Electrum 是一款经典的比特币轻钱包，2011年11月由 Thomas Voegtlin 创建，几乎是和比特币一起成长起来的，迄今一直保持着稳定的更新，是资深币友使用最广泛的钱包之一。

Electrum 支持 Windows、MacOS、Linux 和 Android（安卓）系统，但不支持 iOS （苹果手机系统）。笔者建议使用电脑来操作，因为它的界面设计用的是老的底层技术，好处是占内存不多，老旧设备也都可以用，但在小屏幕上体验不太好。

Electrum 是一款轻量级钱包，它把比特币区块链的数据做了索引，存放在多个高性能服务器上，这样客户端的用户就可以即时查看自己钱包的状态了。相比社区首推的、每次都需要很久时间来同步区块链数据的全节点内置钱包，还是方便了很多。

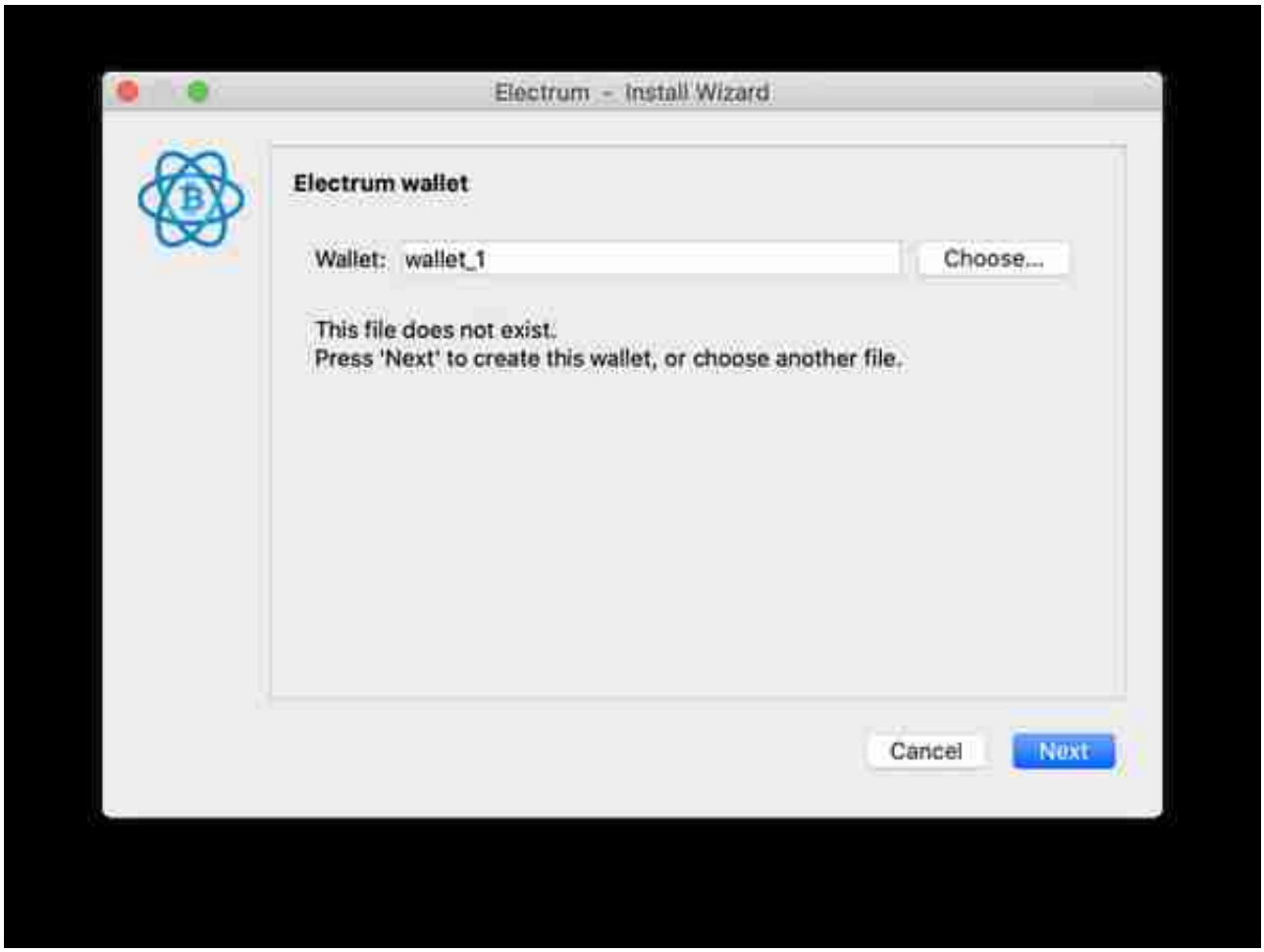
由于 Electrum 是开源的并且由许多行业资深的独立开发者维护，我们可以知道并没有用户的敏感数据会被发送到网上，因此它的安全性尚可。

之所以说尚可，是因为它也曾被黑客利用，向用户发送虚假的软件版本更新信息，使一些下载的用户被盗币了。这个漏洞虽然早已被修复，但很多用户用的是被改过的假软件和早期版本，导致这样的问题一再发生。

这不是 Electrum
独有的问题，在币圈永远不要
用网上搜到的下载站，一定要去官网下载最新的版本。

安装

官方下载地址：https://electrum.org/#download



点击右下角蓝色按钮“Next”，


Electrum - Install Wizard
Keystore
Do you want to create a new seed, or to restore a wallet using an existing seed?
Create a new seed
I already have a seed
Use a master key
Use a hardware device
Back
Next

继续点“Next”，

在中间方框里显示的 12 个单词，就是你的“私钥”助记词，也称为“种子”：

screen crucial funny junk divorce forest mention trophy duty skull vast lunch

实际操作时，
不要像我这样把它拷贝出来或者截图、
拍照
，我是做完这个文档就会抛弃这个钱包的，而读者要用笔纸记录下来，不要用任何电子形式。只要有这 12
个词汇，这个钱包就是属于你的，即使以后这个电脑的数据都丢了也没关系。

记好后点击“Next”，

输入用于加密私钥的密码，打两遍。

当用户的私钥被写入文件保存时，会用这个密码进行加密，这样即使别人得到这个电脑，没有这个密码也无法解锁出私钥。

换句话说，这个密码只是为了保护私钥文件，它不是私钥的一部分，用户后续也可以修改。当用户在新的电脑上恢复钱包时，只需要“种子”就够了，只有“种子”对应着私钥。

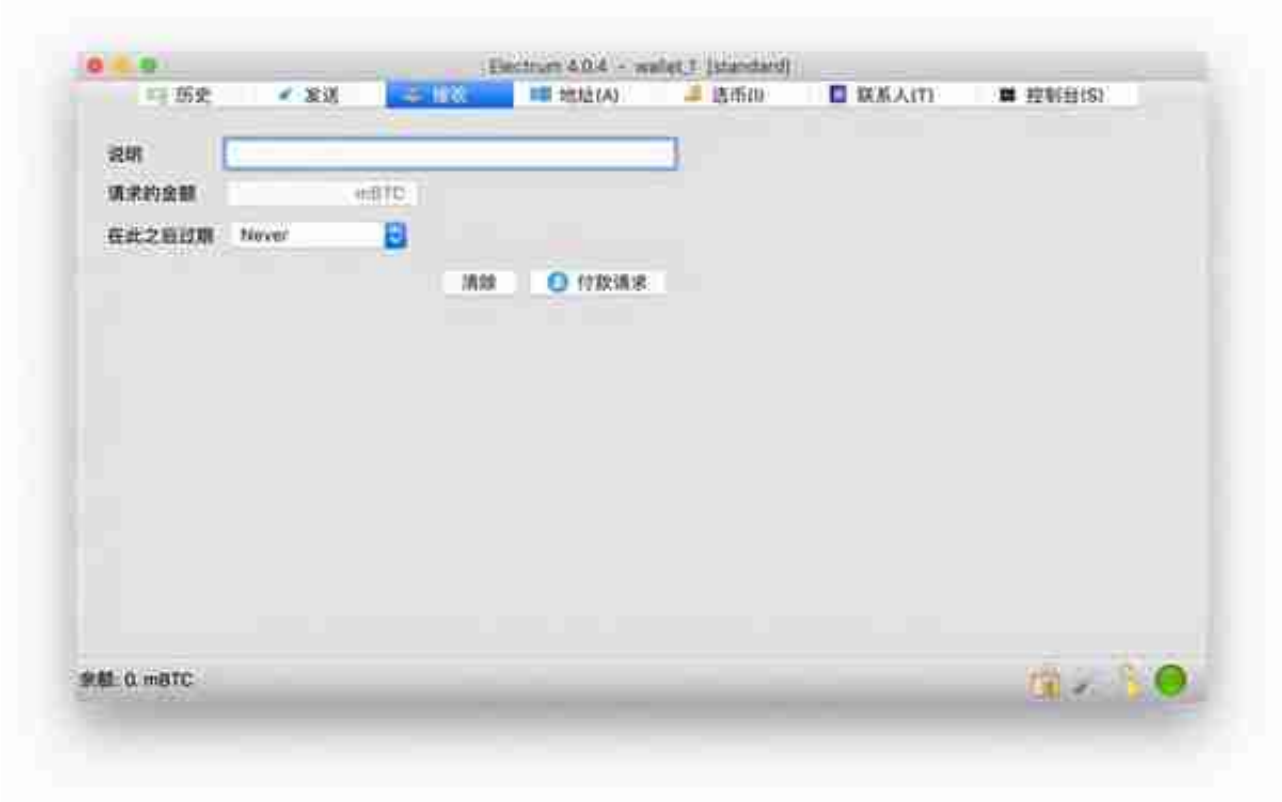
点击“Next”，

将 Language 后的选项改为 “Chinese Simplified” ，再点下面的按钮 “Close” ，然后退出整个程序再重新打开。

这时候如果连接网络，右下角的圆灯变为绿色，就意味着已经连上了服务器，左下角会显示出这个钱包里的比特币总“余额”，白色背景框里是所有历史交易流水（这个钱包此时还没用过，所以是空的）。

如果用户将此机器用于“冷钱包”，则不要连接网络，那么右下角将保持红色。

点击上方按钮条里的“地址（A）”，

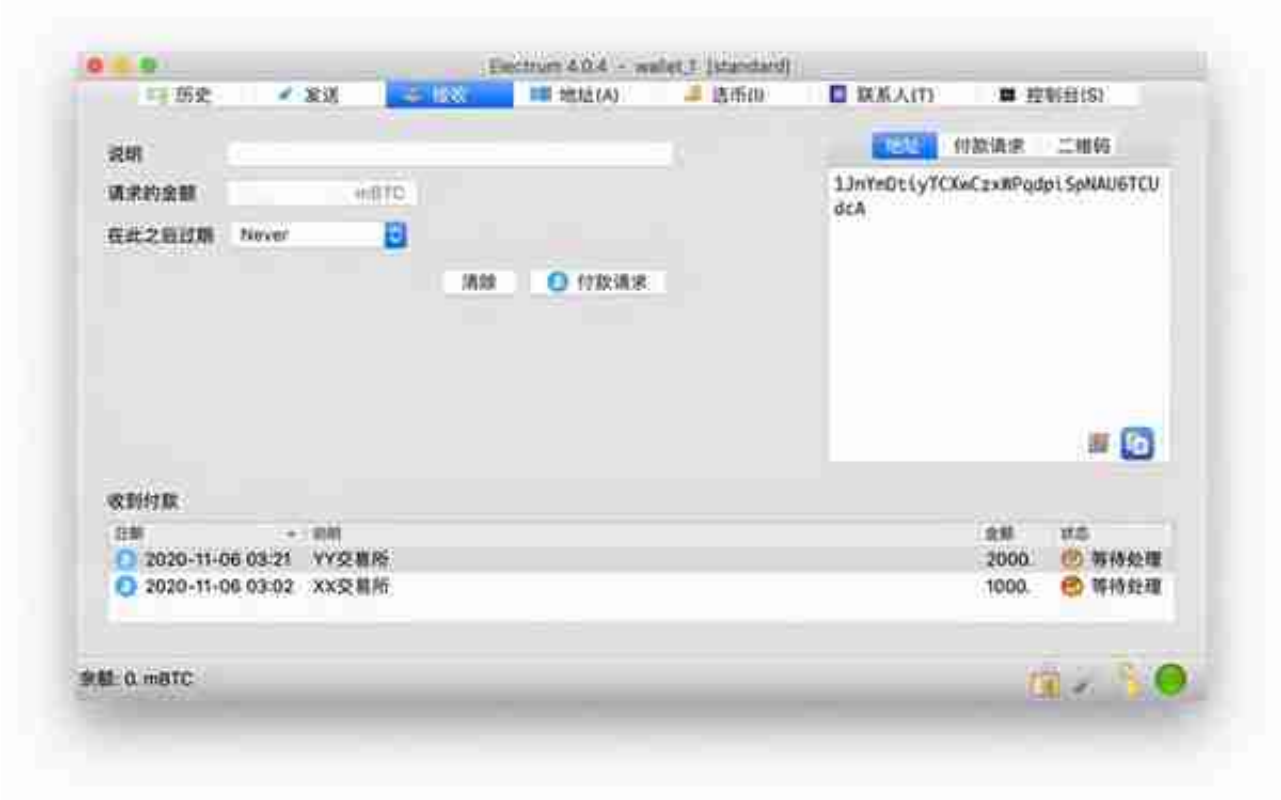


假设我们要从“XX交易所”提币，那么：

- “说明” 建议填写要收款的对方名称，比如“XX交易所”。
- “请求的金额” 填写预期会收到的比特币数量。
- “在此之后过期” 选择“Never”，就是“永不过期”的意思。这个怎么不是中文，毛病。

其实，以上几栏都可以不填写。这些都是为了同时向很多人收款时方便自己查看的标注信息，只会在这台电脑上存在，填写错了也不会对收款产生任何影响。

点击按钮“付款请求”，



点击上方按钮条里的“地址（A）”，可以发现刚刚出现的这两个地址正好是绿色“收款”列表的前两个。

- “支付给” 填写接收者的地址码。
- “说明” 随便写吧，只是留给你自己的备注，要是换了电脑也不存在了。
- “金额” 对方将要收到的比特币的数量。注意这个单位是mBTC（一个比特币的千分之一），比如要发送1个比特币，就写1000。

连上网络，点击“支付”按钮，输入密码点击“发送”，币就发出去了。

发送后实际扣除的比特币数量还包括给矿工的手续费，在发送时 Electrum 会为用户默认选择当前适中的费率，一般没有必要自己定制。

如果想要修改手续费，在发送之前可以点击“高级”按钮弹出交易细节界面，

将“主公钥”里面的内容拷贝出来，放进任何文本编辑器里面存为文件，并插入U盘，将文件移动到里面备用。

在新的工作电脑里安装好 Electrum，创建一个新钱包，名字比如叫“wallet_1查看”，类型为“标准钱包”，
密钥库选择“使用主公钥（主公钥或主私钥）”，点击“下一步”，

在下个页面设置钱包访问密码。这个密码最好和私钥的那个密码不同。

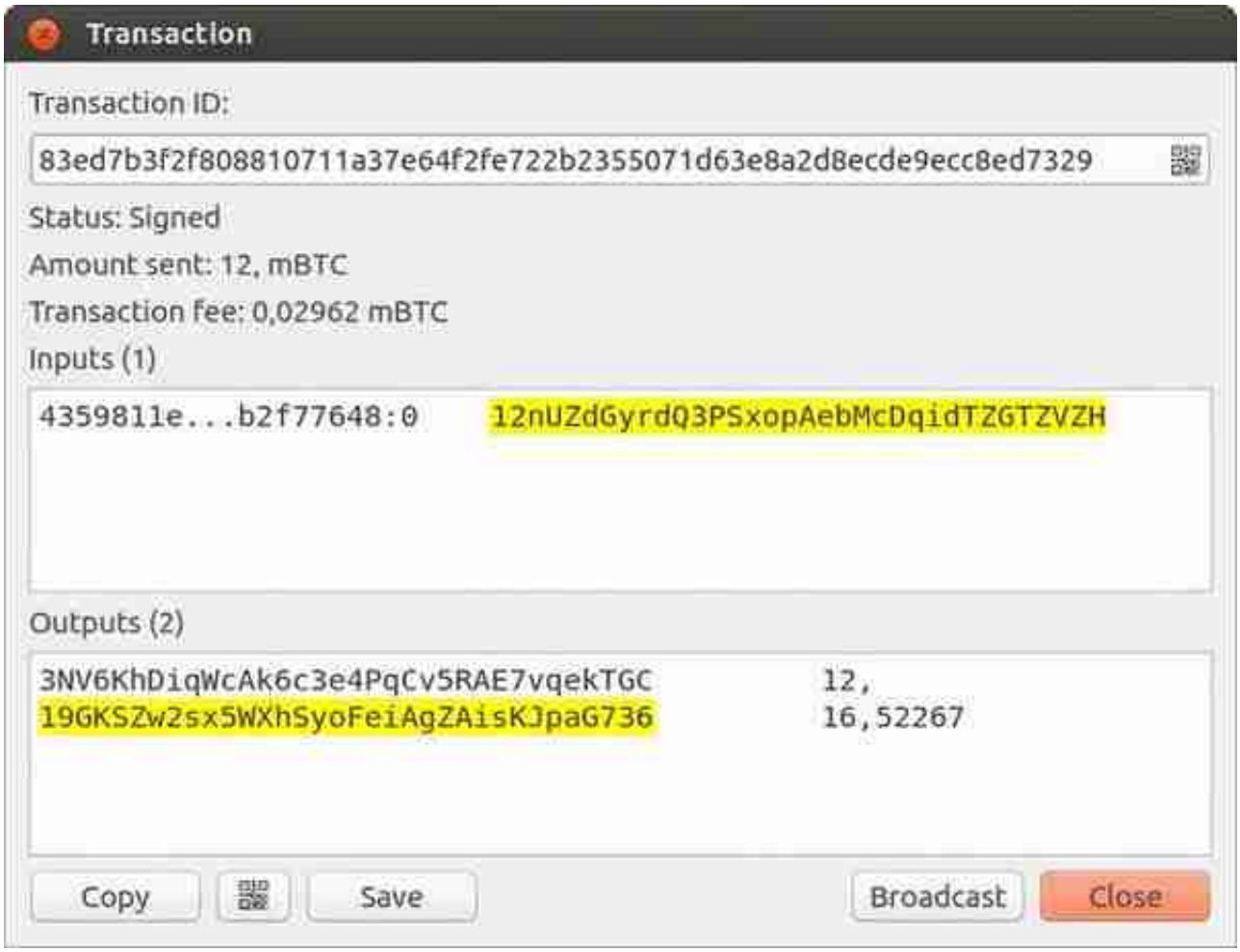
以后只要使用菜单“文件->打开”就可以看到“wallet_1查看“这个仅供查看的钱包了。因为它里面没有私钥，所以即使数据泄露了也没有关系。除非为了发送币再也不用去操作热钱包的那台电脑了。

如何使用冷钱包

在前面这个分别安装有“热钱包”和“仅供查看的钱包”的两台机配置基础上，通过软件操作的一点变化就可以让“热钱包”变成“冷钱包”。

在发送币的时候，“热钱包”模式是在有私钥的机器上操作的。而“冷钱包”由于不会让有私钥的机器联网，所以发送币的操作在“仅供查看的钱包”来发起。

填写好交易信息后不要点“发送”（无意点到也没关系，没有私钥发不出去的），而是点击“预览”按钮，出现下面的窗口：



选择“广播”（Broadcast）按钮，这个签过名的交易就被发送出去了。

这个过程是使用U盘作为在“联网的查看电脑”与“不联网的冷钱包电脑”之间的媒介的，由于物理隔离了存有私钥的冷钱包，让它更加安全。U盘和联网电脑的数据都是可以暴露的，因为它们都不携带私钥信息。

小结

以上介绍了 Electrum 的基本使用方法。关于正式的使用文档，除了官网上的“Documentation” 链接之外，还有个更加详细的非官方版本在“bitcoinelectrum.com”，可惜都是英文的。

我写这个“精解”也是应几个粉丝的要求，也因为网上很少有让人看完就明白的 Electrum
说明文章，发布出来希望可以同时帮助到其他希望设置比特币冷钱包的朋友。