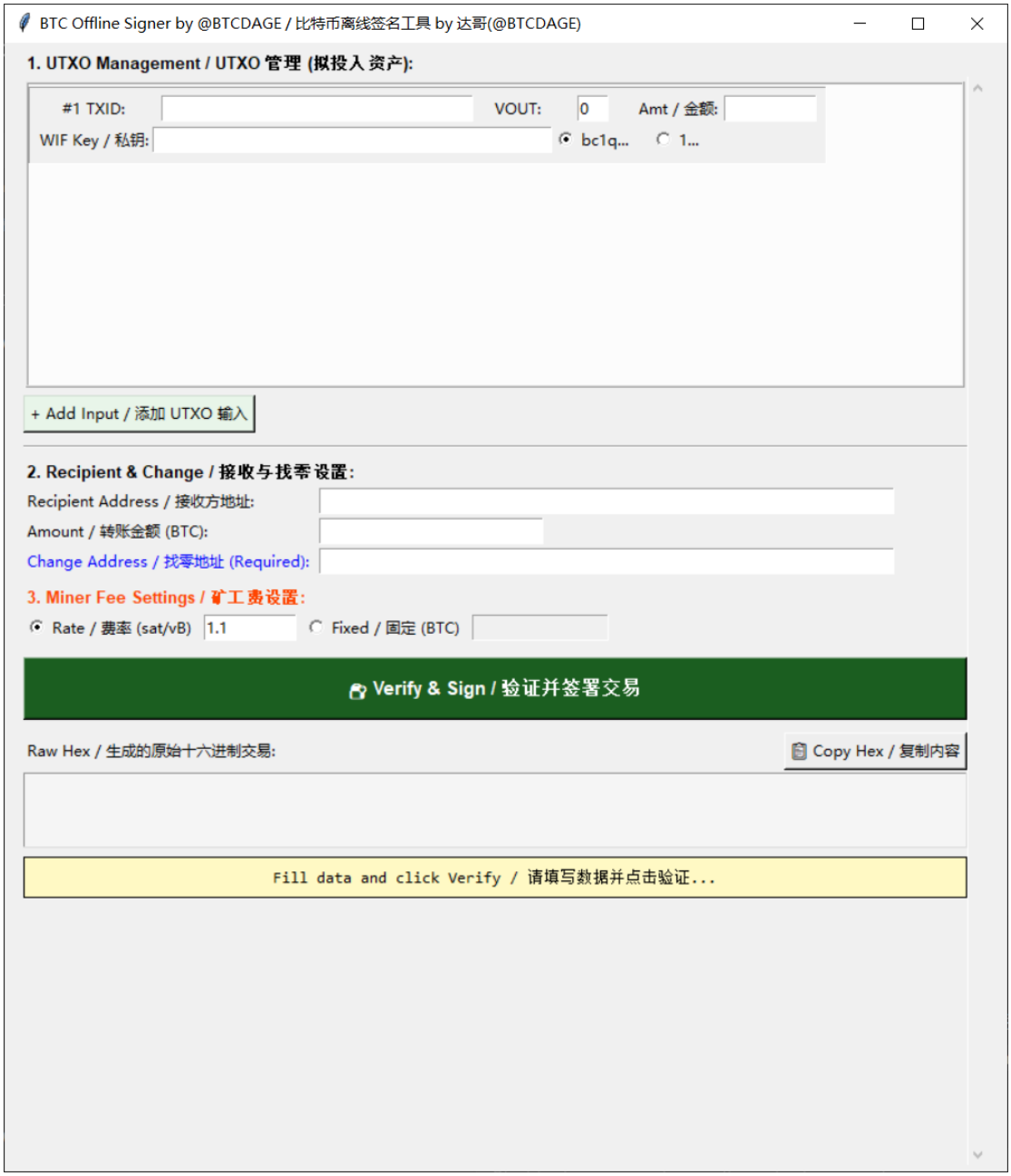


可以看到这个 UTXO 在输出里排在第一行，**所以它的索引（VOUT)是 0。（如果是第二行则索引为 1，以此类推）**

现在我们就在线得到了这个 UTXO 的全部信息。可以进入离线签名的环节了。

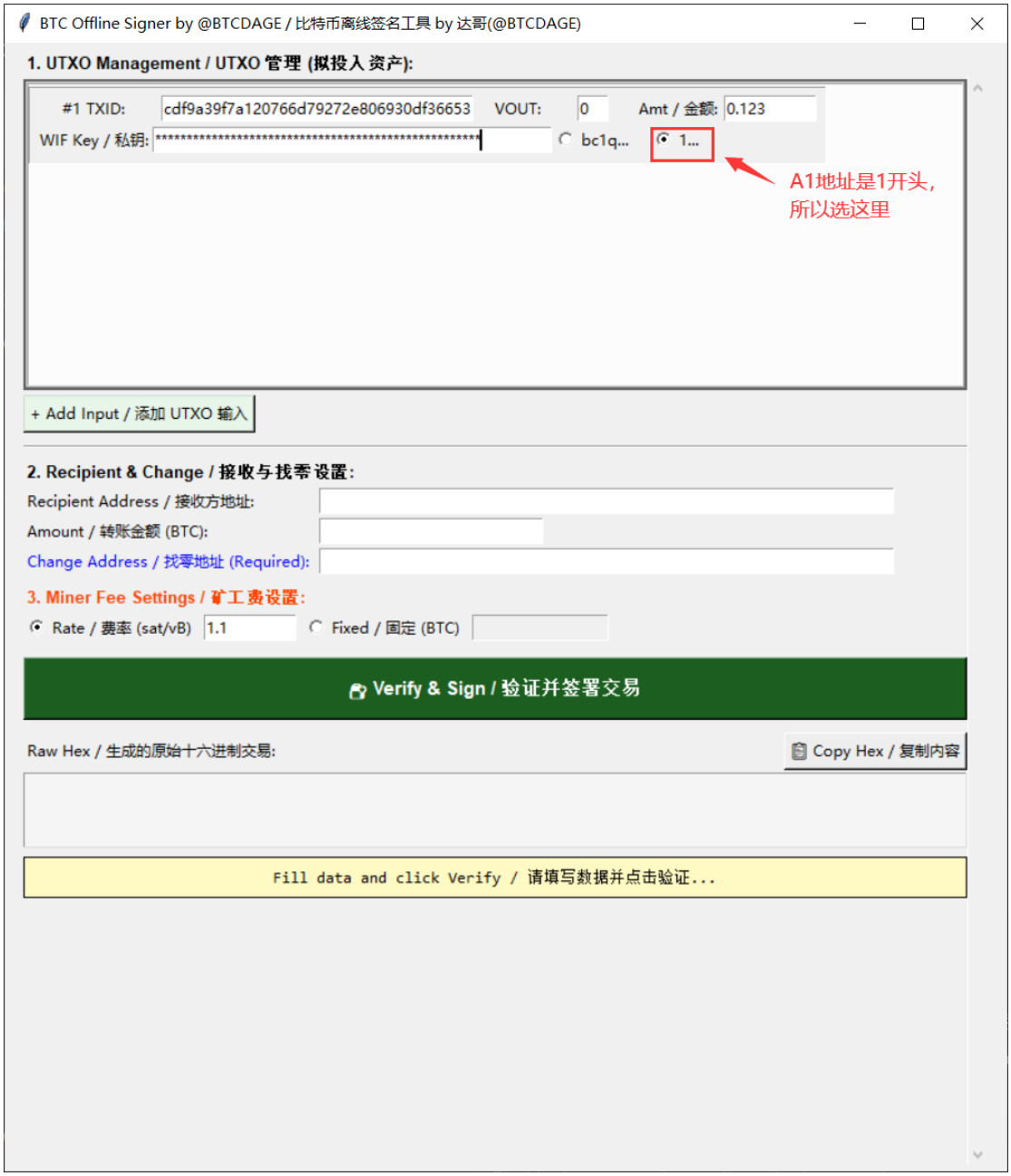
离线签名环节：

现在我们进入离线电脑中，我这里使用虚拟机做测试，虚拟机网卡也被禁用，模拟断网环境。
打开“开源比特币离线签名工具”



第一步、设置输入 UTXO 信息

现在我们是单 UTXO 输入，不需要点击“添加 UTXO 输入“只需要在已有的输入框中填入我们刚才查到的信息：



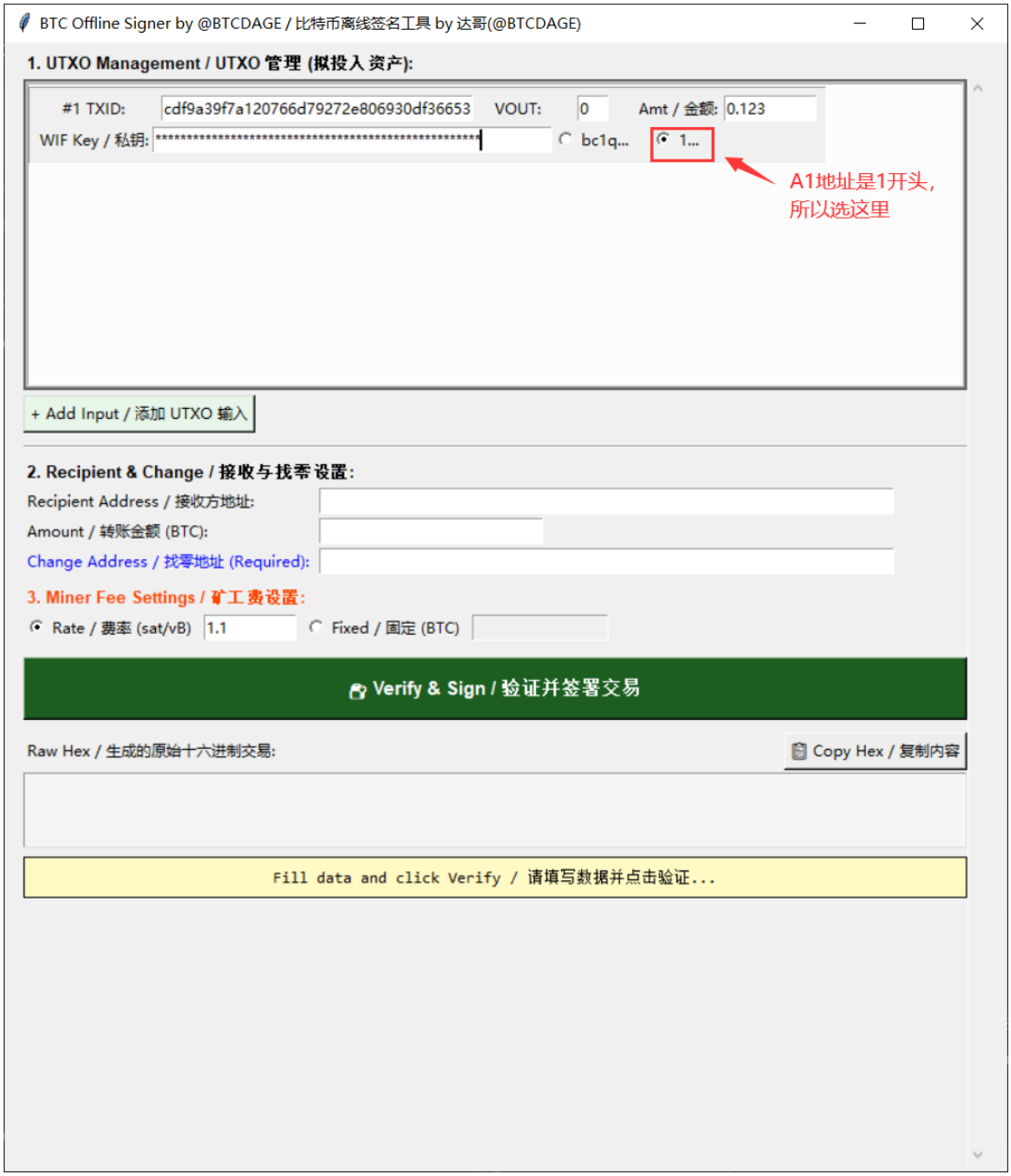
TXID 填入：

da61235f21ed62eaa6bd7dac8825cdf9a39f7a120766d79272e806930df36653

VOUT 填入:0（输出的第一行索引为 0）

私钥填入：

Kx16zC6GucmW88v6iUkT73AVfFQbSPbQdbij4AhKjCyu185bpZPR



第二步、设置接收与找零信息：

接收地址：

B2 地址：

bc1q47rekmjcuxsj996texwjgnj6xm7rw5zt2tjtpu

接收金额：

0.1

找零地址：

C2 地址：

bc1qyup2uhuepy2pyhqp4g4nglwfy3jzkejvk80enw

第三步、设置手续费

这里我们可以先去 https://mempool.space/ 查看当前的矿工费率。我这里就选默认了。

点击 验证签名按钮

Confirmation / 签名确认单

⚠ Scan QR to broadcast / 请扫描二维码广播交易



✅ Signed Successfully / 签名成功!

🚀 Send / 转出: 0.10000000 BTC
🎯 To / 接收: bc1q47rekmjcuxsj996texwjgnj6xm7rw5zt2tjtpu

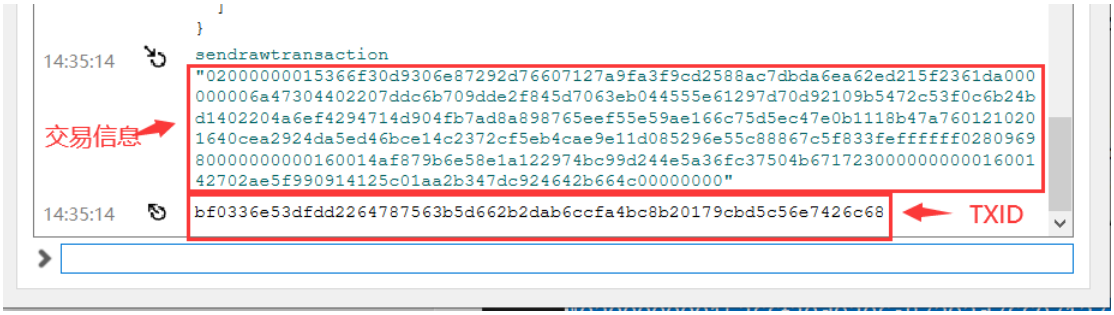
🔨 Fee Rate / 费率: 1.10 sat/vB | Fee / 费用: 0.00000249 BTC
📦 Size / 体积: 227 vB
💰 Change / 找零: 0.02299751 BTC
🏦 Change Addr / 找零地址: bc1qyup2uhuepy2pyhqp4g4nglwfy3jzkejvk80enw



可以看到交易详情，已经签名生成了 十六进制的交易信息，点击复制内容可以复制到记事本，或者扫码获得交易数据。我们这里测试环境仍然使用 nextBTC 的客户端控制台广播交易。在比特币主网中操作的话，可以使用支持广播交易的钱包软件扫二维码进行广播，或者区块浏览器的广播功能广播交易。

在控制台使用广播指令：

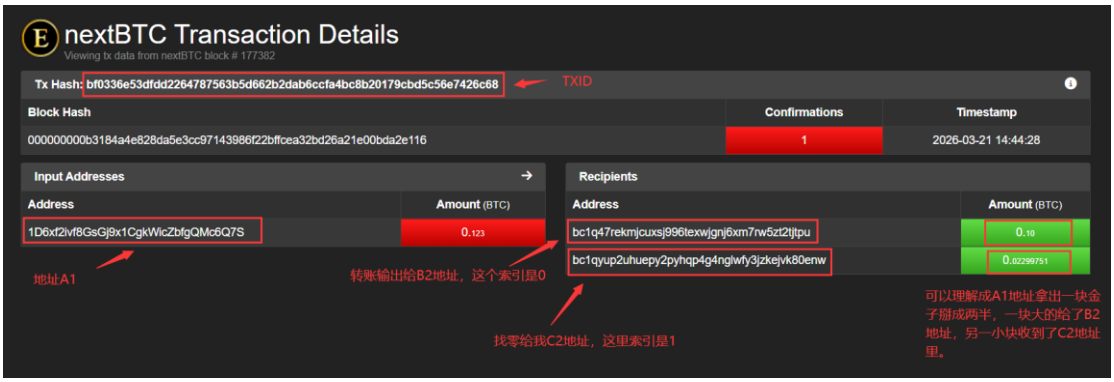
sendrawtransaction "02000000015366f30d9306e87292d76607127a9fa3f9cd2588ac7dbda6ea62ed215f2361da000000006a47304402207ddc6b709dde2f845d7063eb044555e61297d70d92109b5472c53f0c6b24bd1402204a6ef4294714d904fb7ad8a898765eef55e59ae166c75d5ec47e0b1118b47a7601210201640cea2924da5ed46bce14c2372cf5eb4cae9e11d085296e55c88867c5f833feffffff028096980000000000160014af879b6e58e1a122974bc99d244e5a36fc37504b6717230000000000160142702ae5f990914125c01aa2b347dc924642b664c00000000"



交易已广播，等待打包确认，TXID:

`bf0336e53dfdd2264787563b5d662b2dab6ccfa4bc8b20179cbd5c56e7426c68`

打包完成后可以看到这个 UTXO 已经成功转账了。

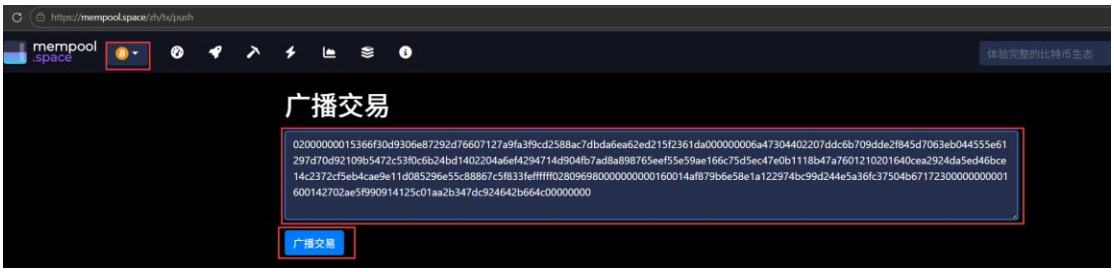


这个实验测试了 从 A1 地址里 把 比特币转到 B2 中一部分，另一部分找零给 C2 地址。

★注意★，钱包客户端广播交易数据必须在线且同步完成。如果你没有同步完成的全节点，可以使用在线的区块浏览器的广播功能：

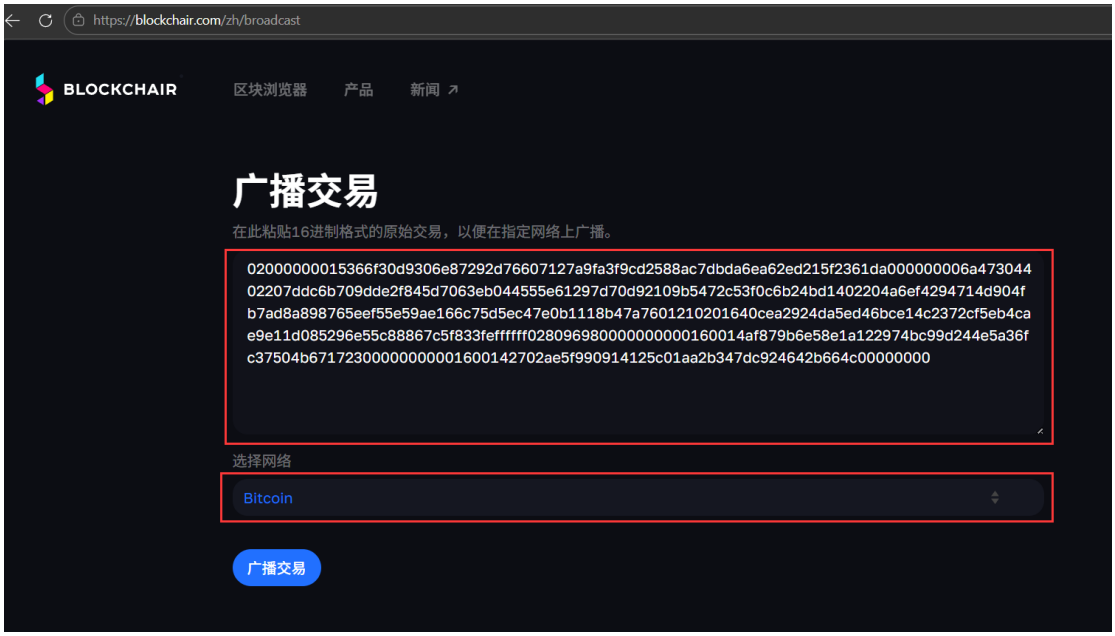
MEMPOOL

https://mempool.space/zh/tx/push



BLOCKCHAIR

https://blockchair.com/zh/broadcast



四、【实验二】多输入（Multi-UTXO）合并转账签名

实验目的：

实验目的： 模拟资金归集。将地址 B2 (0.1 BTC) 和地址 C2 (约 0.0229 BTC) 的两笔 UTXO 合并，向地址 D2 转账 0.05 BTC，剩余资金找零至地址 A2。

操作步骤：

先整理信息：

地址 B2：

bc1q47rekmjcuxsj996texwjgnj6xm7rw5zt2tjtpu

私钥：KwJkcW5XqY6PrxXwZnJ3oTPTr5uRMMN6UEX7oWcJo9faBd9wzaa6

地址 C2：

bc1qyup2uhuepy2pyhqp4g4nglwfy3jzkejvk80enw

私钥：L1Yw9iMFC3HiWnpb9pVuaKSW6o4qucEoMpssGqh2kuybgLmY52hp

地址 D2：

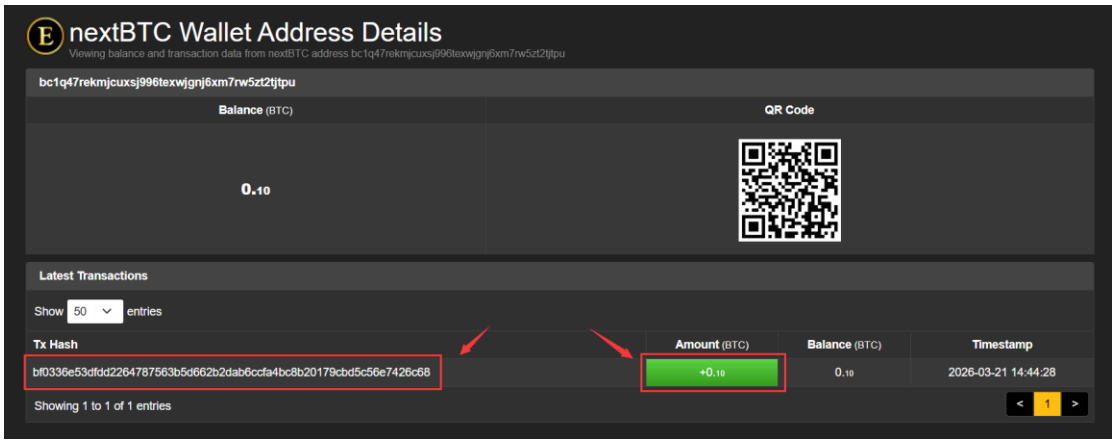
bc1qt0pdkcu2872au4jg80fyv350ftd4fw8uuy5g5c

私钥：接收地址不需要私钥

地址 A2：

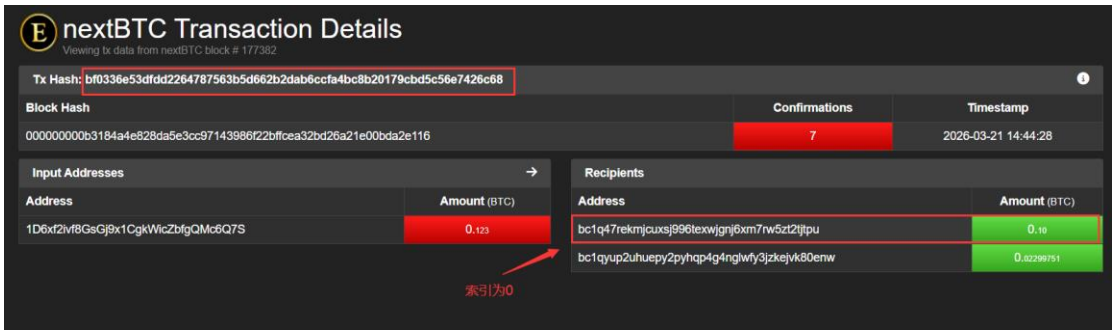
bc1qsnpqcktk2s2vvgz802uej2tj4ac92wpt7e2gmd

私钥：找零接收地址不需要私钥



B2 地址的 0.1 个币 UTXO 来源 TXID 是:

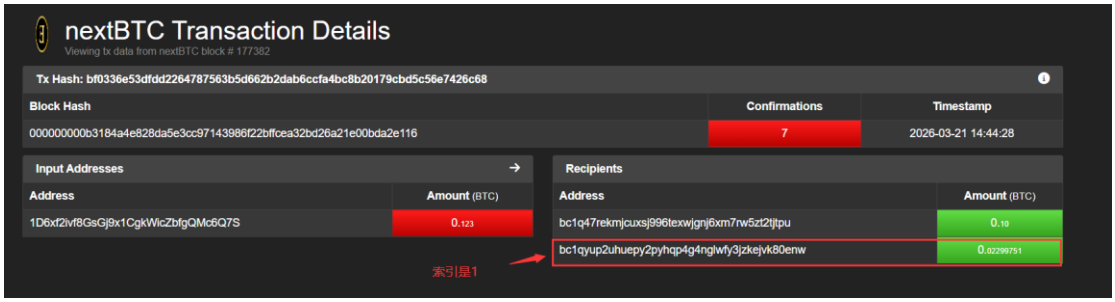
bf0336e53dfdd2264787563b5d662b2dab6ccfa4bc8b20179cbd5c56e7426c68



索引为 0

C2 地址的 0.02299751 个币的 UTXO 来源 TXID 也是:

bf0336e53dfdd2264787563b5d662b2dab6ccfa4bc8b20179cbd5c56e7426c68



索引是 1

现在开始生成签名:

第一步、设置输入 UTXO 信息

现在我们是两个 UTXO 输入，点击“添加 UTXO 输入“，这样就有了两个 UTXO 的设置，输入两个 UTXO 的信息。

第二步、设置接收与找零信息:

接收地址:

D2 地址:

bc1qt0pdkcu2872au4jg80fyv350ftd4fw8uuy5g5c

转账金额:

0.05

找零地址：

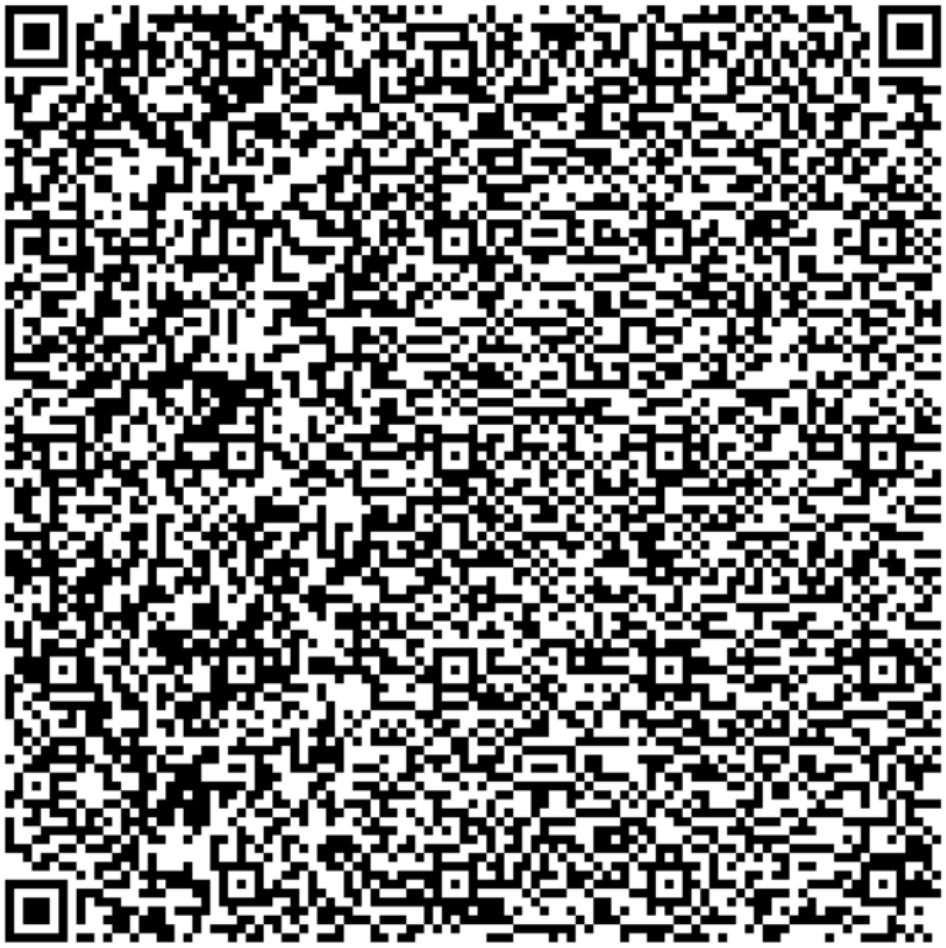
A2 地址：

bc1qsnpqcktk2s2vvgz802uej2tj4ac92wpt7e2gmd



Confirmation / 签名确认单

⚠ Scan QR to broadcast / 请扫描二维码广播交易



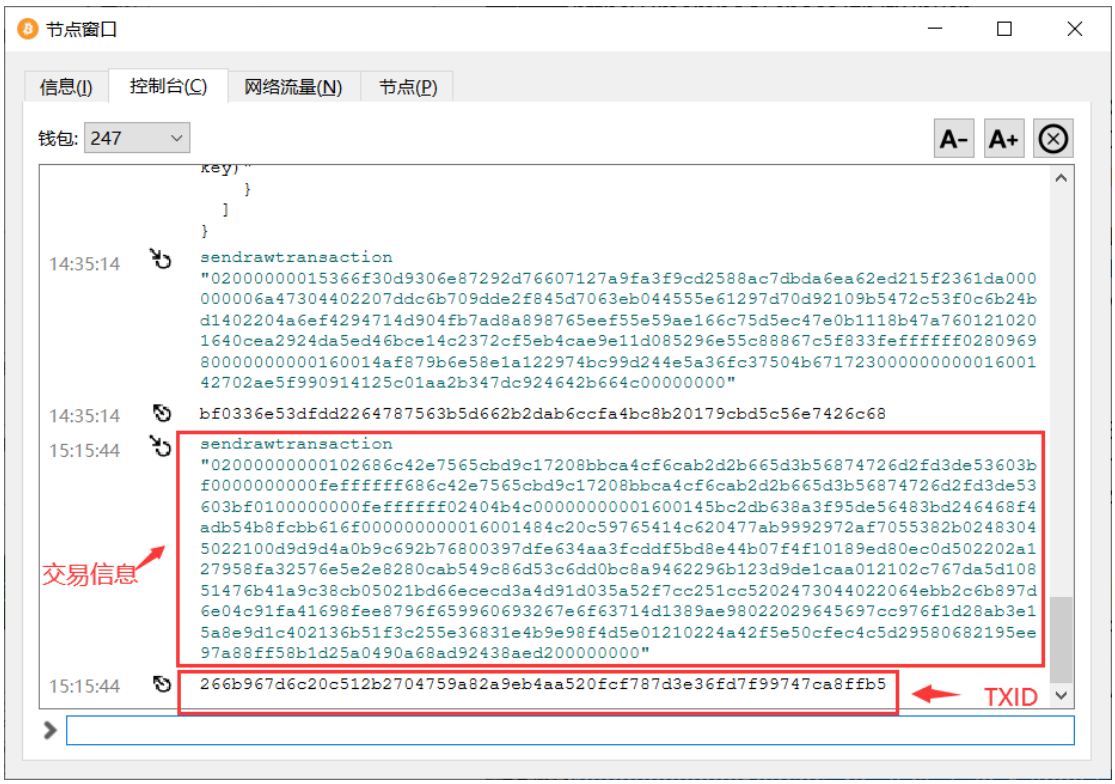
✅ Signed Successfully / 签名成功!

🚀 Send / 转出: 0.05000000 BTC
🎯 To / 接收: bc1qt0pdkcu2872au4jg80fyv350ftd4fw8uuy5g5c

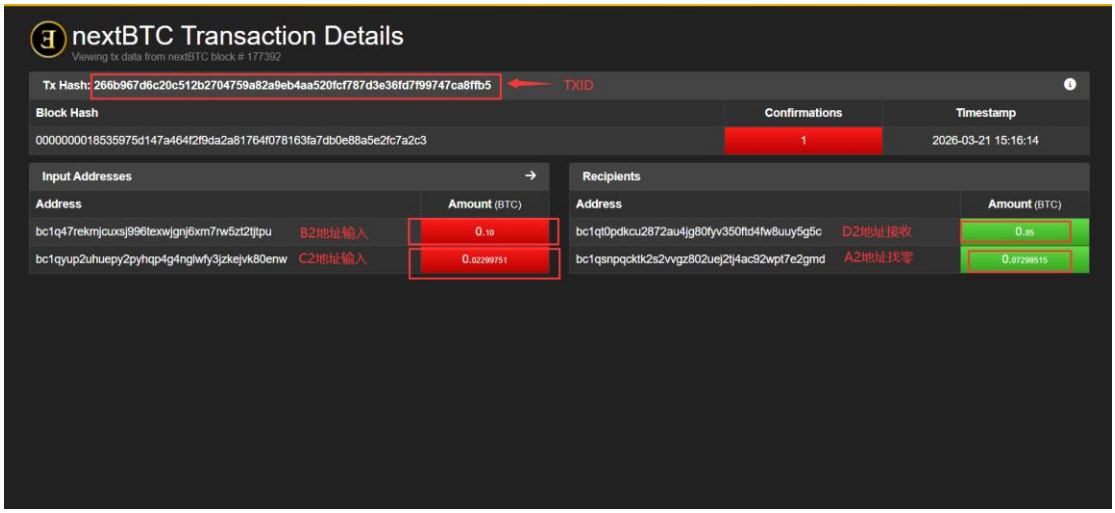
⛏ Fee Rate / 费率: 1.10 sat/vB | Fee / 费用: 0.00000236 BTC
📦 Size / 体积: 215 vB
💰 Change / 找零: 0.07299515 BTC
🏠 Change Addr / 找零地址: bc1qsnpqcktk2s2vvgz802uej2tj4ac92wpt7e2gmd

可以看到交易详情，已经签名生成了 十六进制的交易信息，点击复制内容可以复制到记事本，或者扫码获得交易数据。我们这里测试环境仍然使用 nextBTC 的客户端控制台广播交易。在比特币主网中操作的话，可以使用支持广播交易的钱包软件扫二维码进行广播，或者区块浏览器的广播功能广播交易。

在控制台使用广播指令：
sendrawtransaction
"02000000000102686c42e7565cbd9c17208bbca4cf6cab2d2b665d3b56874726d2fd3de53603bf0000000000feffffff686c42e7565cbd9c17208bbca4cf6cab2d2b665d3b56874726d2fd3de53603bf0100000000feffffff02404b4c0000000000001600145bc2db638a3f95de56483bd246468f4adb54b8fcbb616f0000000000016001484c20c59765414c620477ab9992972af7055382b02483045022100d9d9d4a0b9c692b76800397dfe634aa3fcddf5bd8e44b07f4f10189ed80ec0d502202a127958fa32576e5e2e8280cab549c86d53c6dd0bc8a9462296b123d9de1caa012102c767da5d10851476b41a9c38cb05021bd66ececd3a4d91d035a52f7cc251cc5202473044022064ebb2c6b897d6e04c91fa41698fee8796f659960693267e6f63714d1389ae98022029645697cc976f1d28ab3e15a8e9d1c402136b51f3c255e36831e4b9e98f4d5e01210224a42f5e50cfec4c5d29580682195ee97a88ff58b1d25a0490a68ad92438aed200000000"



交易已广播，等待打包确认，TXID：
`266b967d6c20c512b2704759a82a9eb4aa520fcf787d3e36fd7f99747ca8ffb5`
打包完成后可以看到这个 UTXO 已经成功转账了。



这个实验成功测试了 从 B2 地址和 C2 地址里把两个 UTXO 合并到一起，转到 D2 中一部分，另一部分找零给 A2 地址。

五、常见问题解答 (Q&A)

Q：离线签名后的十六进制消息（Raw Hex）在联网广播时，会暴露私钥吗？
A：绝无可能。 广播的内容是经过私钥加密计算后的“数字签名”和交易指令。这就像你在支票上签了名，别人拿着支票去兑现，银行只能看到你的签名，却无法根据签名逆推出你的印章刻模。

Q：结合高级脑钱包工具，使用此工具可以完全替代软硬件钱包吗？
A：理论上完全可以。 使用高级脑钱包工具离线生成囤币地址，配合本工具在冷环境下生成签名，最后交给区块浏览器广播。在技术层面，这种方案达到了与硬件钱包同等级别的冷隔离（Air-gap）。由于代码开源且运行在通用设备上，它彻底排除了硬件厂商可能存在的供应链后门或固件闭源风险，是追求数字货币主权的极客级安全选择。

Q：填写的“输入金额”必须与实际 UTXO 的大小完全一致吗？
A: 非常关键，务必注意。 如果你填写的“输入金额”大于该 UTXO 的实际金额，签名虽然能成功，但广播时会被全网节点拒绝。更危险的是，如果你填写的金额小于实际金额，比特币协议会将“未被输出覆盖的差额”默认为你打赏给矿工的小费。因此，请务必根据区块浏览器的实测数据，100% 精确地填写输入金额 (Amt)，确保资产不会因误操作而损失。

Q：找零地址可以不设置吗？
A：不可以。 虽然技术上支持将余额找零回原地址，但为了安全性与隐私保护，强烈建议将找零指向你的另一个高级脑地址。遵循“地址不重用（Address Reuse Avoidance）”原则，不仅可以有效防止资产关联导致的隐私泄露，也是比特币安全操作的最佳实践，确保每个地址在完成资金转出后即“作废”。当然如果你是全额转到一个地址，调整收款金额和手续费实现找零额是 0，那么找零地址将收不到币，但是设置时还是要设置一下。

Q：我很害怕误操作导致资产丢失怎么办？
A: 你可以先在 nextBTC 上操作测试, 因为 nextBTC 和比特币主网完全兼容, 所以在 nextBTC 上测试成功，则在主网上表现将会一致。