پرسش‌های رایج

یافتن پاسخ برای پرسشهای رایج و افسانه‌هایی پیرامون بیت‌کوین.

فهرست مطالب

در مورد بیت کوین و حمایت از مصرف کننده چه؟

اقتصاد

بیت‌کوینها چگونه ساخته می شوند؟

چرا بیت‌کوینها باارزش هستند؟

چه چیزی بهای بیت‌کوین را تعیین می‌کند؟

آیا بیت‌کوین می‌تواند ارزش خود را از دست دهد؟

آیا بیت‌کوین حبابی است؟

آیا بیت کوین، ترفند پونزی است؟

آیا بیت کوین به پیشگامان خود بهره ناعادلانه ای نمی دهد؟

آیا متناهی بودن تعداد بیت کوینها، یک محدودیت نخواهد بود؟

آیا بیت کوین در مارپیچ تورم زدایی سقوط نخواهد کرد؟

آیا سفته بازی و نوسانات، مشکلی برای بیت کوین ایجاد نمی کنند؟

چه اتفاقی میافتد اگر کسی همه بیت کوینهای موجود را یکجا بخرد؟

اگر کسی ارز دیجیتال بهتری ساخت چه؟

تراکنش‌ها

چرا باید ۱۰ دقیقه صبر کنم؟

کارمزد یک تراکنش چقدر خواهد بود؟

اگر زمانی که کامپیوترم خاموش است بیت کوینی به من برسد، چه اتفاقی خواهد افتاد؟

همزمان سازی به چه معناست و چرا اینقدر طول می کشد؟

استخراج

استخراج بیت‌کوین یعنی چه؟

استخراج بیت‌کوین به چه صورت است؟

آیا استخراج بیت‌کوین، اتلاف انرژی نیست؟

چگونه استخراج به امنیت بیت کوین کمک می کند؟

برای شروع به کار استخراج به چه چیزهایی نیاز دارم؟

امنیت

آیا بیت‌کوین امن است؟

آیا بیت‌کوین تا کنون هک نشده است؟

آیا کاربران می‌توانند علیه بیت‌کوین توطئه کنند؟

آیا بیت کوین نسبت به محاسبات کوانتمی آسیب پذیر است؟

کمک

می‌خواهم بیشتر بدانم. از کجا می‌توانم اطلاعات بیشتری بگیرم؟

عمومی

بیت‌کوین چیست؟

بیت کوین یک شبکه توافقی است که یک سیستم پرداخت جدید و یک نوع پول‌کاملاً یجیتال را بوجود آورده است. این اولین شبکه پرداخت نقطه به نقطه تمرکز زدایی شده است که توسط کاربرانش بدون هیچگونه اختیار مرکزی و یا واسطه ای، نیرومند شده است. از نقطه نظر یک کاربر، بیت کوین بسیار شبیه پول نقد اینترنتی است. بیت کوین همچنین می تواند به عنوان مهمترین سیستم دفترداری با سه ورودی موجود بشمار آید.

سازنده بیت‌کوین کیست؟

بیت کوین اولین پیاده سازی یک مفهوم به نام "ارز سری" است که اولین بار در سال ۱۹۹۸ توسطِ ی دای در فهرست ایمیل سایفرپانک ها، توصیف شده بود و بیان میکرد که این مفهوم، نوع جدیدی از پول است که برای کنترل تولید و تراکنشهای روی آن، بجای یک مرجع مرکزی، از رمزنگاری استفاده شده است. مشخصات اولین بیت کوین و اثبات مفهوم در سال ۲۰۰۹ توسط ساتوشی ناکاموتو در یک فهرست ایمیل رمزنگاری شده منتشر گردید. ساتوشی بدون آنکه چیز زیادی از خودش فاش سازد، پروژه را به اواخر سال ۲۰۱۰ موکول کرد. از آن موقع این جامعه بطور نمایی با توسعه دهندگان بسیاری که روی بیت کوین کار می کنند، رشد کرده است

گمنامی ساتوشی اغلب باعث نگرانی های ناموجهی می شود که بسیاری از آنها به فهم نادرست از طبیعت متن باز بیت کوین بر می گردد. پروتکل بیت کوین و نرم افزار بصورت باز منتشر شده است و هر توسعه دهنده ای در هر کجای گیتی می تواند کد آنرا بازبینی کرده و یا نسخه تغییر یافته نرم افزار بیت کوین مخصوص خودش را بسازد. تاثیر ساتوشی نیز مانند توسعه دهندگان کنونی، محدود به تغییراتی بود که از دیگران اقتباس می کرد و بنابراین بیت کوین را کنترل نمی کرد. امروزه هویت مخترع بیت کوین به خودی خوداحتمالاً مانند هویت شخصی است که کاغذ را اختراع کرده بود.

چه کسی شبکه‌ی بیت‌کوین را کنترل می‌کند؟

هیچکس مالک شبکه بیت کوین نیست، درست همانطور که هیچکس صاحب تکنوژیی که در ورای ایمیل است، نیست. این کاربران بیت کوین در سراسر جهان هستند که آنرا کنترل می کنند. توسعه دهندگان بیت کوین اگرچه نرم افزار آن را بهبود می بخشند ولی نمی توانند تغییری را بر پروتکل بیت کوین تحمیل کنند،، چرا که هر کاربری آزاد است که نرم افزار خود و نسخه ای که خود می پسندد را استفاده کند. تمامی کاربران، برای اینکه با یکدیگر سازگار بمانند باید از نرم افزاری استفاده کنند که از همان قواعد پیروی می کند. بیت کوین تنها بشرط اجماع کامل بین تمامی کاربران، می تواند بدرستی کار کند. بنابراین تمامی کاربران و توسعه دهندگان انگیزه قوی برای حفظ این اجماع را خواهند داشت.

بیت‌کوین چگونه کار می‌کند؟

از دید کاربر، بیت کوین چیزی بیش از یک آپ روی گوشی تلفن همراه و یا یک برنامه کامپیوتری که یک کیف پول بیت کوینی شخصی برایش تهیه کرده و به کاربر اجازه می دهد تا با آن به ارسال یا دریافت بیت کوینها بپردازد، نیست. برای بیشتر کاربران، روش کار بیت کوین در همین حد است.

در پشت این پرده، شبکه بیت کوین یک دفتر کل عمومی به نام "زنجیره بلاک" را به اشتراک گذاشته است. این دفتر کل شامل تمامی تراکنشهایی است که تا کنون پردازش شده است و به کامپیوتر کاربر اجازه می دهد تا درستی هر تراکنش را بیازماید. اعتبار هر تراکنش به وسیله امضای دیجیتالی مربوط به آدرس های ارسال، محافظت میشود و به همه کاربران اجازه میدهد تا بر ارسال بیت کوینها از آدرسهای بیت کوینی خود، کنترل کامل داشته باشند. افزون بر این، هر کسی می تواند تراکنشها را با استفاده از توان محاسباتی سخت افزاری که ویژه این کار است، پردازش کرده و برای این سرویس، بیت کوینهایی را هم به عنوان جایزه بدست آورد. به اینکاراصطلاحاً "استخراج" می گویند. برای دانستن مطالب بیشتری در مورد بیت کوین به صفحه اختصاصی و برگه اصلی مراجعه کنید.

آیا مردمواقعاً از بیت‌کوین استفاده می‌کنند؟

بله. تعداد روزافزونی از کسب و کارها و افراد از بیت کوین استفاده می کنند. این کسب و کارها ممکن است کسب وکارهایی بصورت رو در رو با مشتری باشد، مانند رستورانها ، آپارتمانها، دفاتر حقوقی و یا سرویسهای آنلاین مانندNamecheap ، WordPress، Redditو یا .Flattr بیت کوین اگرچه پدیده ایِنسبتاً جدید بشمار می آید، اما به سرعت رو به رشد است. در پایان آگست ۲۰۱۳، ارزش تمامی بیت کوینهای در گردش بالغ بر ۱,۵ میلیارد دلار امریکا بود و ارزش بیت کوینهایی که روزانه مبادله می شد، به میلیونها دلار می رسید.

Screenshot

چگونه کسی می تواند بیت‌کوین بدست آورد؟

در صورت پرداخت وجه برای کالا یا خدمات

خرید آن از صرافی بیت کوین

مبادله بیت کوینها با کسی در نزدیکی خود

بدست آوردن بیت کوین از راهاستخراج رقابتی

اگرچه ممکن است افرادی باشند که بخواهند بیت کوینها را در برابر کارت اعتباری یا پرداخت پی پال بفروشند، ولی بیشتر صرافی ها اجازه پرداخت با این روشها را نمی دهند. به این دلیل که در مواردی، کسی بیت کوینهایی را با پی پال خریده و سپس از جانب خود آن تراکنش را برگشت داده است.معمولاً به این گونه موارد، پرداخت برگشتی می گویند.

پرداخت بیت کوین، چقدر دشوار است؟

پرداخت به وسیله بیت کوین، آسانتر از خرید توسط کردیت کارت یا دبیت کارت است و می تواند بدون استفاده از یک حساب تجاری دریافت شود. پرداخت ها از طریق یک برنامه کاربردی کیف پول، چه روی کامپیوتر و چه روی گوشی تلفن هوشمند شما با وارد کردن آدرس گیرنده، مقدار وجه پرداختی و فشردن دکمه ارسال، انجام می شود. بسیاری از کیف پول ها می توانند با اسکن کردن یک کد QR و یا با استفاده از تکنولوژی NFC و تماس دادن دو گوشی تلفن با هم، آدرس گیرنده را آسانتر وارد نمایند.

Screenshot Screenshot

مزایای بیتکوین چیست؟

آزادی پرداخت وجه- هر موقع از شبانه روز و در هر کجای جهان که باشید، ارسال و دریافت فوری هر مبلغ از بیت کوین امکانپذیر است. هیچ روزی تعطیل نیست. هیچ حد و مرزی در کار نیست. هیچ محدودیتی اعمال نخواهد شد. بیت کوین به کاربرانش اجازه می دهد بر پول خود کنترل کامل داشته باشند.

کارمزد های بسیار اندک - در حال حاضر پردازش پرداخت وجه با بیت کوین، بصورت بدون کارمزد و یا با کارمزدی بسیار اندک، انجام می گیرد. کاربران می توانند برای پردازش سریعتر تراکنش خود، کارمزد پرداخت نمایند که در نتیجه تاییدیه تراکنش را سریعتر از شبکه دریافت خواهند کرد. علاوه بر این، پردازشگرهای تجاری هم هستند که سوداگران را در پردازش تراکنش ها، تبدیل بیت کوینها به یک ارز بدون پشتوانه و واریز مبالغ بطور مستقیم و روزانه به حساب بانکی آنها، یاری دهند. چون این تراکنشها بر مبنای بیت کوین است، کارمزدهایی به مراتب کمتر از کارمزدهای شبکه کارت اعتباری یا پی پال، از آنها خواسته خواهد شد.

ریسک کمتر برای سوداگران- تراکنشهای بیت کوین امن و برگشت ناپذیر بوده و حاوی اطلاعات شخصی و یا حساس مشتریان نیست. به همین دلیل از سوداگران در برابر ضررهای ناشی از کلاهبرداری یا پرداختهای برگشتی جعلی محافظت می کند و نیازی هم به پیروی از PCI نیست. سوداگران می توانند بسادگی به بازارهای جدیدی قدم بگذارند که هیچ کارت اعتباری در آن در دسترس نباشد و یا نرخ کلاهبرداری به شکل غیرقابل قبولی بالا باشد. دستاوردهای خالص آن عبارتست از: کارمزد کمتر، بازارهای بزرگتر و هزینه های مدیریت کمتر.

امنیت و کنترل - کاربران بیت کوین بر تراکنشهای خود کنترل کامل دارند. غیرممکن است که بتوان معامله کنندگان را مجبور کرد؛ مانند آنچه در روشهای دیگر پرداخت گاهی پیش می آید، مبالغی ناخواسته و یا از پیش اعلام نشده را بپردازند. پرداختهای بیت کوینی بدون اینکه اطلاعات شخصی کسی به تراکنش پیوست شده باشد، انجام می گیرد. به این ترتیب محافظت شدیدی در برابر سرقت هویت ایجاد شده است. کاربران بیت کوینی همچنین می توانند با تهیه بک آپ یا نسخه پشتیبان و رمزگذاری، از پولشان محافظت نمایند.

شفافیت و بی طرف بودن - تمامی اطلاعات در مورد تامین پول بیت کوین بسادگی روی زنجیره بلاک در دسترس همه هست و می توان آنرا بلافاصله درستی آزمایی کرده و از آنها استفاده نمود. هیچ شخص یا سازمانی نمی تواند پروتکل بیت کوین را کنترل و یا دستکاری نماید چون این پروتکل با رمزنگاری، ایمن شده و هسته بیت کوین را از نظر شفافیت، بیطرفی کامل و قابل پیش بینی بودن قابل اعتماد کامل ساخته است.

معایب بیت‌کوین چیست؟

میزان پذیرش - بسیاری از مردم هنوز در مورد بیت کوین آگاهی ندارند. همه روزه، کسب و کارهای بیشتری بیت کوینها را می پذیرند چرا که مزایای آنرا می خواهند، اما این فهرست هنوز کوچک است و نیاز به رشد دارد تا بتوان از فایده های این شبکه بهره جست.

ناپایداری - ارزش کلی بیت کوینهای در گردش و تعداد کسب و کارهایی که از بیت کوین استفاده می کنند، در مقایسه با آنچه که باید باشد، هنوز کم است. بنابراین، رویدادها، معاملات و یا فعالیتهای تجاری‌نسبتاً کمی هستند که می توانند بر بهای بیت کوین اثری چشمگیر داشته باشند.. به لحاظ نظری این ناپایداری، در صورت رشد بازارها و تکنولوژی بیت کوین، کاهش خواهد یافت. پیش از این، جهان هرگز چنین ارز نوپدیدی را به خود ندیده بود، بنابراین تصور اینکه بیت کوین چگونه این راه را به پایان خواهد برد، واقعاً دشوار (و هیجان برانگیز) است.

در حال توسعه بودن - نرم افزار بیت کوین هنوز نسخه بتاست و ویژگی های ناقص بسیاری دارد که بطور فعال در دست توسعه است. ابزارها، ویژگی ها و سرویس های جدید در حال توسعه یافتن هستند تا بیت کوین را امن تر و برای توده مردم دسترس پذیرتر بسازند. بیشتر کسب و کارهای بیت کوینی نوپا بوده و هنوز تحت پوشش بیمه نیستند. بطور کلی، فرایند بلوغ بیت کوین هنوز در جریان است.

چرا مردم به بیت‌کوین اعتماد دارند؟

سهم بزرگی از اعتماد به بیت کوین ناشی از این حقیقت است که‌اصولاً نیازی به اعتماد کردن نیست. بیت کوین‌کاملاً متن باز و تمرکززدایی شده است. یعنی هر کسی می تواند هر زمان که بخواهد به سراسر کد منبع آن، دسترسی داشته باشد. بنابراین هر توسعه دهنده ای در جهان می تواند بدقت درستی طرز کار بیت کوین را بیازماید. هر کسی می تواند شفافیت تمامی تراکنشها و بیت کوین های ساخته شده رافوراً مورد ملاحظه قرار دهد. تمامی پرداختها را می توان بدون اتکا به طرف سومی، انجام داد و کل سیستم از طریق الگوریتمهای رمزنگاری که به دقت نظیر به نظیر مرور شده، درست مثل آنچه در بانکداری آنلاین انجام می شود، محافظت می گردد. هیچ سازمان یا فردی نمی تواند بیت کوین را کنترل کند و حتی اگر تمامی کاربران نتوانند به این شبکه اعتماد کنند، امنیت شبکه پابرجاست.

آیا با بیت‌کوین می‌توانم پولدار شوم؟

هرگز انتظار نداشته باشید با بیت کوین یا هر تکنولوژی نوپدید دیگری، پولدار شوید. این نکته همیشه حائز اهمیت است که باید در مورد هر چیزی که خوبتر از آنچه که بتواند واقعی باشد، به نظر می آید و یا از قوانین اولیه قتصاد پیروی نمی کند، محتاط باشید.

بیت کوین فضای رو به رشدی از نوآوری هاست و فرصت های کسب و کار زیادی دارد که البته شامل خطراتی هم هست. هیچ تضمینی وجود ندارد که چون بیت کوین تا کنون با سرعت زیادی توسعه یافته است، از این پس نیز همچنان به رشد خود ادامه دهد. سرمایه گذاشتن از زمان و منابع روی هر چیزی که به بیت کوین وابسته است، نیاز به کارآفرینی دارد. راههای گوناگونی برای بدست آوردن پول بوسیله بیت کوین هست مانند استخراج، سفته بازی و یا راه انداختن کسب و کارهای جدید. تمامی این روشها رقابتی هستند و هیچ تضمینی وجود ندارد که سودآور هم باشند. . این به خود فرد بستگی دارد که هزینه ها و مخاطراتی را که در این نوع پروژه ها هست، بدرستی ارزیابی کرده باشد.

آیا بیت کوینکاملاً مجازی و غیرمادی است؟

بیت کوین به همان اندازه کارتهای اعتباری و شبکه های بانکداری آنلاین که مردم همه روزه از آنها استفاده می کنند، مجازی است. بیت کوین درست مانند سایر اشکال پول، برای پرداخت آنلاین در فروشگاه های واقعی بکار می رود و نیز می تواند درست مانند سکه های کازاسیوس به شکل فیزیکی پول تبدیل شود، اما پردخت با گوشی های تلفن همراهمعمولاً آسانتر است. ترازهای بیت کوینی در یک شبکه بزرگ توزیع شده ، ذخیره شده است و هیچکس نمی تواند با تقلب آنرا تغییر دهد. به عبارت دیگر، کاربران بیت کوین کنترل اختصاصی بر موجودی خود دارند و بیت کوینهایشانصرفاً به دلیل مجازی بودن، غیب نمی شود.

آیا بیتکوین گمنام است؟

بیت کوین طوری طراحی شده است که به کاربران خود اجازه دهد در سطح حریم خصوصی قابل قبولی، پرداختها را ارسال و یا دریافت نمایند. اما بیت کوین گمنام نیست و نمی توان آنها را با همان سطح حریم خصوصی که پول نقد دارد، عرضه کرد. استفاده از بیت کوین، رکوردهای عمومی گسترده ای از خود به جای می گذارد. مکانیسم های مختلفی برای محافظت از حریم خصوصی کاربران وجود دارد و مکانیسم های بیشتری هم در حال توسعه هستند. به هر حال، قبل از اینکه این ویژگیها بدرستی توسط بیشتر کاربران بیت کوین بکار گرفته شوند، کارهای زیادی هست که باید انجام شود.

نگرانی هایی در باب اینکه محرمانه بودن تراکنشهای بیت کوین به منظور انجام کارهای غیرقانونی است، ایجاد شده است. اما این نگرانی ها هیچ ارزشی ندارد؛ چون بیت کوین بدون تردید تابع قوانین و مقرراتی است که مشابه آن در سیستم های مالی وجود دارد. بیت کوین نمی تواند گمنام تر از پول نقد باشد و احتمال جلوگیری از بررسی های جنایی، در مورد آن کم است. افزون بر آن، بیت کوین نیز طوری طراحی شده که از دامنه گسترده ای از جرایم مالی جلوگیری می کند.

اگر بیتکوینها را از دست بدهم، چه اتفاقی خواهد افتاد؟

اگر کاربری کیف پول خود را گم کند، پول او از گردش خارج می شود. بیت کوینهای گمشده، درست مانند بقیه بیت کوینها همچنان در زنجیره بلاک باقی می مانند، اما برای همیشه به خواب می روند؛ چون هیچکس هیچ راهی ندارد تا کلید(های) محرمانه ای را؛ که بیت کوینها را دوباره قابل خرج کردن می نماید، پیدا کند. نظر به قانون عرضه و تقاضا، وقتی بیت کوینهای کمتری در دسترس باشند، تقاضا برای آنهایی که باقی مانده اند بیشتر می شود و برای جبران این تقاضا، بهای بیت کوینها افزایش می یابد.

آیا بیت کوین، به یک شبکه پرداخت عمده، ارتقاء خواهد یافت؟

شبکه بیت کوین می تواند تعداد بسیار بیشتری تراکنش در ثانیه را نسبت به چیزی که امروزه انجام می دهد، پردازش کند. اما هنوز آماده نیست تا به جایگاه شبکه هایی مانند شبکه های کارتهای اعتباری بزرگ برسد. برای از میان برداشتن محدودیتهای کنونی، کارهایی در دست اقدام است و الزامات آینده بخوبی شناسایی شده اند. از زمان پیدایش شبکه بیت کوین، همه ابعاد آن در فرایند مداومی از بلوغ، بهینه سازی و تخصصی شدن بوده است و انتظار می رود که در سالهای آینده نیز این راه ادامه یابد. با افزایش ترافیک، ممکن است تعداد بیشتری از کاربران بیت کوینی از کلاینتهای سبکتر استفاده کنند و نُدهای شبکه کامل، به سرویسی تخصصی تر تبدیل شوند. برای دانستن جزئیات بیشتر به ارتقاء روی صفحه های ویکی مراجعه کنید.

حقوقی

آیا بیت‌کوین قانونی است؟

تا جایی که ما می دانیم، در بیشتر محاکم قضایی، از نظر قانون بیت کوین غیرقانونی نیست. اما بعضی از دستگاههای قضایی (مانند کشورهای آرژانتین و روسیه) ارزهای خارجی را بشدت محدود و یا ممنوع کرده اند. بعضی دیگر از دستگاههای قضایی (مانند تایلند) ممکن است صدور گواهینامه برای بعضی موجودیتهای خاص،مثلاً صرافی های بیت کوینی را محدود کرده باشند.

قانونگزاران در دستگاههای قضایی مختلف در حال برداشتن گامهایی هستند تا برای افراد و کسب و کارها، قوانینی برای پیوند این تکنولوژی جدید با یک سیستم مالی رسمی و تنظیم شده، وضع نمایند.مثلاً شبکه اجرای جرایم مالی(FinCEN) ؛ که دفتری در وزارت خزانه داری ایالات متحده امریکاست، راهنمای غیرالزام آوری منتشر کرده و در آن به تشریح چگونگی فعالیت های معین در خصوص ارزهای مجازی پرداخته است.

آیا بیت‌کوین برای انجام فعالیت‌های غیرقانونی قابل استفاده است؟

بیت کوین نوعی پول است و پول همواره برای اهداف قانونی و غیرقانونی بکار می رفته است. پول نقد، کارتهای اعتباری و سیستمهای بانکی جاری از نظر استفاده در جرایم مالی، بطور گسترده ای از بیت کوین پیشی می گیرند . بیت کوین توانسته است نوآوری های چشمگیری در سیستم های پرداخت بیاورد و منافع چنین نوآوری هایی اغلب بسیار فراتر از نقطه ضعف های احتمالی آنهاست.

بیت کوین طوری طراحی شده تا در ایمن کردن بیشتر پولسازی یک گام فراتر باشد و نیز حفاظت چشمگیری در برابر بسیاری از اشکال جرایم مالی به عمل آورد.مثلاً جعل کردن بیت کوینها،کاملاً غیرممکن است. کاربران بر پرداختهای خود کنترل کامل دارند و نمی توانند مبالغ تایید نشده را مانند آنچه که در کارتهای اعتباری کلاهبرداری می شود، دریافت کنند. تراکنشهای بیت کوینی برگشت ناپذیر بوده و در برابر پرداختهای برگشتی تقلبی بسیار ایمن هستند. بیت کوین با استفاده از مکانیسمهای مفید و قوی مانند بک آپ یا پشتیبان گیری، رمزنگاری و امضای چندگانه، در برابر دزدی و گم شدن بسیار ایمن شده است.

نگرانی هایی وجود دارد مبنی بر اینکه بیت کوین می تواند برای مجرمین بسیار جذاب باشد چرا که می توان حریم شخصی و پرداختهای برگشت پذیر با آن داشت. اما این ویژگیها در پول نقد و حواله بانکی که بسیار زیاد از آنها استفاده می شود و بخوبی جا افتاده اند، هم وجود دارد. بدون تردید، استفاده از بیت کوین تابع قوانین مشابهی است که‌قبلاً در جای خود در سیستم های مالی موجود گنجانده شده اند و احتمال ندارد که بیت کوین از انجام بررسی های جنایی، جلوگیری کند. بطور کلی، مرسوم است که پیشرفتهای مهم

قبل از اینکه مزایای آنها بخوبی شناخته شود، بحث برانگیز باشند. اینترنت مثال خوبی برای بسیاری از کسانی است که تصوری این چنینی دارند.

آیا بیت کوین می تواند تابع قوانین و مقررات باشد؟

پروتکل بیت کوین به خودی خود، بدون همکاری‌تقریباً تمامی کاربرانش که نرم افزار مورد استفاده شان را خود بر می گزینند، قابل تغییر نیست. تلاش برای اختصاص امتیازهای ویژه به یک مرجع محلی در قوانین شبکه جهانی بیت کوین ، احتمالی شدنی نیست. هر سازمان ثروتمندی می توانست انتخاب کند که برای سخت افزار استخراج طوری سرمایه گذاری کند تا نیمی از قدرت محاسباتی شبکه را در کنترل خود درآورد و بتواند آخرین تراکنشها را بلاک کرده یا برگشت دهد. اما هیچ تضمینی نیست که آنها بتوانند این قدرت را حفظ کنند چرا که میزان سرمایه گذاریش باید بیشتر از تمام استخراج کننده های دیگر در جهان، باشد.

اما وضع مقررات استفاده از بیت کوین، به روشی مشابه سایر ابزارها امکان پذیر است. درست مانند دلار، بیت کوین می تواند برای مقاصد بسیار متفاوتی بکار رود که بعضی از آنها قانونی و برخی دیگر بر اساس بعضی از محاکم قانونگذاری، غیر قانونی خواهند بود. از این لحاظ بیت کوین هیچ فرقی با دیگر ابرازها یا منابع ندارد و در هر کشوری، می تواند تابع قوانین و مقررات آن کشور باشد. بر اساس بعضی قوانین محدود کننده، استفاده از بیت کوین همچنین میتواند دشوار باشد. در اینصورت تعیین درصد کاربرانی که از این تکنولوژی استفاده می کنند، سخت خواهد بود. دولتی که بیت کوین را ممنوع می کند، از کسب و کارهای داخلی و بازارهای رو به رشد جلوگیری کرده و نوآوری را به سوی دیگر کشورها می راند. چالش پیش روی قانونگذاران مثل همیشه توسعه راه حل هایی است که در عین کارا بودن، رشد بازارها و کسب و کارهای نوپدید را دچار مشکل نکند.

درباره بیت‌کوین و مالیاتهای آن چه؟

بیت کوین ارز بدون پشتوانه ای نیست که در هر دستگاه قضایی، پولی قانونی بشمار بیاید، اما مشمولیت مالیاتی اغلب فارغ از واسطه ی بکار رفته، شامل حال بیت کوین هم می شود. قوانین بسیار گوناگونی در بسیاری از دستگاههای قضایی وضع شده است که می تواند درآمد، فروش، دستمزد، بهره های سرمایه ای و یا اشکال دیگر مشمولیت های مالیاتی را برای بیت کوین ایجاد کند.

در مورد بیت کوین و حمایت از مصرف کننده چه؟

بیت کوین دست مردم را باز می گذارد تا با شرایط خودشان، تراکنش انجام دهند. هر کاربری می تواند مانند پول نقد، پرداختها را ارسال و یا دریافت کند اما همچنین می توانند در قراردادهای پیچیده تری هم مشارکت کنند. چند امضایی، اجازه می دهد که یک تراکنش توسط شبکه پذیرفته شود تنها اگر تعداد معینی از اعضاء یک گروه تعریف شده، موافق امضا کردن آن تراکنش باشند. این باعث نوآوری در توسعه سرویس های میانجی حل اختلاف در آینده خواهند شد. چنین سرویسهایی می توانند در صورت عدم توافق بین طرفین، در نقش طرف سومی برای تایید یا رد تراکنش وارد عمل شوند، بدون اینکه بر پول آنها کنترل داشته باشند. برخلاف پول نقد و یا دیگر روشهای پرداخت، بیت کوین همیشه یک سند عمومی از انجام تراکنش از خود بر جای میگذارد که بطور بالقوه می تواند به عنوان مدرکی بر علیه کسب و کارهایی که کلاهبرداری می کنند، بکار گرفته شود.

شایان ذکر است که سوداگران که همواره به وجهه عمومی خود برای بقای کسب و کارشان وابسته اند و به کارمندانشان حقوق می پردازند، در هنگام معامله با مصرف کنندگان جدید خود، سطح دسترسی یکسانی به اطلاعات ندارند. بیت کوین هم فرد و هم کسب و

کارها را در برابر پرداخت های برگشتی تقلبی محافظت می کند و در عین حال به مصرف کننده این انتخاب را می دهد که چنانچه نخواهد به یک سوداگر خاص اعتماد کند، خواستار حفاظت بیشتر باشد.

اقتصاد

بیت‌کوینها چگونه ساخته می شوند؟

بیت کوینها در فرایندی رقابتی و تمرکز زدایی شده که "استخراج" نام دارد، تولید می شوند. این فرایند مستلزم آن است که افراد از شبکه برای خدمات خود، جایزه دریافت کنند. استخراج کنندگان بیت کوین تراکنش ها را پردازش کرده و با استفاده از سخت افزار تخصصی، شبکه را ایمن کرده و در عوض آن بیت کوینهای جدید جمع آوری می نمایند.

طراحی پروتکل بیت کوین به گونه ایست که بیت کوینهای جدید را با نرخ ثابتی تولید می کند. به این ترتیب استخراج بیت کوین یک کسب و کار رقابتی خواهد شد. اگر استخراج کنندگان بیشتری به شبکه بپیوندند، سودآوری‌مرتباً دشوار خواهد شد و استخراج کنندگان باید بدنبال بازده برای کاهش هزینه های استخراج باشند. هیچ مرجع مرکزی یا توسعه دهنده ای، اختیار آنرا ندارد تا سیستم را برای افزایش سود، کنترل یا دستکاری کند.هرنُد بیت کوین در جهان، هر آنچه را که در تطابق با قوانینی که انتظار میرود سیستم از آن پیروی کند، نباشد حذف خواهد کرد.

بیت کوینها با نرخی کاهنده و قابل پیش بینی، تولید می شوند. تعداد بیت کوینهای جدیدی که هر سال تولید می شود، بطور اتوماتیک در طول زمان نصف می شود تا اینکه مجموع بیت کوینهای موجود به ۲۱ میلیون برسد. از این هنگام به بعد، دیگر بیت کوینی صادر نخواهد شد. در این نقطه،احتمالاً بطور اختصاصی به استخراج کنندگان بیت کوین مقدار کمی کارمزد تراکنش پرداخت خواهد شد.

چرا بیت‌کوینها باارزش هستند؟

بیت کوینها ارزشمندند چون به عنوان شکلی از پول، مفید هستند. بیت کوین ویژگیهای پولی دارد (پایداری، قابلیت حمل و نقل، تعویض پذیری، کمیابی، بخش پذیری و شناخت پذیری). ویژگیهای بیت کوین بر مبنای خواص ریاضی استوار شده است، نه بر مبنای خاصیتهای فیزیکی (مانند طلا و نقره) و نه بر اساس اعتماد بر مرجعی مرکزی (مانند ارزهای بدون پشتوانه). مختصر آنکه، این ریاضیات است که بیت کوین را پشتیبانی می کند. با این ویژگی ها، تمام آنچه که برای شکلی از پول بودن و ارزش داشتن لازم است، اعتماد و پذیرش است. در مورد بیت کوین، رشد کاربران، سوداگران و کسب و کارهای نوپا، گویای مطلب است. مانند تمامی ارزها، بیت کوین ارزش خود را تنها و بطور مستقیم از کسانی می گیرد که آنرا برای پرداخت وجه پذیرفته اند.

چه چیزی بهای بیت‌کوین را تعیین می‌کند؟

بهای بیت کوین با قانون عرضه و تقاضا معلوم می شود. با افزایش تقاضا برای بیت کوین، بهای آن نیز افزایش می یابد و با کاهش تقاضا، از بهای آن کاسته می شود. تعداد بیت کوینهای در گردش محدود است و بیت کوین های جدید با نرخی کاهنده و قابل پیش بینی تولید می شوند که به این معنی است که تقاضا باید تابعی از این سطح تورم باشد تا بتواند قیمت را ثابت نگهدارد. چون بازار بیت

کوین در مقایسه با آنچه باید باشد، هنوز کوچک است، بنابراین، برای بالا و پایین رفتن قیمت بازار نیاز به مقدار چشمگیری پول نیست و در نتیجه قیمت بیت کوین هنوز بسیار متغیر است.

بهای بیت‌کوین، ۲۰۱۳ تا ۲۰۱۵

chart

آیا بیت‌کوین می‌تواند ارزش خود را از دست دهد؟

بله.تاریخ پر است از ارزهایی که ورشکست شدند و دیگر استفاده ای از آنها نمی شودمثلاً مارک آلمان در دوران جمهوری ویمار و اخیراً نیز دلار زیمبابوه. اگر چه که شکست ارزهای قبلیمعمولاً به دلیل تورم زیاد بود که غیرممکن است برای بیت کوین اتفاق بیفتد، ولی همواره احتمال شکستهای فنی، ارزهای رقیب، مسایل سیاسی و جز آن وجود دارد. یک قاعده سرانگشتی ساده می گوید که هیچ ارزی را نبایدمطلقاً ایمن از ورشکستگی یا شرایط دشوار دانست. بیت کوین در طی سالها پس از آغاز به کارش، ثابت کرده که قابل اعتماد است و پتانسیل زیادی برای رشد دارد. اما هیچکس در آن موقعیت نیست که بتواند آینده بیت کوین را پیش بینی کند.

آیا بیت‌کوین حبابی است؟

این افزایش سریع قیمت نیست که حباب ایجاد می کند، بلکه ارزش بیش از حد گذاردن بصورت مصنوعی است که موجب تصحیح ناگهانی رو به پایین شده و به تشکیل حباب می انجامد. هر گاه صدها هزاران نفر از مشارکت کنندگان در بازار، انتخابهایی بر مبنای عملکرد فردی داشته باشند باعث می شود که قیمت بیت کوینها زمانی که قیمت بازار درحال تعیین شدن است، نوسان کند. دلیل تغییرات احساسی می تواند سلب اعتماد از بیت کوین، اختلاف زیاد بین ارزش و قیمت که بر مبنای اقتصاد بیت کوینی نباشد، پوشش مطبوعاتی فزاینده که موجب تحریک تقاضای سوداگرانه می شود، ترس از عدم قطعیت و شور وشوق غیرمنطقی خارج از عرف روز و حرص و طمع باشد.

آیا بیت کوین، ترفند پونزی است؟

ترفند پونزی یک عملیات سرمایه گذاری کلاهبردارانه است که به سرمایه گذاران بجای آنکه از محل سود حاصل از کسب و کار بهره پرداخت شود، از پول خود آنها یا از پولی که توسط سرمایه گذاران بعدی فراهم می شود، سود پرداخت می کند. ترفند پونزی بگونه ای طراحی شده است که چنانچه اگر مشارکت کنندگان جدید به تعداد کافی وجود نداشته باشد، با ضرو زیان آخرین سرمایه گذاران خود، فرو خواهد پاشید.

بیت کوین یک پروژه نرم افزاری رایگان بدون هیچگونه مرجعیت مرکزی است.در نتیجه، هیچکس در موقعیتی نخواهد بود که بتواند در مورد بازگشت سرمایه گذاری، نمایندگی های جعلی بسازد. درست مانند دیگر ارزهای اصلی دیگر مثل طلا، دلار امریکا، یورو، ین و غیره، هیچ قدرت خریدی تضمین شده ای وجود ندارد و نرخ مبادله آزادنه شناور است. این به حالت ناپایداری خواهد انجامید که در آن صاحبان بیت کوینها می توانند بطور غیرمنتظره ای پول بدست آورده و یا از دست بدهند. گذشته از گمانه زنی ها، بیت کوین همچنین یک سیستم پرداخت با ویژگیهای مفید و رقابتی است که هزاران کاربر و کسب و کار از آن استفاده می کنند.

آیا بیت کوین به پیشگامان خود بهره ناعادلانه ای نمی دهد؟

بعضی از پیشگامان تعداد زیادی بیت کوین داشتند چون خطر کرده و زمان و منابع را در یک تکنولوژی محقق نشده ای که دیگران بندرت از آن استفاده می کردند و برقراری مناسب امنیت آن به مراتب سخت تر بود، سرمایه گذاری کرده بودند. بسیاری از پیشگامان تعداد زیادی بیت کوین را اندک زمانی پیش از اینکه ارزشمند شود، خرج کرده یا فروخته بودند و فقط مقدار کمی از آن را قبل از اینکه بتوانند سود خوبی ببرند، خریده بودند. هیچ تضمینی نیست که بهای بیت کوین افزایش و یا کاهش یابدکاملاً شبیه به سرمایه گذاری در یک کسب و کار نوپاست که هم می تواند به واسطه مفید و مردم پسند بودن آن بر ارزشش افزود و یا اینکه هرگز پیشرفتی حاصل نکرد. بیت کوین هنوز در دوران نوزادی خود است و با دیدی بسیار بلندمدت طراحی شده است. به سختی می توان تصور کرد که چگونه می توانست نسبت به پیشگامان خود کمتر جانبداری کند و کاربران امروز آن شاید فردا، پیشگامان اولیه بیت کوین محسوب شوند و شاید هم نه.

آیا متناهی بودن تعداد بیت کوینها، یک محدودیت نخواهد بود؟

بیت کوین از این جهت که فقط تا ۲۱ میلیون عدد از آن ساخته خواهد شد، منحصر به فرد است. اما این هرگز یک محدودیت بشمار نمی آید، چون بیت کوینها می توانند با واحدهای کوچکتر از یک بیت کوین،مثلاً بیت، شمارش شوند. یک بیت کوین ۱،۰۰۰،۰۰۰ بیت است. اگر در آینده با کوچکتر شدن اندازه متوسط تراکنش، نیازی احساس شود، بیت کوینها می توانند تا ۸ رقم اعشار (۰،۰۰۰۰۰۰۰۱ بیت کوین) و بطور بالقوه حتی واحدهای کوچکتر، تقسیم گردند.

آیا بیت کوین در مارپیچ تورم زدایی سقوط نخواهد کرد؟

بر طبق نظریه مارپیچ تورم زدایی، اگر انتظار سقوط قیمتها برود، مردم خرید را به آینده موکول خواهند کرد تا از قیمتهای کمتر، بهره ببرند. این سقوط در تقاضا به نوبه خود سوداگران را وادار خواهد کرد تا با کاهش قیمت های خود در جهت تحریک تقاضا تلاش کنند که اینکار مشکل را بدتر کرده و به رکود اقتصادی خواهد انجامید.

هر چند این نظریه، در میان بانکداران مرکزی راهی مردم پسند برای توجیه تورم است ولی به نظر نمی رسد که همیشه درست باشد و در میان اقتصاددانان مورد مناقشه بوده است. لوازم الکترونیکی مصرفی، مثالی از یک بازار است که قیمتهای آنداِئماً در حال کاهش بوده ولی دچار رکود نمی شود. به همین شکل، ارزش بیت کوینها در طول زمان افزایش یافته و اندازه اقتصاد بیت کوینی هنوز هم پا به پای آن بشدت در حال رشد است. به دلیل آنکه، هم ارزش ارز و هم اندازه اقتصاد آن در سال ۲۰۰۹ ، از صفر شروع شده است؛ بیت کوین یک مثال نقض برای این نظریه است که نشان می دهد گاهی این نظریه باید نادرست باشد.

با وجود این، بیت کوین طراحی نشده است که یک ارز ضد تورمی باشد. دقیق تر آنست که بگوییم قرار بود بیت کوین در سالهای اول یک ارز تورمی باشد و سپس در سالهای بعد پایدار شود. تنها زمانی مقدار بیت کوینهای در گردش کاهش خواهد یافت که مردم کیف پول خود را از روی بی دقتی گم کرده و بک آپ یا پشتیبان هم تهیه نکرده باشند. اگر زیرساختهای پولی ثابت و اقتصاد پایدار باشد، ارزش ارز باید همیشه یکسان باقی بماند.

آیا سفته بازی و نوسانات، مشکلی برای بیت کوین ایجاد نمی کنند؟

این همان مسئله مرغ و تخم مرغ است. یک اقتصاد با مقیاس بزرگ برای تثبیت قیمت بیت کوین، باید کاربران و کسب و کارهای بیشتری را توسعه دهد. برای توسعه یافتن یک اقتصاد به اندازه ای بزرگتر، کاربران و کسب و کارها در پی ثبات قیمت ها خواهند بود.

خوشبختانه نوسانات بر مزایای اصلی بیت کوین به عنوان یک سیستم پرداخت وجه که پولی را از نقطه الف به نقطه ب می رساند، تاثیری ندارد. برای کسب و کارها امکان پذیر است که پرداختهای بیت کوینی رافوراً به ارز محلی خود تبدیل کنند و اینکار به آنها اجازه می دهد تا از مزایای بیت کوین بدون اینکه مشمول نوسانات قیمت شوند، استفاده کنند. بسیاری از کاربران بیت کوین را بخاطر امکانات و ویژگی های منحصر به فرد و مفید آن برگزیده اند. با چنین راهکارها و مشوقهایی، امکان رشد و بلوغ بیت کوین و توسعه آن، تا مرحله ای که نوسانات قیمت در آن محدود گردد، وجود دارد.

چه اتفاقی میافتد اگر کسی همه بیت کوینهای موجود را یکجا بخرد؟

تنها کسری از بیت کوینهایی که تا کنون صادر شده، در بازار مبادلات برای فروش گذاشته شده اند. بازارهای بیت کوینی، رقابتی هستند یعنی قیمت بیت کوین بر اساس عرضه و تقاضا، افزایش و یا کاهش خواهد یافت. افزون بر این، تا چندین دهه ی آینده، بیت کوینهای جدید همچنان صادر خواهند شد. بنابراین حتی بیشتر خریداران مصمم هم نخواهند توانست تمام بیت کوینهای موجود را یکجا بخرند. این البته به آن معنا نیست که بازارها در برابر دستکاری قیمت آسیب پذیر نیستند، بلکه بدان معناست که هنوز آن مقدار پول هنگفت در بازار موجود نیست تا بتواند قیمتها را بالا و پایین ببرد و بنابراین بیت کوین تا کنون یک دارایی نوسان دار باقی مانده است.

اگر کسی ارز دیجیتال بهتری ساخت چه؟

چنین اتفاقی ممکن است بیافتد. بیت کوین، تا کنون به میزان قابل ملاحظه ای، مردم پسندترین ارز مجازی تمرکززدایی شده است، اما نمی توان تضمین کرد که در آینده هم این موقعیت را حفظ کند. هم اکنون تعدادی ارزهای دیگر هم هستند که از بیت کوین الهام گرفته اند ولی‌احتمالاً درست است تصور کنیم که یک ارز جدید باید بسیار بهبود یابد تا بتواند به لحاظ داشتن بازارهای با ثبات، بر بیت کوین پیشی بگیرد حتی اگر این امر غیرقابل پیش بینی باقی بماند. تا زمانی که بخش های اساسی پروتکل تغییر نکند، بیت کوین میتواند اصلاحات و بهبودهای یک ارز رقابتی را داشته باشد.

تراکنش‌ها

چرا باید ۱۰ دقیقه صبر کنم؟

دریافت یک وجه پرداختی با بیت کوین،تقریباً آنی است. اما بطور متوسط یک تاخیر ۱۰ دقیقه ای لازم است تا شبکه بتواند با ضمیمه کردن آن تراکنش به یک بلاک، تایید آنرا شروع کرده تا بیت کوینهای رسیده به شما، قابل خرج کردن شوند. تایید به معنای آن است که شبکه به توافق رسیده است که بیت کوینهایی که دریافت کرده اید برای شخص دیگری فرستاده نشده بوده و جزیی از اموال شماست. وقتی تراکنش شما به یک بلاک پیوست شد، در زیر بلاکهایی که بعد از آن می آیند و بطور نمایی این توافق را یکپارچه کرده و خطر برگشت خوردن تراکنش را کاهش می دهند، دفن می شود. هر کاربری آزادست تا تعداد تاییدیه های تراکنش را خود تعیین کند، اما اغلب ٦ تاییدیه به قدر همان ٦ ماه صبر کردن برای تراکنش یک کارت اعتباری، ایمن به نظر می رسد.

کارمزد یک تراکنش چقدر خواهد بود؟

بیشتر تراکنشها بدون کارمزد قابل پردازش هستند، اما اغلب کاربران را تشویق می کنند که داوطلبانه اندکی کارمزد هم پرداخت کنند تا تراکنشهایشان سریعتر تایید شود و نیز دستمزد ی هم به استخراج کنندگان داده شود. اگر کارمزدی هم درخواست شود ،معمولاً بیش از چند سنت نخواهد بود. چنانچه لازم باشد، کلاینت بیت کوینی شمامعمولاً خواهد کوشید تا مقدار کارمزد مناسبی را برآورد کند.

کارمزد تراکنش، نوعی حفاظت است در برابر کاربرانی که با ارسال تراکنشهایشان شبکه را اورلود می کنند. نحوه دقیق عملکرد کارمزد هنوز در حال توسعه بوده و با گذشت زمان تغییر می کند. چون کارمزد به مقدار بیت کوین ارسالی مربوط نمی شود، ممکن است خیلی کم (۰,۰۰۰۵ بیت کوین برای یک انتقال ۱۰۰۰ بیت کوینی) و یا بطور ناعادلانه ای زیاد (۰,۰۰٤ بیت کوین برای یک پرداخت ۰,۰۲ بیت کوینی) بنظر آید. مبلغ کارمزد، با خصوصیاتی چون داده ی تراکنش و تکرار تراکنش، تعریف می شود.مثلاً اگر شما به دفعات زیاد، مبالغ کمی را دریافت کنید، آنگاه کارمزد ارسال بیشتر خواهد بود. چنین پرداختهایی را می توان مقایسه کرد با زمانی که بخواهید صورتحساب رستوران را با سنت بپردازید. خرج کردن سریع مقادیر کمی از بیت کوینهایتان نیز می تواند مشمول کارمزد شود. اگر فعالیت شما تابع الگوی تراکنشهای عادی باشد، مبلغ کارمزد بسیار کم خواهد بود.

اگر زمانی که کامپیوترم خاموش است بیت کوینی به من برسد، چه اتفاقی خواهد افتاد؟

اشکالی ندارد. دفعه بعد که برنامه کیف پول خود را راه اندازی می کنید، بیت کوینها ظاهر خواهند شد. در واقع، این نرم افزار روی کامپیوتر شما نیست که بیت کوینها را دریافت می کند، بلکه آنها در یک دفتر کل عمومی که بین تمام دستگاههای روی شبکه به اشتراک گذاشته شده است، ضمیمه می شوند. اگر هنگامی که برنامه کلاینت کیف پول شما در حال اجرا نیست، بیت کوینی برایتان بفرستند، دفعه بعدی که شما برنامه را راه اندازی کنید، برنامه بلاکها را دانلود کرده و در جریان تراکنشهایی که تا حالا از آنها بی خبر بوده اید، قرار خواهید گرفت و سرانجام بیت کوینها ظاهر می شوند، انگار که همین الان رسیده باشند. کیف پول فقط وقتی لازم است که بخواهید بیت کوینها را خرج کنید.

همزمان سازی به چه معناست و چرا اینقدر طول می کشد؟

همزمان سازی طولانی فقط برای کلاینتهای فول‌نُدی مانند هسته بیت کوین، الزامی است. به لحاظ فنی، همزمان سازی، فرایند دانلود کردن و درستی آزمایی تراکنشهای بیت کوینی پیشین روی شبکه است. برای اینکه بعضی کلاینتهای بیت کوین، بتوانند تراز قابل خرج کردنِ کیف پول بیت کوینی شما را محاسبه کرده و تراکنشهای جدید بسازند، لازم است که از تمام تراکنشهای پیشین آگاه باشند. این گام می تواند منابع زیادی طلب کند و نیاز به پهنای باند و فضای ذخیره سازی کافی دارد تا یک زنجیره بلاک با اندازه کامل را بسازد. برای حفظ امنیت بیت کوینها به اندازه کافی، مردم باید همچنان از کلاینتهای فول‌نُد استفاده کنند چرا که این کلاینتها درستی آزمایی و تقویت تراکنشها را انجام می دهند.

استخراج

استخراج بیت‌کوین یعنی چه؟

استخراج، فرایند صرف توان محاسبه برای پردازش تراکنشها، ایمن سازی شبکه و همزمان نگهداشتن همه با هم در سیستم است. می توان آنرا به منزله مرکز داده های بیت کوین تصور کرد؛ بجز آنکه طوری طراحی شده است که برای استخراج کنندگانی که در تمام کشورها در حال کارند،کاملاً تمرکز زدایی شده باشد و هیچ کسی کنترلی بر شبکه نداشته باشد. به این فرایند در قیاس با استخراج

طلا، استخراج می گویند چون مکانیسم گذرایی دارد که با آن بیت کوینهای جدید صادر می شوند. اما بر خلاف استخراج طلا، استخراج بیت کوین در ازای سرویسهای مفیدی که برای عملکرد یک شبکه پرداخت امن لازم است، جایزه ای هم در نظر می گیرد. تا وقتی آخرین بیت کوین صادر نشده باشد، استخراج بیت کوین همچنان الزامی است.

استخراج بیتکوین به چه صورت است؟

هر کسی می تواند با اجرای نرم افزار روی سخت افزاری ویژه، یک استخراج کننده بیت کوین باشد. نرم افزار استخراج، به انتشار تراکنشها در شبکه یP2P ، گوش فرا داده و اقدامات مقتضی جهت پردازش و تایید این تراکنش ها را انجام می دهد. استخراج کنندگان بیت کوین به این دلیل به این کار می پردازند که کارمزد تراکنشی را که کاربران برای پردازش سریعتر تراکنش های خود می پردازند، دریافت نموده و نیز بیت کوینهای تازه تولید شده را بر طبق یک فرمول ثابت به جریان اندازند.

تراکنشهای جدید برای آنکه پذیرفته شوند باید در بلاکی همراه با سند ریاضی انجام کار قرار گیرند. این مدرک ها را بسختی می توان تولید کرد ، چون هیچ راهی برای تولید آنها نیست، مگر میلیاردها بار محاسبه در ثانیه. استخراج کنندگان باید این محاسبات را انجام دهند تا سرانجام شبکه، بلاک های آنها را بپذیرد و به آنها پاداش دهد. هر چه تعداد استخراج کنندگان بیشتر شود، شبکه یافتن بلاکهای مجاز را بطور خودکار دشوارتر می کند تا مطمئن شود که زمان متوسط برای یافتن یک بلاک، همان ۱۰ دقیقه باقی خواهد ماند. در نتیجه، استخراج یک کار بسیار رقابتی است که هیچ استخراج کننده ای نمی تواند کنترلی بر آنچه که درون زنجیره بلاک است، داشته باشد.

برای تحمیل ترتیب زمانی بر زنجیره بلاک ، سند انجام کار طوری طراحی می شود که به بلاک قبلی وابسته باشد. به همین دلیل برگشت دادن تراکنشهای قبلی بطور نمایی دشوار می شود چرا که لازم است سند انجام کار روی تمامی بلاکهای دنباله آن، دوباره محاسبه گردند.اگر در یک زمان، دو بلاک پیدا شود استخراج کنندگان ابتدا به کار روی بلاکی که اول دریافت می پردازند و سپس به محض آنکه بلاک بعدی پیدا شد به طولانیترین زنجیره بلاکها سوییچ خواهند کرد. به این ترتیب به استخراج کنندگان اجازه داده خواهد شد که اجماعی جهانی را بر مبنای قدرت پردازش، حفظ کرده و آنرا ایمن نمایند.

استخراج کنندگان بیت کوین نه می توانند با تقلب کردن پاداش خود را افزایش دهند و نه می توانند تراکنشهای تقلبی را که ممکن است شبکه بیت کوین را خراب کند، پردازش نمایند، چون تمامیذُدهای بیت کوینی بر اساس پروتکل بیت کوین، هر گونه بلاکی را که شامل داده های غیرمجاز باشد، نخواهند پذیرفت. در نتیجه، حتی اگر نتوان به تمامی استخراج کنندگان بیت کوین اعتماد کرد، امنیت شبکه همچنان برقرار خواهد بود.

آیا استخراج بیتکوین، اتلاف انرژی نیست؟

بندرت می توان مصرف انرژی را برای اداره کردن و برقرار کردن امنیت یک سیستم پرداخت، اتلاف خواند. مانند هر سرویس پرداخت دیگری، استفاده از بیت کوین مستلزم هزینه های پردازش است. سرویسهای لازم برای عملکرد سیستم های پولی گسترده کنونی، مانند بانکها، کارتهای اعتباری و نیز خودروهای زرهی نیز انرژی زیادی مصرف می کنند. هرچند که بر خلاف بیت کوین، مصرف کل انرژی آنها شفاف نیست و نمی توان براحتی آنرا اندازه گیری کرد.

استخراج بیت کوین به گونه ای طراحی شده که در طول زمان بهینه تر شده و سخت افزارهایی خاصی را استفاده کند که انرژی کمتری مصرف می کنند و هزینه های استخراج بتدریج با تقاضا متناسب گردد. هر زمان که استخراج بیت کوین کمتر رقابتی شده و نیز سودآوری کمتری داشته باشد، بعضی از استخراج کنندگان دست از فعالیت خواهند کشید. افزون براین، تمام آن انرژی که صرف استخراج می شود، در پایان به گرما تبدیل خواهد شد و بیشتر استخراج کنندگانی که سود می کنند از این گرما استفاده خوبی خواهند کرد. یک شبکه که کارایی آن بهینه سازی شده، شبکه ایست که‌عملاً هیچگونه انرژی اضافی مصرف نمی کند. هر چند که این یک ایده آل است، اقتصاد استخراج بگونه ایست که هر استخراج کننده ای تلاش می کند به آن دست یابد.

چگونه استخراج به امنیت بیت کوین کمک می کند؟

استخراج چیزی شبیه به یک بخت آزمایی رقابتی ایجاد کرده و کار را برای کسانی که می خواهند بطور پی در پی بلاکهای تراکنشی جدیدی به زنجیره بلاک بیفزایند، دشوار کرده است. به این ترتیب از اینکه هر کسی بتواند قدرت بلاک کردن تراکنشهای خاصی را بدست بیاورد، جلوگیری کرده و از بیطرفی شبکه محافظت به عمل آورده میشود. همچنین اجازه داده نخواهد شد که افراد با تعویض بخشهایی از زنجیره بلاک، مخارج خودشان را کم کرده و از دیگر کاربران کلاهبرداری نمایند. استخراج، برگشت دادن یک تراکنش قدیمی را با الزام به بازنویسی تمام بلاکهایی که در ادامه این تراکنش آمده اند، بطور نمایی دشوارتر ساخته است.

برای شروع به کار استخراج به چه چیزهایی نیاز دارم؟

در اوایل عمر بیت کوین، هر کسی می توانست با استفاده از CPU کامپیوترش، یک بلاک جدید پیدا کند. هر چه بر تعداد استخراج کنندگان افزوده شد، دشواری یافتن بلاکهای جدید هم بشدت زیاد شد تا جایی که امروزه تنها روش استخراج مقرون به صرفه را با استفاده از سخت افزارهای خاص، بکار می گیرند . برای اطلاعات بیشتر از BitcoinMining.com دیدن کنید.

امنیت

آیا بیت‌کوین امن است؟

تکنولوژی بیت کوین- پروتکل آن و رمزنگاری- سابقه ردیابی امنیتی قوی دارد و شبکه بیت کوین‌احتمالاً بزرگترین پروژه محاسباتی توزیع شده در جهان است. بیشترین آسیب پذیری بیت کوین ناشی از خطای کاربر است. ممکن است فایلهای کیف پول بیت کوینی که کلیدهای محرمانه لازم را ذخیره می کند، بطور تصادفی حذف، گم و یا دزدیده شوند، درست مانند آنکه پول نقد واقعی، به شکل دیجیتال ذخیره شده باشد. خوشبختانه کاربران می توانند اقدامات امنیتی مطمئنی را بکار بندند تا از پول خود محافظت کنند یا از آن دسته از تامین کنندگان خدمات که سطوح امنیتی خوب و نیز بیمه بر علیه دزدی یا گم شدن ارائه می کنند، استفاده نمایند.

آیا بیت‌کوین تا کنون هک نشده است؟

سالها پس از پیدایش بیت کوین، هنوز قوانین پروتکل و رمزنگاریی که در آن استفاده شده، معتبر است و این نشانه خوبی است از اینکه مفهوم آن بخوبی طراحی شده است. اما در طول زمان نقایص امنیتی در پیاده سازی نرم افزارهای مختلف، یافته و برطرف شده است. امنیت نرم افزار بیت کوین همانند نرم افزارهای دیگر، به سرعت پیدا شدن عیبها و رفع آنها بستگی دارد. هر چه این موارد بیشتر کشف شوند، بیت کوین بلوغ بیشتری بدست خواهد آورد.

بین دزدی و رخنه های امنیتی که در کسب و کارها و مبادلات مختلف رخ می دهد، اغلب سوء تفاهم هایی وجود دارد. هر چند هر دوی اینها ناخوشایندند ولی هیچکدام نه به معنای هک شدن خود بیت کوین است و نه نشان از عیوب ذاتی بیت کوین دارد؛ درست مثل سرقت از یک بانک که به معنای تقلبی بودن دلار نیست. اما دقیقتر آنست که بگوییم مجموعه کاملی از اقدامات خوب و راه حلهای امنیتی شهودی لازم است تا از پول کاربران محافظت بهتری بعمل آید و خطرات کلی از دست دادن پولشان کاهش یابد. در طول چندین سال گذشته، ویژگیهای امنیتی مانند رمزگذاری کیف پول، کیف پولهای آفلاین، کیف پولهای سخت افزاری و تراکنشهای چندامضایی، بسرعت توسعه یافته اند.

آیا کاربران می‌توانند علیه بیت‌کوین توطئه کنند؟

تغییر دادن پروتکل بیت کوین به این آسانی ها ممکن نیست. هر مشتری بیت کوینی که از همان قوانین یکسان پیروی نکند نمی تواند قوانین خودش را به کاربران دیگر اعمال کند. همانطور که بر طبق مشخصات فعلی، خرج کردن دوباره در همان زنجیره بلاک ممکن نیست، خرج کردن بیت کوینها بدون یک امضای مجاز هم ممکن نیست. بنابراین امکان ندارد که بتوان مقادیر کنترل نشده ای از بیت کوینها را به یکباره تولید کرد، دارایی کاربران دیگر را خرج نمود، شبکه را برای همیشه از کار انداخت و یا کارهایی از این دست انجام داد.

اما به هر حال، بیشتر استخراج کنندگان می توانند تراکنشهای اخیر را بدلخواه بلاک کرده و یا برگشت دهند. بسیاری از کاربران نیز می توانند برای اعمال و پذیرش بعضی تغییرات، فشار وارد کنند. چون بیت کوین فقط زمانی بدرستی کار می کند که بین تمامی کاربران اجماع کامل حاصل شده باشد، بنابراین تغییر دادن پروتکل می تواند بسیار دشوار باشد و لازم است اکثریت قریب به اتفاق کاربران این تغییرات را بپذیرند به گونه ای که بقیه کاربران‌تقریباً هیچ انتخابی جز پیروی از اکثریت را نداشته باشند. به عنوان یک قاعده کلی، بسختی می توان تصور کرد که چرا یک کاربر بیت کوین باید تغییری را بپذیرد که ممکن است پول او را به خطر بیندازد.

آیا بیت کوین نسبت به محاسبات کوانتمی آسیب پذیر است؟

بله. بطور کلی بیشتر سیستم های متکی بر رمزنگاری، سیستمهای بانکی هستند. اما هنوز کامپیوترهای کوانتمی حتی وجود ندارند و گمان نمی رود که تا چند صباحی در آینده هم پا به عرصه وجود گذارند. بر فرض که کامپیوترهای کوانتمی را بتوان تهدیدی قریب الوقوع برای بیت کوین بشمار آورد، می توان پروتکل را طوری ارتقا داد که از الگوریتمهای پسا-کوانتومی استفاده کند. با توجه به اهمیت این بروزرسانی، می توان با خیال راحت انتظار داشت که توسعه دهندگان پروتکل را بدقت بازبینی کرده و تمامی کاربران بیت کوین آنرا بپذیرند.