



فول نود بیت کوین چیست و چرا هر کاربر
بیت کوین باید یک فول نود شخصی اجرا کند

یک شبکه کامپیوتری^۱ به زبان ساده چیست و شبکه بیت کوین بر اساس چه مدلی طراحی شده و چگونه کار می کند؟

به مجموعه‌ای از کامپیوترهایی که از طریق یکی از پروتکل‌های ارتباطی^۲ به یکدیگر متصل هستند، یک شبکه کامپیوتری گفته می‌شود. به هریک از کامپیوترهای تشکیل دهنده این شبکه «گره» یا «نود^۳» گفته می‌شود و این نودها قادرند داده‌های خود را در شبکه با یکدیگر به اشتراک بگذارند.

یکی از پرکاربردترین معماری‌های شبکه‌های کامپیوتری، مدل «سرویس گیرنده-سرویس دهنده^۴» است. در این مدل یک سرویس دهنده مرکزی (سرور) قادر است اطلاعات مورد نیاز را برای سرویس گیرندگان (کاربران) فراهم کند. برای نمونه، سایت یک فروشگاه آنلاین را در نظر بگیرید؛ کاربران با استفاده از یک مرورگر به سرور مرکزی این شرکت وصل می‌شوند و لیست اقلام این فروشگاه آنلاین را مشاهده می‌کنند.

توانایی و ظرفیت این شبکه در پاسخگویی به سرویس گیرندگان متعدد بسیار بالاست ولی به دو دلیل نمی‌توان از این مدل برای ایجاد یک «پول» مقاوم در برابر سانسور^۵ استفاده کرد:

۱. تمرکز: این معماری متمرکز است و می‌توان کل شبکه را با خاموش کردن، یا از دسترس خارج کردن سرویس دهنده (سرور) مرکزی از کار انداخت.
۲. اعتماد: کاربران راهی برای اعتبارسنجی داده‌های دریافت شده از سرویس دهنده مرکزی ندارند و باید به آن اعتماد کنند.

1 Computer Network
2 Communication Protocols
3 Node
4 Client-Server
5 Censorship resistant

شبکه بیت کوین برای حل دو مشکلی که پیشتر مطرح شد بر اساس معماری متفاوتی طراحی شده است. در این معماری برخلاف مدل سرویس دهنده-سرویس گیرنده؛ که در آن سرویس دهنده (سرور) در مرکز قرار می گیرد و همه سرویس گیرندگان اطلاعات مورد نیازشان را از این سرویس دهنده مرکزی دریافت می کنند، هیچ تفاوتی میان نودهای تشکیل دهنده شبکه وجود ندارد. هر نود همه اطلاعات مورد نیاز خود را از یک یا چند نود موجود در شبکه دریافت می کند و نودهای دیگر نیز می توانند اطلاعات مورد نیازشان را از این نود مورد نظر دریافت کنند؛ این نود هم سرویس دهنده است، هم سرویس گیرنده. نام این مدل، معماری همتا-به-همتا^۱ است. در این معماری نودهای شبکه هیچ تفاوتی با یکدیگر ندارند.

از کار انداختن شبکه های همتا-به-همتا بسیار دشوار، و تقریباً محال است. یک نمونه بسیار معروف از به کار گیری این معماری در دنیای واقعی، شبکه «بیت تورنت»^۲ است. این شبکه علیرغم مشکلات حقوقی که شرکت های بزرگ فیلم سازی و تهیه کنندگان موسیقی برای آن بوجود آوردند، و تلاش های جدی ای که از جانب مخالفان این شبکه برای متوقف کردن آن انجام گرفت، همچنان به کار خود ادامه می دهد و به نظر نمی رسد راهی قطعی برای از کار انداختن آن وجود داشته باشد.

تمرکز در معماری همتا-به-همتا با حذف سرویس دهنده مرکزی از بین می رود. از این رو این نوع شبکه، به «شبکه غیرمتمرکز»^۳ نیز معروف است.

1 Peer-to-peer (p2p)
2 BitTorrent Protocol
3 Decentralized Network

فول نود بیت کوین چیست و چگونه کار می کند؟

یک «فول نود»^۱ بیت کوین به زبان ساده، یکی از کامپیوترهای شبکه همتا-به-همتای بیت کوین است که نرم افزار بیت کوین بر روی آن اجرا شده باشد. این فول نود تفاوت چندانی با یک پایگاه داده (دیتابیس)^۲ که دارایی افراد را به آن‌ها اختصاص می دهد، ندارد. هر تراکنش^۳ بیت کوین وضعیت فعلی این پایگاه داده را با حذف مالکان قدیمی و اضافه کردن مالکان جدید، به روزرسانی می کند.

نرم افزار بیت کوین شما برای اطلاع از آخرین تغییرات، در بستر شبکه غیر متمرکز بیت کوین با بقیه نودهای شبکه ارتباط برقرار می کند و تراکنش‌ها و بلاک‌های جدید را از آن‌ها درخواست می کند.

این نود به محض دریافت یک بلاک جدید، آن را با مجموعه‌ای از قوانین خاصی که به «قوانین اجماع»^۴ معروف هستند، تطابق می دهد و اعتبار آن را می سنجد. اگر فرآیند تأیید اعتبار با موفقیت انجام شود، این نود پایگاه داده خود را با تغییر مالکیت‌های ناشی از تراکنش‌های موجود در بلاک جدید، به روزرسانی می کند.

این «قوانین اجماع» می تواند طیف وسیعی از قوانین را پوشش دهد؛ از محدوده سائز بلاک، تا بررسی این که در تک تک این تراکنش‌ها، فقط مالک فعلی ثبت شده در پایگاه داده قادر به خرج کردن بیت کوین‌ها است (به استثنای بیت کوین‌هایی که در هر بلاک به عنوان پاداش به ماینرها پرداخت می شود).

1 Full node
2 Database
3 Transaction
4 Consensus Rules

نام پایگاه داده‌ای که وضعیت فعلی مالکیت‌ها را در خود ذخیره می‌کند، «مجموعهٔ UTXO»^۱ است. هر نود در شبکه باید از یک نسخهٔ کامل از این مجموعه نگهداری کند تا قادر به تأیید بلاک‌ها و تراکنش‌های جدید باشد، زیرا بدون در اختیار داشتن آن از صاحبان فعلی کوین‌ها اطلاع ندارد.

پس از استفاده از بلاک‌ها برای به‌روزرسانی مجموعهٔ UTXO، نیازی به ذخیرهٔ آن‌ها نیست (در موارد نادر ممکن است لازم باشند، ولی ما اینجا برای ساده کردن موضوع آن‌ها را نادیده می‌گیریم). این موضوع نودهای آرشیوی^۲ را که بلاک‌ها را ذخیره می‌کنند از نودهای «کم‌حجم شده»^۳ که این بلاک‌ها را بعد از فرآیند اعتبارسنجی نادیده می‌گیرند و آن‌ها را ذخیره نمی‌کنند، از یکدیگر متمایز می‌کند.

اجرای فول نود چه تأثیری روی افزایش قابلیت اطمینان^۴ شبکهٔ بیت کوین در معماری همتا-به-همتا دارد؟

همانطور که پیشتر گفتیم در یک شبکهٔ همتا-به-همتا سرویس‌دهندهٔ متمرکزی وجود ندارد، بنابراین هر نود جدید پس از پیوستن به شبکه برای اولین بار، باید زنجیرهٔ بیت کوین را از اولین بلاک که در تاریخ سوم ژانویه سال ۲۰۰۹ توسط ساتوشی ناکاموتو ساخته شده، تا آخرین بلاک - که توسط ماینرهای شبکه تولید شده است، - برای تهیهٔ دیتابیس UTXO خود از نودهای موجود در شبکه دریافت کند. به این کار اصطلاحاً «دانلود بلاک‌ها برای بار اول»^۵ گفته می‌شود.

1 Unspent Transaction Output (UTXO)
2 Archival Node
3 Pruned Node
4 Reliability
5 Initial Block Download (IBD)

یکی از کاربردهای فول نودهای اجرا شده توسط کاربران، نگهداری از آرشیو بلاک‌های شبکه بیت کوین و ارسال آن‌ها به نودهایی است که به شبکه می‌پیوندند. پیکربندی و اجرای یک فول نود در این حالت به افزایش قابلیت اطمینان شبکه بیت کوین کمک بزرگی می‌کند.

براساس آمارهای سایت‌هایی که به ارائه آمار در مورد شبکه بیت کوین می‌پردازند، در حال حاضر حدود ۱۱,۳۰۰ نود با این پیکربندی در شبکه همتا-به-همتای بیت کوین وجود دارد.¹

اجرای یک فول نود چه کمکی به حفاظت از قوانین پروتکل بیت کوین می‌کند؟

یکی از مهم‌ترین دلایل اجرای یک فول نود بیت کوین، به کار بستن آن برای تأیید تراکنش‌های شخصی افراد یا به‌طور دقیق‌تر اعتبارسنجی بیت کوین‌های دریافت شده است. فول نود شما کار اعتبارسنجی همه تراکنش‌ها و سابقه همه آن‌ها را فقط به این دلیل انجام می‌دهد که این کار پیش‌نیاز تأیید کردن تراکنش‌های شما است.

اما چرا تأیید تراکنش‌های شخصی شما تا این اندازه اهمیت دارد؟ چون بدون آن، نمی‌توانید از «اصالت» بیت کوینی که دریافت کرده‌اید، اطمینان حاصل کنید. تأیید اصالت بیت کوین‌های دریافت شده یعنی تطبیق قوانین اجماع اعمال شده توسط نرم‌افزاری که از نظر شما نماینده «بیت کوین» است.

فرض کنید از یک کیف پول بیت کوین روی گوشی تلفن همراه خود استفاده می‌کنید، و این برنامه اطلاعات مربوط به تراکنش‌های شما را از سرورهای شرکت مربوطه دریافت

¹ <https://bitnodes.io>

می‌کند. سؤال این است، از کجا مطمئن هستید تراکنش‌هایی که این شرکت در قالب نرم‌افزار کیف پول به شما ارائه کرده مطابق با قوانین پروتکل بیت کوین، و از نظر دیگران نیز معتبر هستند؟ از کجا مطمئن هستید که دیگران کوین‌هایی که برایشان ارسال می‌کنید را به‌عنوان بیت کوین از شما می‌پذیرند؟

تنها راه برای اطمینان از اصل بودن بیت کوین‌هایی که دریافت می‌کنید، اعتبارسنجی آن‌ها و تطبیق آن‌ها با قوانین پروتکل بیت کوین است، بر این اساس محافظت از قوانین پروتکل بیت کوین یعنی امتناع از پذیرش کوین‌هایی که با قوانین پروتکل شبکه بیت کوین مطابقت ندارند و مردود نمودن آن‌ها.

چرا نمی‌توانم برای تأیید اصالت بیت کوین‌های دریافت شده‌ام به بلاک اکسپلوررهای^۱ معروف اعتماد کنم؟

بلاک اکسپلوررها سرویس‌هایی مبتنی بر وب هستند و کاربران را قادر می‌سازند با استفاده از یک مرورگر وب^۲ اطلاعات بلاک‌ها، تراکنش‌ها، و موجودی آدرس‌ها را مشاهده کنند. یکی از معروف‌ترین آن‌ها سایت mempool.space است.

یک راه این است که با مقایسه اطلاعات تراکنش در منابع مختلف از اصالت بیت کوین دریافت شده اطمینان حاصل کرد، برای نمونه می‌توان اطلاعات تراکنش را در چند سرویس کاوشگر تراکنش‌ها و بلاک‌های شبکه بیت کوین (معروف به بلاک اکسپلورر) بررسی و تأیید کرد. این روش به دو سناریوی محتمل منتهی می‌شود:

1 Block Explorer

2 Web Browser

یا کاربران این سرویس‌ها به قدری کم هستند که نمی‌توان روی اطمینان حاصل شده از آن‌ها حسابی باز کرد، یا آنقدر محبوب هستند که اکثریت قابل توجهی از کاربران دیگر نیز برای تأیید تراکنش‌های خود به آن‌ها اعتماد می‌کنند.

اما در حالی که این روش مشکل شخص شما در کسب اطمینان از پذیرفته شدن تراکنش‌ها توسط دیگران را حل می‌کند، خطر بسیار بزرگتری برای همه کاربران بیت کوین به وجود خواهد آورد:

در این صورت، اگر کاربران شبکه بیت کوین برای اعتبارسنجی تراکنش‌هایشان فقط از چند سرویس محبوب به عنوان «مرجع» استفاده کنند، این سرویس‌ها قادرند بدون اطلاع اکثریت کاربران، قوانین اجماع شبکه بیت کوین را تغییر دهند.

به عنوان مثال، آن‌ها می‌توانند تصمیم بگیرند که از این پس، هر بلاک باید شامل تراکنشی باشد که ۱۰ بیت کوین به عنوان کارمزد از هیچ خلق^۱، و به آدرسی که تحت کنترل آن‌ها است ارسال می‌کند.

ماینرها نیز ناچارند از این قوانین اطاعت کنند، و گرنه این «نودهای بزرگ» بلاک‌های آن‌ها را نخواهند پذیرفت و در این صورت سرمایه آن‌ها صرف تولید بلاک‌هایی می‌شود که اکثر کاربران قبول ندارند و در نتیجه پاداشی برای ساخت آن‌ها دریافت نخواهند کرد. (اصلاً ممکن است این نودهای بزرگ نقش ماینرها را به کلی حذف کنند) و اقلیت کوچکی که فول نودهای خود را اجرا می‌کنند باید بین پذیرش قوانین جدیدی که از جانب نودهای بزرگ دیکته می‌شود، و قوانین قدیمی که بلاک‌های حاوی قوانین جدید را نمی‌پذیرند یکی را انتخاب کنند. شایان ذکر است که انتخاب دوم یعنی پذیرش قوانین شبکه‌ای که اکثریت مردم از آن استفاده نمی‌کنند.

1 Out of thin air

با ادامه یافتن این شرایط کار به جایی می‌رسد که قوانین شبکه توسط تعداد انگشت‌شماری از کسب‌وکارهایی دیکته می‌شود که قدرت تقریباً نامحدودی روی قوانین اجماع شبکه بیت کوین دارند، زیرا اکثریت بازیگران اقتصادی شبکه آنها را به صورت کورکورانه دنبال می‌کنند.

اجرای فول نود چه تاثیری روی حفاظت از حریم خصوصی کاربران دارد؟

در صورتی که نرم‌افزار کیف پول شما اطلاعات زنجیره بیت کوین را برای دریافت، ارسال، و نمایش موجودی شما از سرورهای عمومی دریافت می‌کند، حریم خصوصی مالی شما در خطر است. این نرم‌افزارها راهی جز ارسال اطلاعات خصوصی کیف پول شما برای این سرورهای عمومی ندارند و هرکس از جمله تأمین‌کننده اینترنت^۱ شما، یا کسی که به شبکه داخلی شما دسترسی دارد، می‌تواند به اطلاعات مالی شما دست پیدا کند.

این موضوع در مورد مشاهده موجودی در یک بلاک اکسپلورر عمومی نیز صادق است. حریم خصوصی مالی شما زمانی که شناسه تراکنش^۲، یا آدرس بیت کوین خود در این سایت‌ها وارد می‌کنید در خطر است، زیرا سایت مورد نظر اطلاعات کاملی از دارایی بیت کوین و همچنین آدرس IP شما دارد.

روش‌های متنوعی برای حفظ حریم خصوصی کاربران بدون اجرای فول نود و از طریق به کارگیری از شبکه تور^۳ وجود دارد ولی این روش‌ها به اندازه اجرای فول نود شخصی مؤثر نیستند.

1 Internet Provider
2 Transaction Id (txid)
3 Tor Network

اگر فردی کیف پول خود را به فول نود شخصی اش متصل نکند و صرفاً قصد اجرای یک فول نود داشته باشد، این فول نود تا چه اندازه به حفاظت از قوانین شبکه بیت کوین کمک می کند؟

کمترین کمکی که یک فول نود متصل به شبکه بیت کوین می تواند به حفاظت از قوانین شبکه بیت کوین کند این است که بلاک ها و تراکنش هایی که منطبق با قوانین پروتکل بیت کوین هستند را در شبکه «بازپخش»^۱ و به فول نودهای دیگر برساند. در شرایط عادی و با توجه به هزینه ترافیک اینترنتی مصرفی این فول نود، ممکن است اجرای این نود - صرفاً برای کمک به قابلیت اطمینان شبکه - امری اقتصادی نباشد.

ولی در نظر داشته باشید در شرایط خاصی که شبکه بیت کوین به منظور تغییر قوانین پروتکل در انتظار اجرای یک سافت فورک است^۲، یا احتمال حمله به قوانین پروتکل بیت کوین وجود دارد (مناقشه ساینز بلاک^۳)، اجرای یک فول نود تحت هر شرایطی اعلام حمایت از قوانین پروتکل بیت کوین منتخب کاربران است و به حفاظت از آن کمک خواهد کرد.

فول نود بیت کوین بر روی چه دستگاه هایی قابل اجرا است؟

نرم افزار فول نود بیت کوین بسیار بهینه پیاده سازی شده و برای اجرای آن به دستگاه خاصی نیاز نیست. هر کامپیوتر دسکتاپ خانگی، یا لپ تاپی که پردازنده آن حدوداً در طول ۱۰ سال گذشته ساخته شده باشد قادر به اجرای نرم افزار بیت کوین خواهد بود.

1 Relay

2 https://www.reddit.com/r/Bitcoin/comments/nz5r4y/psa_with_taproot_locked_in_it_is_a_good_idea_to

3 https://twitter.com/bitcoind_me/status/1365248075783155714?s=20

این نرم افزار همچنین قابلیت اجرا شدن روی «کامپیوترهای تک بُردی^۱» مانند «رزبری پای^۲» را نیز دارد. نرم افزارهای مختلفی برای آماده سازی یک رزبری پای و به کار گرفتن آن به عنوان یک فول نود وجود دارد. برای مشاهده ویدیوی نحوه راه اندازی آن به پیوست مراجعه کنید.

در حال حاضر فول نود بیت کوین شما در حالت «کم حجم شده^۳» به حدود ۵ گیگابایت، و در حالت آرشیوی به حدود ۵۵۰ گیگابایت فضای هارد دیسک نیاز خواهد داشت. امکان اجرای فول نود بر روی HDD وجود دارد ولی برای کسب بهترین تجربه کاربری پیشنهاد می شود از هارد SSD برای این کار استفاده شود.

اجرای یک فول نود بیت کوین به چه مقدار پهنای باند و ترافیک اینترنت نیاز دارد؟

برای پاسخ به این سؤال باید سناریوهای مختلفی را در نظر بگیریم:

فرض کنید فردی برای حفظ حریم خصوصی مالی خود یک فول نود بیت کوین اجرا می کند و کیف پول بیت کوین خود را نیز به این فول نود متصل کرده است. این فول نود فقط باید در مواقعی روشن و متصل به اینترنت باشد که صاحب کیف پول قصد ارسال بیت کوین داشته باشد. در این صورت در حال حاضر این فول نود روزانه حدود کمتر از ۲۰۰ مگابایت ترافیک اینترنت مصرف خواهد کرد.

مقدار مصرف ترافیک اینترنت یک فول نود بستگی به نحوه پیکربندی آن دارد. اگر فردی به عنوان مسئول فول نود قصد کمک به قابلیت اطمینان شبکه بیت کوین را داشته

1 Single-board computer
2 Raspberry Pi
3 Pruned node

باشد می‌تواند آن را به صورت یک فول نود آرشیوی پیکربندی، و آرشیو بلاک‌های بیت کوین را برای نودهایی که به شبکه می‌پیوندند فراهم کند. در این صورت یک فول نود بیت کوین ممکن است در حال حاضر روزانه با توجه به پهنای باندی که در اختیار دارد تا چند ده گیگابایت ترافیک اینترنت مصرف کند.

مقدار ترافیک ارسالی به دیگر نودهای شبکه هم‌تا-به-هم‌تای بیت کوین تحت کنترل مسئول فول نود است و در صورت نیاز می‌توان آن را برای مدیریت ترافیک مصرفی نود محدود کرد. یک فول نود همواره روشن و متصل به اینترنت، در صورتی که حجم ترافیک ارسال شده به شبکه در آن محدود شده باشد، در حال حاضر روزانه به حدود کمتر از ۱ گیگابایت ترافیک اینترنت نیاز خواهد داشت.

ترافیک اولیه مورد نیاز برای آماده‌سازی دیتابیس UTXO در یک فول نود «کم‌حجم شده»^۱ در صورتی که مایل به دانلود این دیتابیس به صورت از پیش تهیه شده باشید، در حال حاضر حدود ۵ گیگابایت است.^۲ (در این صورت شما به فرد یا مجموعه‌ای که دیتابیس UTXO را تهیه کرده است اعتماد می‌کنید. این روش در شرایطی پیشنهاد می‌شود که نرم‌افزار بیت کوین را شخصاً دانلود، و از درستی نرم‌افزار از طریق اعتبارسنجی امضای دیجیتال آن اطمینان دارید. برای مشاهده آموزش تصویری به پیوست مراجعه کنید.)

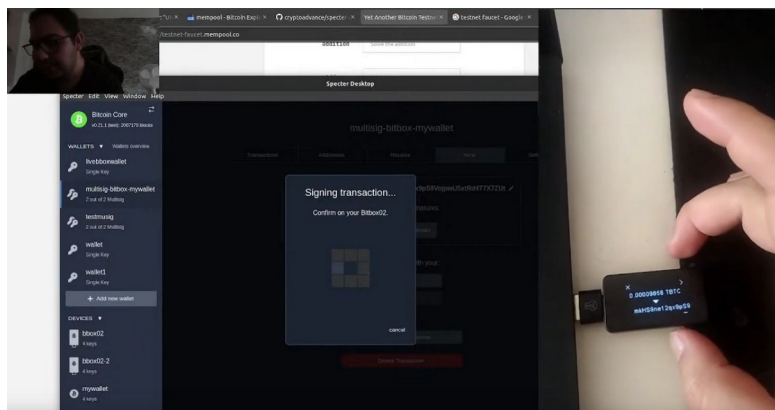
در غیر این صورت اگر قصد دارید فول نود شما دیتابیس UTXO را به طور مستقل و مستقیماً از بلاک‌های زنجیره بیت کوین آماده‌سازی کند نیاز به دانلود همه بلاک‌های زنجیره بیت کوین خواهید داشت که در حال حاضر به حدود ۴۰۰ گیگابایت ترافیک اینترنت نیاز دارد. زمان مورد نیاز برای دانلود بلاک‌های زنجیره بیت کوین برای اولین بار^۳، رابطه مستقیمی با پهنای باند فراهم شده برای فول نود شما دارد ولی پس از به اتمام رسیدن

1 Pruned node

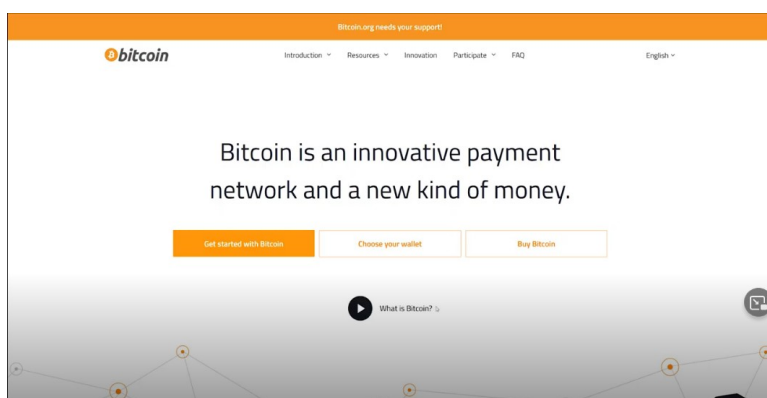
2 <https://prunednode.today>

3 IBD

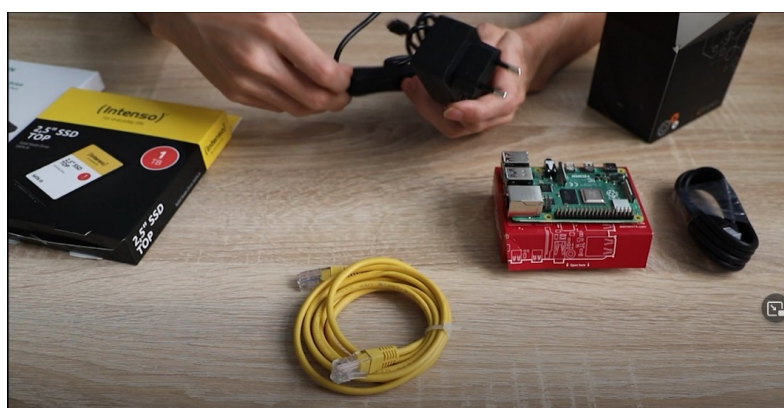
آن، فول نود شما به پهنای باند زیادی نیاز ندارد و یک اینترنت ADSL معمولی خانگی برای اجرای آن کفایت می‌کند.



راهاندازی فول نود بیت کوین و اتصال کیف پول Specter و یک کیف پول سخت‌افزاری به آن در حالت تک امضایی (روی شبکه تست بیت کوین)



راهاندازی فول نود بیت کوین در حالت Pruned با استفاده از نرم‌افزار Bitcoin Core



راهاندازی فول نود بیت کوین با استفاده از نرم‌افزار Umbrel

نسخه اول این راهنما، ترجمه یک رشته توئیت از کاربر توئیتر [@benkaufman](#) و گردآوری و ترجمه آن توسط ر.فرد انجام پذیرفته است. مطالب تکمیلی این راهنما در نسخه دوم توسط ر.فرد گردآوری و تألیف، و قالب کار به صورت سؤال و جواب بازنگارش شد.

تشکر می کنیم از [@Ali2kCom](#) که در تهیه محتوای نسخه دوم به ما یاری رساند، و همچنین [@mytechmix](#) برای بازبینی فنی این کار.

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

منابع فارسی بیت کوین
نسخه دوم - ویراست اول
پائیز ۱۴۰۰