راهنمای استفاده از پروژه JADE

کیف پول سخت افزاری شرکت Blockstream

و نحوه اتصال آن به کیف پول بلو والت

کیف پول سخت افزاری JADE:

JADE یک کیف پول سخت افزاری میباشد که توسط شرکت Blockstream ساخته شده، air gapped و متن باز بوده و از یک هسته ESP32 درون خود استفاده میکند. در این مقاله قصد بر این است که یکی از روش های امن نگهداری و ارسال بیت‌کوین را به زبان فارسی به شما آموزش بدهیم. این مقاله برگرفته شده از ویدئو زیر از کانال یوتیوب 402 Payment Required با عنوان Bitcoin self custody میباشد.

https://youtu.be/H-wjIfwFOq4

امیدوارم این مقاله برای شما مفید واقع شود و بتونید به خوبی از آن استفاده بکنید.

در مرحله اول لازم به ذکر است که بگوییم این روش به هیچ عنوان یک روش پیشنهادی نیست و صرفا یک آموزش بوده و استفاده یا عدم استفاده از آن به عهده هر شخص میباشد.

همانطور که احتمالا میدانید نگهداری بیت‌کوین یک موضوع مهم و شخصی بوده و روش نگهداری آن برای هر شخص میتواند فرق داشته باشد. در این آموزش ما از کیف پول سخت افزاری JADE از شرکت Blockstream استفاده میکنیم. از این کیف پول سخت افزاری برای نگهداری کلمات بازیابی استفاده کنیم و موجودی بیت‌کوین خود را روی کیف پول بلووالت (bluewallet) مشاهده مینماییم. در اینجا کیف پول بلووالت به عنوان یک کیف پول ناظر (watch only) استفاده میشود. همچنین در صورتی که به ساخت کلمات بازیابی توسط هیچ شخص یا دیوایس واسطه ای اعتماد ندارید میتوانیم کلمات بازیابی را با استفاده از تاس و bip-39 خودمان تولید بکنیم (طبق این آموزش که به فارسی موجود میباشد https://bitcoind.me/blobs/tuts/gen_bip39_bitcoin_seed_farsi.pdf) و به این کیف پول سخت افزاری اضافه بکنید.

باید توجه داشته باشید که این کیف پول از هسته ESP32 استفاده میکند و در هر حالت به اینترنت متصل نمیباشد و هیچگونه ارتباطی با دنیای بیرون نخواهد داشت و به اصطلاح(air gapped) میباشد .البته چون این هسته دارای وای فای و بلوتوث میباشد برخی افراد که احتیاط زیادی دارند این را یک مشکل میدانند و استفاده از seed signer را پیشنهاد میکنند. این کیف پول سخت افزاری دارای یک صفحه نمایش ,oled یک دکمه و یک اسکرول در بالای ماژول قرار دارد و دارای یک دوربین در پشت دستگاه برای اسکن کردن است. اگر بخواهید خودتان این کیف پول را بسازید باید قطعات را جداگانه تهیه کنید و سر هم بندی آن را انجام بدهید. که باید از ماژول LILYGO TTGO ، باتری و یک ماژول دوربین استفاده بکنید.

ماژول آماده این کیف پول اندازه بسیار کوچکی داشته و تقریبا به اندازه کف یک دست میباشد.

روند کار به این شکل خواهد بود که ما با استفاده از JADE کلمات بازیابی را تولید میکنیم (یا طبق گفته بالاتر میتوانیم خودمان کلید را تولید کنیم و به دستگاه بدهیم) و در مرحله بعدی XPUB کیف پولمان را از JADE به بلووالت ایمپورت میکنیم تا بتوانیم موجودی خود را در کیف پول آنلاین مشاهده بکنیم.

بنابراین ما یک کیف پول سخت افزاری داریم که air gapped بوده و کلمات بازیابی و کلیدهای ما هیچگونه تماس یا ارتباطی با اینترنت نداشته‌اند. و یک کیف پول ناظر (watch only) داریم که میتوانیم با آن فقط موجودی بیت‌کوین خود و دریافت را داشته باشیم، و ما فقط زمانی از JADE استفاده میکنیم که بخواهیم تراکنش ارسالی داشته باشیم، که توسط این دستگاه امضا شود.

توجه از این کیف پول میشود با استفاده از کابل USB هم به کیف پول Green وصل شد اما برای air gappedبودن از انجام این کار صرفه نظر شده است.

این کیف پول میتواند کلمات بازیابی را به صورت یک Qrcode در آورده تا برای هربار وارد کردن آن به دستگاه با دوربین اسکن شود. چون وارد کردن ۲۴ کلمه بازیابی با دستگاهی به این اندازه و فقط یک اسکرول برای حرکت دادن روی صفحه نمایش، کاری حوصله سر بر و نسبتا دشواری خواهد بود.

نگهداری کلمات بازیابی از مهم ترین بحث های نگهداری بیت‌کوین میباشد. طبق جمله مشهور

Not your keys, Not your coins

اگر شما در نگهداری این کلمات کوتاهی بکنید تمامی بیت‌کوین خود را از دست خواهید داد.

در استفاده از JADE دو راهکار دارید، یا کلمات را وارد کیف پول کنید و در حافظه آن نگهدارید یا آن را در جایی نگهداری کنید و فقط زمانی میخواهید که تراکنش ارسالی داشته باشید آن را وارد دستگاه بکنید. که روش دوم از امنیت بیشتری برخوردار است. حال به سراغ آموزش کیف پول رفته، پس از روشن کردن دستگاه از شما میخواهد که آن را راه اندازی اولیه کنید.

در مرحله بعدی از ما میخواهد که یک ولت جدید با کلمات بازیابی جدید برای ما تولید کند یا کلمات بازیابی که خودمان داشتیم را به آن اضافه بکنیم.

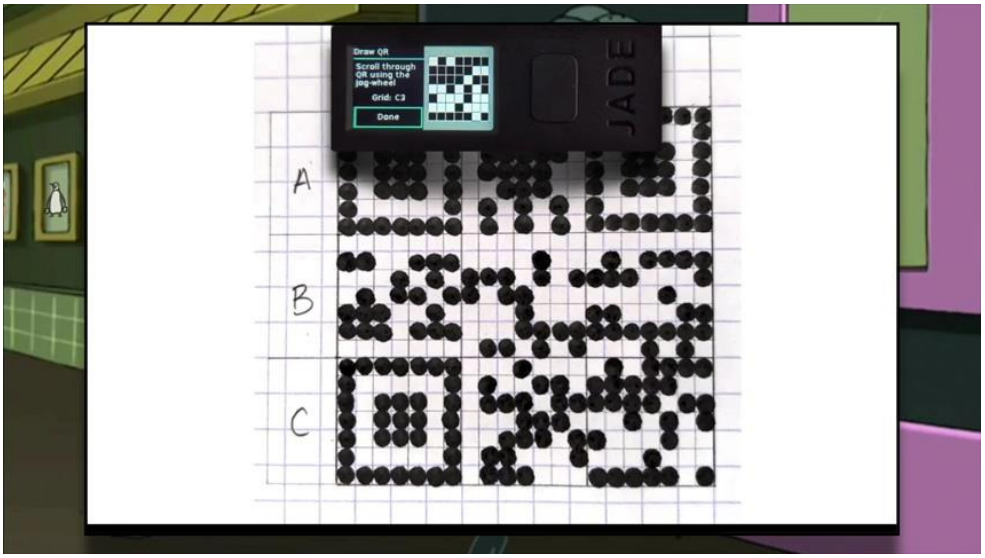
در صورت انتخاب New از ما میخواهد که آیا از ۱۲ کلمه بازیابی میخواهیم استفاده بکنیم یا برای استفاده از ۲۴ کلمه به منوی Advanced میرویم.

حال با انتخاب کردن ایجاد ۱۲ کلمه بازیابی آن را جایی یادداشت میکنیم.

در مرحله بعدی برای اینکه برای اینکه بررسی کنیم کلمات ایجاد شده را به درستی یادداشت کرده ایم، یک بار دستگاه را restart میکنیم و این بار از گزینه Recover بعد از روشن شدن دستگاه برای وارد کردن کلمات بازیابی استفاده میکنیم.

این بار به بخش Advanced رفته و recovery phrase login را انتخاب کنید، از شما میخواهد کلمات بازیابی خودتان که ۱۲ کلمه یا ۲۴ کلمه هست را را به دستگاه وارد کنید. همچنین گزینه Scan Qr برای اسکن کردن کلمات هم موجود میباشد.

اگر به صـورت کلمه به کلمه کلمات بازیابی را وارد بکنید در انتها به شـما میگوید که آیا میخواهید این کلمات را به صورت Qrcode داشته باشید؟ و اگر بله را انتخاب کنید یک تمپلیت به شما نشان میدهد و از شما میخواهد به دقت آن را ترسیم کرده و کلمات را به شکل یک Qrcode نمایش میدهد.



در مرحله بعد از شما میپرسد که آیا میخواهید از pass phrase برای کلمات بازیابی خود استفاده بکنید که در صورت نیاز میتوانیم از pass phrase برای کلمات بازیابی استفاده بکنیم.

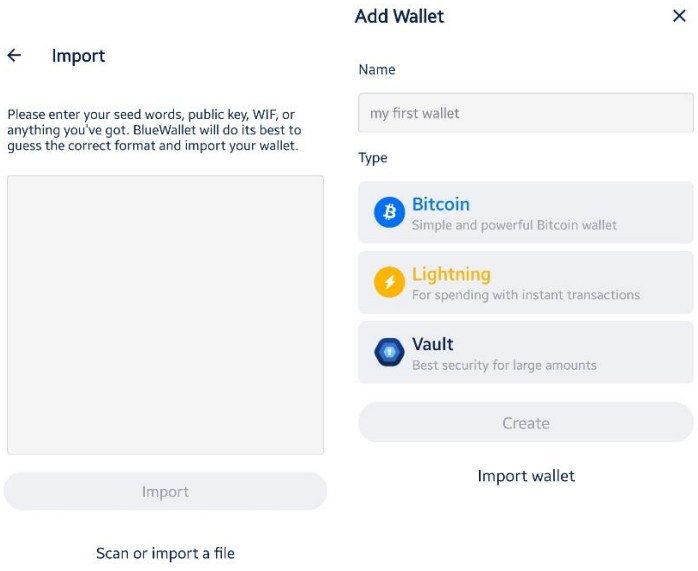
و در مرحله آخر برای اضافه شدن کلمات بازیابی به دستگاه از شما سوال میکند که آیا میخواهید با استفاده از Qrcode از کیف پول استفاده بکنید یا استفاده از usb cable که ما برای امنیت بیشتر از Qrcode استفاده میکنیم.

تا این مرحله ما از کیف پول استفاده کردیم و کلمات بازیابی را ایجاد کردیم. از قسمت settings به بخش device میرویم و با factory reset دستگاه را ریست میکنیم.

دســـتگاه را دوباره راه اندازی کردیم و کلمات را وارد کردیم تا صـــحت و درســـتی کلمات را بســـنجیم و دســـتگـاه را reset factory کردیم تـا مطمعن شـــویم کـه کلمـات در آن ذخیره نبـاشـــنـد. در مرحله بعدی میخواهیم با وارد کردن کلمات به دســـتگاه کلید عمومی را به کیف پول بلووالت وارد کنیم تا یک کیف پول ناظر برای دریافت بیت‌کوین و دیدن موجودی داشته باشیم.

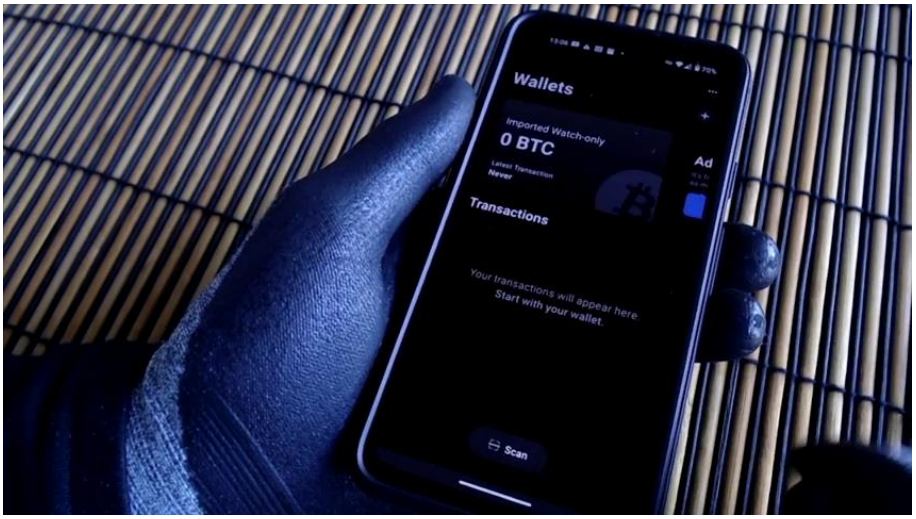
دوباره با راه اندازی دســـتگاه و وارد کردن کلمات بازیابی به آن به بخش settings رفته و گزینه Xpub export را انتخاب کنید.

یک Qrcode به شما نشان میدهد که همان آدرس عمومی کیف پول شماست که باید آن را به بلووالت وارد بکنید. برای وارد کردن کلید عمومی به بلووالت وارد نرم افزار آن شوید و import wallet را انتخاب کنید و با scan کردن Qrcode از روی کیف پول JADE شما کیف پول خود را به حالت ناظر بر روی گوشی موبایل خود دارید.



از منوی settings در بلووالت گزینه show addresses را انتخاب کنید و میتوانید آدرس‌های دریافتی که توسط کلمات خصوصی شما تولید شدند را مشاهده و توسط این آدرسها میتوانید بیت‌کوین دریافت کنید.

برای اطمینان از اینکه آدرسهای دریافتی در بلووالت متعلق به خود ما هستند میتوان یک تراکنش دریافت در کیف پول ناظر ایجاد کرد، و در منوی اصلی JADE گزینه scan را انتخاب میکنیم و آدرس دریافتی را اسکن میکنیم .اگر آدرس تراکنش دریافتی ایجاد شده از آدرسهای اصلی خود ما باشد JADE آن را تایید میکند و مطمعن میشویم که برای دریافت مشکلی وجود نخواهد بود. و میتوانیم بیت‌کوین دریافت کنیم.



حال مقداری بیت‌کوین به یکی از آدرسها ارسال شده است و میخواهیم آنرا خرج کرده که نحوه ارسال بیت‌کوین را از طریق JADE بررسی کنیم.

برای ارسال بیت‌کوین یک تراکنش ارسال توسط بلووالت ایجاد کنید و مقدار بیت‌کوین برای ارسال و فی را مشخص و تراکنش را ایجاد کنید.

پس از ایجاد تراکنش یک Qrcode از تراکنش به شما داده میشود به یک PSBT میباشد. در نرم افزار بلووالت مشخص شده است که شما اجازه ارسال بیت‌کوین را ندارید چون یک کیف پول ناظر هستید و برای ارسال بیت‌کوین باید این PSBT امضا شود. امضا این تراکنش توسط کیف پولی باید انجام شود که کلید خصوصی شما را در اختیار دارد و در این آموزش این کیف پول JADE میباشد.

ما Qrcode ایجاد شده توسط بلووالت را توسط JADE اسکن میکنیم و مشخصات تراکنش در کیف پول JADEنشان داده میشود که شما حتما حتما باید آن را با تراکنش در بلووالت تطبیق بدهید و از صحت آن اطمینان حاصل کنید.

پس از امضا تراکنش توسط JADE که کلید های خصوصی ما را در اختیار دارد یک Qrcode جدید آشکار میشود که یک PSBT جدید است از تراکنش امضا شده. توسط بلووالت PSBT امضا شده را اسکن میکنیم و حال تراکنش را به شبکه بیت‌کوین ارسال میکنیم و منتظر میمانیم تا تایید شود و ارسال انجام پذیرد.

این راهنما برای " استفاده عموم " منتشر میشود و بازنشر آن به هر شکل آزاد است.

سازنده:

حمیدرضا

Follow me on

Twitter : @hamid_rreza

Nostr : npub1jjw63779gl2lan6yu2fz3w67ruja40mnh8s3npvhesx82m4yvlsq4wg49z