فناوری پشت پرده بیت‌کوین چگونه می‌تواند دنیا را تغییر دهد

بیت کوین؛ چیزی بیشتر از یک پول الکترونیکی است

فناوری پشت بیت‌کوین به افرادی که به همدیگر اعتماد ندارند یا همدیگر را نمی‌شناسند کمک می‌کند تا دفتر حساب ایجاد کنند. این امر نشان‌دهنده چیزی بیش از یک واحد پول الکترونیکی است.

وقتی پلیس هندوراس در سال ۲۰۰۹ برای دستگیری او آمد، ماریانا کاتالینا ایساگیره هنوز هم در خانه محقری که از سی سال پیش در آن ساکن بود، زندگی می‌کرد. برخلاف اکثر همسایگانش در تگوسیگالپای پایتخت، او سند رسمی برای زمینی که روی آن سکونت داشت را نیز در اختیار داشت؛ اما انجمن دارایی‌های هندوراس نشان می‌داد که نام فرد دیگری نیز به‌عنوان مالک روی آن زمین به چشم می‌خورد و آن فرد توانسته قاضی دادگاه را مجاب کند که حکم جلب ماریانا را بدهد. تا زمانی که مشکلات قانونی آن ملک حل‌وفصل شود خانه خانم ایساگیره به‌طور کلی ویران شده بود.

این چیزها در کشورهایی که املاک و مالکیت اراضی به‌خوبی مدیریت نمی‌شود یا فساد وجود دارد، همه‌روزه اتفاق می‌افتد. این مسئله کشورهای زیادی در دنیا را شامل می‌شود. نبود حقوق امن دارایی‌ها منبع شایعی برای ناامنی و بی‌عدالتی است. این موضوع حتی باعث می‌شود تا نتوان از زمین‌ها به‌عنوان محل سرمایه‌گذاری و ایجاد شغل بهره گرفت.

به‌نظر می‌رسد چنین مشکلی به‌هیچ عنوان ارتباطی با بیت‌کوین نداشته باشد که یک واحد پول مبتنی بر رمزنگاری زیرکانه است و میان

جایی در گذشته

کاربردهای دیگر زنجیره بلوکی و «دفتر حساب‌های توزیع‌شده» دیگر از به دام انداختن دزد الماس تا تبادل سهام در بازار بورس گسترده هستند: بازار تبادل بورس به‌زودی از سیستم مبتنی بر زنجیره بلوکی برای ثبت تبادلات در شرکت‌های خصوصی استفاده خواهد کرد. بانک انگلستان که به استفاده نکردن از تکنولوژی‌های روز معروف است از این ایده به وجد آمده است. در یکی از تحقیقات سال پیش آنها ذکر شده است که دفتر حساب‌های توزیع‌شده، نوآوری چشمگیری دارند که می‌توانند تاثیرات شگرفی در صنعت مالی داشته باشد. ذهن سیاست‌مداران، استفاده از زنجیره‌های بلوکی را فراتر از آن می‌بیند. وقتی تعاونی‌ها و جناح‌های چپ در «اویشر فست» پاریس برای کمک به سازمان‌هایی گردهم آمده بودند که می‌توانستند به جایگاه دارندگان عظیم داده مانند فیس‌بوک ضربه بزنند، تقریباً در هر بحثی عبارت زنجیره بلوکی به گوش می‌رسید. لیبرال‌ها دنیایی را تصور می‌کنند که در آن مقررات دولتی با قراردادهای بین فردی جایگزین شده باشند که در آن از برنامه‌نویسی زنجیره بلوکی استفاده می‌شود. زنجیره بلوکی، حیات خود را از ذهن سازنده ناشناس و باهوش بیت‌کوین با نام مستعار ساتوشی ناکاموتو آغاز کرد. آن‌طوری که او در مقاله‌ای منتشر کرد بیت‌کوین درواقع «نسخه کاملاً فردبه‌فرد پول الکترونیکی است». بیت‌کوین برای استفاده به‌عنوان پول نقد باید قابلیت دست‌به‌دست شدن داشته باشد بدون اینکه وارد حساب اشتباهی شود و نباید دوبار توسط یک فرد مورد استفاده قرار گیرد. برای رسیدن به رویای آقای ناکاموتو در مورد سیستم غیرمرکزگرا، اجتناب از چنین سوءاستفاده‌هایی باید بدون کمک از سوی هر طرف ثالث قابل اعتماد، مانند بانک‌ها صورت پذیرد که خود پشت سیستم پرداخت فعلی هستند.

این زنجیره بلوکی است که جایگزین آن طرف ثالث خواهد بود. با دارا بودن پایگاه داده‌ای مشتمل بر تمامی پرداخت‌های صورت‌گرفته از طریق بیت‌کوین‌های در گردش، زنجیره بلوکی می‌تواند در هر مقطعی ثابت کند که چه‌کسی مالک چه‌چیزی است. این دفتر حساب توزیع‌شده روی هزاران رایانه در سراسر دنیا - گره‌های بیت‌کوینی - کپی می‌شود و در دسترس عموم نیز قرار دارد؛ اما در کنار باز بودن آن، قابل اعتماد و ایمن نیز هست. این موضوع از طریق فنون ریاضی و رایانشی پیچیده موجود در «مکانیسم توافقی» آن امکان‌پذیر شده است - فرآیندی که به‌وسیله آن گره‌ها روی نحوه به‌روزرسانی زنجیره‌های بلوکی بعد از تراکنش‌های بیت‌کوینی بین افراد به توافق می‌رسند.

فرض کنید آلیس می‌خواهد هزینه خدماتی را پرداخت کند که باب به او ارائه داده است. هر دوی آنها «کیف پول» بیت‌کوینی دارند؛ نرم‌افزاری که با آن همانند دسترسی وب از طریق مرورگر می‌توان به زنجیره بلوکی دسترسی پیدا کرد، تنها با این تفاوت که هویت فرد به سیستم اعلام نمی‌شود. تراکنش با درخواست کیف پول آلیس به زنجیره بلوکی برای مقداری کمتر نشان دادن موجودی کیف پول آلیس به نسبت باب آغاز می‌شود.

شبکه برای تأیید این تغییر، مراحلی را طی می‌کند. با انتشار این درخواست از طریق شبکه برای کنترل روی گره‌ها و از طریق کنترل دفتر حساب، مشخص می‌شود که آیا آلیس واقعاً به اندازه‌ای که قصد خرج کردن دارد، موجودی بیت‌کوین دارد یا نه. اگر همه مراحل درست طی شده باشند، گره‌های خاصی با نام کاوشگران، درخواست آلیس را با دیگر تراکنش‌های موجه دیگر برای ایجاد بلوک جدید برای زنجیره بلوکی در یک بسته قرار می‌دهد.

با تکرار این مراحل، داده‌ها از طریق عملگر رمزنگاری «هش» به‌صورت نواری از اعداد در یک طول مشخص تبدیل می‌شوند (نمودار را ببینید). این هشینگ همانند دیگر انواع رمزنگاری، مسیری یک‌طرفه است. رفتن از سمت داده‌ها به هش آنها آسان است؛ اما نمی‌توان از هش به داده رسید؛ اما با اینکه هش داده‌ای را دربر ندارد، اما هر داده، هش مخصوص خود را دارد. با تغییر آنچه که وارد بلوک می‌شود به هر ترتیب ممکن - تغییر یک عدد در تراکنش - و آن هش متفاوت خواهد بود.

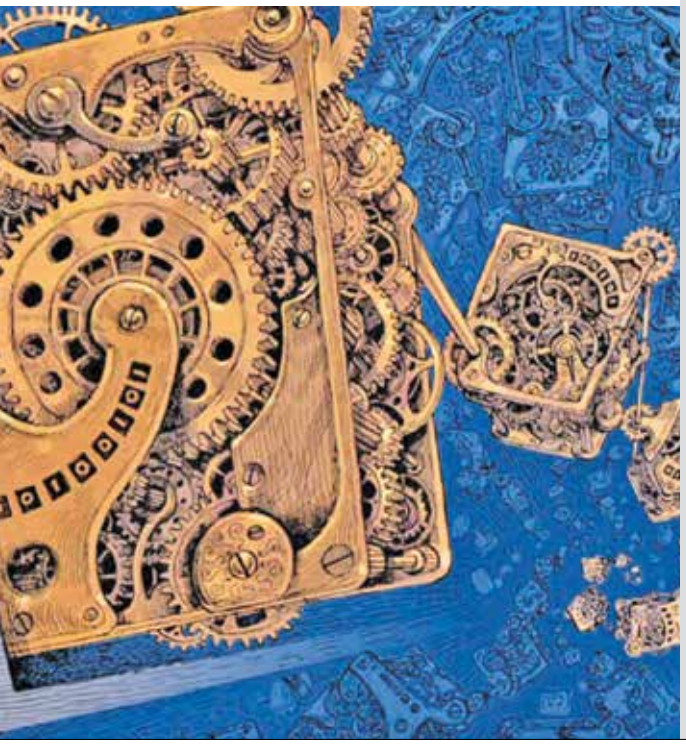
گروه‌های ضددولت و حتی تبهکاران محبوبیت زیادی دارد؛ اما بنیان رمزنگاری بیت‌کوین که «زنجیره بلوکی» نام دارد، کاربردی فراتر از پول نقد و ارز دارد. در واقع روشی به افرادی ارائه می‌کند که همدیگر را نمی‌شناسند یا به هم اعتماد نمی‌کنند تا بتوانند سوابقی از دارایی‌های هم داشته باشند که مورد تأیید همه‌طرف‌هاست. این روشی برای ایجاد و حفظ اعتماد است.

به همین دلیل سیاستمدارانی که قصد داشتند انجمن دارایی‌های هندوراس را پاک‌سازی کنند از شرکت دانش‌بنیان آمریکایی «فکتوم» خواستند تا نمونه‌ای از ثبت دارایی‌ها را برمبنای زنجیره‌های بلوکی برای آنها ایجاد کنند. ابراز علاقه به این ایده در یونان که سیستم ثبت املاک درستی ندارد و تنها ۷درصد اراضی به‌طور مناسبی نقشه‌بندی شده‌اند نیز شنیده شده است.

آقای ناکاتومو یک «پلتفرم باز» ایجاد کرده است؛ سیستمی توزیع‌شده که کارهای روی آن قابل بررسی و اکتشاف کامل هستند

اجرا در سایه

هش با دیگر داده‌ها در تیتر بلوک پیشنهادی قرار داده می‌شوند. این تیتر سپس اساس یک پازل جالب ریاضی می‌شود که بازهم در آن از عملگر هش استفاده شده است. این پازل را تنها می‌توان با آزمون و خطا حل کرد. در شبکه، کاوشگران از میان تریلیون‌ها احتمال به‌دنبال جواب پازل هستند. وقتی که یک کاوشگر سرانجام به یک پاسخ می‌رسد، گره‌های دیگر



سریعاً جواب به‌دست آمده او را کنترل می‌کنند (که بازهم مسیری یک‌طرفه است: حل کردن مشکل و کنترل آن آسان است) و هر گرهی که به تایید این راه‌حل می‌پردازد، بلوک را به‌روزرسانی می‌کند. هش موجود در تیتر نوار شناسایی جدید، بلوک می‌شود و اکنون این بلوک جزیی از دفتر حساب خواهد شد. پرداخت آلیس به باب و دیگر تراکنش‌های موجود در بلوک، این‌گونه مورد تأیید قرار می‌گیرد.

مرحله پازل، سه ویژگی را معرفی می‌کند که امنیت بیت‌کوین را افزایش می‌دهد. شما نمی‌توانید پیش‌بینی کنید که چه‌کسی زنجیره بلوکی را در لحظه‌ای معین به‌روزرسانی خواهد کرد مگر اینکه یک کاوشگر پرتلاش باشید. با این کار دیگر تقلب بسیار سخت خواهد بود.

دومین ویژگی افزون، تاریخچه است. هر تیتر جدید یک هش از تیتر بلوک قبلی را در خود دارد که به‌ترتیب آن بلوک هم خود یک هش از تیتر قبل‌تر را در خـــود دارد و همین‌طور تا اولین بلوک ادامه می‌یابد. این توالی، بلوک‌ها را همانند زنجیر به‌هم وصل می‌کند. به‌دلیل ثبت داده در دفتر حساب از ابتدا، ایجاد تیتر برای آخرین بلوک اهمیت چندانی ندارد. با تغییر در هر بخش دلخواه حتی در بلوک‌های اولیه، تیتر آن بلوک تغییر پیدا خواهد کرد. این یعنی تغییر در همه بلوک‌های بعدی. دفتر حساب با شناسه آخرین بلوک تطابق پیدا نخواهد کرد و درنتیجه مردود خواهد بود.

آیا راهی برای دور زدن این مراحل وجود دارد؟ فرض کنید در میانـــه راه نظر آلیس در مورد پرداخت هزینه به باب تغییر کند و بخواهد با بازنویسی تاریخچه، تغییری در کیف پولش ایجاد نشود. اگر او کاوشگر باهوشی بود می‌توانست پازل مربوطه را حل کرده و نســـخه جدید از زنجیره بلوکی را ایجاد کند؛ اما در حینی که او چنین قصدی داشته باشد، دیگر اعضای حاضر در شبکه، زنجیره بلوکی اصلی را بسیار طویل کرده‌اند و گره‌ها هم روی طولانی‌ترین زنجیره موجود کار می‌کنند. این قانون دو کاوشگر را که تقریباً هم‌زمان توانسته باشند پازل را با ایجاد چیزی بیش از یک انشعاب موقت در شبکه حل کنند متوقف کرده و همچنین جلوی تقلب را نیز می‌گیرد. برای اینکه آلیس، سیستم را مجبور کند تا نسخه جدید او را بپذیرد باید زنجیره را با سرعت بیشتری از بقیه حاضران در شبکه طویل‌تر کند. این هدف آلیس بدون کنترل بیش از ۵۰ درصد رایانه‌های سیستم – معروف به حمله ۵۱درصد – امکان‌پذیر نیست.

رویاها در برخی اوقات جذاب می‌شوند

بدون در نظر گرفتن ســـختی‌های موجود در مسیر آسیب زدن به شبکه، سؤال اساسی‌تری مطرح می‌شود: اصلاً چرا باید جزیی از چنین سیستمی بود؟

سومین ویژگی که مرحله حل پازل می‌افزاید، مشوق‌هاست. کاوشگری که بتواند پازل را حل کند، ۲۵ بیت‌کوین یعنی معادل ۷۵۰۰ دلار با نرخ امروزی تبادل ارز بیت‌کوینی، برنده می‌شود. هرچند این هوش موردنیاز، به‌خودی‌خود واحد بیت‌کوین را جذاب نمی‌کند. ارزش بیت‌کوین غیرقابل پیش‌بینی و ناپایدار است (چارت صفحه بعدی را ببینید) و میزان کلی در گردش آن نیز محدود است؛ اما مکانیسم زنجیره بلوکی بسیار عالی کار می‌کند. بنابر وب‌سایت blockchain.info که چنین تحرکاتی را کنترل می‌کند، حدود ۱۲۰هزار تراکنش روزانه از این طریق به زنجیره بلوکی اضافه می‌شود که معادل ۷۵ میلیون دلار آمریکا ارزش دارد. درحال‌حاضر، ۳۳۸هزار بلوک وجود دارد که حجم دفتر حساب به این ترتیب نزدیک به ۴۵ گیگابایت است.

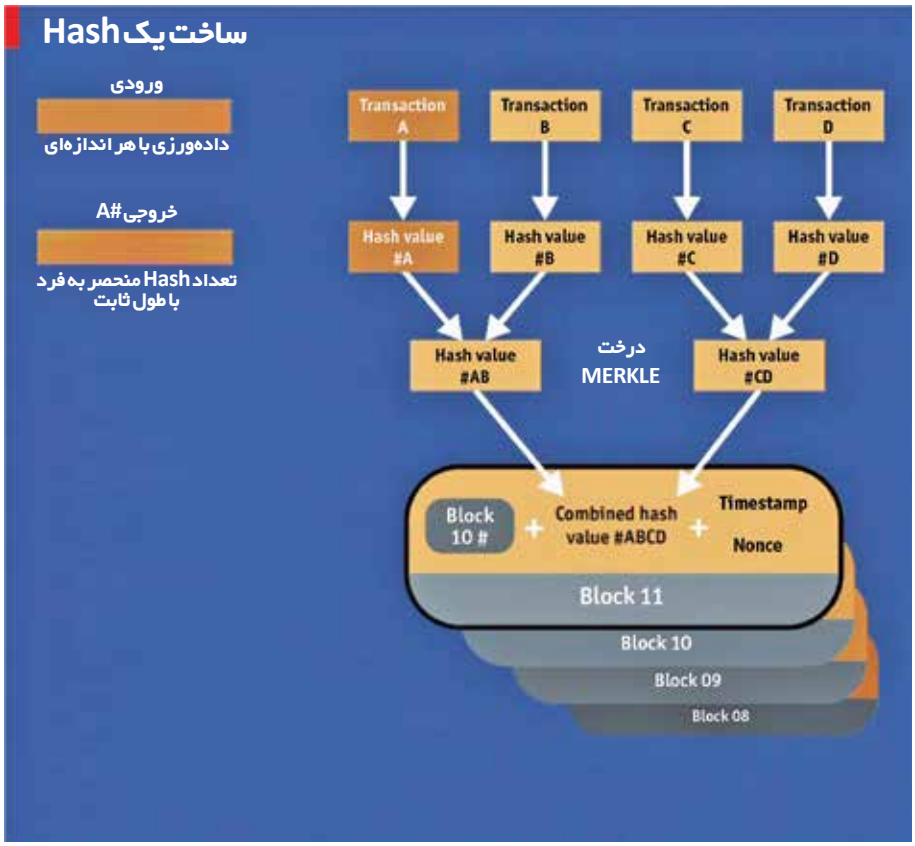
بیشتر داده‌ها در زنجیره بلوکی مربوط به بیت‌کوین‌ها هستند؛ اما لزوماً نیز چنین نیست. آقای ناکاتومو یک «پلتفرم باز» ایجاد کرده است؛ سیستمی توزیع‌شده که کارهای روی آن قابل بررسی و اکتشاف کامل هســـتند. مثال بارز از چنین پلتفرمی، خود اینترنت است؛ سیستم‌های عامل اندروید و ویندوز نیز از این نوع سامانه‌ها هستند. اپلیکیشن‌هایی را که برای کار کردن وابسته به برخی ویژگی‌های پایه زنجیره بلوکی هستند می‌توان به‌راحتی توســـعه داد، بدون اجازه از کسی یا پرداخت پول. «اینترنت بالاخره پایگاه داده عمومی در اختیار دارد». این جمله کریس دیکسون از شرکت سرمایه‌گذاری آندریسن هورویتز است که چندین شرکت بیت‌کوینی را از جمله «کوین‌بیس» (فعال در زمینه ارائه کیف پول) و «۲۱» (فروشنده تجهیزات انکشاف بیت‌کوینی) ایجاد کرده است.

درحال‌حاضر پیشنهادهای زنجیره بلوکی در سه دسته جای می‌گیرند. اولین دسته، مزیت انتقال هر نوع دارایی را با زنجیره بلوکی پیش می‌کشد. یکی از شرکت‌های دانش‌بنیان ارائه‌کننده چنین امکانی، «کولو» است. این شرکت مکانیسمی به‌وجود آورده است که می‌توان با آن هر تراکنش کوچک بیت‌کوینی (گره بیت‌کوینی) را با افزودن داده‌های اضافی به آنها به شکل برگه سهام و مالکیت فلزات قیمتی درآورد که اصطلاحاً به آن «رنگ» کردن تراکنش می‌گویند.

حفاظت از زمین و املاک، نمونه‌ای از دسته دوم پیشنهادهاست: اپلیکیشن‌هایی که از زنجیره بلوکی به‌عنوان ماشین اعتمادسازی استفاده می‌کنند. تراکنش‌های بیت‌کوینی را می‌توان با قطعات کوچک داده ترکیب کرد و به همان شکل وارد دفتر حساب کرد. دفتر حساب به این ترتیب مرجعی برای پیگیری موارد باارزش می‌شود. «اورلجر» از زنجیره بلوکی برای حفاظت از اشیای قیمتی استفاده می‌کند: به‌عنوان مثال، می‌تواند اطلاعات زنجیره بلوکی در مورد ویژگی‌های متمایز یک سنگ قیمتی را در خود نگه دارد تا بتوان درصورت سرقت آن سنگ، اصالت و هویت آن را گواهی کرد. «وان‌نیم» می‌تواند اطلاعات شخصی را بدون نیاز به رمزعبور نگه‌داری کند و «کوین‌اســـپارک» به‌عنوان یک دفتر تأیید اسناد عمل می‌کند. به یاد داشته باشید، به‌جز تراکنش‌های اولیه بیت‌کوینی برای استفاده از این اپلیکیشن‌ها به درجه‌ای از اعتماد نیاز داریم؛ شما باید مطمئن باشید که این واسطه‌ها به‌درستی داده‌ها را ذخیره و پردازش می‌کنند.

سومین دسته از پیشنهادها، جاه‌طلبانه‌تر از بقیه است: «قراردادهای هوشمند» که می‌توانند به‌صورت خودکار تحت شرایط پیش‌بینی شده هش خود را اعمـــال کنند. بیت‌کوین قابلیت برنامه‌ریزی برای دسترس‌پذیر بودن تنها در نوع خاصی از شرایط را دارد. یک حالت استفاده

ازآنجایی‌که کاوشگران، اطلاعات سخت‌افزاری خود را مخفی نگه می‌دارند، هیچ‌کسی نمی‌داند که در واقع شبکه چقدر انرژی را به مصرف می‌رساند



از چنین ویژگی به تأخیر انداختن پرداخت به کاوشگران تا افزوده شدن ۹۹ یا تعداد بیشتری از بلوک‌هاست که مشوق دیگری برای نگه‌داشتن بیت‌کوین در وضعیت قابل قبول است.

«لایت‌هاوس»، پروژه‌ای که توسط مایک هیبرن- یکی از برنامه‌نویسان بزرگ در دنیای بیت‌کوین- آغاز شده است، خدمت جمع‌آوری سرمایه غیرتمرکزگرایی است که از این اصل برای کار خود بهره می‌برد. آقای هیبرن می‌گوید طرح او از رقبای غیربیت‌کوینی ارزان‌تر تمام شده و مستقل‌تر خواهد بود، زیرا دولت‌ها نخواهند توانست جلوی چنین پروژه‌هایی را درصورت باب میل نبودن‌شان بگیرند.

انرژی واگیردار است

ورود دفتر حساب‌های توزیع شده از نظر آلبرت ونگر در شرکت USV که شرکت سرمایه‌گذار چند پروژه دانش‌بنیان مانند «اوپن‌بازار» در نیویورک است، «فصل جدیدی از امکانات را به‌روی همه باز کرده است»؛ اما با همه جذابیت‌های زنجیره بلوکی، منتقدان به امنیت و مقیاس‌پذیری آن تردیدهای جدی دارنـــد. آنچه می‌تواند برای بیت‌کوین و چند اپلیکیشن محدود کارساز باشد، ممکن است نتواند نیازهای میلیون‌ها کاربر خدمات مختلف جهان را پشتیبانی کند. با اینکه طراحی هوشمندانه آقای ناکاتومو تا به اینجای کار خود را غیرقابل نفوذ نشان داده است، محققان دانشگاهی تاکتیک‌هایی را شناسایی کرده‌اند که یک کاوشگر با امکانات زیاد بتواند زنجیره بلوکی را بدون در اختیار داشتن ۵۱درصد زنجیره، تحت کنترل خود داشته باشد و کنترل بخش قابل‌توجهی از منابع شبکه به نظر راحت‌تر از قبل می‌رسد. چیزی که قبلاً کاری تفریحی به‌حساب می‌آمد اینکه انکشاف بیت‌کوین در اختیار «ائتلاف»های بزرگ قرار دارد که در آنها کاوشگران خرد، تلاش‌ها و دستاوردهای خود را به‌اشتراک می‌گذارند و عاملان پایگاه‌های داده بزرگ در چین به‌خصوص مغولستان داخلی قرار دارند که برق در آن مناطق فوق‌العاده ارزان است. نگرانی دیگر، تاثیرات محیطی است. با در اختیار نداشتن روش دیگری برای اطمینان از حسن‌نیت کاوشگران، معماری بیت‌کوین آنها را مجبور می‌کند تا کارهای رایانشی سختی انجام دهند؛ این «تصدیق کار» که بدون آن خبری از جایزه نیست تا همه افرادی که وارد این بازی می‌شوند، سختی کار را تحمل کرده باشند؛ اما با این اوصاف درنهایت کارهای رایانشی بیهوده زیادی به انجام می‌رسد. بنابر blockchain.info، کاوشگران شبکه درحال‌حاضر ۴۵۰ هزار تریلیون راه‌حل را در هر ثانیه امتحان می‌کنند و همه این محاسبات به انرژی نیاز دارند.

در ماه‌های اخیر بانک‌هایی علاقه خود را به زنجیره‌های بلوکی خصوصی به‌عنوان روشی برای داشتن دفتر حساب‌های غیرقابل دستکاری نشان دادند

از آنجایی که کاوشگران، اطلاعات سخت‌افزاری خود را مخفی نگه می‌دارند، هیچ‌کسی نمی‌داند که در واقع شـــبکه چقدر انرژی را به مصرف می‌رساند. اگر همه از بهینه‌ترین سخت‌افزارها استفاده کنند، مصرف برق سالیانه شبکه چیزی در حدود ۲ تراوات در ساعت خواهد بود- کمی بیش از مصرف برق ۱۵۰هزار نفر ساکن بخش کینگ در کالیفرنیای مرکزی. البته با تخمین بدبینانه این مقدار تا ۴۰ تراوات در ساعت خواهد رسید که معادل مصرف برق ۱۰ میلیون ساکن بخش لس‌آنجلس است. هرچه تعداد بیشتری از افراد، بیت‌کوین را به‌کار گیرند این مشکل بزرگ‌تر هم می‌شود.

با وجود صرف چنین سهمی از منابع انرژی، استفاده از بیت‌کوین همچنان محدود است. به‌دلیل اینکه آقای ناکاتومو تصمیم گرفته است تا حجم یک بلوک را در یک مگابایت یا نزدیک به ۱۴۰۰ تراکنش محدود کند، هر بلوک تنها می‌تواند هفت تراکنش را در هر ثانیه مدیریت کند که عدد کوچکی در مقابل ۱۷۳۶ تراکنش‌های شرکت «ویزا» در آمریکاست. بلوک‌ها را می‌توان بزرگ‌تر ساخت، اما بلوک‌های بزرگ زمان زیادی برای گردش در شـــبکه نیاز دارند که ریسک انشعاب آن را بالاتر می‌برد.

پلتفرم‌های قبلی نیز چنین مشکلی را تجربه کردند. وقتی میلیون‌ها نفر توانستند بعد از ورود مرورگرها، اولین‌بار در دهه ۹۰ به اینترنت دسترسی پیدا کنند، متخصصان پیش‌بینی کردند که اینترنت به رکودی شدید برسد؛ اما هنوز هم زنده و پویا است. به همین شکل بیت‌کوین هنوز هم در حال جنب‌وجوش است. رایانه‌های کاوشگری بسیار بهینه‌ای وجود دارند و مکانیسم‌هایی پیشنهاد شده‌اند که انرژی کمتری را مصرف می‌کنند. توسعه‌دهندگان همچنین ویژگی افزونه‌ای را با نام «رعد و برق» معرفی کرده‌اند که می‌تواند تعداد زیادی از تراکنش‌های کوچک را خارج از زنجیره بلوکی مدیریت کند. سرعت بالاتر اینترنت هم می‌تواند به انتقال بهتر زنجیره‌های بزرگ کمک کند.

مشکل در اینجا کمبود راه‌حل‌ها نیست؛ بلکه «فرآیند بهبود بیت‌کوین» است که انتخاب

راه‌حل‌های پیشنهادی را مشکل می‌کند. اِعمال تغییرات باید با توافق بخش اعظمی از جامعه بیت‌کوینی صورت گیرد که به‌وجود آوردن نقطه مشترک تفکر برای این افراد کار راحتی نیست. جنگ داخلی را فرض کنید که دلیل آن حجم بلوک‌ها باشد. یک طرف دعوا، ادعا می‌کند که افزایش سریع اندازه بلوک‌ها به تجمع بیشتر در صنعت کاوش منجر می‌شود و بیت‌کوین را به یک پردازشگر رایج پرداخت‌ها تبدیل خواهد کرد. در طرف دیگر، ادعا می‌شود که اگر کار دیگر انجام نپذیرد، سیستم با توجه به اینکه هر فرآیند ساعت‌ها به‌طول خواهد انجامید به‌طور کلی نابود خواهد شد.

وقفه‌ای در جنگ

هیین و گاوین اندرسون از دیگر بزرگان بیت‌کوین، رهبران کمپ حامیان افزایش اندازه بلوک‌ها هستند. آنها از شرکت‌های کاوشگری خواسته‌اند که نسخه جدیدی از بیت‌کوین را نصب کنند تا بتوانند اندازه بزرگ‌تری از بلوک‌ها را پشتیبانی کنند. برخی از این شرکت‌ها که درخواست آنها را پذیرفته‌اند از مشکلاتی نظیر حملات سایبری رنج می‌برند و سیستم خود را به‌عنوان نشانه‌ای برای اعلام وجود خطر یا نیاز به به‌روزرسانی به انجام تراکنش‌های کوچک محدود می‌کند. همه این‌ها به تلاش‌هایی که در جهت ارائه جایگزینی برای بلوک‌های زنجیره‌ای صورت می‌پذیرد، انرژی مضاعفی داده است. تلاش‌هایی که برای ذخیره‌سازی دفترحساب‌های توزیع شده بهینه‌سازی شده‌اند و نه برای ارز دیجیتال بودن بیت‌کوین. «مولتی‌چین» پلتفرم ساختن زنجیره بلوک خود ارائه شده توسط «کوین ساینسز»، نشان می‌دهد که چه‌چیزی امکان‌پذیر است. در کنار ارائه امکان ساخت یک زنجیره بلوک عمومی همانند آن‌چه که در بیت‌کوین وجود دارد، کاربران مورد تأیید می‌توانند زنجیره‌های خصوصی خود را ایجاد کنند. اگر تمامی کاربران از همان ابتدا مورد تأیید قرار بگیرند، نیاز به کاوشگری و تصدیق کار از بین می‌رود یا کاهش می‌یابد و واحد پول موجود در دفتر حساب یک ارزش افزون به خود می‌گیرد.

اولین صنعتی که از این دست زنجیره‌های جدید استفاده کرد همان صنعتی بود که شکست‌های آن، مشوق آقای ناکاتومو در آغاز کارش بود: صنعت اقتصاد.

در ماه‌های اخیر بانک‌هایی علاقه خود را به زنجیره‌های بلوکی خصوصی به‌عنوان روشی برای داشتن دفتر حساب‌های غیرقابل دستکاری نشان دادند. عجیب‌تر اینکه، یکی از دلایل وجود چنین علاقه‌ای این است که این فناوری از لیبرالیسم ضددولتی به‌دنیا آمد که تطابق با مقررات ضدپولشویی و هویت مشتریان را برای بانک‌ها آسان می‌کرد؛ اما جذابیت اصلی آن از جای دیگری منشاء می‌گیرد.

تاریخ‌نگاران صنعتی می‌نویسند که نیروهای جدید غالباً قبل از اینکه فرآیندهایی مورد استفاده آنها به‌وجود آیند، توسعه داده می‌شوند. وقتی موتورهای الکتریکی برای اولین‌بار ساخته شدند از آنها همانند موتورهای بخار بزرگ قدیمی بهره‌برداری می‌شد. دهه‌ها طول کشید تا تولیدکنندگان متوجه شوند که می‌توان با استفاده از تعداد زیادی از موتورهای الکتریکی غیرمتمرکز، ساختار ساخت و تولید محصولات را به‌طور کلی تغییر داد. بانک انگلستان در گزارش خود در مورد ارزهای دیجیتال، چیزی مشابه همین موضوع را می‌بینند. بانک‌ها فرآیندهای درونی خود را با کمک رایانه‌ها دیجیتال کرده‌اند، اما ساختار سازمانی خود را برای تطابق با آن تغییر نداده‌اند. سیستم‌های پرداخت هنوز هم مرکزگرا هستند: تراکنش‌ها هنوز هم باید مورد تأیید بانک مرکزی قرار بگیرند. وقتی مؤسسات مالی می‌خواهند با همدیگر کار کنند، هماهنگ‌سازی صورت‌حساب‌ها نیز کاری زمان‌بر است که باعث افزایش ریسک و هزینه می‌شود.

دفترحساب‌های توزیع شده که صورت‌ها را می‌توانند در عرض چند دقیقه یا حتی ثانیه حل و فصل کنند، نقش بسیار زیادی در حل مشکلات بانکداری دیجیتال دارد. آنها همچنان می‌توانند در صرفه‌جویی هزینه بانک‌ها نیز مؤثر باشند: بنابر بانک «سانتاندر» از سال ۲۰۲۲ چنین دفترهایی می‌توانند هر سال برای این صنعت، صرفه‌جویی به‌همراه بیاورند. سازندگان این فناوری هم باید ثابت کنند که می‌توانند از پس بار تراکنش‌های سریع و بسیار زیادتر از بیت‌کوین‌ها برآیند؛ اما بانک‌های بزرگ درحال‌حاضر به‌دنبال تعیین استانداردها برای این فناوری نوظهور هستند. یکی از آنها به نام UBS، پیشنهاد ایجاد «سکه حل‌وفصل» استاندارد را داده است. اولین سفارش برای شرکت دانش‌بنیان R3 CEV فعال در زمینه زنجیره‌های بلوکی که UBS و ۲۳ بانک دیگر روی آن سرمایه‌گذاری کرده‌اند، توسعه معماری استاندارد برای دفترهای حساب خصوصی بوده است.

مشکل بانک‌ها فقط مختص به آنها نیست. تمام شرکت‌ها و دستگاه‌های عمومی از پایگاه‌های داده غیرسازگار و با هزینه نگهداری بالا برای تعامل با همدیگر گله دارند. این مشکلی است که «اتریوم» که به جرات می‌توان گفت که جاه‌طلبانه‌ترین پروژه در زمینه دفترهای حساب توزیع شده است، قصد حل آن را دارد. دفترهای حساب

تاریخ‌نگاران صنعتی می‌نویسند که نیروهای جدید غالباً قبل از اینکه فرآیندهایی مورد استفاده آنها به‌وجود آیند، توسعه داده می‌شوند

توزیع شده اتریوم که محصول کار ویتالیک بوترین، برنامه‌نویس ۲۱ ســاله قهار از کانادا است، می‌تواند با داده‌هایی بیشتری به نسبت بیت‌کوین کار کند و همراه اینها برنامه‌نویسی وجود دارد که به کاربران اجازه می‌دهد تا مخاطبان هوشمندتری ایجاد کنند تا آنها بتوانند صورت پرداخت خودکاری به‌وجود آورند که با ورود محموله پرداخت می‌شود یا اینکه می‌توانند به مالک خود حق‌السهم سود را از محل سودهای شرکت بپردازند. بنابر نظر آقای بوترین، چنین هوشی به ایجاد «سازمان‌های غیرمرکزگرای مستقل» - شرکت‌های مجازی وضع‌کننده قانون برای اجرا بر روی زنجیره بلوکی اتریوم - کمک می‌کند.

اینترنت اشیا یکی از نقاطی است که این ایده‌ها می‌توانند تاثیرات تندتری بگذارند؛ شبکه‌ای از میلیاردها اشیایی که قبلاً صامت بودند مانند یخچال، دستگیره درب و آبپاش‌ها. طبق گزارش اخیر IBM باعنوان «دموکراسی تجهیزات» که ایده پیگیری و مدیریت همه این تجهیزات به‌صورت متمرکز امکان‌پذیر نیست و حتی احمقانه است؛ در آن صورت تجهیزات به‌راحتی مورد حمله تبهکاران سایبری و نظارت دولتی قرار می‌گرفتند. به‌نظر می‌رسد دفتر ثبت توزیع شده جایگزین خوبی باشد.

نوعی از برنامه‌پذیری که اتریوم ارائه می‌کند تنها محدود به امکان پیگیری و ثبت وقایع مایملک افراد نمی‌شود؛ بلکه اجازه می‌دهد از این امکان به‌نحوی دیگر استفاده کرد. به این ترتیب سوییچ خودرویی که در زنجیره بلوکی اتریوم قرار می‌گیرد، به‌نحوی که در مقررات داخلی آمده است، قابلیت خرید و فروش یا اجاره را دارد که شِمای جدید نفربه‌نفری در مبادله و کرایه خودرو ایجاد می‌کند. علاوه بر این، برخی صحبت‌ها در مورد استفاده از این تکنولوژی برای تبدیل خودروهای بدون نیاز به راننده به‌صورت خودمختار در حال به‌واقعیت پیوستن است. چنین خودروهایی می‌توانند با پس‌انداز مقداری از پول دیجیتالی که از اجاره دادن خودرو به‌دست می‌آورند، طبق برنامه برای پرداخت سوخت و تعمیرات و پارکینگ استفاده کنند.

رسوچه گفته بود؟

عجیب نیست که چنین ایده‌هایی بیش از حد جاه‌طلبانه خوانده شوند. اولین بلوک اتریوم تنها در همین آگوست مورد کاوش قرار گرفت و به همین دلیل اکوسیستم کوچکی از شرکت‌های دانش‌بنیان حول آن جمع شده‌اند که بوترین دلیل آن را کمبود منابع مالی‌اش عنوان کرد؛ اما جزییات اینکه کــدام زنجیره بلوکی خاص موفقیت‌آمیز خواهد بود از دید کلی نسبت به

اینترنت اشیا یکی از نقاطی است که این ایده‌ها می‌توانند تاثیرات تندتری بگذارند؛ شبکه‌ای از میلیاردها اشیایی که قبلاً صامت بودند مانند یخچال، دستگیره درب و آبپاش‌ها

دفترهای حساب توزیع شده در شرکت‌های بزرگ و جدید کمتر اهمیت دارد. علی‌رغم توانایی بالای جامعه برای تمسخر حسابداران، سازوکار دفترهای حساب بسیار مهم است.

دنیای امروزی شدیداً در پی ثبت دوگانه سوابق است. سیستم استاندارد ثبت دارایی‌ها و بدهی‌ها مهم‌ترین بخش درک موقعیت مالی یک شرکت است. با اینکه طبق گفته ورنر سومبارت جامعه‌شناس آلمانی در اوایل قرن بیستم، نظام سرمایه‌داری چنین سیستم ثبتی را برای رشد خود در پیش گرفت، اما بازهم می‌توان آن را مورد سؤال قرار داد. با اینکه این سیستم در دوران رنسانس در ایتالیا شروع شد، رشدش به‌اندازه رشد سرمایه‌داری در دنیا سریع نبود و تنها در اواخر قرن نوزدهم، خارج از ایتالیا به‌کار گرفته شد؛ اما در اینکه این روش ثبتی از اهمیت بالایی در ثبت وقایع شرکت و نیز درک جایگاه آن برخوردار است، شکی وجود ندارد. دفترهای حسابی که دیگر نیازی به حفظ شدن توسط شرکت یا یک دولت ندارند، می‌توانند به‌مرور زمان تغییراتی را در چگونگی کارکرد شرکت‌ها و دولت‌ها به‌وجود آورد؛ اینکه چه‌چیزی از آنها انتظار می‌رود و چه‌چیزی بدون حضور آنها می‌توان انجام داد. رسیدن به این نکته که سیستم‌های غیرمتمرکز ثبت وقایع به‌اندازه همتایان مرکزگرایشان قابل‌اعتماد هستند می‌تواند موجب تغییرات گسترده‌ای شود.

چنین ایده‌هایی هنوز هم به بررسی بیشتری نیاز دارد؛ زنجیره‌های بلوکی هنوز هم در محافل کوچکی کاربردی شده‌اند و تردیدهایی در مورد میزان گسترش آنها و مقیاس‌پذیری وجود دارد. آنها ممکن اســت با مقاومت نیز روبه‌رو شوند. برخی از منتقدان بیت‌کوین آن را به‌صورت آخرین ابزاری برای گسترش «ایدئولوژی کالیفرنیایی» که با وعده موفقیت با عدم مرکزگرایی مبتنی بر فناوری و درعین‌حال نادیده گرفتن واقعیت‌های قدرت‌ها عملا پول‌ها را به جیب تعداد اندکی از ثروتمندان سرازیر می‌کند. ایده ایجاد اعتماد بدون استفاده از قدرت دموکراسی، قانون و مشروعیت و تنها از طریق کدها، به‌خودی‌خود ایده جذاب و قدرتمندی نیست. درعین‌حال، دنیایی که ثبت وقایع آن از طریق فرمول‌های ریاضی و نه به‌دست بشر انجام می‌شود، می‌تواند مزایای بسیاری داشته باشد. خانم ایساگیره بازداشت‌شده، بهتر از همه می‌تواند از مزایای چنین دنیایی بهره‌مند شود. اگر زنجیره‌های بلوکی، پارادوکس اساسی را در خود داشته باشند تنها می‌تواند این باشد: با ارائه روشی برای چیدمان حال و گذشته با رمزنگاری، آنها می‌توانند آینده را تغییر دهند.