

ایجاد امن کیف پول تک امضایی (Native Segwit (P2WPKH) با استفاده از Sparrow، Electrum و Seed Signer

ابزارهای مورد نیاز:

- (۱) ۱ عدد لپتاپ متصل به اینترنت با سیستم عامل لینوکس و مجهز به دوربین که bitcoin core روی آن نصب شده و با آخرین وضعیت شبکه بیتکوین همگام باشد. این لپتاپ میبایست دارای کیف پول های Sparrow و Electrum باشد و کیف پول Sparrow در آن به bitcoin core نصب شده روی لپتاپ متصل باشد.
- (۲) ۱ عدد لپتاپ ایزوله با پردازنده intel و مجهز به دوربین که یا جدید بوده یا سابقه مشخص و قابل اعتمادی داشته باشد و کارت های شبکه و بی سیم اش (wifi و bluetooth) قابل جدا شدن باشند و جدا شده باشند. باتری این لپتاپ میبایست سالم و کاملاً شارژ شده باشد تا در مراحل کار نیازی به اتصال به شبکه برق نداشته باشد. باتری این لپتاپ میبایست قابل تعویض باشد. این لپتاپ ایزوله نمیبایست هیچگاه بعد از این، برای کاری به جز اجرای پروتکل حاضر به کار گرفته شود. در صورت نیاز به اجرای مجدد این پروتکل و قصد استفاده مجدد از این لپتاپ، این لپتاپ میبایست پس از پایان کار در پاکت امنیتی قرار گرفته و در محل امنی نگهداری شود که در دسترس کسی جز عملگر قرار نداشته باشد.
- (۳) ۱ عدد فلش usb به ظرفیت حداقل ۸ گیگابایت که میبایست نو و باز نشده باشد. این فلش را از محلی معتبر تهیه کنید. توجه کنید که port این فلش با هردو لپتاپ همخوان باشد.
- (۴) اتصال اینترنت که با سیم LAN قابل اتصال به لپتاپ متصل به اینترنت (۱) باشد.
- (۵) ۱ عدد گوشی موبایل که از طریق شبکه همراه به اینترنت متصل باشد. توجه کنید که این گوشی نمیبایست در زمان انجام فرآیند به اینترنت موجود در محل (۴) متصل باشد.
- (۶) ۱ عدد seed signer به همراه SD card حاوی image اجرا کننده seed signer.
- (۷) ۱ عدد power bank یا منبع تغذیه پورتابل جهت تأمین برق seed signer.
- (۸) ۱ سیم رابط usb به micro-usb جهت اتصال seed signer (۶) به منبع تغذیه (۷).
- (۹) ۱ دستگاه چاپگر.
- (۱۰) ۱ عدد seed plate تیتانیومی.
- (۱۱) ۱ عدد ماژیک.
- (۱۲) ۱ عدد center punch یا سمبه اتوماتیک.
- (۱۳) ۱ عدد فندک.
- (۱۴) ۲ عدد خودکار روان یا روان نویس که بتوانید بدون فشار آوردن زیاد با آن بنویسید.
- (۱۵) چند برگ کاغذ معمولی آتش گیر.
- (۱۶) ۱ ظرف برای آتش زدن کاغذ.
- (۱۷) فضای ایزوله و امن و مجزا که فاقد دید از بیرون یا دوربین بوده و قابل قفل کردن نیز باشد. این فضا میبایست فاقد سیستم اطفای حریق باشد یا سیستم اطفای حریق آن موقتاً غیرفعال شده باشد.
- (۱۸) فضای معمولی که دارای اتصال اینترنت باشد.
- (۱۹) مقداری بیتکوین در آدرسی تحت کنترل عملگر.
- (۲۰) یک passphrase که داخل یک پاکت امن قرار دارد.

نامتغیرها:

- (۲۱) لپ‌تاپ ایزوله (۲) می‌بایست صرفاً در فضای ایزوله (۱۷) روشن شده و کار کند.
- (۲۲) لپ‌تاپ ایزوله (۲) نمی‌بایست در هنگامی که روشن است به برق متصل شود.
- (۲۳) لپ‌تاپ متصل به اینترنت (۱) می‌بایست صرفاً در فضای معمولی (۱۸) روشن شده و کار کند.

مراحل ایجاد کیف پول:

(۲۴) اجسام زیر را در فضاهای مشخص شده قرار دهید. لپ‌تاپ ایزوله را در حالی که خاموش است به شارژ وصل کنید.

فضای ایزوله		فضای معمولی	
خاموش.	لپ‌تاپ ایزوله	خاموش.	لپ‌تاپ متصل به اینترنت
خاموش.	Seed signer	آکبند.	فلش
داخل seed signer.	SD card مربوط به seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
نا متصل.	Power bank	موجود.	روان‌نویس
نا متصل.	سیم رابط usb به micro-usb	خاموش.	چاپگر
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان‌نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		

(۲۵) لپ‌تاپ متصل به اینترنت را به روز رسانی کنید. برای این کار مطمئن شوید که این لپ‌تاپ به اینترنت متصل است. سپس ترمینال را باز کنید و دستورهای زیر را وارد کنید و منتظر بمانید تا به‌روزرسانی‌ها انجام شوند.

```
sudo apt-get update
```

```
sudo apt-get upgrade -y
```

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله		فضای معمولی	
خاموش.	لپ‌تاپ ایزوله	روشن.	لپ‌تاپ متصل به اینترنت
خاموش.	Seed signer	آکبند.	فلش
داخل seed signer.	SD card مربوط به seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
نا متصل.	Power bank	موجود.	روان‌نویس
نا متصل.	سیم رابط usb به micro-usb	خاموش.	چاپگر
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان‌نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		

(۲۶) سیستم عامل Tails OS را از طریق لپ‌تاپ متصل به اینترنت از آدرس <https://tails.net/install/download/index.en.html> دانلود کنید. فلش را از حالت آکبند خارج کنید و طبق دستورالعملی که در همان صفحه شرح داده شده است، Tails را روی فلش نصب کنید. اگر فایل دریافت شده، مطابق دستورالعمل صحت سنجی نشد، **پروتکل را متوقف کنید** در صورت صحت فایل، پس از نصب آن مطابق دستورالعمل، از طریق نرم‌افزار Disks در لپ‌تاپ متصل به اینترنت، فضای خالی موجود در فلش را به یک پارتیشن تبدیل کنید.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
خاموش.	لپ تاپ ایزوله	روشن.	لپ تاپ متصل به اینترنت
خاموش.	Seed signer	متصل به لپ‌تاپ متصل به اینترنت.	فلش
داخل seed signer.	SD card مربوط به seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
نا متصل.	Power bank	موجود.	روان نویس
نا متصل.	سیم رابط usb به micro-usb	خاموش.	چاپگر
خام.	seed plate نیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		

(۲۷) کیف پول Sparrow را از طریق لپ‌تاپ متصل به اینترنت، از آدرس [/https://www.sparrowwallet.com/download](https://www.sparrowwallet.com/download) دریافت کنید. نسخه‌ای که می‌بایست دریافت کنید، نسخه لینوکس (Ubuntu/Debian) **(Linux (Intel/AMD)** است. مطابق دستورالعمل ارائه شده در صفحه دانلود Sparrow، اصالت فایل دریافت شده را بررسی کنید. اگر اصالت فایل تایید شد، فایل deb. دریافت شده را در فضای پارتیشن‌ی که در (۲۶) روی فلش ایجاد کردید در کپی کنید. در غیر این صورت **پروتکل را متوقف کنید.**

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله			
خاموش.	لپ تاپ ایزوله	روشن.	لپ تاپ متصل به اینترنت
خاموش.	Seed signer	متصل به لپ‌تاپ متصل به اینترنت.	فلش
داخل seed signer.	SD card مربوط به seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
نا متصل.	Power bank	موجود.	روان‌نویس
نا متصل.	سیم رابط usb به micro-usb	خاموش.	چاپگر
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان‌نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		

(۲۸) فلش را از لپ‌تاپ متصل به اینترنت جدا کنید. لپ‌تاپ را قفل کنید. پیش از رفتن، با گوشی موبایل چک کنید که مدل لپ‌تاپ ایزوله چگونه می‌تواند از روی یک فلش usb بوت شود. سپس به همراه فلش به فضای ایزوله بروید.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
خاموش.	لپ‌تاپ ایزوله	قفل.	لپ‌تاپ متصل به اینترنت
خاموش.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
داخل seed signer.	SD card مربوط به seed signer	موجود.	روان‌نویس
نا متصل.	Power bank	خاموش.	چاپگر
نا متصل.	سیم رابط usb به micro-usb		
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان‌نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
نامتصل.	فلش		

(۲۹) اگر شارژ لپ‌تاپ ایزوله کامل شده است، آن را از برق جدا کنید. سپس فلش را به لپ‌تاپ ایزوله متصل کنید. لپ‌تاپ را روشن کنید و آن را روی سیستم عامل Tails OS بوت کنید. هیچگاه زمانی که لپ‌تاپ ایزوله به برق متصل است روشن‌اش نکنید.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
روشن.	لپ‌تاپ ایزوله	قفل.	لپ‌تاپ متصل به اینترنت
خاموش.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
داخل seed signer.	SD card مربوط به seed signer	موجود.	روان‌نویس
نا متصل.	Power bank	خاموش.	چاپگر
نا متصل.	سیم رابط usb به micro-usb		
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان‌نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ‌تاپ ایزوله.	فلش		

(۳۰) در صفحه نخست Tails OS روی علامت + زیر Additional Settings کلیک کنید. سپس روی Administration Password دبل کلیک کنید. سپس یک رمز دلخواه که می‌بایست در طول پروتکل به خاطر سپارید را در دو فیلد Administration Password و Confirm وارد کنید. سپس روی دکمه Add که در صورت یکسان بودن ورودی های دو فیلد مذکور فعال می‌شود کلیک کنید. سپس که به صفحه قبلی بازمی‌گردیم، روی Start Tails کلیک کنید. بعد از چند لحظه Tails آماده کار می‌شود.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
روشن.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
خاموش.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
داخل seed signer.	SD card مربوط به seed signer	موجود.	روان نویس
نا متصل.	Power bank	خاموش.	چاپگر
نا متصل.	سیم رابط usb به micro-usb		
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		

(۳۱) روی Places در نوار بالایی صفحه دسکتاپ Tails کلیک کنید و Computer را انتخاب نمایید. در نوار کناری پنجره‌ای که باز می‌شود، اگر پارتیشن موضوع (۲۶) به درستی ایجاد شده باشد، زیر Trash یک Volume خواهید دید که محل نگهداری فایل نصب Sparrow است. روی xxGB Volume کلیک کنید. دیالوگ وارد کردن رمز پدیدار می‌شود. رمز تعیین شده در (۳۰) را وارد نمایید. درایو باز شده و فایل deb. نصب Sparrow نمایان می‌گردد. داخل پنجره‌ای که باز شده کلیک راست کنید و Open in Terminal را انتخاب کنید. در ترمینال این دستور را وارد کنید:

```
sudo dpkg -i ./sparrow_XXXXXX_amd64.deb
```

رمز خود (۳۰) را در پرامپت وارد کنید. Sparrow نصب می‌شود. بعد از اتمام نصب، ترمینال را ببندید. پنجره درایو را نیز ببندید.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
روشن.	لپ‌تاپ ایزوله	قفلی.	لپ‌تاپ متصل به اینترنت
خاموش.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
داخل seed signer.	SD card مربوط به seed signer	موجود.	روان‌نویس
نا متصل.	Power bank	خاموش.	چاپگر
نا متصل.	سیم رابط usb به micro-usb		
خام.	seed plate نیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان‌نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ‌تاپ ایزوله.	فلش		

(۳۲) از نوار بالای Tails روی Applications کلیک کنید. از گزینه های سمت چپ، Internet را انتخاب کنید. می بایست Sparrow را در گزینه های سمت راست ببینید. روی آن کلیک کنید. پنجره Sparrow باز می شود. در اولین پنجره روی Next کلیک کنید. در دومین پنجره روی Next کلیک کنید. در سومین پنجره روی Next کلیک کنید. در چهارمین پنجره روی Later or Offline Mode کلیک کنید. در پنجره ای که باز می شود مطمئن شوید که Policy Type روی Single Signature و Script Type روی Native Segwit (P2WPKH) قرار دارند. در قسمت Descriptor می بایست نوشته wpkh(Keystore) را مشاهده کنید. در قسمت Keystores روی New or Imported Software Wallet کلیک کنید. در نوار آبی رنگ سمت چپ، Software Wallet را انتخاب کنید. در قسمت سمت راست، مقابل قسمت (BIP۳۹) Mnemonic Words، ۲۴ Words Use را انتخاب کنید و رویش کلیک کنید. سپس روی Generate New کلیک کنید. جاهای خالی با ۲۴ کلمه پر شدند. روی باکس رو به روی Use passphrase? کلیک کنید. در پنجره هشداری که باز می شود روی Yes کلیک کنید و سپس در فضای تایپ ایجاد شده روی Passphrase:، passphrase موضوع (۲۰) را وارد کنید.

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله		فضای معمولی	
روشن.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
خاموش.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
داخل seed signer.	SD card مربوط به seed signer	موجود.	روان نویس
نا متصل.	Power bank	خاموش.	چاپگر
نا متصل.	سیم رابط usb به micro-usb		
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		

(۳۳) یک برگ کاغذ را روی یک سطح ترجیحاً شیشه ای قرار دهید و ۲۴ کلمه را با دقت و به ترتیب و با یادداشت شماره هایشان روی کاغذ یادداشت کنید. این کلمات را به نمونیک نام خواهیم برد.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
روشن.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
خاموش.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
داخل seed signer.	SD card مربوط به seed signer	موجود.	روان نویس
نا متصل.	Power bank	خاموش.	چاپگر
نا متصل.	سیم رابط usb به micro-usb		
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		

(۳۴) روی Confirm Backup... کلیک کنید و سپس روی Re-enter Words... کلیک کنید. سپس تمام کلمات را به همان ترتیبی که روی کاغذ نوشتید در جاهای خالی وارد کنید. سپس روی Confirm Backup... کلیک کنید. اگر کلمات را اشتباه وارد کرده باشید، با نوشته قرمز رنگ Import Error در صفحه بعد مواجه می شوید. در این صورت دوباره روی دکمه Use ۲۴ Words... کلیک کنید و مراحل را از (۳۲) تکرار کنید. توجه کنید که با تکرار، کلمات جدیدی برایتان تولید می شوند. کاغذ قبلی را که اشتباه یادداشت یا وارد کرده بودید، پاره کنید و داخل ظرف آتش دان قرار دهید. اگر مکرراً با مشکل مواجه می شوید، **پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.** اگر کلمات را درست وارد کرده باشید، در صفحه بعد دکمه Import Keystore آبی می شود. در باکس نوشتاری زیر قسمت قبل، این نوشته را مشاهده می کنید: m/84'/0'/0' مطلقاً این نوشته را دستکاری نکنید. روی Import Keystore کلیک کنید. در پنجره ای که باز می شود passphrase (۲۰) را وارد کنید و روی Ok کلیک کنید. اگر اشتباه وارد کنید، در صفحه بعد با نوشته قرمز Import Error و زیر نوشته Re-entered passphrase did not match مواجه می شوید. در این صورت دوباره روی Import Keystore کلیک کنید. اگر مجدداً و با دقت به passphrase این مقدار مورد قبول نبود، در (۳۲) مقدار را اشتباه وارد کرده بودید و می بایست از (۳۲) دوباره شروع کنید. اگر مکرراً با مشکل مواجه می شوید، **پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.** در صورت وارد کردن مقدار درست، به صفحه اصلی بر می گردید و این بار در قسمت Keystores یک سربرگ با نام BIP۳۹ مشاهده می کنید. در قسمت پایین، سمت راست، روی Apply کلیک کنید. نیازی نیست رمزی برای کیف پول وارد کنید. روی No Password کلیک کنید. اکنون می بایست کلیه آیکون های نوار آبی سمت راست در Sparrow فعال شده باشند.

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله		فضای معمولی	
لپ تاپ ایزوله	روشن.	لپ تاپ متصل به اینترنت	قفل.
Seed signer	خاموش.	گوشی موبایل	روشن و متصل به شبکه همراه.
SD card مربوط به seed signer	داخل seed signer.	روان نویس	موجود.
Power bank	نا متصل.	چاپگر	خاموش.
سیم رابط usb به micro-usb	نا متصل.		
seed plate تیتانیومی	خام.		
سمبه اتوماتیک	موجود.		
ماژیک	موجود.		
فندک	موجود.		
روان نویس	موجود.		
ظرف آتش دان	موجود.		
چند برگ کاغذ	موجود.		
چند پاکت امنیتی	موجود.		
پاکت حاوی passphrase	موجود و حساس.		
فلش	متصل به لپ تاپ ایزوله.		
یک برگ کاغذ حاوی نمونیک	موجود و حساس.		

(۳۵) سر usb سیم رابط (۸) را به power bank و سر micro usb آن را به پورت micro usb منتهی الیه سمت چپ seed signer متصل کنید. کمی صبر کنید تا seed signer روشن شود و پیغام سبز رنگ You can remove the SD card now در قسمت پایین صفحه نمایشش ظاهر شود. سپس SD card را از seed signer خارج کنید.

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله		فضای معمولی	
لپ تاپ متصل به اینترنت	قفلی.	لپ تاپ ایزوله	روشن.
گوشی موبایل	روشن و متصل به شبکه همراه.	Seed signer	روشن.
روان نویس	موجود.	SD card مربوط به seed signer	خارج از seed signer.
چاپگر	خاموش.	Power bank	متصل.
		سیم رابط usb به micro-usb	متصل.
		seed plate تیتانیومی	خام.
		سمبه اتوماتیک	موجود.
		ماژیک	موجود.
		فندک	موجود.
		روان نویس	موجود.
		ظرف آتش دان	موجود.
		چند برگ کاغذ	موجود.
		چند پاکت امنیتی	موجود.
		پاکت حاوی passphrase	موجود و حساس.
		فلش	متصل به لپ تاپ ایزوله.
		یک برگ کاغذ حاوی نمونیک	موجود و حساس.

(۳۶) در صفحه اصلی seed signer، Seeds را انتخاب کنید. سپس گزینه ۲۴-word seed Enter را انتخاب کنید. حال تمام کلمات را به ترتیب از روی کاغذ (۳۳) به seed signer وارد کنید. در صفحه Finalize Seed، گزینه BIP-۳۹ Passphrase را انتخاب کنید. سپس passphrase (۲۰) را وارد نمایید. برای تایید، پایینترین کلید سمت راست seed signer که مقابلش در صفحه نمایش seed signer یک تیک سبز قرار دارد را بفشارید. در صفحه Verify Passphrase در seed signer، passphrase (۲۰) را مشاهده می کنید. مطمئن شوید که صحیح است. بالای دکمه Edit passphrase در seed signer دو عبارت مشاهده می کنید که با >> جدا شده اند. عبارت سمت راست می بایست با عبارتی که روی صفحه لپ تاپ ایزوله در قسمت Keystores، زیر برگه BIP۳۹، مقابل Master fingerprint مشاهده می کنید، یکسان باشد. اگر این دو یکی بودند دکمه Done در seed signer را انتخاب کنید و فشار دهید. اگر یکی نبودند seed signer را از کابل متصل به آن جدا کنید و مراحل را از (۳۵) مجدداً تکرار کنید. اگر باز هم یکی نبودند پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.

فضای ایزوله		فضای معمولی	
روشن.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
روشن.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
خارج از seed signer.	SD card مربوط به seed signer	موجود.	روان نویس
متصل.	Power bank	خاموش.	چاپگر
متصل.	سیم رابط usb به micro-usb		
خام.	seed plate نیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		

(۳۷) Seed signer را از کابل جدا کنید. سپس SD card محتوی seed signer را داخل محلش در دستگاه seed signer قرار دهید و seed signer را دوباره به کابل usb متصل به power bank متصل کنید. توجه کنید که می بایست از پورت منتهی الیه سمت چپ seed signer استفاده کنید. کمی صبر کنید تا seed signer روشن شود و پیغام سبز رنگ You can remove the SD card now در قسمت پایین صفحه نمایشش ظاهر شود. سپس SD card را از seed signer خارج کنید. در پنجره Sparrow در لپ تاپ ایزوله، در قسمت Keystore، در سربرگ BIP۳۹، در قسمت انتهایی، مقابل xpub / zpub یک رشته اعداد و حروف بلند می بینید که با xpub شروع می شود. در سمت دیگر این باکس حاوی حروف و اعداد، دو آیکون مشاهده می کنید. روی آیکون پایینی که دو فلش برعکس است کلیک کنید تا نوشته داخل باکس تغییر کند و با zpub شروع شود. سپس روی آیکون بالایی که نماد یک QR Code است کلیک کنید. یک QR Code نمایش داده می شود. در صفحه اصلی seed signer وارد قسمت Tools شوید. اولین گزینه که تصویر یک دوربین است و مقابلش New seed نوشته شده است را انتخاب کنید. می بایست خروجی دوربین seed signer را مشاهده کنید. دوربین seed signer را به صورت مناسب مقابل QR Code بگیرید و جوی استیک seed signer را برای عکس گرفتن فشار دهید. توجه کنید که تمام QR Code داخل تصویر وجود داشته باشد. حالا می بایست QR Code را روی صفحه seed signer ببینید. پنجره نمایش QR Code را در لپ تاپ ایزوله ببندید. در Sparrow در نوار آبی سمت چپ، روی Settings کلیک کنید. سپس روی گزینه Advanced... که در پایین سمت راست قرار دارد کلیک کنید. یک عدد دلخواه انتخاب کنید که می بایست روی یک برگ کاغذ یادداشت اش کنید. عدد مذکور را مقابل Gap limit: وارد کنید. سپس روی Close کلیک کنید. حال روی دکمه Apply در پایین سمت راست کلیک کنید. پنجره ای باز می شود که در مورد رمز کیف پول است. روی No Password کلیک کنید. سپس از نوار آبی سمت چپ، گزینه Addresses را انتخاب کنید. زیر Receive Addresses تعدادی آدرس بیتکوینی مشاهده می کنید. به انتهای لیست بروید و آخرین آدرس را روی همان برگه کاغذ یادداشت نمایید. گزینه Settings در نوار آبی رنگ سمت چپ Sparrow را انتخاب کنید و مقدار مقابل Master fingerprint: را روی همان کاغذ یادداشت نمایید. لپ تاپ ایزوله را قفل کنید.

وضعیت پس از انجام گام

فضای ایزوله		فضای معمولی	
قفل.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
روشن.	Seed signer	روشن و متصل به شبکه همراه.	گوشی موبایل
خارج از seed signer.	SD card مربوط به seed signer	موجود.	روان نویس
متصل.	Power bank	خاموش.	چاپگر
متصل.	سیم رابط usb به micro-usb		
خام.	seed plate تیتانیومی		
موجود.	سمبه اتوماتیک		
موجود.	ماژیک		
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		
موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint		

(۳۸) بدون اینکه seed signer را از power bank جدا کنید، seed signer و power bank و قطعه کاغذ حاوی Master fingerprint (۳۷) و SD card حاوی seed signer را بردارید. به همراه seed signer و power bank و قطعه کاغذ حاوی Master fingerprint و SD card حاوی seed signer از محیط ایزوله خارج شوید. محیط ایزوله را قفل کنید. توجه کنید که برگه کاغذ حاوی کلمات mnemonic و passphrase و کامپیوتر ایزوله در فضای ایزوله قرار دارند. این اجسام بسیار حساس هستند و دسترسی غیر مجاز به آنها به معنی از دست رفتن بیتکوین‌ها است. پس اطمینان حاصل کنید که کسی به جز خودتان تا پایان فرایند وارد اتاق ایزوله نمی‌شود.

وضعیت پس از انجام گام			
فضای معمولی		فضای ایزوله (قفل شده)	
لپ تاپ متصل به اینترنت	قفل.	لپ تاپ ایزوله	قفل.
گوشی موبایل	روشن و متصل به شبکه همراه.	seed plate تیتانیومی	خام.
روان نویس	موجود.	سمبه اتوماتیک	موجود.
چاپگر	خاموش.	ماژیک	موجود.
Seed signer	روشن.	فندک	موجود.
SD card مربوط به seed signer	خارج از seed signer.	روان نویس	موجود.
Power bank	متصل.	ظرف آتش دان	موجود.
سیم رابط usb به micro-usb	متصل.	چند برگ کاغذ	موجود.
یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint	موجود.	چند پاکت امنیتی	موجود.
		پاکت حاوی passphrase	موجود و حساس.
		فلش	متصل به لپ تاپ ایزوله.
		یک برگ کاغذ حاوی نمونیک	موجود و حساس.

(۳۹) لپ‌تاپ متصل به اینترنت را باز کنید و Electrum را باز کنید. اگر قبلاً کیف پولی در Electrum ساخته بوده باشید، صفحه‌ای نمایش داده می‌شود که در آن می‌بایست روی Create New Wallet کلیک کنید. اگر چنین نباشد، Electrum در همان ابتدا وارد صفحه درخواست نام برای کیف پول جدید خواهد شد. نامی برای کیف پول انتخاب کنید. روی Next کلیک کنید. گزینه Standard wallet را انتخاب کنید. سپس روی Next کلیک کنید. گزینه Use a master key را انتخاب کنید. صفحه‌ای باز می‌شود که در گوشه پایین سمت راست آن آیکون یک دوربین وجود دارد. روی آیکون دوربین کلیک کنید. حال seed signer را در حالی که QR Code عکس گرفته شده از صفحه لپ‌تاپ ایزوله (۳۷) را نمایش می‌دهد، مقابل دوربین لپ‌تاپ متصل به اینترنت قرار دهید. بعد از اسکن، نوشته‌ای که با zpub شروع می‌شود را در باکس نوشتاری مشاهده خواهید نمود. روی Next کلیک کنید. رمزی را برای کیف پول انتخاب کنید که می‌بایست در طول پروتکل به یادش داشته باشید. روی Finish کلیک کنید و اجازه دهید باکس مقابل Encrypt wallet file چک شده باقی بماند. با یک پیغام هشدار مواجه خواهید شد که می‌گوید کیف پول شما watch-only است. روی Ok کلیک کنید. Seed signer را از سیم اتصالش جدا کنید. حال در منوی بالای Electrum منوی View را انتخاب کنید. اگر گزینه‌های Console و Addresses تیک نخورده بودند، روی آنها کلیک کنید تا هردو تیک داشته باشند. حال به صفحه اصلی الکترا بازگردید. می‌بایست یک سربرگ به نام Console مشاهده کنید. روی آن کلیک کنید. چیزی شبیه به Terminal خواهید دید. حال عدد دلخواه روی کاغذ (۳۷) را معادل x فرض کنید. حال دستور زیر را در قسمت شبیه خط فرمان در Console بعد از علامت >>> وارد کنید.

wallet.change_gap_limit(x)

سپس Enter را فشار دهید. عبارت True را مشاهده خواهید کرد. حالا وارد قسمت Addresses در Electrum شوید. لیستی از آدرس‌ها را مشاهده خواهید نمود. به انتهای لیست بروید. آخرین آدرسی که مقابلش عبارت receiving نوشته شده است را پیدا کنید. حال این آدرس را با آدرسی که یادداشت کرده بودید مقایسه کنید. این دو می‌بایست یکی باشند. اگر چنین نبود پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله (قفل شده)			
قفلی.	لپ‌تاپ ایزوله	روشن.	لپ‌تاپ متصل به اینترنت
خام.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان‌نویس
موجود.	ماژیک	خاموش.	چاگر
موجود.	فندک	خاموش.	Seed signer
موجود.	روان‌نویس	خارج از seed signer.	SD card مربوط به seed signer
موجود.	ظرف آتش دان	نا متصل.	Power bank
موجود.	چند برگ کاغذ	نا متصل.	سیم رابط usb به micro-usb
موجود.	چند پاکت امنیتی	موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ‌تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		

(۴۰) سربرگ Receive در صفحه اصلی Electrum را انتخاب کنید. روی دکمه Create Request کلیک کنید. در سمت راست صفحه‌ای که ظاهر می‌شود، یک باکس مشاهده می‌کنید. در بالای باکس دکمه‌ای که دارای یک آیکن هم هست مشاهده می‌کنید. اگر روی دکمه نوشته شده Bitcoin URI، روی آن کلیک کنید تا به Address تغییر کند. در این حالت یک آدرس در باکس نوشتاری مشاهده خواهید نمود. می‌توانید روی دکمه سمت راست Address که آیکن یک QR Code را دارد کلیک کنید تا QR Code آدرس در باکس نمایش داده شود. حال از طریق یک کیف پول موبایلی یا هر طریق دیگری، مقدار کمی بیتکوین به آدرسی که در باکس نمایش داده شده است واریز کنید. پس از واریز، وارد سربرگ History در صفحه اصلی Electrum شوید و منتظر بمانید تا دریافت این مقدار در کیف پول تایید شود.

وضعیت پس از انجام گام			
فضای ایزوله (قفل شده)		فضای معمولی	
قفل.	لپ تاپ ایزوله	روشن.	لپ تاپ متصل به اینترنت
خام.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان نویس
موجود.	ماژیک	خاموش.	چاپگر
موجود.	فندک	خاموش.	Seed signer
موجود.	روان نویس	خارج از seed signer.	SD card مربوط به seed signer
موجود.	ظرف آتش دان	نا متصل.	Power bank
موجود.	چند برگ کاغذ	نا متصل.	سیم رابط usb به micro-usb
موجود.	چند پاکت امنیتی	موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		

(۴۱) هنگامی که مشاهده نمودید این مقدار به کیف پولتان در لپ‌تاپ متصل به اینترنت که در Electrum مشاهده‌اش می‌کنید واریز شد، کیف پول Sparrow را در لپ‌تاپ متصل به اینترنت باز کنید. از منوی فایل Sparrow گزینه New Wallet را انتخاب کنید. نامی برای کیف پول انتخاب کنید. در صفحه‌ای که باز می‌شود، گزینه xPub / Watch Only را در قسمت Keystores و تحت سربرگ ۱ Keystore انتخاب کنید. سپس به کیف پول Electrum که در لپ‌تاپ متصل به اینترنت باز است برگردید. از نوار بالای Electrum منوی Wallet را انتخاب کنید. سپس Information را انتخاب کنید. از پنجره‌ای که باز می‌شود، نوشته‌های موجود در باکس زیر Master Public Key را که با zpub شروع می‌شود، کپی کنید. سپس پنجره را ببندید. به Sparrow بازگردید. داخل باکس مقابل xpub کلیک راست کنید و Paste را انتخاب کنید تا همان نوشته‌ها را مشاهده نمایید. مقابل Derivation: این عبارت را تایپ کنید: 'm/۸۴/'/۰'. حال مطمئن شوید که Policy Type روی Single Signature قرار دارد و Script Type هم روی Native Segwit (P2WPKH) قرار دارد. در مقابل Master fingerprint: هم مقداری را که روی کاغذ یادداشت کرده‌اید وارد کنید. روی دکمه Apply کلیک کنید. یک Password برای کیف پول انتخاب کنید که می‌بایست تا انتهای پروتکل به خاطرش بسپارید. روی Set Password کلیک کنید. می‌بایست بتوانید تراکنش ورودی قبلی به کیف پولان را در Sparrow هم ببینید. حال گزینه Receive در منوی آبی رنگ سمت چپ صفحه را انتخاب کنید. روی آیکنی که انتهای سمت راست باکس حاوی آدری در مقابل Address قرار دارد کلیک کنید تا آدرس دریافت کپی شود. سپس روی Send از منوی آبی سمت چپ Sparrow کلیک کنید. در باکس مقابل Pay to: کلیک راست کنید و آدرس را در آن paste کنید. یک مقدار دلخواه در مقابل Label: وارد کنید. مقداری متناسب با موجودی کیف پول که بتوانید با باقی‌مانده آن Fee را نیز پرداخت کنید در Amount وارد کنید. مقدار fee را نیز انتخاب نمایید. سپس روی >> Create Transaction در قسمت پایین سمت راست کلیک کنید. سپس روی Finalize Transaction for Signing کلیک کنید. حال در ردیف دکمه‌های پایین روی Show QR کلیک کنید. حال SD card حاوی seed signer را در دستگاه seed signer قرار دهید و دستگاه را به power bank متصل کنید تا روشن شود. هنگامی که پیغام You can remove the SD card now روی صفحه ظاهر شد، SD card را از دستگاه seed signer خارج کنید. حالا در seed signer گزینه Scan را انتخاب کنید و دوربین seed signer را جهت اسکن QR Code تولید شده توسط Sparrow، رو به روی صفحه لپ‌تاپ متصل به اینترنت بگیرید تا اسکن انجام شود. هنگامی که اسکن به درستی انجام شود، در دستگاه seed signer وارد صفحه‌ای خواهید شد که عنوان Select Signer دارد. بدون اینکه دستگاه seed signer را از power bank جدا کنید، آن را کنار بگذارید. پنجره حاوی QR Code را ببندید. روی یک برگ کاغذ، حداقل ۱۰ کاراکتر اول مقابل Txid: که زیر Transaction قرار دارد را یادداشت کنید. دوباره چک کنید که مطمئن شوید درست یادداشت کرده‌اید. در همان برگ کاغذ، بخش‌هایی از ابتدا و انتهای آدرس‌های ورودی و خروجی تراکنش را که در قسمت میانی صفحه Sparrow نمایش داده شده است، به همراه مقادیر هریک با ذکر واحد سنجش یادداشت کنید. این مقادیر با نکه داشتن نشانگر موس روی ورودی و خروجی های تراکنش در Sparrow قابل مشاهده هستند. دوباره چک کنید که درست یادداشت کرده باشید. سپس لپ‌تاپ متصل به اینترنت را قفل کنید.

وضعیت پس از انجام گام

فضای ایزوله (قفل شده)		فضای معمولی	
قفل.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
خام.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان نویس
موجود.	ماژیک	خاموش.	چاپگر
موجود.	فندک	روشن.	Seed signer
موجود.	روان نویس	خارج از seed signer.	seed signer مربوط به SD card
موجود.	ظرف آتش دان	متصل.	Power bank
موجود.	چند برگ کاغذ	متصل.	سیم رابط usb به micro-usb
موجود.	چند پاکت امنیتی	موجود.	یک برگ کاغذ حاوی اطلاعات تراکنش
موجود و حساس.	پاکت حاوی passphrase	موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		

(۴۲) کاغذ حاوی Transaction ID و آدرس های ورودی و خروجی و مقادیر و seed signer و power bank متصل به آن و SD card محتوی seed signer را بردارید و با خود به فضای ایزوله ببرید.

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله (قفل شده)			
قفل.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
خام.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان نویس
موجود.	ماژیک	خاموش.	چاپگر
موجود.	فندک	موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		
روشن.	Seed signer		
خارج از seed signer.	SD card مربوط به seed signer		
متصل.	Power bank		
متصل.	سیم رابط usb به micro-usb		
موجود.	یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس های خروجی تراکنش		

(۴۳) seed signer که می بایست هنوز روشن باشد را بردارید و گزینه ۲۴-word seed Enter را انتخاب کنید. سپس کلمات را به ترتیب از روی کاغذ حاوی نمونیک که در فضای ایزوله قرار دارد در seed signer وارد کنید. سپس passphrase را با انتخاب BIP-۳۹ Passphrase وارد کنید و سپس Done را انتخاب کنید. Seed signer بعد از پردازش، وارد صفحه Review PSBT می شود. گزینه Review Details را انتخاب کنید. سپس در Seed signer گزینه Review Recipients را انتخاب کنید. در بالای صفحه بعد می بایست عبارت Self-transfer را ببینید. آدرس و مقدار هر خروجی را در seed signer با sparrow و یادداشت کاغذی خود مقایسه کنید. گزینه Next را در seed signer انتخاب کنید تا تمام خروجی ها را ببینید. در انتها Approve PSBT را انتخاب کنید. یک QR Code متحرک در Seed signer خواهید دید. لپ تاپ ایزوله را قفل کنید.

وضعیت پس از انجام گام			
فضای ایزوله		فضای معمولی	
قفل.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
خام.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان نویس
موجود.	ماژیک	خاموش.	چاپگر
موجود.	فندک	موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		
روشن.	Seed signer		
خارج از seed signer.	SD card مربوط به seed signer		
متصل.	Power bank		
متصل.	سیم رابط usb به micro-usb		
موجود.	یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس های خروجی تراکنش		

(۴۴) بدون اینکه seed signer را از power bank جدا کنید، به همراه seed signer و سیم رابط و power bank از فضای ایزوله خارج شوید. فضای ایزوله را قفل کنید.

وضعیت پس از انجام گام			
فضای معمولی		فضای ایزوله (قفل شده)	
لپ تاپ متصل به اینترنت	قفل.	لپ تاپ ایزوله	قفل.
گوشی موبایل	روشن و متصل به شبکه همراه.	seed plate تیتانیومی	خام.
روان نویس	موجود.	سمبه اتوماتیک	موجود.
چاپگر	خاموش.	ماژیک	موجود.
یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint	موجود.	فندک	موجود.
Seed signer	روشن.	روان نویس	موجود.
Power bank	متصل.	ظرف آتش دان	موجود.
سیم رابط usb به micro-usb	متصل.	چند برگ کاغذ	موجود.
		چند پاکت امنیتی	موجود.
		پاکت حاوی passphrase	موجود و حساس.
		فلش	متصل به لپ تاپ ایزوله.
		یک برگ کاغذ حاوی نمونیک	موجود و حساس.
		SD card مربوط به seed signer	خارج از seed signer.
		یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس‌های خروجی تراکنش	موجود.

(۴۵) لپ‌تاپ متصل به اینترنت را باز کنید. از پنجره Sparrow گزینه Scan QR را انتخاب کنید. صفحه seed signer را مقابل دوربین لپ‌تاپ بگیرید تا اسکن انجام شود. پس از انجام اسکن، seed signer را از power bank جدا کنید. حال در Sparrow روی دکمه Broadcast Transaction کلیک کنید تا تراکنش به شبکه بیتکوین ارسال شود. تراکنش تایید نشده را می‌بایست در هر دو کیف پول Electrum و Sparrow مشاهده کنید. حال منتظر بمانید تا بلاک حاوی تراکنش استخراج شود و این تراکنش را در هر دو کیف پول Sparrow و Electrum به صورت تایید شده مشاهده کنید.

وضعیت پس از انجام گام		فضای معمولی	
فضای ایزوله (قفل شده)			
قفل.	لپ تاپ ایزوله	روشن.	لپ تاپ متصل به اینترنت
خام.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان نویس
موجود.	ماژیک	خاموش.	چاپگر
موجود.	فندک	موجود.	یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint
موجود.	روان نویس	خاموش.	Seed signer
موجود.	ظرف آتش دان	نا متصل.	Power bank
موجود.	چند برگ کاغذ	نا متصل.	سیم رابط usb به micro-usb
موجود.	چند پاکت امنیتی		
موجود و حساس.	پاکت حاوی passphrase		
متصل به لپ‌تاپ ایزوله.	فلش		
موجود و حساس.	یک برگ کاغذ حاوی نمونیک		
خارج از seed signer.	SD card مربوط به seed signer		
موجود.	یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس‌های خروجی تراکنش		

(۴۶) اگر تراکنش تایید شده را در هر دو کیف پول مشاهده نکردید، پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید. اگر مشاهده کردید یعنی تا کنون مراحل به درستی انجام شده‌اند و مشکلی نیست. حال به همراه seed signer و سیم رابط و power bank و کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint به فضای ایزوله بروید. لپ‌تاپ متصل به اینترنت را قفل کنید.

وضعیت پس از انجام گام			
فضای معمولی		فضای ایزوله	
لپ‌تاپ متصل به اینترنت	قفل.	لپ‌تاپ ایزوله	قفل.
گوشی موبایل	روشن و متصل به شبکه همراه.	seed plate تیتانیومی	خام.
روان‌نویس	موجود.	سمبه اتوماتیک	موجود.
چاپگر	خاموش.	ماژیک	موجود.
		فندک	موجود.
		روان‌نویس	موجود.
		ظرف آتش دان	موجود.
		چند برگ کاغذ	موجود.
		چند پاکت امنیتی	موجود.
		پاکت حاوی passphrase	موجود و حساس.
		فلش	متصل به لپ‌تاپ ایزوله.
		یک برگ کاغذ حاوی نموتیک	موجود و حساس.
		SD card مربوط به seed signer	خارج از seed signer.
		یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس‌های خروجی تراکنش	موجود.
		Seed signer	خاموش.
		Power bank	نا متصل.
		سیم رابط usb به micro-usb	نا متصل.
		یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint	موجود.

(۴۷) لپ‌تاپ ایزوله را باز کنید. در Sparrow وارد بخش Settings از نوار آبی سمت چپ شوید. روی View Seed... در میان صفحه کلیک کنید تا ۲۴ کلمه ظاهر شوند. حال تمام کلمات را با دقت و به ترتیب با ماژیک روی صفحه تیتانیومی علامت‌گذاری کنید. هنگامی که علامت‌گذاری تمام شد، SD card حاوی seed signer را داخل دستگاه seed signer قرار دهید و دستگاه را به منبع تغذیه متصل کنید تا روشن شود. هنگامی که پیغام You can remove the SD card now را مشاهده کردید، SD card را از دستگاه خارج کنید. حالا در seed signer گزینه Seeds را انتخاب کنید. سپس ۲۴-word seed Enter را انتخاب کنید. حال به ترتیب از روی صفحه تیتانیومی، ۲۴ کلمه را در seed signer وارد کنید. در صفحه Finalize Seed، گزینه BIP-۳۹ Passphrase را انتخاب کنید. سپس passphrase (۲۰) را وارد نمایید. برای تایید، پایبندترین کلید سمت راست seed signer که مقابلش در صفحه نمایش seed signer یک تیک سبز قرار دارد را بفشارید. در صفحه Verify Passphrase در seed signer، passphrase (۲۰) را مشاهده می‌کنید. مطمئن شوید که صحیح است. بالای دکمه Edit passphrase در seed signer دو عبارت مشاهده می‌کنید که با >> جدا شده‌اند. عبارت سمت راست می‌بایست با عبارتی که روی صفحه لپ‌تاپ ایزوله در پنجره Sparrow در قسمت Keystores، زیر برگه BIP۳۹، مقابل Master fingerprint مشاهده می‌کنید، یکسان باشد. اگر این دو یکی بودند دکمه Done در seed signer را انتخاب کنید و فشار دهید. اگر یکی نبودند علامت‌های روی صفحه تیتانیومی را با کلمات seed که در Sparrow نمایش داده شده‌اند مجدداً تطبیق دهید. سپس seed signer را از کابل متصل به آن جدا کنید و مراحل را این گام را مجدداً تکرار کنید. اگر باز هم یکی نبودند **پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.** اگر fingerprint ها یکی بودند، علامت‌هایتان روی صفحه تیتانیومی را با کلمات یادداشت شده روی کاغذ حاوی نمونیک مجدداً چک کنید. اگر یکی نبودند، نبودند **پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.** اگر یکی بودند، با استفاده از سمبه اتوماتیک، تمام علامت‌های روی صفحه تیتانیومی را نشانه‌گذاری کنید. می‌توانید برای هر نشان ۲ ضربه وارد کنید تا اثر گودتر شود. حالا یک کاغذ بردارید و به ترتیب ۴ حرف ابتدایی ۲۴ کلمه در صفحه تیتانیومی را با ذکر شماره رویش یادداشت کنید. پس از یادداشت، این مقادیر را با کلمات روی کاغذ حاوی نمونیک مطابقت دهید تا یکی باشند. اگر نبودند، در نوشتن اشتباه کرده‌اید و می‌بایست مجدداً نوشته را با صفحه تیتانیومی مطابقت دهید. حالا از روی passphrase هم روی ۲ کاغذ مجدداً بنویسید. شما حالا ۳ نسخه کاغذی از passphrase، ۲ نسخه کاغذی از نمونیک و یک نسخه تیتانیومی از نمونیک دارید. هر کدام را در پاکت‌های امنیتی جدا قرار داده و مهر و موم کنید. روی پاکت‌ها بنویسید که نمونیک هستند یا passphrase. لپ‌تاپ ایزوله را خاموش کنید و فلش را از آن جدا کنید. لپ‌تاپ ایزوله و فلش و شارژر لپ‌تاپ ایزوله را داخل یک پاکت امنیتی قرار دهید و مهر و مومش کنید. تمام سایر کاغذهایی که حاوی نوشته‌ای هستند و در فضای ایزوله هستند را داخل ظرف آتش‌دان قرار داده و آتش بزنید.

وضعیت پس از انجام گام

فضای ایزوله		فضای معمولی	
خاموش و داخل پاکت امنیتی.	لپ تاپ ایزوله	قفل.	لپ تاپ متصل به اینترنت
حاوی نمونیک و داخل پاکت امنیتی.	seed plate تیتانیومی	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	سمبه اتوماتیک	موجود.	روان نویس
موجود.	ماژیک	خاموش.	چاپگر
موجود.	فندک		
موجود.	روان نویس		
موجود.	ظرف آتش دان		
موجود.	چند برگ کاغذ		
موجود.	چند پاکت امنیتی		
موجود و داخل پاکت امنیتی.	پاکت حاوی passphrase		
موجود و داخل پاکت امنیتی.	کاغذ حاوی passphrase		
موجود و داخل پاکت امنیتی.	کاغذ حاوی passphrase		
نامتصل و داخل پاکت امنیتی.	فلش		
موجود و داخل پاکت امنیتی.	یک برگ کاغذ حاوی نمونیک		
موجود و داخل پاکت امنیتی.	یک برگ کاغذ حاوی نمونیک		
خارج از seed signer.	SD card مربوط به seed signer		
خاموش.	Seed signer		
نا متصل.	Power bank		
نا متصل.	سیم رابط usb به micro-usb		

(۴۸) تعداد ۷ پاکت امنیتی مهر و موم شده و سایر پاکت‌های امنیتی خالی را بردارید و با خود از فضای ایزوله خارج کنید. فضای ایزوله را قفل کنید.

فضای ایزوله (قفل شده)		فضای معمولی	
موجود.	سمبه اتوماتیک	قفلی.	لپ تاپ متصل به اینترنت
موجود.	ماژیک	روشن و متصل به شبکه همراه.	گوشی موبایل
موجود.	فندک	موجود.	روان نویس
موجود.	روان نویس	خاموش.	چاپگر
موجود.	ظرف آتش دان	خاموش و داخل پاکت امنیتی.	لپ تاپ ایزوله
موجود.	چند برگ کاغذ	نامتصل و داخل پاکت امنیتی.	فلش
خارج از seed signer.	SD card مربوط به seed signer	موجود.	چند پاکت امنیتی
خاموش.	Seed signer	حاوی نمونیک و داخل پاکت امنیتی.	seed plate نیتانیومی
نامتصل.	Power bank	موجود و داخل پاکت امنیتی.	پاکت حاوی passphrase
نامتصل.	سیم رابط usb به micro-usb	موجود و داخل پاکت امنیتی.	کاغذ حاوی passphrase
		موجود و داخل پاکت امنیتی.	کاغذ حاوی passphrase
		موجود و داخل پاکت امنیتی.	یک برگ کاغذ حاوی نمونیک
		موجود و داخل پاکت امنیتی.	یک برگ کاغذ حاوی نمونیک

(۴۹) پاکت امنیتی حاوی لپ‌تاپ ایزوله و فلش را داخل گاوصندوق قرار دهید. سایر پاکت‌های امنیتی حاوی نمونیک و passphrase می‌بایست در مکان‌های امن جدا از هم نگهداری شوند. حال لپ‌تاپ متصل به اینترنت را باز کنید. در Sparrow گزینه Settings را از نوار آبی سمت چپ انتخاب کنید. سپس روی دکمه Export در قسمت پایین سمت چپ کلیک کنید. از پنجره‌ای که باز می‌شود، Output Descriptor را بیابید و در مقابل آن روی دکمه Show... کلیک کنید. یک پنجره حاوی یک QR Code باز می‌شود. در پایین آن روی دکمه Save PDF... کلیک کنید. محلی را برای ذخیره فایل انتخاب کنید. سپس به محل ذخیره رفته و فایل pdf را چاپ کنید. با استفاده از این QR Code خواهید توانست کیف پول watch only مربوط به این پروتکل را مشاهده نمایید. حال کلیه فایل‌های کیف پول ایجاد شده توسط Sparrow و Electrum را از سیستم خود پاک کنید. برای پیدا کردن مسیر ذخیره فایل‌ها در هریک از این کیف پول‌ها، گزینه‌های Open Wallet... و Open را در منوی File انتخاب کنید. لپ‌تاپ متصل به اینترنت را خاموش کنید.

وضعیت پس از انجام گام			
فضای معمولی		فضای ایزوله (قفل شده)	
لپ تاپ متصل به اینترنت	خاموش.	سمبه اتوماتیک	موجود.
گوشی موبایل	روشن و متصل به شبکه همراه.	ماژیک	موجود.
روان‌نویس	موجود.	فندک	موجود.
چاپگر	خاموش.	روان‌نویس	موجود.
لپ تاپ ایزوله	خاموش و داخل پاکت امنیتی.	ظرف آتش دان	موجود.
فلش	نامتصل و داخل پاکت امنیتی.	چند برگ کاغذ	موجود.
چند پاکت امنیتی	موجود.	SD card مربوط به seed signer	خارج از seed signer.
seed plate تیتانیومی	حاوی نمونیک و داخل پاکت امنیتی.	Seed signer	خاموش.
پاکت حاوی passphrase	موجود و داخل پاکت امنیتی.	Power bank	نا متصل.
کاغذ حاوی passphrase	موجود و داخل پاکت امنیتی.	سیم رابط usb به micro-usb	نا متصل.
کاغذ حاوی passphrase	موجود و داخل پاکت امنیتی.		
یک برگ کاغذ حاوی نمونیک	موجود و داخل پاکت امنیتی.		
یک برگ کاغذ حاوی نمونیک	موجود و داخل پاکت امنیتی.		
کاغذهای چاپ شده حاوی QR Code برای ایجاد کیف پول watch only	موجود.		

(۵۰) به فضای ایزوله بروید و پاکسازی اش کنید. پاکت های امنیتی را از فضای معمولی به مکان های امن منتقل کنید.