比特币“时间胶囊”

基于离线签名工具 PRO(V0.2)的时间锁（CLTV）

实验教程

@BTCDAGE

2026-03-22

Nostr: npub17ahz4xa3hvkvvhh4wguzzqknp8p7l5nyzzqc3z53uq538r5qgn0q40z7pw

目录

一、 实验环境与准备 2

二、 在线准备阶段：资金注入 4

三、【实验一】生成时间锁“胶囊”地址 B3 6

四、【实验二】资金注入与普通转账测试 (A2 -> B3) 9

五、【实验三】锁定性测试：未到期强制广播 18

六、【实验四】解锁测试：到期后成功广播 23

七、常见问题解答 (Q&A) 25

本教程默认用户已经阅读上一篇

《比特币冷热分离：基于 NextBTC 的离线签名实验教程》

已经测试并理解了

比特币离线签名工具 V0.1

的使用方法

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：

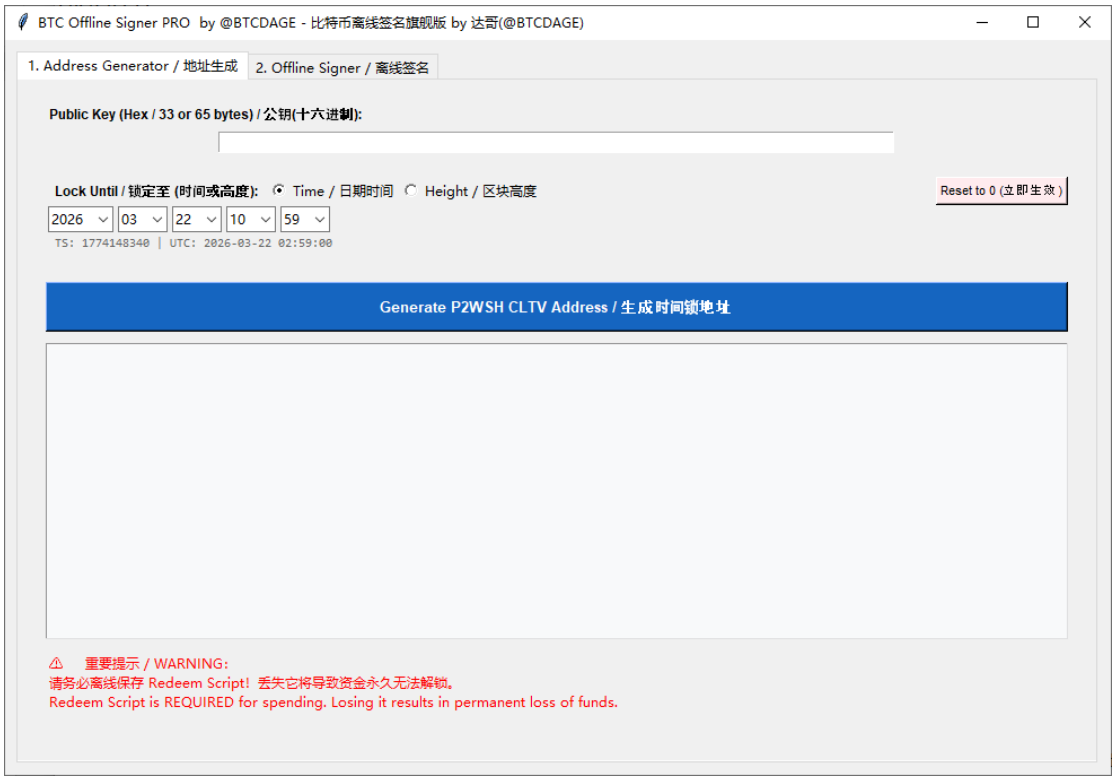
高级脑钱包生成器：用于生成原始公私钥对。

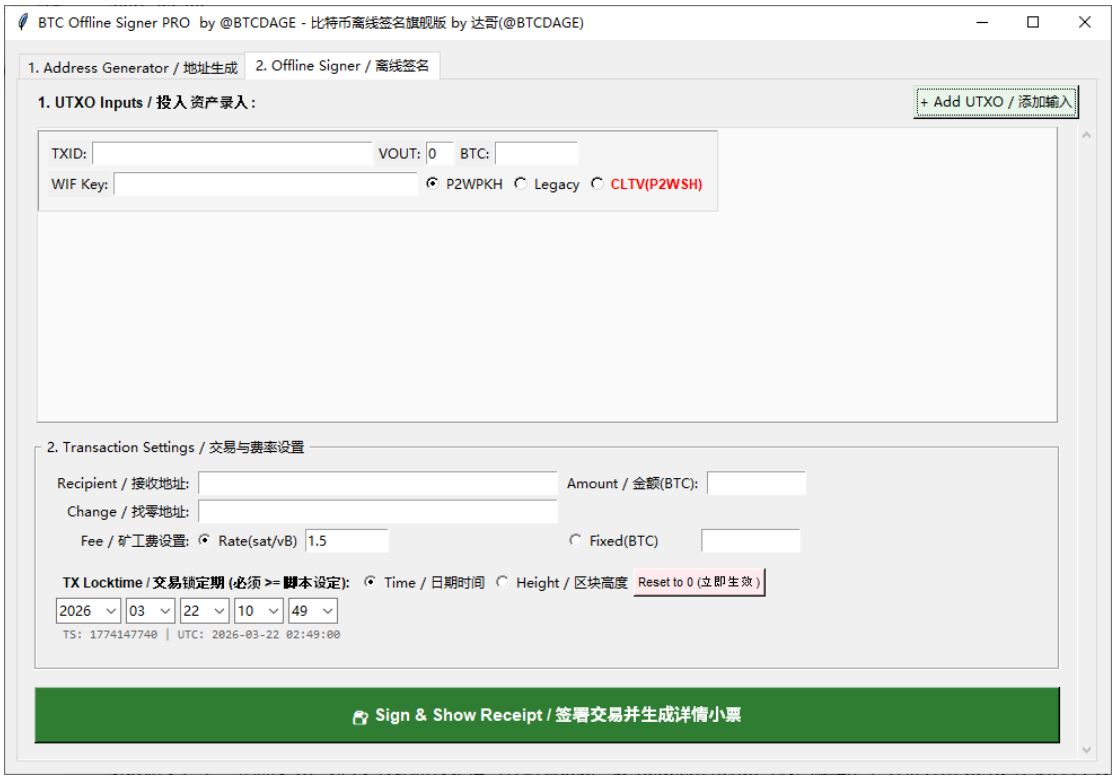


开源地址：https://github.com/btcdage2000/BrainWalletGenerator

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

比特币离线签名工具 PRO (V0.2)：支持 CLTV 分页、自动保存赎回脚本





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两组基础地址：
地址 A：用于初始资金持有。记录 私钥 A 和 地址 A2 (Bech32)。
地址 B：用于接收找零。记录 私钥 B、公钥 B (Hex) 和 地址 B2 (Bech32)。
★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：



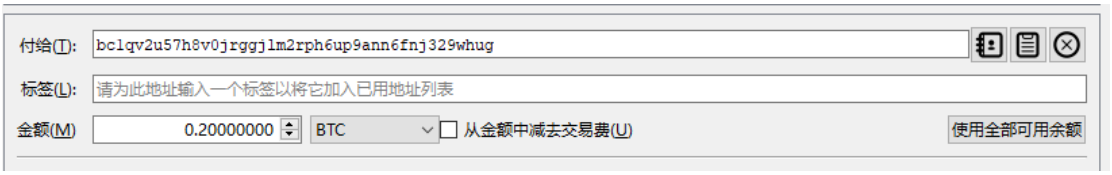
这次我们只取 Bech32 地址和公钥私钥。
A
地址 A2：bc1qv2u57h8v0jrggjlm2rph6up9ann6fnj329whug
私钥 A: Kx9XohRHqewAUpkZFjyz6EZnssChxqBvV6bpLW9hxqhHJ2w6gPo3
公钥 A: 03d03623d1e6b425615007c8759fc85f542cb353b579431ad49fb918f2c067d09d
B
地址 B2：bc1qea52r0pfwa0ecnetspv83m27yra4r4snymrycs
私钥 B: L3PMcvqpKyQu1UQq6NbGYKvjzKLQhcR97WxHaPrThATq35At88nR
公钥 B: 0373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26d

二、 在线准备阶段：资金注入

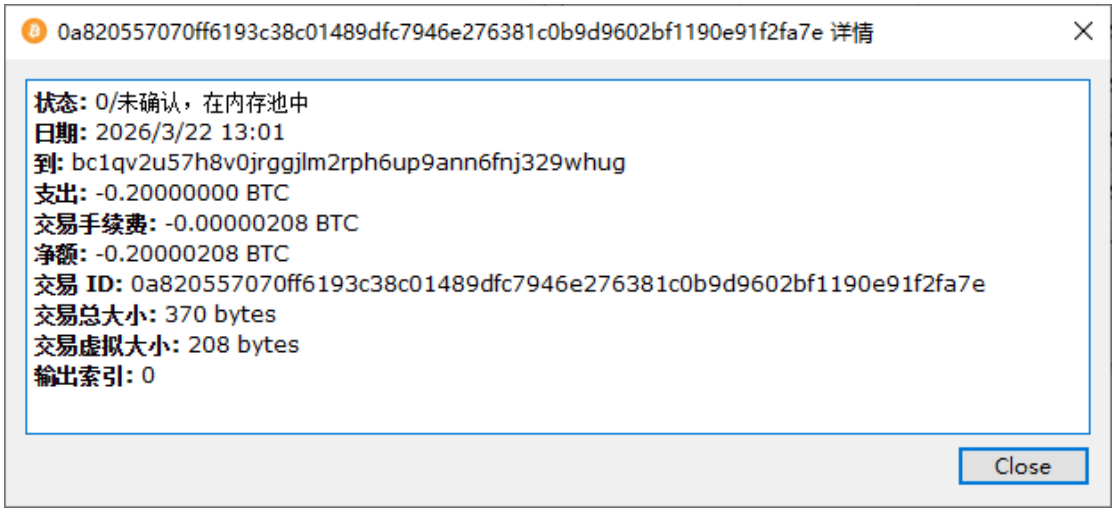
在联网环境下，向地址 A2 转入 0.2 BTC。此步骤模拟从交易所提币到高级脑地址“囤饼”的动作（**注：若您已熟练掌握《比特币冷热分离：基于 NextBTC 的离线签名实验教程》中的基础转账操作，可快速略过此步骤**）。

地址 A2：

bc1qv2u57h8v0jrggjlm2rph6up9ann6fnj329whug

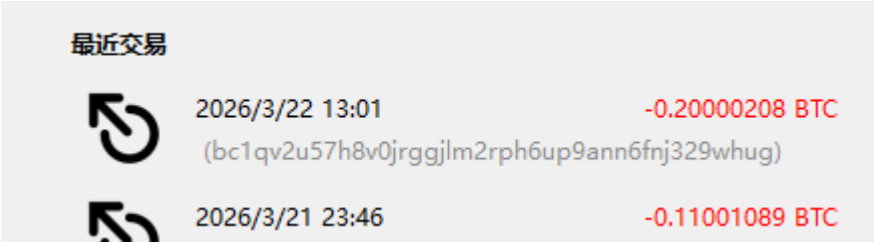


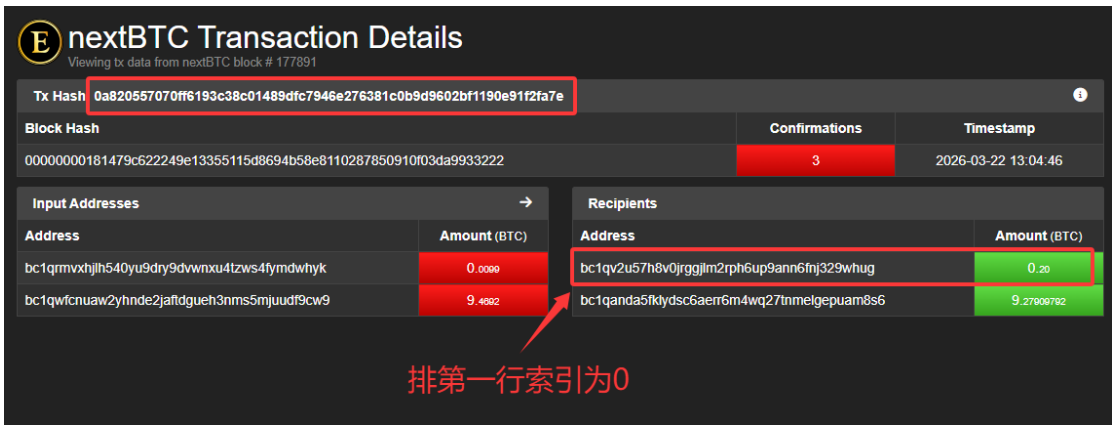


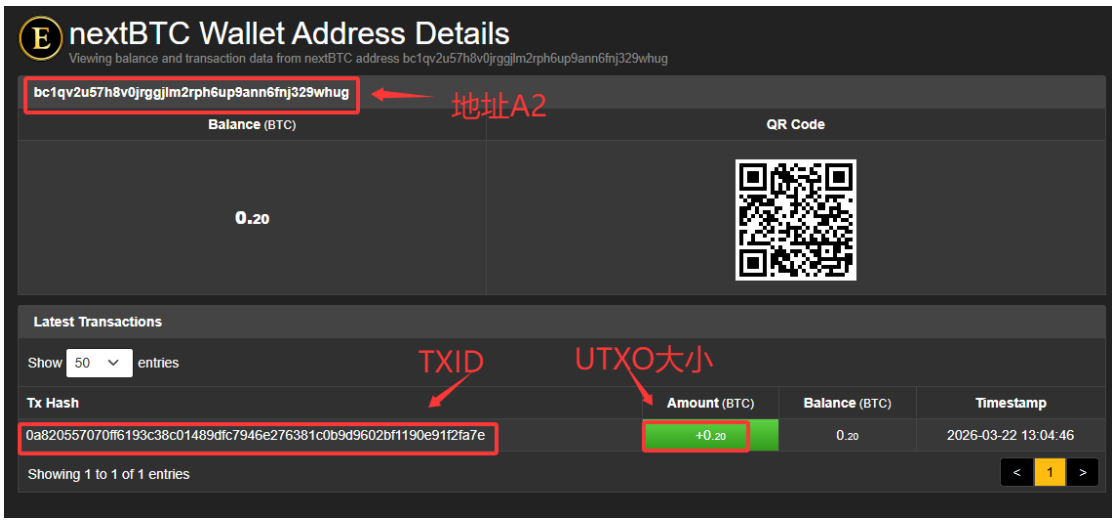


（注意，其实这里就可以看到移动一个 UXTO 所需的关键信息：“交易 ID (TXID)”和“输出索引 (VOUT)”）

等待区块打包后，转账就成功了。







三、【实验一】生成时间锁“胶囊”地址 B3

实验目的：

利用 B 组地址的公钥，创建一个只能在 2 小时后由私钥 B 开启的“时间胶囊”地址。

操作步骤：

整理信息：

B 组公钥：

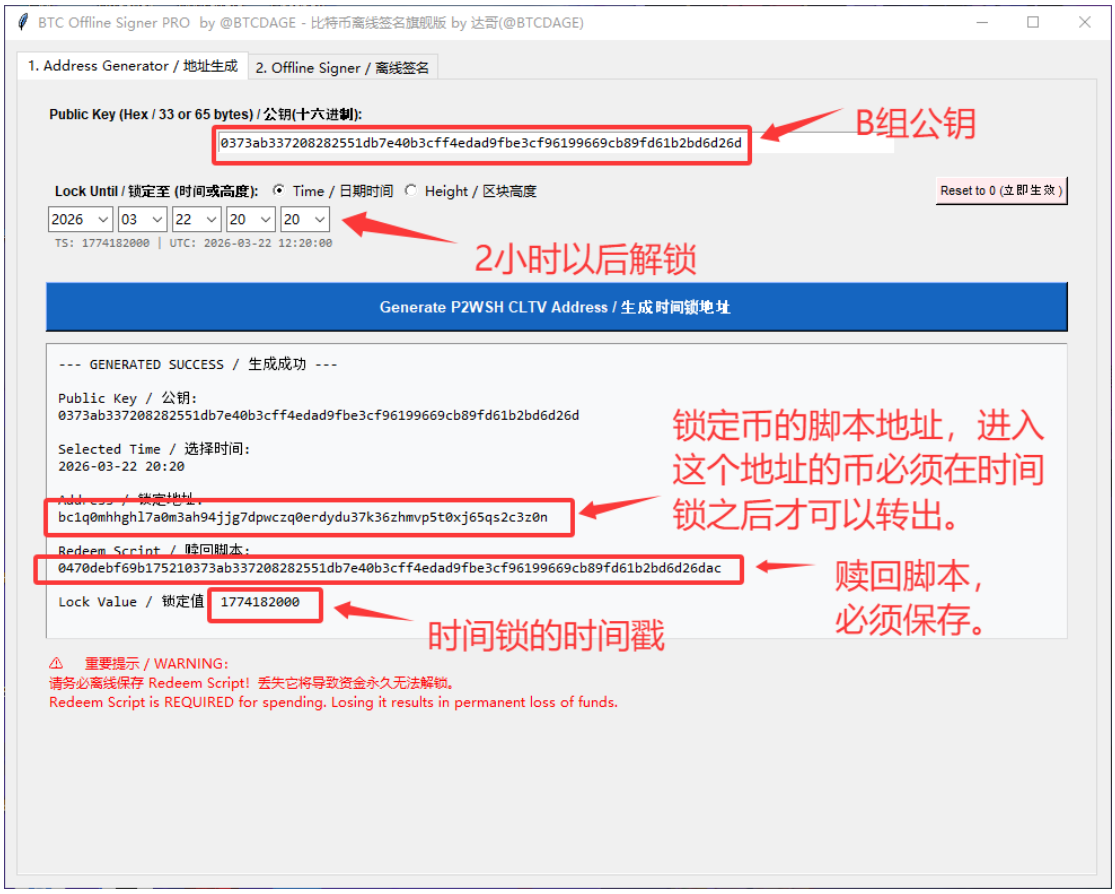
0373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26d

私钥：生成时间锁脚本地址不需要私钥（但是你必须要有，不然以后无法转出币）

现在时间：

2026 年 3 月 22 日 18：20

打开离线签名工具，切换至 [1. Address Generator / 地址生成] 分页。



输入公钥：填入 公钥 B (Hex)。

0373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26d

设置锁定时间：

切换至 Time / 日期时间 模式。

选择当前时间往后推约 2 小时（例如当前 **18：20**，设为 **20:20**）。

生成地址：点击蓝色按钮。

参数意义：工具会通过 OP_CLTV 逻辑将锁定值与公钥编织成一段 Redeem Script（赎回脚本），并推导出 bc1q 开头的 P2WSH 地址。这个地址的所有币，由 script + transaction locktime + sequence 共同约束**（工具已自动处理 sequence 参数，用户无需手动设置）**，在锁定时间未到达之前都是无法转出的（限制并不来自地址本身，而是来自花费该 UTXO 时必须满足的脚本与交易条件）。转出这个地址的币除了需要私钥之外，也需要提供赎回脚本。

可以这么理解：时间锁脚本地址相当于一个设定了倒计时的透明保险箱。

Redeem Script（赎回脚本） 是这个保险箱的设计图纸和规则说明；而你的私钥才是开箱的钥匙。

想要从这个地址转出比特币，你必须同时向网络提供：

1、这套设计图纸（证明你知晓锁定规则）；

2、合法的私钥签名（证明你是主人）；
3、并且比特币网络的“链上共识时间”必须已经跨过了图纸上规定的 LockTime。
点击按钮后生成地址，会提供一切参数。
--- GENERATED SUCCESS / 生成成功 ---

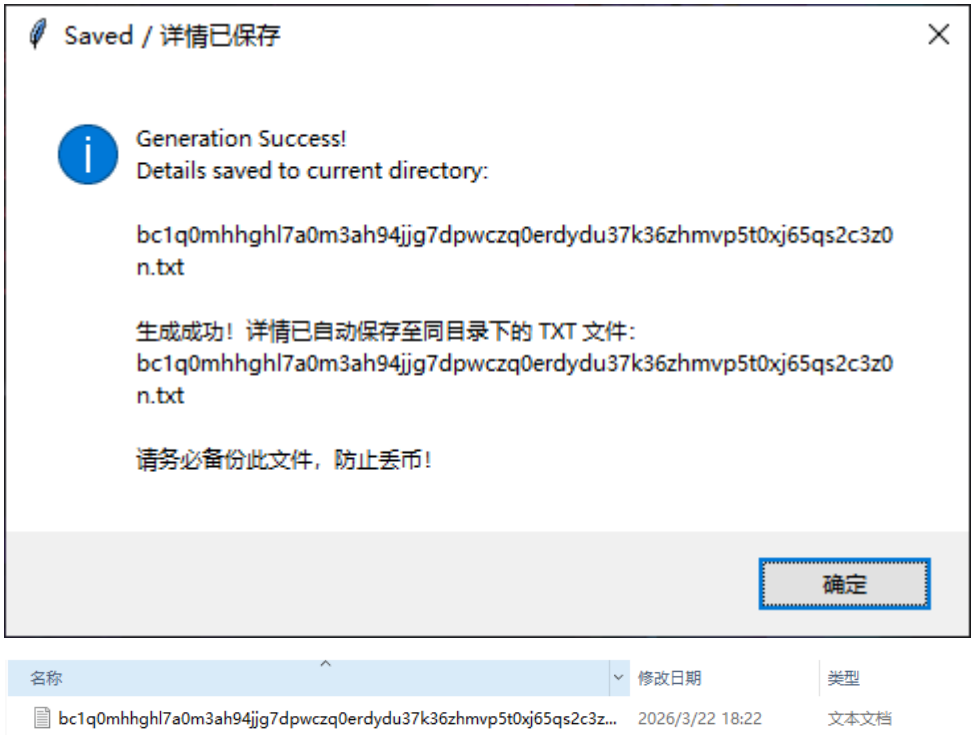
Public Key / 公钥:
0373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26d

Selected Time / 选择时间:
2026-03-22 20:20

Address / 锁定地址:
bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n

Redeem Script / 赎回脚本:
0470debf69b175210373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26dac

Lock Value / 锁定值: 1774182000
此时检查程序所在目录，会自动生成一个以地址命名的 .txt 文件。
文件包含：公钥、选择的人读时间、生成的锁定地址、以及最关键的 Redeem Script。请妥善保存此文件，它是未来解锁的唯一凭证。




bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

--- GENERATED SUCCESS / 生成成功 ---

Public Key / 公钥:
0373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26d

Selected Time / 选择时间:
2026-03-22 20:20

Address / 锁定地址:
bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n

Redeem Script / 赎回脚本:
0470debf69b175210373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26dac

Lock Value / 锁定值: 1774182000

现在我们得到了**地址 B3**:
bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n
★注意★它的私钥公钥就是 B 组地址的私钥公钥。
私钥 B:
L3PMcvqpKyQu1UQq6NbGYKvjzKLQhcR97WxHaPrThATq35At88nR
公钥 B:
0373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26d

该地址可以随时接收转入的 UTXO，但其花费能力受到时间锁约束。

下面我们将实验证明。

四、【实验二】资金注入与普通转账测试（A2 -> B3）

实验目的：

验证普通离线签名功能，并将资金注入时间锁地址 B3。找零地址为 B2。

操作步骤：

整理信息：

地址 A2：

bc1qv2u57h8v0jrggjlm2rph6up9ann6fnj329whug

私钥：Kx9XohRHqewAUpkZFjyz6EZnssChxqBvV6bpLW9hxqhHJ2w6gPo3

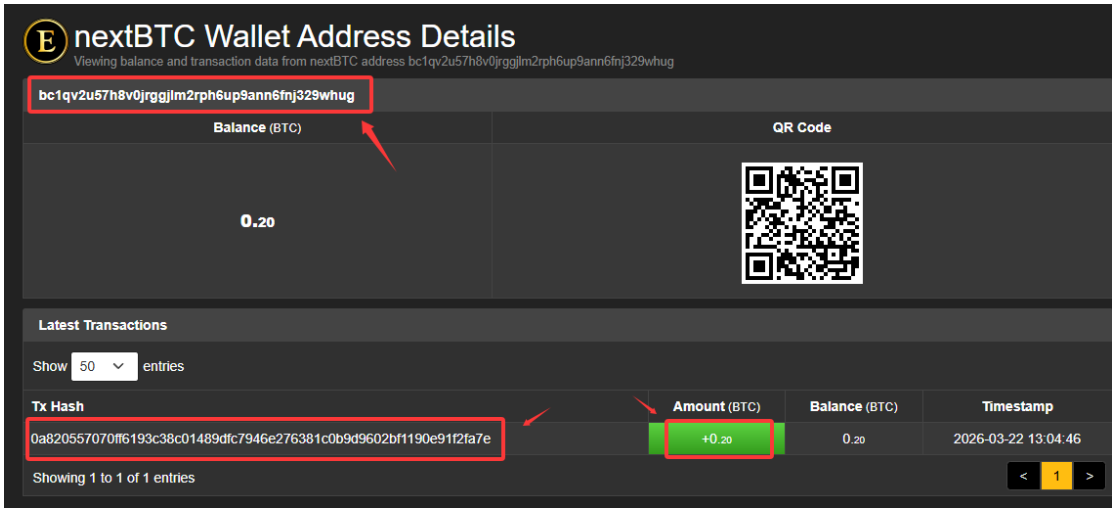
地址 B3：

bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n

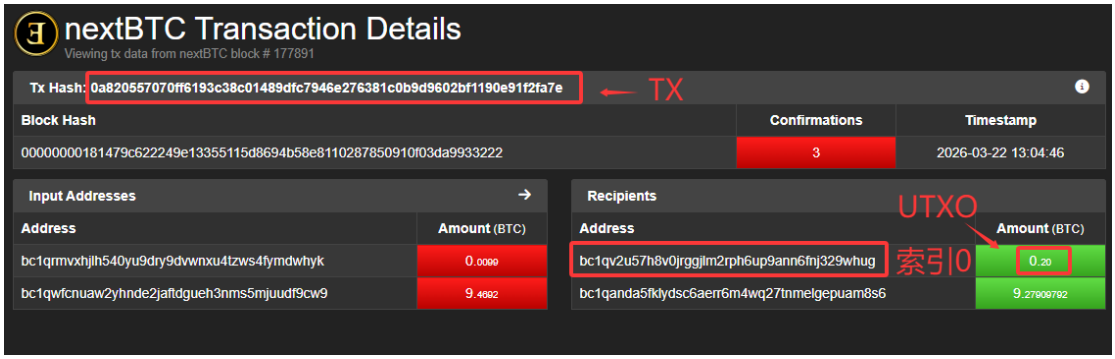
私钥：接收地址不需要私钥

地址 B2：

bc1qea52r0pfwa0ecnetspv83m27yra4r4snymrycs
私钥：找零接收地址不需要私钥



A2 地址的 0.2 个币 UTXO 来源 TXID 是：
0a820557070ff6193c38c01489dfc7946e276381c0b9d9602bf1190e91f2fa7e

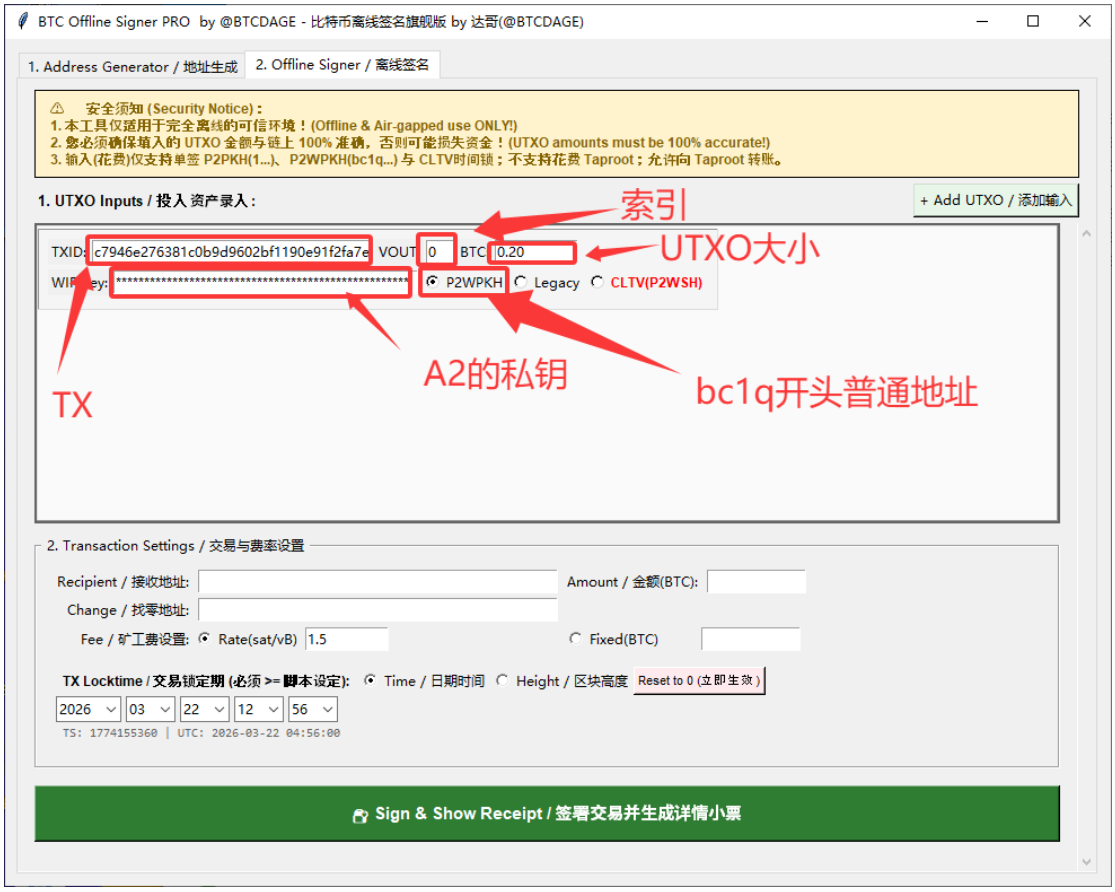


索引为 0

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 V0.2”

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：



第二步、设置接收与找零信息：

接收地址：

B3 地址：

bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n

转账金额：

0.1

找零地址：

B2 地址：

bc1qea52r0pfwa0ecnetspv83m27yra4r4snymrycs

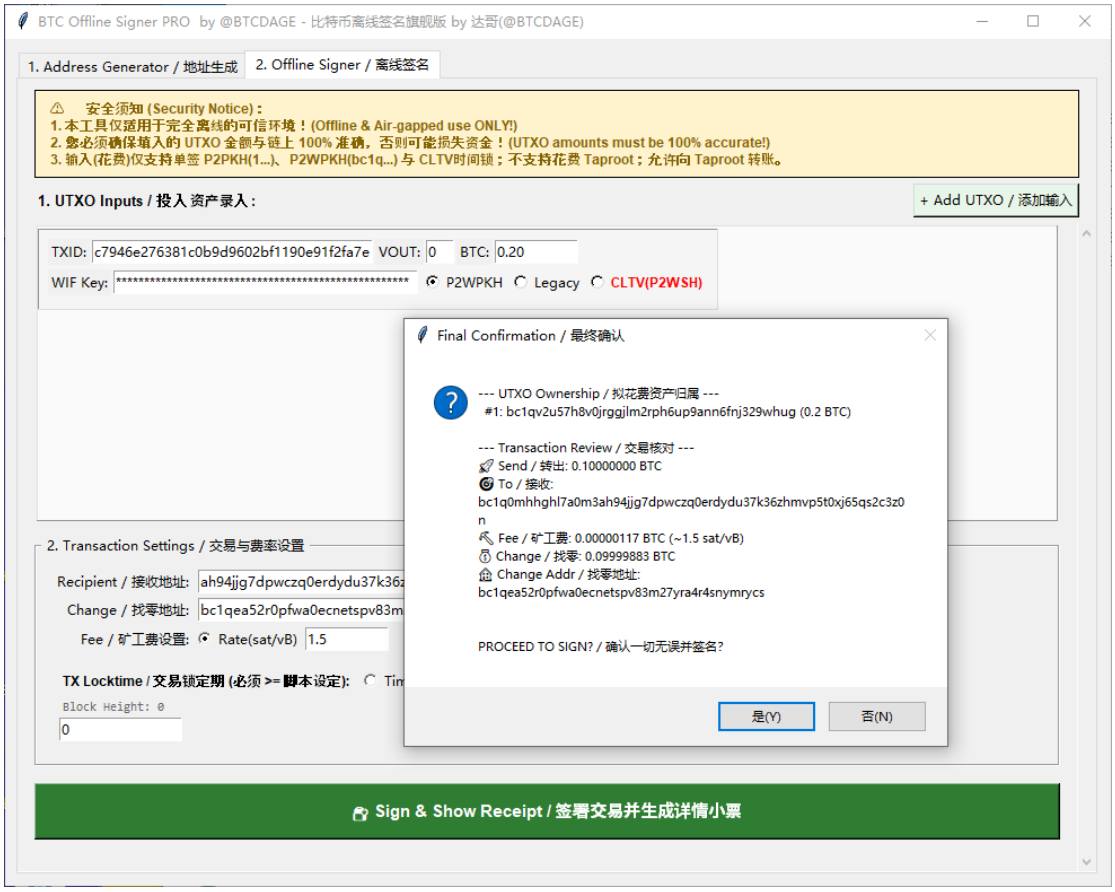


第三步、设置手续费和 Locktime。

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。

值得注意的是，向时间锁地址转账（存入资产）只是一个普通的花费动作，不需要设置 Locktime（Locktime 用于声明这笔交易何时可以被网络接受），直接点击 Reset to 0 即可。

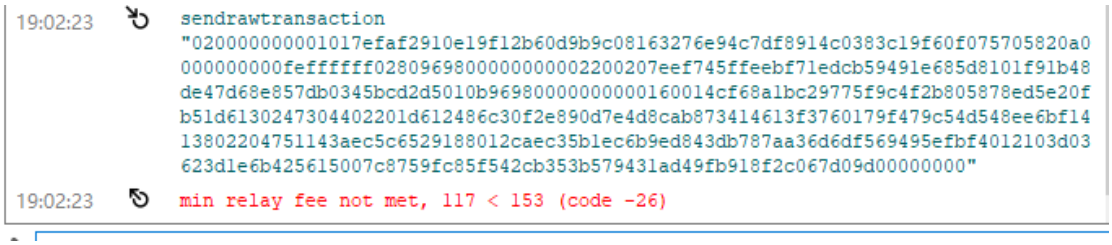
点击 验证签名按钮



检查小票信息，确认没问题后点“是”。

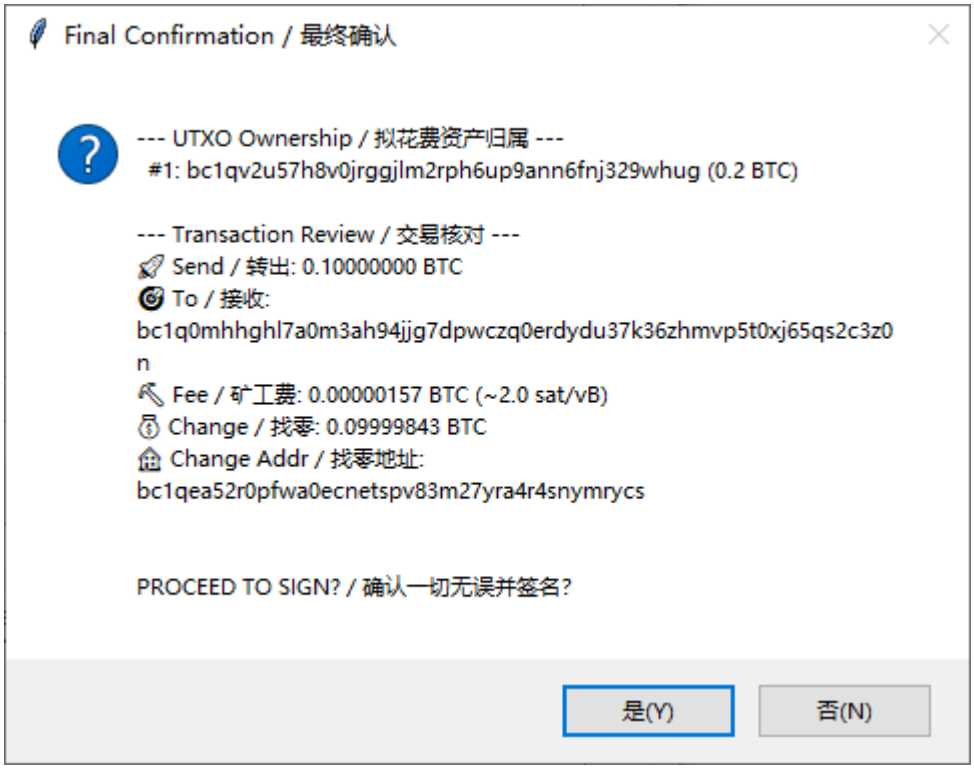


签名成功。生成了 十六进制的交易信息，点击复制内容可以复制到记事本，或者扫码获得交易数据。我们这里测试环境仍然使用 nextBTC 的客户端控制台广播交易。若在比特币主网操作，您可以使用支持离线签名的热钱包软件扫描二维码发送，或直接将十六进制代码粘贴到各类区块浏览器（如 Mempool）的广播页面中发送交易。



哈哈，手续费给少了。从截图报错 min relay fee not met 可以看出，这笔交易的矿工费（117 sats）低于全网节点的最低转发门槛（153 sats），因此被节点直接拒绝。

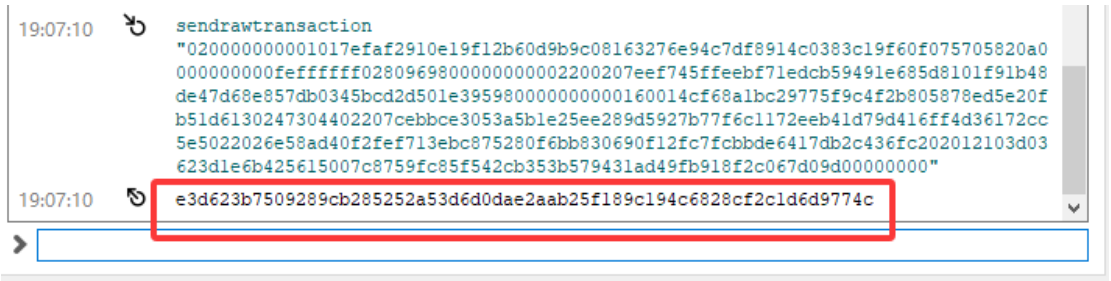
我们回到工具中，稍微提高费率（Fee Rate）重新生成签名：



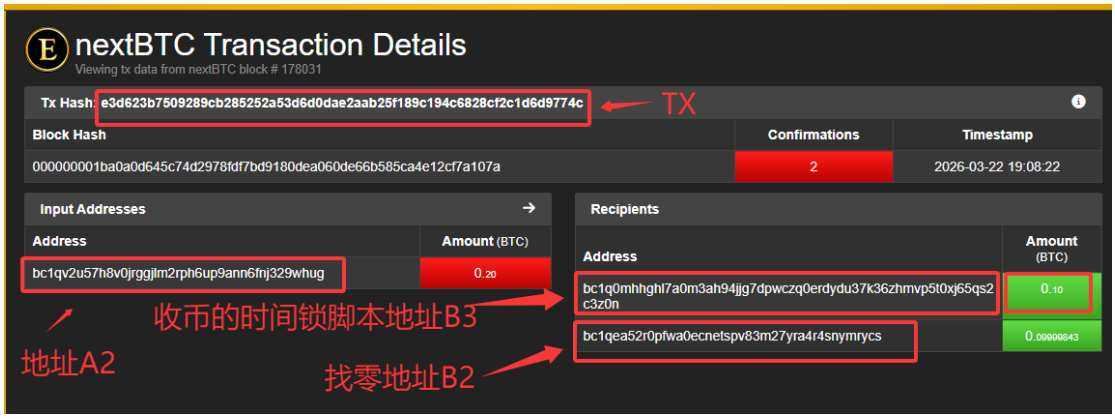


sendrawtransaction
"020000000001017efaf2910e19f12b60d9b9c08163276e94c7df8914c0383c19f60f075705820
a0000000000feffffff02809698000000000002200207eef745ffeebf71edcb59491e685d8101f91b

48de47d68e857db0345bcd2d501e3959800000000000160014cf68a1bc29775f9c4f2b805878e
d5e20fb51d6130247304402207cebbce3053a5b1e25ee289d5927b77f6c1172eeb41d79d416f
f4d36172cc5e5022026e58ad40f2fef713ebc875280f6bb830690f12fc7fcbbde6417db2c436fc2
02012103d03623d1e6b425615007c8759fc85f542cb353b579431ad49fb918f2c067d09d0000
0000"

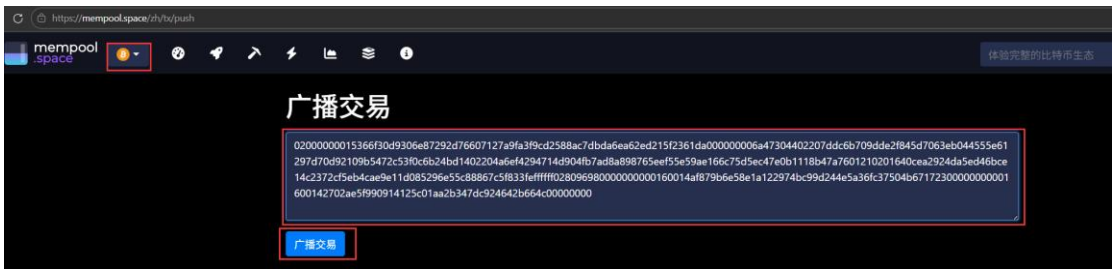


成功广播了交易信息。等待打包确认，TXID:
e3d623b7509289cb285252a53d6d0dae2aab25f189c194c6828cf2c1d6d9774c
打包完成后可以看到这个 UTXO 已经成功转账了。



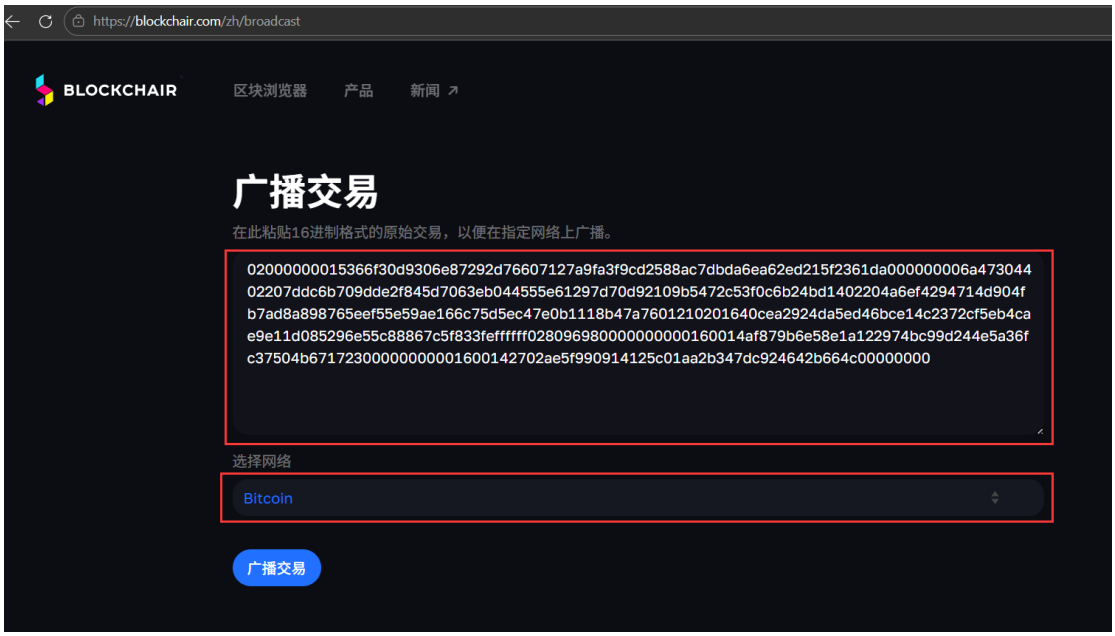
这个实验测试了 从 A2地址里 把 比特币 转到 时间锁脚本地址B3 中一部分（0.1 个），另一部分找零给 B2 地址。

★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



五、【实验三】锁定性测试：未到期强制广播

实验目的：

验证在设定日期到达前，资金是否被数学逻辑硬性锁定。试图将 B3 资金转出到 A2，找零地址为 B2。

操作步骤：

整理信息：

地址 B3：

bc1q0mhhghl7a0m3ah94jjg7dpwczq0erdydu37k36zhmvp5t0xj65qs2c3z0n

私钥：L3PMcvqpKyQu1UQq6NbGYKvjzKLQhcR97WxHaPrThATq35At88nR

地址 A2：

bc1qv2u57h8v0jrggjlm2rph6up9ann6fnj329whug

私钥：接收地址不需要私钥

地址 B2：

bc1qea52r0pfwa0ecnetspv83m27yra4r4snymrycs

私钥：找零接收地址不需要私钥

确认时间：确认当前时间 19：17 未达到 B3 设定的解锁时间 20:20。



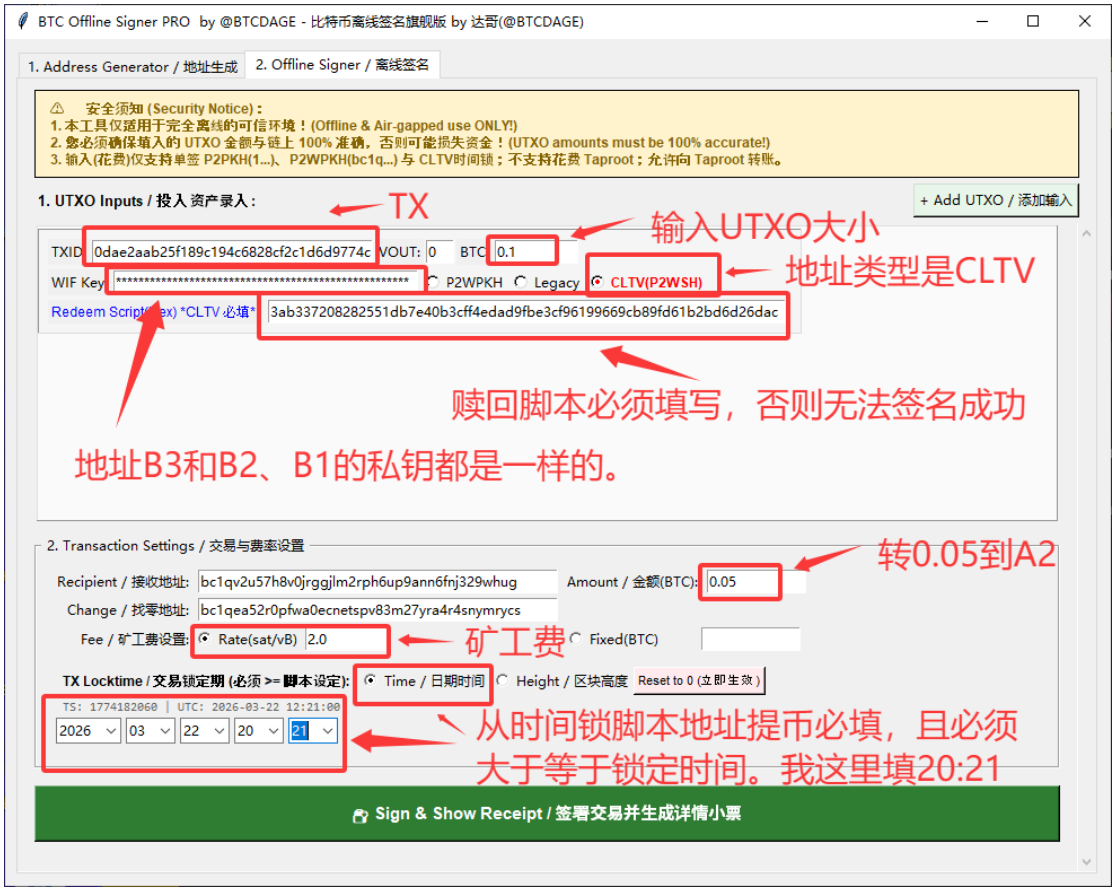
B3 地址的 0.1 个币来源 TXID 是:

e3d623b7509289cb285252a53d6d0dae2aab25f189c194c6828cf2c1d6d9774c



索引为 0

离线签名环节：



因为 B3 是一个受 CLTV 保护的时间锁地址。

所以除了常规的 TXID、VOUT 索引、UTXO 金额和私钥外，还必须填入当时生成地址时配套生成的赎回脚本 (Redeem Script)。

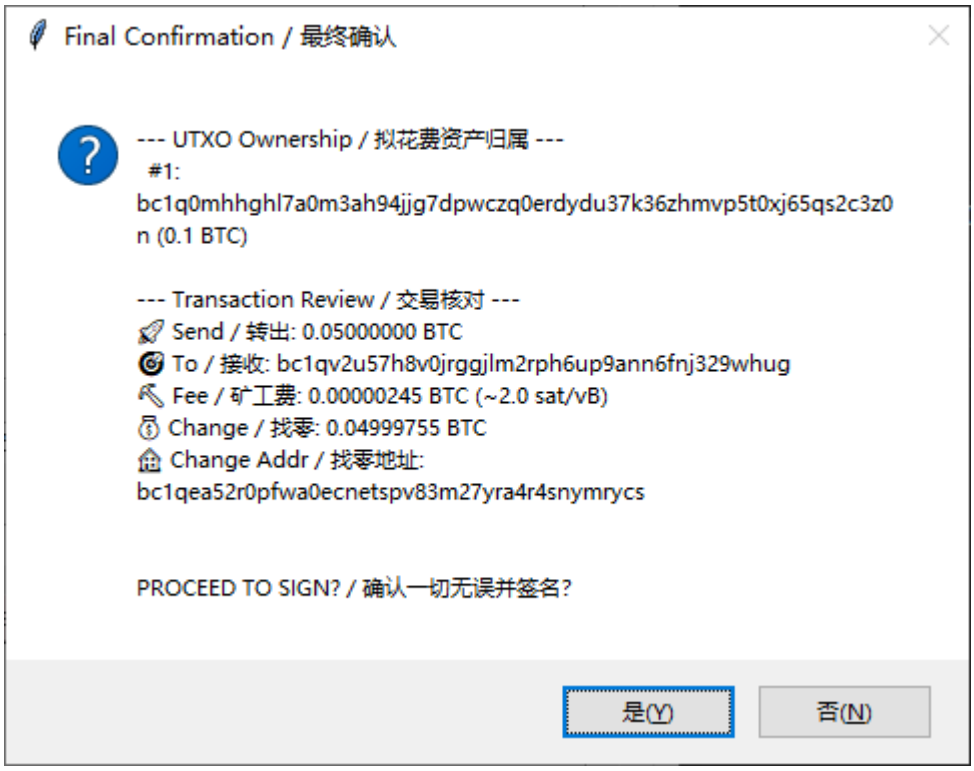
地址类型也要选择 CLTV(P2WSH)。

另外，第二步除了填写接收地址、找零地址、发送金额和手续费之外，还需要填写 Locktime。

而且这个值必须≥生成地址时填写的 Lock Until。

因为我们测试时填的是 2026-03-22 20:20，这里我就填了 2026-03-22 20:21。

点击 验证签名按钮



检查小票信息，确认没问题后点“是”。



sendrawtransaction
"020000000001014c77d9d6c1f28c82c694c189f125ab2aae0d6d3da5525228cb899250b723d6e30000000000feffffff02404b4c0000000000160014 62b94f5cec7c86844bfb50c37d7025ece7a4ce514b4a4c0000000000160014cf68a1bc29775f9c4f2b805878ed5e20fb51d613024730440

2202186164bf80ed886bdd6117cdc5775fb7a2b6d830492a9c4b83b06fae7bc4bc7022052d31
14caa378e5c7cec19e41f3ff2ae120a9c322893cc3827368e7134eb0c6c012a0470debf69b1752
10373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26dacacdebf69
"

签名成功。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。



因为当前时间才 19:33:04，没有到达我签署交易时声明的解锁时间（20:21），所以全网节点直接从底层拒绝接收这个转账请求（交易未满足网络的“最终性条件”，报 non-final 错误）。我们等到解锁时间到了以后再试。

这个实验成功测试了 未到解锁时间强制广播交易信息会返回：non-final 错误 (code -26)。

六、【实验四】解锁测试：到期后成功广播

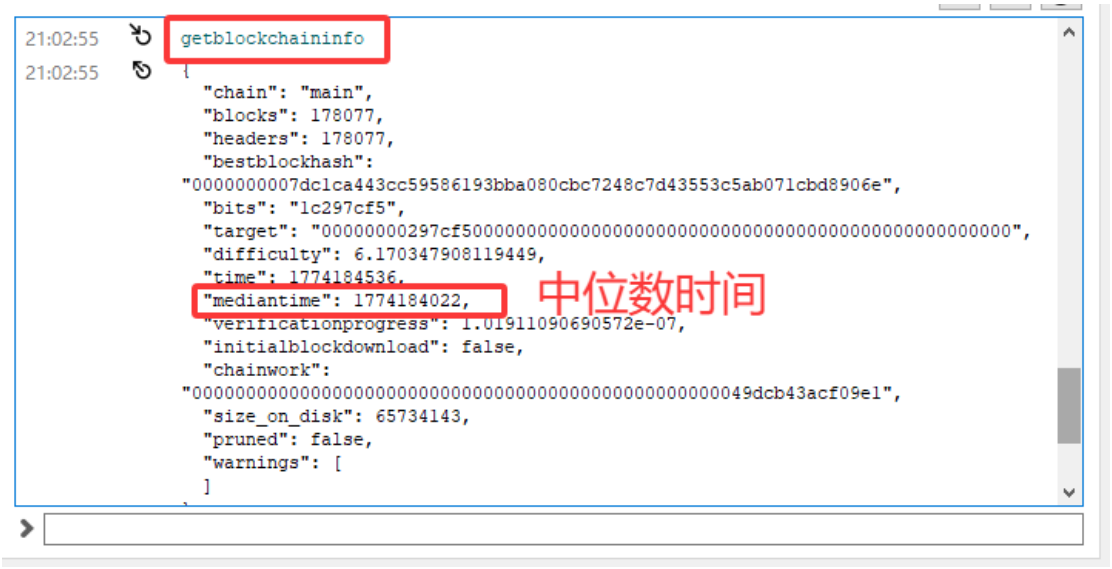
实验目的：

验证时间一旦到达，之前生成的签名信息将恢复有效。

操作步骤：

等待链上时间中位数（MTP）跨过我们签署交易时设定的 Locktime（20:21）

虽然我们设定的解锁时间是 20:21，但由于比特币的链上时间（中位数）比现实时间慢大约 1 小时，我们需要在现实中等到 21:00 左右。
现在是 21:02，我们可以通过 getblockchaininfo 命令查看当前的共识时间（共识时间是链上最近 11 个区块的中位数）。



链上共识时间是　1774184022 ,已经大于我们签名的 1774182060 。

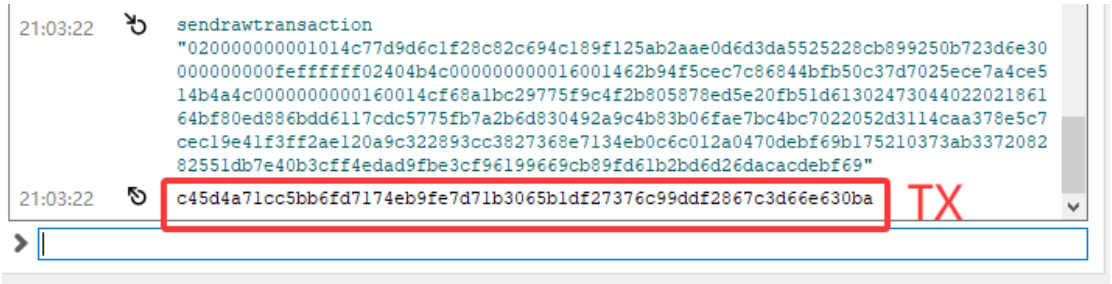
再次广播：

在参数设置正确的前提下，无需重新签名！直接复制【实验三】中因为时间未到而广播失败的那个 Raw Hex。

在联网机器再次执行广播指令。

sendrawtransaction

"020000000001014c77d9d6c1f28c82c694c189f125ab2aae0d6d3da5525228cb899250b723d6e30000000000feffffff02404b4c0000000000160014 62b94f5cec7c86844bfb50c37d7025ece7a4ce514b4a4c0000000000160014cf68a1bc29775f9c4f2b805878ed5e20fb51d6130247304402202186164bf80ed886bdd6117cdc5775fb7a2b6d830492a9c4b83b06fae7bc4bc7022052d3114caa378e5c7cec19e41f3ff2ae120a9c322893cc3827368e7134eb0c6c012a0470debf69b175210373ab337208282551db7e40b3cff4edad9fbe3cf96199669cb89fd61b2bd6d26dacacdebf69"



广播成功，返回 TXID：

`c45d4a71cc5bb6fd7174eb9fe7d71b3065b1df27376c99ddf2867c3d66e630ba`

在区块浏览器查询，资金已成功从时间锁地址 B3 转入 B2。



实验结论：时间锁顺利解锁，资产安全提取。

七、常见问题解答 (Q&A)

Q：为什么生成地址后一定要保存那个 TXT 文件?
A：普通地址只需私钥。时间锁地址需要“私钥+赎回脚本”。如果脚本丢失，全网没人知道这笔钱的锁定参数，资金将永久消失。

Q：TX Locktime 必须设置为和脚本里的锁定时间相等或者更晚吗?
A：是的，这是比特币的共识机制（BIP-65）。赎回脚本（保险箱）规定了“不准早于 12 点开启”，那么你发出的转账申请（TX Locktime）必须向全网声明“我要在 12 点（或之后）花费”。如果你申请书上写的时间早于保险箱设定的时间，节点就会判定逻辑冲突并直接拒绝。

Q：普通转账误加了时间锁怎么办?
A：如果你的 TX Locktime 选成了未来，交易就会变成“延时交易”。在你广播时，节点会直接拒绝这笔交易（报错 non-final），它根本不会进入内存池。因此，你无需担心资金被卡住，也不需要加手续费进行 RBF 覆盖。你只需使用相同的 UTXO，重新签署一笔 Locktime=0（点击 Reset to 0 按钮）的普通交易，直接广播即可立即生效。

Q：为什么现实时间已经过了我设定的 Locktime，广播时仍然报错 non-final (code -26)?
A： 这是因为比特币网络存在 MTP（过去 11 个区块时间中位数）延迟。为了防止矿工篡改时间，比特币不使用电脑的本地时间，而是取最新 11 个区块时间的“中位数”作为全网共识时间。这个共识时间通常比现实时间慢大约 1 小时。可以在全节点上通过命令“**getblockchaininfo**”查询，返回的“**mediantime**”字段就是这个共识时间的时间戳。
遇到这种情况不要慌，只需耐心等待大约 1 小时，等网络出块把“共识时间”推移到你设定的时间之后，同一串 Hex 即可广播成功。

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 在交易结构与脚本规则层面高度兼容比特币主网，所以在 nextBTC 上测试成功，则在主网上表现将会一致。