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

**ابزارهای مورد نیاز:**

1. ۱ عدد لپ‌تاپ متصل به اینترنت با سیستم‌عامل 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 پول‌های Electrum و Sparrow باشد و کیف پول Sparrow در آن به bitcoin core نصب شده روی لپ‌تاپ متصل باشد.
2. ۱ عدد لپ‌تاپ ایزوله با پردازنده intel و مجهز به دوربین که یا جدید بوده یا سابقهٔ مشخص و قابل اعتمادی داشته باشد و کارت‌های شبکه و بی‌سیم‌اش (wifi و bluetooth) قابل جدا شدن باشند و جدا شده باشند. باتری این لپ‌تاپ می‌بایست سالم و کاملا 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.
3. ۱ عدد فلشusb به ظرفیت حداقل ۸ گیگابایت که می‌بایست نو و بازنشده باشد. این فلش را از محلی معتبر تهیه کنید. توجه کنید که port این فلش با هردو لپ‌تاپ همخوان باشد.
4. اتصال اینترنت که با سیم LAN قابل اتصال به لپ تاپ متصل به اینترنت ‏(1) باشد.
5. 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 ‏(4) متصل باشد.
6. ۱ عدد seed signer به همراه SD card حاوی image اجرا کننده seed signer.
7. ۱ عدد power bank یا منبع تغذیه پورتابل جهت تأمین برق seed signer.
8. ۱ سیم رابط usb به micro-usb جهت اتصال seed signer ‏(6) به منبع تغذیه ‏(7).
9. ۱ دستگاه چاپگر.
10. ۱ عدد seed plate تیتانیومی.
11. ۱ عدد ماژیک.
12. ۱ عدد center punch یا سمبه اتوماتیک.
13. ۱ عدد فندک.
14. ۲ عدد خودکار روان یا روان‌نویس که بتوانید بدون فشار آوردن زیاد با آن بنویسید.
15. چند برگ کاغذ معمولی آتش گیر.
16. ۱ ظرف برای آتش زدن کاغذ.
17. 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.
18. فضای معمولی که دارای اتصال اینترنت باشد.
19. مقداری بیتکوین در آدرسی تحت کنترل عملگر.
20. یک passphrase که داخل یک پاکت امن قرار دارد.

**نامتغیرها:**

1. لپ‌تاپ ایزوله ‏(2) می‌بایست صرفاً در فضای ایزوله ‏(17) روشن شده و کار کند.
2. لپ‌تاپ ایزوله ‏(2) نمی‌بایست در هنگامی که روشن است به برق متصل شود.
3. لپ‌تاپ متصل به اینترنت ‏(1) می‌بایست صرفاً در فضای معمولی ‏(18) روشن شده و کار کند.

**مراحل ایجاد کیف پول:**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | خاموش. | لپ تاپ ایزوله | خاموش. |
| فلش | آکبند. | Seed signer | خاموش. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | SD card مربوط به seed signer | داخل seed signer. |
| روان‌نویس | 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. |
| روان‌نویس | موجود. |
| ظرف آتش دان | موجود. |
| چند برگ کاغذ | موجود. |
| چند پاکت امنیتی | موجود. |
| پاکت حاوی passphrase | موجود و حساس. |

1. 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** | |
| لپ تاپ متصل به اینترنت | روشن. | لپ تاپ ایزوله | خاموش. |
| فلش | آکبند. | Seed signer | خاموش. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | SD card مربوط به seed signer | داخل seed signer. |
| روان‌نویس | 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. |
| روان‌نویس | موجود. |
| ظرف آتش دان | موجود. |
| چند برگ کاغذ | موجود. |
| چند پاکت امنیتی | موجود. |
| پاکت حاوی passphrase | موجود و حساس. |

شما در فضای معمولی هستید

1. 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.

شما در فضای معمولی هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | روشن. | لپ تاپ ایزوله | خاموش. |
| فلش | متصل به لپ‌تاپ متصل به اینترنت. | Seed signer | خاموش. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | SD card مربوط به seed signer | داخل seed signer. |
| روان‌نویس | 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. |
| روان‌نویس | موجود. |
| ظرف آتش دان | موجود. |
| چند برگ کاغذ | موجود. |
| چند پاکت امنیتی | موجود. |
| پاکت حاوی passphrase | موجود و حساس. |

1. کیف پول Sparrow را از طریق لپ‌تاپ متصل به اینترنت، از آدرس <https://www.sparrowwallet.com/download/> دریافت کنید. نسخه‌ای که می‌بایست دریافت کنید، نسخهٔ لینوکس (**Linux (Intel/AMD)** (Ubuntu/Debian)) 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 ‏(26) روی فلش ایجاد کردید در کپی کنید. در غیر این صورت پروتکل را متوقف کنید.

شما در فضای معمولی هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | روشن. | لپ تاپ ایزوله | خاموش. |
| فلش | متصل به لپ‌تاپ متصل به اینترنت. | Seed signer | خاموش. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | SD card مربوط به seed signer | داخل seed signer. |
| روان‌نویس | 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. |
| روان‌نویس | موجود. |
| ظرف آتش دان | موجود. |
| چند برگ کاغذ | موجود. |
| چند پاکت امنیتی | موجود. |
| پاکت حاوی passphrase | موجود و حساس. |

1. 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.

شما از فضای معمولی به فضای ایزوله وارد می‌شوید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | خاموش. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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 | نامتصل. |

1. 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.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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. |

1. 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 می شود.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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. |

1. روی Places در نوار بالایی صفحه دسکتاپ Tails کلیک کنید و Computer را انتخاب نمایید. در نوار کناری پنجره‌ای که باز می شود، اگر پارتیشن موضوع ‏(26) 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 می شود. رمز تعیین شده در ‏(30) را وارد نمایید. درایو باز شده و فایل .deb نصب Sparrow نمایان می گردد. داخل پنجره ای که باز شده کلیک راست کنید و Open in Terminal را انتخاب کنید. در ترمینال این دستور را وارد کنید:

شما در فضای ایزوله هستید

sudo dpkg -i ./sparrow\_xxxxx\_amd64.deb

رمز خود ‏(30) را در پرامپت وارد کنید. Sparrow نصب می شود. بعد از اتمام نصب، ترمینال را ببندید. پنجره درایو را نیز ببندید.

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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. |

1. 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 روی New Wallet کلیک کنید و اسمی برای کیف پول انتخاب نمایید. سپس روی Create Wallet 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(Keystore1) 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 Mnemonic Words (BIP39)، Use 24 Words 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 رو یه روی Passphrase:، passphrase موضوع ‏(20) را وارد کنید.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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. |

1. یک برگ کاغذ را روی یک سطح ترجیاً 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.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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 نمونیک | موجود و حساس. |

1. 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 24 Words… کلیک کنید و مراحل را از ‏(32) 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 آتش‌دان قرار دهید. اگر مکرراً با مشکل مواجه می‌شوید، 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 ‏(20) 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 مجددا و با دقت به passphrase این مقدار مورد قبول نبود، در ‏(32) مقدار را اشتباه وارد کرده بودید و می بایست از ‏(32) دوباره شروع کنید. اگر مکرراً با مشکل مواجه می‌شوید، 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 BIP39 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.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | خاموش. |
| روان‌نویس | موجود. | SD card مربوط به seed signer | داخل seed signer. |
| چاپگر | خاموش. | Power bank | نا متصل. |
|  | | سیم رابط usb به micro-usb | نا متصل. |
| seed plate تیتانیومی | خام. |
| سمبه اتوماتیک | موجود. |
| 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 نمونیک | موجود و حساس. |

1. سر usb سیم رابط ‏(8) 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.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | روشن. |
| روان‌نویس | 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. |
| 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 نمونیک | موجود و حساس. |

1. در صفحه اصلی seed signer، Seeds را انتخاب کنید. سپس گزینه Enter 24-word seed را انتخاب کنید. حال تمام کلمات را به ترتیب از روی کاغذ ‏(33) به seed signer وارد کنید. در صفحه Finalize Seed، گزینه BIP-39 Passphrase را انتخاب کنید. سپس passphrase ‏(20) 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 ‏(20) 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 لپ‌تاپ ایزوله در قسمت Keystores، زیر برگه BIP39، 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 ‏(35) مجددا تکرار کنید. اگر باز هم یکی نبودند پروتکل را متوقف کنید. شما یا تحت حمله قرار دارید یا قادر به اجرای پروتکل نیستید.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | روشن. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | روشن. |
| روان‌نویس | 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. |
| 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 نمونیک | موجود و حساس. |

1. 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 لپ‌تاپ ایزوله، در قسمت Keystore، در سربرگ BIP39، در قسمت انتهایی، مقابل xpub / zpub: یک رشته اعداد و حروف بلند می‌بینید که با xpub شروع می‌شود. در سمت دیگر این باکس حاوی حروف و اعداد، دو آیکون مشاهده می‌کنید. 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، رویSettings 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 یادداشت‌اش کنید. عدد مذکور را مقابل Gap limit: وارد کنید. سپس روی Close کلیک کنید. حال روی دکمه Apply در پایین سمت راست کلیک کنید. پنجره‌ای باز می‌شود 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 می‌کنید. 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.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | قفل. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | Seed signer | روشن. |
| روان‌نویس | 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. |
| 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 نمونیک | موجود و حساس. |
| یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint | موجود. |

1. بدون اینکه seed signer را از power bank جدا کنید، seed signer و power bank و قطعه کاغذ حاوی Master fingerprint ‏(37) 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 پاکت حاوی 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 بیتکوین ها است. پس اطمینان حاصل کنید که کسی به جز خودتان تا پایان فرایند وارد اتاق ایزوله نمی شود.

شما از فضای ایزوله به فضای معمولی وارد می‌شوید

|  |  |  |  |
| --- | --- | --- | --- |
| **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. |
| روان‌نویس | موجود. | سمبه اتوماتیک | موجود. |
| چاپگر | خاموش. | ماژیک | موجود. |
| Seed signer | روشن. | فندک | موجود. |
| SD card مربوط به seed signer | خارج از seed signer. | روان‌نویس | 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 لپ‌تاپ ایزوله. |
| یک برگ کاغذ حاوی نمونیک | موجود و حساس. |

1. لپ‌تاپ متصل به اینترنت را باز کنید و Electrum را باز کنید. اگر قبلا 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 ‏(37) 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 الکترام بازگردید. می‌بایست یک سربرگ به نام Console مشاهده کنید. روی آن کلیک کنید. چیزی شبیه به Terminal خواهید دید. حال عدد دلخواه روی کاغذ ‏(37) را معادل x فرض کنید. حال دستور زیر را در قسمت شبیه خط فرمان در Console بعد از علامت >>> وارد کنید.

شما در فضای معمولی هستید

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)** | |
| لپ تاپ متصل به اینترنت | روشن. | لپ تاپ ایزوله | قفل. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | seed plate تیتانیومی | خام. |
| روان‌نویس | موجود. | سمبه اتوماتیک | موجود. |
| چاگر | خاموش. | ماژیک | موجود. |
| Seed signer | خاموش. | فندک | موجود. |
| SD card مربوط به seed signer | خارج از seed signer. | روان‌نویس | موجود. |
| Power bank | نا متصل. | ظرف آتش دان | موجود. |
| سیم رابط usb به micro-usb | نا 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 لپ‌تاپ ایزوله. |
| یک برگ کاغذ حاوی نمونیک | موجود و حساس. |

1. 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 آیکون 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 آیکون 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.

شما در فضای معمولی هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله (قفل شده)** | |
| لپ تاپ متصل به اینترنت | روشن. | لپ تاپ ایزوله | قفل. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | seed plate تیتانیومی | خام. |
| روان‌نویس | موجود. | سمبه اتوماتیک | موجود. |
| چاپگر | خاموش. | ماژیک | موجود. |
| Seed signer | خاموش. | فندک | موجود. |
| SD card مربوط به seed signer | خارج از seed signer. | روان‌نویس | موجود. |
| Power bank | نا متصل. | ظرف آتش دان | موجود. |
| سیم رابط usb به micro-usb | نا 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 لپ‌تاپ ایزوله. |
| یک برگ کاغذ حاوی نمونیک | موجود و حساس. |

1. 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 Wallet را در قسمت Keystores و تحت سربرگ Keystore 1 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/84'/0'/0' 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 آیکونی 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 QR Code 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 زیرTransaction 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 نگه 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.

شما در فضای معمولی هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **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. |
| روان‌نویس | موجود. | سمبه اتوماتیک | موجود. |
| چاپگر | خاموش. | ماژیک | موجود. |
| Seed signer | روشن. | فندک | موجود. |
| SD card مربوط به seed signer | خارج از seed signer. | روان‌نویس | موجود. |
| Power bank | متصل. | ظرف آتش دان | موجود. |
| سیم رابط usb به micro-usb | متصل. | چند برگ کاغذ | موجود. |
| یک برگ کاغذ حاوی اطلاعات تراکنش | موجود. | چند پاکت امنیتی | موجود. |
| یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint | موجود. | پاکت حاوی passphrase | موجود و حساس. |
|  | | فلش | متصل به لپ‌تاپ ایزوله. |
| یک برگ کاغذ حاوی نمونیک | موجود و حساس. |

1. 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.

شما از فضای معمولی به فضای ایزوله وارد می‌شوید

|  |  |  |  |
| --- | --- | --- | --- |
| **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. |
| روان‌نویس | موجود. | سمبه اتوماتیک | موجود. |
| چاپگر | خاموش. | ماژیک | موجود. |
| یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint | 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 نمونیک | موجود و حساس. |
| Seed signer | روشن. |
| SD card مربوط به seed signer | خارج از seed signer. |
| Power bank | متصل. |
| سیم رابط usb به micro-usb | متصل. |
| یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس‌های خروجی تراکنش | موجود. |

1. seed signer که می بایست هنوز روشن باشد را بردارید و گزینه Enter 24-word seed 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-39 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. لپ‌تاپ ایزوله را قفل کنید.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | قفل. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | seed plate تیتانیومی | خام. |
| روان‌نویس | موجود. | سمبه اتوماتیک | موجود. |
| چاپگر | خاموش. | ماژیک | موجود. |
| یک برگ کاغذ حاوی عدد دلخواه و آدرس و Master fingerprint | 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 نمونیک | موجود و حساس. |
| Seed signer | روشن. |
| SD card مربوط به seed signer | خارج از seed signer. |
| Power bank | متصل. |
| سیم رابط usb به micro-usb | متصل. |
| یک برگ کاغذ حاوی بخشی از Transaction ID و آدرس‌های خروجی تراکنش | موجود. |

1. 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.

شما از فضای ایزوله به فضای معمولی وارد می‌شوید

|  |  |  |  |
| --- | --- | --- | --- |
| **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. |
| روان‌نویس | 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. | روان‌نویس | 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 لپ‌تاپ 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. |

1. 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 Electrum و Sparrow به صورت تایید شده مشاهده کنید.

شما در فضای معمولی هستید

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

1. اگر تراکنش تایید شده را در هردو 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.

شما از فضای معمولی به فضای ایزوله وارد می‌شوید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ 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 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. |
| 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. |

1. 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 Enter 24-word seed را انتخاب کنید. حال به ترتیب از روی صفحه تیتانیومی، ۲۴ کلمه را در seed signer وارد کنید. در صفحه Finalize Seed، گزینه BIP-39 Passphrase را انتخاب کنید. سپس passphrase ‏(20) 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 ‏(20) 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 لپ‌تاپ ایزوله در پنجره Sparrow در قسمت Keystores، زیر برگه BIP39، 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 علامت‌های روی صفحه تیتانیومی را با کلمات seed که در Sparrow نمایش داده شده‌اند مجددا تطبیق دهید. سپس seed signer را از کابل متصل به آن جدا کنید و مراحل را این گام را مجددا 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 مجددا 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 نشانه گذاری 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 اشتباده کرده‌اید و می‌بایست مجددا نوشته را با صفحه تیتانیومی مطابقت دهید. حالا از روی passphrase هم روی ۲ کاغذ مجددا 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 پاکت ها 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.

شما در فضای ایزوله هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله** | |
| لپ تاپ متصل به اینترنت | قفل. | لپ تاپ ایزوله | خاموش و داخل پاکت امنیتی. |
| گوشی موبایل | روشن و متصل به شبکه همراه. | seed plate تیتانیومی | حاوی نمونیک و داخل پاکت امنیتی. |
| 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 داخل پاکت امنیتی. |
| کاغذ حاوی passphrase | موجود و داخل پاکت امنیتی. |
| کاغذ حاوی passphrase | موجود و داخل پاکت امنیتی. |
| فلش | نامتصل و داخل پاکت امنیتی. |
| یک برگ کاغذ حاوی نمونیک | موجود و داخل پاکت امنیتی. |
| یک برگ کاغذ حاوی نمونیک | موجود و داخل پاکت امنیتی. |
| SD card مربوط به seed signer | خارج از seed signer. |
| Seed signer | خاموش. |
| Power bank | نا متصل. |
| سیم رابط usb به micro-usb | نا متصل. |

1. 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.

شما از فضای ایزوله به فضای معمولی وارد می‌شوید

|  |  |  |  |
| --- | --- | --- | --- |
| **وضعیت پس از انجام گام** | | | |
| **فضای معمولی** | | **فضای ایزوله (قفل شده)** | |
| لپ تاپ متصل به اینترنت | قفل. | 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. |

1. پاکت امنیتی حاوی لپ‌تاپ ایزوله و فلش را داخل گاوصندوق قرار دهید. سایر پاکت‌های امنیتی حاوی نمونیک و passphrase می بایست 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.

شما در فضای معمولی هستید

|  |  |  |  |
| --- | --- | --- | --- |
| **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. |

1. به فضای ایزوله بروید و پاکسازی‌اش کنید. پاکت‌های امنیتی را از فضای معمولی به مکان‌های امن منتقل کنید.

اتمام