21 میلیون سکه مجازی

اگر حتی یک مورد از ویژگی‌های سیستم بانکی و مالی کنونی (به ویژه در سطح بین‌المللی) شما را ناخشنود می‌کند، شاید از خودتان پرسیده باشید که فناوری‌های وب چه راه‌کاری برای بهبود سیستم کنونی پیش‌رو می‌نهند. اما وب و ابزارهای آن برای بانک‌داران ناآشنا نیستند. پس شاید وب نمی‌تواند راه‌کار بهبود نارسایی‌های کنونی باشد، زیرا هم‌اکنون بانک‌ها به گستردگی از فناوری‌های وب استفاده می‌کنند. یا شاید هم راه‌کارهایی که وب برای بهبود اساسی وضع موجود ارائه می‌کند، به‌طور گزینشی برگرفته شده‌اند. اگرچه راه‌کاری که بیت‌کوین (bitcoin) پیش‌رو می‌نهد، جایگزین سیستم مالی کنونی است، به‌سادگی بهبوددهنده آن نیست، زیرا هنوز در سال‌های آغازین خود است و ناچار به هم‌زیستی با سیستم سنتی است.

این مطلب یکی از مقالات پرونده ویژه «**بیت‌کوین**» است. برای دانلود کل پرونده ویژه اینجا کلیک کنید.

شاید بیت‌کوین موفق شود خود را جایگزین سیستم کنونی کند، شاید هم (مانند بسیاری از پروژه‌های هیجان‌انگیز دیگر) به تاریخ وب بپیوندد. اما ایده‌هایی که بیت‌کوین براساس آن‌ها بنا شده است و ابزارهایی را که بر پایه آن ایده‌ها ارائه می‌کند، به احتمال بسیار، آمده‌اند تا بمانند. مجموع توان پردازشی کامپیوترهایی که روی گره‌های شبکه بیت‌کوین به نگه‌داری حساب‌ها مشغول هستند، بیش از هشت برابر مجموع توان پردازشی 500 ابررایانه برتر جهان است. این حجم فزاینده سرمایه‌گزاری و نیز شمار استارت‌آپ‌هایی که بیت‌کوین را موضوع کسب‌وکارشان قرار داده‌اند، می‌تواند یادآور حباب دات‌کام باشد یا می‌تواند مقدمه‌ای باشد بر آینده پول. بیت‌کوین یکی دیگر از زاده‌های وب است؛ وب نیازهایی را برای ما اختراع می‌کند که پیش‌تر از این وجود نداشتند و در همان حال ابزارهایی را دراختیارمان می‌گذارد که با آن‌ها می‌توانیم راه‌حل‌های تازه‌ای برای نیازهای تازه و کهنه‌مان بسازیم. پیش از نگاه به چیستی بیت‌کوین، خوب است به چرایی آن بنگریم؛ انگیزه‌های پیدایش بیت‌کوین و سیستم‌های مشابه آن چه بوده‌اند؟

برخی ایرادهای سیستم مالی کنونی

سیستم پولی و مالی کنونی اگرچه یکی از بزرگ‌ترین مصرف‌کنندگان وب است، در ذات خود از دوران وب بسیار پیش مانده است. کافی است یک بار خواسته باشید مقدار نه‌چندان زیادی پول را از حساب‌تان در یک کشور به کشوری دیگر منتقل کنید تا بدانید این کار برای شهروندان عادی چه اندازه دشوار و گران‌قیمت است.

تحریم‌های مالی بر ضد کشورمان یکی از بهانه‌های همیشگی بانک‌های بین‌المللی برای کارشکنی در امور مالی شهروندان ایرانی است، اما ملیت‌های دیگری هستند که در این وضعیت با ما شریک‌اند. هر قدر کشور مبدا یا مقصد تراکنش مالی، وضع مالی یا بین‌المللی بدتری داشته باشد، شهروندانش برای خدمات مالی با دشواری بیش‌تری روبه‌رو هستند و درصد بالاتری از مبلغ‌های تراکنش را نیز باید به مؤسسه‌های مالی و بانکی بپردازند. تبدیل میان واحدهای پولی گوناگون نیز مشکلی است که در مرحله بعدی پدیدار می‌شود و مبلغی دیگر از دارایی در حال انتقال صرف کارمزد تبدیل ارز می‌شود.

این وضعیت به هم‌سانی روی وب شباهتی ندارد؛ سطح دسترسی به فناوری‌های مختلف روی وب (گذشته از سرعت اینترنت و مسائل مربوط به همان تحریم‌ها) به مکانی که از آن‌جا به وب دسترسی می‌یابید، بستگی ندارد.

ایمیلی که (برای نمونه) از حساب جیمیل‌تان می‌فرستید، مشمول همان محدودیت‌هایی (مثلاً درباره اندازه فایل‌های ضمیمه) است که یک کاربر در کشور دیگر دارد و تقریباً با سرعت یکسانی هم فرستاده و دریافت می‌شود. این که ایمیل شما به چه زبانی نوشته شده باشد یا طول چه اندازه باشد هم تأثیر چندانی بر سرعت ارسال و دریافت آن ندارد.
اگرچه فناوری‌های وب بسیاری از هزینه‌های سنتی مؤسسه‌های مالی را کاهش داده یا حتی حذف کرده‌اند و سرعت عملیات آن‌ها را بالا برده‌اند، مشتریان عادی خدمات مالی این تغییرها را، دست‌کم در سطح بین‌المللی، چندان حس نمی‌کنند. انتقال پول میان دو کشور بین دو حساب الکترونیکی، ممکن است چند روز طول بکشد و حتی ممکن است میزان کارمزد تراکنش به‌طور دقیق پیش از ارائه خدمات به مشتریان اعلام نشود. گذشته از این‌ها، ناچارید به مؤسسه مالی خود اعتماد کنید و اگر آن‌ها تصمیم بگیرند که برای نمونه، تراکنش‌های شما را مشکوک اعلام کنند و حساب‌تان را ببندند یا دارایی‌تان را مصادره کنند، متوجه خواهید شد که اطلاعات مالی شما کاملاً هم پیش بانک محفوظ نیست.

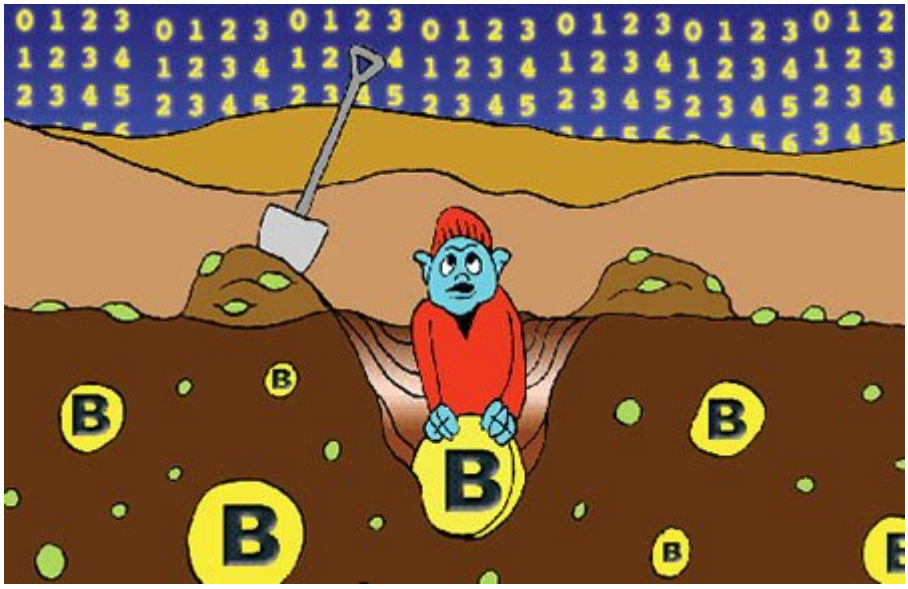
سیستم بانکی هنوز همان سرشت متمرکزی را دارد که در فیلم‌های وسترن دیده‌ایم؛ یک نهاد متمرکز، ثروت بسیاری را انباشته و توزیع و گردش آن را کنترل می‌کند و برای ایمن شدن مخزن‌های پول، اسناد و اشیا پر ارزش، تنها می‌توان لایه‌های امنیتی فزاینده‌ای به دور آن‌ها ایجاد کرد

همین مؤسسه‌های مالی و بانکی، هنگامی که در کشورهایی مانند امریکا یا ایسلند با سیاست‌های نادرست موجب بحران مالی می‌شوند، چنان قدرت و نفوذی دارند که دولت مرکزی تنها می‌تواند برای نجات دادن آنان (و نه مجازات کردن‌شان) بکوشد، مثلاً با تزریق نقدینگی به بازار یا حتی به‌طورمستقیم به بانک‌های خصوصی، که نتیجه آن کاهش ارزش دارایی‌های مالی همه مردم است. این وضعیت نه با دوران وب هم‌خوانی دارد و نه با اصول دموکراسی. نه اطلاعات شخصی شما پیش بانک‌ها محفوظ است و نه ارزش دارایی‌تان. هرگونه خرابی احتمالی در سیستم بانک نیز می‌تواند اطلاعات شما را در معرض خطر قرار دهد.
سیستم بانکی هنوز همان سرشت متمرکزی را دارد که در فیلم‌های وسترن دیده‌ایم؛ یک نهاد متمرکز، ثروت بسیاری را انباشته و توزیع و گردش آن را کنترل می‌کند و برای ایمن شدن مخزن‌های پول، اسناد و اشیا پر ارزش، تنها

می‌توان لایه‌های امنیتی فزاینده‌ای به دور آن‌ها ایجاد کرد که دسترسی کاربران مشروع و صاحبان قانونی به آن دارایی‌ها را نیز دشوار می‌کند. اگر برای این سیستم جانشینی بخواهیم، باید بدترین ویژگی‌های آن را نداشته باشد، سیستم تازه باید نامتمرکز باشد، چه در انباشت دارایی‌ها و اطلاعات مشتریان و چه در قدرت تصمیم‌گیری.

ایجاد واحد پول و گردش مالی در سیستم بیت‌کوین

بیت‌کوین یک واحد پولی مجازی، نامتمرکز و رمزنگاشته است. در حالی‌که واحدهای پول واقعی را داریم، چرا باید به یک واحد پول مجازی اهمیت بدهیم یا ارزش مالی برای آن در نظر بگیریم؟ نیرومندترین واحد پولی جهان، دلار امریکا است. چه چیزی دلار را واقعی می‌کند و بیت‌کوین را مجازی؟ قوانین مالی دولت امریکا. این موضوع با جزئیات متفاوت، درباره همه واحدهای پولی عمده درست است. واقعی بودن یک واحد پول، بیش‌تر یک مفهوم تاریخی است که وابستگی آن واحد پول به مجموعه سیستم دولتی و قوانین یک کشور را نشان می‌دهد. قوانین، مجموعه قراردادهای اجتماعی هستند. بنابراین، مجموعه‌ای از قراردادهای میان کاربران وب نیز می‌توانند در عمل شکل قانون بیابند، اگرچه پیدا است که ملاحظه‌های بسیاری در این میان وجود دارد که در این‌جا نمی‌توان به آن‌ها پرداخت. همانند قوانین ملی و بین‌المللی، پشتوانه‌هایی لازم است که اجرایی شدن هر مجموعه قانون را تضمین کند. پس اگر مجموعه‌ای منطقی از قوانین برای سیستم بیت‌کوین وجود داشته باشد و پشتوانه‌هایی برای ضمانت اجرایی آن قانون‌ها، می‌توان یک شرط لازم برای اعتبار یافتن بیت‌کوین را برآورد. شرط مهم دیگر، آن است که مجموعه به نسبت بزرگی از سودگران و مصرف‌کنندگان از این سیستم استفاده کنند؛ بازی‌گرانی که براساس آن قوانین بازی کنند.



مبنای کار بیت‌کوین، یک دفتر حساب همگانی است که ریز تمام تراکنش‌ها، از آغاز بیت‌کوین در سال 2009 تاکنون، در آن ثبت شده است و پیوسته نیز تراکنش‌های تازه به آن افزوده می‌شوند. افزودن تراکنش‌ها به این دفتر حساب (ledger) یک‌به‌یک انجام نمی‌شود، بلکه هر ده دقیقه یک بار، مجموعه تراکنش‌های تازه در قالب یک بلوک به این دفتر افزوده می‌شود. این دفتر حساب یک فایل نه چندان بزرگ (حدود 18 گیگابایت در حال حاضر) است که همه کاربران سیستم بیت‌کوین می‌توانند آن را داشته باشند. بیت‌کوین در ضمن یک سیستم peer to peer یا به اختصار P2P است. گره‌های این شبکه، کامپیوترهایی هستند که به اعتبارسنجی و ثبت تراکنش‌های تازه می‌پردازند و مجموعه تراکنش‌های تازه را در قالب بلوک‌های تازه به دفتر حساب می‌افزایند.

مبنای کار بیت‌کوین، یک دفتر حساب همگانی است که ریز تمام تراکنش‌ها، از آغاز بیت‌کوین در سال 2009 تاکنون، در آن ثبت شده است و پیوسته نیز تراکنش‌های تازه به آن افزوده می‌شوند.

کاربران بیت‌کوین از راه نرم‌افزاری که روی کامپیوتر رومیزی یا دستگاه‌های همراه خود نصب می‌کنند، تراکنش‌های خود را به انجام می‌رسانند. هر کاربر می‌تواند یک کپی کامل از دفتر حساب را داشته باشد که به او امکان سنجش اعتبار تراکنش‌های دریافتی‌اش را می‌دهد. در ضمن هر کاربر یک کیف پول (wallet) الکترونیکی دارد که حاوی

کلیدهای او است. مجموعه کلیدهای هر کاربر و سابقه تراکنش‌های صورت‌گرفته با آن کلیدها در گذشته که در دفتر حساب ثبت شده‌اند، جایگزین حساب بانکی و موجودی آن در سیستم سنتی است؛ یعنی به جای آن که یک نهاد مرکزی براساس سابقه تراکنش‌های گذشته یک کاربر بداند که موجودی حساب وی چقدر است، مجموعه این تراکنش‌ها در دسترس همه کاربران دیگر است و آن‌ها می‌توانند براساس تراکنش‌ها از موجودی حساب (دراین‌جا کلید همگانی) یکدیگر با خبر باشند. همه تراکنش‌ها در بیت‌کوین با سیستم کلید همگانی و خصوصی انجام می‌شوند. فرض کنید کاربر A می‌خواهد 0.015 واحد بیت‌کوین (حدود ده دلار امریکا، بر مبنای ارزش برابری کنونی بیت‌کوین با دلار) را به کاربر B منتقل کند. در کیف پول هر کاربر ممکن است چندین کلید موجود باشد که هر یک میزان مشخصی اعتبار بیت‌کوینی دارد و نتیجه تراکنش‌های پیشینی است که کاربر در آن‌ها بیت‌کوین دریافت کرده است. در هنگام انجام دادن تراکنش‌های تازه، کاربر از این کلیدها خرج می‌کند. اگر برای نمونه، کاربر A از دو کلید استفاده کند که یکی 0.005 و دیگری 0.012 واحد بیت‌کوین (BTC) اعتبار داشته باشند، پیغام تراکنش را با کلید خصوصی هر یک از این دو موجودی امضا می‌کند و به نام کاربر B (در واقع به نام کلید همگانی تعیین شده برای این تراکنش از سوی کاربر B) می‌فرستد. دریافت‌کننده مستقیم این پیام به‌طور معمول کاربر B نیست، بلکه گره‌های مختلف روی شبکه هستند که میان کاربر A و B قرار دارند. این پیغام، آدرس تراکنش‌هایی را در بر دارد که در ضمن آن‌ها کاربر A مبلغ‌های یادشده را دریافت کرده است و امضای آن با کلید خصوصی هر یک از آن دو موجودی ثابت می‌کند که کاربر A صاحب راستین این مبلغ‌ها است. برای سنجش اعتبار ادعای کاربر A، گره‌های شبکه به دفتر حساب مراجعه می‌کنند تا دریابند که کاربر A به راستی دریافت‌کننده آن مبلغ‌ها با کلیدهای مربوط به آن‌ها بوده است. به این شکل، برای سنجش اعتبار پرداخت‌ها نیازی به یک مؤسسه مرکزی نیست. در ضمن، همه چیزی که کاربران به یکدیگر فاش می‌کنند، کلیدهای همگانی خودشان است و نیز آدرس اینترنتی خود، که دومی به‌سادگی قابل پوشاندن است. زیرا، جمع 0.005 و 0.012 به اندازه 0.002 BTC بیش‌تر از مبلغ تراکنش است، کاربر A یک پرداخت به اندازه 0.002 BTC هم از این تراکنش به یک کلید همگانی خودش انجام می‌دهد. این اساس یک تراکنش ساده در سیستم بیت‌کوین است. کاربر دریافت‌کننده وجه، زمانی می‌تواند از دریافت آن مطمئن باشد که ثبت آن را در بلوک بعدی دفتر حساب همگانی بیابد. برای اطمینان بیش‌تر، دریافت‌کننده می‌تواند صبر کند تا چند بلوک بیش‌تر به دفتر حساب افزوده شود و ثبت تراکنش همچنان در همان بلوک یا دست‌کم در بلوک‌های بعدی باقی مانده باشد. دلیل این که ممکن است چنین چیزی رخ ندهد، در ادامه بررسی می‌شود.

مهم‌ترین مشکل برای چنین سیستمی، امکان استفاده دوباره یا چندباره از یک کلید (چند بار خرج کردن یک اعتبار مشخص) توسط کاربران متقلب است. وجود داشتن دفتر حساب همگانی در نخستین مرحله جلوی چنین تقلب‌هایی را می‌گیرد. اما امکان دیگری برای تقلب مطرح می‌شود، این که کاربری بتواند دفتر حساب همگانی را به‌گونه‌ای تغییر دهد که مبلغی را که در یک تراکنش پرداخته به خودش بازگرداند؛ یعنی درواقع تراکنش ثبت‌شده را پاک کند. چنین امکانی نیازمند آن است که این کاربر درمقایسه با نسبت به مجموع گره‌های شبکه توان محاسباتی بالاتری داشته باشد. این گره‌ها تراکنش‌های تازه را جمع‌آوری می‌کنند و با الگوریتم ویژه‌ای (تابع hash) آن‌ها را با هم ترکیب می‌کنند تا بلوک تازه دفتر حساب را با کلید hash تازه متناظر با آن بسازند. به دفتر حساب، زنجیره بلوک‌ها (block chain) نیز گفته می‌شود. زیرا، قید ویژه‌ای برای ساختن کلید hash بلوک‌های تازه وجود دارد که برای برآوردن آن تنها با آزمون و خطا می‌توان چندین بار محاسبه کلید hash را تکرار کرد، رقابت شدیدی میان گره‌های شبکه برای یافتن کلید تازه در جریان است. گره برنده، یک BTN (یک واحد کامل) بیت‌کوین پاداش دریافت می‌کند که در هنگام افزودن بلوک تازه به دفتر حساب برای آن گره صادر می‌شود، این تنها راه صدور بیت‌کوین‌های تازه و انگیزه اصلی رقابت میان گره‌های شبکه است.

برای آن که کاربری بتواند در مجموعه تراکنش‌های بلوک تازه دست ببرد، باید توان محاسباتی آن دست‌کم از نیمی از کل دیگر شبکه بالاتر باشد تا تراکنشی را که در آن پرداختی به کاربر دیگر انجام داده است گزینشی حذف کند و به جای آن تراکنشی را بنشاند که در آن موجودی همان کلیدهای پرداختی را به یک کلید همگانی متعلق به خودش پرداخته است. اما در چنین حالتی، این کاربر درخواهد یافت که با شرکت در رقابت برای یافتن کلیدهای hash تازه، درآمد بیش‌تری به دست خواهدآورد تا این که بخواهد توان محاسباتی عظیمش را در رقابت پرخطر برای تقلب صرف کند. ضمانت اجرایی قانون‌های شبکه بیت‌کوین به‌طور عمده از همین جا ناشی می‌شود که اقدام به تقلب پرهزینه‌تر از به کار گرفتن امکانات در دسترس برای شرکت در رقابت قانونی است. تا زمانی که بیش از نصف گره‌های شبکه به‌طور سازمان‌یافته خراب‌کاری نکنند، امکان دوباره خرج‌کردن موجودی‌ها بسیار کم می‌شود. اقتصاد محاسبات یکی از ارکان امنیت سیستم بیت‌کوین است.

محاسبه کلید قابل قبول (با اِعمال قید ریاضی مشخص‌شده) برای هر کلید hash تازه برای بلوک جدید، در یک

کامپیوتر عادی به‌طور متوسط سال‌ها طول می‌کشد. گره‌های شبکه معمولاً کامپیوترهای بسیار بزرگ با سخت‌افزار اختصاصی هستند و مجموعه آن‌ها به‌طور متوسط هر کلید را در ده دقیقه می‌یابند. اگر کاربر خراب‌کاری بخواهد به شیوه‌ای که گفتیم در یک بلوک دست ببرد، برای آن که مطمئن باشد تراکنش مورد نظرش پذیرفته خواهد شد، نمی‌تواند به ثبت یک بلوک اکتفا کند، بلکه باید بکوشد چند بلوک پی‌درپی را محاسبه و ثبت کند، چراکه اگر بلوک اول را گره دیگری محاسبه کرد (که تراکنش پرداخت به کاربر B را در بر دارد) و گره‌های شبکه آن بلوک را برگیرند و بلوک‌های بعدی را بر آن اساس محاسبه کنند، محاسبه یک بلوک حاوی تراکنش موذیانه کاربر A (که در آن پرداخت را به جای کاربر B به خودش انجام داده بود) بی‌اثر می‌شود، چراکه آن بلوک به دفتر حساب افزوده نخواهد شد. این جنبه مهم دیگری از سازوکار سیستم بیت‌کوین و انعطاف‌پذیری آن به ناهم‌زمانی است؛ ممکن است بیش از یک گره شبکه هم‌زمان بلوک تازه‌ای را محاسبه کنند، در این صورت این دو بلوک مختلف به احتمال مجموعه کاملاً یکسانی از تراکنش‌ها را در بر ندارند. هر دو بلوک تازه به گره‌های شبکه فرستاده می‌شوند و هر گره، نخستین بلوک تازه‌ای را که دریافت کرده است، مبنای محاسبه بلوک بعدی قرار می‌دهد، تراکنش‌های تازه‌ای که در بلوک دریافت نشده‌اند نیز برای محاسبه بلوک بعدی استفاده خواهند شد. به محض این که یک گره بتواند بلوک بعدی را حساب کند و برای بقیه بفرستد، عملاً برنده محاسبه قبلی مشخص می‌شود: بلوکی که مبنای رشته بلندتر بلوک‌ها قرار گرفته است. تأیید شدن یک بلوک به این شیوه انجام می‌شود؛ مبنا قرار گرفتن یک بلوک برای بلوک‌های بعدی به مفهوم پذیرفته شدن آن است. هر گره شبکه محاسبه بلوک بعدی را با برگرفتن بلندترین زنجیره بلوک‌ها که به دستش می‌رسد، آغاز می‌کند.

نرخ صدور سکه‌های تازه برای برنده محاسبه بلوک‌ها روند نزولی دارد، به‌گونه‌ای که در نهایت بیش از 21 میلیون بیت‌کوین صادر نخواهد شد و بخشی از همین مقدار نیز بر اثر از دست رفتن کلیدهای متناظر با آن‌ها از دست رفته یا خواهند رفت. بنابراین، اقتصاد بیت‌کوین، کاملاً غیرتورمی و نیز انقباضی است، اما در مقدار بیت‌کوین‌های در گردش کمبودی ایجاد نخواهد شد. همچنان که در اثر افزایش تقاضا، ارزش واحد بیت‌کوین در برابری با واحدهای پولی دیگر بالا می‌رود، می‌توان کسرهای کوچک‌تری از آن را در تراکنش‌ها به کار برد. هم‌اکنون می‌توان تا یک صد میلیون‌ام بیت‌کوین را در تراکنش‌ها به کار برد که به این کسر از بیت‌کوین، نام «ساتوشی» داده‌اند. ساتوشی ناکاموتو مؤلف مقاله‌ای در سال 2009 بوده است که در آن اساس سیستم بیت‌کوین را توضیح داده است. به‌طور دقیق مشخص نیست که آیا واقعاً چنین شخصی وجود دارد یا چندین شخصیت حقیقی و شاید حقوقی دیگر در پس این نام پنهانند!

کاستی‌های بیت‌کوین

غیبت نظارت دولتی و دخالت بانکی در بیت‌کوین (دست‌کم تا این‌جا) یک پیامد منفی هم دارد، اگر هنگام داد و ستد بیت‌کوین سرمایه‌تان را از دست بدهید، نمی‌توانید به بانک‌تان شکایت کنید و دولت نیز به احتمال کاری برای‌تان انجام نخواهد داد. البته، این به معنی آن نیست که پشتیبانی حرفه‌ای از مشتریان و سوداگران بیت‌کوین وجود ندارد. صدها

شرکت که بیش‌تر در مرحله استارت‌آپ هستند، خدمات مختلف مربوط به بیت‌کوین را انجام می‌دهند. اما یک اصل ثابت همیشه درباره داد و ستدهای بیت‌کوینی برقرار است: و این که اگر کلید محرمانه‌تان فاش شد و کسی از آن برای دسترسی به کیف پول‌تان استفاده کرد، بیت‌کوین‌هایی که از دست می‌دهید بازیافتنی نیستند.
اگر به هر دلیل، اطلاعات بخشی یا همه کیف پول بیت‌کوین خود را از دست بدهید (مثلاً در اثر خراب شدن هارددیسک کامپیوترتان که از آن نسخه پشتیبان نگرفته‌اید)، بیت‌کوین‌های شما از دست خواهند رفت و نه شما و نه هیچ کس دیگری نخواهد توانست به آن‌ها دسترسی پیدا کند. چنین حادثه‌ای چند بار برای مالکان مختلف بیت‌کوین رخ داده است و بنابراین مقدار کلی بیت‌کوین‌های در گردش هرگز به سقف 21 میلیونی خود نخواهد رسید.
اگر فرض کنیم شما کاربر محتاطی هستید و بیت‌کوین‌های‌تان هیچ گاه بر اثر بی‌احتیاطی و حادثه از دست‌تان نمی‌روند، باز هم یک مشکل همیشگی بر سر راه استفاده آسان از بیت‌کوین وجود دارد، که البته شاید بسیاری آن را مشکل به شمار نیاورند؛ هر کاربر و هر کاونده بیت‌کوین (Bitcoin miner) یک کپی از دفترحساب بیت‌کوین را روی کامپیوتر خود (در هر شکلی، از گوشی همراه گرفته تا یک سرور بزرگ) دارد، تنها به این وسیله است که می‌توان حساب بیت‌کوین‌ها و مالکان‌شان را نگاه داشت. مشکل این است که حجم این دفتر حساب، که همه تراکنش‌ها از آغاز پیدایش بیت‌کوین را ثبت کرده است، اکنون حدود 18 گیگابایت است و اندازه آن با گذشت زمان افزایش خواهد یافت.
روند زمانی افزایش حجم این فایل هم‌اکنون خطی است، اما با افزایش شمار کاربران و تراکنش‌ها، کاملاً ممکن است روند افزایش حجم این فایل شتاب بگیرد. مشخص نیست که بدیلی کارا و ایمن برای سیستم کنونی وجود داشته باشد، که در آن هر کاربر مجبور نباشد چنین حجمی از داده را همواره دنبال خود بکشد، اما واضح است که چنین وضعیتی اگر هم همیشگی باشد، برخلاف روند فزاینده گرایش به محاسبات ابری است.
همانند طلا و کانی‌های پرارزش دیگر، مصرف‌کنندگان بیت‌کوین هم شاید از کاوندگان آن غافل باشند؛ مصرف انرژی بسیار بالای شبکه گسترده کاوندگان بیت‌کوین، یکی از کاستی‌های مهم آن انگاشته می‌شود.
اگرچه این حجم بالای محاسبات رمزنگاری، تضمین‌کننده سازگاری، امنیت و پوشیدگی کل شبکه است، اما حجم انرژی مصرفی آن تا حدی بالا است که برخی از کاوندگان بیت‌کوین از گرمای کامپیوترهای خود در زمستان برای گرمایش خانه خود استفاده می‌کنند. تأمین هزینه این تجهیزات و انرژی مصرفی آن‌ها تنها با تکیه بر بیت‌کوین‌های تازه‌ای ممکن است که برندگان محاسبه به دست می‌آورند.
هم اکنون نیز در ثبت تراکنش‌های تازه، کاوش‌گران اولویت را به تراکنش‌هایی می‌دهند که ثبت‌کنندگان‌شان مبلغی را داوطلبانه به عنوان کارمزد به کاوش‌گران می‌پردازند. به تدریج که نرخ صدور سکه‌های تازه کاهش پیدا می‌کند، کاوندگان ناچار خواهند بود فقط تراکنش‌های کاربرانی را ثبت کنند که به طور داوطلبانه به کاوش‌گران کارمزد می‌پردازند. این روند به احتمال استفاده از بیت‌کوین را گران‌تر خواهد کرد و رقابت تازه‌ای را میان بازار بیت‌کوین و بازار مالی سنتی رقم خواهد زد.

بزرگ‌ترین هیاهوی رسانه‌ای بر ضد بیت‌کوین برمبنای پوشیدگی بسیار بالای آن است. پوشیدگی هویت پرداخت‌کنندگان و دریافت‌کنندگان، مرحله نخست پوشیدگی بیت‌کوین است، زیرا سازمان‌های اطلاعاتی و جاسوسی مانند NSA همواره

می‌توانند این تراکنش‌ها را با ردیابی آدرس‌های اینترنتی، به کاربران مربوط کنند. اما با استفاده از ابزارهایی همچون tor، که آدرس کاربران را نیز مخفی می‌کنند، کاربران بیت‌کوین می‌توانند تراکنش‌هایی کاملاً پوشیده و (دست‌کم به‌طور نظری) غیرقابل ردیابی انجام دهند.
چنین امکانی به طبع می‌تواند استفاده‌های غیرقانونی هم پیدا کند؛ مانند پول‌شویی، فرار از پرداخت مالیات، خرید و فروش کالای غیرقانونی و پشتیبانی مالی از سازمان‌ها و گروه‌های غیرقانونی یا زیرزمینی. مشهورترین نمونه استفاده از بیت‌کوین در این زمینه، سایت Silk road بوده است که با ساختاری همانند eBay، عرصه خرید و فروش انواع مواد مخدر، اسلحه و مهمات و حتی خدمات غیرقانونی بود. خرید و فروش روی این سایت تنها با بیت‌کوین انجام می‌گرفت. این سایت در ماه اکتبر سال 2013 توسط FBI بسته و مدیر آن بازداشت شد، اما تخمین زده می‌شود مدیر آن سرمایه‌ای هنگفت در حساب‌های بیت‌کوین خود داشته باشد که دست FBI از آن کوتاه است. نمونه مشهور دیگر استفاده از پوشیدگی بیت‌کوین، سایت ویکی‌لیکس است که هزینه‌های خود را از راه کمک‌های اهدایی در قالب بیت‌کوین تأمین می‌کند. استفاده از یک بیت‌کوین برای فعالیت‌های فراقانونی موضوع بلندترین فریادهای مخالفان بیت‌کوین است. البته بیت‌کوین تنها ابزاری نیست که از آن برای تراکنش‌های مالی غیرقانونی استفاده می‌شود. برای نمونه، بیش‌ترین حجم قاچاق اسلحه در جهان بر پایه دلار امریکا صورت می‌پذیرد.
بیت‌کوین شاید در کنترل بانک‌ها و دولت‌ها نباشد، اما ساده‌انگاری است که سیستم آن را تضمین‌کننده خودکار عدالت اجتماعی بدانیم. برای نمونه، در حدود 29 درصد کل بیت‌کوین صادرشده تاکنون، در مالکیت تنها 47 نفر است.
خریدهای هنگفت اولیه، توزیع بسیار ناهمگونی را در بازار جوان بیت‌کوین ایجاد کرده‌اند و ظرفیت ایجاد شوک در آینده را دارند.
حدود نیمی از بیت‌کوینی که تاکنون صادر شده است (و شاید هم بیش از آن) در گردش نیست و این احتکار بیت‌کوین از دلایل بالا رفتن قیمت واحد بیت‌کوین است. افزون بر آن، چنین حجمی از احتکار ممکن است چشم‌انداز نگران‌کننده‌ای از آینده بیت‌کوین ترسیم کند، شمار کوچکی از کاربران در هر زمانی می‌توانند با تزریق حجمی چشم‌گیر از بیت‌کوین به بازار، ارزش آن را دچار نوسان کنند.
اگرچه به‌طور منطقی دلیلی برای این کار وجود ندارد (زیرا به کاهش ارزش داشته‌های همان کاربران می‌انجامد)، انجام‌پذیر بودن این اقدام نگران‌کننده است.

هیجان‌زده باشید، اما نه بیش از حد

در هنگام نگارش این متن، بهای هر بیت‌کوین در حدود 630 دلار امریکا است. قیمت هر بیت‌کوین در آغاز عرضه آن کم‌تر از یک سنت بود. پس کسانی که در آن هنگام خرید کردند، اکنون سرمایه‌داران موفقی به شمار می‌روند. بهای بیت‌کوین در مقایسه با دلار روند افزایشی کاملاً یک‌نواختی نداشته است. ورشکستگی MT Gox در توکیو در سال 2013 که پیامد از دست رفتن دویست‌هزار بیت‌کوین آن بود، شوک بزرگی بر بازار بیت‌کوین بود. همچنین هنگامی که دولت چین استفاده از بیت‌کوین و همه پول‌های «مجازی» دیگر برای داد و ستد کالا و خدمات «واقعی» را ممنوع اعلام کرد، بهای بیت‌کوین در مقایسه با پول‌های رایج جهان به شدت کاهش یافت. اما در هر دو مورد و در موردهای دیگر، بیت‌کوین به سرعت کاهش ارزش خود را جبران کرد و بهای آن حتی از میزان پیش از شوک بالاتر رفت. شاید غیرمنطقی نباشد که آینده بیت‌کوین را بسیار روشن بدانیم، اما این را هم باید در نظر داشت که موضع‌گیری دولت‌ها درباره بیت‌کوین می‌تواند نقش مهمی در آینده آن داشته باشد و وضعیت در این باره هنوز چندان روشن نیست.
بسیاری از دولت‌ها با احتیاط به این موضوع نزدیک شده‌اند و شمار بسیار کمی نیز از آن استقبال کرده‌اند. آلمان، فنلاند، کانادا و امریکا از جمله کشورهایی هستند که در آن‌ها می‌توان از بیت‌کوین برای خرید و فروش کالا و خدمات (به شرط توافق دو طرف) استفاده کرد و نخستین خودپرداز بیت‌کوین در اکتبر 2013، در شهر ونکوور کانادا راه‌اندازی شده است. اگر شرایط خارج از سیستم بیت‌کوین تغییر چندانی نکند، با توجه به محدود بودن عرضه و افزایش تقاضا، می‌توان تصور کرد که بهای واحد آن افزایش پیدا کند، همچنین، کسب‌وکارهای فراوانی بر همین پایه ایجاد شده‌اند.

سرمایه‌گذاری برخی از شخصیت‌های حقیقی و حقوقی مطرح در دره سیلیکون مبنایی برای تبلیغات بسیاری از بازاریابانی است که می‌کوشند شما را به خریدن و اندوختن بیت‌کوین ترغیب کنند. اما باید در نظر داشت که سرمایه‌داران عمده در سیلیکون در چندین صنعت مختلف سرمایه‌گذاری‌های خطرپذیر می‌کنند و صِرف ورود آنان به یک زمینه، تضمینی برای سودآوری آن نیست. حتی اگر تا سال دیگر بیت‌کوین کاملاً از عرصه تراکنش‌های مالی محو شود، ایده‌های شکل‌دهنده به آن و سیستمی که بر مبنای آن ایده‌ها تشکیل شده است، به‌یقین مبنای حرکت‌های مشابه در آینده خواهند بود و تا همین حالا نیز چندین سیستم موازی بیت‌کوین (مانند لایت‌کوین) ایجاد شده و در حال فعالیت هستند. میزان رشد کنونی بیت‌کوین و پیچیدگی سیستمی که پیرامون آن شکل گرفته است، بی‌شک فراتر از پیش‌بینی دقیق طراح یا طراحان نخستین آن بوده است. دگردیسی این سیستم از عامل‌های پیچیده فراوانی در بیرون و درون آن تأثیر خواهد پذیرفت، چراکه پای پول در میان است!

تاریخ انتشار:
20 مرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/cover-story/1201