همه‌چیز در مورد بیت کوین

۱- سؤالات عمومی

۱-۱ بیت کوین چیست؟

بیت کوین یک شبکه توافقی است که یک سیستم پرداخت جدید و یک نوع پول کاملاً دیجیتال را به وجود آورده است. این اولین شبکه پرداخت نقطه‌به‌نقطه تمرکززدایی شده است که توسط کاربرانش بدون هیچ‌گونه اختیار مرکزی و یا واسطه‌ای، نیرومند شده است. ازنقطه‌نظر یک کاربر، بیت کوین بسیار شبیه پول نقد اینترنتی است. بیت کوین همچنین می‌تواند به‌عنوان مهم‌ترین سیستم دفترداری با سه ورودی موجود بشمار آید.

۱-۲ سازنده بیت کوین کیست؟

بیت کوین اولین پیاده‌سازی یک مفهوم به نام ارز سری است که اولین بار در سال ۱۹۹۸ توسط وِی دای در فهرست ایمیل سایفرپانک‌ها، توصیف‌شده 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 استفاده‌شده است. مشخصات اولین بیت کوین و اثبات مفهوم در سال ۲۰۰۹ توسط ساتوشی ناکاموتو در یک فهرست ایمیل رمزنگاری‌شده منتشر گردید. ساتوشی بدون آنکه چیز زیادی از خودش فاش سازد، پروژه را به اواخر سال ۲۰۱۰ موکول کرد. از آن موقع این جامعه به‌طور نمایی با توسعه دهندگان بسیاری که روی بیت کوین کار می‌کنند، رشد کرده است.

گمنامی ساتوشی اغلب باعث نگرانی‌های ناموجهی می‌شود که بسیاری از آن‌ها به فهم نادرست از طبیعت متن‌باز بیت کوین برمی‌گردد. پروتکل بیت کوین و نرم‌افزار به‌صورت باز منتشرشده است و هر توسعه‌دهنده‌ای در هرکجای گیتی می‌تواند کد آن را بازبینی کرده و یا نسخه تغییریافته نرم‌افزار بیت کوین مخصوص خودش را بسازد. تأثیر ساتوشی نیز مانند توسعه‌دهندگان کنونی، محدود به تغییراتی بود که از دیگران اقتباس می‌کرد و بنابراین بیت کوین را کنترل نمی‌کرد. امروزه هویت مخترع بیت کوین به‌خودی‌خود احتمالاً مانند هویت شخصی است که کاغذ را اختراع کرده بود.

۱-۳ چه کسی کنترل‌کننده شبکه بیت کوین است؟

هیچ‌کس مالک شبکه بیت کوین نیست، درست همان‌طور که هیچ‌کس صاحب تکنولوژیی که در ورای ایمیل است، نیست. این کاربران بیت کوین در سراسر جهان هستند که آن را کنترل می‌کنند. توسعه‌دهندگان بیت کوین اگرچه نرم‌افزار آن را بهبود می‌بخشند ولی نمی‌توانند تغییری را بر پروتکل بیت کوین تحمیل کنند، چراکه هر کاربری آزاد است که نرم‌افزار خود و نسخه‌ای که خود می‌پسندد را استفاده کند. تمامی کاربران، برای اینکه با یکدیگر سازگار بمانند باید از نرم‌افزاری استفاده کنند که از همان قواعد پیروی می‌کند. بیت کوین تنها به‌شرط

اجماع کامل بین تمامی کاربران، می‌تواند به‌درستی کار کند؛ بنابراین تمامی کاربران و توسعه‌دهندگان انگیزه قوی برای حفظ این اجماع را خواهند داشت.

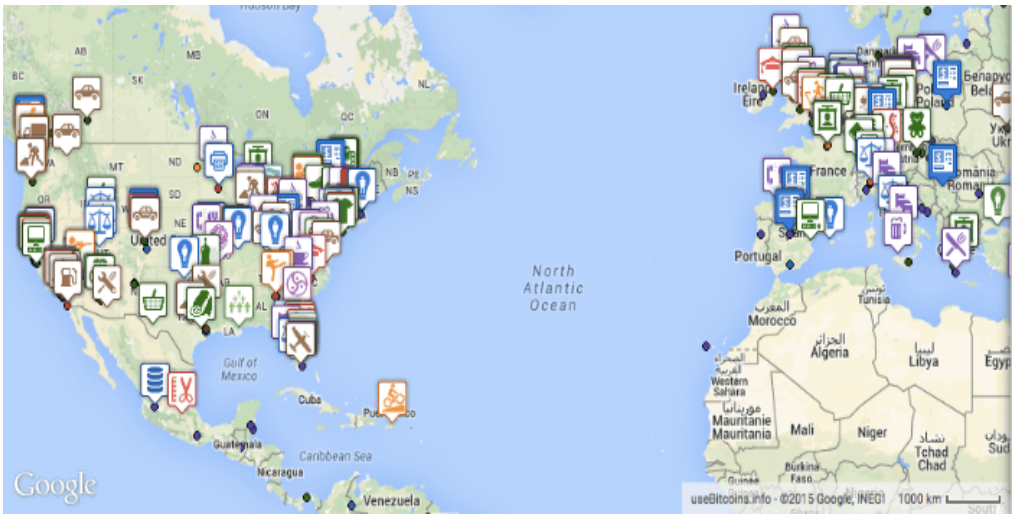
۱-۴ عملکرد بیت کوین چگونه است؟

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 تهیه‌کرده و به کاربر اجازه می‌دهد 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 تاکنون پردازش‌شده است و به کامپیوتر کاربر اجازه می‌دهد تا درستی هر تراکنش را بیازماید. اعتبار هر تراکنش به‌وسیله امضای دیجیتالی مربوط به آدرس‌های 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، هرکسی می‌تواند تراکنش‌ها را با استفاده از توان محاسباتی سخت‌افزاری که ویژه این کار است، پردازش کرده و برای این سرویس، بیت کوین‌هایی را هم به‌عنوان جایزه به دست آورد. به این کار اصطلاحاً "استخراج" می‌گویند.

۱-۵ آیا مردم واقعاً از بیت کوین استفاده می‌کنند؟

تعداد روزافزونی از کسب و کارها و افراد از بیت کوین استفاده می‌کنند. این کسب‌وکارها ممکن است کسب‌وکارهایی به‌صورت رودررو با مشتری باشد، مانند رستوران‌ها، کاشانه‌ها، دفاتر حقوقی و یا سرویس‌های آنلاین مانند Namecheap، WordPress، Reddit و یا Flattr. بیت کوین اگرچه پدیده‌ای نسبتاً جدید بشمار می‌آید، اما به‌سرعت رو به رشد است. در پایان آگوست ۲۰۱۳، ارزش تمامی بیت کوینهای در گردش بالغبر ۱،۵ میلیارد دلار امریکا بود و ارزش بیت کوین‌هایی که روزانه مبادله می‌شد، به میلیون‌ها دلار می‌رسید.



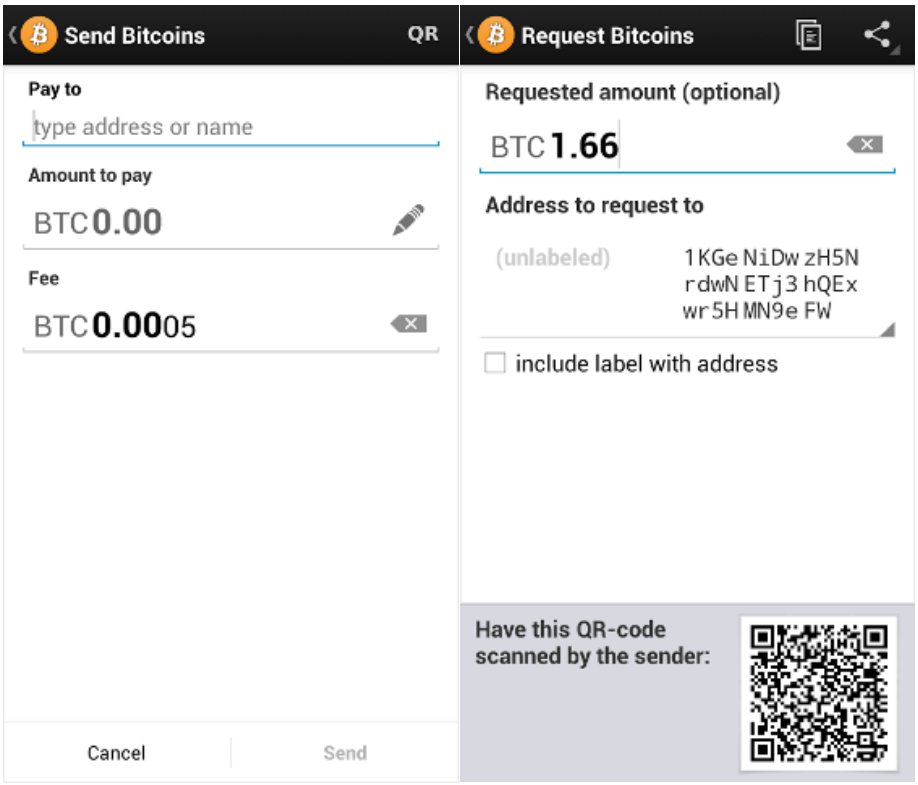
۱-۶ چگونه می‌توان بیت کوین به دست آورد؟

- در صورت پرداخت وجه برای کالا یا خدمات
- خرید آن از صرافی بیت کوین
- مبادله بیت کوین‌ها با کسی در نزدیکی خود
- به دست آوردن بیت کوین از راه استخراج رقابتی

اگرچه ممکن است افرادی باشند که بخواهند بیت کوین‌ها را در برابر کارت اعتباری یا پرداخت پی پال بفروشند، ولی بیشتر صرافی‌ها اجازه پرداخت با این روش‌ها را نمی‌دهند. 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 این‌گونه موارد، پرداخت برگشتی می‌گویند.

۱-۷ پرداخت بیت کوین چقدر دشوار است؟

پرداخت به‌وسیله بیت کوین، آسان‌تر از خرید توسط کردیت کارت یا دبیت کارت است و می‌تواند بدون استفاده از یک حساب تجاری دریافت شود. پرداخت‌ها از طریق یک برنامه کاربردی کیف پول، چه روی کامپیوتر و چه روی گوشی تلفن هوشمند شما با واردکردن آدرس گیرنده، مقدار وجه پرداختی و فشردن دکمه ارسال، انجام می‌شود. بسیاری از کیف پول‌ها می‌توانند با اسکن کردن یک کد QR و یا با استفاده از تکنولوژی NFC و تماس دادن دوگوشی تلفن باهم، آدرس گیرنده را آسان‌تر وارد نمایند.



۱-۸ مزایای بیت کوین چیست؟

۱-۸-۱ آزادی پرداخت وجه

هر موقع از شبانه‌روز و در هرکجای جهان که باشید، ارسال و دریافت فوری هر مبلغ از بیت کوین امکان‌پذیر است. هیچ روزی تعطیل نیست. هیچ حدومرزی در کار نیست. هیچ محدودیتی اعمال نخواهد شد. بیت کوین به کاربرانش اجازه می‌دهد بر پول خودکنترل کامل داشته باشند.

۱-۸-۲ کارمزدهای بسیار اندک

در حال حاضر پردازش پرداخت وجه با بیت کوین، به‌صورت بدون کارمزد و یا با کارمزدی بسیار اندک، انجام می‌گیرد. کاربران می‌توانند برای پردازش سریع‌تر تراکنش خود، کارمزد پرداخت نمایند که درنتیجه تأییدیه تراکنش را سریع‌تر از شبکه دریافت خواهند کرد. علاوه بر این، پردازشگرهای تجاری هم هستند که سوداگران را در پردازش تراکنش‌ها، تبدیل بیت کوین‌ها به یک ارز بدون پشتوانه و واریز مبالغ به‌طور مستقیم و روزانه به‌حساب بانکی آن‌ها، یاری دهند. چون این تراکنش‌ها بر مبنای بیت کوین است، کارمزدهایی به‌مراتب کمتر از کارمزدهای شبکه کارت اعتباری یا پی پال، از آن‌ها خواسته خواهد شد.

۱-۸-۳ ریسک کمتر برای سوداگران

تراکنش‌های بیت کوین امن و برگشت‌ناپذیر 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 می‌کند و نیازی هم به پیروی از PCI نیست. سوداگران می‌توانند به‌سادگی 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 عبارت است از: کارمزد کمتر، بازارهای بزرگ‌تر و هزینه‌های مدیریت کمتر.

۱-۸-۴ امنیت و کنترل

کاربران بیت کوین بر تراکنش‌های خودکنترل کامل دارند. غیرممکن است که بتوان معامله‌کنندگان را مجبور کرد؛ مانند آنچه در روش‌های دیگر پرداخت گاهی پیش می‌آید، مبالغی ناخواسته و یا از پیش اعلام‌نشده را بپردازند. پرداخت‌های بیت کوینی بدون اینکه اطلاعات شخصی کسی به تراکنش پیوست شده باشد، انجام می‌گیرد. به‌این‌ترتیب محافظت شدیدی در برابر سرقت هویت ایجادشده است. کاربران بیت کوینی همچنین می‌توانند با تهیه بک آپ یا نسخه پشتیبان و رمزگذاری، از پولشان محافظت نمایند.

۱-۸-۵ شفافیت و بی‌طرف بودن

تمامی اطلاعات در مورد تأمین پول بیت کوین به‌سادگی روی زنجیره بلاک در دسترس همه هست و می‌توان آن را بلافاصله درستی آزمایی کرده و از آن‌ها استفاده نمود. هیچ شخص یا سازمانی نمی‌تواند پروتکل بیت کوین را کنترل و یا دست‌کاری نماید چون این پروتکل با رمزنگاری، ایمن شده و هسته بیت کوین را ازنظر شفافیت، بی‌طرفی کامل و قابل پیش‌بینی بودن قابل‌اعتماد کامل ساخته است.

۱-۹ معایب بیت کوین چیست؟

۱-۹-۱ میزان پذیرش

بسیاری از مردم هنوز در مورد بیت کوین آگاهی ندارند. همه‌روزه، کسب‌وکارهای بیشتری بیت کوین‌ها را می‌پذیرند چراکه مزایای آن را می‌خواهند، اما این فهرست هنوز کوچک است و نیاز به رشد دارد تا بتوان از فایده های این شبکه بهره جست.

۱-۹-۲ ناپایداری

ارزش کلی بیت کوین‌های در گردش و تعداد کسب‌وکارهایی که از بیت کوین استفاده می‌کنند، در مقایسه با آنچه باید باشد، هنوز کم است؛ بنابراین، رویدادها، معاملات و یا فعالیت‌های تجاری نسبتاً کمی هستند که می‌توانند بر بهای بیت کوین اثری چشمگیر داشته باشند. به لحاظ نظری این ناپایداری، در صورت رشد بازارها و فنّاوری بیت کوین، کاهش خواهد یافت. پیش‌ازاین، 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.

۱-۹-۳ درحال‌توسعه بودن

نرم‌افزار بیت کوین هنوز نسخه بتاست و ویژگی‌های ناقص بسیاری دارد که به‌طور فعال در دست توسعه است. ابزارها، ویژگی‌ها و سرویس‌های جدید درحال‌توسعه یافتن هستند تا بیت کوین را امن‌تر و برای توده مردم دسترس‌پذیر تر بسازند. بیشتر کسب‌وکارهای بیت کوینی نوپا بوده و هنوز تحت پوشش بیمه نیستند. به‌طورکلی، فرایند بلوغ بیت کوین هنوز در جریان است.

۱-۱۰ چرا مردم به بیت کوین اعتماد دارند؟

سهم بزرگی از اعتماد به بیت کوین ناشی از این حقیقت است که اصولاً نیازی به اعتماد کردن نیست. بیت کوین کاملاً متن‌باز و تمرکززدایی شده است؛ یعنی هرکسی می‌تواند هر زمان که بخواهد به سراسر کد منبع آن، دسترسی داشته باشد؛ بنابراین هر توسعه‌دهنده‌ای در جهان می‌تواند به‌دقت درستی طرز کار بیت کوین را بیازماید. هرکسی می‌تواند شفافیت تمامی تراکنش‌ها و بیت کوین‌های ساخته‌شده را فوراً مورد ملاحظه قرار دهد. تمامی پرداخت‌ها را می‌توان بدون اتکا به‌طرف سومی، انجام داد و کل سیستم از طریق الگوریتم‌های رمزنگاری که به‌دقت نظیر به نظیر مرور شده، درست مثل آنچه در بانکداری آنلاین انجام می‌شود، محافظت می‌گردد. هیچ سازمان یا فردی نمی‌تواند بیت کوین را کنترل کند و حتی اگر تمامی کاربران نتوانند به این شبکه اعتماد کنند، امنیت شبکه پابرجاست.

۱-۱۱ آیا با بیت کوین می‌توان پولدار شد؟

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 می‌آید و یا از قوانین اولیه اقتصاد پیروی نمی‌کند، محتاط باشید. بیت کوین فضای رو به رشدی از نوآوری‌هاست و فرصت‌های کسب‌وکار زیادی دارد که البته شامل خطراتی هم هست. هیچ تضمینی وجود ندارد که چون بیت کوین تاکنون با سرعت زیادی توسعه‌یافته است، ازاین‌پس 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 به دست آوردن پول به‌وسیله بیت کوین هست مانند استخراج، سفته‌بازی و یا راه انداختن کسب‌وکارهای جدید. تمامی این روش‌ها رقابتی هستند و هیچ تضمینی وجود ندارد که سودآور هم باشند. این به خود فرد بستگی دارد که هزینه‌ها و مخاطراتی را که در این نوع پروژه‌ها هست، به‌درستی ارزیابی کرده باشد.

۱-۱۲ ماهیت بیت کوین چیست؟

بیت کوین به همان اندازه کارت‌های اعتباری و شبکه‌های بانکداری آنلاین که مردم همه‌روزه از آن‌ها استفاده می‌کنند، مجازی است. بیت کوین درست مانند سایر اشکال پول، برای پرداخت آنلاین در فروشگاه‌های واقعی بکار می‌رود و نیز می‌تواند درست مانند سکه‌های کازاسیوس به شکل فیزیکی پول تبدیل شود، اما پرداخت با گوشی‌های تلفن همراه معمولاً آسان‌تر است. ترازهای بیت کوینی در یک شبکه بزرگ توزیع‌شده، ذخیره‌شده است و هیچ‌کس نمی‌تواند با تقلب آن را تغییر دهد. به‌عبارت‌دیگر، کاربران بیت کوین کنترل اختصاصی بر موجودی خوددارند و بیت کوین‌هایشان صرفاً به دلیل مجازی بودن، غیب نمی‌شود.

۱-۱۳ آیا بیت کوین گمنام است؟

بیت کوین طوری طراحی‌شده 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 نمی‌توان آن‌ها را با همان سطح حریم خصوصی که پول نقد دارد، عرضه کرد. استفاده از بیت کوین، رکوردهای عمومی گسترده‌ای از خود به‌جای می‌گذارد. مکانیسم های مختلفی برای محافظت از حریم خصوصی کاربران وجود دارد و مکانیسم‌های بیشتری هم درحال‌توسعه هستند. به‌هرحال، قبل از اینکه این ویژگی‌ها به‌درستی توسط بیشتر کاربران بیت کوین بکار گرفته شوند، کارهای زیادی هست که باید انجام شود.

نگرانی‌هایی در باب اینکه محرمانه بودن تراکنش‌های بیت کوین به‌منظور انجام کارهای غیرقانونی است، ایجادشده است؛ اما این نگرانی‌ها هیچ ارزشی ندارد؛ چون بیت کوین بدون تردید تابع قوانین و مقرراتی است که مشابه آن در سیستم‌های مالی وجود دارد. بیت کوین نمی‌تواند گمنام‌تر از پول نقد باشد و احتمال جلوگیری از بررسی‌های جنایی، در مورد آن کم است. افزون بر آن، بیت کوین نیز طوری طراحی‌شده که از دامنه گسترده‌ای از جرائم مالی جلوگیری می‌کند.

۱-۱۴ چگونه بیت کوین‌های ازدست‌رفته قابل بازیابی است؟

اگر کاربری کیف پول خود را گم کند، پول او از گردش خارج می‌شود. بیت کوین‌های گمشده، درست مانند بقیه بیت کوین‌ها همچنان در زنجیره بلاک باقی می‌مانند، اما برای همیشه به خواب می‌روند؛ چون هیچ‌کس هیچ راهی ندارد تا کلید (های) محرمانه‌ای را؛ که بیت کوین‌ها را دوباره قابل‌خرج کردن می‌نماید، پیدا کند. نظر به قانون عرضه و تقاضا، وقتی بیت کوین‌های کمتری در دسترس باشند، تقاضا برای آن‌هایی که باقی‌مانده‌اند بیشتر می‌شود و برای جبران این تقاضا، بهای بیت کوین‌ها افزایش می‌یابد.

۱-۱۵ آیا بیت کوین، به یک شبکه پرداخت عمده ارتقاء خواهد یافت؟

شبکه بیت کوین می‌تواند تعداد بسیار بیشتری تراکنش در ثانیه را نسبت به چیزی که امروزه انجام می‌دهد، پردازش کند؛ اما هنوز آماده نیست تا به جایگاه شبکه‌هایی مانند شبکه‌های کارت‌های اعتباری بزرگ برسد. برای از میان برداشتن محدودیت‌های کنونی، کارهایی در دست اقدام است و الزامات آینده به‌خوبی شناسایی‌شده‌اند. از زمان پیدایش شبکه بیت کوین، همه ابعاد آن در فرایند مداومی از بلوغ، بهینه‌سازی و تخصصی شدن بوده است و انتظار می‌رود 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 تخصصی‌تر تبدیل شوند. برای دانستن جزئیات بیشتر به ارتقاء روی صفحه‌های ویکی مراجعه کنید.

۲- سؤالات حقوقی

۲-۱ آیا بیت کوین قانونی است؟

تا جایی که ما می‌دانیم، در بیشتر محاکم قضایی، ازنظر قانون بیت کوین غیرقانونی نیست؛ اما بعضی از دستگاه‌های قضایی (مانند کشورهای آرژانتین و روسیه) ارزهای خارجی را بشدت محدود و یا ممنوع کرده‌اند. بعضی دیگر از دستگاه‌های قضایی (مانند تایلند) ممکن است صدور گواهینامه برای بعضی موجودیت‌های خاص، مثلاً صرافی‌های بیت کوینی را محدود کرده باشند. قانون‌گذاران در دستگاه‌های قضایی مختلف در حال برداشتن گام‌هایی هستند تا برای افراد و کسب‌وکارها، قوانینی برای پیوند این تکنولوژی جدید با یک سیستم مالی رسمی و تنظیم‌شده، وضع نمایند. مثلاً شبکه اجرای جرائم مالی (FinCEN)؛ که دفتری در وزارت خزانه‌داری ایالات‌متحده امریکاست، راهنمای غیر الزام‌آوری منتشر کرده و در آن به تشریح چگونگی فعالیت‌های معین در خصوص ارزهای مجازی پرداخته است.

۲-۲ آیا بیت کوین برای فعالیت‌های غیرقانونی قابل‌استفاده است؟

بیت کوین نوعی پول است و پول همواره برای اهداف قانونی و غیرقانونی بکار می‌رفته است. پول نقد، کارت‌های اعتباری و دستگاه‌های بانکی جاری ازنظر استفاده در جرائم مالی، به‌طور گسترده‌ای از بیت کوین پیشی می‌گیرند. بیت کوین توانسته است نوآوری‌های چشمگیری

در دستگاه‌های پرداخت بیاورد و منافع چنین نوآوری‌هایی اغلب بسیار فراتر از نقطه‌ضعف‌های احتمالی آن‌هاست.

بیت کوین طوری طراحی‌شده تا:

- در ایمن کردن بیشتر پول‌سازی یک گام فراتر باشد.
- نیز حفاظت چشمگیری در برابر بسیاری از اشکال جرائم مالی به عمل آورد. مثلاً جعل کردن بیت کوین‌ها، کاملاً غیرممکن است.
- کاربران بر پرداخت‌های خودکنترل کامل دارند و نمی‌توانند مبالغ تائید نشده را مانند آنچه در کارت‌های اعتباری کلاه‌برداری می‌شود، دریافت کنند.
- تراکنش‌های بیت کوینی برگشت‌ناپذیر 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 گم‌شدن بسیار ایمن شده است.

نگرانی‌هایی وجود دارد مبنی بر اینکه بیت کوین می‌تواند برای مجرمین بسیار جذاب باشد چراکه می‌توان حریم شخصی و پرداخت‌های برگشت‌پذیر با آن داشت؛ اما این ویژگی‌ها در پول نقد و حواله بانکی که بسیار زیاد از آن‌ها استفاده می‌شود و به‌خوبی جاافتاده‌اند، هم وجود دارد. بدون تردید، استفاده از بیت کوین تابع قوانین مشابهی است که قبلاً در جای خود در دستگاه‌های مالی موجود گنجانده‌شده‌اند و احتمال ندارد که بیت کوین از انجام بررسی‌های جنایی، جلوگیری کند. به‌طورکلی، مرسوم است که پیشرفت‌های مهم قبل از اینکه مزایای آن‌ها به‌خوبی شناخته شود، بحث‌برانگیز باشند. اینترنت مثال خوبی برای بسیاری از کسانی است که تصوری این‌چنینی دارند.

۳-۲ آیا بیت کوین می‌تواند تابع قوانین و مقررات باشد؟

پروتکل بیت کوین به‌خودی‌خود، بدون همکاری تقریباً تمامی کاربرانش که نرم‌افزار مورداستفاده‌شان را خود برمی‌گزینند، قابل‌تغییر نیست. تلاش برای اختصاص امتیازهای ویژه به یک مرجع محلی در قوانین شبکه جهانی بیت کوین، احتمالی شدنی نیست. هر سازمان ثروتمندی می‌توانست انتخاب کند که برای سخت‌افزار استخراج طوری سرمایه‌گذاری 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 چراکه میزان سرمایه گذاریش باید بیشتر از تمام استخراج‌کننده‌های دیگر در جهان، باشد.

اما وضع مقررات استفاده از بیت کوین، به روشی مشابه سایر ابزارها امکان‌پذیر است. درست مانند دلار، بیت کوین می‌تواند برای مقاصد بسیار متفاوتی بکار رود که بعضی از آن‌ها قانونی و برخی دیگر بر اساس بعضی از محاکم قانون‌گذاری، غیرقانونی خواهند بود. از این لحاظ بیت کوین هیچ فرقی با دیگر ابرازها یا منابع ندارد و در هر کشوری، می‌تواند تابع قوانین و مقررات آن کشور باشد. بر اساس بعضی قوانین محدودکننده، استفاده از بیت کوین همچنین می‌تواند دشوار باشد. در این صورت تعیین درصد کاربرانی که از این فنّاوری استفاده می‌کنند، سخت خواهد بود. دولتی که بیت کوین را ممنوع می‌کند، از کسب‌وکارهای داخلی و بازارهای رو به رشد جلوگیری کرده و نوآوری را به‌سوی

دیگر کشورها می‌راند. چالش پیش روی قانون‌گذاران مثل همیشه توسعه راه‌حل‌هایی است که در عین کارا بودن، رشد بازارها و کسب‌وکارهای نوپدید را دچار مشکل نکند.

۲-۴ مالیات چقدر بر بیت کوین اثرگذار است؟

بیت کوین ارز بدون پشتوانه‌ای نیست که در هر دستگاه قضایی، پولی قانونی بشمار بیاید، اما مشمولیت مالیاتی اغلب فارغ از واسطه‌ی بکار رفته، شامل حال بیت کوین هم می‌شود. قوانین بسیار گوناگونی در بسیاری از دستگاه‌های قضایی وضع‌شده است که می‌تواند درآمد، فروش، دستمزد، بهره‌های سرمایه‌ای و یا اشکال دیگر مشمولیت‌های مالیاتی را برای بیت کوین ایجاد کند.

۲-۵ بیت کوین تا چه حد از مصرف‌کننده حمایت می‌کند؟

بیت کوین دست مردم را باز می‌گذارد تا با شرایط خودشان، تراکنش انجام دهند. هر کاربری می‌تواند مانند پول نقد، پرداخت‌ها را ارسال و یا دریافت کند اما همچنین می‌توانند در قراردادهای پیچیده‌تری هم مشارکت کنند. چند امضایی، اجازه می‌دهد که یک تراکنش توسط شبکه پذیرفته شود تنها اگر تعداد معینی از اعضاء یک گروه تعریف‌شده، موافق امضا کردن آن تراکنش باشند. این باعث نوآوری در توسعه سرویس‌های میانجی حل اختلاف در آینده خواهند شد. چنین سرویس‌هایی می‌توانند در صورت عدم توافق بین طرفین، در نقش طرف سومی برای تائید 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 به‌طور بالقوه می‌تواند به‌عنوان مدرکی علیه کسب‌وکارهایی که کلاه‌برداری می‌کنند، بکار گرفته شود.

شایان‌ذکر است که سوداگران که همواره به وجهه عمومی خود برای بقای کسب‌وکارشان وابسته‌اند و به کارمندانشان حقوق می‌پردازند، در هنگام معامله با مصرف‌کنندگان جدید خود، سطح دسترسی یکسانی به اطلاعات ندارند. بیت کوین هم فرد و هم‌کسب و کارها را در برابر پرداخت‌های برگشتی تقلبی محافظت می‌کند و درعین‌حال به مصرف‌کننده این انتخاب را می‌دهد که چنانچه نخواهد به یک سوداگر خاص اعتماد کند، خواستار حفاظت بیشتر باشد.

۳- سؤالات اقتصادی

۳-۱ بیت کوین‌ها چگونه ساخته می‌شوند؟

بیت کوین‌ها در فرایندی رقابتی و تمرکززدایی شده که "استخراج" نام دارد، تولید می‌شوند. این فرایند مستلزم آن است که افراد از شبکه برای خدمات خود، جایزه دریافت کنند. استخراج‌کنندگان بیت کوین تراکنش‌ها را پردازش کرده و با استفاده از سخت‌افزار تخصصی، شبکه را ایمن کرده و در عوض آن بیت کوین‌های جدید جمع‌آوری می‌نمایند.

طراحی پروتکل بیت کوین به گونه ایست که بیت کوین‌های جدید را با نرخ ثابتی تولید می‌کند. به‌این‌ترتیب استخراج بیت کوین یک کسب‌وکار رقابتی خواهد شد. اگر استخراج‌کنندگان بیشتری به شبکه بپیوندند، سودآوری مرتباً دشوار خواهد شد و استخراج‌کنندگان باید به دنبال بازده برای کاهش هزینه‌های استخراج باشند. هیچ مرجع مرکزی یا توسعه‌دهنده‌ای، اختیار آن‌ها ندارد تا سیستم را برای افزایش سود، کنترل یا دست‌کاری کند. هر نُد بیت کوین در جهان، هر آنچه را که در تطابق با قوانینی که انتظار می‌رود سیستم از آن پیروی کند، نباشد حذف خواهد کرد.

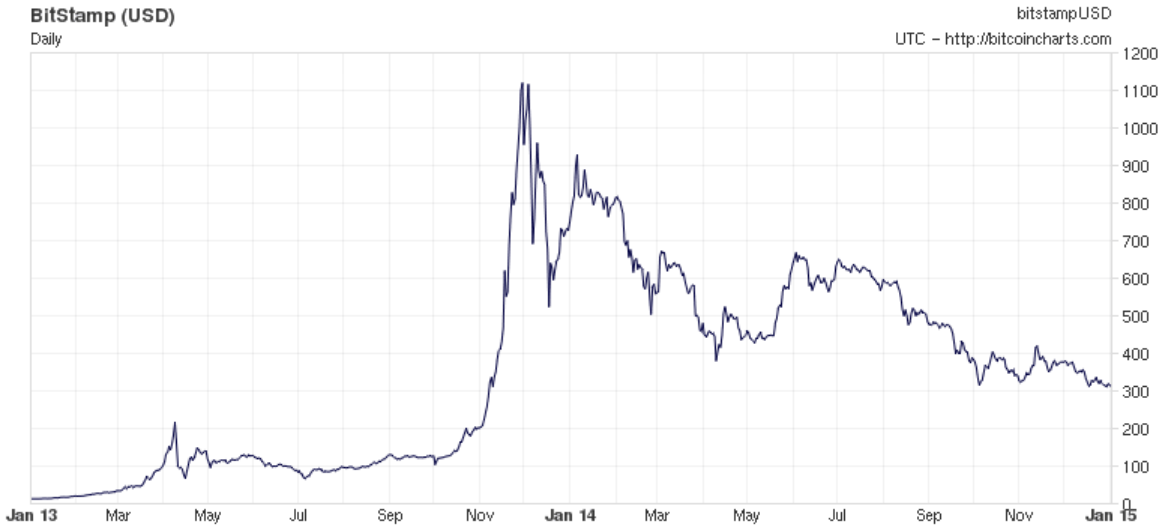
بیت کوین‌ها با نرخی کاهنده و قابل پیش‌بینی، تولید می‌شوند. تعداد بیت کوین‌های جدیدی که هرسال تولید می‌شود، به‌طور خودکار در طول زمان نصف می‌شود تا اینکه مجموع بیت کوین‌های موجود به ۲۱ میلیون برسد. از این هنگام به بعد، دیگر بیت کوینی صادر نخواهد شد. در این نقطه، احتمالاً به‌طور اختصاصی به استخراج‌کنندگان بیت کوین مقدار کمی کارمزد تراکنش پرداخت خواهد شد.

۲-۳ چرا بیت کوین‌ها باارزش هستند؟

بیت کوین‌ها ارزشمندند چون به‌عنوان شکلی از پول، مفید هستند. بیت کوین ویژگی‌ها پولی دارد (پایداری، قابلیت حمل‌ونقل، تعویض‌پذیری، کمیابی، بخش‌پذیری و شناخت پذیری). ویژگی‌ها بیت کوین بر مبنای خواص ریاضی استوارشده 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 می‌کند. با این ویژگی‌ها، تمام آنچه برای شکلی از پول بودن و ارزش داشتن لازم است، اعتماد و پذیرش است. در مورد بیت کوین، رشد کاربران، سوداگران و کسب‌وکارهای نوپا، گویای مطلب است؛ مانند تمامی ارزها، بیت کوین ارزش خود را تنها و به‌طور مستقیم از کسانی می‌گیرد که آن را برای پرداخت وجه پذیرفته‌اند.

۳-۳ چه چیزی بهای بیت کوین را تعیین می‌کند؟

بهای بیت کوین با قانون عرضه و تقاضا معلوم می‌شود. با افزایش تقاضا برای بیت کوین، بهای آن نیز افزایش می‌یابد و با کاهش تقاضا، از بهای آن کاسته می‌شود. تعداد بیت کوین‌های در گردش محدود است و بیت کوین‌های جدید با نرخی کاهنده و قابل پیش‌بینی تولید می‌شوند که به این معنی است که تقاضا باید تابعی از این سطح تورم باشد تا بتواند قیمت را ثابت نگه دارد. 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 درنتیجه قیمت بیت کوین هنوز بسیار متغیر است.



۳-۴ آیا بیت کوین می‌تواند ارزش خود را از دست دهد؟

بله. تاریخ پر است از ارزهایی که ورشکست شدند و دیگر استفاده‌ای از آن‌ها نمی‌شود. مثلاً مارک آلمان در دوران جمهوری ویمار و اخیراً نیز دلار زیمبابوه. اگرچه که شکست ارزهای قبلی معمولاً به دلیل تورم زیاد بود که غیرممکن است برای بیت کوین اتفاق بیفتد، ولی همواره احتمال شکست‌های فنی، ارزهای رقیب، مسائل سیاسی و جز آن وجود دارد. یک قاعده سرانگشتی ساده می‌گوید که هیچ ارزی را نباید مطلقاً ایمن از ورشکستگی یا شرایط دشوار دانست. بیت کوین در طی سال‌ها پس از آغاز به کارش، ثابت کرده که قابل‌اعتماد است و پتانسیل زیادی برای رشد دارد؛ اما هیچ‌کس در آن موقعیت نیست که بتواند آینده بیت کوین را پیش‌بینی کند.

۳-۵ آیا بیت کوین حبابی است؟

این افزایش سریع قیمت نیست که حباب ایجاد می‌کند، بلکه ارزش بیش‌ازحد گذاردن به‌صورت مصنوعی است که موجب تصحیح ناگهانی رو به پایین شده و به تشکیل حباب می‌انجامد. هرگاه صدها هزاران نفر از مشارکت‌کنندگان در بازار، انتخاب‌هایی بر مبنای عملکرد فردی داشته باشند باعث می‌شود که قیمت بیت کوین‌ها زمانی که قیمت بازار درحال‌توسعه تعیین شدن است، نوسان کند.

دلیل تغییرات احساسی می‌تواند:

- 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 سوداگرانِ می‌شود،
- ترس از عدم قطعیت و شور و شوق غیرمنطقی خارج از عرف روز و حرص و طمع باشد.

۳-۶ آیا بیت کوین، ترفند پونزی است؟

ترفند پونزی یک عملیات سرمایه‌گذاری کلاه‌برداران است که به سرمایه‌گذاران بجای آنکه از محل سود حاصل از کسب‌وکار بهره پرداخت شود، از پول خود آن‌ها یا از پولی که توسط سرمایه‌گذاران بعدی فراهم می‌شود، سود پرداخت می‌کند. ترفند پونزی به‌گونه‌ای طراحی‌شده است که چنانچه اگر مشارکت‌کنندگان جدید به تعداد کافی وجود نداشته باشد، با ضرر زیان آخرین سرمایه‌گذاران خود، فرو خواهد پاشید.

بیت کوین یک پروژه نرم‌افزاری رایگان بدون هیچ‌گونه مرجعیت مرکزی است. درنتیجه، هیچ‌کس در موقعیتی نخواهد بود که بتواند در مورد بازگشت سرمایه‌گذاری، نمایندگی‌های جعلی بسازد. درست مانند دیگر ارزهای اصلی دیگر مثل طلا، دلار امریکا، یورو، ین و غیره، هیچ قدرت خریدی تضمین‌شده‌ای وجود ندارد و نرخ مبادله آزادانه شناور است. این به حالت ناپایداری خواهد انجامید که در آن صاحبان بیت کوین‌ها می‌توانند به‌طور غیرمنتظره‌ای پول به دست آورده و یا از دست بدهند. گذشته از گمانه‌زنی‌ها، بیت کوین همچنین یک سیستم پرداخت با ویژگی‌ها مفید و رقابتی است که هزاران کاربر و کسب‌وکار از آن استفاده می‌کنند.

۳-۷ آیا بیت کوین به پیشگامان خود بهره ناعادلانه‌ای نمی‌دهد؟

بعضی از پیشگامان تعداد زیادی بیت کوین داشتند چون خطر کرده و زمان و منابع را در یک فنّاوری محقق نشده‌ای که دیگران بندرت از آن استفاده می‌کردند و برقراری مناسب امنیت آن به‌مراتب سخت‌تر بود، سرمایه‌گذاری 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 یابد. کاملاً شبیه به سرمایه‌گذاری در یک کسب‌وکار نوپاست که هم می‌تواند به‌واسطه مفید و مردم‌پسند 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 طراحی‌شده است. به‌سختی می‌توان تصور کرد که چگونه می‌توانست نسبت به پیشگامان خود کمتر جانب‌داری کند و کاربران امروز آن شاید فردا، پیشگامان اولیه بیت کوین محسوب شوند و شاید هم نه.

۳-۸ آیا متناهی بودن تعداد بیت کوین‌ها، یک محدودیت نخواهد بود؟

بیت کوین ازاین‌جهت که فقط تا ۲۱ میلیون عدد از آن ساخته خواهد شد، منحصربه‌فرد است؛ اما این هرگز یک محدودیت بشمار نمی‌آید، چون بیت کوین‌ها می‌توانند 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 می‌توانند تا ۸ رقم اعشار (۰,۰۰۰۰۰۰۰۱ بیت کوین) و به‌طور بالقوه حتی واحدهای کوچک‌تر، تقسیم گردند.

۳-۹ آیا بیت کوین در مارپیچ تورم‌زدایی سقوط نخواهد کرد؟

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

هرچند این نظریه، در میان بانکداران مرکزی راهی مردم‌پسند برای توجیه تورم است ولی به نظر نمی‌رسد که همیشه درست باشد و در میان اقتصاددانان مورد مناقشه بوده است. لوازم الکترونیکی مصرفی، مثالی از یک بازار است که قیمت‌های آن دائماً در حال کاهش بوده ولی دچار رکود نمی‌شود. به همین شکل، ارزش بیت کوین‌ها در طول زمان افزایش‌یافته و اندازه اقتصاد بیت کوینی هنوز هم پا به‌پای آن بشدت در حال رشد است. به دلیل آنکه، هم ارزش ارز و هم‌اندازه اقتصاد آن در سال ۲۰۰۹، از صفر شروع‌شده است؛ بیت کوین یک مثال نقض برای این نظریه است که نشان می‌دهد گاهی این نظریه باید نادرست باشد.

باوجوداین، بیت کوین طراحی نشده است که یک ارز ضد تورمی باشد. دقیق‌تر آن است 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 بی‌دقتی گم‌کرده و بک آپ یا پشتیبان هم تهیه نکرده باشند. اگر زیرساخت‌های پولی ثابت و اقتصاد پایدار باشد، ارزش ارز باید همیشه یکسان باقی بماند.

۳-۱۰ آیا سفته‌بازی و نوسانات، مشکلی برای بیت کوین ایجاد نمی‌کنند؟

این همان مسئله مرغ و تخم‌مرغ است. یک اقتصاد با مقیاس بزرگ برای تثبیت قیمت بیت کوین، باید کاربران و کسب‌وکارهای بیشتری را توسعه دهد. برای توسعه یافتن یک اقتصاد به‌اندازه‌ای بزرگ‌تر، کاربران و کسب‌وکارها در پی ثبات قیمت‌ها خواهند بود. خوشبختانه نوسانات بر مزایای اصلی بیت کوین به‌عنوان یک سیستم پرداخت وجه که پولی را از نقطه الف به نقطه ب می‌رساند، تأثیری ندارد. برای کسب‌وکارها امکان‌پذیر است که پرداخت‌های بیت کوینی را فوراً به ارز محلی خود تبدیل کنند و این کار به آن‌ها اجازه می‌دهد تا از مزایای بیت کوین بدون اینکه مشمول نوسانات قیمت شوند، استفاده کنند. بسیاری از کاربران بیت کوین را به خاطر امکانات و ویژگی‌های منحصربه‌فرد و مفید آن برگزیده‌اند. با چنین راهکارها و مشوق‌هایی، امکان رشد و بلوغ بیت کوین و توسعه آن تا مرحله‌ای که نوسانات قیمت در آن محدود گردد، وجود دارد.

۳-۱۱ چه اتفاقی میافتد اگر کسی همه بیت کوین‌های موجود را یکجا بخرد؟

تنها کسری از بیت کوین‌هایی که تاکنون صادرشده، در بازار مبادلات برای فروش گذاشته‌شده‌اند. 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 دهه‌ی 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 آسیب‌پذیر 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 تاکنون یک دارایی نوسان دار باقی‌مانده است.

۱۲-۳ اگر کسی ارز دیجیتال بهتری ساخت چه؟

چنین اتفاقی ممکن است بیافتد. بیت کوین، تاکنون به میزان قابل‌ملاحظه‌ای، مردم‌پسندترین ارز مجازی تمرکززدایی شده است، اما نمی‌توان تضمین کرد که در آینده هم این موقعیت را حفظ کند. هم‌اکنون تعدادی ارزهای دیگر هم هستند که از بیت کوین الهام گرفته‌اند ولی احتمالاً درست است تصور کنیم که یک ارز جدید باید بسیار بهبود یابد تا بتواند به لحاظ داشتن بازارهای باثبات، بر بیت کوین پیشی بگیرد حتی اگر این امر غیرقابل‌پیش‌بینی باقی بماند. تا زمانی که بخش‌های اساسی پروتکل تغییر نکند، بیت کوین می‌تواند اصلاحات و بهبودهای یک ارز رقابتی را داشته باشد.

۱۳-۳ نحوه تراکنش‌ها چگونه است؟

دریافت یک وجه پرداختی با بیت کوین، تقریباً آنی است؛ اما به‌طور متوسط یک تأخیر ۱۰ دقیقه‌ای لازم است تا شبکه بتواند با ضمیمه کردن آن تراکنش به یک بلاک، تائید آن‌ها شروع کرده تا بیت کوین‌های رسیده به شما، قابل‌خرج کردن شوند. تائید به معنای آن است که شبکه به توافق رسیده است که بیت کوین‌هایی که دریافت کرده‌اید برای شخص دیگری فرستاده نشده بوده و جزئی از اموال شماست. وقتی تراکنش شما به یک بلاک پیوست شد، در زیر بلاک‌هایی که بعدازآن می‌آیند و به‌طور نمایی این توافق را یکپارچه کرده و خطر برگشت خوردن تراکنش را کاهش می‌دهند، دفن می‌شود. هر کاربری آزاد است تا تعداد تأییدیه‌های تراکنش را خود تعیین کند، اما اغلب ۶ تأییدیه به‌قدر همان ۶ ماه صبر کردن برای تراکنش یک کارت اعتباری، ایمن به نظر می‌رسد.

۱۴-۳ کارمزد یک تراکنش چقدر خواهد بود؟

بیشتر تراکنش‌ها بدون کارمزد قابل‌پردازش هستند، اما اغلب کاربران را تشویق می‌کنند که داوطلبانه اندکی کارمزد هم پرداخت کنند تا تراکنش‌هایشان سریع‌تر تائید شود و نیز دستمزدی هم به استخراج‌کنندگان داده شود. اگر کارمزدی هم درخواست شود، معمولاً بیش از چند سنت نخواهد بود. چنانچه لازم باشد، کلاینت بیت کوینی شما معمولاً خواهد کوشید تا مقدار کارمزد مناسبی را برآورد کند.

کارمزد تراکنش، نوعی حفاظت است در برابر کاربرانی که با ارسال تراکنش‌هایشان شبکه را اور لود می‌کنند. نحوه دقیق عملکرد کارمزد هنوز درحال‌توسعه بوده و باگذشت زمان تغییر می‌کند. چون کارمزد به مقدار بیت کوین ارسالی مربوط نمی‌شود، ممکن است خیلی کم (۰,۰۰۰۵ بیت کوین برای یک انتقال 1000بیت کوینی) و یا به‌طور ناعادلانه‌ای زیاد (۰,۰۰۴ بیت کوین برای یک پرداخت ۰,۰۲ بیت کوینی) به نظر آید. مبلغ کارمزد، با خصوصیاتی چون داده‌ی تراکنش و تکرار تراکنش، تعریف می‌شود. مثلاً اگر شما به‌دفعات زیاد، مبالغ کمی را دریافت کنید، آنگاه کارمزد ارسال بیشتر خواهد بود. چنین پرداخت‌هایی را می‌توان مقایسه کرد بازمانی که بخواهید صورتحساب

رستوران را با سنت بپردازید. خرج کردن سریع مقادیر کمی از بیت کوین‌هایتان نیز می‌تواند مشمول کارمزد شود. اگر فعالیت شما تابع الگوی تراکنش‌های عادی باشد، مبلغ کارمزد بسیار کم خواهد بود.

۳-۱۵ 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 راه‌اندازی می‌کنید، بیت کوین‌ها ظاهر خواهند شد. درواقع، این نرم‌افزار روی کامپیوتر شما نیست که بیت کوین‌ها را دریافت می‌کند، بلکه آن‌ها در یک دفتر کل عمومی که بین تمام دستگاه‌های روی شبکه به اشتراک گذاشته‌شده است، ضمیمه می‌شوند. اگر هنگامی‌که برنامه کلاینت کیف پول شما در حال اجرا نیست، بیت کوینی برایتان بفرستند، دفعه بعدی که شما برنامه را راه‌اندازی کنید، برنامه بلاک‌ها را دانلود کرده و در جریان تراکنش‌هایی که تا حالا از آن‌ها بی‌خبر بوده‌اید، قرار خواهید گرفت و سرانجام بیت کوین‌ها ظاهر می‌شوند، انگار که همین‌الان رسیده باشند. کیف پول فقط وقتی لازم است که بخواهید بیت کوین‌ها را خرج کنید.

۳-۱۶ هم‌زمان‌سازی به چه معناست و چرا این‌قدر طول می‌کشد؟

هم‌زمان‌سازی طولانی فقط برای کلاینت‌های فول نُدی مانند هسته بیت کوین، الزامی است. به لحاظ فنی، هم‌زمان‌سازی، فرایند دانلود کردن و درستی آزمایی تراکنش‌های بیت کوینی پیشین روی شبکه است. برای اینکه بعضی کلاینت‌های بیت کوین، بتوانند تراز قابل‌خرج کردنِ کیف پول بیت کوینی شما را محاسبه کرده و تراکنش‌های جدید بسازند، لازم است که از تمام تراکنش‌های پیشین آگاه باشند .این گام می‌تواند منابع زیادی طلب کند و نیاز به پهنای باند و فضای ذخیره‌سازی کافی دارد تا یک زنجیره بلاک با اندازه کامل را بسازد. برای حفظ امنیت بیت کوین‌ها به‌اندازه کافی، مردم باید همچنان از کلاینت‌های فول نُد استفاده کنند چراکه این کلاینت‌ها درستی آزمایی و تقویت تراکنش‌ها را انجام می‌دهند.

۴- استخراج

۴-۱ استخراج بیت کوین یعنی چه؟

استخراج، فرایند صرف توان محاسبه برای پردازش تراکنش‌ها، ایمن‌سازی شبکه و هم‌زمان نگه‌داشتن همه باهم در سیستم است. می‌توان آن‌ها به‌منزله مرکز داده‌های بیت کوین تصور کرد؛ به‌جز آنکه طوری طراحی‌شده است که برای استخراج‌کنندگانی که در تمام کشورها در حال کارند، کاملاً تمرکززدایی شده باشد و هیچ‌کسی کنترلی بر شبکه نداشته باشد. به این فرایند در قیاس با استخراج طلا، استخراج می‌گویند چون مکانیسم گذرایی دارد که با آن بیت کوین‌های جدید صادر می‌شوند؛ اما برخلاف استخراج طلا، استخراج بیت کوین درازای سرویس‌های مفیدی که برای عملکرد یک شبکه پرداخت امن لازم است، جایزه‌ای هم در نظر می‌گیرد. تا وقتی آخرین بیت کوین صادر نشده باشد، استخراج بیت کوین همچنان الزامی است.

۴-۲ استخراج بیت کوین به چه صورت است؟

هرکسی می‌تواند با اجرای نرم‌افزار روی سخت‌افزاری ویژه، یک استخراج‌کننده بیت کوین باشد. نرم‌افزار استخراج، به انتشار تراکنش‌ها در شبکه‌ی P2P، گوش فراداده و اقدامات مقتضی جهت پردازش و تائید این تراکنش‌ها را انجام می‌دهد. استخراج‌کنندگان بیت کوین به این دلیل به این کار می‌پردازند که کارمزد تراکنشی را که کاربران برای پردازش سریع‌تر تراکنش‌های خود می‌پردازند، دریافت نموده و نیز بیت کوین‌های تازه تولیدشده 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 مدرک‌ها را به‌سختی می‌توان تولید کرد، چون هیچ راهی برای تولید آن‌ها نیست، مگر میلیاردها بار محاسبه در ثانیه .استخراج‌کنندگان باید این محاسبات را انجام دهند تا سرانجام شبکه، بلاک‌های آن‌ها را بپذیرد و به آن‌ها پاداش دهد. هر چه تعداد استخراج‌کنندگان بیشتر شود، شبکه یافتن بلاک‌های مجاز را به‌طور خودکار دشوارتر می‌کند تا مطمئن شود که زمان متوسط برای یافتن یک بلاک، همان ۱۰ دقیقه باقی خواهد ماند. درنتیجه، استخراج یک کار بسیار رقابتی است که هیچ استخراج‌کننده‌ای نمی‌تواند کنترلی بر آنچه درون زنجیره بلاک است، داشته باشد.

برای تحمیل ترتیب زمانی بر زنجیره بلاک، سند انجام کار طوری طراحی می‌شود که به بلاک قبلی وابسته باشد. به همین دلیل برگشت دادن تراکنش‌های قبلی به‌طور نمایی دشوار می‌شود چراکه لازم است سند انجام کار روی تمامی بلاک‌های دنباله آن، دوباره محاسبه گردند. اگر در یک‌زمان، دو بلاک پیدا شود استخراج‌کنندگان ابتدا به کار روی بلاکی که اول دریافت می‌پردازند و سپس به‌محض آنکه بلاک بعدی پیدا شد به طولانی‌ترین زنجیره بلاک‌ها سوییچ خواهند کرد. به‌این‌ترتیب به استخراج‌کنندگان اجازه داده خواهد شد که اجماعی جهانی را بر مبنای قدرت پردازش، حفظ کرده و آن‌ها ایمن نمایند.

استخراج‌کنندگان بیت کوین نه می‌توانند با تقلب کردن پاداش خود را افزایش دهند و نه می‌توانند تراکنش‌های تقلبی را که ممکن است شبکه بیت کوین را خراب کند، پردازش نمایند، چون تمامی نُدهای بیت کوینی بر اساس پروتکل بیت کوین، هرگونه بلاکی را که شامل داده‌های غیرمجاز باشد، نخواهند پذیرفت. درنتیجه، حتی اگر نتوان به‌تمامی استخراج‌کنندگان بیت کوین اعتماد کرد، امنیت شبکه همچنان برقرار خواهد بود.

۴-۳ آیا استخراج بیت کوین، اتلاف انرژی نیست؟

بندرت می‌توان 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 هزینه‌های پردازش است. سرویس‌های لازم برای عملکرد دستگاه‌های پولی گسترده کنونی، مانند بانک‌ها، کارت‌های اعتباری و نیز خودروهای زرهی نیز انرژی زیادی مصرف می‌کنند. هرچند که برخلاف بیت کوین، مصرف کل انرژی آن‌ها شفاف نیست و نمی‌توان به‌راحتی آن را اندازه‌گیری کرد.

استخراج بیت کوین به‌گونه‌ای طراحی‌شده که در طول زمان بهینه‌تر شده و سخت‌افزارهایی خاصی را استفاده کند که انرژی کمتری مصرف می‌کنند و هزینه‌های استخراج به‌تدریج با تقاضا متناسب گردد. هر زمان که استخراج بیت کوین کمتر رقابتی شده و نیز سودآوری کمتری داشته باشد، بعضی از استخراج‌کنندگان دست از فعالیت خواهند کشید. افزون بر این، تمام آن انرژی که صرف استخراج می‌شود، در پایان به گرما تبدیل خواهد شد و بیشتر استخراج‌کنندگانی که سود می‌کنند از این گرما استفاده خوبی خواهند کرد. یک شبکه که کارایی آن بهینه‌سازی شده، شبکه ایست که عملاً هیچ‌گونه انرژی اضافی مصرف نمی‌کند. هرچند که این‌یک ایده آل است، اقتصاد استخراج به گونه ایست که هر استخراج‌کننده‌ای تلاش می‌کند به آن دست یابد.

۴-۴ چگونه استخراج به امنیت بیت کوین کمک می‌کند؟

استخراج چیزی شبیه به یک بخت‌آزمایی رقابتی ایجاد کرده و کار را برای کسانی که می‌خواهند به‌طور پی‌درپی بلاک‌های تراکنشی جدیدی به زنجیره بلاک بیفزایند، دشوار کرده است. به‌این‌ترتیب از اینکه هرکسی بتواند قدرت بلاک کردن تراکنش‌های خاصی را به دست بیاورد، جلوگیری کرده و از بی‌طرفی شبکه محافظت به عمل‌آورده 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 آمده‌اند، به‌طور نمایی دشوارتر ساخته است.

۴-۵ برای شروع به کار استخراج به چه چیزهایی نیاز دارم؟

در اوایل عمر بیت کوین، هرکسی می‌توانست با استفاده از CPU کامپیوترش، یک بلاک جدید پیدا کند. هر چه بر تعداد استخراج‌کنندگان افزوده شد، دشواری یافتن بلاک‌های جدید هم بشدت زیاد شد تا جایی که امروزه تنها روش استخراج مقرون‌به‌صرفه را با استفاده از سخت‌افزارهای خاص، بکار می‌گیرند.

۶- امنیت

۶-۱ آیا بیت کوین امن است؟

فنّاوری بیت کوین- پروتکل آن و رمزنگاری- سابقه ردیابی امنیتی قوی دارد و شبکه بیت کوین احتمالاً بزرگ‌ترین پروژه محاسباتی توزیع‌شده در جهان است .بیشترین آسیب‌پذیری بیت کوین ناشی از خطای کاربر است. ممکن است فایل‌های کیف پول بیت کوینی که کلیدهای محرمانه لازم را ذخیره می‌کند، به‌طور تصادفی حذف، گم و یا دزدیده شوند، درست مانند آنکه پول نقد واقعی، به شکل دیجیتال ذخیره‌شده باشد. خوشبختانه کاربران می‌توانند اقدامات امنیتی مطمئنی را بکار بندند تا از پول خود محافظت کنند یا از آن دسته از تأمین‌کنندگان خدمات که سطوح امنیتی خوب و نیز بیمه علیه دزدی یا گم‌شدن ارائه می‌کنند، استفاده نمایند.

۶-۲ آیا بیت کوین تاکنون هک نشده است؟

سال‌ها پس از پیدایش بیت کوین، هنوز قوانین پروتکل و رمزنگاری که در آن استفاده‌شده، معتبر است و این نشانه خوبی است از اینکه مفهوم آن به‌خوبی طراحی‌شده است؛ اما در طول زمان نقایص امنیتی در پیاده‌سازی نرم‌افزارهای مختلف، یافته و برطرف شده است. امنیت نرم‌افزار بیت کوین همانند نرم‌افزارهای دیگر، به‌سرعت پیدا شدن عیب‌ها و رفع آن‌ها بستگی دارد. هر چه این موارد بیشتر کشف شوند، بیت کوین بلوغ بیشتری به دست خواهد آورد.

بین دزدی و رخنه‌های امنیتی که در کسب‌وکارها و مبادلات مختلف رخ می‌دهد، اغلب سوءتفاهم‌هایی وجود دارد. هرچند هردوی 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 آن است که بگوییم مجموعه کاملی از اقدامات خوب و راه‌حل‌های امنیتی شهودی لازم است تا از پول کاربران محافظت بهتری به عمل 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 سخت‌افزاری و تراکنش‌های چند امضایی، به‌سرعت توسعه‌یافته‌اند.

۶-۳ آیا کاربران می‌توانند علیه بیت کوین توطئه کنند؟

تغییر دادن پروتکل بیت کوین به این آسانی‌ها ممکن نیست. هر مشتری بیت کوینی که از همان قوانین یکسان پیروی نکند نمی‌تواند 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 نشده‌ای از بیت کوین‌ها را به‌یک‌باره تولید کرد، دارایی کاربران دیگر را خرج نمود، شبکه را برای همیشه از کار انداخت و یا کارهایی ازاین‌دست انجام داد.

اما به‌هرحال، بیشتر استخراج‌کنندگان می‌توانند تراکنش‌های اخیر را به‌دلخواه بلاک کرده و یا برگشت دهند. بسیاری از کاربران نیز می‌توانند برای اعمال و پذیرش بعضی تغییرات، فشار وارد کنند. چون بیت کوین فقط زمانی به‌درستی کار می‌کند که بین تمامی کاربران اجماع کامل حاصل‌شده باشد، بنابراین تغییر دادن پروتکل می‌تواند بسیار دشوار باشد و لازم است اکثریت قریب به‌اتفاق کاربران این تغییرات را بپذیرند به‌گونه‌ای که بقیه کاربران تقریباً هیچ انتخابی جز پیروی از اکثریت را نداشته باشند. به‌عنوان یک قاعده کلی، به‌سختی می‌توان تصور کرد که چرا یک کاربر بیت کوین باید تغییری را بپذیرد که ممکن است پول او را به خطر بیندازد.

۷-۳ آیا بیت کوین نسبت به محاسبات کوانتمی آسیب‌پذیر است؟

بله. به‌طورکلی بیشتر دستگاه‌های متکی بر رمزنگاری، دستگاه‌های بانکی هستند؛ اما هنوز کامپیوترهای کوانتمی حتی وجود ندارند و گمان نمی‌رود که تا چند صباحی در آینده هم پا به عرصه وجود گذارند. برفرض که کامپیوترهای کوانتمی را بتوان تهدیدی قریب‌الوقوع برای بیت

کوین بشمار آورد، می‌توان پروتکل را طوری ارتقا داد که از الگوریتم‌های پسا-کوانتومی استفاده کند. با توجه به اهمیت این به‌روزرسانی، می‌توان با خیال راحت انتظار داشت که توسعه‌دهندگان پروتکل را به‌دقت بازبینی کرده و تمامی کاربران بیت کوین آن‌ها بپذیرند.