



مروری بر روش‌های امن
نگهداری از بیت کوین؛ از مبتدی تا پیشرفته

سخنی با خوانندگان

در این خودآموز روش‌های نگهداری امن از بیت کوین را قدم به قدم از سطح مبتدی تا پیشرفته توضیح می‌دهیم. دقت کنید، برای نگهداری از بیت کوین روش‌های متعددی وجود دارد و هرکس باید شخصا با توجه به شعار بیت کوین که «بانک خود باشید» نسبت به انتخاب روشی که به نظر او بهترین روش است اقدام کند.

ارقام و محدوده‌های پیشنهاد شده برای انتخاب روش نگهداری از بیت کوین نسبت به سرمایه، صرفا به این دلیل معرفی شده‌اند تا خواننده یک دید کلی از موضوع داشته باشد و به هیچ وجه قطعی و استاندارد نیستند. هرکس باید نسبت به توانایی و اندازه دارایی خود نسبت به انتخاب یک روش مناسب برای نگهداری از سرمایه‌اش اقدام کند.

چه بسا نگهداری از بیت کوین روی صرافی برای شخصی که امکانات و ابزارهای لازم را برای در اختیار گرفتن کلیدهای بیت کوین ندارد، روش مناسب‌تری باشد. هرچند در این روش فرد باید ریسک از دست دادن دارایی خود را هم بپذیرد.

دانش و مقدار دارایی شما باید با روش نگهداری شما از بیت کوین تان مطابقت داشته باشد. اگر به حوزه بیت کوین تازه وارد شده‌اید و مقدار زیادی بیت کوین در صرافی یا نزد یکی از دوستان معتمد خود به امانت گذاشته‌اید باید این نکته را در نظر بگیرید که بیت کوین مثل اسکناس است، هرکس به کلیدخصوصی شما دسترسی داشته باشد در واقع صاحب اختیار آن خواهد بود.

موجودی بیت کوین شما در پورتال صرافی فقط یک عدد است که در سیستم حسابداری آن ذخیره شده است. هرچند بیت کوین‌های صرافی‌ها تحت یک سیستم امنیتی فوق‌العاده حساس نگهداری می‌شوند، اگر تحت هر شرایطی هکرها به آن دسترسی پیدا کنند، این بیت کوین‌ها به سرقت خواهد رفت و شما می‌مانید و بخت‌تان برای پس گرفتن بیت کوین‌هایی که در آن صرافی یا سایت قرار داده بودید. اگر فکر می‌کنید این اتفاق محال ممکن است درباره هک صرافی‌های مختلف در سرتاسر جهان تحقیق کنید.

بهترین راه نگهداری از بیت کوین این است که مسئولیت نگهداری از کلید خصوصی آن را شخصا به عهده بگیرید. هر کس که از عهده انجام کارهای معمولی با سیستم‌عامل موبایل و کامپیوتر شخصی‌اش برمی‌آید قادر خواهد بود از بیت کوین‌هایش هم نگهداری کند و این مساله کار پیچیده‌ای نیست.

اما قبل از هر اقدامی باید برای انجام دادن آن آموزش ببینید و این موضوعی است که به هیچ‌وجه نباید به‌سادگی از کنار آن رد شوید. پس زمان بگذارید و روش‌های مختلف را بررسی کنید و بعد برای به‌عهده گرفتن مسئولیت نگهداری از کلیدهای خصوصی بیت کوین‌تان تصمیم بگیرید.

راهنمای زیر را تا انتها مطالعه کنید و قبل از هر اقدامی حتما روی شبکه تست بیت کوین تمرین کنید تا خیال شما از هر نظر راحت باشد و با یک اشتباه کوچک سرمایه و دارایی خود را از دست ندهید.

گردآوری: ر.فرد

منابع فارسی بیت کوین

سطوح و روش‌های مختلف نگهداری امن از بیت کوین؛ بسته به میزان دارایی

نهنگ (پیشرفته)	کوسه (ماهر)	دلفین (با تجربه)	ماهی کوچک (مبتدی)	
ارقام بالا - موسسات مالی	۳-۶ برابر <u>درآمد سالانه</u>	۲-۳ برابر <u>درآمد سالانه</u>	۲ برابر <u>درآمد ماهانه</u>	مناسب برای نگهداری از دارایی تا ماکزیمم*
کلداستوریج چند امضائی	کلداستوریج تک امضائی	کیف پول دسکتاپ	کیف پول موبایل	ابزار و روش
فول نود و سرویس‌های اختصاصی (تور) (Archival)	فول نود اختصاصی (تور) (Pruned)	سرورهای عمومی	سرورهای عمومی	ارسال و دریافت تراکنش‌ها از
اختصاصی	عمومی (تور)	عمومی	عمومی	بلاک اکسپلورر
بالا	قابل قبول	پایین	پایین	حریم خصوصی در سطح شبکه**
کاغذ و تاس	کاغذ و تاس	کیف پول + کلمه ۱۲م	کیف پول	ساختن کلید خصوصی با
بالا	بالا	خوب	قابل قبول	کیفیت کلید خصوصی***

* دقت کنید، این ارقام ممکن است برای هر فرد متفاوت باشند.

** برای مشاهده توضیحات درباره حریم خصوصی به بخش پیوست مراجعه کنید.

*** کیفیت آنتروپی^۱ (امنیت) کلید خصوصی ساخته شده.

1 Entropy



ماهی کوچک
(سطح مبتدی)

کیف پول موبایل BlueWallet

آموزش نصب و طرز کار این کیف پول را در ویدیوی زیر به فارسی ببینید.



<https://archive.org/details/blue-wallet-mcsaeid>

ویژگی‌ها

- کیف پول اپن سورس^۱ با حدود ۳ سال سابقه فعالیت.
- روی سیستم‌عامل‌های موبایل iOS و android اجرا می‌شود.
- با وجود اینکه یک اپلیکیشن موبایل است، قابلیت‌های خوبی به کاربر می‌دهد.

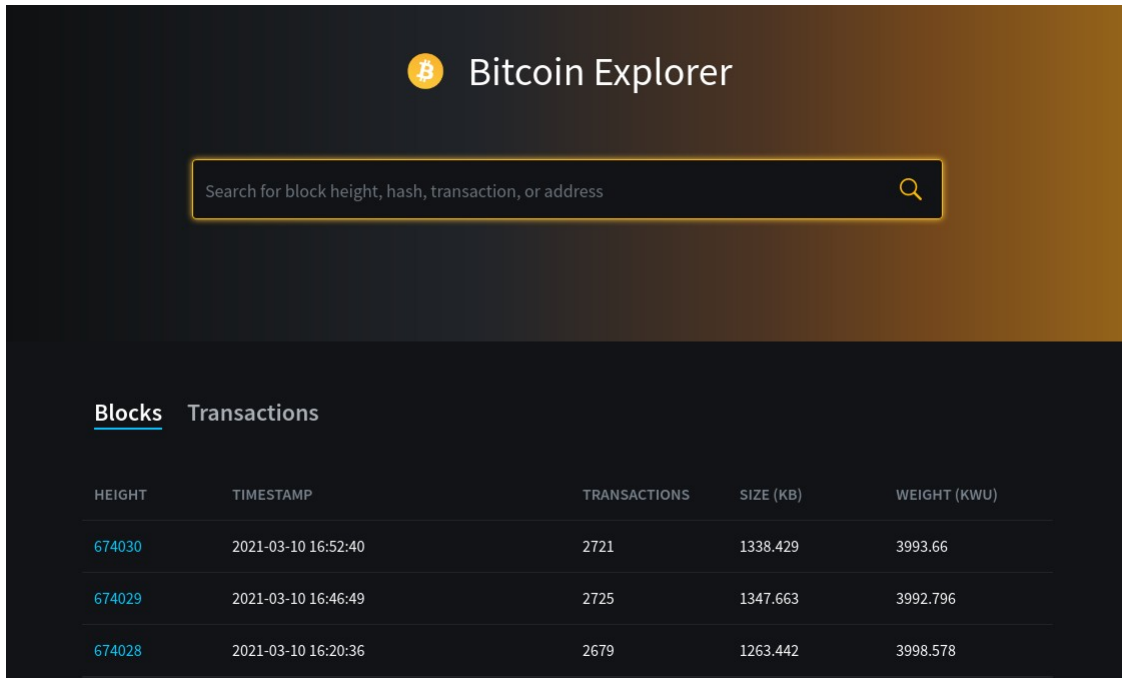
نکته خیلی مهم: شما باید از کلمات بازیابی^۲ تولید شده توسط این کیف پول یک نسخه پشتیبان تهیه کنید. همچنین باید یک رمز عبور دشوار روی کیف پول بیت کوین خود تعریف کنید. برای آگاهی بیشتر به پیوست مراجعه کنید.

1 Open source

2 Seed words

بلاک اکسپلورر Block Explorer

برای اطلاع از وضعیت تراکنش‌های بیت‌کوینی از بلاک اکسپلوررها استفاده می‌شود. ویدیوی زیر روش کار با این سرویس‌های عمومی را به فارسی آموزش می‌دهد.



HEIGHT	TIMESTAMP	TRANSACTIONS	SIZE (KB)	WEIGHT (KWU)
674030	2021-03-10 16:52:40	2721	1338.429	3993.66
674029	2021-03-10 16:46:49	2725	1347.663	3992.796
674028	2021-03-10 16:20:36	2679	1263.442	3998.578

<https://archive.org/details/block-explorer>

سرویس‌های عمومی و رایگان بلاک اکسپلورر

1. <https://live.blockcypher.com/btc>
2. <https://blockstream.info>

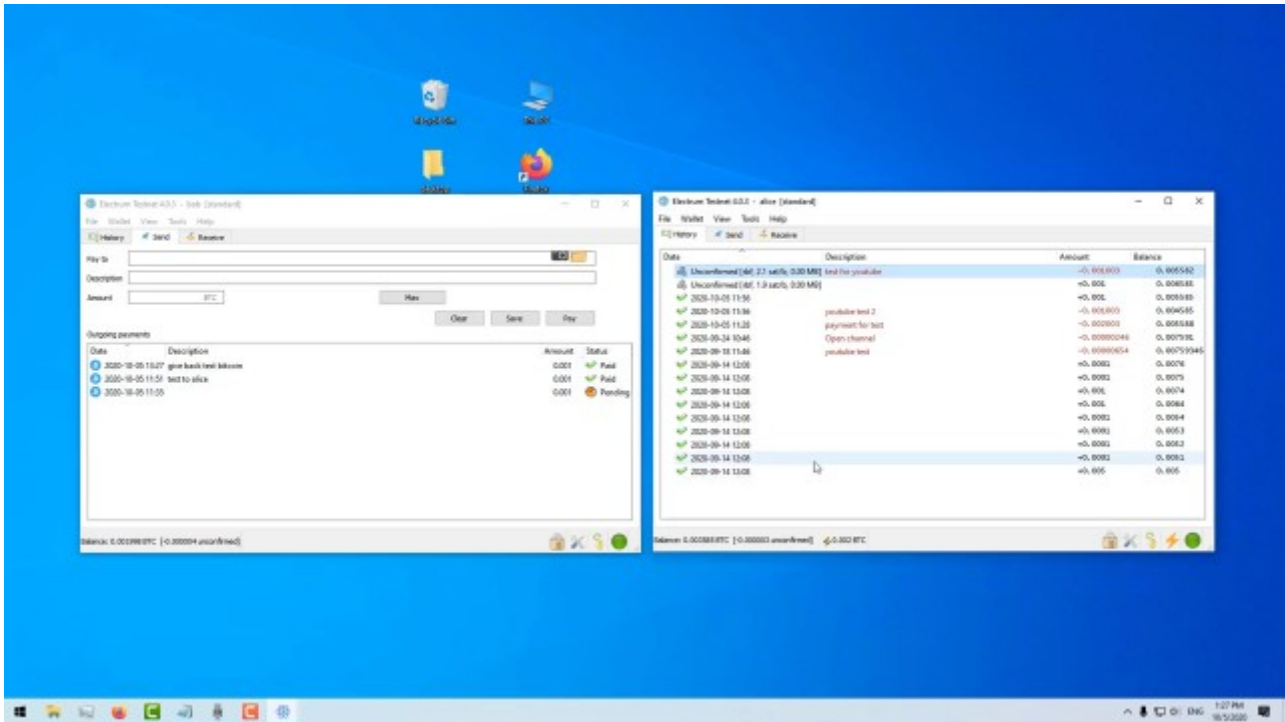
نکته خیلی مهم: استفاده از سرویس‌های عمومی اثر مستقیم روی حریم خصوصی مالی می‌گذارند و آن را کاهش می‌دهند. این مشکل در مراحل بالاتر با استفاده از سرویس‌های اختصاصی رفع می‌شود.



دلفین
(سطح با تجربه)

کیف پول دسکتاپ Electrum Wallet

آموزش نصب و طرز کار این کیف پول را در ویدیوی زیر به فارسی ببینید.



<https://archive.org/details/electrum-wallet>

ویژگی‌ها

- این کیف پول اپن سورس^۱ است و حدود ۱۰ سال سابقه فعالیت دارد.
- روی همه سیستم‌عامل‌های دسکتاپ نصب می‌شود و امکانات متنوعی دارد.

نکته خیلی مهم: شما باید از کلمات بازیابی^۲ تولید شده توسط این کیف پول یک نسخه پشتیبان تهیه کنید. همچنین باید یک رمز عبور دشوار روی کیف پول بیت کوین خود تعریف کنید. برای آگاهی بیشتر به پیوست مراجعه کنید.

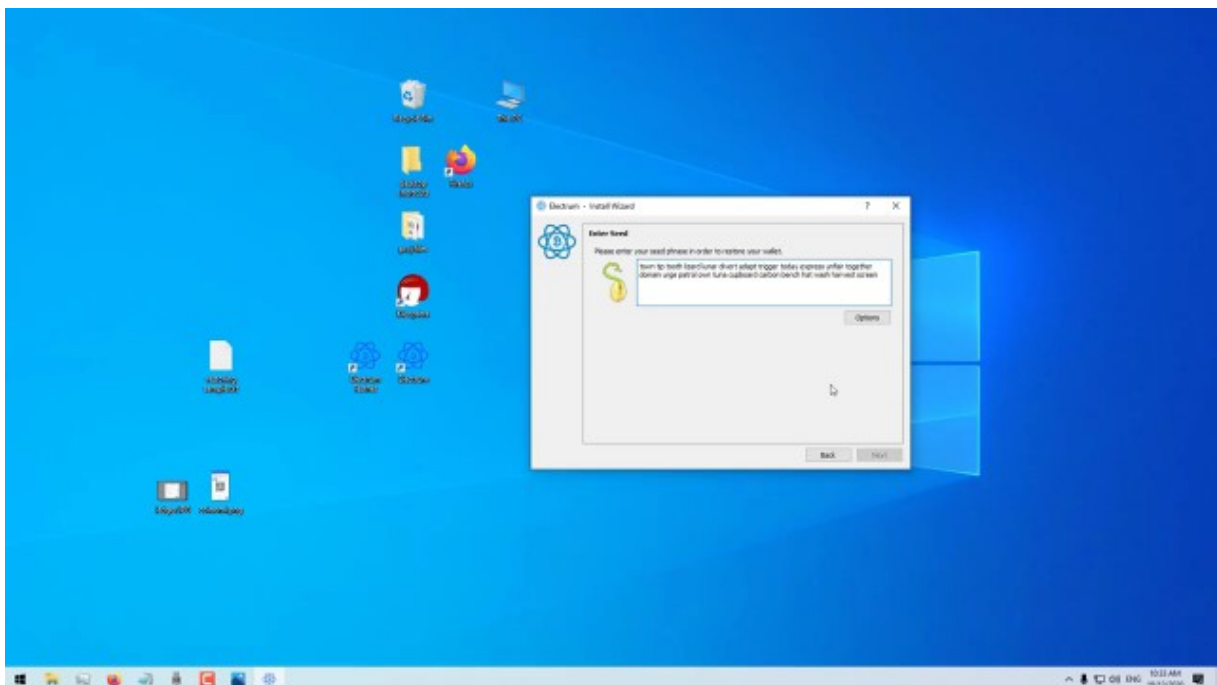
1 Open source
2 Seed words

کلمه سیزدهم یا پسرینز^۱

برای افزایش امنیت کلمات بازیابی که توسط کیف پول شما ساخته شده است، می‌توانید یک کلمه (یا حتی جمله) به عنوان کلمه سیزدهم به آن اضافه کنید. در زمان بازیابی^۲ کیف پول باید این کلمه را هم در اختیار داشته باشید. برای اطلاعات بیشتر ویدیوی زیر را ببینید و به پیوست مراجعه کنید.

نکته مهم درباره کلمات بازیابی تولید شده توسط کیف پول الکترام

کلمات بازیابی تولید شده توسط این کیف پول فقط درون همین کیف پول بازیابی می‌شوند. برای اطلاعات بیشتر و آموزش روش بازیابی، ویدیوی فارسی زیر را ببینید.

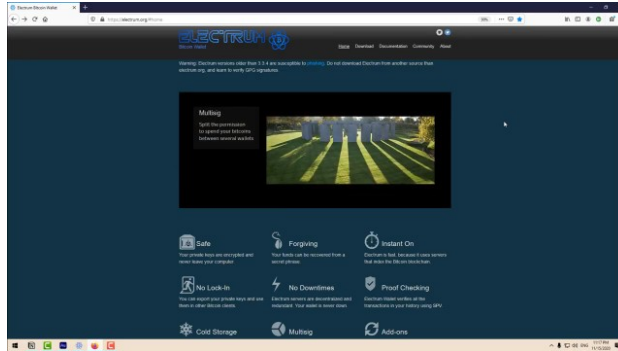


https://archive.org/details/20201225_20201225_1240

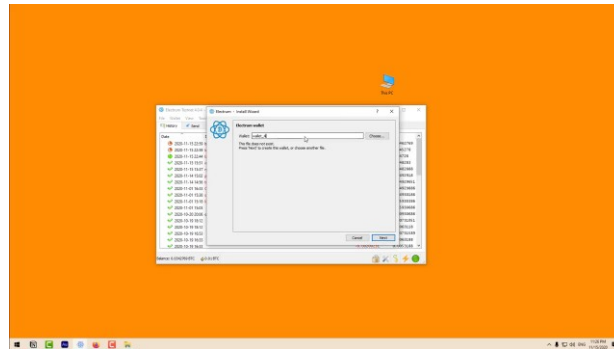
- 1 passphrase
- 2 restore

امکانات مختلف کیف پول دسکتاپ الکترام

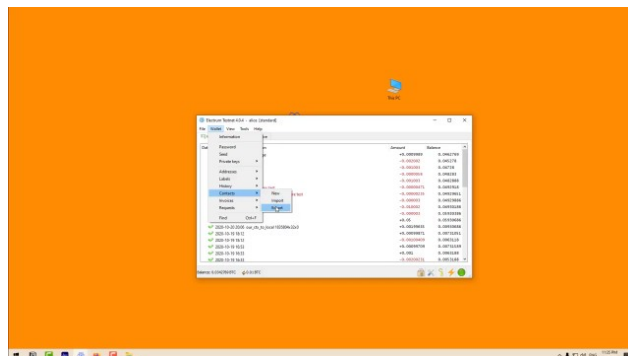
کیف پول دسکتاپ الکترام طیف گسترده‌ای از امکانات را برای کاربران خود فراهم می‌کند. برای اطلاع از این امکانات ویدیوهای زیر را که در سه قسمت و به فارسی تهیه شده‌اند ببینید.



https://archive.org/details/20201225_20201225_1246



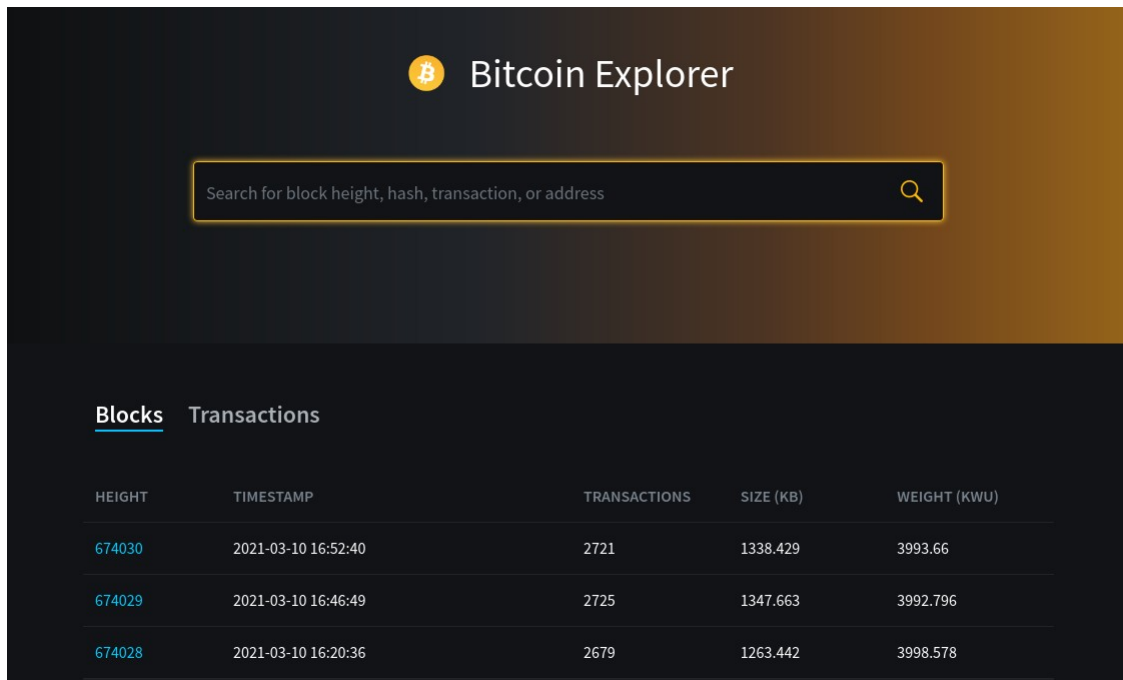
https://archive.org/details/20201225_20201225_1248



https://archive.org/details/20201225_20201225_1244

بلاک اکسپلورر Block Explorer

برای اطلاع از وضعیت تراکنش‌های بیت‌کوینی از بلاک اکسپلوررها استفاده می‌شود. ویدیوی زیر روش کار با این سرویس‌های عمومی را به فارسی آموزش می‌دهد.

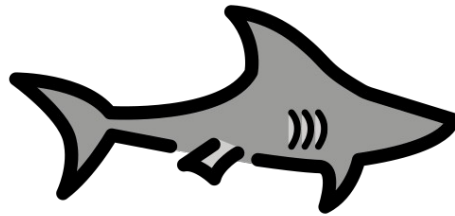


<https://archive.org/details/block-explorer>

سرویس‌های عمومی و رایگان بلاک اکسپلورر

1. <https://live.blockcypher.com/btc>
2. <https://blockstream.info>

نکته خیلی مهم: استفاده از سرویس‌های عمومی عمومی اثر مستقیم روی حریم خصوصی مالی می‌گذارند و آن را کاهش می‌دهند. این مشکل در مراحل بالاتر با استفاده از سرویس‌های اختصاصی رفع می‌شود.

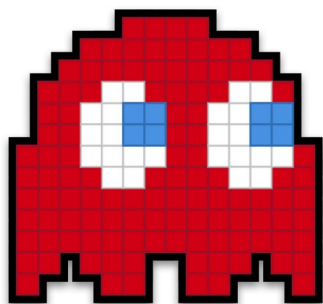


کوسه
(سطح ماهر)

یک لپ‌تاپ برای اجرای فول نود بیت کوین و نرم‌افزار Specter Desktop در حالت ناظر^۱ و یک عدد تاس برای تولید کلمات بازیابی^۲ (به پیوست مراجعه کنید)



تولید کلمات بازیابی
با استفاده از کاغذ و تاس



کیف پول
Specter Desktop



یک لپ‌تاپ یا دسکتاپ
با مشخصات معمولی

به همراه یکی از گزینه‌های زیر به‌عنوان کیف پول کلداستوریج^۳



کیف پول موبایل
الکترام آفلاین



کیف پول
سخت‌افزاری



لپ‌تاپ یا یک سیستم
آفلاین به‌صورت VM

1 Watching only
2 BIP39 Seed Words
3 Cold storage

نصب فول نود کم حجم^۱ بیت کوین

روش نصب فول نود بیت کوین را در ویدیوی آموزشی فارسی زیر ببینید.



<https://archive.org/details/pruned-bitcoin-node>

- برای اجرای بیت کوین فول نود در حالت کم حجم، دسکتاپ یا لپ تاپ شما باید
- به اینترنت متصل باشد ولی می توانید آن را خاموش کنید و فقط در زمان استفاده از کیف پول و برای دریافت یا ارسال بیت کوین آن را روشن و به اینترنت متصل کنید.
- با توجه به اینکه کلید خصوصی^۲ شما به صورت آفلاین (کلداستوریج) و در مکانی جدا از سیستم آنلاین شما ذخیره شده است، می توانید نرم افزارهای مورد نیاز روزانه را بر روی سیستم آنلاین خود نصب کنید. یعنی لازم نیست این سیستم را فقط به کیف پول بیت کوین خود اختصاص دهید. هرچند اگر با این سیستم بی پروا به هر سایتی سر می زنید و هر نرم افزاری روی آن اجرا می کنید بهتر است مراقب باشید.

1 Pruned

2 Private key

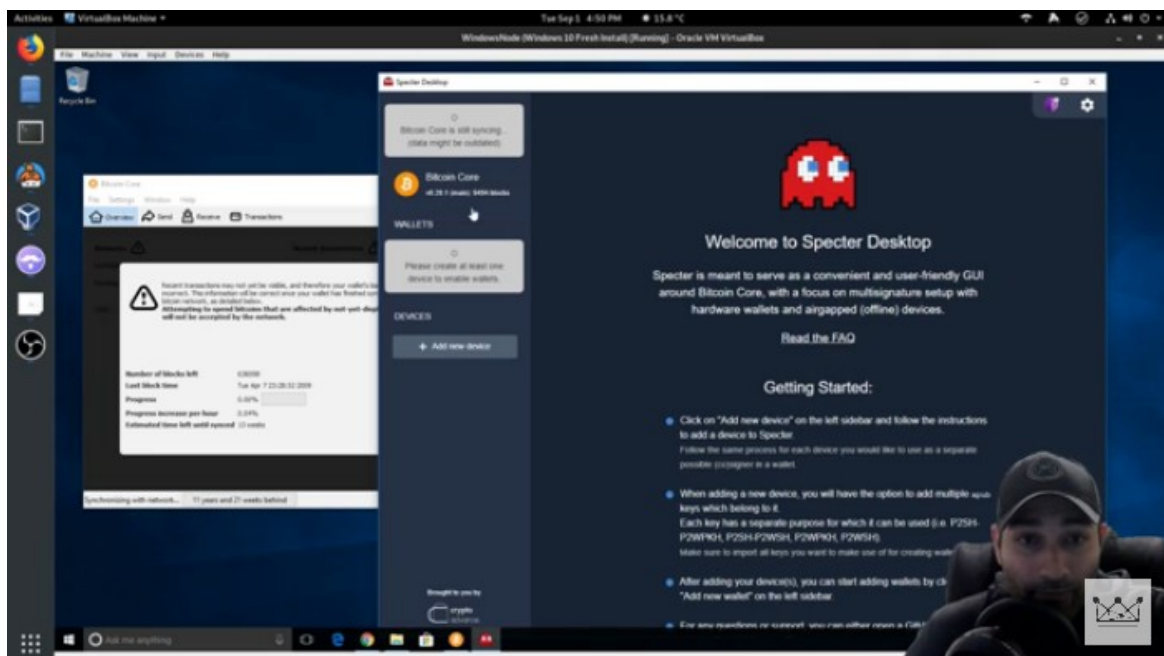
کیف پول اسپکتر Specter Desktop

ویژگی‌ها

- اپن سورس و قابل نصب بر روی همه سیستم‌های عامل
- قابلیت اتصال به فول نود شخصی
- قابلیت به کار گیری کیف پول‌های سخت افزاری و کار در حالت ناظر^۱

برای اطلاع بیشتر از قابلیت‌های این کیف پول صفحه سوالات تکراری^۲ آن را در صفحه گیت‌هاب^۳ پروژه بخوانید.

این ویدیو به زبان انگلیسی روش نصب بر روی سیستم عامل ویندوز را آموزش می‌دهد. طرز استفاده از Specter به همراه یک کیف پول سخت‌افزاری روی شبکه تست بیت کوین، در پیوست همین راهنما قرار دارد.



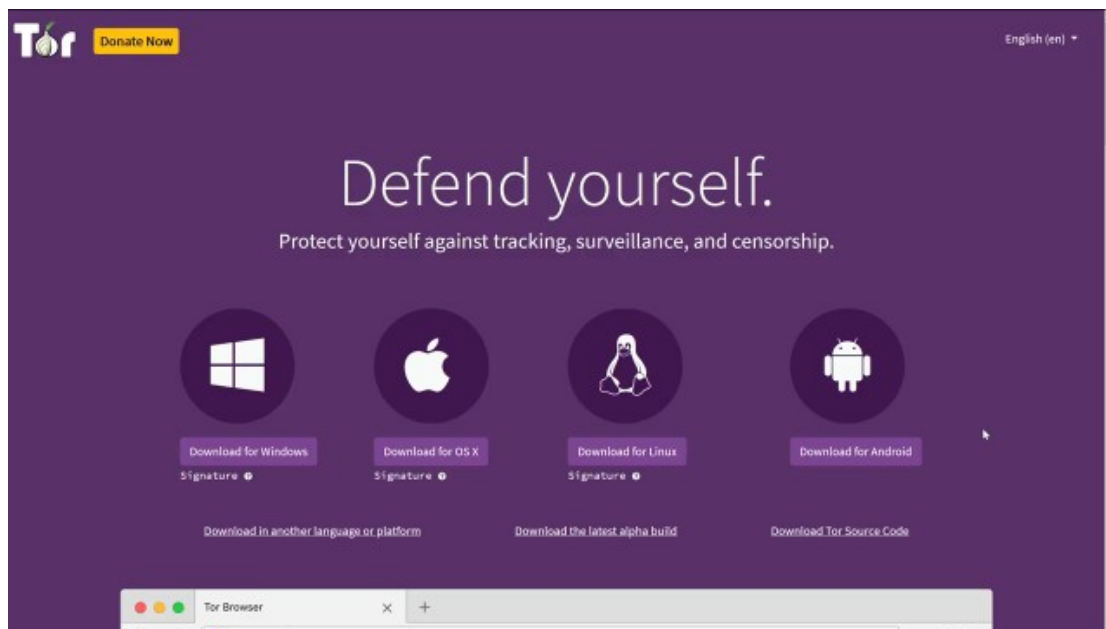
<https://www.youtube.com/watch?v=4koKF2MDXtk>

- 1 Watching only
- 2 FAQ
- 3 <https://github.com/cryptoadvance/specter-desktop/blob/master/docs/faq.md>

بلاک اکسپلورر Block Explorer

برای اطلاع از وضعیت تراکنش‌های بیت‌کوینی از بلاک اکسپلوررها استفاده می‌شود. برای حفظ حریم خصوصی مالی در سطح متوسط، در زمان بازدید از اکسپلوررهای عمومی از مرورگر تور^۱ استفاده می‌کنیم.

روش نصب مرورگر تور را در ویدیوی آموزشی فارسی زیر ببینید.

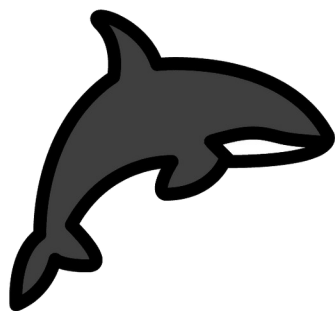


<https://archive.org/details/electrum-bitcoind>

سرویس‌های عمومی و رایگان بلاک اکسپلورر

1. oxt.me
2. <https://blockstream.info>
<http://explorerzydxu5ecjrkwceayqybizmpjjznk5izmitf2modhcsuqlid.onion>

1 Tor browser



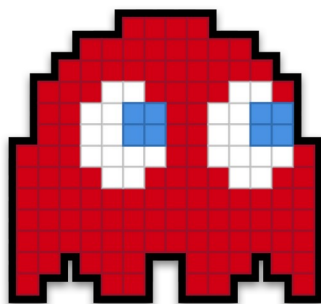
نهنگ
(سطح پیشرفته)

ابزارهای لازم

یک لپ تاپ برای اجرای فول نود بیت کوین به همراه آرشیو بلاک های بیت کوین^۱، و نرم افزار Specter Desktop به عنوان یکی از امضاء کنندگان و تنظیم آن در حالت ناظر^۲، و یک عدد تاس برای تولید کلمات بازیابی^۳ (به پیوست مراجعه کنید)



تولید کلمات بازیابی
با استفاده از کاغذ و تاس



کیف پول
Specter Desktop



یک لپ تاپ یا دسکتاپ
با مشخصات فنی تقریباً بالا^۴

به همراه کیف پول های سخت افزاری (انتخاب اختیاری)، و سرویس بلاک اکسپلورر



کیف پول موبایل
الکترام آفلاین



کیف پول
سخت افزاری

BTC RPC Explorer

Network Summary		
Height	Blockchain	Timestamp
181 / 181,000	181,000,000	181,000,000
Difficulty	Exchange Rate	Block Size
15,782,387	181,000,000	1,000,000
Pending Tx	Unspent Sat	Miner Cap
17,407	55,864,348,000	1,000,000,000
Fee Target	Total Supply	
55,864,348,000	181,000,000,000	
Block Time (min)		
10-15 (10-15)		

Tools

- Nodes Status
- Block Chain
- Block Analysis
- Mining Summary
- Transaction Data
- Network Summary
- Difficulty History
- Miner Details
- Network Pending Tx
- Price
- RPC Explorer
- BTC Terminal
- Blockchain

بلاک اکسپلورر
اختصاصی

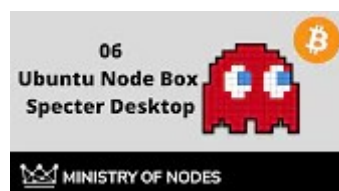
- 1 Bitcoin archival node
- 2 Watching only
- 3 BIP39 Seed Words
- 4 At least: i3 CPU, 8GB RAM, 1TB SSD

نصب نرم افزارها و سرویس ها

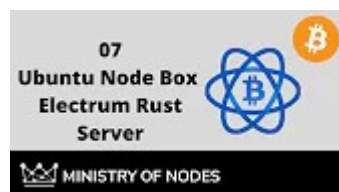
در حال حاضر ویدیوی آموزشی فارسی برای نصب کیف پول و سرویس های لازم در سطح پیشرفته تهیه نشده است. ویدیوهای آموزشی زیر روش نصب سرویس های لازم را از قدم اول بر روی سیستم عامل لینوکس به زبانی روان آموزش می دهند.



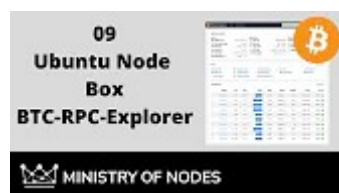
نصب فول نود بیت کوین
در حالت فول آرشیو



نصب کیف پول
Specter Desktop



نصب زیرساخت
لازم برای بلاک اکسپلورر



نصب بلاک اکسپلورر

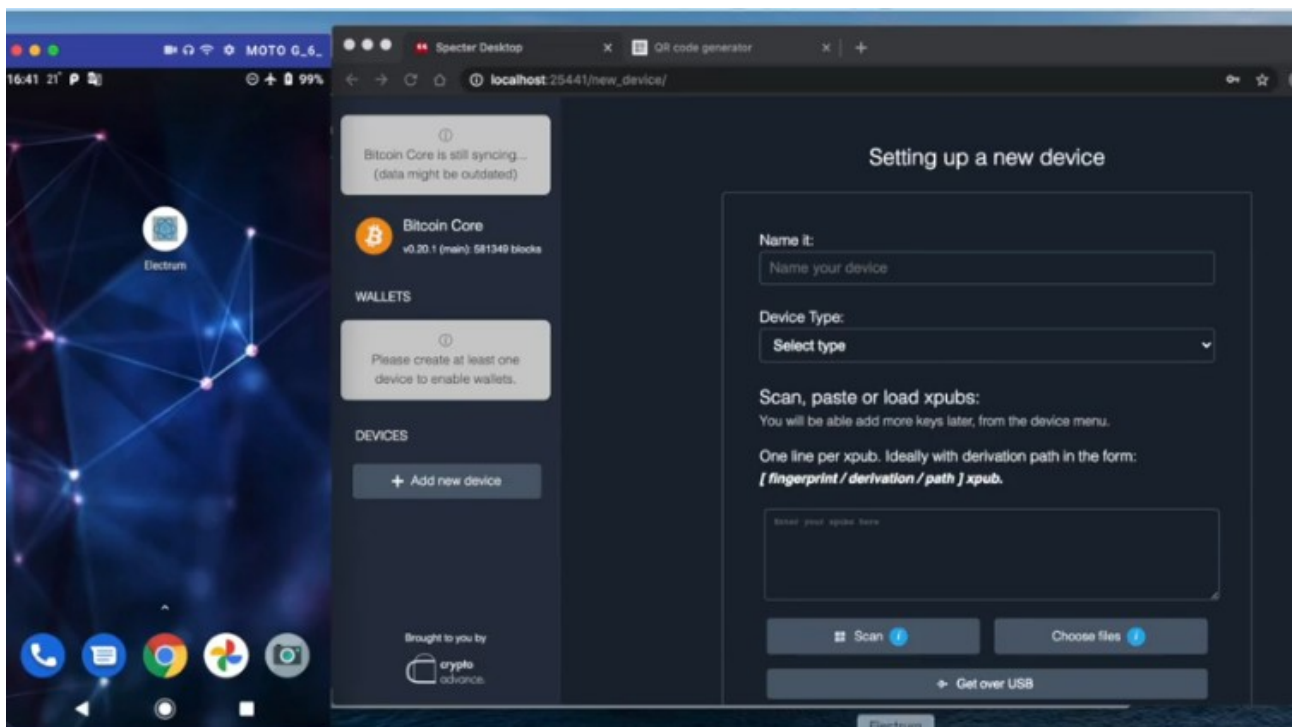
برای مشاهده همه ویدیوهای این مجموعه به آدرس زیر بروید

<https://www.youtube.com/playlist?list=PLCRbH-IWlcw29000N0lQV6efxuCA5Ja8c>

کیف پول اسپکتر در حالت چند امضائی

از روش‌های متنوعی می‌توان در اسپکتر یک کیف پول چند امضائی ساخت. در حال حاضر ویدیوی آموزشی طرز کار با این کیف پول به زبان فارسی تهیه نشده است. ویدیوی آموزشی زیر طرز کار این کیف پول در حالت چند امضائی را به زبان انگلیسی آموزش می‌دهد.

در این ویدیو برای ساختن یک کیف پول چند امضائی ۲ از ۳، از یک کیف پول الکترا بر روی یک گوشی موبایل در حالت هواپیما، به علاوه یک کیف پول دسکتاپ الکترا، به همراه کیف پول Bitcoin Core که همیشه در حالت آنلاین قرار دارد استفاده می‌شود.

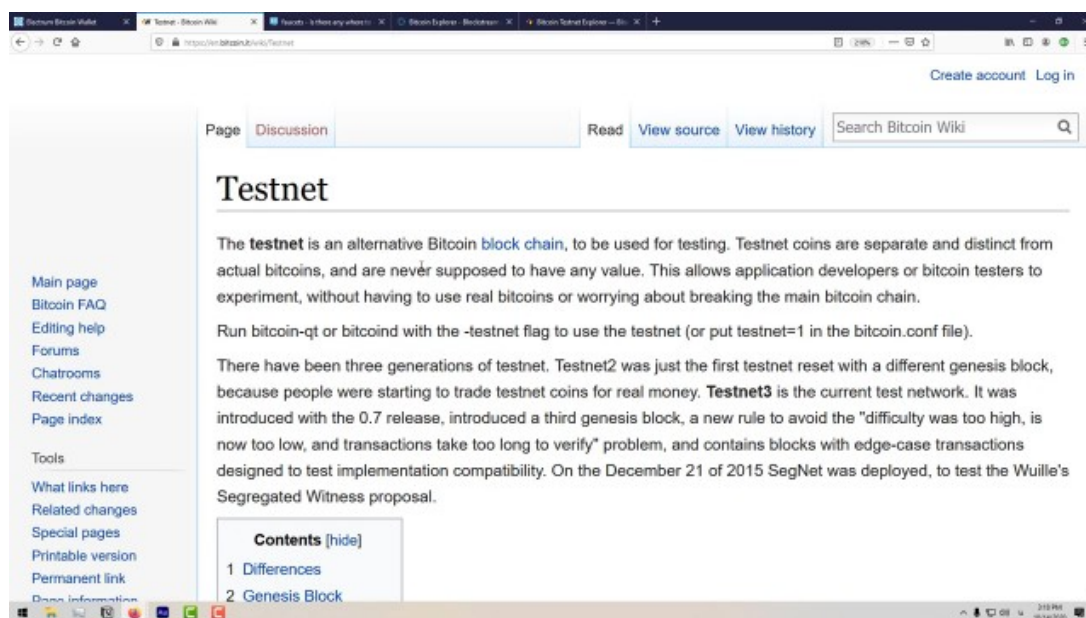


<https://www.youtube.com/watch?v=4YXkLLh2srA>

این بخش شامل اطلاعات تکمیلی و پاسخ به پرسش‌هایی است که ممکن است برای خوانندگان پیش آمده باشد.

چطور می‌توان این روش‌ها را در یک محیط آموزشی و بدون ترس از دست دادن دارایی تمرین کرد؟

شبکه بیت کوین یک شبکه برای انجام تست و تمرین با بیت کوین‌های مشقی^۱ به نام «تستنت»^۲ دارد. کوین‌ها در این شبکه ارزش مالی ندارند و صرفاً برای تمرین به کار گرفته می‌شوند. در ویدیوی زیر نحوه کار با شبکه تستنت و به دست آوردن کوین‌های مشقی به زبان فارسی توضیح داده شده است.



<https://archive.org/details/testnet>

- 1 Testnet bitcoin (tBTC)
- 2 Testnet

فرق کلمات بازیابی^۱، پسریز^۲، و پسورد^۳ در چیست؟

درک این مفاهیم در عین سادگی بسیار مهم و تعیین کننده است.

کلمات بازیابی

این کلمات در واقع نماد کلید خصوصی^۴ کیف پول شما هستند. برای همین همه کیف پول‌های بیت کوین بعد از ساختن این کلمات از شما می‌خواهند آن‌ها را حتما یادداشت کنید و در یک جای امن نگهداری کنید. هر کس به این کلمات دسترسی داشته باشد، در واقع صاحب‌اختیار بیت کوین‌های ذخیره شده در آن است.

پسریز

این کلمه (یا کلمات) در واقع به کلمات بازیابی اضافه می‌شوند و آن را بسط می‌دهند. دلیل آن این است که با این روش شما امنیت کلید خصوصی خود را افزایش می‌دهید. در انتخاب آن دقت کنید و از انتخاب کاراکترهای خاص که فقط در زبان‌های خاصی وجود دارند پرهیز کنید. پسریز شما به اندازه کلمات بازیابی اهمیت دارند و در هنگام بازیابی بیت کوین‌ها به آن نیاز دارید.

پسورد

نرم‌افزار کیف پول شما از پسورد استفاده می‌کند و فایل کیف پول شما را برای امنیت بیشتر با آن رمزگذاری می‌کند. حتما از یک پسورد دشوار که قابل حدس زدن نیست استفاده کنید. برای بازیابی بیت کوین‌هایتان نیازی به دانستن پسورد نخواهید داشت.

1 Seed / mnemonic
2 passphrase
3 password
4 Private key

به طور کلی برای دریافت، نگهداری، و انتقال بیت کوین به چه ابزارهایی نیاز داریم؟

ما برای دریافت، نگهداری، و ارسال بیت کوین به اجزاء زیر نیاز داریم.

- کلید خصوصی
- وسیله‌ای برای امضای تراکنش‌ها
- نرم‌افزار کیف پول بیت کوین

تفاوت میان این اجزاء مختلف ممکن است در ابتدا کمی گیج‌کننده به نظر برسد، ولی شناخت آن‌ها به درک بهترین روش‌های نگهداری از بیت کوین کمک زیادی می‌کند.

کلید خصوصی

کلید خصوصی شما اغلب شامل لیستی از ۱۲ یا ۲۴ کلمه است که در اختیارتان قرار می‌گیرد. این کلمات بسیار حساس، محرمانه، و خصوصی هستند و شما برای امضای تراکنش‌های خود به آن‌ها نیاز خواهید داشت. هرکسی به کلید خصوصی شما دسترسی داشته باشد می‌تواند بیت کوین شما را خرج، یا به حساب خود منتقل کند، برای همین باید تا جایی که ممکن است از آن‌ها مراقبت کنید.

همچنین اگر قصد دارید از کسی بیت کوین دریافت کنید، برای ساختن یک آدرس بیت کوین به کلید خصوصی شما نیاز است. اگر بعداً بخواهید این بیت کوین دریافت شده را خرج یا برای فرد دیگری ارسال کنید، برای ساختن امضای دیجیتالی مختص به این آدرس، مجدداً به کلید خصوصی نیاز پیدا خواهید کرد. این امضای دیجیتالی ثابت می‌کند فردی که می‌خواهد کوین‌ها را از یک آدرس مشخص به یک آدرس دیگر منتقل کند،

در واقع همان کسی است که آدرس مبدأ را تولید کرده، چون کلید خصوصی فقط در اختیار صاحب کوین‌ها (یا به عبارت دیگر صاحب آدرس مبدأ) است. به‌طور خلاصه، کلید خصوصی اطلاعات محرمانه‌ای است که افراد با استفاده از آن مالکیت بر کوین‌هایشان را اثبات می‌کنند.

وسيله‌ای برای امضای تراکنش‌ها

از آنجا که نمی‌توان امضای دیجیتال یک تراکنش بیت کوین را به‌صورت دستی از روی کلید خصوصی محاسبه کرد، نیاز به وسیله‌ای پیدا می‌کنیم که این کار را برای ما انجام دهد. این وسیله قادر است جزئیات تراکنش مورد نظر و کلید خصوصی را از ما بگیرد و یک تراکنش امضا شده برای ما تولید کند.

این وسیله اغلب می‌تواند یک کامپیوتر معمولی یا تلفن همراه هوشمند شما باشد، اما یک گزینه محبوب دیگر استفاده از یک سخت‌افزار اختصاصی برای این کار است. به این وسیله یک کیف پول سخت‌افزاری گفته می‌شود که به‌طور خاص فقط برای امضا کردن تراکنش‌های بیت کوین از آن استفاده می‌شود.

دلیل اصلی رایج بودن این دستگاه‌ها این است که قادرند کلید خصوصی شما را در یک سخت‌افزار آفلاین ذخیره کنند و برای امضای تراکنش‌ها نیازی به وارد کردن کلید خصوصی روی کامپیوتر یا تلفن همراه هوشمند شما که به اینترنت متصل، و نرم‌افزارها و احیاناً بدافزارهای مختلفی روی آن‌ها نصب است، نخواهد بود. با این روش کلید خصوصی شما در معرض خطر قرار نمی‌گیرد و امنیت آن تأمین می‌شود.

درک تفاوت بین «کلید خصوصی» و «وسیله‌ای که تراکنش‌ها را امضا می‌کند» ضروری است. هرچند ممکن است این وسیله علاوه بر امضای تراکنش‌های شما، کلید خصوصی شما را هم تولید و از آن نگهداری کند، اما اصولاً این دو با هم متفاوت هستند.

می‌توانید کلید خصوصی خود را در هر وسیله‌ای که برای امضای تراکنش‌ها به کار گرفته می‌شود وارد و از آن استفاده کنید. کلید خصوصی شما هیچگونه وابستگی به این وسیله ندارد. این وسیله صرفاً برای انجام عملیات رمزنگاری و تولید امضای دیجیتال تراکنش‌های شما به کار گرفته می‌شود، در واقع بیت کوین‌های شما هیچگونه وابستگی به این وسیله ندارند و فقط به کلید خصوصی شما وابسته‌اند.

این وسیله یک دستگاه الکترونیکی است که برای امضا کردن تراکنش‌های شما مورد استفاده قرار می‌گیرد. شما اطلاعات ورودی تراکنش را به آن می‌دهید و این وسیله با استفاده از کلید خصوصی شما امضای دیجیتالی لازم را بر اساس قواعد رمزنگاری تولید و در نهایت تراکنش امضا شده را به عنوان خروجی به شما تحویل می‌دهد. این وسیله برای تولید امضای دیجیتال تراکنش از اطلاعات محرمانه و خصوصی شما یعنی کلید خصوصی استفاده می‌کند.

نرم‌افزار کیف پول بیت کوین

سومین جزء این پازل، نرم‌افزار کیف پول بیت کوین است که مسئول برقراری ارتباط و تعامل با شبکه بیت کوین است. نرم‌افزار کیف پول برای رصد کوین‌هایی که متعلق به کلید خصوصی افراد هستند (UTXO)، آماده‌سازی تراکنش‌ها قبل از امضا شدن آن‌ها توسط وسیله‌ای که آن‌ها را امضا می‌کند، و در نهایت انتشار آن‌ها در شبکه بیت کوین، مورد استفاده قرار می‌گیرد.

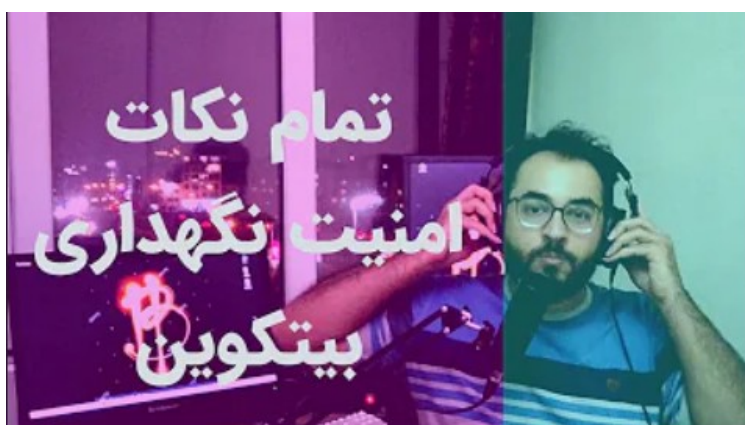
اگرچه ممکن است نرم افزار کیف پول و وسیله امضای تراکنش‌ها در قالب یک دستگاه با یکدیگر ترکیب شده باشند (مثل یک کیف پول داغ، که شما کلید خصوصی خود را روی یک کامپیوتر یا تلفن همراه هوشمندی که به اینترنت متصل است وارد می‌کنید)، اما اغلب برای اطمینان از آفلاین بودن مکانی که کلید خصوصی در آن نگهداری می‌شود، آن‌ها را از یکدیگر جدا می‌کنند.

نرم افزار کیف پول بیت کوین باید هر از چندگاهی به اینترنت وصل باشد تا بتواند اطلاعات مربوط به UTXOهای افراد را از شبکه بیت کوین دریافت، و تراکنش‌های امضا شده آنان را روی شبکه منتشر کند.

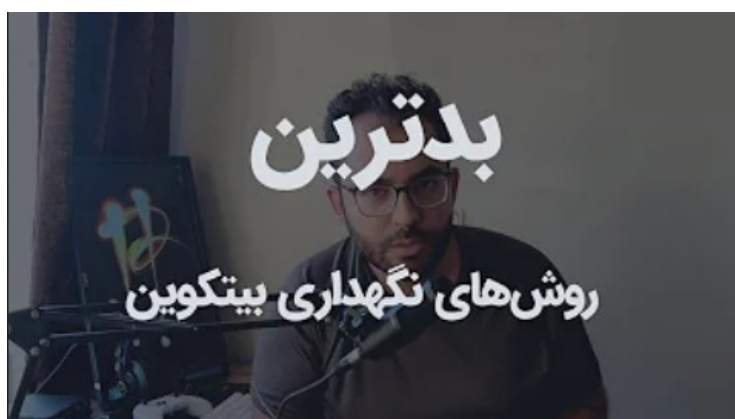
(این بخش ترجمه رشته توثیقی از [Ben Kaufman](#)، یکی از توسعه‌دهندگان کیف پول [Specter Wallet](#) است.)

روش درست نگهداری و پشتیبان گیری از کلمات بازیابی^۱

نگهداری از بیت کوین کار بسیار حساسی است و باید به درستی این کار را انجام داد. در این ویدیوها نکته‌هایی که درباره نگهداری از بیت کوین باید در نظر بگیرید به زبان فارسی توضیح داده شده است.



<https://archive.org/details/hold-bitcoin-securely-tips>



<https://archive.org/details/how-not-to-hold-bitcoin>

1 Seed words

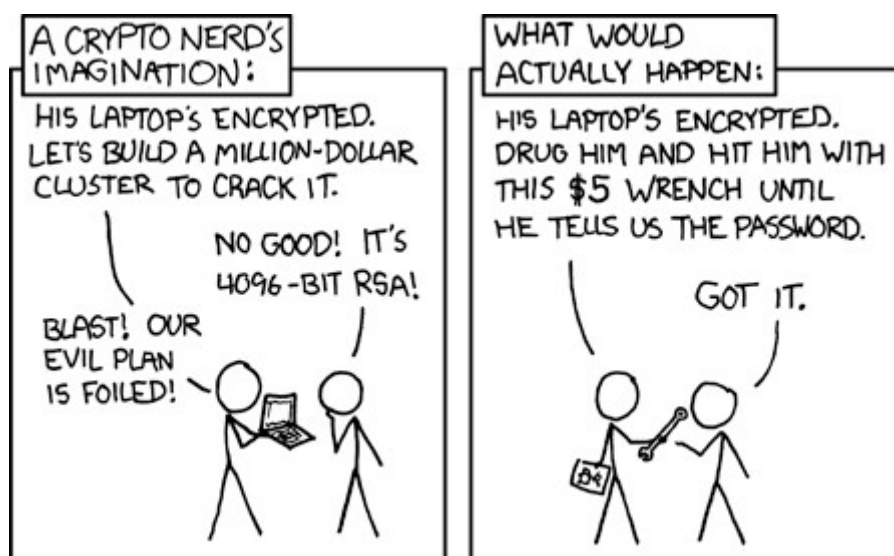
مفهوم امنیت فیزیکی در روش‌های نگهداری از بیت کوین

معمولاً ذهن افراد با شنیدن کلمه «امنیت» به سمت روش‌های پیچیده رمزنگاری و حفظ اطلاعات مربوط به کلیدهای خصوصی بیت کوین‌شان می‌رود. اما همان‌طور که پیشتر اشاره کردیم در مقوله نگهداری از بیت کوین، امنیت یک موضوع چندوجهی است که باید با دقت به آن پرداخته شود. یک نمونه که از قبل درباره آن توضیح دادیم بحث در نظر گرفتن امنیت در هنگام تولید کلیدهای خصوصی است.

امنیت فیزیکی هم یکی دیگر از حوزه‌های مهم در زمینه نگهداری امن از بیت کوین است و در این قسمت سعی می‌کنیم در دو بخش مجزا آن را بررسی کنیم.

تأمین امنیت فیزیکی کلیدهای خصوصی

ممکن است شما کلید خصوصی بیت کوین خود را با استفاده از یک روش کاملاً امن رمزگذاری کرده باشید ولی از طرف دیگر در نظر داشته باشید که اگر شما حریم خصوصی مالی خود را به خوبی حفظ نکرده باشید، این امکان وجود دارد که فرد یا افرادی انگیزه داشته باشند تا با اعمال خشونت و زور به کلیدهای خصوصی شما دسترسی پیدا کنند و بیت کوین شما را به سرقت ببرند.



برای حل این مشکل از یک روش مؤثر به نام «انکار موجه»^۱ استفاده می‌کنیم که در هر ۴ سطح معرفی شده در این راهنما قابل پیاده‌سازی و استفاده است.

- سطح ماهی کوچک

کیف پول بلووالت^۲ از قابلیت انکار موجه پشتیبانی می‌کند.

- سطح دلفین و کوسه

با استفاده از کلمات ۱۳ هم مختلف و در نتیجه ساختن کیف پول‌های متعدد می‌توان قابلیت انکار موجه را پیاده‌سازی کرد.

- سطح نهنگ

در این سطح با توجه به استفاده از کیف پول‌های سخت‌افزاری، می‌توان از روش‌های زیر امنیت فیزیکی کلیدهای خصوصی را تأمین کرد

○ کیف پول‌های سخت‌افزاری اغلب قابلیتی دارند که اگر کاربر به جای رمز ورود اصلی، یک رمز ورود که خودش از قبل تعیین کرده را وارد کند، آن کیف پول سخت‌افزاری کیف پول دومی که قبلاً کاربر مقدار ناچیزی بیت کوین در آن ذخیره کرده را نشان می‌دهند و کیف پول اصلی را پنهان می‌کنند.

○ کیف پول‌های سخت‌افزاری اغلب قابلیتی دارند که اگر کاربر به جای رمز ورود اصلی، یک رمز ورود که خودش از قبل تعیین کرده را وارد کند، آن کیف پول مورد نظر به اصطلاح می‌سوزد و به هیچ روشی نمی‌توان به کلیدهای خصوصی آن دسترسی پیدا کرد.

○ کیف پول‌های سخت‌افزاری اغلب روی بُرد الکترونیکی خود نقطه‌ای دارند که اگر آن نقطه تحت ضربه شدید قرار گیرد یا با یک جسم تیز سوراخ شود، دیگر به هیچ روشی نمی‌توان به کلیدهای خصوصی ذخیره شده در آن دسترسی پیدا کرد.

1 Plausible deniability

2 BlueWallet

○ می‌توان با جاگذاری کیف پول‌های سخت‌افزاری مختلف در مکان‌های مختلف، امنیت کلیدهای خصوصی ذخیره شده در آن‌ها را تا حد بسیار زیادی بالا برد. برای مثال فرض کنید شما از یک سیستم چند امضائی ۳ از ۵ برای تأمین امنیت کلیدهای خصوصی خود استفاده می‌کنید؛ در این صورت می‌توانید ۴ تا از کیف پول‌های سخت‌افزاری مورد استفاده در این سیستم را در مکان‌های مختلف نگهداری کنید. این مکان‌ها می‌توانند در گاوصندوق بانک یا شعبه‌های مختلف شرکت شما در شهر یا حتی کشورهای مختلف باشد.

تأمین امنیت فیزیکی سخت‌افزار کیف پول

این موضوع رابطه مستقیم با مقوله حفظ حریم خصوصی مالی شما دارد. سناریوی زیر را در نظر بگیرید، فرض کنید برای محافظت از کلیدهای خصوصی بیت‌کوین‌تان همه توصیه‌های ایمنی را به کار بسته‌اید و از ابزارهای سطح نهنگ استفاده کرده‌اید. اگر کسی به سخت‌افزاری که فول نود و کیف پول شما بر روی آن اجرا می‌شود (اینجا لپ‌تاپ و نرم‌افزار اسپکتر^۱) دسترسی فیزیکی پیدا کند، اگر اطلاعات کیف پول شما رمزنگاری نشده باشد (مثل کیف پول فول نود بیت‌کوین کور^۲) این فرد از لیست کوین‌ها^۳ و موجودی بیت‌کوین شما اطلاع پیدا خواهد کرد و حریم خصوصی مالی شما مستقیماً زیر سؤال خواهد رفت.

دقت کنید؛ استفاده از VPS برای راه‌اندازی یک فول نود بیت‌کوین با توجه به دسترسی مسئولان و کارمندان شرکت فراهم کننده خدمات ابری^۴ و دسترسی به سخت‌افزار فول نود شما، همین مخاطرات را با خود در پی دارد.

1 Specter desktop
2 Bitcoin core
3 UTXO
4 Cloud VPS hosting

روش ساخت کلمات بازیابی با استفاده از کاغذ و تاس

ساختن «کلید خصوصی»^۱ اولین و مهم‌ترین قدم برای نگهداری بدون واسطه و امن از بیت کوین است. شما با نصب و استفاده از یک کیف پول روی گوشی موبایل خود، در واقع به کُد و سیستم عامل تلفن همراه خود «اعتماد» کرده‌اید تا برای شما یک کلید خصوصی بیت کوین بسازند. برای همین است که این روش برای مبالغ پایین (سطح ماهی کوچک) پیشنهاد می‌شود.

برای ساختن یک کلید خصوصی بسیار امن می‌توانید از روش کاغذ و تاس استفاده کنید که در فایل راهنمای زیر به تفصیل در مورد آن شرح داده شده است. فراموش نکنید؛ سهل‌انگاری در تولید کلید خصوصی بیت کوین برابر با از دست دادن سرمایه شما است.



روش تولید **Seed** استاندارد **BIP39**
با استفاده از کاغذ و تاس

https://bitcoind.me/blobs/tuts/gen_bip39_bitcoin_seed_farsi.pdf

1 Private key

راه‌اندازی فول نود و سرویس‌های مورد نیاز روی بُرد رزبری پای

نرم‌افزارها و سرویس‌های لازم برای نصب و راه‌اندازی فول نود و کیف پول بیت کوین بر روی کامپیوترهای دسکتاپ قابل نصب هستند ولی ممکن است همگان قادر به انجام این روش نباشند. به همین منظور پروژه‌هایی به‌وجود آمده‌اند که می‌توان با به‌کارگیری از آنها این سرویس‌ها را روی بردهای توسعه‌پذیر مثل رزبری پای^۱ (نسخه ۴) راه‌اندازی کرد. یکی از معروف‌ترین این پروژه‌ها پروژه «آمبرل»^۲ است.

در زمان نگارش این مطلب تهیه اقلام مورد نیاز برای راه‌اندازی فول نود با استفاده از این روش حدود ۵-۶ میلیون تومان هزینه دارد.



آموزش راه‌اندازی نود بیت کوین با استفاده از نرم‌افزار آمبرل

1 Raspberry Pi
2 Umbrel

گزینه‌های موجود کیف پول سخت‌افزاری

در بازار جهانی کیف پول‌های متنوعی برای نگهداری امن از بیت‌کوین تولید شده است. با این وجود دسترسی به این کیف پول‌ها با توجه به کم‌ارزش شدن ریال برای کسانی که در ایران زندگی می‌کنند محدود است. از کیف پول‌های موجود در بازار می‌توان به COLD CARD و TREZOR اشاره کرد. یک گزینه بسیار جالب نیز پروژه SeedSigner است که در ادامه این راهنما روش ساخت این دستگاه را مورد بررسی قرار خواهیم داد.

معمولاً در یک کیف پول چند امضائی از برندهای مختلف کیف پول‌های سخت‌افزاری استفاده می‌شود تا اگر احیاناً یک باگ نرم یا سخت‌افزاری در یکی از آنها وجود داشت، دیگری مصون باشد. این روش باعث امنیت بیشتر روش نگهداری خواهد شد.

خریداری فول نود^۱ بیت‌کوین به صورت آماده^۲

ممکن است راه‌اندازی و نگهداری از نرم‌افزارها و سرویس‌های مورد نیاز برای راه‌اندازی یک فول نود بیت‌کوین برای همگان امکان‌پذیر نباشد. بنابراین شرکت‌های مختلفی سخت‌افزار و نرم‌افزارهای مورد نیاز برای راه‌اندازی و به کار گرفتن یک فول نود بیت‌کوین را در قالب یک محصول برای استفاده مشتریان ارائه می‌کنند. تا امروز نمونه‌های این محصولات در کشورمان مشاهده نشده است.

از فول نودهای آماده موجود در بازار جهانی می‌توان به Casa Node و Nodl و Umbrel اشاره کرد.

1 Full node
2 Node in a box

معرفی پروژه SeedSigner و کاربرد آن در تولید امضای تراکنش‌ها

همانطور که پیشتر گفتیم برای ارسال بیت کوین و امضای تراکنش‌ها - به‌ویژه در حالت ایزوله^۱ - به وسیله‌ای برای تولید امضاء نیاز داریم. SeedSigner در واقع یک پروژه اپن-سورس برای ساختن چنین دستگاهی است. فرق بسیار مهمی که این پروژه با دیگر پروژه‌های معروف به «کیف پول سخت‌افزاری^۲» دارد این است که هر کس در هر کجای دنیا می‌تواند قطعات لازم برای ساختن این دستگاه را شخصاً از بازار تهیه، و به ساختن آن اقدام کند.

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

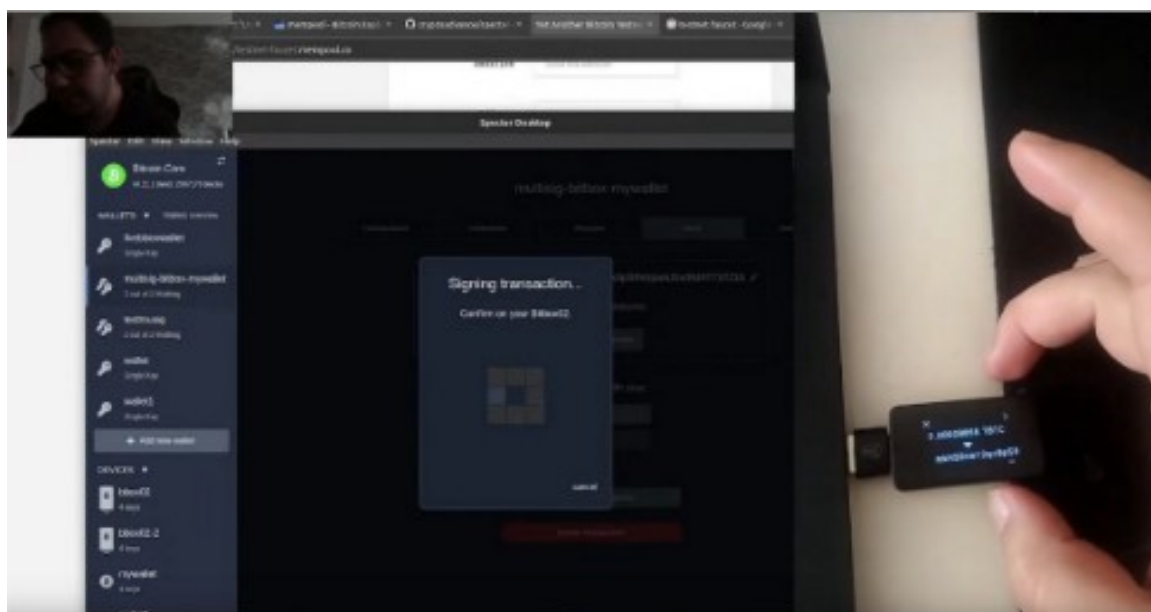


راهنمای آموزشی ساخت SeedSigner

- 1 Air Gapped
- 2 Hardware Wallet

اتصال کیف پول Specter به فول نود شخصی و استفاده از آن در حالت تک امضایی با استفاده از کیف پول سخت افزاری BitBox02 روی شبکه تست بیت کوین

در این ویدیو همه موارد لازم برای راه اندازی Specter و اتصال یک کیف پول سخت افزاری به آن آموزش داده می شود. مشاهده این ویدیو را به همه علاقه مندان به مبحث نگهداری امن از بیت کوین پیشنهاد می کنیم.



https://www.youtube.com/watch?v=4zQIIkB9_yQ

تعیین تکلیف کلید خصوصی بیت کوین پیش از مرگ؛ ارث یا وصیت

یکی از مهم‌ترین مسائلی که در زمان نگهداری بیت کوین باید به آن توجه کرد مسئله ارث و میراث بیت کوین و کلیدهای خصوصی است.

اگر بیت کوین‌های فرد متوفی در اختیار صرافی باشد، تا جایی که نویسندگان این مطلب اطلاع دارند راه یا قانونی برای انتقال دارایی او به خانواده وی وجود ندارد (مگر اینکه آنها به اطلاعات ورود به حساب صرافی این فرد دسترسی داشته باشند).

ضیا صدر در یکی از لایوهای خود این موضوع را با یک وکیل آشنا به بیت کوین مطرح کرده است که می‌توانید در آدرس زیر مشاهده کنید.



https://archive.org/details/bitcoin_inheritance_farsi

حریم خصوصی در بیت کوین

اگر تا اینجا به خواندن ادامه داده‌اید احتمالاً به نگهداری امن از بیت کوین‌هایتان اهمیت می‌دهید. یکی دیگر از حوزه‌های کمتر شناخته شده بیت کوین که نیاز به محافظت دارد، مقوله «حریم خصوصی مالی»^۱ است. در این بخش تلاش می‌کنیم این مفهوم را به زبانی ساده توضیح دهیم.

حریم خصوصی یکی از موضوعات بسیار جالب در حوزه بیت کوین است. هم ساده است، هم پیچیده؛ به عبارت دیگر «سهل و ممتنع» است. بحث حریم خصوصی از این نظر سهل است که درک آن آسان است، می‌دانیم چرا به آن نیاز داریم ولی اجرای آن دشوار است. با طرح یک مثال سعی می‌کنیم این موضوع را توضیح دهیم.

فرض کنید شما به همراه دوست‌تان در حال رانندگی به سمت بانک خود هستید تا برای یک کار اداری پرینت گردش حساب بگیرید. در حین رانندگی به یک خودرو مشکوک می‌شوید و احتمال می‌دهید شما را تعقیب می‌کند. سعی می‌کنید خونسردی خود را حفظ کنید و به راه خود ادامه می‌دهید و به بانک می‌رسید.

درخواست را به کارمند بانک می‌دهید و منتظر آماده شدن پرینت می‌شوید و بعد از گذشت چند دقیقه متوجه می‌شوید فردی در بلندگوی بانک که مملو از مشتریان است در حال خواندن ریزتراکنش‌های شما و اطلاعات هویتی شما است. در این موقعیت چه حالی می‌شوید.

در هر دو مورد حس می‌کنید حریم خصوصی شما پایمال شده است

در بیت کوین هم شرایط مشابهی پیش می‌آید. از طرفی وقتی شما با یک کیف پول بیت کوین به شبکه متصل می‌شوید، از افرادی که به مودم wifi منزل شما وصل شده‌اند تا تأمین کننده اینترنت^۱ شما (یعنی شرکت‌هایی که از آنها اینترنت گرفته‌اید) تا سرورهایی که کیف پول شما به آن وصل شده است تا موجودی بیت کوین را به شما نشان بدهد، همه از اطلاعاتی که کیف پول شما در شبکه منتشر می‌کند اطلاع دارند؛ مثل خودروی مشکوکی که شما را تعقیب می‌کرد. حریم خصوصی در این سطح به «حریم خصوصی در سطح شبکه^۲» معروف است.

از جانب دیگر با توجه به اینکه اطلاعات «همه» دریافت‌ها و ارسال‌ها در بلاک‌چین بیت کوین به صورت عمومی و کاملاً شفاف وجود دارند، و با توجه به اینکه اطلاعات هویتی شما در صرافی که از آن بیت کوین خریداری می‌کنید نگهداری می‌شود، شرایطی شبیه به موقعیت بانک پیش می‌آید و حریم خصوصی شما با ابزارهایی که تکنولوژی ساخت پیچیده‌ای ندارند، به راحتی در معرض خطر قرار می‌گیرد. حریم خصوصی در این سطح به «حریم خصوصی در سطح کوین^۳» معروف است.

ممکن است شما بگویید «خب مشکلی نیست، من چیزی برای پنهان کردن ندارم و کار خلافی انجام نمی‌دهم و ترسی از آشکار بودن تراکنش‌هایم ندارم» و در این مورد کاملاً حق با شماست. ولی همچنان یک مشکل باقی است: «اینکه علاوه بر بانک که مورد اعتماد شماست، دوست شما و افراد غریبه هم از تراکنش‌های مالی شما اطلاع پیدا کرده‌اند.»

این در واقع مشکلی است که حل آن به آسانی درک آن نیست. این موضوع از روز اول پدید آمدن بیت کوین دغدغه فعالان حریم خصوصی در بیت کوین بوده و تا امروز راه حل آسانی برای آن پیدا نشده است.

1 ISP
2 Network level privacy
3 UTXO level privacy

نکته بسیار مهم این است که رسیدن به حریم خصوصی مالی در شبکه بیت کوین و استفاده از ابزارهای آن نیاز به تحقیق و مطالعه پیوسته برای شناخت ابزارها و روش‌های تامین حریم خصوصی در سطح شبکه و کوین دارد.

برای شروع، مقاله زیر را که مقدمه‌ای بر مفهوم حریم خصوصی در سطح کوین و معرفی ابزارهای این حوزه است بخوانید.



مقدمه‌ای بر حریم خصوصی بیت کوین
و سؤال و جواب درباره ویرل پول سامورایی

<https://bitcoind.me/blobs/tuts/bitcoin-privacy-and-whirlpool-qna-farsi.pdf>

گردآوری این راهنما توسط ر.فرد انجام گرفته و در طول زمان با ابزارها و آموزش‌های جدید به‌روز خواهد شد.

این راهنما تحت مجوز «مالکیت عمومی» منتشر می‌شود و بازنشر آن به هر شکل آزاد است.

ویراست چهارم

پاییز ۱۴۰۰

bitcoind.me

منابع فارسی بیت‌کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی‌زبان بیت‌کوین تالیف یا ترجمه شده‌اند