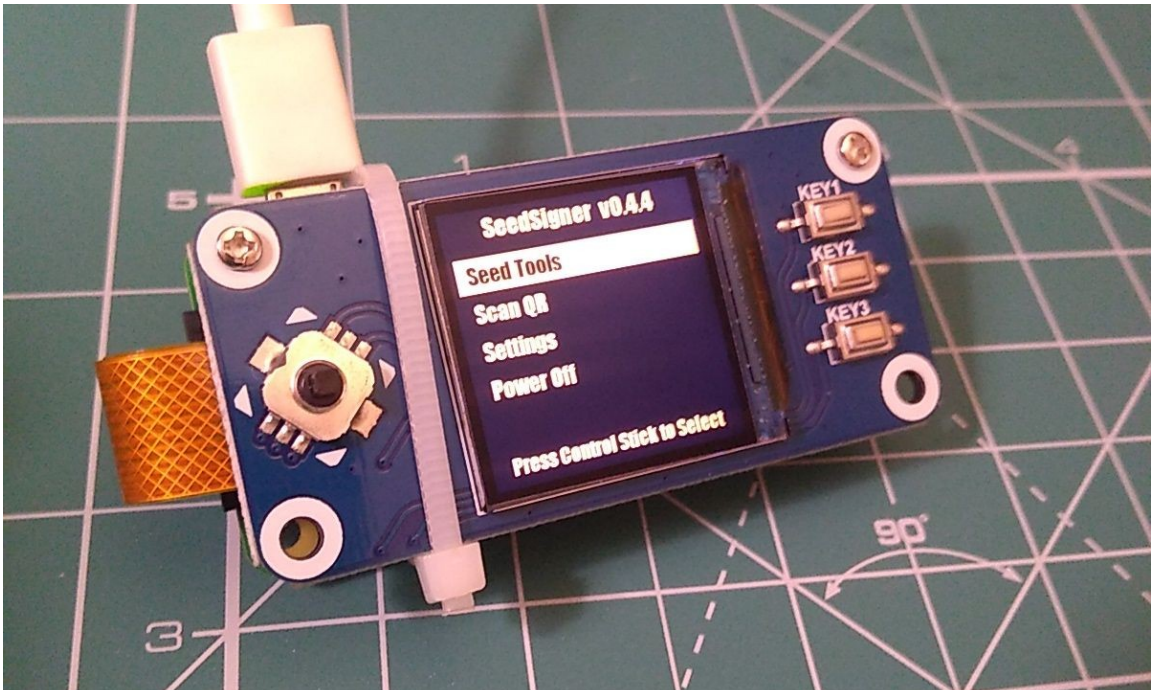


راهنمای آموزشی پروژهٔ SeedSigner

(و بکارگیری آن در کیف پول BlueWallet در حالت ایزوله)

پروژهٔ SeedSigner چیست و چه قابلیت‌هایی دارد؟

برای ارسال بیت‌کوین و امضای تراکنش‌ها -به‌ویژه در حالت ایزوله،- به وسیله‌ای برای تولید امضاء نیاز داریم. SeedSigner درواقع یک پروژهٔ اپن-سورس برای ساختن چنین دستگاهی است. فرق بسیار مهمی که این پروژه با دیگر پروژه‌های معروف به «کیف پول سخت‌افزاری[1]» دارد این است که هرکس در هرکجای دنیا می‌تواند قطعات لازم برای ساختن این دستگاه را شخصاً از بازار تهیه، و به ساختن آن اقدام کند.

هدف این پروژه پایین آوردن هزینه و پیچیدگی‌های کیف پول‌های چند امضاییِ بیت‌کوین است. این پروژه برای رسیدن به این هدف به همگان این فرصت را می‌دهد تا با استفاده از قطعات سخت‌افزاری ارزان‌قیمتی که در هرجای دنیا در دسترس عموم است، یک دستگاه با هزینهٔ کمتر از ۵۰ دلار برای خود بسازند. این دستگاه امکان امضای تراکنش‌های بیت‌کوین را برای کاربران خود در محیطی کاملاً ایزوله فراهم می‌سازد.

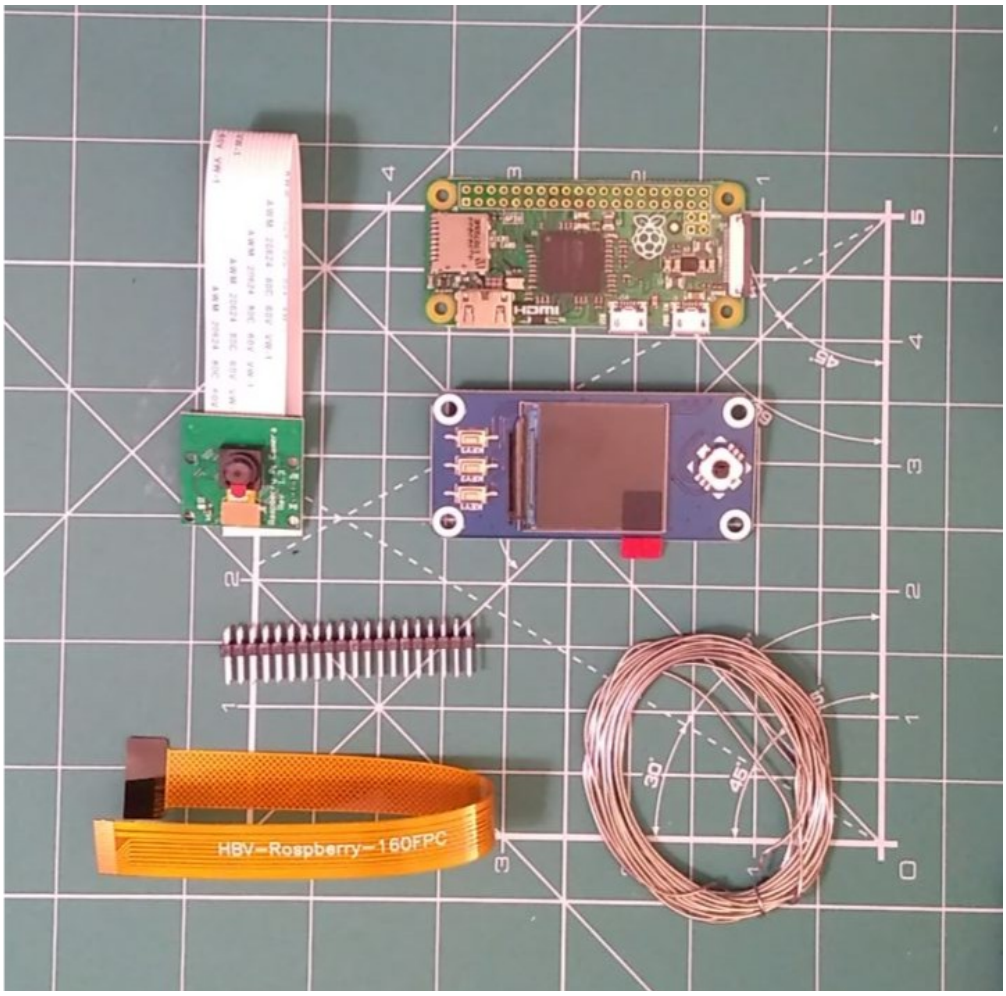
با توجه به اینکه این دستگاه دارای صفحه‌نمایش و دوربین است می‌تواند طیف گسترده‌ای از نیازهای مربوط به «امضای تراکنش‌ها» را به خوبی انجام دهد و به‌عنوان نمونه در مقایسه با ColdCard که محیط ایزوله را از طریق بکارگیری حافظهٔ microSD پیاده‌سازی می‌کند، بسیار آسانتر است.

کاربردهای SeedSigner به‌صورت تیتروار به شرح زیر است:

- امکان امضای تراکنش‌های تک امضایی و چند امضایی با بکارگیری از روش PSBT در یک محیط کاملاً ایزوله[2].
- امکان وارد کردن ۳ کلید خصوصی مجزا در حافظهٔ این دستگاه.

1 Hardware Wallet
2 Air-gapped

- پشتیبانی از طیف گسترده‌ای از کیف پول‌های معتبر مانند: Specter Wallet و Sparrow Wallet و BlueWallet.
- پشتیبانی از شبکهٔ تست بیت‌کوین.
- ساخت کلید خصوصی با استفاده از عکسی که دوربین این دستگاه می‌گیرد.
- ساخت کلید خصوصی با استفاده از تاس.
- امکان تولید کلمهٔ ۱۲ یا ۲۴ ام برای افرادی که کلید خصوصی خود را با کاغذ و تاس تولید می‌کنند.
- امکان اضافه شدن پسفریز[1] به کلیدهای خصوصی.



قطعات لازم برای ساختن یک SeedSigner

1 Passphrase

قطعات لازم[1]

- بُرد رزبری‌پای زیرو (نسخهٔ ۱.۳)[2]
- هَت نمایشگر ۱.۳ اینچی. ۲۴۰ x ۲۴۰ پیکسل (ساخت Waveshare)[3]
- ماژول دوربین رزبری‌پای[4] (5MP, 1080p, v1.3)
- کابل فلت دوربین مخصوص بُرد رزبری‌پای زیرو
- مموری MicroSD با حداقل ۴ گیگابایت فضا

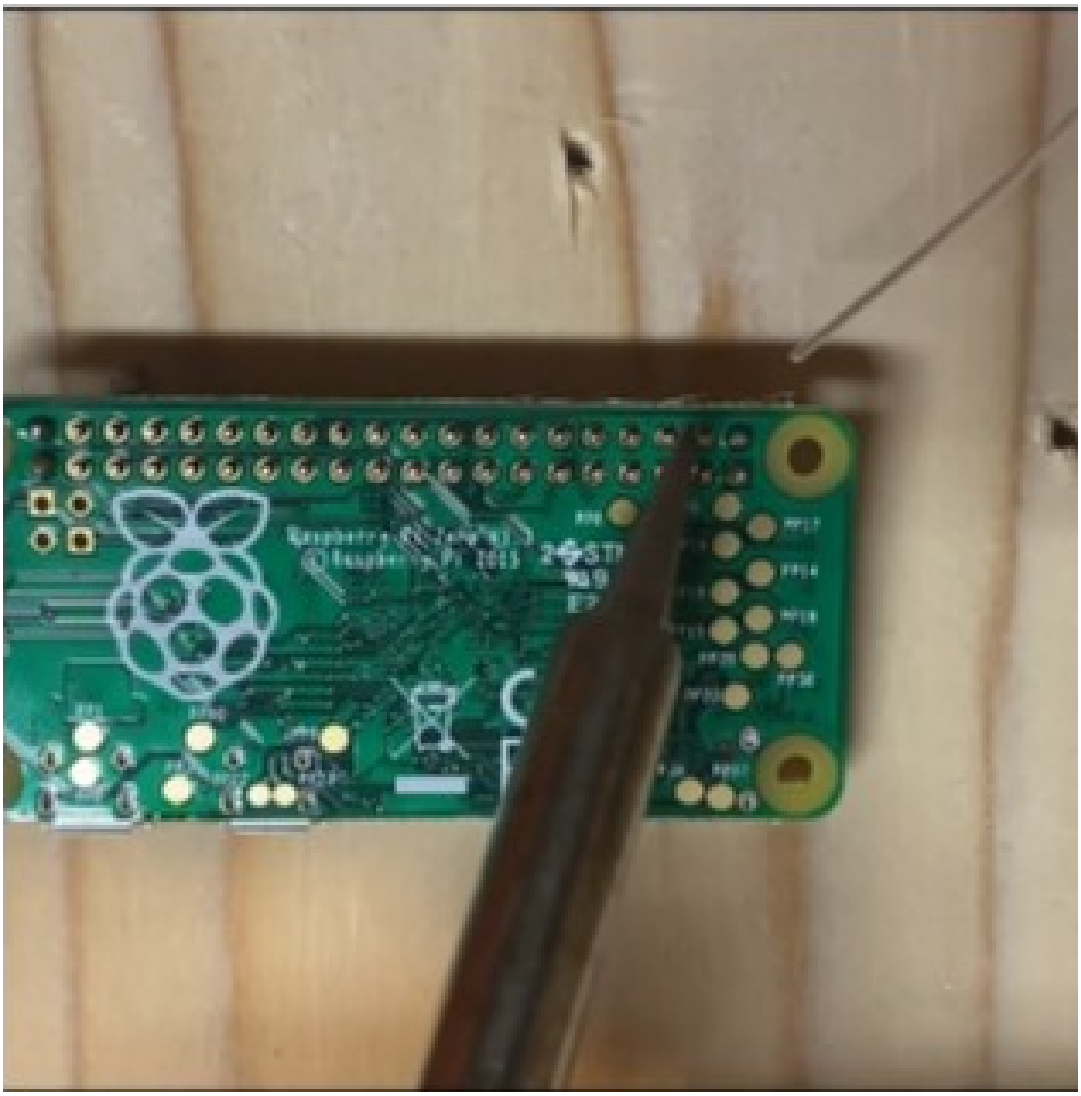
در نسخهٔ WH پین هدر از طرف شرکت سازنده بر روی بردهای رزبری‌پای نصب شده است ولی با توجه به اینکه این نسخه دارای چیپ وای-فای است، پیشنهاد می‌شود برای حذف خطر نشت کلید خصوصی از طریق پردازندهٔ رادیویی، نسخه زیرو را تهیه و هدر را شخصاً لحیم‌کاری کنید. در این صورت به لوازم زیر نیاز پیدا خواهید کرد:

- پین هِدر ۲۰ x ۲ نری مستقیم با فاصله پین ۲.۵۴ میلی‌متر
- قلع و هویه برای لحیم‌کاری

همهٔ این قطعات را می‌توان از فروشگاه‌ها یا سایت‌های عرضهٔ قطعات الکترونیکی تهیه کرد. اگر امکان خرید حضوری دارید پیشنهاد می‌کنیم به بازار قطعات الکترونیکی در خیابان جمهوری حوالی پل حافظ بروید و این قطعات را حضوری تهیه کنید. هزینهٔ تهیهٔ این قطعات در پاییز سال ۱۴۰۰ حدود ۱ تا ۱.۲ میلیون تومان است.

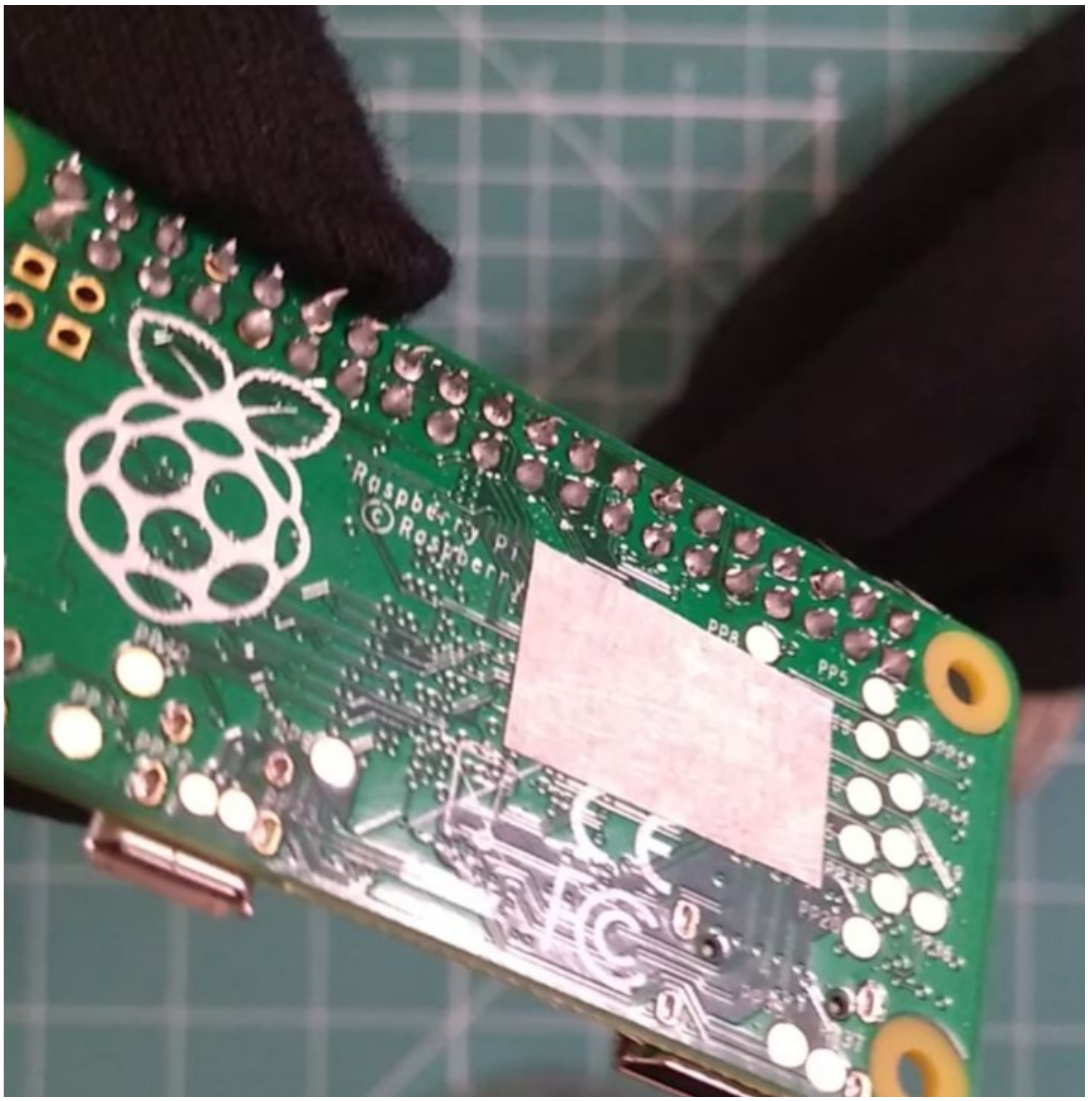
1 https://seedsigner.com/hardware
2 Raspberry Pi Zero (version 1.3)
3 WaveShare 1.3 inch LCD hat with 240×240 pixel display
4 Pi Zero compatible camera module

مرحلهٔ اول: لحیم‌کاری پین هِدر روی بُرد



ویدیوی آموزشی لحیم‌کاری پین هدر روی رزبری‌پای زیرو

نوک هویه را کنار پین و روی بُرد بگذارید و پس از گذشت سه ثانیه قلع را بین پین و نوک هویه بچسبانید تا آب شود و قسمت مسی روی برد را بپوشاند. در انتها نوک هویه را روی هدر پین به سمت بالا سُر دهید و آن را از روی بُرد بردارید.

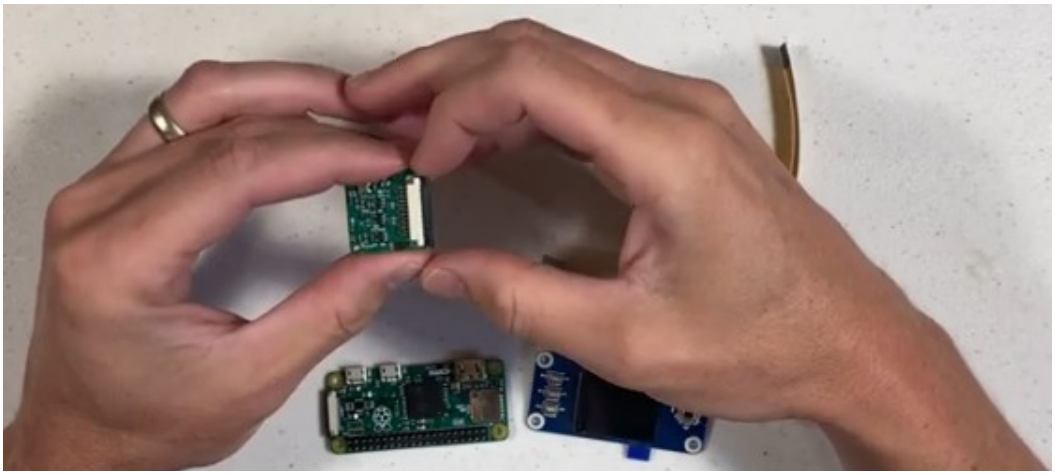


توجه کنید که پین‌ها نباید با یکدیگر اتصال پیدا کنند. اگر مقدار قلع روی پایه‌ها زیاد بود سعی کنید با مذاب کردن مجدد و کشیدن آن‌ها به سمت بالا از مقدار آن کم کنید.

در پایان کار، لحیم‌کاری را با چشم، یا به کمک یک ذره‌بین بررسی و از درستی آن اطمینان حاصل کنید.

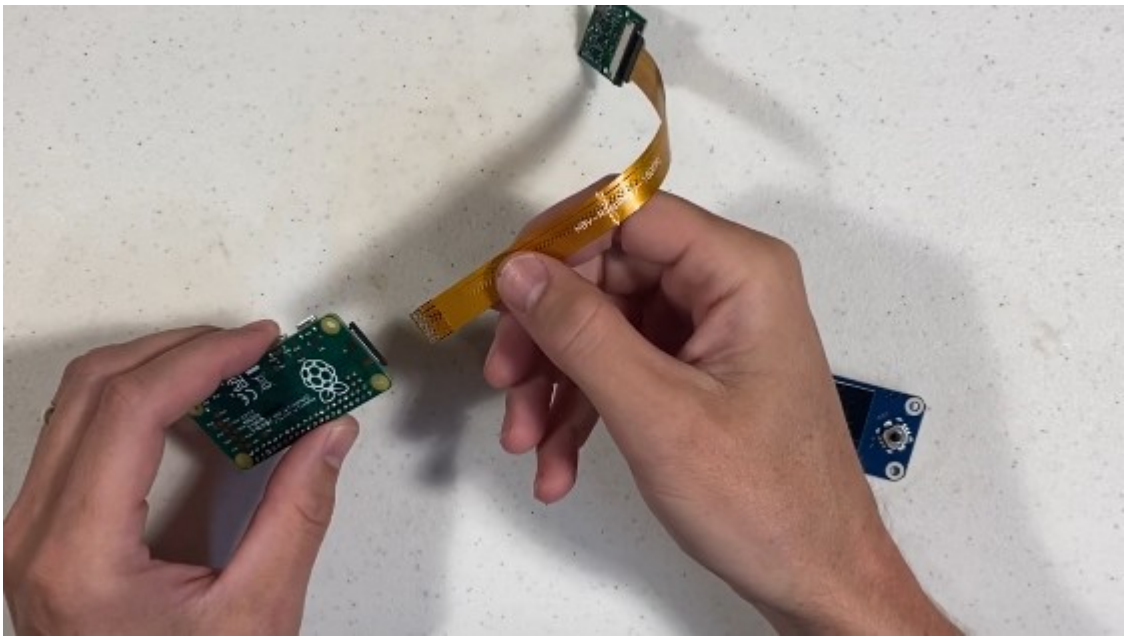
مرحلهٔ دوم: نصب دوربین

کابل فلت سفید از پیش نصب شده روی دوربین رزبری‌پای باید با کابل فلت مخصوص رزبری‌پای زیرو که اغلب به رنگ طلایی است، تعویض شود. برای انجام این کار نگهدارندهٔ کابل را به آرامی حدود ۱ میلیمتر به بیرون بکشید و کابل سفید را آزاد کنید.



ویدیوی آموزشی اتصال کابل به دوربین

سپس سر عریض کابل طلایی را وارد کنید و بست نگهدارنده را به آرامی فشار دهید تا به جای اولیهٔ خود بازگردد. به جهت کابل دقت کنید. اگر این بست از جای خود خارج شد یا یکی از خارهای آن بیرون آمد، دوباره آن را به آرامی در جای خود قرار داده و با کمی فشار جا بزنید.



ویدیوی آموزشی اتصال کابل به برد

این کار را برای سمت دیگر کابل فلت دوربین تکرار کنید و آن را به برد رزبری‌پای وصل کنید. به جهت وارد شدن کابل فلت دقت کنید.

مرحلهٔ سوم: جاگذاری صفحه نمایش

ویدیوی آموزشی جاگذاری صفحه‌نمایش

پین‌های صفحه نمایش را با پین هِدرهای روی برد تراز کنید و با انگشتان خود از پایین و بالا آرام به بُرد و صفحه‌نمایش فشار وارد کنید تا صفحه‌نمایش در جای خود قرار گیرد.

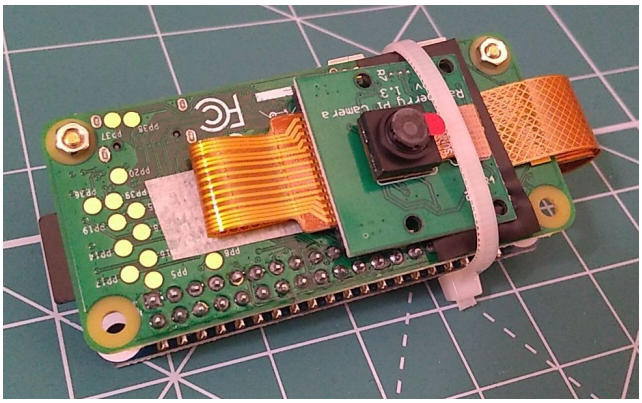
مرحلهٔ چهارم: آماده‌سازی مموری

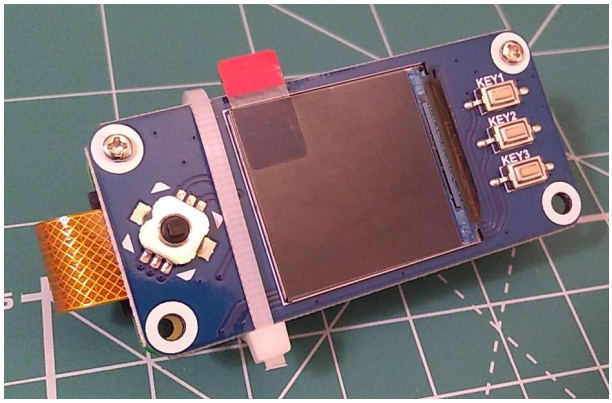
برای آماده‌سازی مموری باید به مخزن گیت‌هابِ پروژه[1] بروید و در بخش Releases آخرین نسخه را دانلود کنید. در زمان نگارش این راهنما آخرین نسخهٔ منتشر شده نسخهٔ v0.4.4 است.

- ابتدا فایل zip شده را دانلود و سپس آن را از حالت فشرده خارج کنید.
- فایل img را با استفاده از نرم‌افزار Balena Etcher[2] یا نرم‌افزارهای مشابه روی مموری کپی کنید.
- مموری را در خشاب تعبیه شده روی برد رزبری وارد کنید. به جهت وارد شدن مموری دقت کنید.
- پیشنهاد می‌شود قبل از کپی کردن فایل img اعتبار آن را از طریق امضای دیجیتال آن بررسی کنید.

1 https://github.com/SeedSigner/seedsigner/releases
2 https://www.balena.io/etcher

مرحلهٔ نهایی: فیکس کردن قطعات و اتصال منبع تغذیه





این دستگاه به منبع تغذیهٔ خاصی نیاز ندارد و می‌توان آن را با اتصال یک کابل با اینترفیس microUSB به یک شارژر موبایل یا حتی یک پاوربانک راه‌اندازی کرد. می‌توانید با چسب یا بست کمربندی قطعات را سر جای خود محکم کنید. همواره دقت کنید که نباید فشار زیادی به این قطعات وارد شود.

پس از اتصال کابل تغذیه، دستگاه بوت می‌شود و پس از گذشت حدود ۴۵ تا ۶۰ ثانیه آمادهٔ استفاده خواهد بود. پس از بالا آمدن کامل SeedSigner به بخش تنظیمات بروید و روی آیتم Input/Output Tests کلیک کنید. با این کار سیستم‌عامل SeedSigner ورودی و خروجی‌های دستگاه را بررسی می‌کند و شما نیز می‌توانید با جوی‌استیک و کلیدهای کناری، درستی کارکرد دستگاه را تست کنید.

برای آزمایش دوربین به صفحهٔ اصلی برگردید و منوی Scan QR را انتخاب کنید تا دوربین دستگاه روشن شود و پیش‌نمایش را بر روی صفحه LCD مشاهده کنید. بعد از آزمایش دستگاه می‌توانید قابلیت‌های مختلف آن را در آیتم‌های مختلف منوی این دستگاه کوچک و جالب بررسی کنید.

اگر به پرینتر سه‌بعدی دسترسی دارید می‌توانید برای SeedSigner خود یک قاب بسازید. برای کسب اطلاعات بیشتر و دانلود فایلِ قاب به گیت‌هاب[1] پروژه مراجعه کنید.

برای ارتباط مستقیم با تیم توسعهٔ این پروژه به گروه رسمی تلگرام آن‌ها به آدرس https://t.me/joinchat/GHNuc_nhNQjLPWsS بپیوندید.

1 https://github.com/SeedSigner/seedsigner

ایجاد یک کیف پول امن روی موبایل در حالت ایزوله

با استفاده از BlueWallet در تعامل با SeedSigner

در این قسمت از نرم‌افزار BlueWallet به‌عنوان کیف پول استفاده می‌کنیم و SeedSigner برای ساخت کلید خصوصی و امضا کردن تراکنش‌هایی که توسط کیف پول ساخته شده است، بکار گرفته می‌شود. کیف پول ایجاد شده بر روی BlueWallet به‌صورت Watching-Only است و فقط قابلیت ساخت آدرس‌های جدید و دریافت بیت‌کوین را دارد و کلید خصوصی بر روی آن ذخیره نشده است. بنابراین برای انتقال بیت‌کوین از روی این کیف پول، تراکنش ارسالی می‌بایست توسط SeedSigner امضا شود.

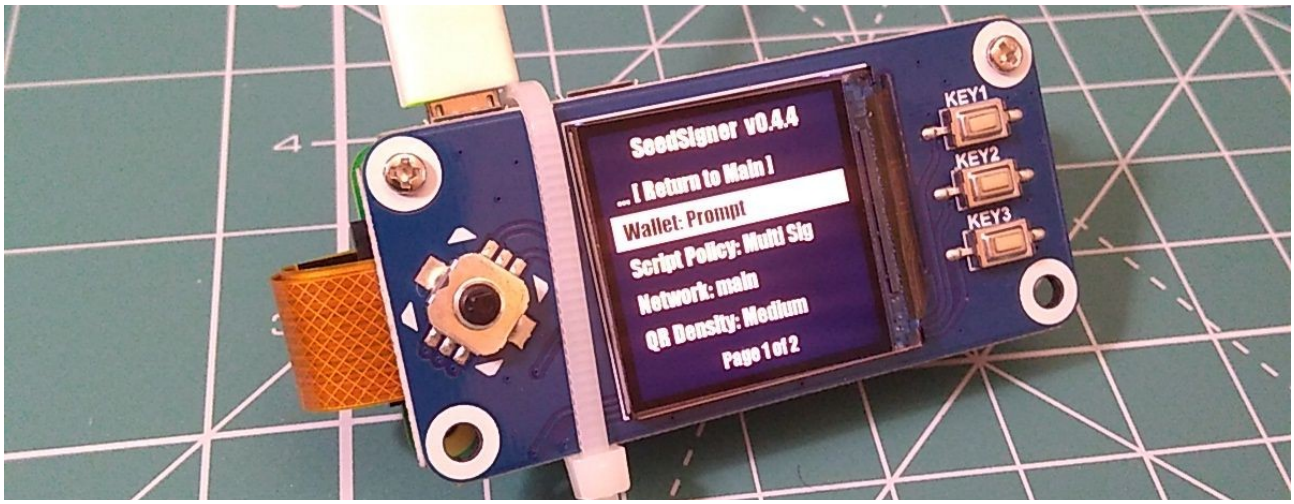
لطفاً در نظر داشته باشید پروژهٔ SeedSigner همچنان در حال توسعه است و ممکن است رابط کاربری آن در نسخه‌های بعدی تغییر کند. با این حال با توجه به پایه‌ای بودن مفاهیمی که در این راهنمای آموزشی مطرح شده، این مطلب در آینده نیز می‌تواند برای مخاطبان گرامی مفید باشد.

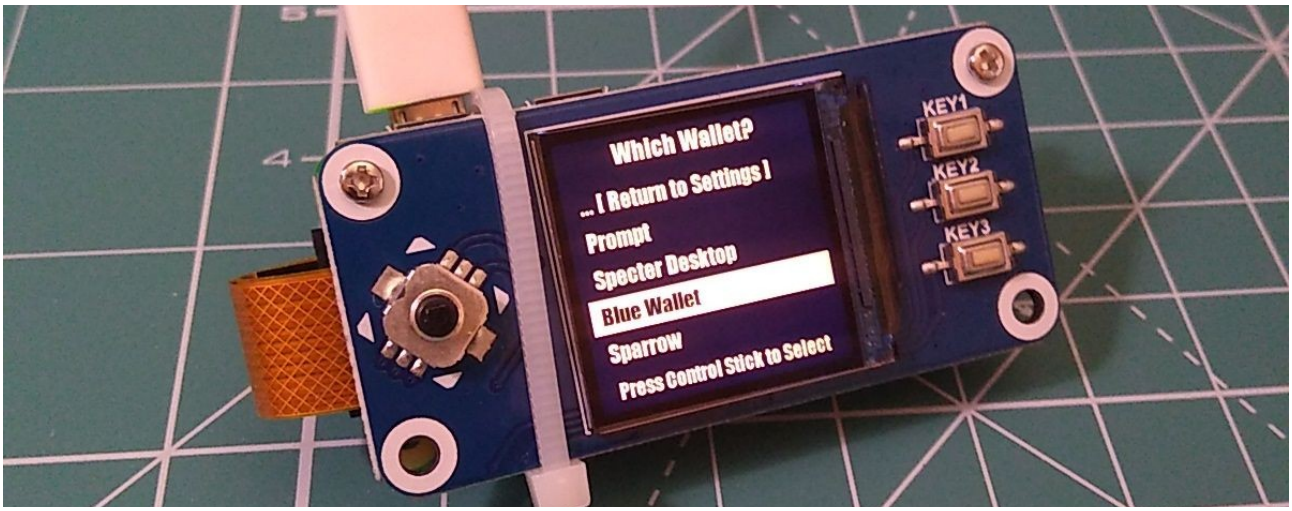
در این راهنمای آموزشی موارد زیر را انجام خواهیم داد:

۱. تنظیم دستگاه SeedSigner برای کار با کیف پول BlueWallet و در حالت تک امضاء.
۲. ساخت یک کلید خصوصی با استفاده از SeedSigner.
۳. نمایش xPub کلید خصوصی مورد نظر روی صفحه‌نمایش دستگاه.
۴. وارد کردن xPub کلید خصوصی ساخته شده در نرم‌افزار BlueWallet و ساختن یک کیف پول Watching-Only بر روی موبایل و واریز بیت‌کوین به آن.
۵. تنظیم کیف پول ایجاد شده برای تعامل با SeedSigner.
۶. تعامل BlueWallet و SeedSigner با یکدیگر برای امضای تراکنش و انتقال بیت‌کوین از کیف پولی که در حالت Watching-Only کار می‌کند.

تنظیم دستگاه برای کار با کیف پول `BlueWallet` و در حالت تک امضاء

در قسمت تنظیمات روی گزینهٔ `Wallet` کلیک کنید و کیف پول `BlueWallet` را انتخاب کنید.





در مرحلهٔ بعد همچنان در قسمت تنظیمات روی منوی Script Policy کلیک کنید و آیتم تک امضاء را انتخاب کنید.

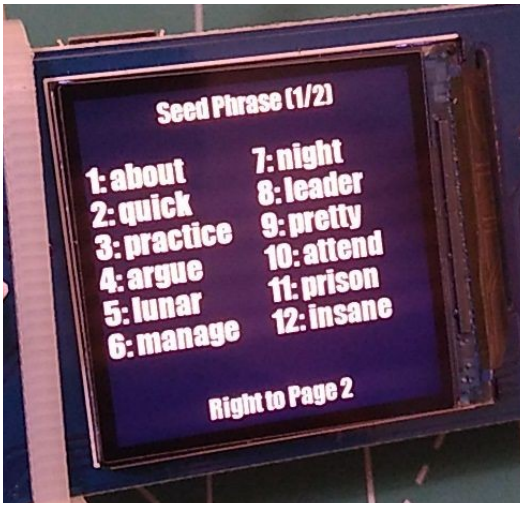
مرحلهٔ اول: تولید کلید خصوصی روی SeedSigner

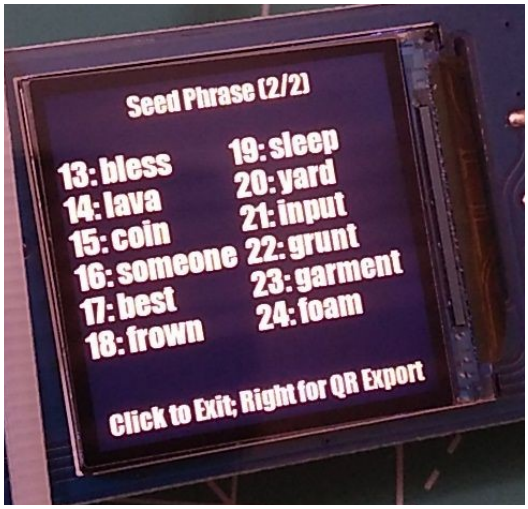
دستگاه SeedSigner قادر است یک عکس با دوربین خود ثبت کند و با ادغام آنتروپی موجود در عکس و منابع دیگری که در سیستم‌عامل وجود دارند، یک کلید خصوصی تولید کند. شما می‌توانید کلید خصوصی خود را از هر روشی که بیشتر می‌پسندید تولید، و به مطالعهٔ راهنما ادامه دهید.

برای تولید یک کلید خصوصی با استفاده از دوربین، در منوی Seed Tools دستگاه با استفاده از جوی‌استیک روی گزینهٔ Generate Seed With Image کلیک کنید.

پس از فعال شدن دوربین و مشاهدهٔ پیش‌نمایش روی LCD، با استفاده از دکمهٔ جوی‌استیک یک عکس بگیرید و برای رفتن به مرحلهٔ بعد جوی‌استیک را به سمت راست فشار دهید تا عکسی که گرفتید به‌عنوان منبع آنتروپی مورد استفاده قرار گیرد.

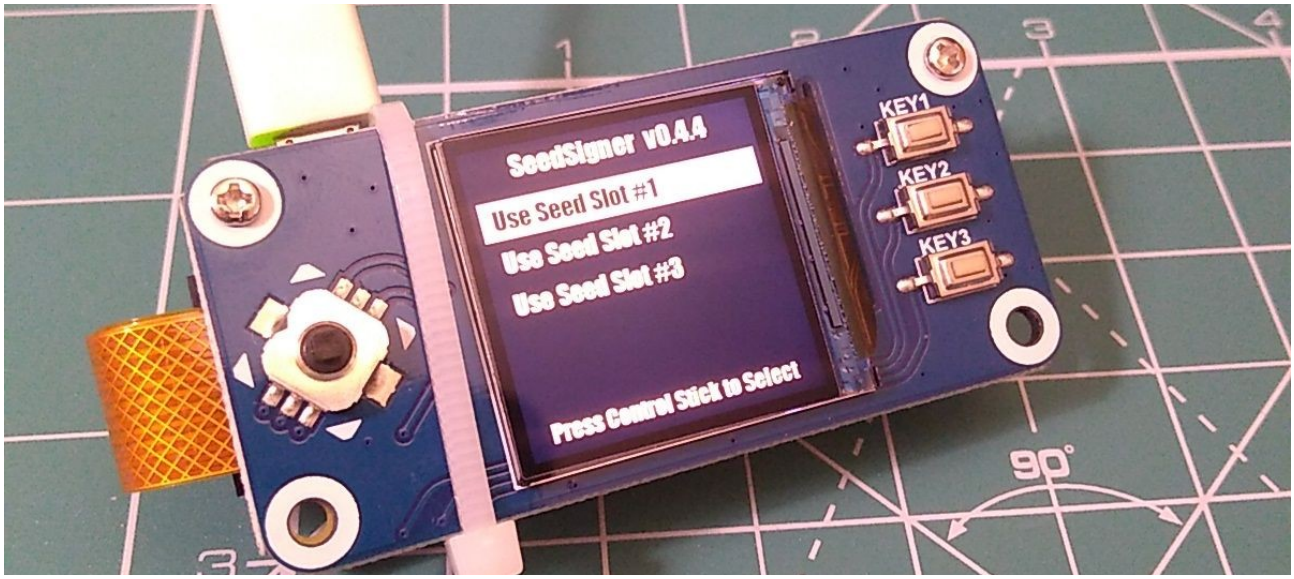
سپس دستگاه ۲۴ کلمهٔ بازیابی شما را در دو صفحه به شما نمایش می‌دهد.



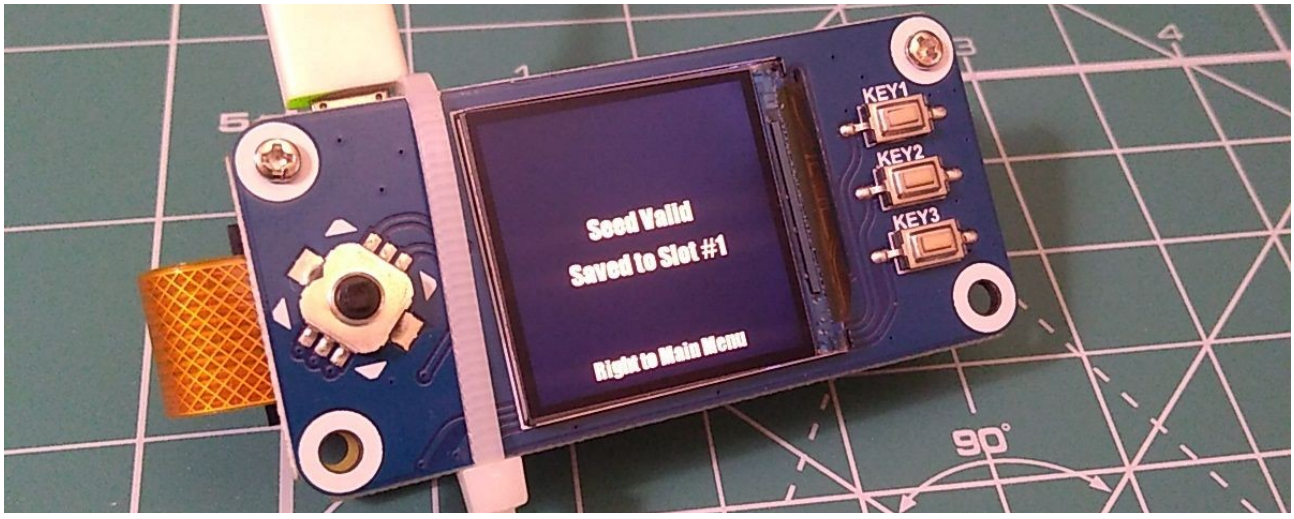


با فشار دادن جوی‌استیک به سمت راست، دستگاه یک کُد QR به شما نمایش می‌دهد که می‌توان از آن برای بکاپ‌گیری از کلمات بازیابی استفاده کرد. برای اطلاعات بیشتر این رشته توئیت را ببینید.

با خروج از این قسمت دستگاه به شما پیشنهاد ذخیره کردن کلید خصوصی تولید شده را می‌دهد. شما می‌توانید آن را در یکی از ۳ جایگاهی که در این دستگاه تعبیه شده است، ذخیره کنید.

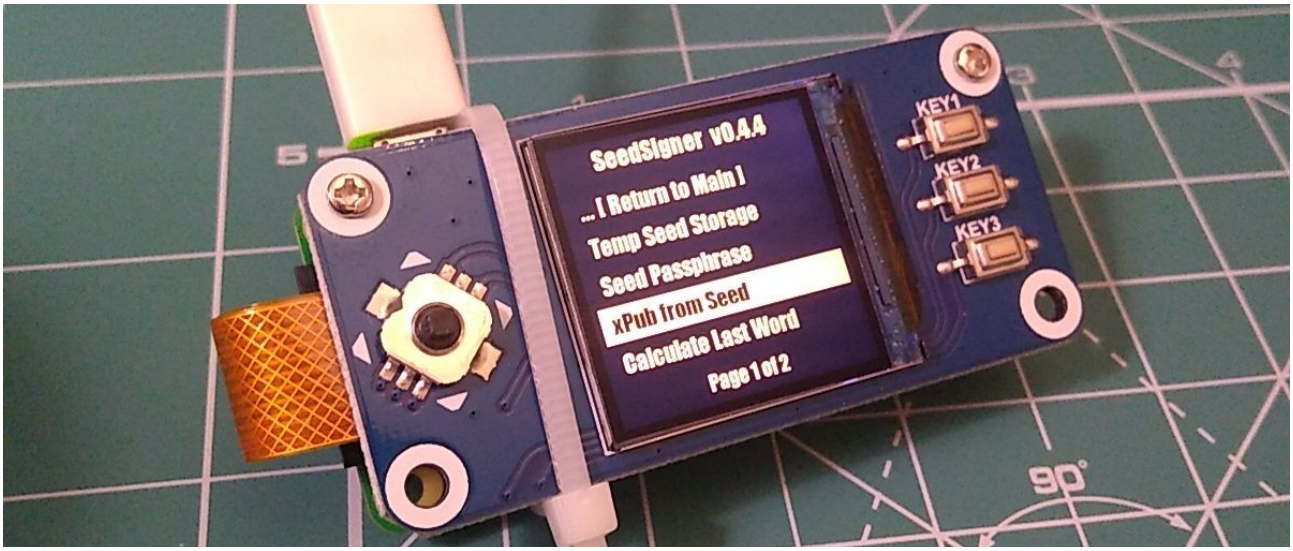


در نهایت پیغام معتبر بودن و ذخیره شدن کلید خصوصی را از دستگاه دریافت خواهید کرد.



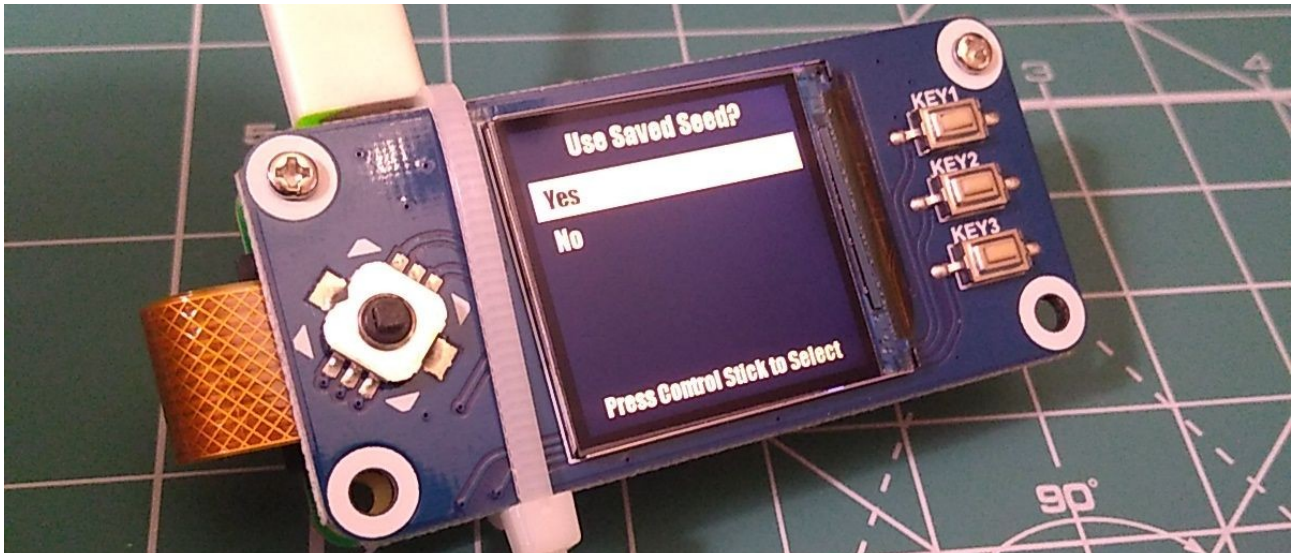
مرحلهٔ دوم: نمایش xPub کلید خصوصی مورد نظر روی صفحه‌نمایش دستگاه

برای ایجاد یک کیف پول «فقط ناظر[1]» در BlueWallet به xPub کلید خصوصی که در مرحلهٔ قبل ساخته شده، نیاز داریم. برای به‌دست آوردن آن از منوی اصلی روی Seed Tools و سپس xPub From Seed کلیک کنید.



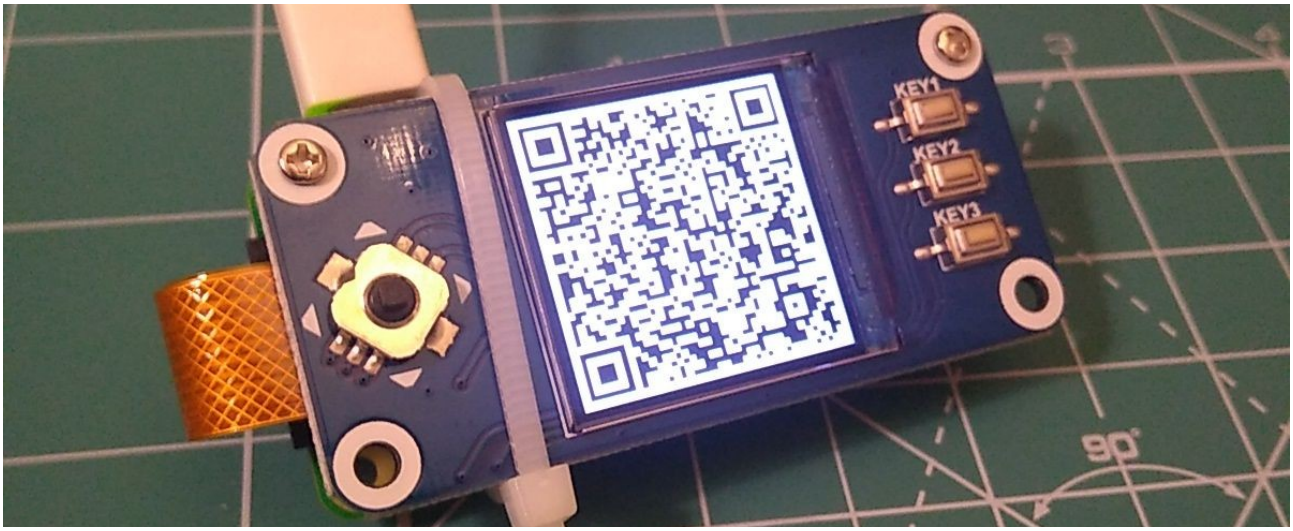
1 Watching-Only

در این مرحله دستگاه از شما می‌پرسد که آیا کلید خصوصی ذخیره کرده‌اید و اگر بله، می‌خواهید از کدامیک استفاده کنید.



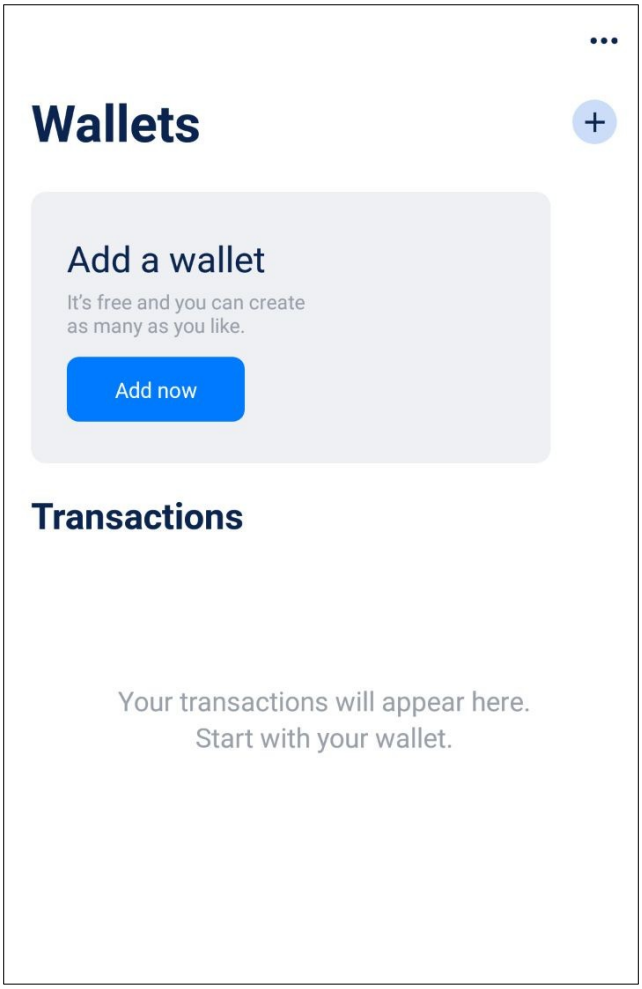
پس از انتخاب، دستگاه اطلاعاتی را در مورد xPub کلید خصوصی مورد نظر نشان می‌دهد

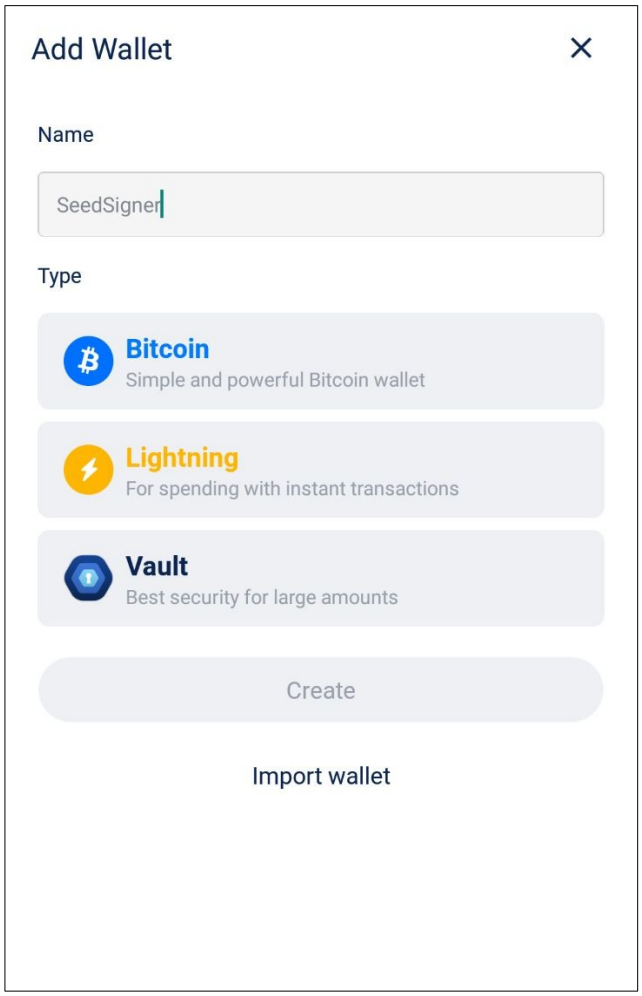
و سپس xPub را در قالب یک کُد QR نمایش می‌دهد.



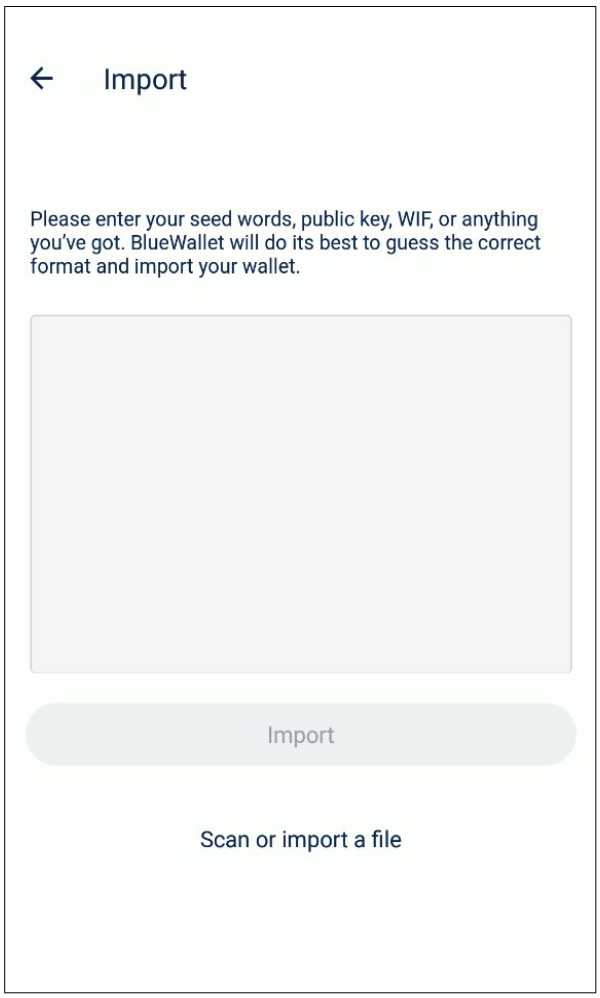
مرحلهٔ سوم: ایجاد کیف پول در نرم‌افزار `BlueWallet` در حالت `Watching-Only` با استفاده از `xPub` تولید شده در مرحلهٔ قبل

کیف پول `BlueWallet` را باز کنید و دکمهٔ `Add now` را بزنید. سپس یک نام دلخواه برای این کیف پول وارد کنید و دکمهٔ `Import wallet` را بزنید.



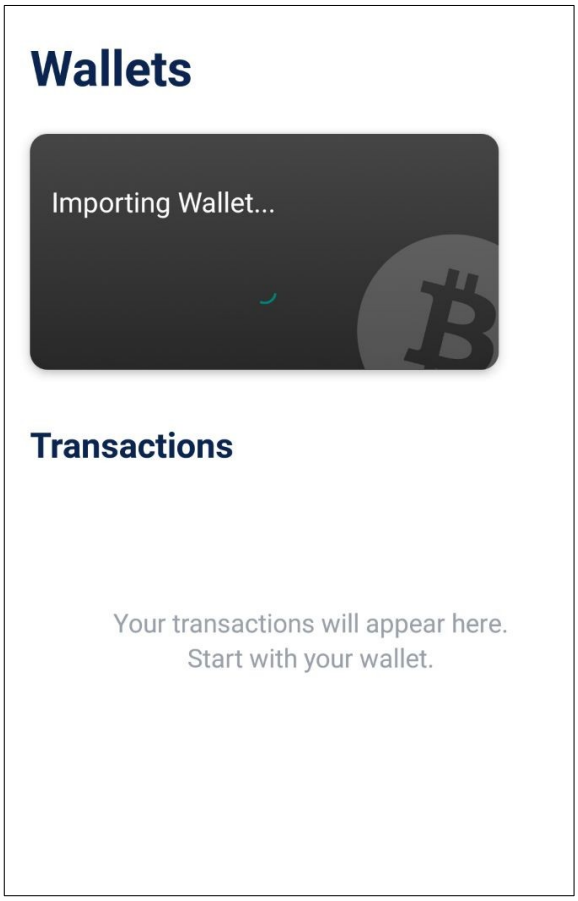


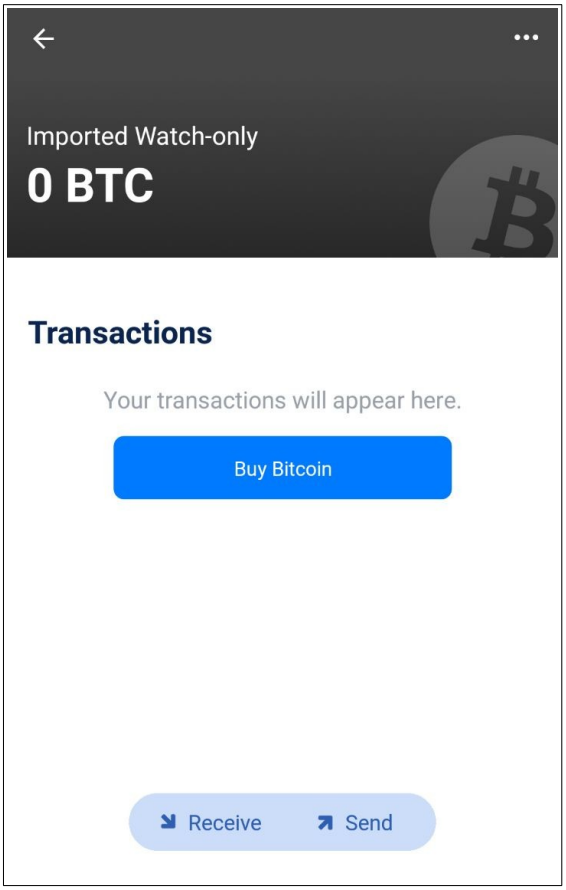
با زدن دکمهٔ `Scan or import a file` دوربین گوشی فعال می‌شود. برای ایجاد کیف پول، `xPub` نمایش داده شده بر روی نمایشگر `SeedSigner` را اسکن کنید.



در این مرحله `BlueWallet` اقدام به ایجاد کیف پول می‌کند و در نهایت پیامی مبنی بر موفقیت‌آمیز بودن این امر نمایش می‌دهد.

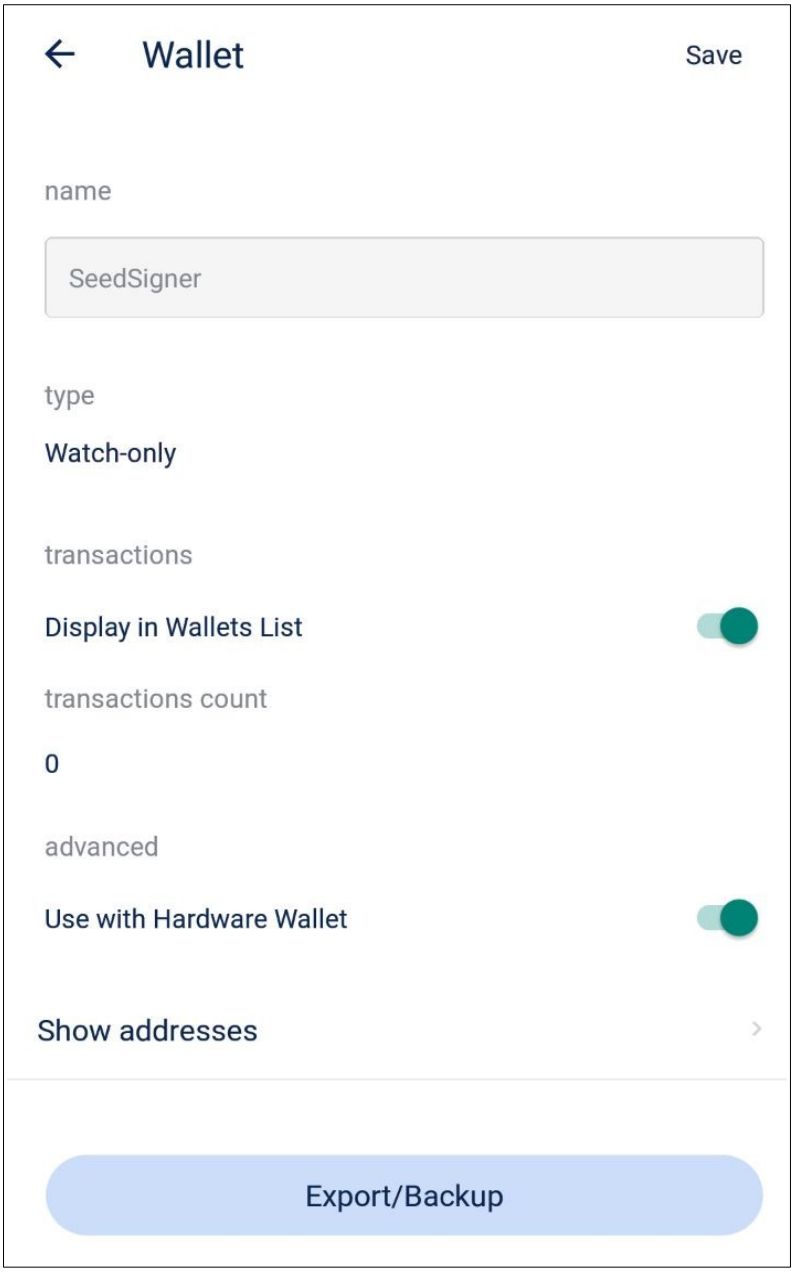
این کیف پول فقط قابلیت دریافت و نمایش موجودی بیت‌کوین شما را دارد و با توجه به در اختیار نداشتن کلید خصوصی، به‌صورت مستقل قادر به امضا کردن تراکنش‌های شما نیست.





مرحلهٔ چهارم: تنظیم کیف پول ایجاد شده برای فعال‌سازی قابلیت تعامل با یک کیف پول سخت‌افزاری

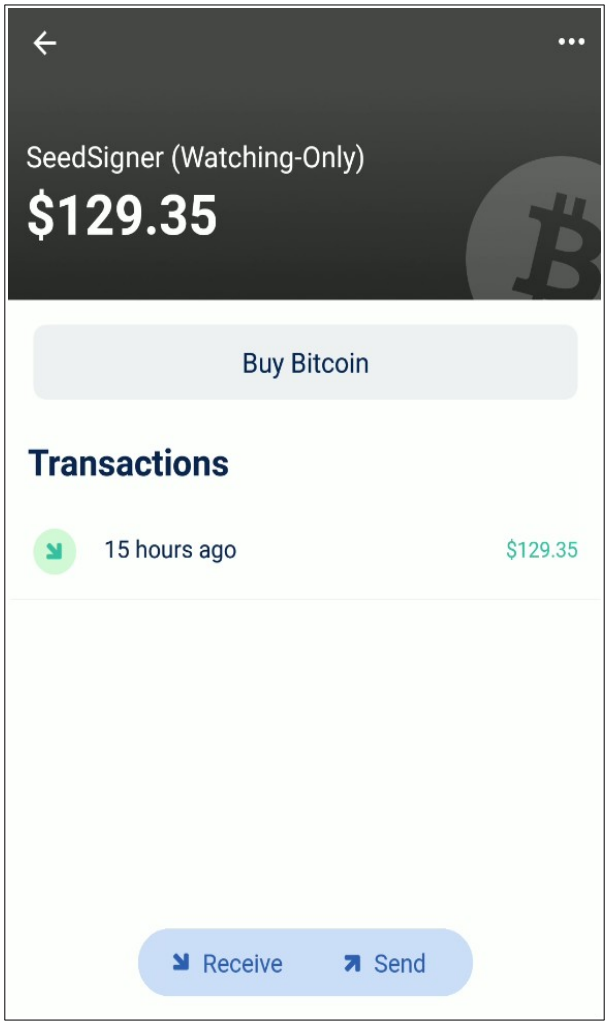
برای این منظور با زدن روی دکمهٔ سه نقطه‌ای که در بالای سمت راست کیف پول قرار دارد به بخش تنظیمات بروید و گزینهٔ `Use with Hardware Wallet` را فعال کنید.



مرحلهٔ پنجم: ارسال بیت‌کوین به کیف پول ایجاد شده

دقت کنید: قبل از ارسال بیت‌کوین به این کیف پول از در اختیار داشتن کلمات بازیابی که روی دستگاه SeedSigner شما تولید شده است، اطمینان حاصل کنید. اگر کلید خصوصی تولید شده را در اختیار نداشته باشید، همهٔ بیت‌کوین‌هایی که به آدرس‌های این کیف پول ارسال می‌شود را از دست خواهید داد.

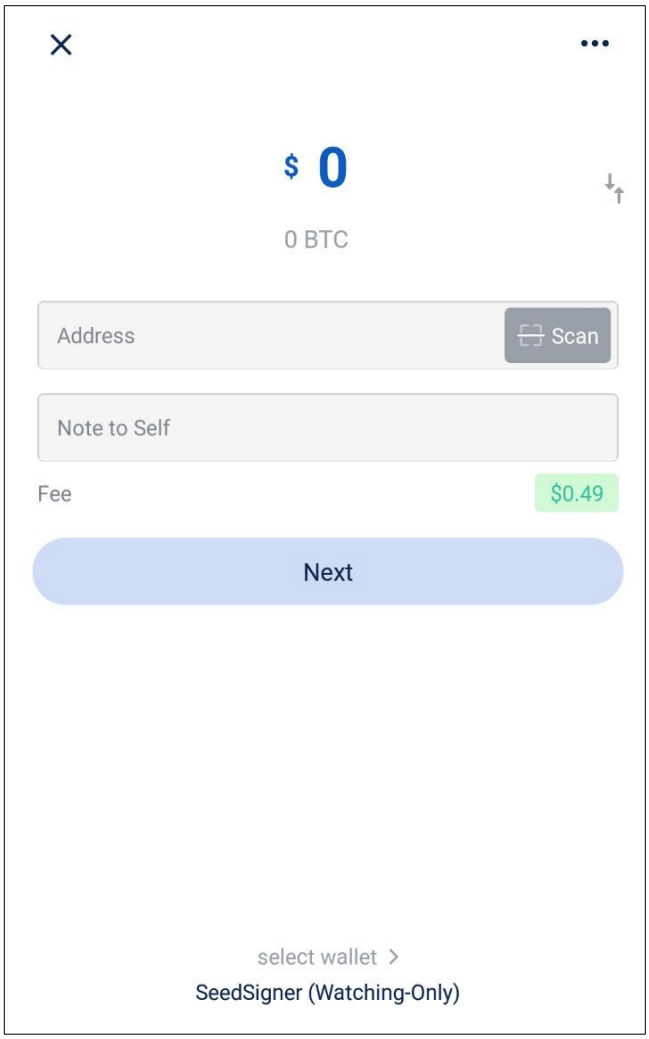
دکمهٔ Receive یا «دریافت» را بزنید تا یک آدرس بیت‌کوین تولید و نمایش داده شود.



مرحلهٔ پایانی: انتقال بیت‌کوین از کیف پول BlueWallet و امضای تراکنش در تعامل با SeedSigner

بعد از زدن روی دکمهٔ Send یا «ارسال»، صفحهٔ جدیدی باز می‌شود. آدرس مقصد، کارمزد تراکنش، و مقدار بیت‌کوین را در آن وارد کنید و روی دکمهٔ Next بزنید.

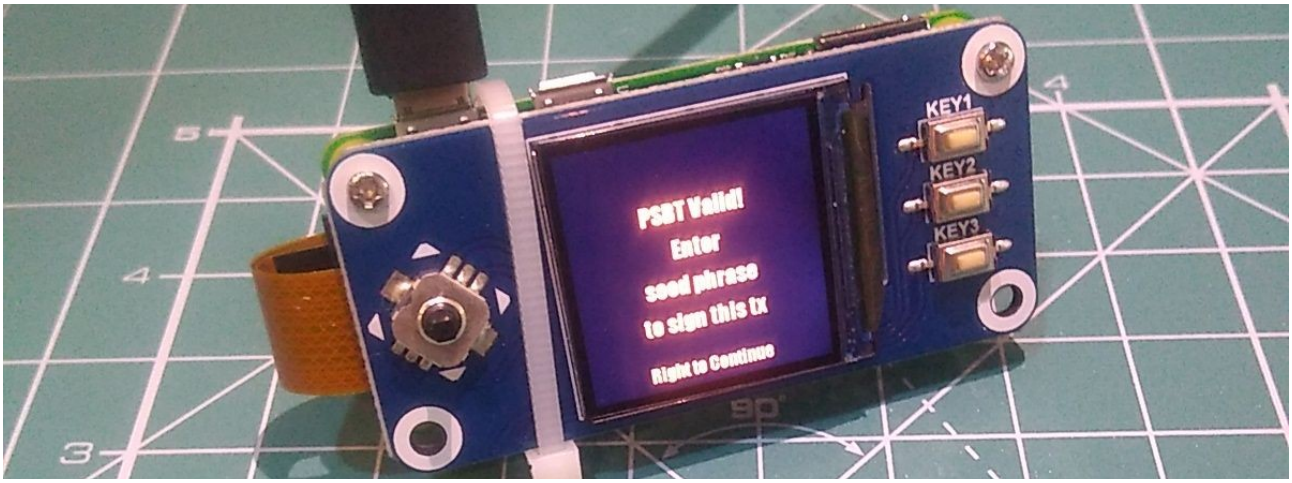
کیف پول BlueWallet با اطلاعاتی که در اختیار دارد، یک تراکنش بدون امضا[1] تولید، و آن را به‌صورت یک کُد QR نمایش می‌دهد. دستگاه SeedSigner با توجه به در اختیار داشتن کلید خصوصی، قادر است این تراکنش را امضاء کند.



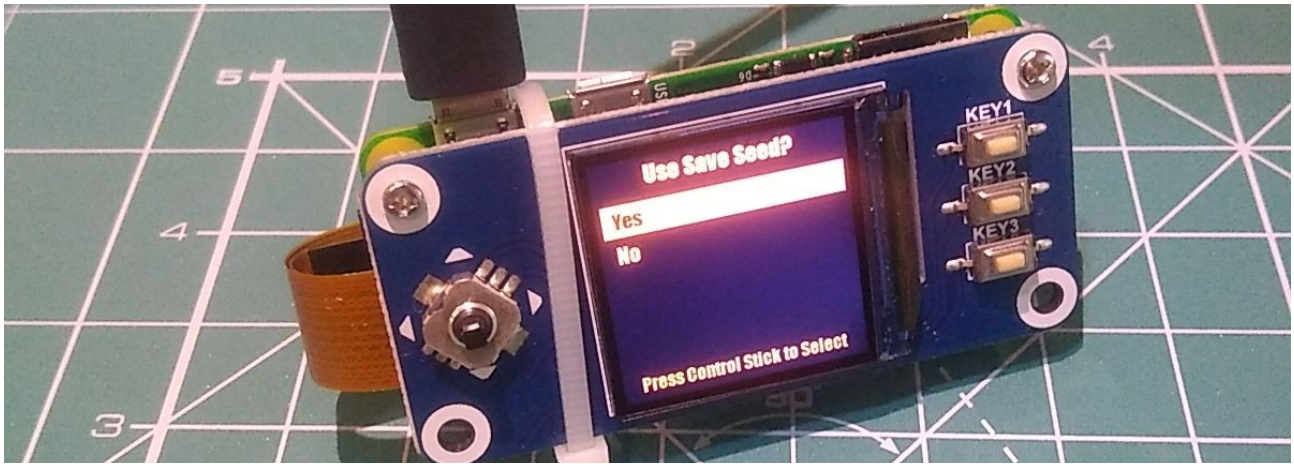
1 Partially Signed Bitcoin Transaction (PSBT)

در منوی اصلی SeedSigner روی گزینهٔ Scan QR کلیک، و کُد QR نمایش داده شده بر روی کیف پول BlueWallet را با دوربین دستگاه اسکن کنید.

در صورتی که این مرحله با موفقیت انجام شود، دستگاه پیامی مبنی بر معتبر بودن PSBT اسکن شده به شما نمایش می‌دهد.



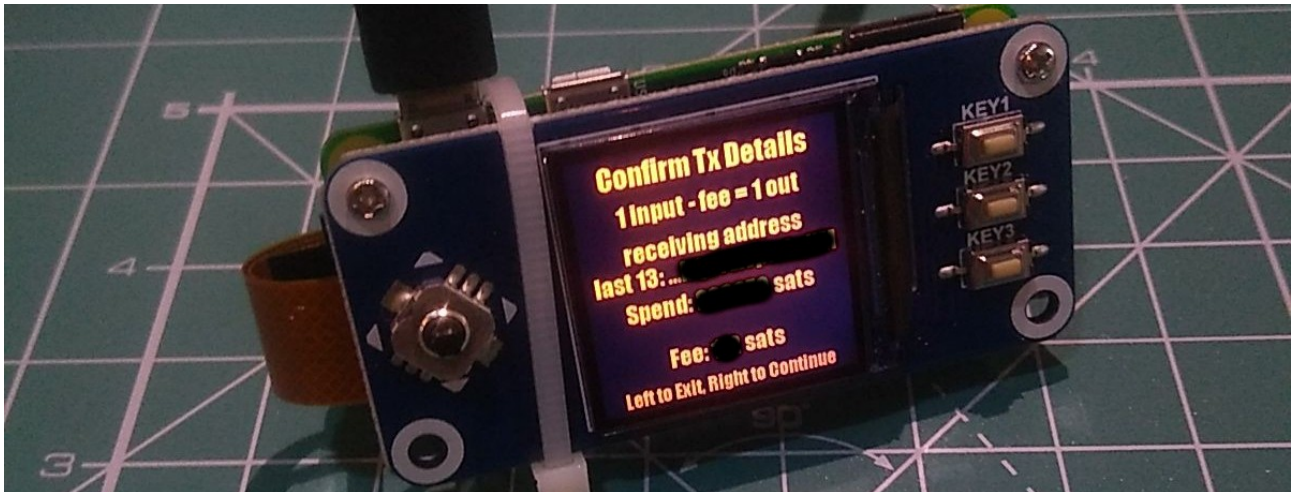
سپس کلید خصوصی ذخیره شده در دستگاه را انتخاب کنید.



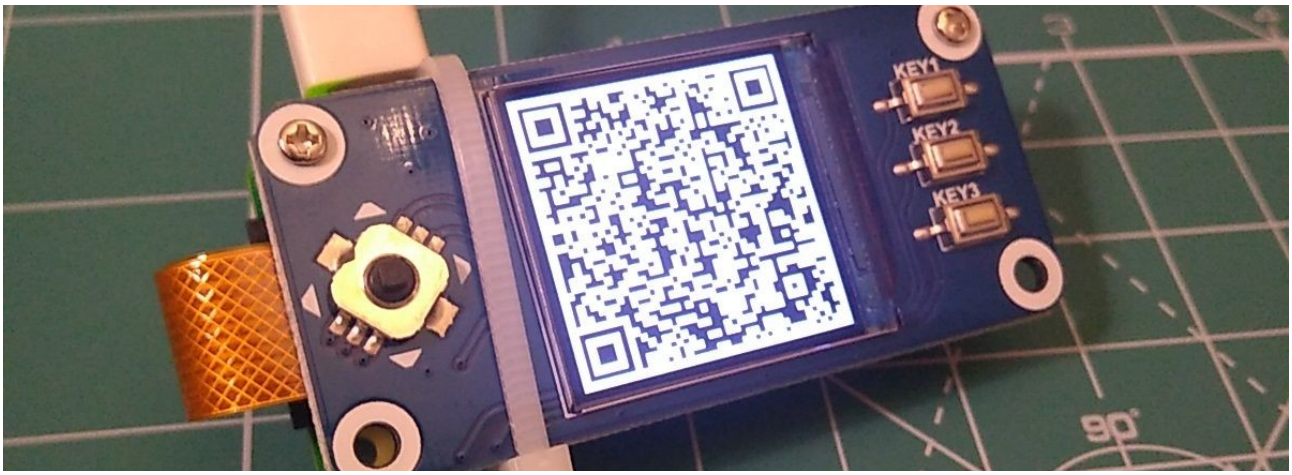
دستگاه در این مرحله امکان وارد کردن پسفریز[1] را به شما می‌دهد. در صورتی که در زمان تولید کلید خصوصی پسفریز تعیین کرده‌اید، در این مرحله همان مقدار را وارد کنید. در غیر این صورت با انتخاب گزینهٔ No به مرحلهٔ بعد بروید.

1 Passphrase

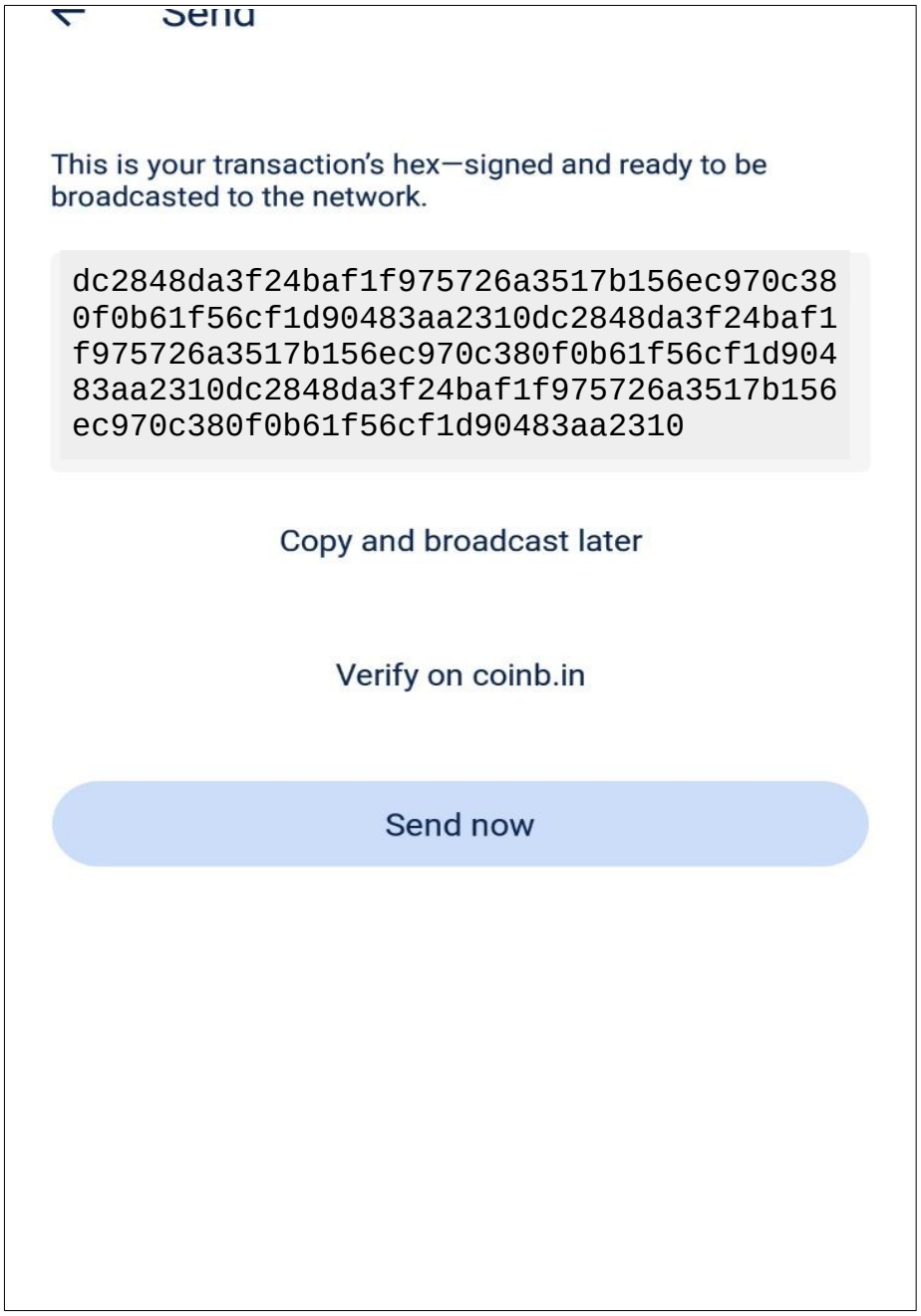
در این مرحله SeedSigner قبل از امضاء تراکنش از شما می‌خواهد اطلاعات مربوط به این تراکنش را بررسی و در صورت تأیید به مرحلهٔ بعد بروید. در این قسمت می‌توانید حروف پایانی آدرس، مقدار بیت‌کوین در حال انتقال، و کارمزدی که برای تراکنش تعیین شده را بازبینی کنید. در صورت صحیح بودن اطلاعات می‌توانید با فشار دادن جوی‌استیک به سمت راست، تراکنش را امضاء کنید.



پس از اتمام کار، SeedSigner مجموعه‌ای از کُدهای QR را به‌صورت انیمیشن بر روی LCD به نمایش درمی‌آورد. در این مرحله می‌بایست بر روی کیف پول BlueWallet دکمهٔ Scan Signed Transaction را بزنید و با استفاده از دوربین تلفن همراه خود، کُدهای QR نمایش داده شده بر روی LCD دستگاه را اسکن کنید.



در صورت موفقیت‌آمیز بودن این مرحله، روی کیف پول BlueWallet صفحه‌ای جدید باز می‌شود و اطلاعات تراکنش امضاء شده را نمایش می‌دهد. برای انتشار[1] این تراکنش بر روی شبکهٔ بیت‌کوین، دکمهٔ Send now را بزنید. کیف پول BlueWallet تراکنش شما را به شبکهٔ بیت‌کوین ارسال، و پیام موفقیت‌آمیز بودن آن را نمایش می‌دهد.



1 Broadcast

این راهنما توسط یکی از مخاطبان محترم سایت که به موضوعات حریم خصوصی و روش کار ایزوله با کیف پول‌ها علاقه‌مند است تهیه شده، و بازبینی و صفحه‌بندی آن توسط سایت منابع فارسی صورت گرفته است.

منابع فارسی بیت‌کوین
ویراست اول
پاییز ۱۴۰۰