مطالبی درباره روش تولید و نگهداری «کلید خصوصی بیت‌کوین»

آذر ۹۸

درباره کلید خصوصی بیت‌کوین

حتما بارها این جمله رو شنیدید «فلان کیف‌پول سخت یا نرم افزاری خیلی امنه»، اما واقعا «امنیت» اینجا چه معنی‌هایی میتونه داشته باشه؟ برای درک این مفهوم باید کمی به عقب برگردیم یعنی حتی قبل از تولید کلیدخصوصی و آدرس بیت‌کوین.

در سیستم بیت‌کوین از یک روش رمزنگاری استفاده شده که برای بهره بردن از اون احتیاج به یک جفت کلید داریم. اگر بخوایم ساده‌تر به این دو کلید نگاه کنیم، اونها شبیه به یک آدرس عمومی و یک رمز هستن. باز برای اینکه موضوع بهتر جابیفته می‌تونیم بگیم یکی از این کلیدها رمز خصوصی و اون یکی آدرس عمومی حساب ماست. یک چیزی شبیه به ایمیل: شما یک رمز خصوصی دارید و یک آدرس عمومی. آدرس رو به همه میدید که براتون ایمیل بفرستن اما برای ارسال ایمیل باید حتما رمز خصوصی خودتونو بدونید. توی سیستم بیت‌کوین هم اینطوریه شما یک رمز خصوصی دارید و یک آدرس که اون آدرس رو بصورت عمومی به دیگران میدین که براتون بیت‌کوین ارسال کنن اما اگر بخواین از بیت‌کوین‌هاتون برای دیگران ارسال کنید باید رمز خصوصی‌تون رو بدونین. این باعث می‌شه که کسی نتونه بیت‌کوین فرد دیگه‌ای رو ارسال یا خرج کنه.

پس تا اینجا متوجه شدیم که باید یک رمز بسازیم و توی متون فنی بیت‌کوین به این رمز می‌گن «کلید خصوصی» اما این کلید خصوصی فقط یک کلید نیست، بلکه یک «شاه کلیده». فرض کنید شما یک آپارتمان چند طبقه دارید و هرکدوم از واحدهای این آپارتمان شما یک کلید مخصوص خودشونو دارن حالا شما که صاحب همه اونها هستید علاوه بر کلیدی که هرکدوم از واحدها بطور جداگانه دارن، یک شاه‌کلید هم دارید که به همه قفل‌ها می‌خوره و اونها رو باز می‌کنه. حالا اگر برگردیم به سیستم بیت‌کوین لازمه اون «کلید خصوصی» که قبلا حرفش رو زدیم یک «شاه کلید» باشه چون باید بتونیم ازش ده ها و شاید صدها جفت (کلید و آدرس) بیت‌کوین بسازیم.

در متون عمومی یا فنی بیت‌کوین کسی به اون کلید موردنظر «شاه کلید» نمی‌گه و اسمش رو گذاشتن seed. در واقع روش کار کیف‌پول‌های بیت‌کوین به این صورته که اونها seed رو برای شما می‌سازن یا از شما می‌گیرن و از اونجا به بعد کار ساختن کلیدها و آدرس‌های متعددی که باهاشون کار می‌کنید پشت صحنه و بر پایه اون انجام می‌شه.
اگر به این اسم دقت کنید می‌بینید که مفهوم همون شاه‌کلید خودمونو داره چون مثل بذری می‌مونه که در نهایت مارو به کلیدهای خصوصی و آدرسهامون می‌رسونه. ما اینجا از این به بعد به کلید خصوصی اصلی که صحبتش رو کردیم میگیم «کلیدخصوصی بیت‌کوین» و به کلیدخصوصی هر کدوم از آدرس‌ها می‌گیم «کلید خصوصی آدرس بیت‌کوین»

خب حالا فرض کنید شما میخواید یک کیف‌پول بیت‌کوین درست کنید. سوال من از شما اینه که چطوری «کلید خصوصی بیت‌کوین» خودتونو انتخاب می‌کنید؟

برای جواب به این سوال باید دوباره یک مثال بزنیم که شما باهاش آشنایی دارید: فرض کنید برای ثبت نام وارد سایت جیمیل شدید و می‌خواهید یک حساب ایمیل بسازید. گوگل اطلاعات شما را می‌گیره و در آخر از شما میخواد یک رمز انتخاب کنید. قبلترها هر پسوردی رو میتونستید انتخاب کنید مثلا شماره موبایلتون اما هرچی گذشت سایتها قوانین تعیین پسوردشون رو سخت‌تر کردن فکر میکنید چرا؟ دلیلش خیلی ساده اس چون اونها میخوان از اطلاعات ایمیل شما محافظت کنن و هرکسی نتونه با حدس زدن رمز شما به محتویات ایمیل شما دسترسی داشته باشه. حالا فرض کنید پای دارایی شما وسط باشه. حالا شما برای انتخاب کلیدخصوصی حساب فرضی بیت‌کوین‌تون چقدر سختگیری می‌کنید؟

خوشبختانه نیازی نیست کاربرهای بیت‌کوین برای تعیین کلیدخصوصی به خودشون زحمت بدن چون تولید اون توسط کامپیوتر و به راحتی انجام می‌شه. مثلا این پایین می‌تونید یک کلیدخصوصی بیت‌کوین رو ببینید:

```
39BD194E3B989D612E6ED5BF485BAE130D53F5F532F29585E98ECD298282A5C3
```

چطور ممکنه که یه نفر بتونه این رو حفظ کنه؟

این سوال کاملا منطقیه و برای حل اون راهکاری پیشنهاد کردن که بشه این کلید خصوصی بیت‌کوین رو به تعدادی کلمه تبدیل کنیم تا بتونیم راحت تر به خاطر بسپریم. این کلمات مجموعه‌ای از ۲۰۴۸ کلمه منحصربفرد هستن که لیستشون در یک استاندارد توی شبکه بیت‌کوین تعریف شده و کامپیوتر شما با یک روش مشخص کل رمز یا همون کلید خصوصی شما رو به ۲۴ (یا گاهی ۱۲) کلمه تبدیل می کنه. حالا حتما فهمیدید که چرا هر کیف پولی روی گوشی یا کامپیوترتون نصب می‌کنید به شما چند کلمه نشون میده و ازتون میخواد حتما اونها رو یک جایی بنویسید و ازش نگهداری کنید.

کلمات متناظر با کلید خصوصی ۶۴کاراکتری ما اینها هستند:

```
defy trip fatal jaguar mean rack rifle survey satisfy drift twist champion
steel wife state furnace night consider glove olympic oblige donor novel left
```

این ۲۴ کلمه، کلمات متناظر کلیدخصوصی ۶۴کاراکتری هستن که بالاتر نشون دادیم و ترتیب کلمات هم مهمه. در واقع این کلمات همون کلید خصوصی بالا هستن فقط برای اینکه کاربرها بتونن راحت‌تر اونها رو یادداشت کنن تبدیل به این کلمات قابل فهم شدن.

حالا که قراره کلید خصوصی ما رو کامپیوتر ما تعیین کنه از کجا معلوم کلیدخصوصی ۲ نفر یکسان انتخاب نشه؟

جواب این سوال بدون اینکه بخوایم خودمون رو درگیر ریاضیات و علوم کامپیوتر کنیم اینه که داخل همه سیستم‌عامل‌ها (ویندوز مکینتاش و لینوکس) یک منبع تولید بی‌نظمی درنظر گرفته شده و هر زمان که ما از سیستم‌عامل درخواست یک عدد تصادفی می‌کنیم، سیستم‌عامل با استفاده از اون بی‌نظمی مقداری رو برمی‌گردونه. ممکنه این سوال برای شما پیش بیاد که سیستم‌عامل درعمل چطور می‌تونه این اعداد تصادفی رو تولید کنه؟ به عبارت دیگه اونها چطور «بی‌نظمی» تولید می‌کنن؟

جواب به این سوال برمی‌گرده به منابع تولید بی‌نظمی که ساده‌ترین اونها ۱-فاصله‌های زمانی فشردن کلیدهای کیبورد و ۲-حرکت‌های نشانگر موس بر روی صفحه هستند.

در واقع شما با استفاده از کیبورد و موس کامپیوترتون دارید به سیستم عاملتون کمک می‌کنید تا برای شما بی‌نظمی تولید کنه و درنهایت از این داده‌های تصادفی برای تولید «کلید خصوصی» بیت‌کوین شما استفاده می‌کنه. اگر دقت کرده باشید بعضی از سایت‌هایی که آدرس بیت‌کوین تولید می‌کنن از شما می‌خوان نشانگر موس‌تون به مقدار معینی روی صفحه حرکت بدید تا کلید خصوصی و آدرس شما تولید بشه.

چطور می‌شه از تصادفی بودن کلید خصوصی که والت کامپیوتر/موبایل/سخت‌افزاری من تولید کرده اطمینان حاصل کرد؟

جواب این سوال اینه که راهی برای تایید امنیت یا به عبارت دیگه تضمین تصادفی بودن کلید خصوصی تولید شده نیست جز بررسی کد اونها درصورتی که اپن سورس باشن و در واقع با استفاده کردن از اونها بهشون اعتماد کردیم.

«با توجه به مطالبی که مطرح شد حالا می‌شه گفت که کلید خصوصی بیت‌کوین باید از یک عدد کاملا تصادفی ساخته بشه و روش ساختنش توی امنیتش اثر زیادی داره»

چطور می‌شه یک کلید خصوصی با امنیت بالا تولید کنیم؟

برای تولید بی‌نظمی باید به دنبال منابع دیگه‌ای علاوه بر چیزی که سیستم عامل فراهم می کنه باشیم. ساده‌ترین و دم دست ترین چیزی که به ما امکان تولید اعداد تصادفی و بی‌نظم رو می‌ده استفاده از تاس هست. با یک یا چند تاس سالم می‌شه داده‌ی بی‌نظم و تصادفی تولید کرد. تاس سالم یعنی تاسی که بخاطر ویژگی‌های فیزیکی و ظاهریش گرایش به یک عدد خاص نداشته باشه. معمولا این تاس ها بصورت مکعب مربع ساخته می‌شن و لبه های اونها تیزه و مثل تاس های رایج لبه‌های اریب ندارن.

روش تولید کلید خصوصی با استفاده از تاس چیست؟

ابزارهای اپن‌سورسی برای تولید کلید خصوصی بیت‌کوین و کلمات متناظرش با استفاده از بی‌نظمی های تولید شده از پرتاب تاس و سیستم عامل موجوده. در علم رمزنگاری ثابت شده که اگر دو بی‌نظمی رو با هم ترکیب کنیم، نتیجه‌ی به دست اومده از تک تک عوامل سازنده‌اش بی‌نظمی بیشتری داره. یکی از معروف‌ترین اونها پروژه «گلیسیر» هست که آدرسش در پایین آورده شده. همچنین یک پروژه اپن‌سورس دیگه هم معرفی شده که یک رابط گرافیکی برای تولید کلیدخصوصی به کمک تاس داره.

- https://github.com/GlacierProtocol/GlacierProtocol
- https://github.com/bitcoinfromscratch/bfs-dice

اگر با مفاهیم کلیدخصوصی و نحوه ساخت آن کاملا آشنا نیستید فقط برای آموزش و یادگیری از این ابزارها استفاده کنید. اگر نه به احتمال خیلی زیاد ممکنه بیت‌کوین‌هاتون رو از دست بدید و هیچ کسی نمی‌تونه برای برگردوندنشون بهتون کمک کنه.

درباره کیف پول بیت‌کوین

کیف‌پول بیت‌کوین الکترام از قدیمی‌ترین و خوشنام‌ترین کیف‌پول‌های بیت‌کوینه که اگر به روش درست ازش استفاده بشه از درجه امنیت بالایی برخورداره. این راهنما به شما کمک می‌کنه از این کیف پول برای نگهداری از کلیدخصوصی بیت‌کوین در حالت آفلاین و برای مشاهده موجودی از حالت آنلاین استفاده کنید.

این راهنما فرض رو بر این می‌گذاره که شما:

- کلید خصوصی (کلمه‌های BIP39 mnemonic) بیت‌کوینتون رو ساختید. حالا یا با ابزار استفاده از تاس یا یک کیف‌پول نرم/سخت افزاری که خودتون دارید
- بطور کلی کار کردن با الکترام رو بلدین – اگر بلد نیستید از یوتوب یاد بگیرید
- نرم‌افزار الکترام رو برای سیستم عامل موردنظرتون دانلود کردید و امضای دیجیتال اون رو چک کردید
- بلدید با virtual machine کار کنید و یک ویندوز-۱۰ تحت virtual-box یا حالا هر نرم‌افزار virtualization دیگه‌ای بالا آوردید

تنظیمات لازم بعد از نصب ویندوز-۱۰ روی virtual-box:

(هرجا مشکلی بود از یوتوب یاد بگیرید باید چکار کنید. این تنظیمات خیلی ساده هستن و راحت می‌تونید انجامشون بدید)

- بعد از نصب کامل ویندوز-۱۰ اون رو خاموش کنید و از تنظیمات virtual-box به قسمت Network برید و کلا اون رو غیرفعال کنید (کلید خصوصی ما روی اونه پس باید همیشه آفلاین باشه)
- دوباره ویندوز روی vm رو روشن کنید و بعد از اینکه کامل بالا اومد VBoxGuestAdditions رو نصب کنید
- از تنظیمات virtual-box مورد shared clipboard رو به حالت bidirectional تنظیم کنید.

- باید از طریق virtual-box یک فولدر رو با ویندوز vm به اشتراک بگذارید تا بتونید فایل نصب الکترام رو به ویندوز روی vm بدید. (بعد از کپی فایل نصب الکترام روی vm می‌تونید این فولدر اشتراکی رو حذف کنید)

تا اینجا شما باید:

- یک سیستم متصل به اینترنت داشته باشید که روش با استفاده از نرم‌افزار virtual-box یک ویندوز تحت vm بالا آوردید که آفلاینه.
- فایل نصب الکترام رو از نظر اصالت بررسی کردید و داخل ویندوز vm (که آفلاینه) کپی کردید
- clipboard سیستم شما و ویندوز روی vm به اشتراک گذاشته شدن و می‌تونید یک متن رو از notepad بصورت دوطرفه کپی پیست کنید.
- کلمه‌های mnemonic رو کنار دستتون آماده دارید

حتما قبل از اینکه روی شبکه اصلی بیت‌کوین کار کنید یک بار روی شبکه تست‌نت روش کار رو تست کنید و تا مطمئن نشدید روی شبکه اصلی نرید. پایین تر توضیح داده شده که چطور الکترام رو با شبکه تست تست‌نت بیت‌کوین بالا بیارید

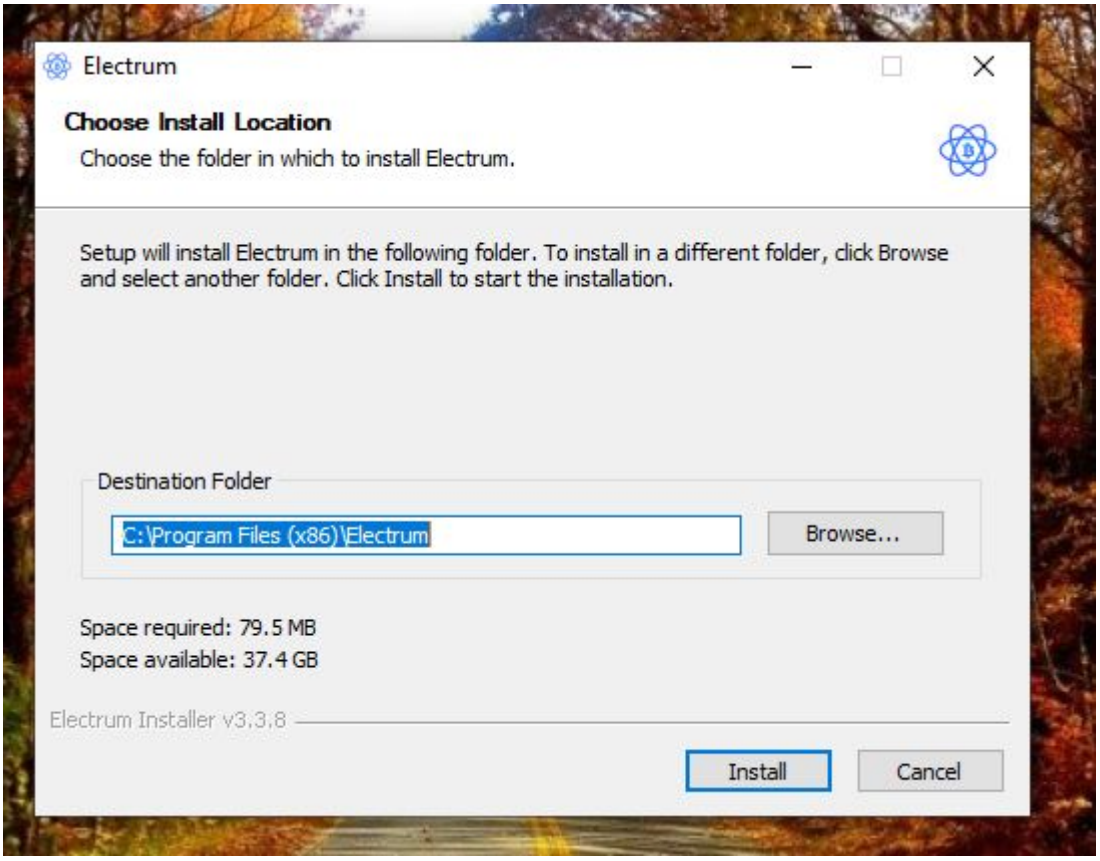
کلیات روش کار: اینجا روش کار توضیح داده میشه. اونهایی که با الکترام کار کردن ممکنه همین توضیح کوتاه براشون کفایت کنه. اگر توضیحات بیشتری لازم بود عکسهای پایین رو ببینید. اگر راهنمای پایین براتون نامفهوم بود یعنی شما نیاز به اطلاعات اولیه دارید و باید از اینترنت یا دوستاتون در حد استفاده از الکترام یاد بگیرید و بعد دوباره برگردید.
ما یک کلید خصوصی بیت‌کوین ساختیم که مهم‌ترین و حیاتی ترین قسمت کار با بیت‌کوینه. هرکس اون کلید رو داشته باشه اختیار بیت‌کوینها دست اونه. پس اصلا منطقی نیست اون کلید رو روی سیستمی بگذاریم که به اینترنت وصله. چون کلی ویروس و بدافزار توی سیستم ما هست که میتونه کلید خصوصی ما رو بدزده. پس کاری که باید بکنیم اینه که کلید خصوصیمونو توی یک سیستم بگذاریم که آفلاینه. تا اینجا ما تونستیم از کلید خصوصیمون خیلی خوب مراقبت کنیم اما یک مشکلی پیش میاد و اون مشکل اینه که اگر ما به اینترنت و شبکه بیت‌کوین وصل نباشیم چطور میخوایم بفهمیم بیت‌کوینهایی که به آدرسهای ما ارسال کردن چندتا کانفرم دارن؟ یا اصلا چقدر بیت‌کوین توی کیف پول ما هست؟

این مشکل رو با استفاده از ۲سیستم حل می‌کنیم. یک سیستم به اینترنت و شبکه بیت‌کوین وصله و یکی دیگه هست که کلید خصوصی ما داخلشه و آفلاینه. حالا فقط یک مشکل دیگه هست که باید حل کنیم. اگر قراره یکی از کیف‌پول ها به اینترنت وصل باشه چه فرقی می‌کنه اگر بخوایم کلید خصوصیمونو واردش کنیم؟ این مشکل رو با استفاده کردن از یک کلید مخصوص حل میکنیم. وقتی توی سیستم آفلاین کلید خصوصیمونو وارد می کنیم، کیف پول الکترام قابلیتی داره که به ما یک کلید بخصوص از روی کلید خصوصی تولید کنه که این کلید ویژگی جالبی داره. وقتی این کلید رو بجای کلید خصوصی وارد الکترام کنیم، کیف پول الکترام می‌تونه از آدرسها و دارایی بیت‌کوین ما خبر داشته باشه ولی نمی تونه اونها رو sign کنه.

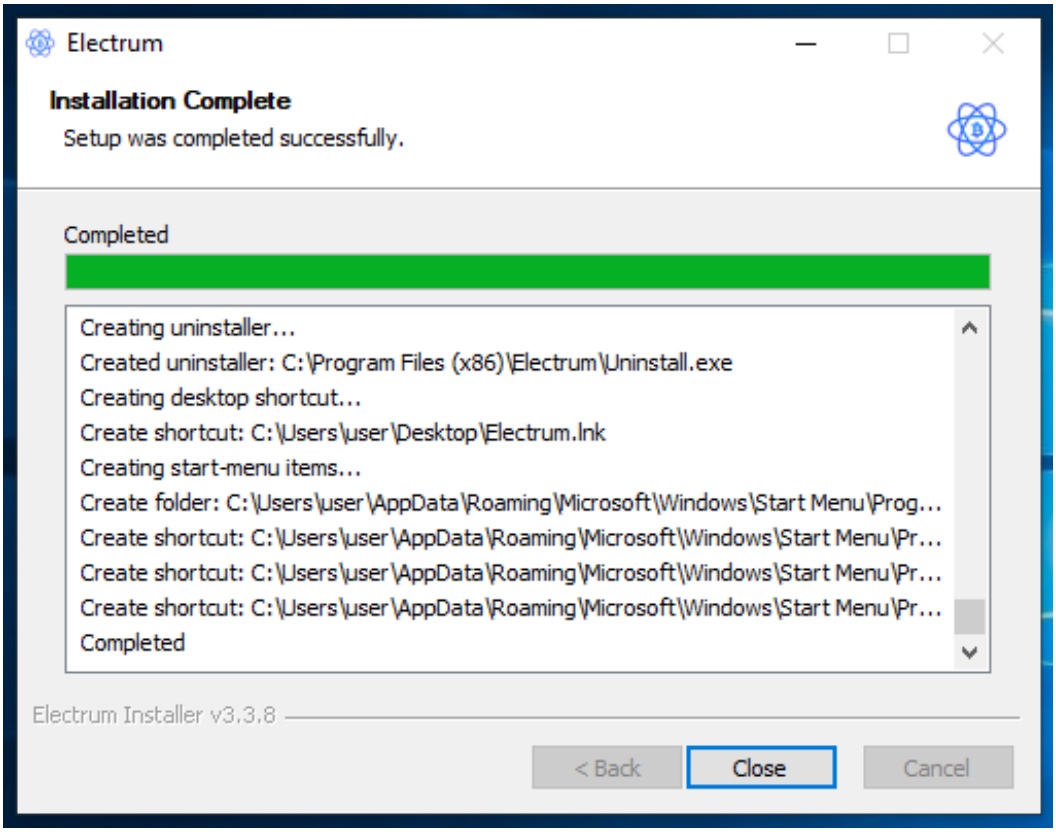
پس روش کار ما اینطوریه که دریافت و رصد دارایی و آدرسهامونو روی سیستمی که به اینترنت وصله انجام میدیم و هروقت خواستیم تراکنش ارسال بیت‌کوینمون رو sign کنیم باید تراکنش رو به سیستم vm که آفلاینه ببریم و کار sign رو اونجا انجام بدیم. برای همینه که بالاتر گفته شده باید clipboard شما بین این دوسیستم به اشتراک گذاشته بشه.

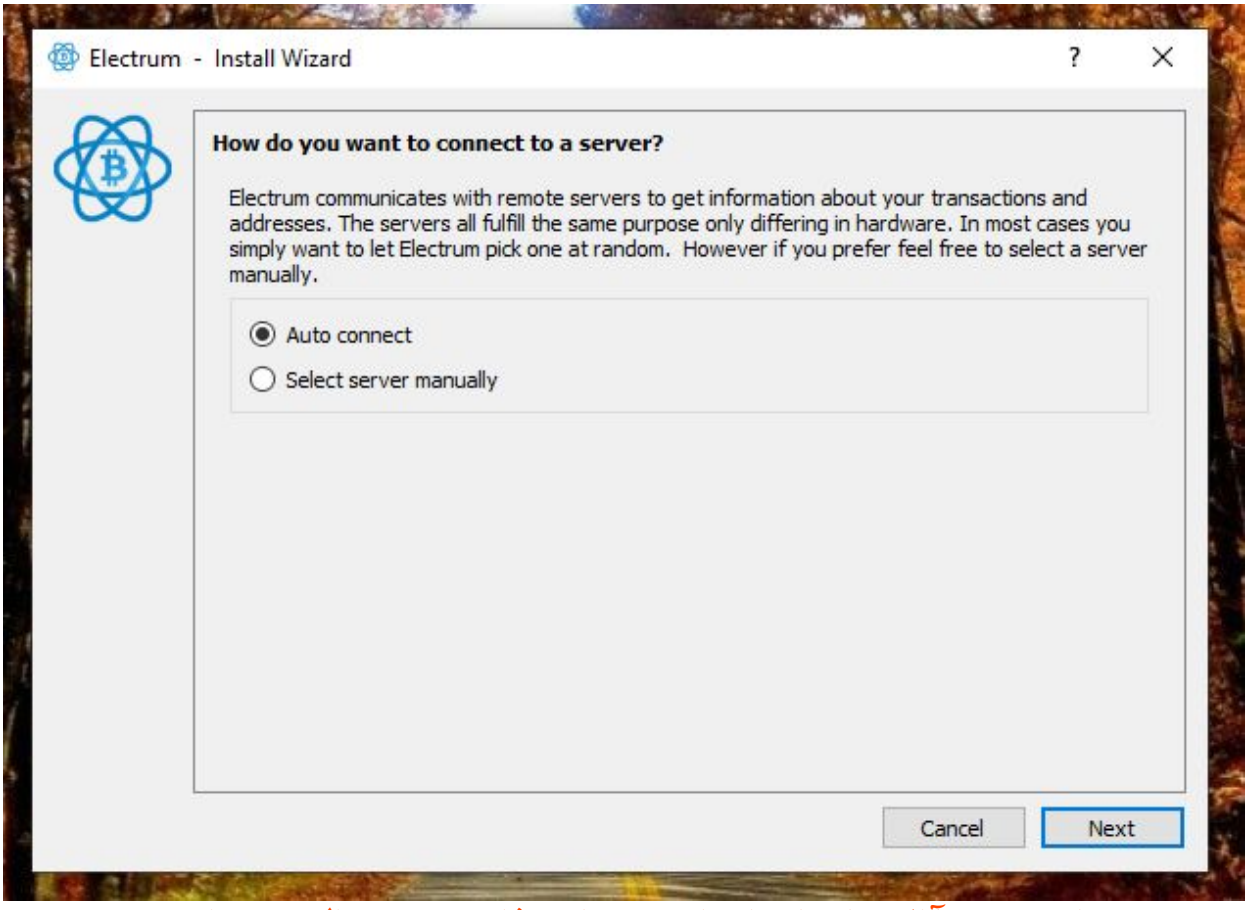
پس ما باید الکترام رو دوجا نصب کنیم: یکبار روی سیستم آفلاین و یکبار دیگه روی سیستم آنلاین. توی عکسهای آموزش پایین سیستم آنلاین به حالت dark درومده تا تفاوت رو راحت تر ببینید.

نصب الکترام روی سیستم vm آفلاین:

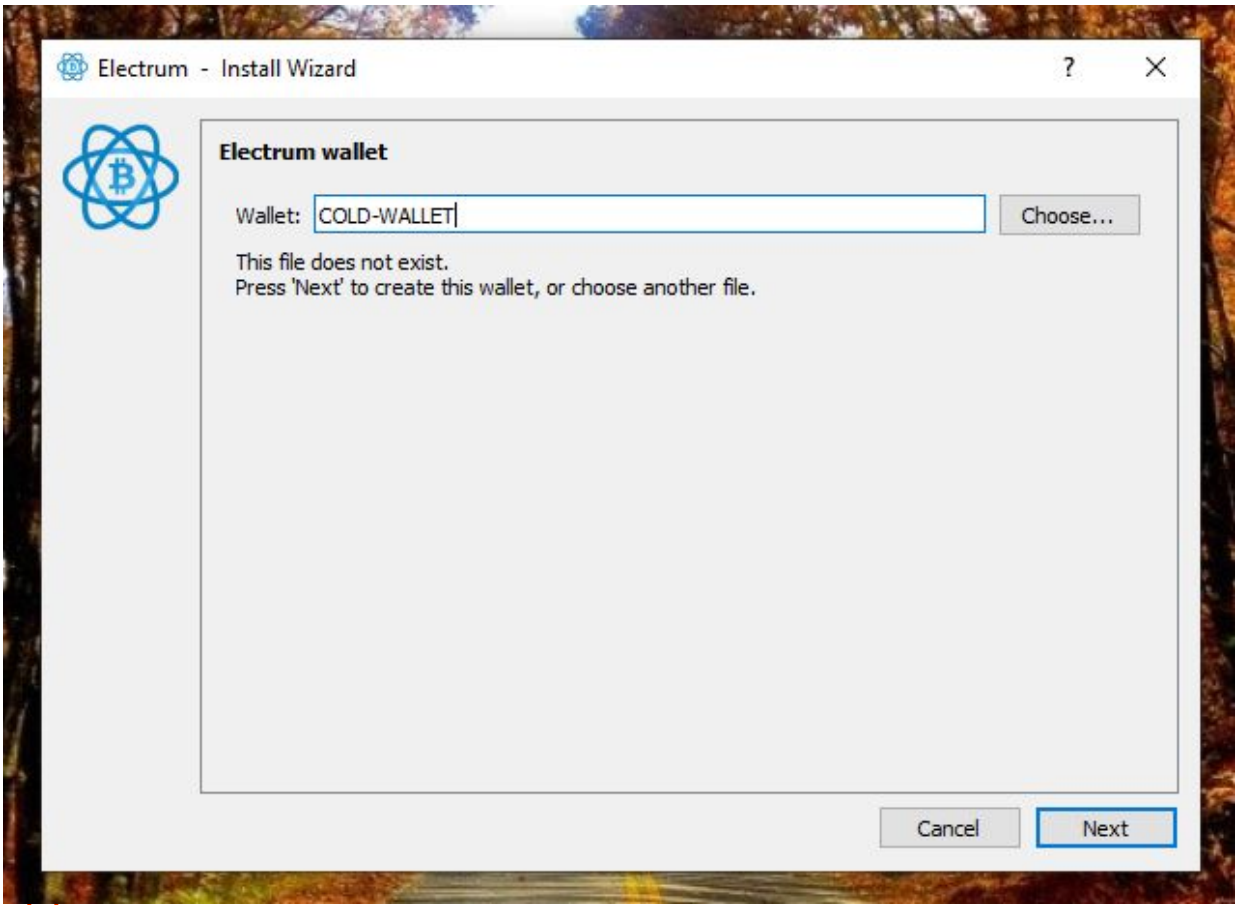


با تنظیمات پیش فرض نصب کنید

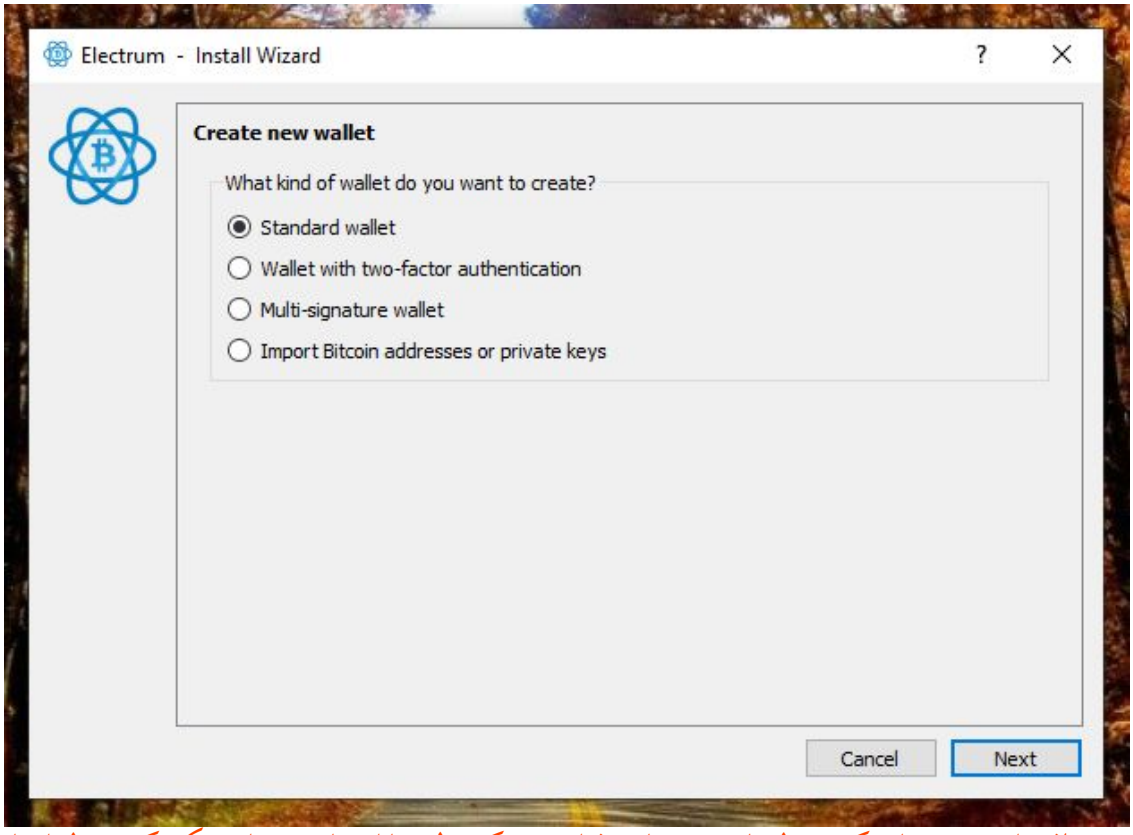




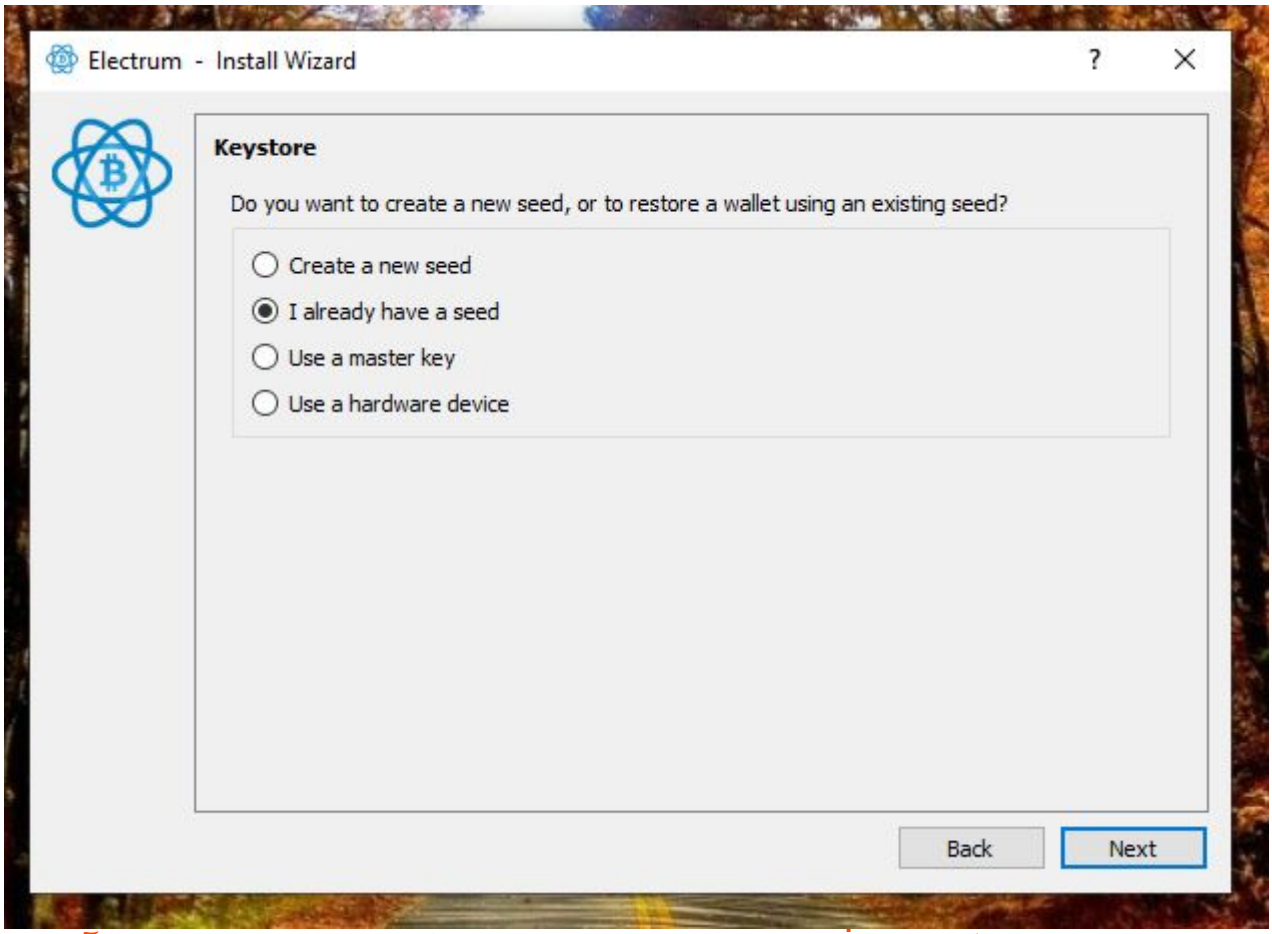
چون این سیستم آفلاینه این انتخاب اهمیتی نداره. بذارید همون حالت پیش فرض بمونه.



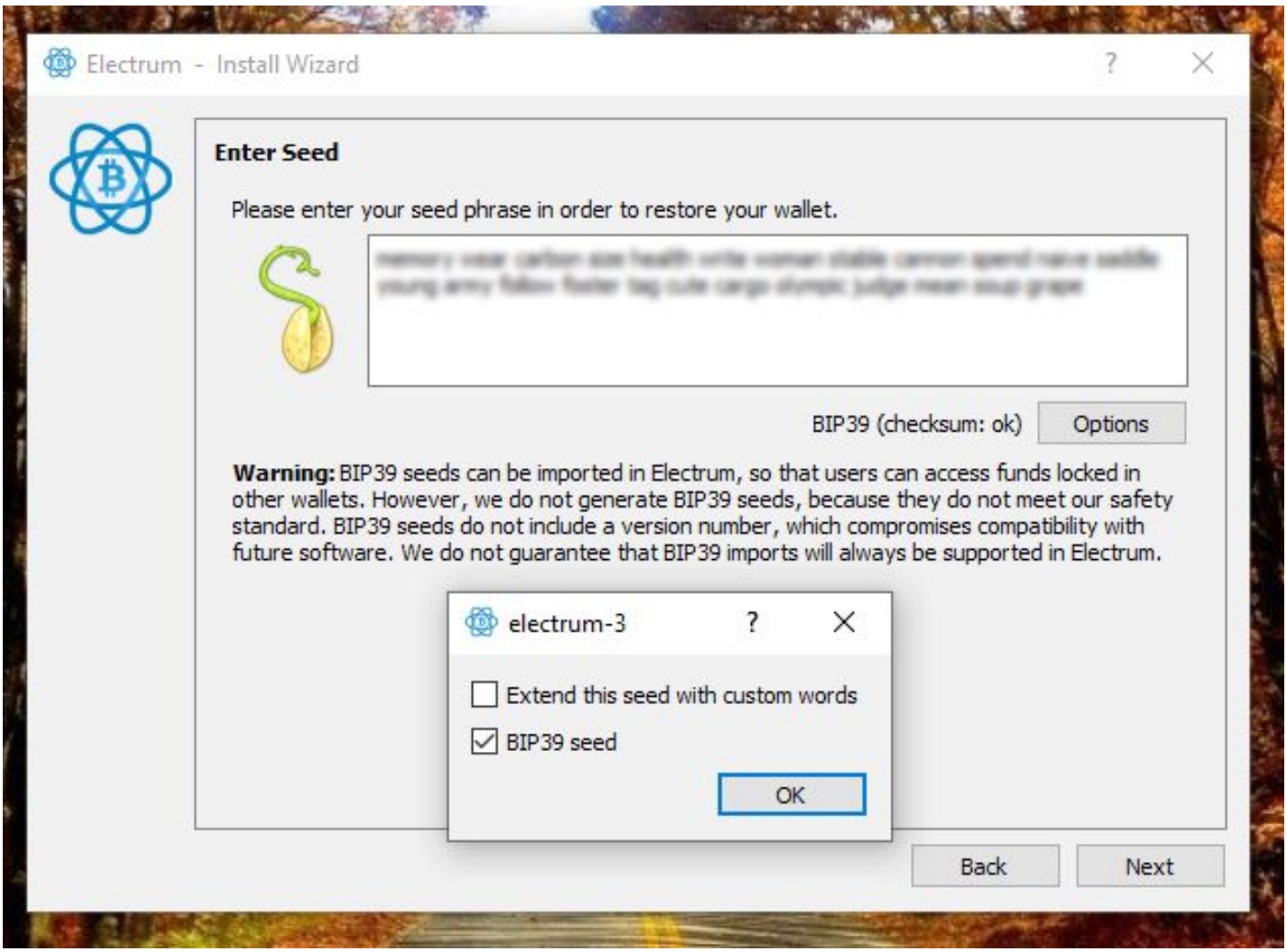
یه اسم بامعنی برای کیف پولتون بذارید. چون این روی سیستم آفلاین داره ساخته میشه بهتره کلمه cold رو بهش اضافه کرد تا از روی اسمش معلوم بشه.



الکترام انواع مختلفی از سرویسها و کیف‌پول‌ها رو پشتیبانی/فراهم می‌کنه ولی ما اینجا می‌خوایم یک کیف‌پول استاندارد بسازیم

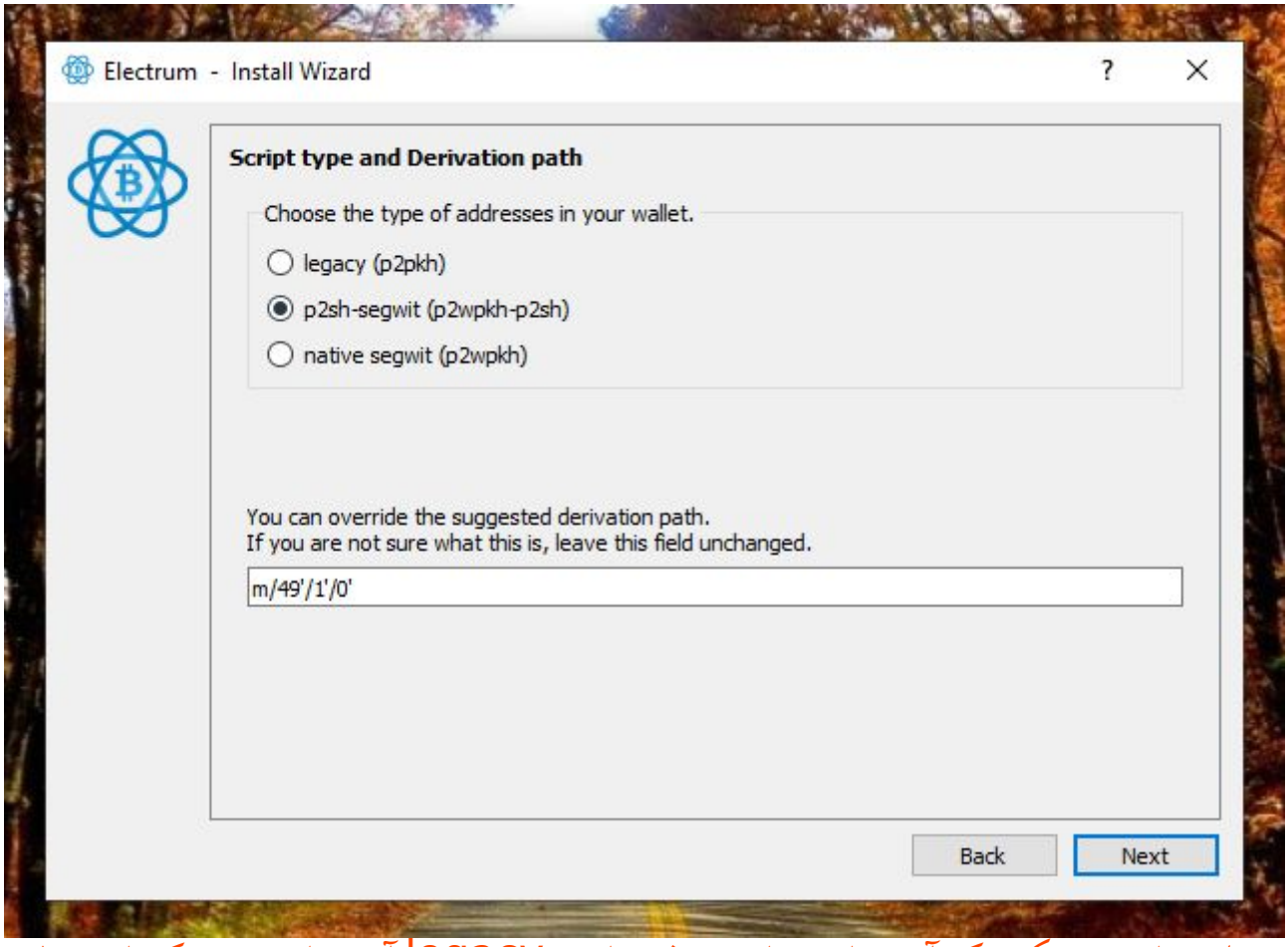


ما کلید خصوصی (یا همون کلمات mnemonic) رو ساختیم و حالا میخوایم توی این سیستم آفلاین اونها رو وارد کنیم. درواقع دلیل اصلی ساختن vm و آفلاین بودن اون اینه که کلید خصوصی بیت‌کوینمونو می‌خوایم داخلش نگهداری کنیم.

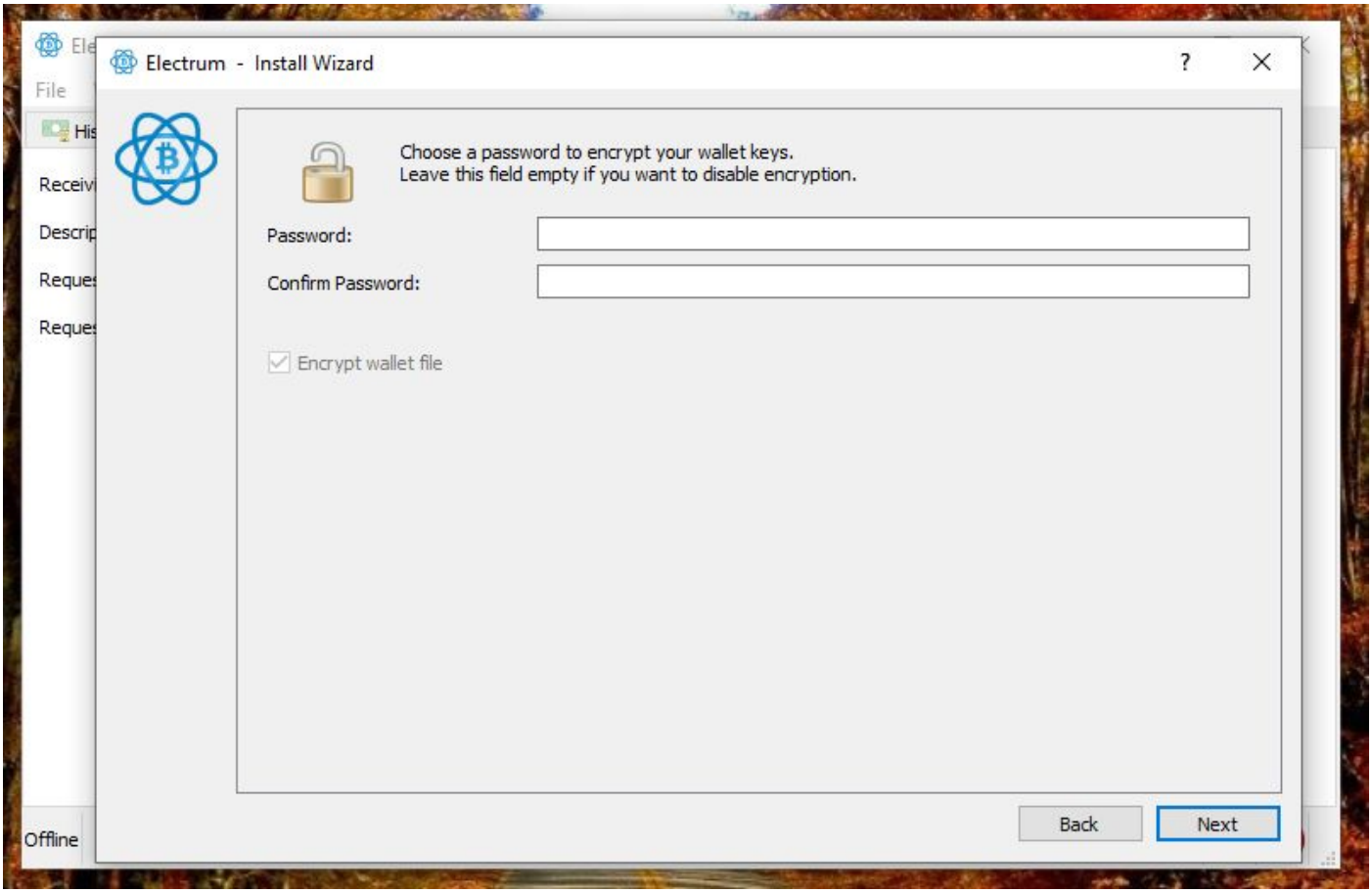


اینجا باید کلمات کلید خصوصی رو وارد کنید و می بینید که بهتون کمک می کنه وارد کنید. حالا اگر خیلی پارانویا دارید می‌تونید از onscreen keyboard ویندوز استفاده کنید. بعد از اینکه کلمات رو وارد کردید روی دکمه Options کلیک کنید و گزینه دوم: BIP۳۹ seed رو بزنید تا الکترام بفهمه شما براساس اون استاندارد کلید خصوصیتونو وارد کردید. درنهایت باید کنار اون دکمه عبارت BIP۳۹ checksum: ok رو ببینید.

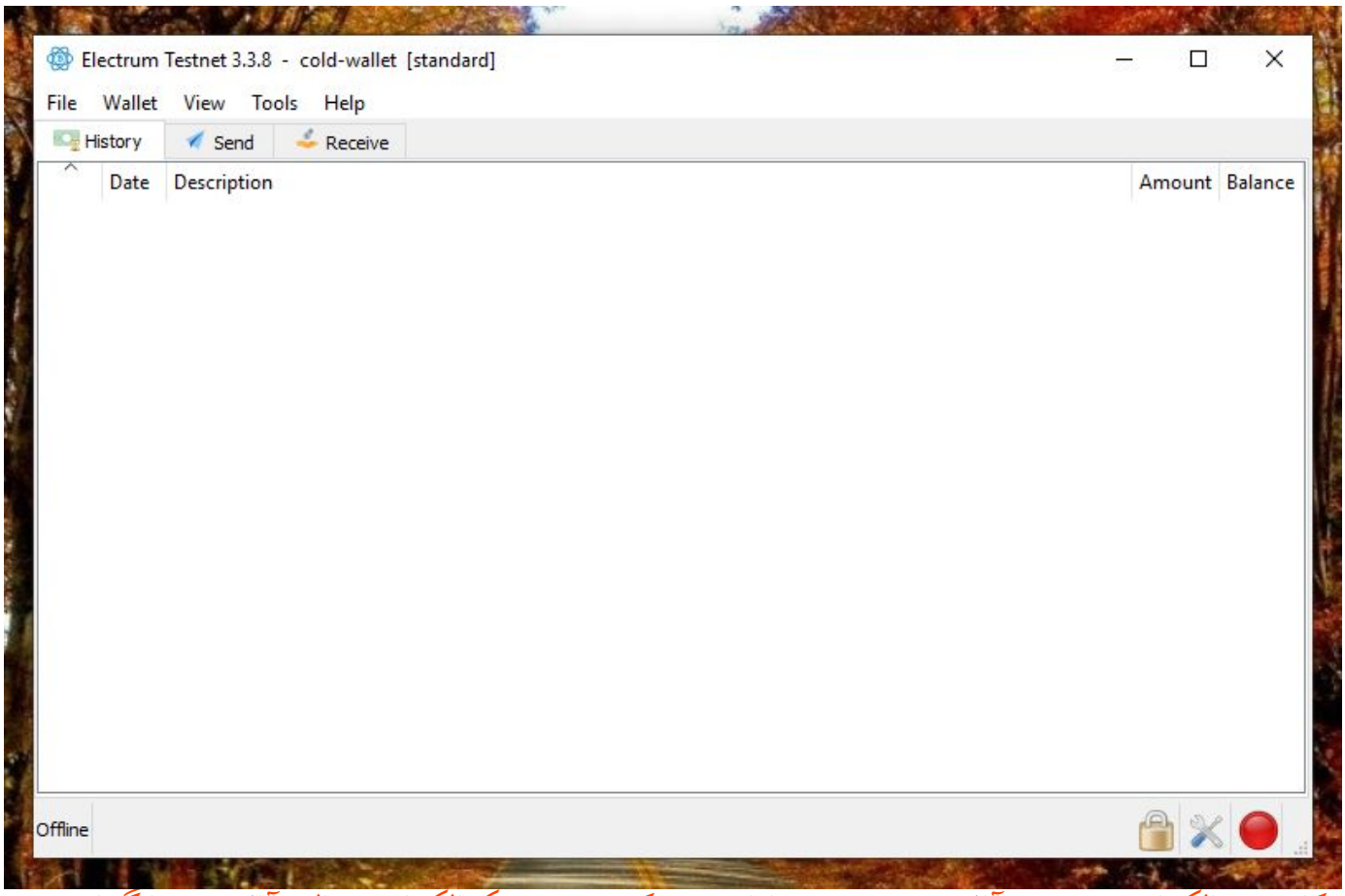
الکترام یک هشدار توی این صفحه به ما نشون می‌ده که باید بدونید چیه. الکترام به دلایلی که از حوصله اینجا خارجه به صورت پیش‌فرض کلمات mnemonic رو با استاندارد BIP۳۹ تولید نمی‌کنه. ولی از راه دکمه Options از اونها پشتیبانی می‌کنه. اگر یک روزی الکترام از استاندارد BIP۳۹ پشتیبانی نکرد باید از کیف‌پول‌هایی که از این استاندارد پشتیبانی می‌کنن استفاده کرد و بهیچوجه مشکلی پیش نخواهد اومد. بخاطر نفوذ و گسترش استاندارد BIP۳۹ به احتمال خیلی زیاد کیف‌پول الکترام به این پشتیبانی ادامه خواهد داد.



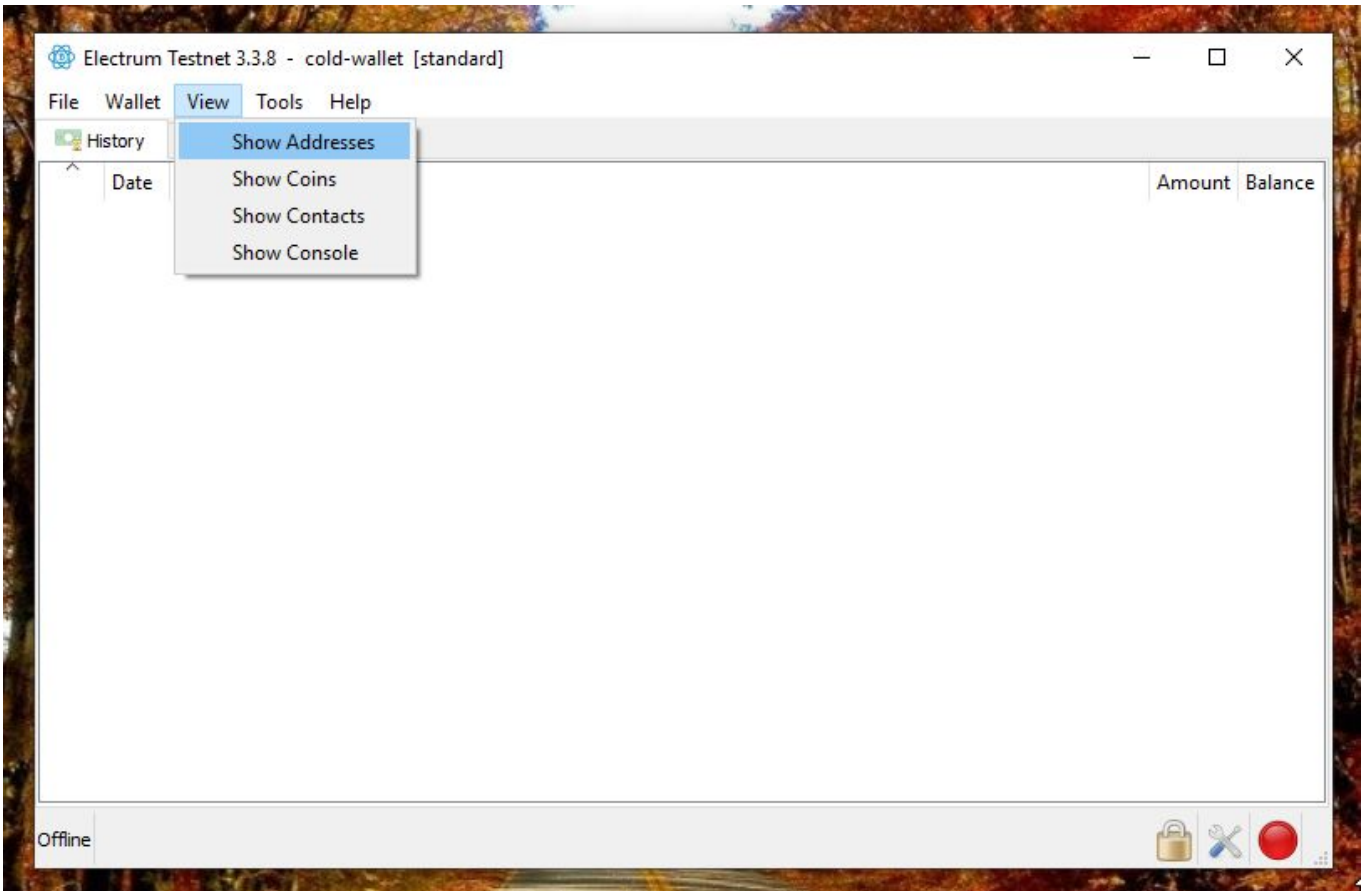
این مرحله شما تعیین میکنید که آدرسهای شما چه ورژنی باشن. legacy آدرسهایی هستن که با عدد ۱ شروع میشن. p۲sh-segwit آدرسهایی هستن که با سگویت سازگاری دارن و با عدد ۳ شروع میشن. native segwit هم آدرسهایی هستن که فول سگویت هستن و با bc۱ شروع میشن. پیشنهاد میشه مورد دوم انتخاب بشه چون بعضی از صرافیها هنوز از سومی پشتیبانی نمیکنن.



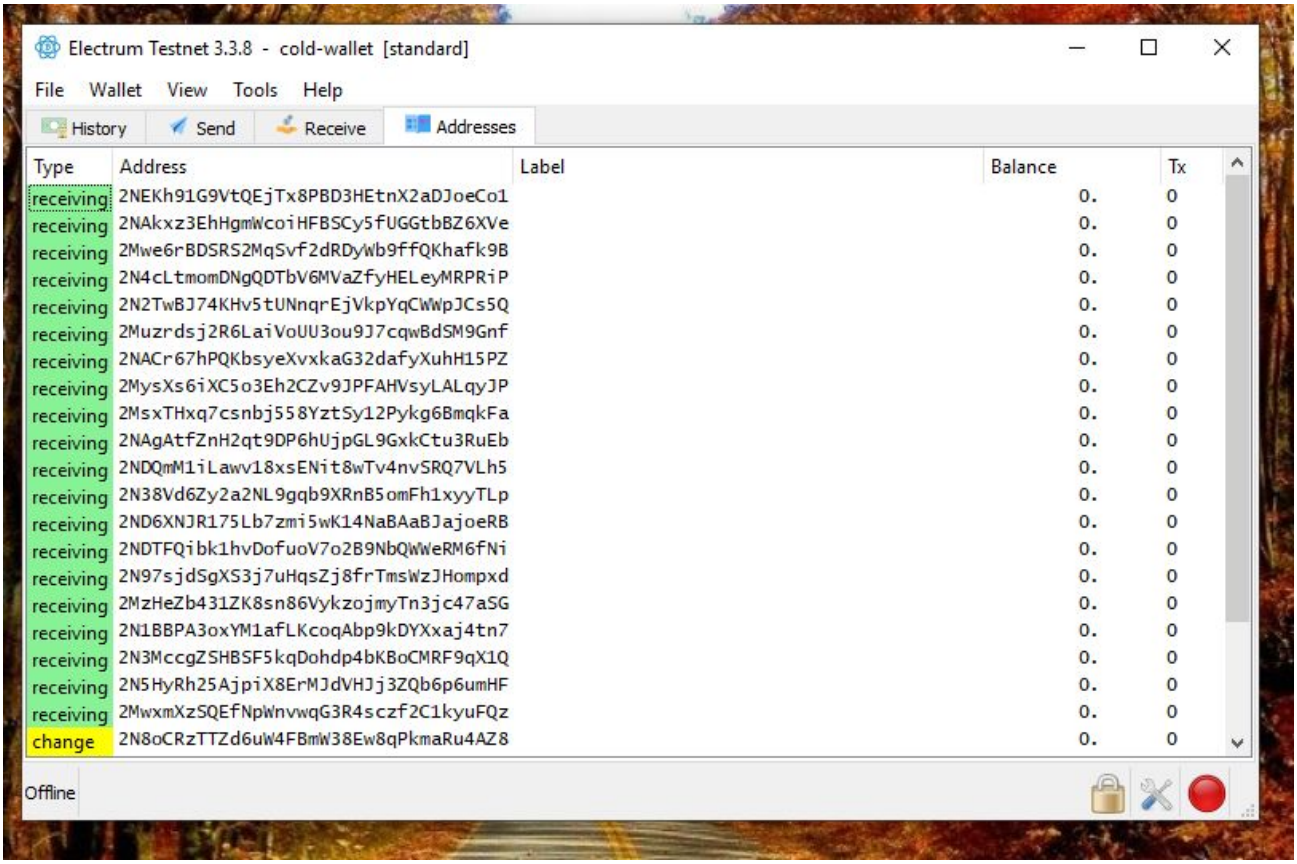
این پسورد ربطی به کلید خصوصی بیت‌کوین شما نداره ولی مهمه. الکترام با این پسورد فایل کیف‌پول شما رو رمزگذاری میکنه. اگر پسورد نگذارید هرکس به vm شما دسترسی داشته باشه می‌تونه به کلید خصوصی شما برسه و بیت‌کوینهاتون رو حتما از دست میدید. اما اگر این پسورد رو فراموش کنید اتفاقی نمیفته چون فقط کافیه یک کیف پول دیگه بسازید و اطلاعات کلید خصوصی و موارد دیگه ای که بالاتر دیدید رو وارد کنید و یک کیف پول جدید بسازید.



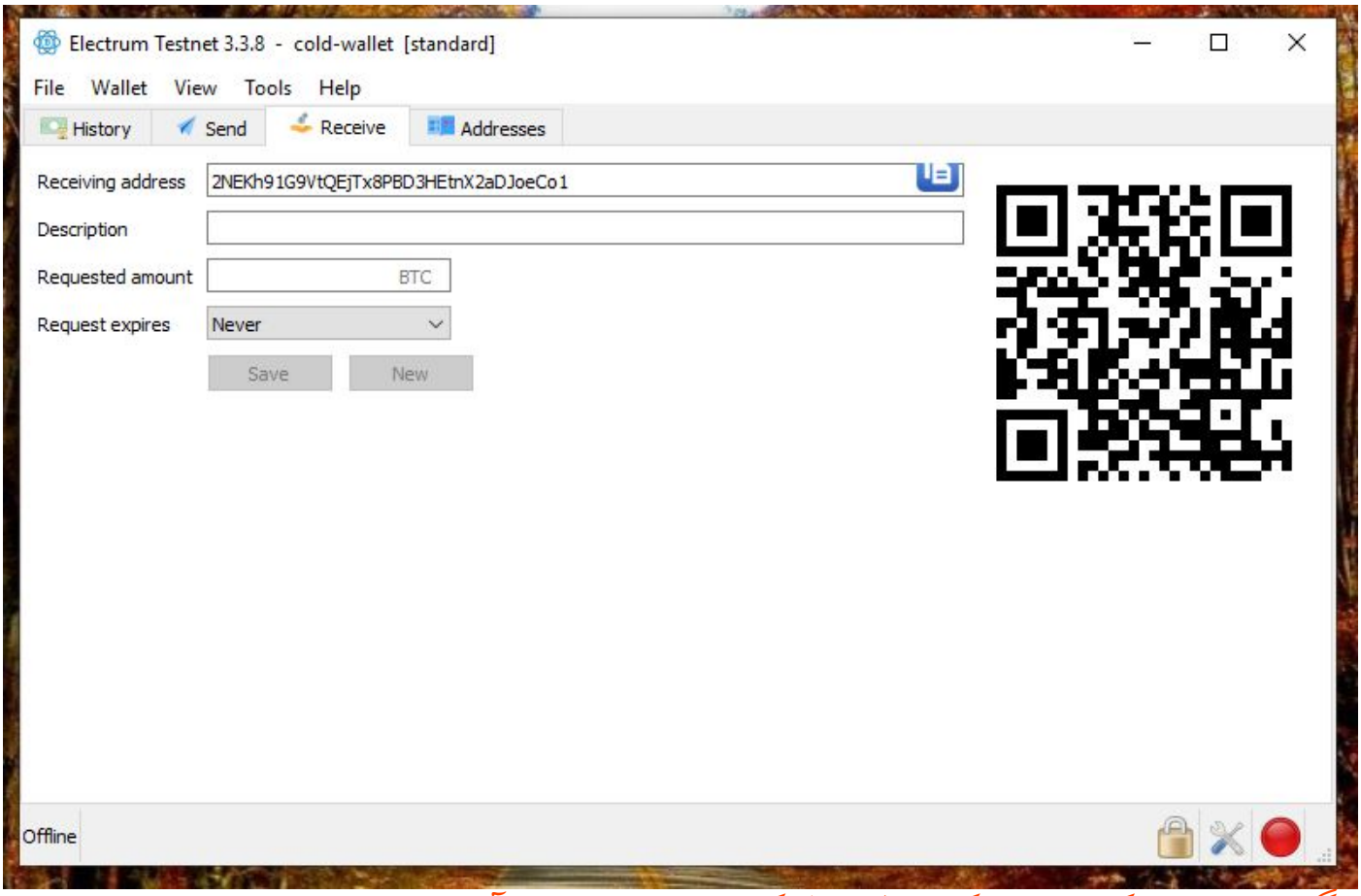
کار نصب الکترام روی سیستم آفلاین تموم شد. حتما باید ببینید که وضعیت شبکه الکترام در حالت آفلاینه و نشانگر قرمز رو پایین صفحه ببینید.



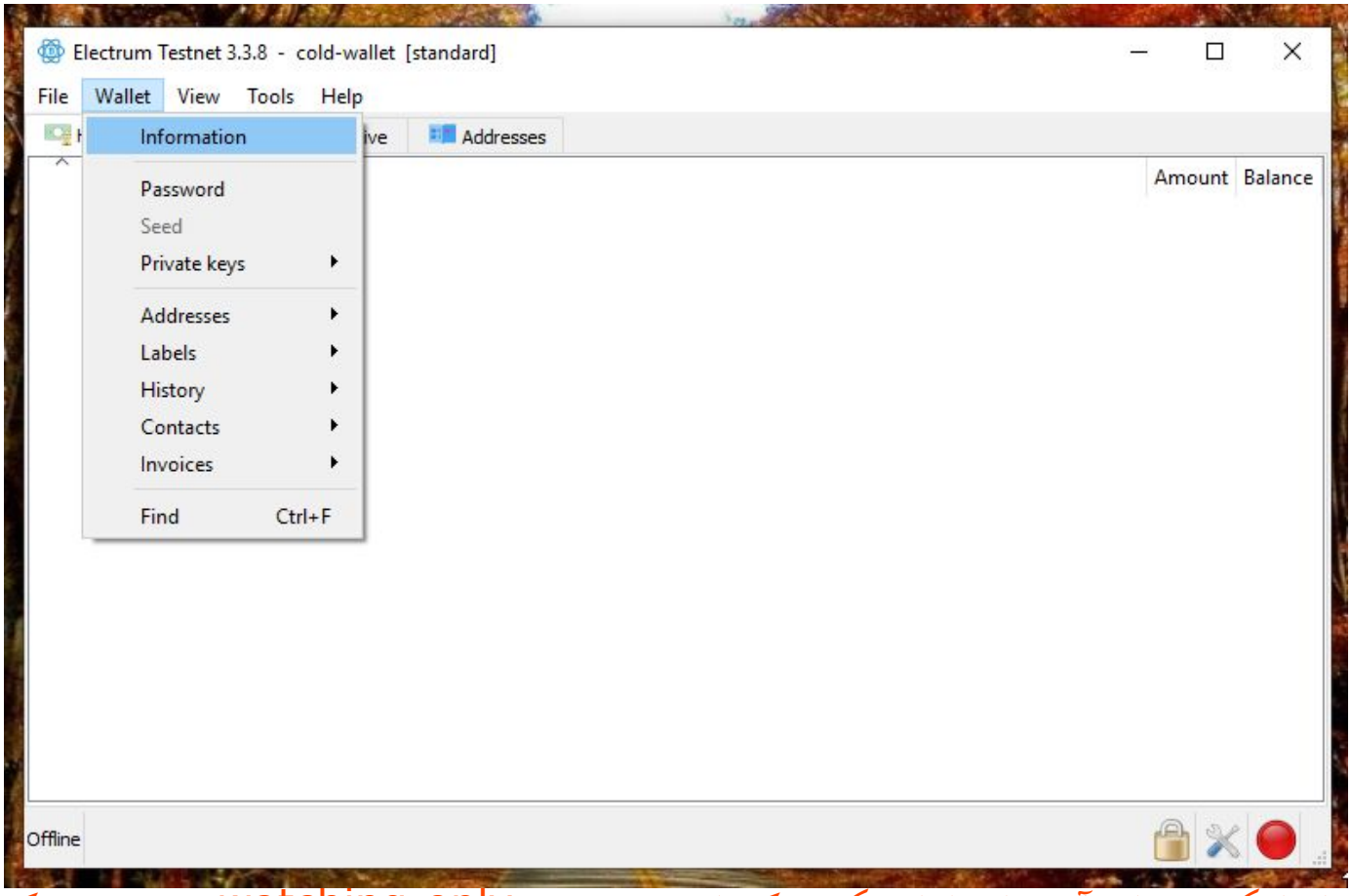
برای دیدن آدرسهای کیف پول منوی show addresses رو بزنید. دیدن آدرسها کمک زیادی میکنه که مطمئن باشید کلید خصوصیتونو درست وارد کردید.



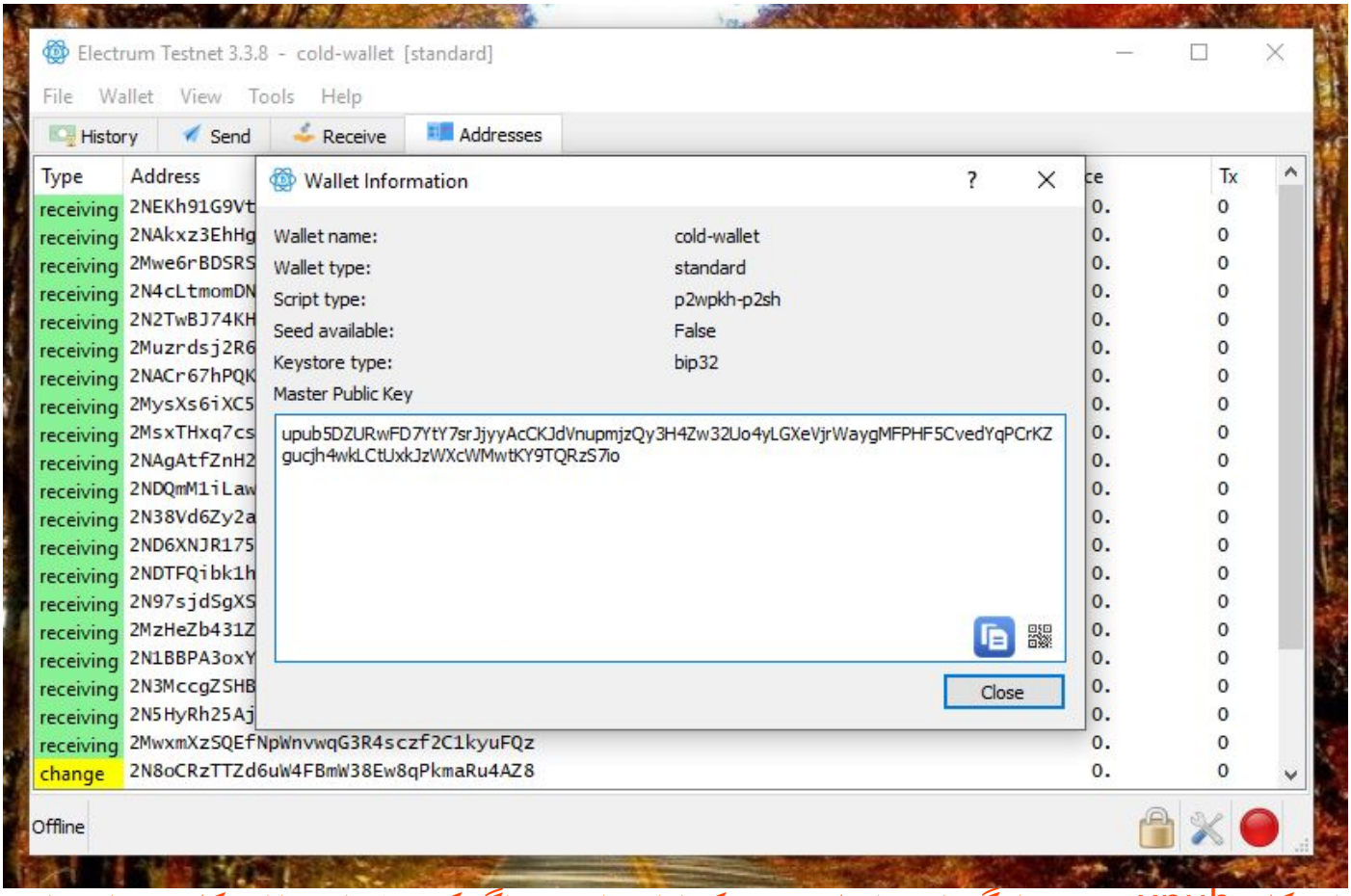
لیست ۲۰-۲۵ آدرس اولتونو میتونید اینجا ببینید. این آدرسها اینجا کاربردی ندارن چون این کیف پول شما فقط برای sign کردن تراکنشها استفاده میشه ولی همونطور که بالا گفته شد آدرسها کمک میکنن شما مطمئن بشید کیف پول درستی رو باز کردید.



اگر خواستید بیت‌کوین به این کیف‌پول منتقل کنید می‌تونید از همون آدرس ها بردارید یا به این صفحه بیاید و آدرسی که بهتون میده رو استفاده کنید.

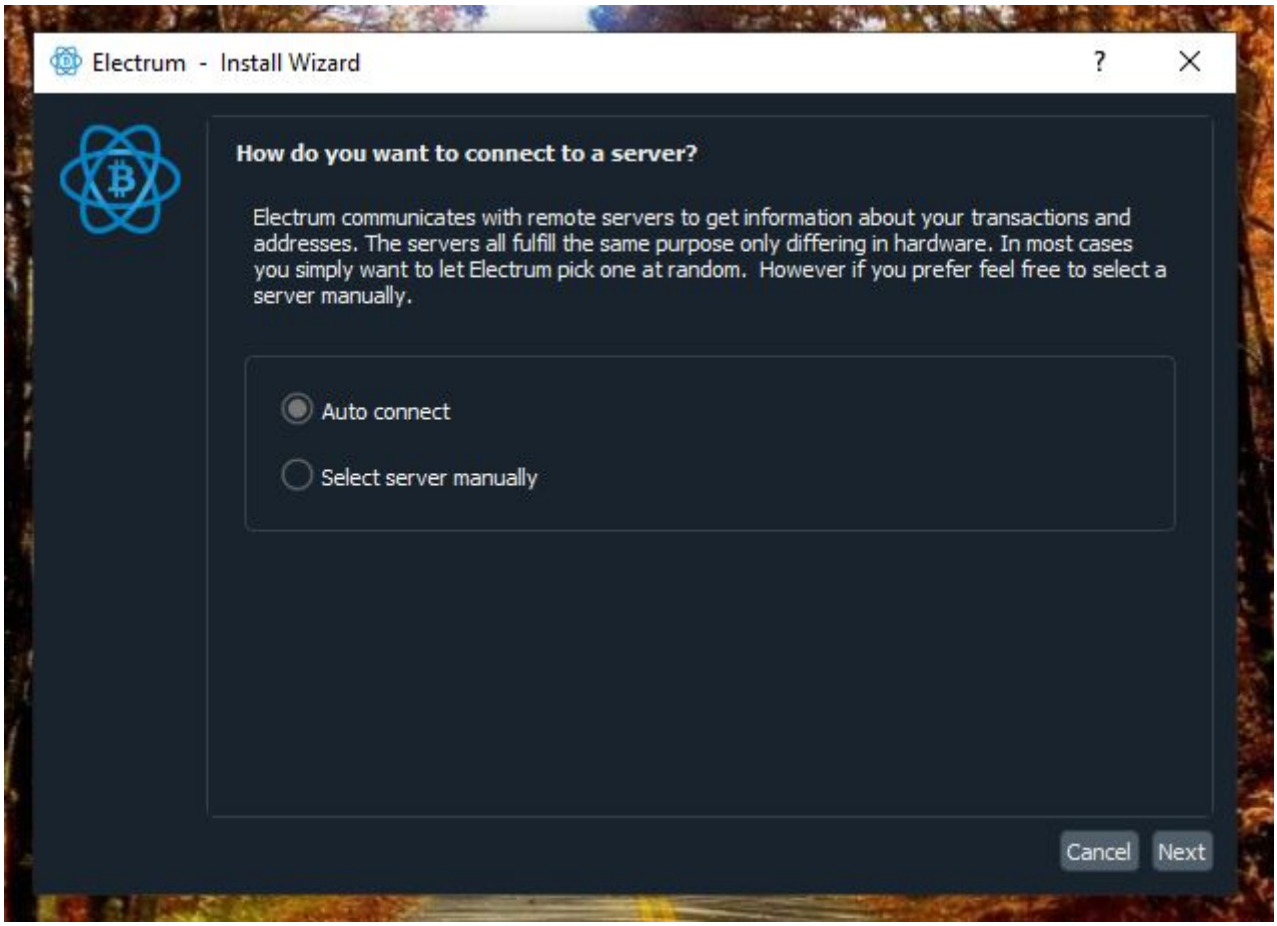


برای اینکه بتونیم این آدرسها و مقدار بیتکوینی که داریم رو بصورت watching-only روی سیستمی که به اینترنت وصله ببینیم باید یک کلید عمومی از کیف پولمون داشته باشیم که بتونه آدرسهای ما رو تولید کنه. این کلید عمومی نمیتونه تراکنشهای خرج کردن یا ارسال بیتکوین ما رو sign کنه پس میتونیم با خیال راحت اون رو توی الکترامی که به اینترنت دسترسی داره وارد کنیم.



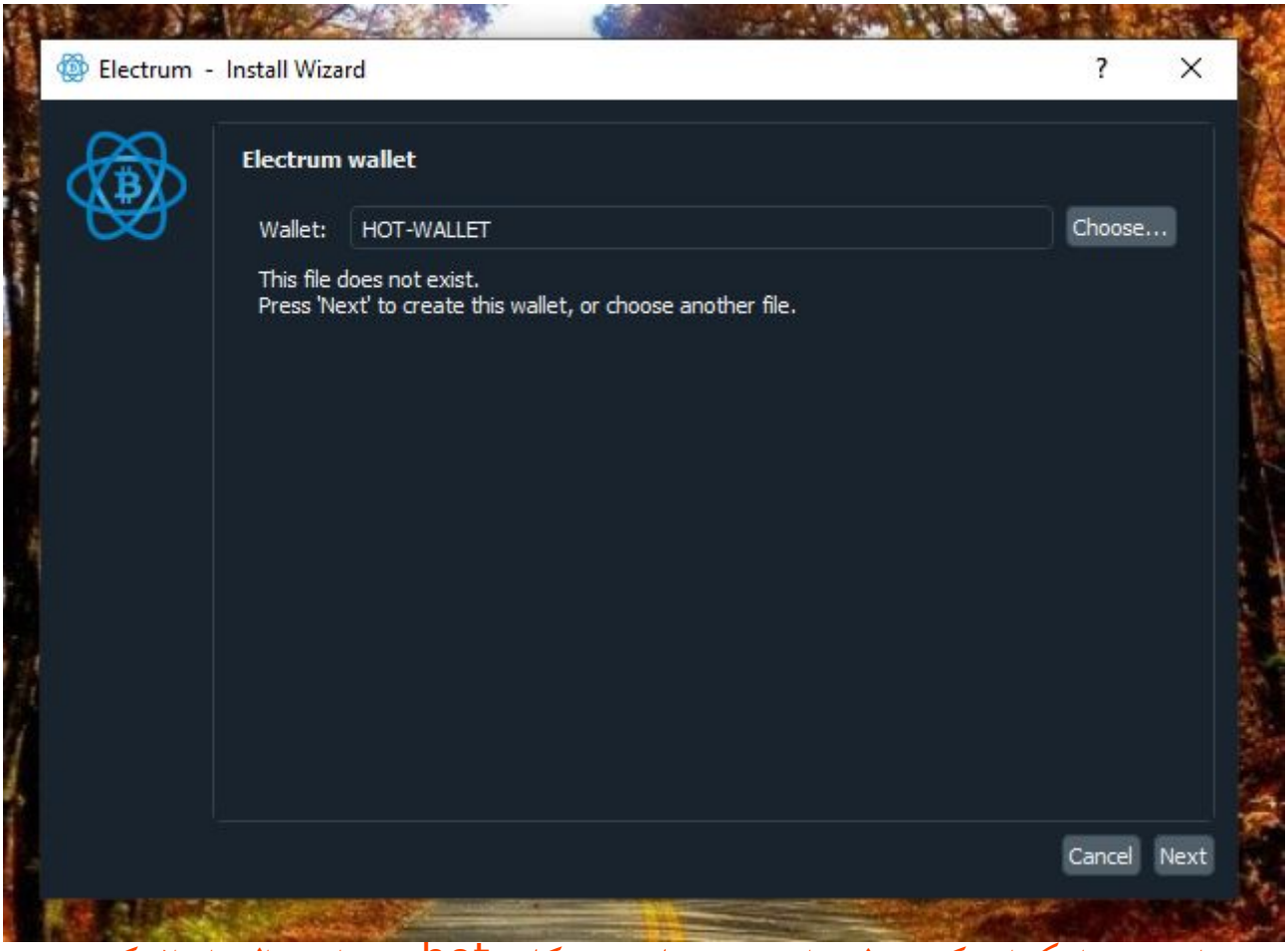
این کلید xpub رو همینجا نگه دارید تا جلوتر ببینیم کجا باید وارد بشه. اگر کسی غیر از شما این کلید رو داشته باشه نمیتونه بیت کوینهای شما رو خرج کنه ولی میتونه ببینه شما چقدر توی این کیف‌پول‌تون بیت‌کوین دارید.

نصب الکترام روی سیستم متصل به اینترنت:

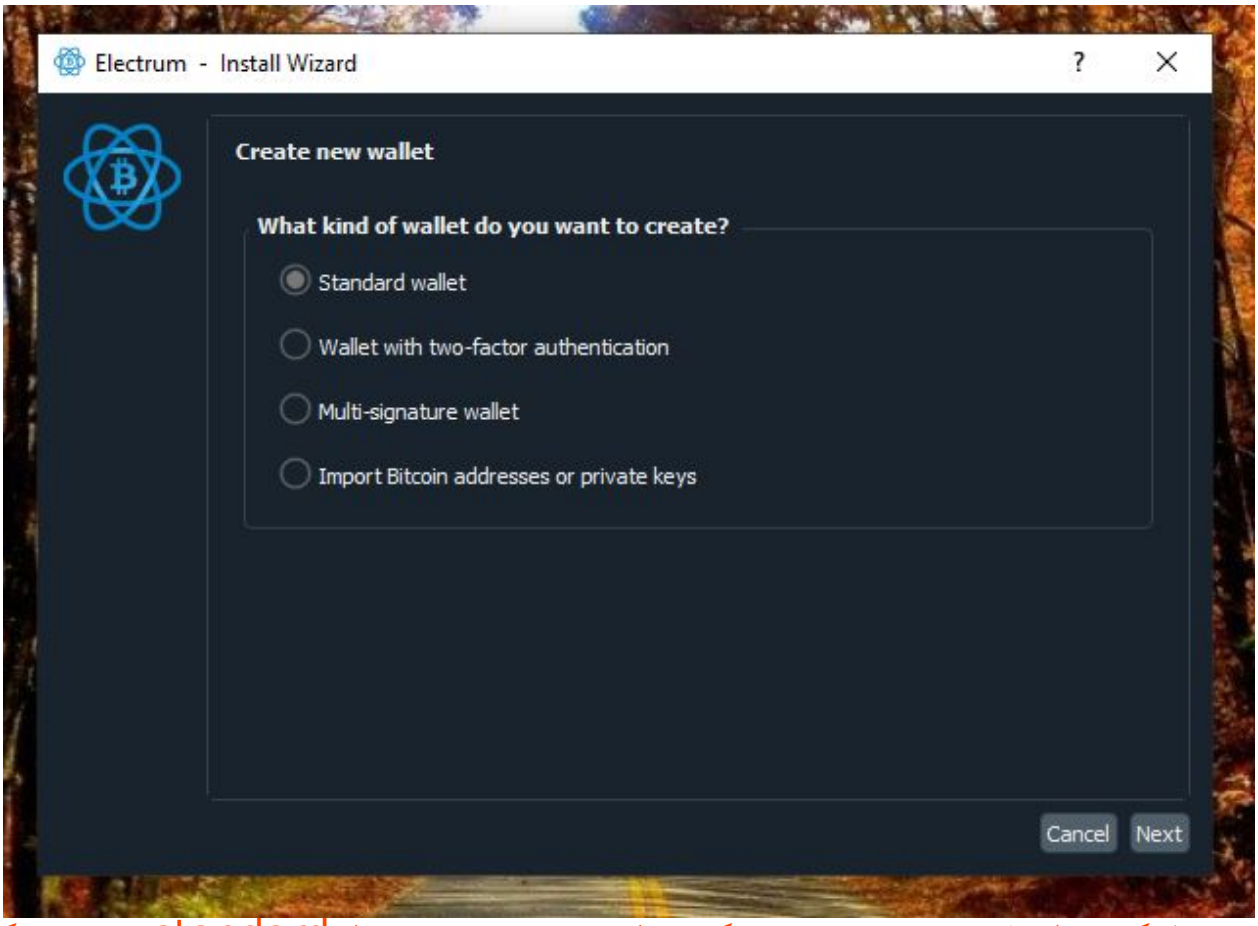


همونطور که روی سیستم آفلاین نصب کردید اینجا هم نصبش کنید و بازش کنید
اینجا از شما می‌پرسه که میخواید به سرور خودتون وصل بشید یا به
سرورهای عمومی الکترام. این موضوع بعدا از نظر پرایوسی مهم میشه ولی
الان حالت auto connect رو انتخاب کنید

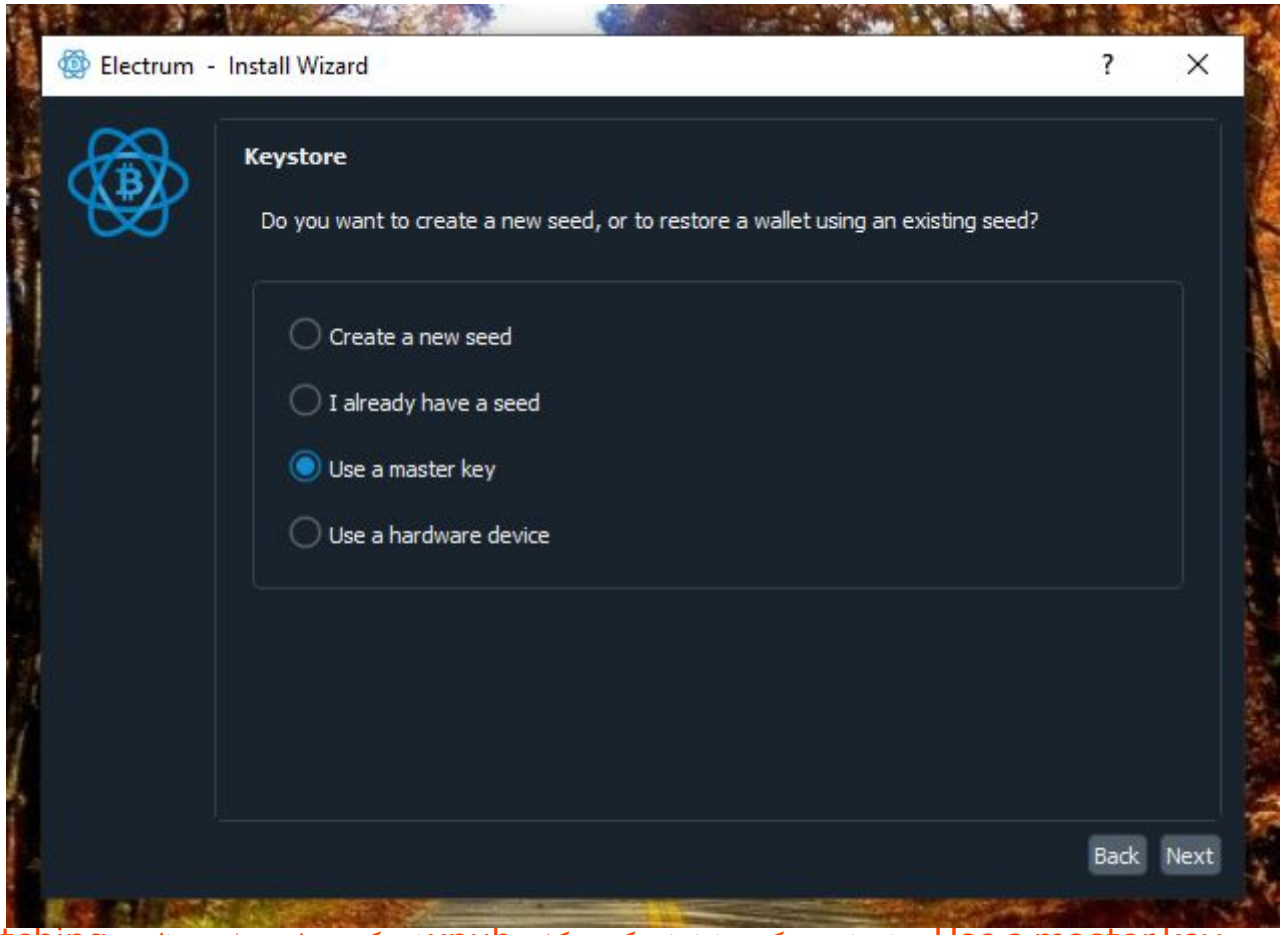
تم دارک رو بعد از تمام شدن نصب می تونید توی تنظیمات فعال کنید



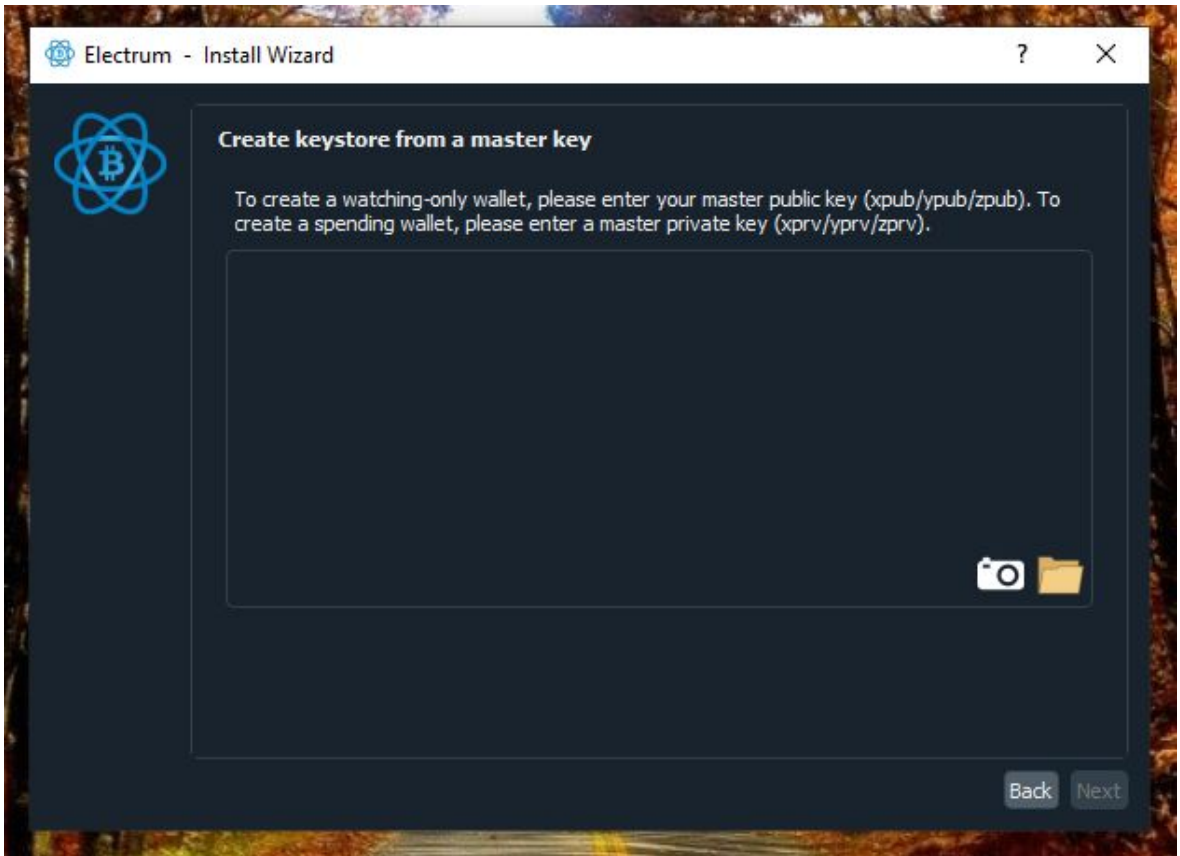
با توجه به اینکه این کیف‌پول به اینترنت وصله، میشه کلمه hot رو به اسم والت اضافه کرد.



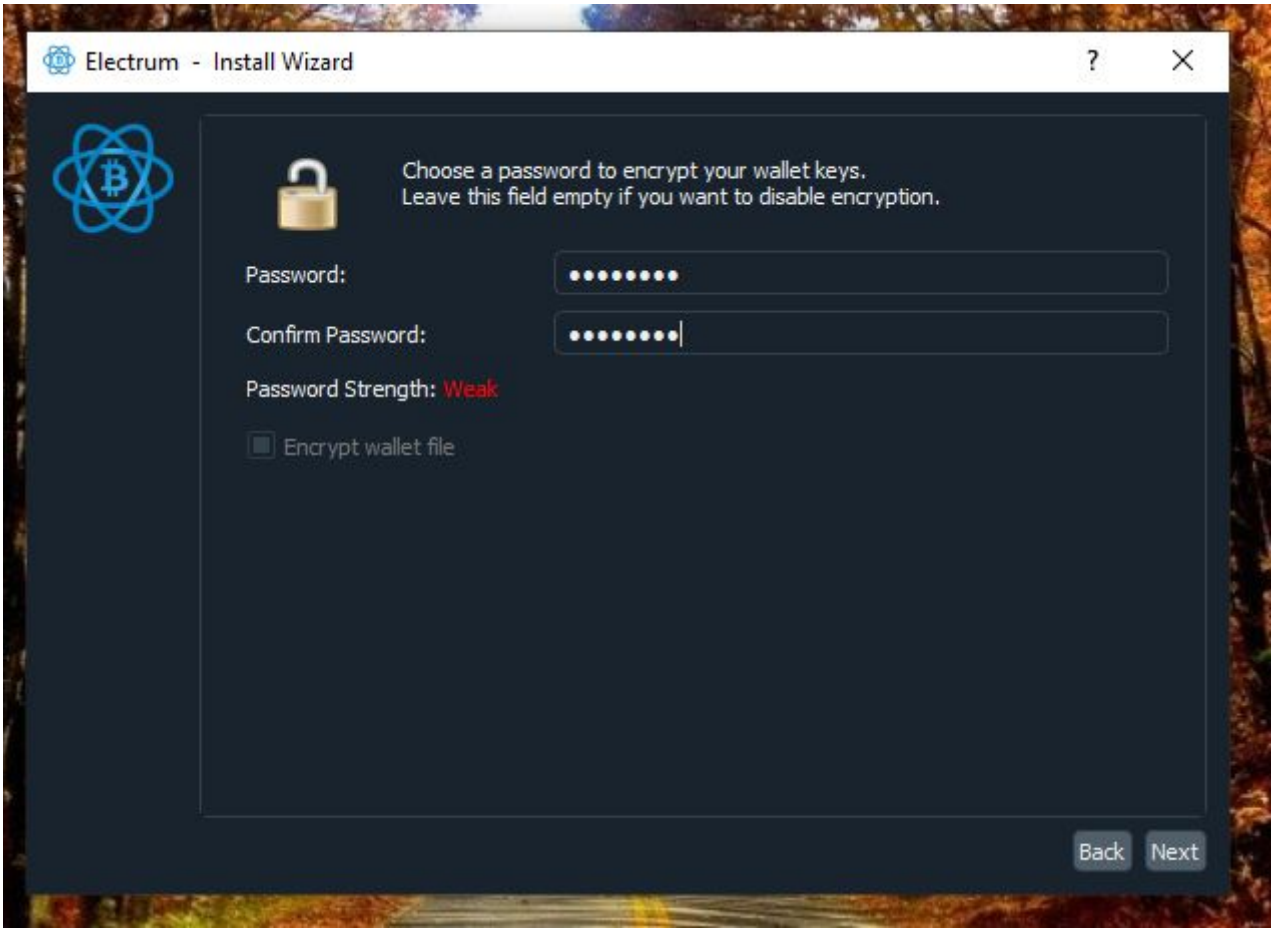
اینجا هم مثل کیف‌پول قبلی می‌پرسه چه نوعی از کیف‌پول می‌خوایم بسازیم و مدل standard رو انتخاب کنید.



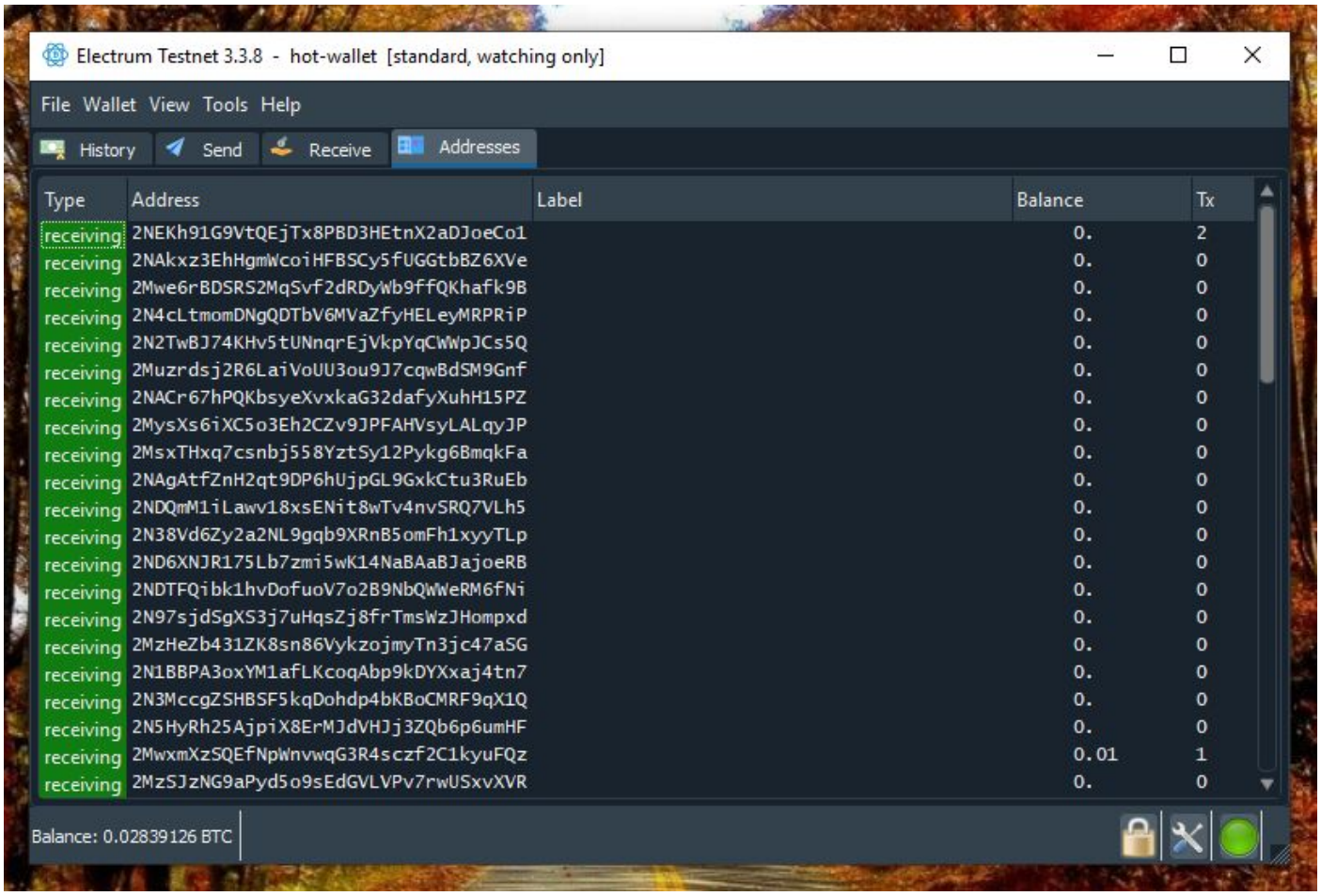
اینجا مورد Use a master key رو انتخاب می‌کنیم تا با وارد کردن کلید xpub این کیف‌پول تبدیل به حالت watching-only بشه. یعنی نتونه تراکنش های ارسال بیت‌کوین ما رو sign کنه ولی بتونه آدرس ها مقداری که بیت‌کوین داریم رو به ما نشون بده.



کلید xpub که بالاتر وقتی داشتیم روی vm الکترام نصب می کردیم رو اینجا کپی کنید.

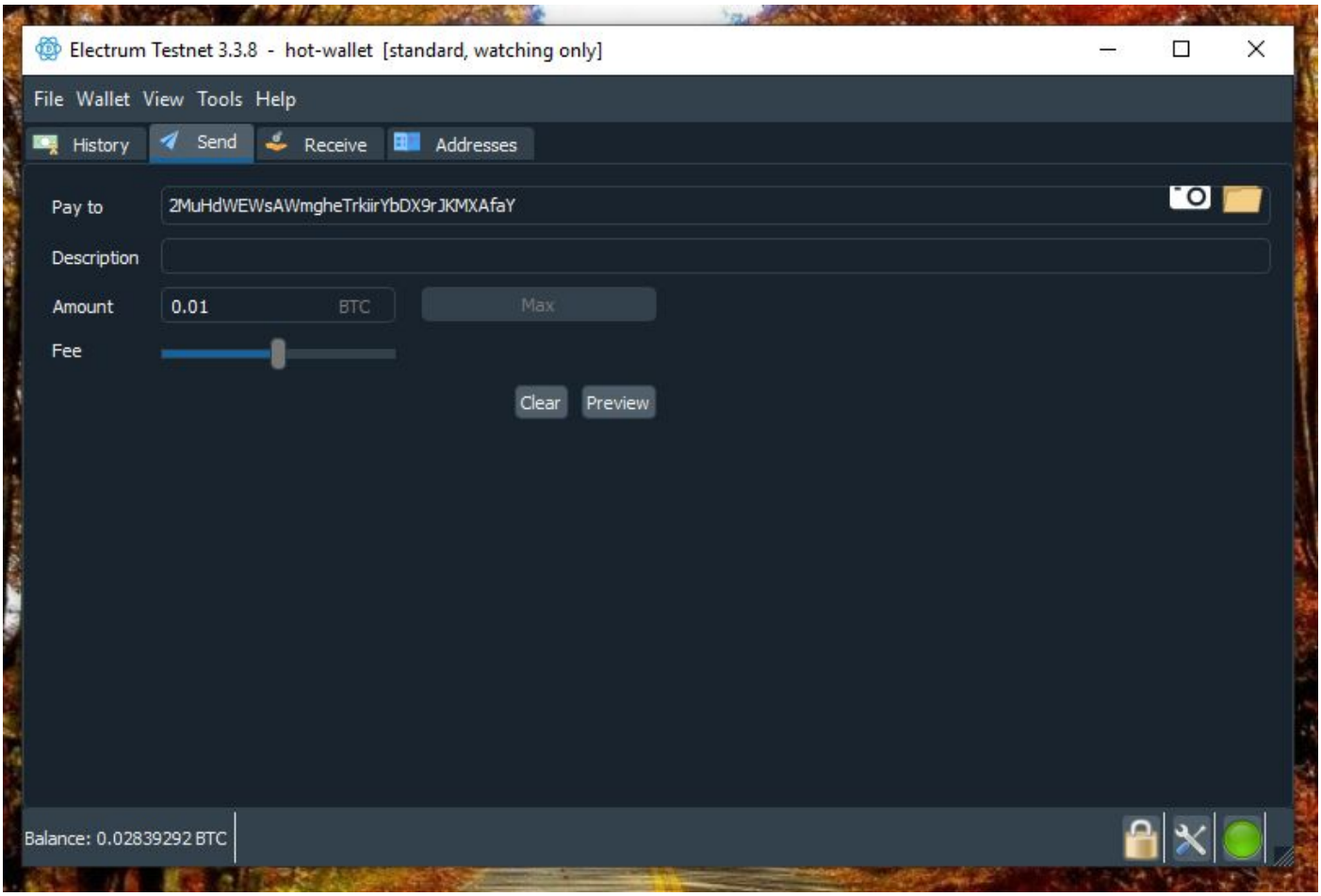


این پسورد ربطی به کلید خصوصی شما نداره. این یک پسوردیه که شما انتخاب می‌کنید تا الکترام فایل کیف‌پول شما رو با این پسورد رمزگذاری کنه. اگر پسورد نگذارید هرکس به کامپیوتر شما دسترسی داشته باشه میتونه xpub شما رو ببینه و از بیت‌کوین‌های شما سردربیاره ولی نمیتونه خرجشون کنه.

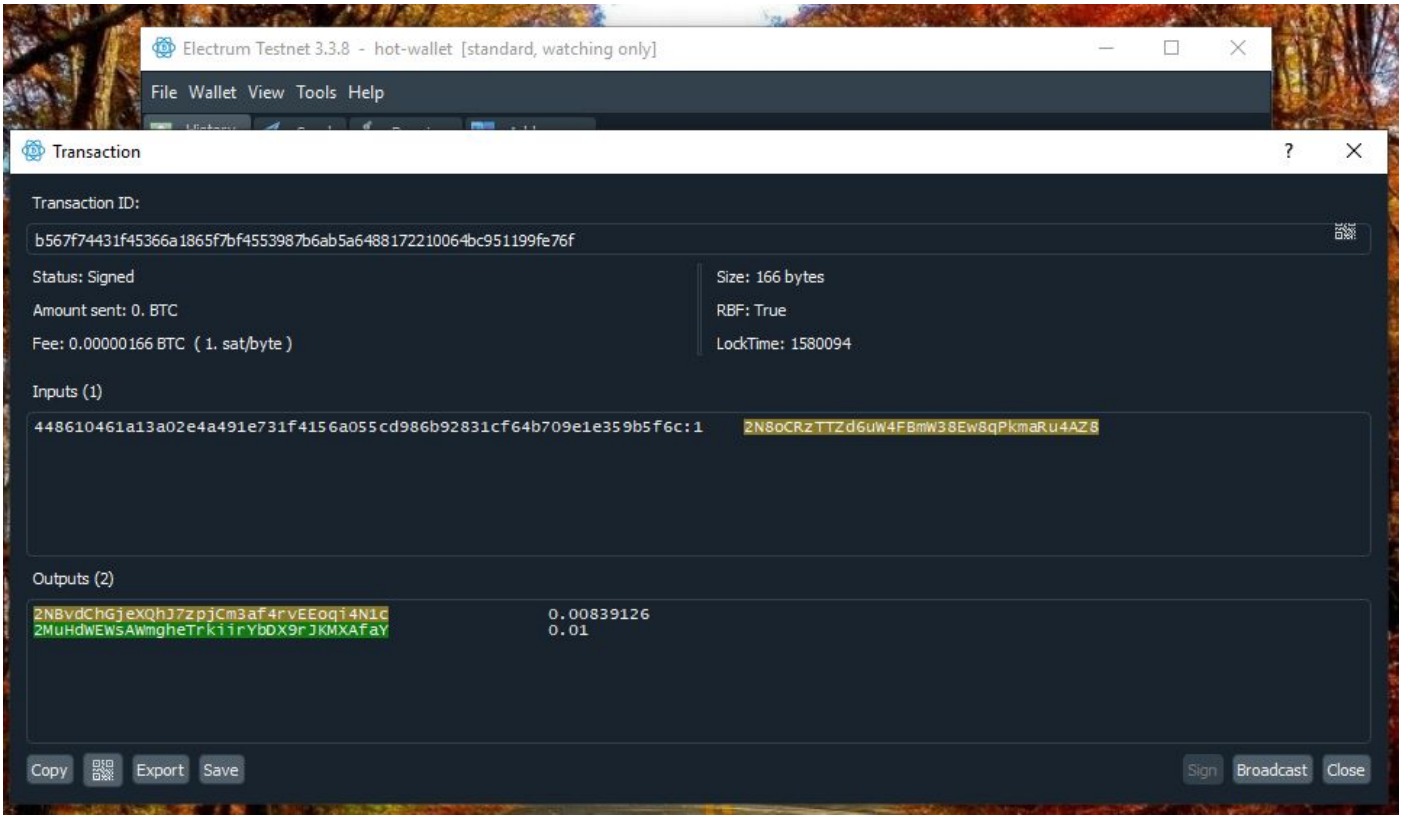


کیف پول آنلاین شما درست شده. حالا به بخش Addresses برید و باید مطمئن بشید که آدرسهایی که اینجا می‌بینید عینا با آدرسهایی که توی والت سیستم آفلاین می‌بینید باشه. این خیلی مهمه. دو-سه تا آدرس رو بصورت رندوم چک کنید و مطمئن بشید که آدرسها مطابقت دارن. برای واریز بیت‌کوین به این کیف‌پول قبلا صحبت شده، فقط کافیه یکی از این آدرسها رو به صرافی یا کسی بدید که براتون به اون آدرس ارسال کنه و بیاد توی کیف‌پولتون. دقت کنید اون بالا نوشته watching-only یعنی این کیف‌پول از کلید خصوصی شما اطلاعی نداره و فقط از موجودی بیت‌کوین و آدرسهای شما خبر داره.

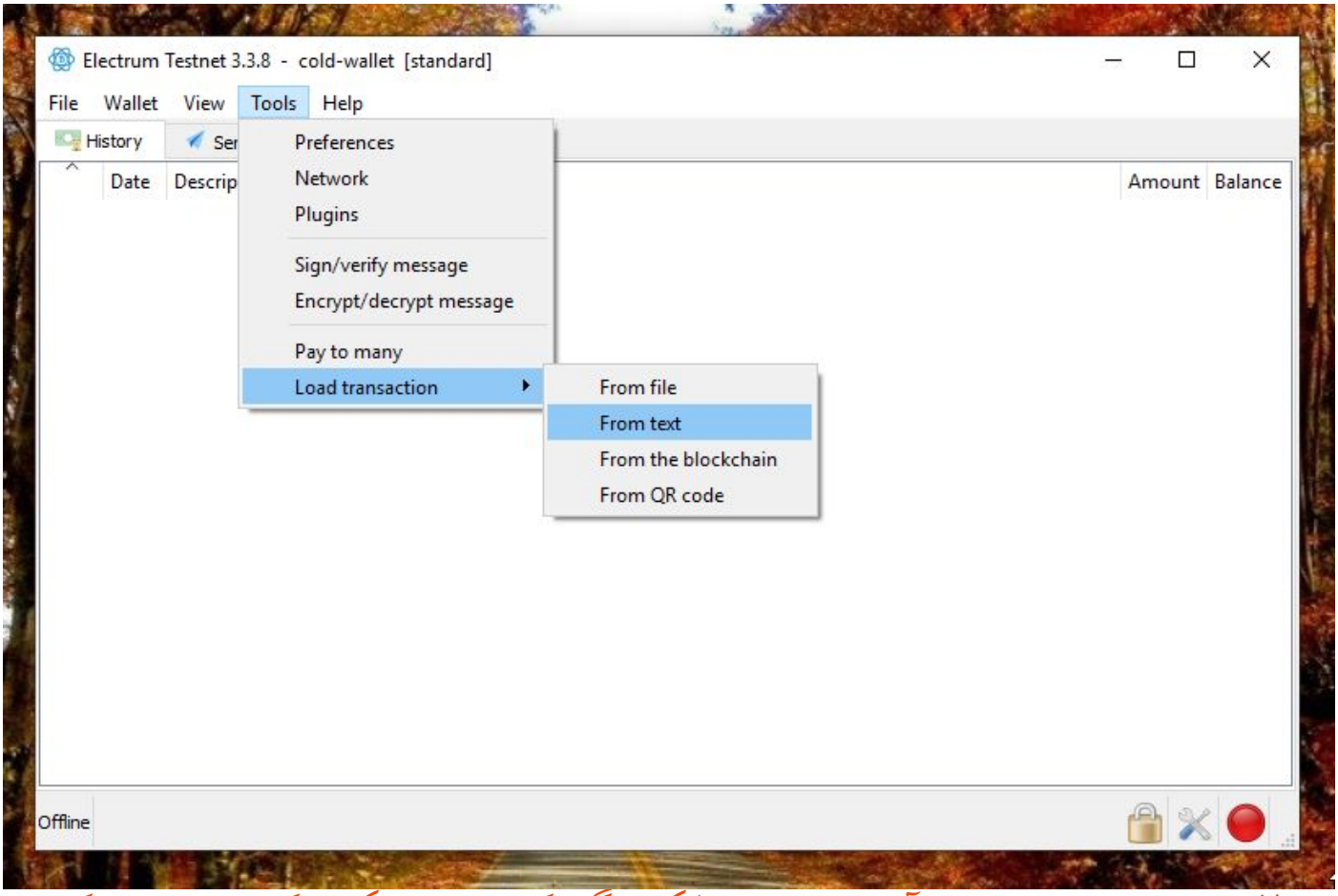
ارسال بیت کوین:



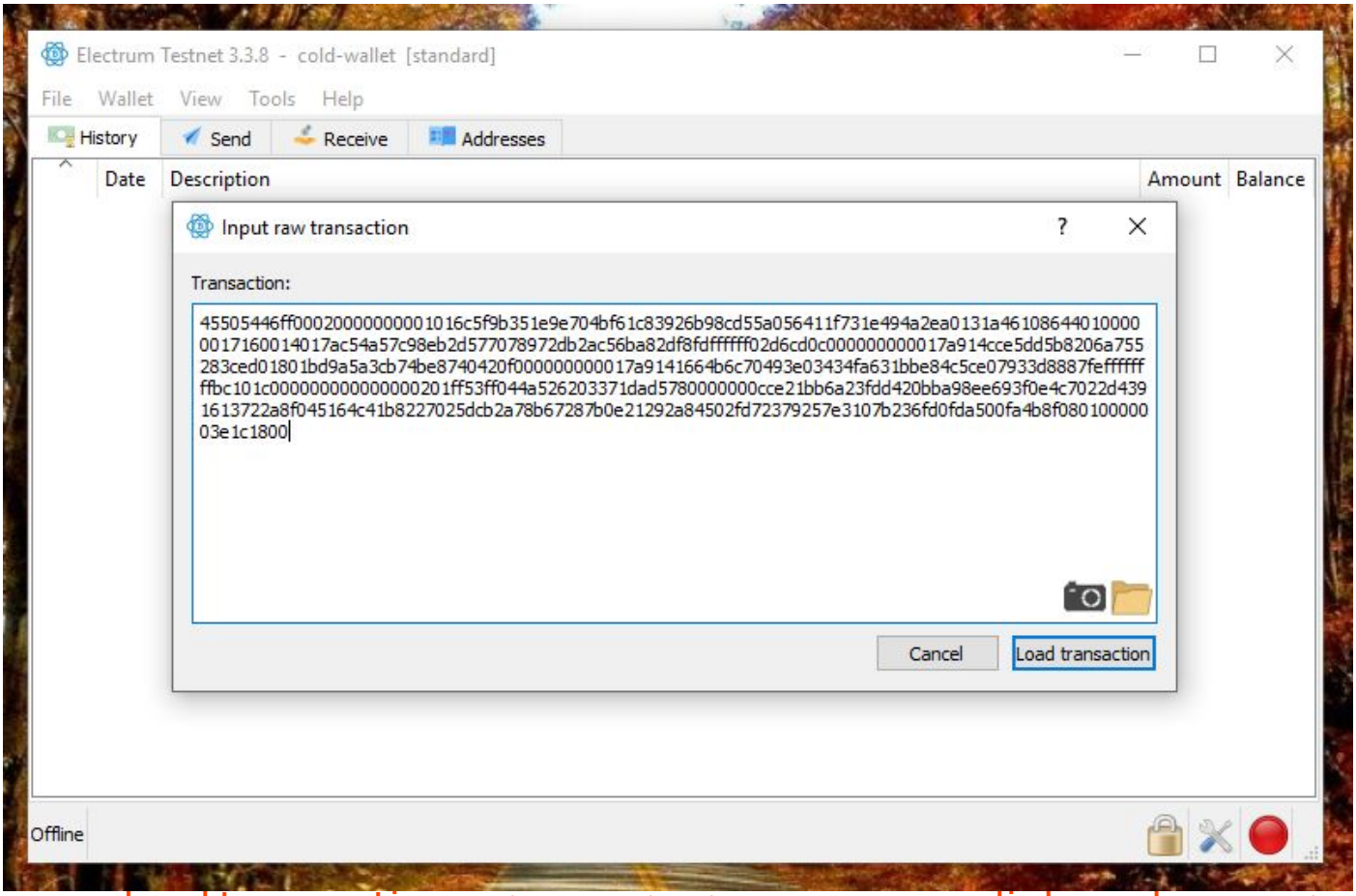
اگر بخواید بیت‌کوین از این کیف‌پول برای کسی ارسال کنید باید از الکترام سیستمی که به اینترنت وصله بخواید براتون یک تراکنش درست کنه. و از بیت‌کوین های شما به اندازه ای که شما می‌خواید به اون آدرس بفرسته. کیف پول الکترام شما با توجه به اطلاعاتی که از مقادیر بیت‌کوین شما و آدرسهای شما داره می‌تونه اینکار رو انجام بده. پس به قسمت send برید و آدرسی که می‌خواید براش بیت‌کوین ارسال کنید رو بزنید. تنها چیزی که می‌بینید فرق کرده اینه که دیگه شما گزینه send رو نمی‌بینید. چون این کیف‌پول شما کلید خصوصی نداره و بلد نیست تراکنش رو sign کنه. کاری که باید بکنیم اینه که باید تراکنش رو ببریم به سیستم vm که آفلاینه و اونجا تراکنش رو sign کنیم.



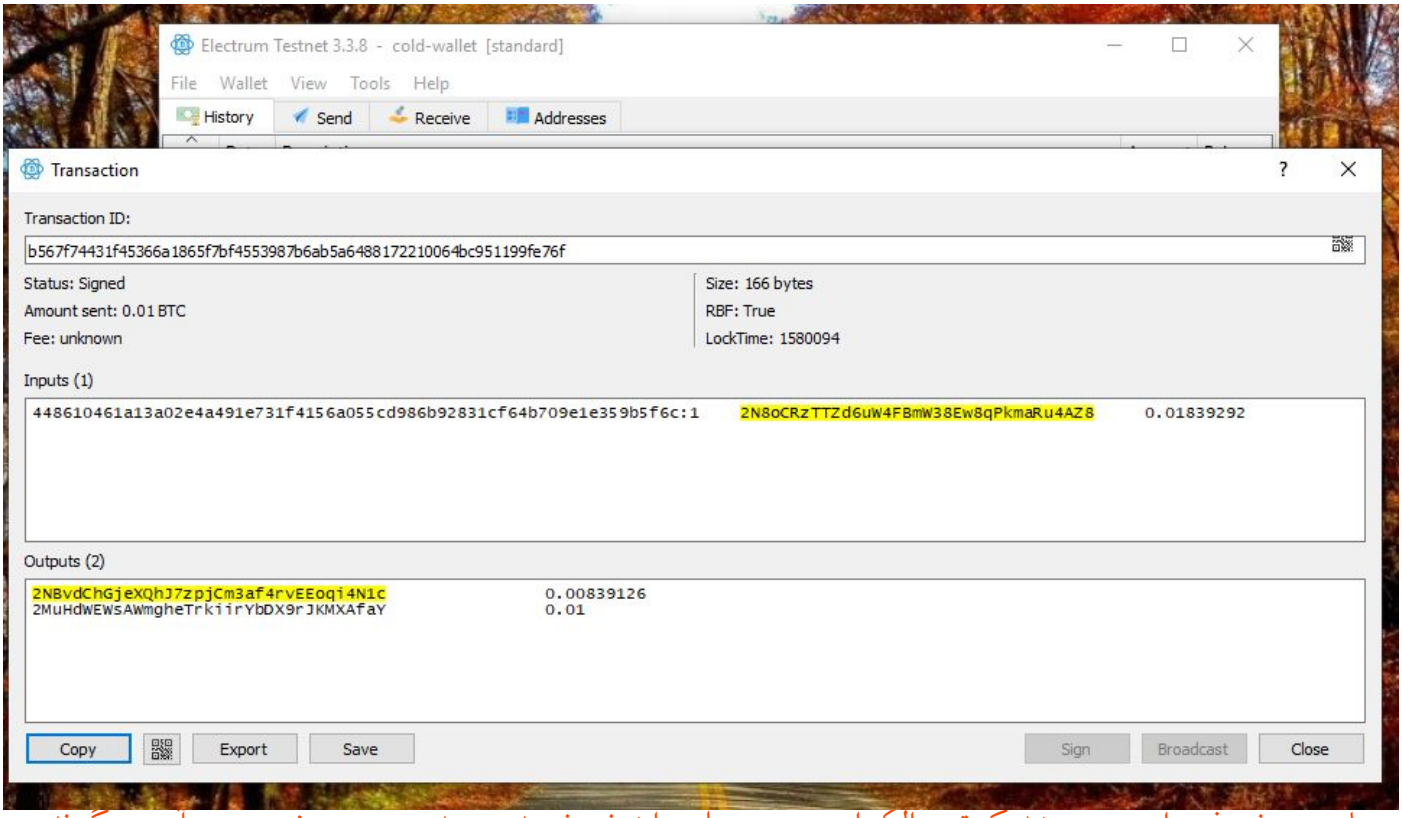
وقتی روی دکمه preview کلیک کنید می‌بینید که این صفحه باز میشه و اطلاعات دقیقتری از بیت‌کوینهایی که قراره توی این تراکنش وارد بشن و آدرسی که میخواید بهش ارسال کنید بهتون نشون می‌ده. اینجا هم آپشن send نداره و کاری که باید بکنید اینه که روی دکمه copy کلیک کنید تا این تراکنش توی clipboard شما ذخیره بشه.



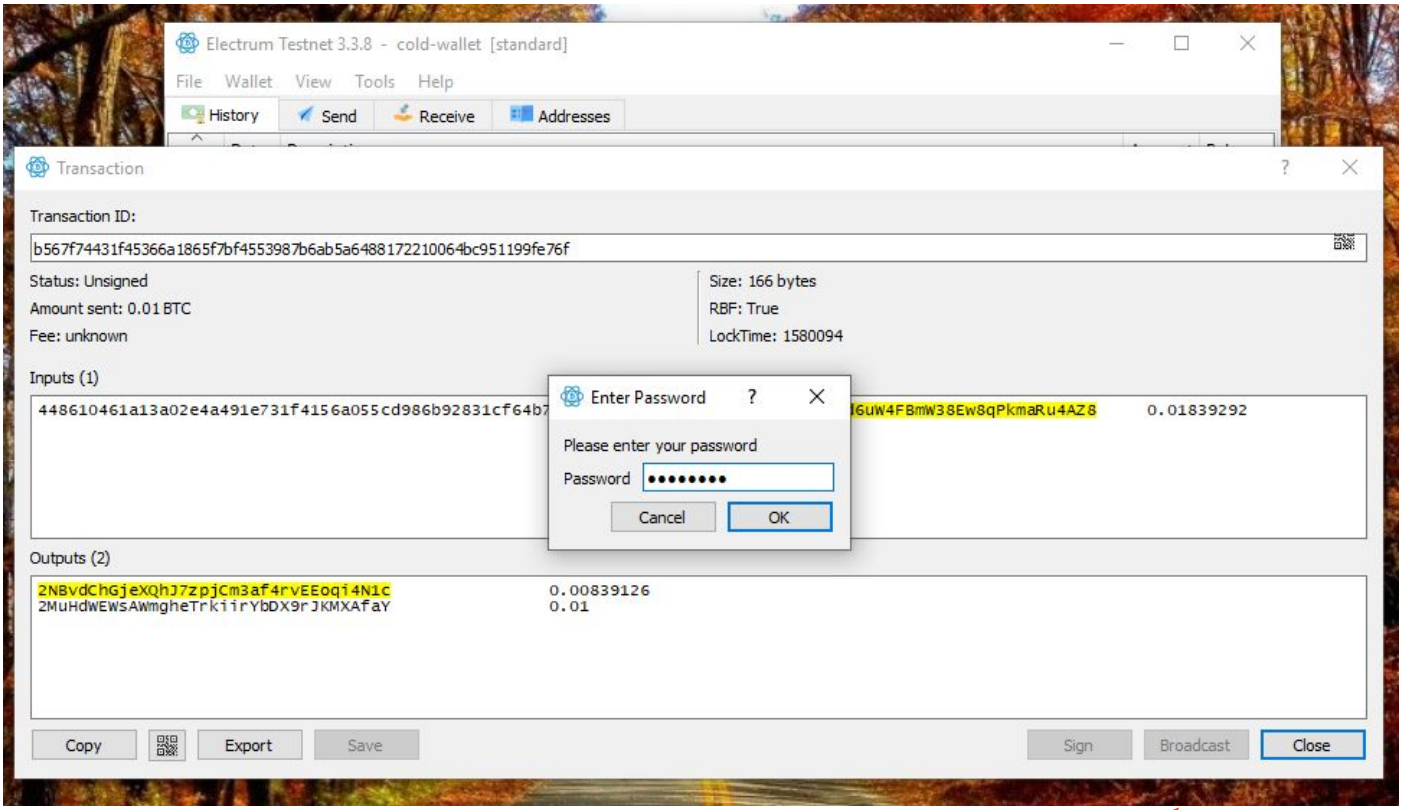
حالا باید برید روی سیستم vm آفلاین و اونجا به التکرام بگین که می‌خواین یک تراکنش رو واردش کنید.



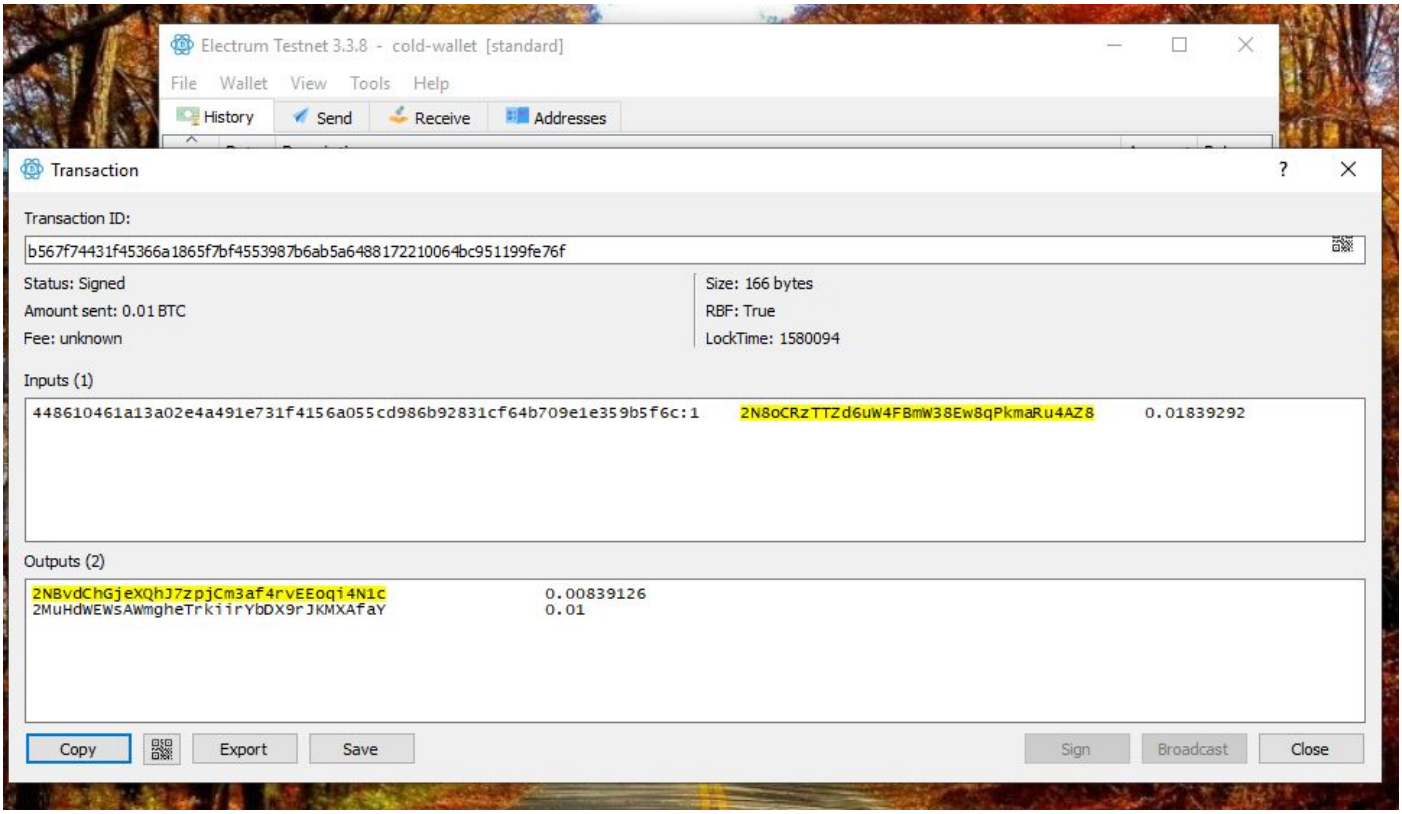
تراکنش داخل clipboard شماست و باید اونجا کپی کنیدش و دکمه load transaction رو بزنید.



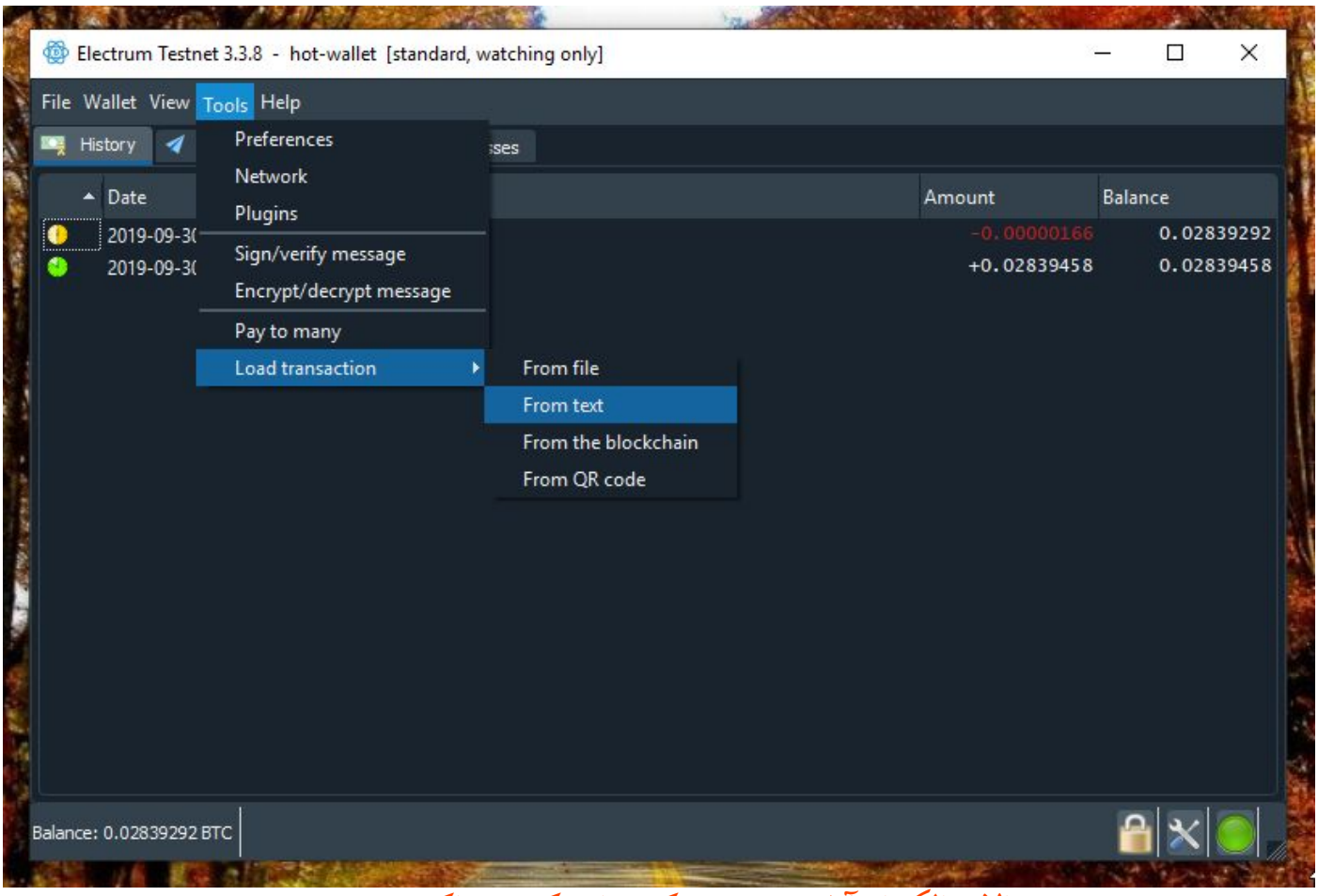
دوباره همون صفحه ای رو می‌بینید که توی الکترام سیستم متصل به اینترنتتون دیده بودید. ورودی و خروجی و آدرس گیرنده و مقدار رو بررسی کنید و حالا دکمه sign رو بزنید.



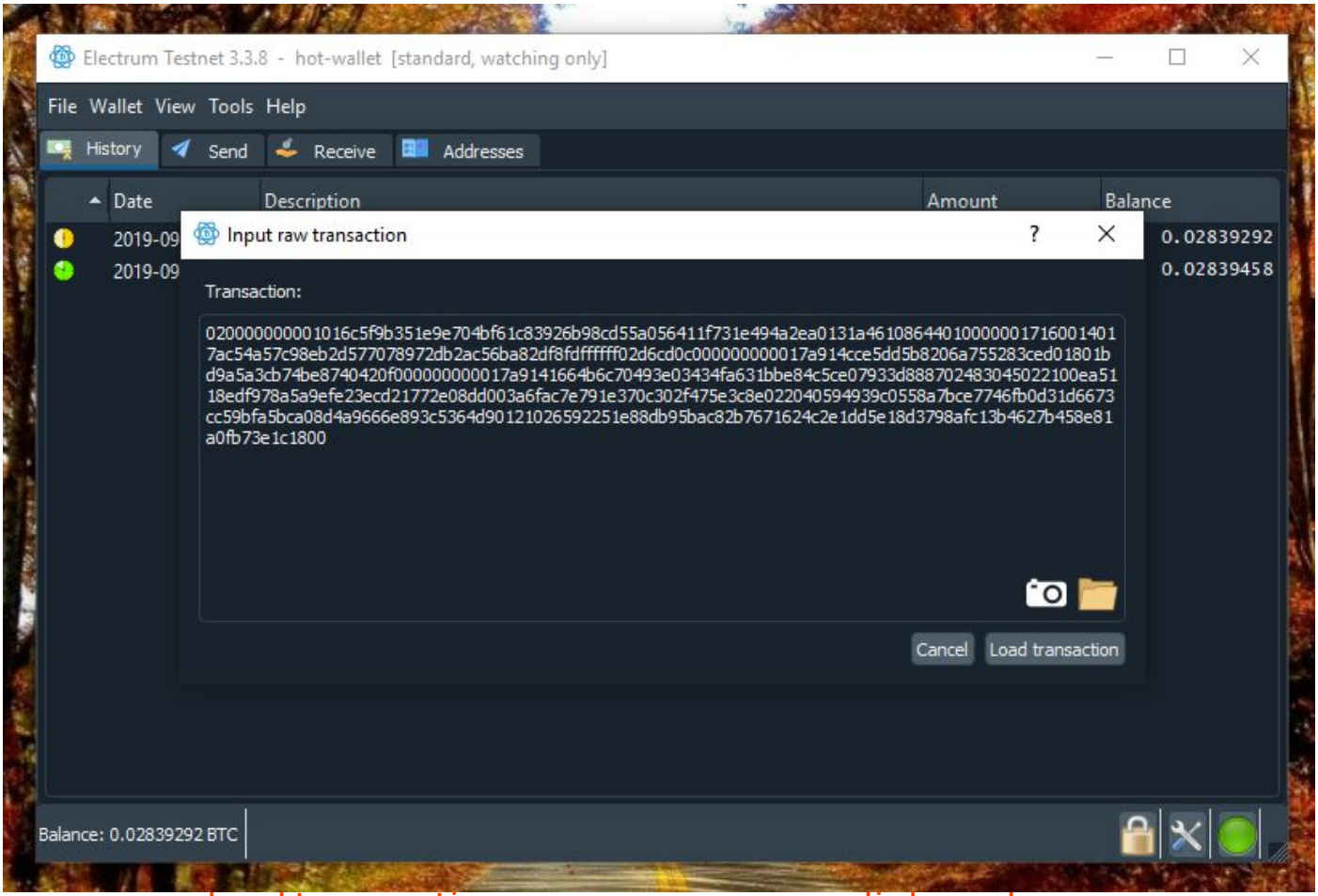
اینجاست که الکترام پسوردی که برای محافظت از کیف‌پول داده بودید رو ازتون می‌خواد. پسورد رو بزنید. اگر خواستید با onscreen keyboard



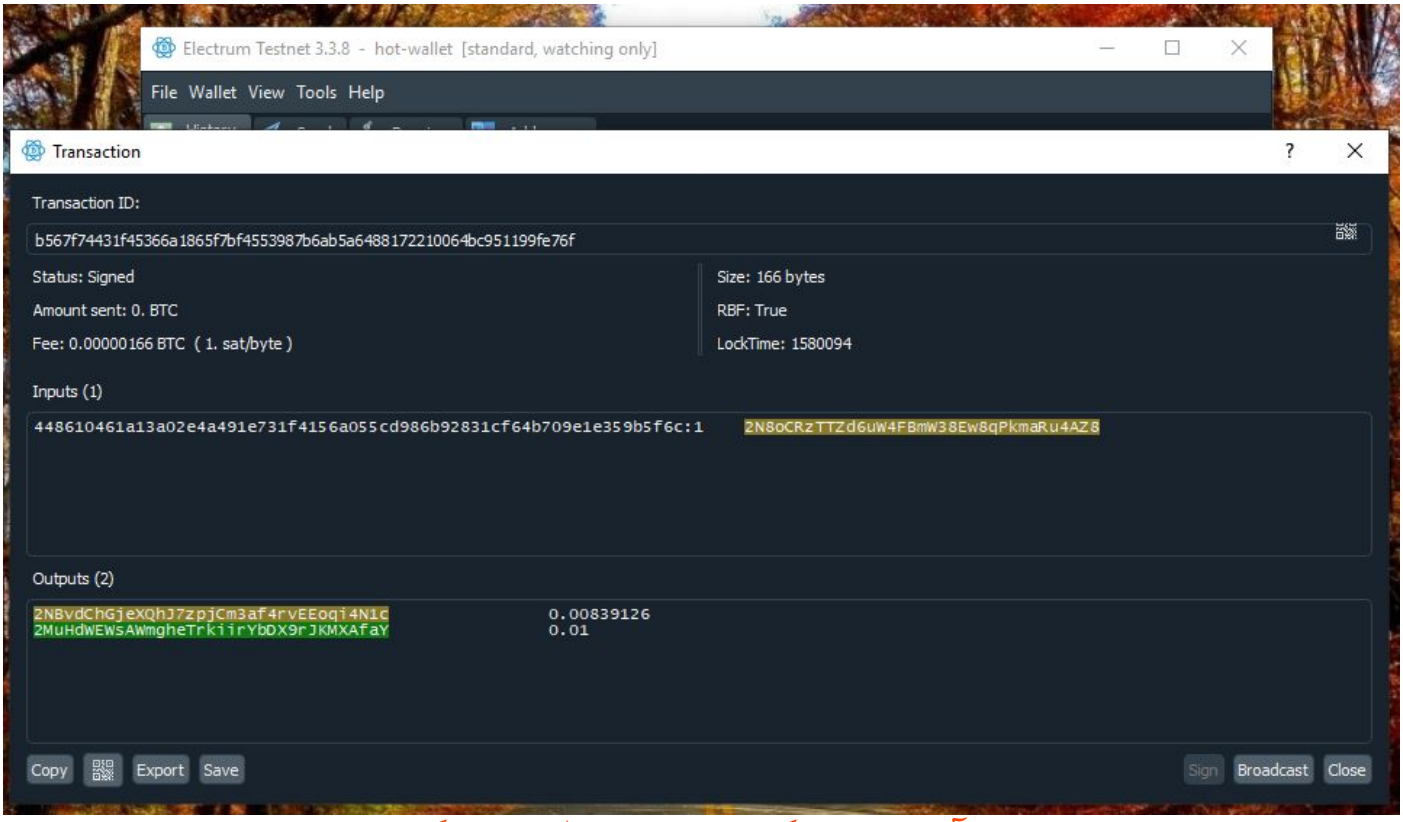
تراکنش شما با موفقیت sign شده ولی این سیستم اینترنت نداره تا بتونه این تراکنش رو به شبکه بیت‌کوین ارسال کنه. پس باید همون کاری که کردیم حالا دوباره برعکس انحام بدیم و این تراکنش sign شده رو به الکترامی که به اینترنت دسترسی داره برسونیم. روی دکمه copy کلیک کنید.



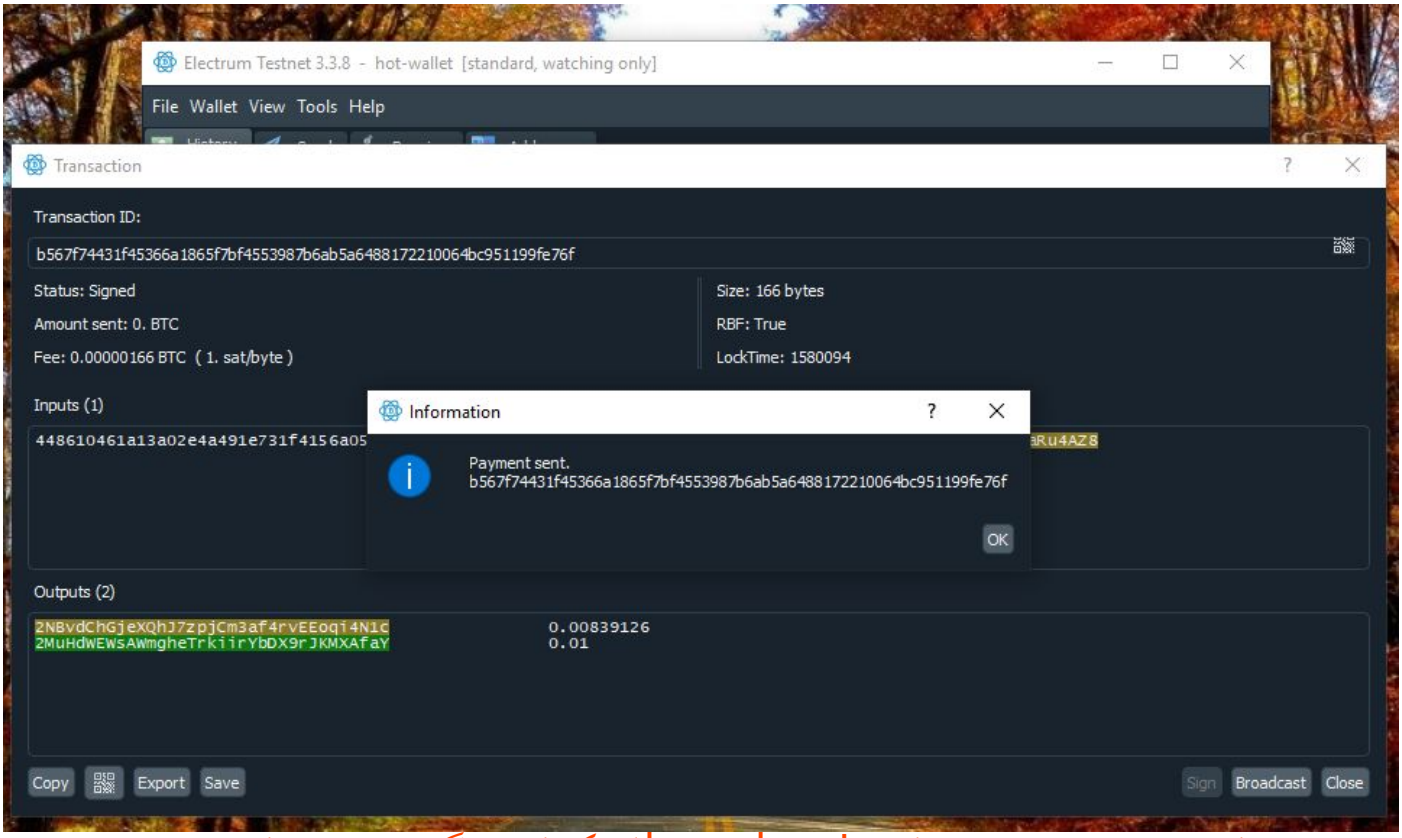
حالا به الکترام آنلاین برید و دکمه وارد کردن تراکنش رو بزنید



تراکنشی که توی clipboard شماست رو اینجا کپی کنید و load transaction رو بزنید.

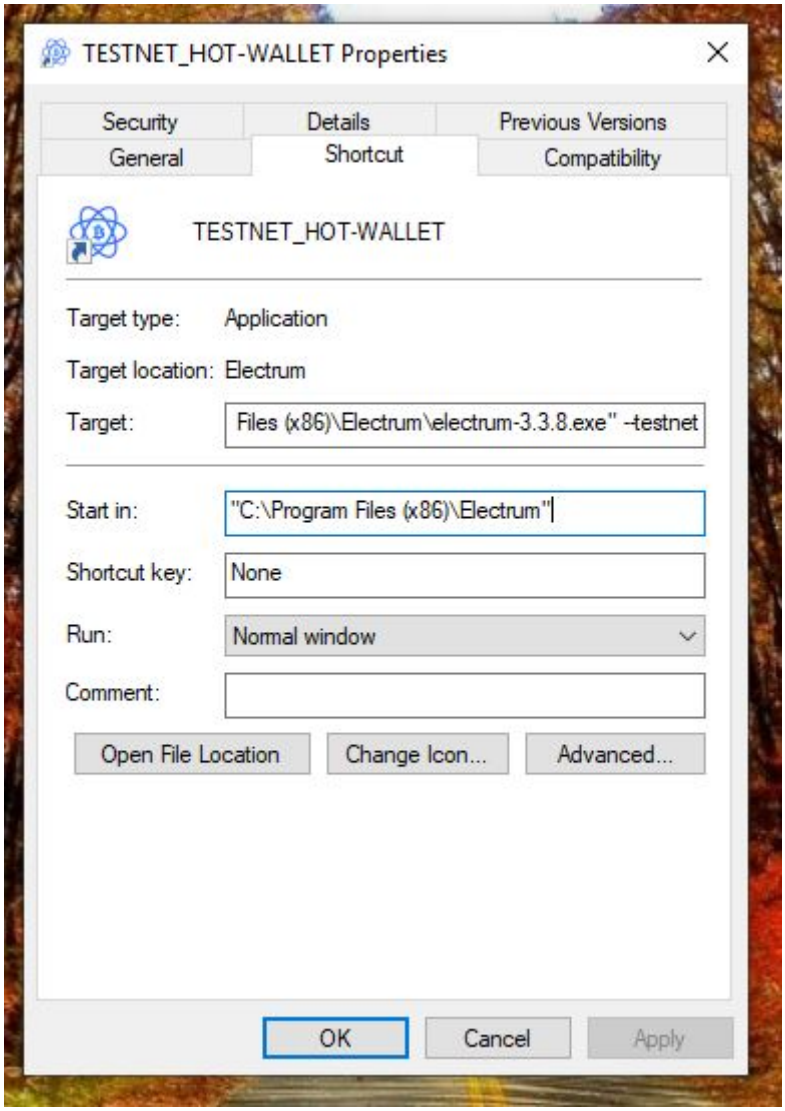


برای آخرین بار تراکنش رو از همه نظر بررسی کنید.



در صورتی که همه چیز درسته روی دکمه broadcast کلیک کنید. اگر همه مراحل کار رو درست انجام داده باشید الکترام تراکنش شما رو با موفقیت به شبکه بیت‌کوین ارسال می کنه و txid اون رو به شما نشون میده.

تنظیم shortcut الکترام برای باز شدن در حالت testnet:



در قسمت target و بعد از جایی که نوشته تمام شده عینا شبیه به عکس کلمه testnet-- رو اضافه کنید. بعد از باز کردن الکترام حتما چک کنید بالای صفحه نوشته شده باشه:

Electrum Testnet

این راهنما با هدف آموزش مفاهیم پایه‌ای بیت‌کوین تهیه شده
و هرگونه استفاده از محتوای آن برای همگان آزاد است.