

فناوری پشت پرده بیت کوین چگونه می تواند دنیا را تغییر دهد

بیت کوین؛ چیزی بیشتر از یک پول الکترونیکی است

فناوری پشت بیت کوین به افرادی که به همدیگر اعتماد ندارند یا همدیگر را نمی شناسند کمک می کند تا دفتر حساب ایجاد کنند. این امر نشان دهنده چیزی بیش از یک واحد پول الکترونیکی است.



زیادی در دنیا را شامل می شود. نبود حقوق امن دارایی ها منبع شایعی برای ناامنی و بی عدالتی است. این موضوع حتی باعث می شود تا نتوان از زمین ها به عنوان محل سرمایه گذاری و ایجاد شغل بهره گرفت.

به نظر می رسد چنین مشکلی به هیچ عنوان ارتباطی با بیت کوین نداشته باشد که یک واحد پول مبتنی بر رمزنگاری زیر کانه است و میان

دیگری نیز به عنوان مالک روی آن زمین به چشم می خورد و آن فرد توانسته قاضی دادگاه را مجاب کند که حکم جلب ماریانا را بدهد. تا زمانی که مشکلات قانونی آن ملک حل و فصل شود خانه خانم ایساگیره به طور کلی ویران شده بود. این چیزها در کشورهایی که املاک و مالکیت اراضی به خوبی مدیریت نمی شود یا فساد وجود دارد، همه روزه اتفاق می افتد. این مسئله کشورهای

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 می کرد. برخلاف اکثر همسایگانش در تگوسیگالپای پایتخت، او سند رسمی برای زمینی که روی آن سکونت داشت را نیز در اختیار داشت؛ اما انجمن دارایی های هندوراس نشان می داد که نام فرد



جایی در گذشته

کاربردهای دیگر زنجیره بلوکی و «دفتر حساب‌های توزیع شده» دیگر از به دام انداختن دزد الماس تا تبادل سهام در بازار بورس گسترده هستند: بازار تبادل بورس به زودی 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 توزیع شده، نوآوری چشمگیری دارند که می‌تواند تأثیرات 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 برنامه‌نویسی زنجیره بلوکی استفاده می‌شود. زنجیره بلوکی، حیات خود را از ذهن سازنده ناشناس و باهوش بیت‌کوین با نام مستعار ساتوشی ناکاموتو آغاز کرد. آن طوری که او در مقاله‌ای منتشر کرد بیت‌کوین در واقع «نسخه کاملاً فرد به فرد 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 غیر مکزگر، 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 صورت گرفته از طریق بیت‌کوین‌های در گردش، زنجیره بلوکی می‌تواند در هر مقطعی ثابت کند که چه کسی مالک چه چیزی است. این دفتر حساب توزیع شده 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 توافق» آن امکان پذیر شده است - فرآیندی که به وسیله 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، مراحل 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» به صورت نواری از اعداد در یک طول مشخص تبدیل می‌شوند (نمودار را ببینید). این هشینگ همانند دیگر انواع رمزنگاری، مسیری یک طرفه 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 ضد دولت 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 همه طرف‌هاست. 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 بر مبنای زنجیره‌های بلوکی برای آنها ایجاد کنند. ابراز علاقه به این ایده در یونان که سیستم ثبت املاک درستی ندارد و تنها ۷ درصد اراضی به‌طور مناسبی نقشه‌بندی شده‌اند نیز شنیده شده است.



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

اجرا در سایه

هش با دیگر داده‌ها در تتر بلوک پیشنهادی قرار داده می‌شوند. این تتر سپس اساس یک پازل جالب ریاضی می‌شود که باز هم 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 به دنبال جواب پازل هستند. وقتی که یک کاوشگر سرانجام به یک پاسخ می‌رسد، گره‌های دیگر



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 به راحتی توسعه 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 بیت کویین را از جمله «کوبین‌بیس» (فعال در زمینه ارائه کیف پول) و «۲۱» (فروشنده تجهیزات انکشاف بیت کویین) ایجاد کرده است.

در حال حاضر 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 به وجود آورده است که می‌توان با آن هر تراکنش کوچک بیت کویین (گره بیت کویین) را با افزودن داده‌های اضافی به آنها به شکل برگه سهام و مالکیت فلزات قیمتی در آورد که اصطلاحاً به آن «رنگ» کردن تراکنش می‌گویند.

حفاظت از زمین و املاک، نمونه‌ای از دسته دوم پیشنهادهاست؛ اپلیکیشن‌هایی که از زنجیره بلوکی به عنوان ماشین اعتمادسازی استفاده می‌کنند. تراکنش‌های بیت کویین 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 با ارزش می‌شود. «اورلجر» از زنجیره بلوکی برای حفاظت از اشیای قیمتی استفاده می‌کند؛ به عنوان مثال، می‌تواند اطلاعات زنجیره بلوکی در مورد ویژگی‌های متمایز یک سنگ قیمتی را در خود نگه دارد تا بتوان در صورت سرقت آن سنگ، اصالت و هویت آن را گواهی کرد. «وان‌نیم» می‌تواند اطلاعات شخصی را بدون نیاز به رمز عبور نگه‌داری کند و «کوبین‌اسپارک» به عنوان یک دفتر تأیید اسناد عمل می‌کند. به یاد داشته باشید، به جز تراکنش‌های اولیه بیت کویین برای استفاده از این اپلیکیشن‌ها به درجه‌ای از اعتماد نیاز داریم؛ شما باید مطمئن باشید که این واسطه‌ها به درستی داده‌ها را ذخیره و پردازش می‌کنند. سومین دسته از پیشنهادها، جاه‌طلبانه‌تر از بقیه است: «قرار داده‌های هوشمند» که می‌توانند به صورت خودکار تحت شرایط پیش‌بینی شده هش خود را اعمال کنند. بیت کویین قابلیت برنامه‌ریزی برای دسترس‌پذیر بودن تنها در نوع خاصی از شرایط را دارد. یک حالت استفاده

شناسه آخرین بلوک تطابق پیدا نخواهد کرد و در نتیجه مردود خواهد بود.

آیا راهی برای دور زدن این مراحل وجود دارد؟ فرض کنید در میانه 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 نسخه 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 طولی 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 طولی تر کند. این هدف آلیس بدون کنترل بیش از ۵۰ درصد رایانه‌های سیستم - معروف به حمله ۵۱ درصد - امکان‌پذیر نیست.

رویاهادر برخی اوقات جذاب می‌شوند بدون در نظر گرفتن سختی‌های موجود در مسیر آسیب زدن به شبکه، سؤال اساسی‌تری مطرح می‌شود: اصلاً چرا باید چیزی از چنین سیستمی بود؟

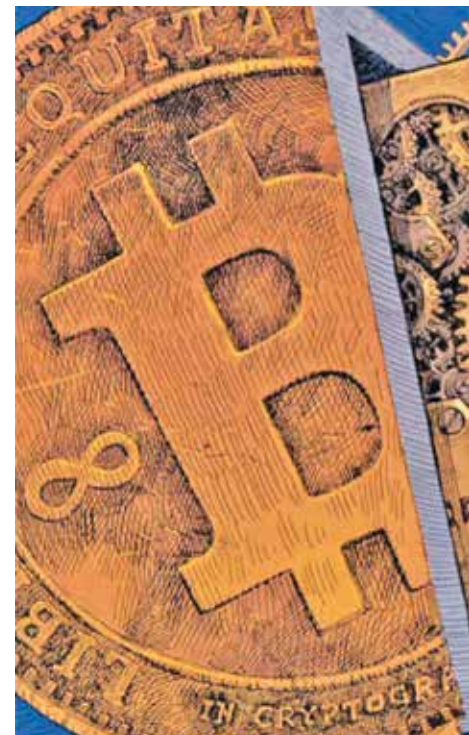
سومین ویژگی که مرحله حل پازل می‌افزاید، مشوق‌هاست. کاوشگری که بتواند پازل را حل کند، ۲۵ بیت کوبین یعنی معادل ۷۵۰۰ دلار با نرخ امروزی تبادل ارز بیت کویین، برنده می‌شود. هر چند این هوش مور دنیا، به خودی خود واحد بیت کوبین را جذاب نمی‌کند. ارزش بیت کوبین غیرقابل پیش‌بینی و ناپایدار است (چارت صفحه بعدی را 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 ۱۲۰ هزار تراکنش روزانه از این طریق به زنجیره بلوکی اضافه می‌شود که معادل ۷۵ میلیون دلار آمریکا ارزش دارد. در حال حاضر، ۳۳۸ هزار بلوک وجود دارد که حجم دفتر حساب به این ترتیب نزدیک به ۴۵ گیگابایت است.

بیشتر داده‌ها در زنجیره بلوکی مربوط به بیت کوبین‌ها هستند؛ اما لزوماً نیز چنین نیست. آقای ناکاتومو یک «پلتفرم باز» ایجاد کرده است؛ سیستمی توزیع شده که کارهای روی آن قابل بررسی و انکشاف کامل هستند. مثال بارز از چنین

سریعاً جواب به دست آمده او را کنترل می‌کنند (که باز هم مسیری یک‌طرفه است: حل کردن مشکل و کنترل آن آسان است) و هر گرهی که به تأیید این راه‌حل می‌پردازد، بلوک را به روزرسانی می‌کند. هش موجود در تیترا نوار شناسایی جدید، بلوک می‌شود و اکنون این بلوک جزئی 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 بیت کوبین را افزایش می‌دهد. شما نمی‌توانید پیش‌بینی کنید که چه کسی زنجیره بلوکی را در لحظه‌ای معین به روزرسانی خواهد کرد مگر اینکه یک کاوشگر پر تلاش باشید. با این کار دیگر تقلب بسیار سخت خواهد بود.

دومین ویژگی افزون، تاریخچه است. هر تیترا جدید یک هش از تیترا قبلی را در خود دارد که به ترتیب آن بلوک هم خود یک هش از تیترا قبل تر را در خود دارد و همین‌طور تا اولین بلوک ادامه می‌یابد. این توالی، بلوک‌ها را همانند زنجیر به هم وصل می‌کند. به دلیل ثبت داده در دفتر حساب از ابتدا، ایجاد تیترا برای آخرین بلوک اهمیت چندانی ندارد. با تغییر در هر بخش دلخواه حتی در بلوک‌های اولیه، تیترا آن بلوک تغییر پیدا خواهد کرد. این یعنی تغییر در همه بلوک‌های بعدی. دفتر حساب با



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

نیست تا همه افرادی که وارد این بازی می شوند، سختی کار را تحمل کرده باشند؛ اما با این اوصاف در نهایت کارهای رایانشی بیهوده زیادی به انجام می رسد. بنابر blockchain.info، کاوشگران شبکه در حال حاضر ۴۵۰ هزار تریلیون راه حل را در هر ثانیه امتحان می کنند و همه این محاسبات به انرژی نیاز دارند.

از آنجایی که کاوشگران، اطلاعات سخت افزاری خود را مخفی نگه می دارند، هیچ کسی نمی داند که در واقع شبکه چقدر انرژی را به مصرف می رساند. اگر همه از بهینه ترین سخت افزارها استفاده کنند، مصرف برق سالیانه شبکه چیزی در حدود ۲ تراوات در ساعت خواهد بود - کمی بیش از مصرف برق ۱۵۰ هزار نفر ساکن بخش کینگ در کالیفرنیا مرکزی. البته با تخمین بدبینانه این مقدار تا ۴۰ تراوات در ساعت خواهد رسید که معادل مصرف برق ۱۰ میلیون ساکن بخش لس آنجلس است. هر چه تعداد بیشتری از افراد، بیت کوین را به کار گیرند این مشکل بزرگ تر هم می شود.

با وجود صرف چنین سهمی از منابع انرژی، استفاده از بیت کوین همچنان محدود است. به دلیل اینکه آقای ناکاتومو تصمیم گرفته است تا حجم یک بلوک را در یک مگابایت یا نزدیک به ۱۴۰۰ تراکنش محدود کند، هر بلوک تنها می تواند هفت تراکنش را در هر ثانیه مدیریت کند که عدد کوچکی در مقابل ۱۷۳۶ تراکنش های شرکت «ویزا» در آمریکا است. بلوک ها را می توان بزرگ تر ساخت، اما بلوک های بزرگ زمان زیادی برای گردش در شبکه نیاز دارند که ریسک انشعاب آن را بالاتر می برد.

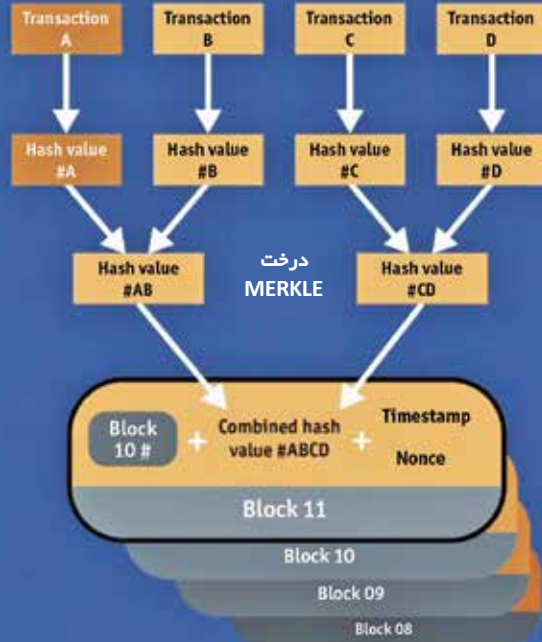
پلتفرم های قبلی نیز چنین مشکلی را تجربه کردند. وقتی میلیون ها نفر توانستند بعد از ورود مرورگرها، اولین بار در دهه ۹۰ به اینترنت دسترسی پیدا کنند، متخصصان پیش بینی کردند که اینترنت به رکودی شدید برسد؛ اما هنوز هم زنده و پویا است. به همین شکل بیت کوین هنوز هم در حال جنب و جوش است. رایانه های کاوشگری بسیار بهینه ای وجود دارند و مکانیسم هایی پیشنهاد شده اند که انرژی کمتری را مصرف می کنند. توسعه دهندگان همچنین ویژگی افزونه ای را با نام «رعد و برق» معرفی کرده اند که می تواند تعداد زیادی از تراکنش های کوچک را خارج از زنجیره بلوکی مدیریت کند. سرعت بالاتر اینترنت هم می تواند به انتقال بهتر زنجیره های بزرگ کمک کند.

مشکل در اینجا کمبود راه حل ها نیست؛ بلکه «فرآیند بهبود بیت کوین» است که انتخاب

ساخت یک Hash

ورودی
داده ورزی با هر اندازه ای

خروجی A#
تعداد Hash منحصر به فرد با طول ثابت



در ماه های اخیر بانک هایی علاقه خود را به زنجیره های بلوکی خصوصی به عنوان روشی برای داشتن دفتر حساب های غیر قابل دستکاری نشان دادند

بیت کوین و چند اپلیکیشن محدود کار ساز باشد، ممکن است نتواند نیازهای میلیون ها کاربر خدمات مختلف جهان را پشتیبانی کند. با اینکه طراحی هوشمندانه آقای ناکاتومو تا به اینجای کار خود را غیر قابل نفوذ نشان داده است، محققان دانشگاهی تاکتیک هایی را شناسایی کرده اند که یک کاوشگر با امکانات زیاد بتواند زنجیره بلوکی را بدون در اختیار داشتن ۵۱ درصد زنجیره، تحت کنترل خود داشته باشد و کنترل بخش قابل توجهی از منابع شبکه به نظر راحت تر از قبل می رسد. چیزی که قبلاً کاری تفریحی به حساب می آمد اینکه انکشاف بیت کوین در اختیار «ائتلاف» های بزرگ قرار دارد که در آنها کاوشگران خرد، تلاش ها و دستاوردهای خود را به اشتراک می گذارند و عاملان پایگاه های داده بزرگ در چین به خصوص مغولستان داخلی قرار دارند که برق در آن مناطق فوق العاده ارزان است. نگرانی دیگر، تاثیرات محیطی است. با در اختیار نداشتن روش دیگری برای اطمینان از حسن نیت کاوشگران، معماری بیت کوین آنها را مجبور می کند تا کارهای رایانشی سختی انجام دهند؛ این «تصدیق کار» که بدون آن خبری از جایزه

از چنین ویژگی به تأخیر انداختن پرداخت به کاوشگران تا افزوده شدن ۹۹ یا تعداد بیشتری از بلوک هاست که مشوق دیگری برای نگه داشتن بیت کوین در وضعیت قابل قبول است. «لایت هاوس» پروژه ای که توسط مایک هیبرن - یکی از برنامه نویسان بزرگ در دنیای بیت کوین - آغاز شده است، خدمت جمع آوری سرمایه غیر تمرکزگرای است که از این اصل برای کار خود بهره می برد. آقای هیبرن می گوید طرح او از رقبا غیر بیت کوینی ارزان تر تمام شده و مستقل تر خواهد بود، زیرا دولت ها نخواهند توانست جلوی چنین پروژه هایی را در صورت باب میل نبودن شان بگیرند.

انرژی واگیر دار است

ورود دفتر حساب های توزیع شده از نظر آلبرت ونگر در شرکت USV که شرکت سرمایه گذار چند پروژه دانش بنیان مانند «اوپن بازار» در نیویورک است، «فصل جدیدی از امکانات را به روی همه باز کرده است»؛ اما با همه جذابیت های زنجیره بلوکی، منتقدان به امنیت و مقیاس پذیری آن تردیدهای جدی دارند. آنچه می تواند برای

دفتر حساب‌های 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 «سائتاندر» از سال ۲۰۲۲ چنین دفترهایی می‌توانند هر سال برای این صنعت، صرفه‌جویی به همراه بیاورند. سازندگان این فناوری هم باید ثابت کنند که می‌توانند از پس بار تراکنش‌های سریع و بسیار زیادتر از بیت‌کوین‌ها برآیند؛ اما بانک‌های بزرگ در حال حاضر به دنبال تعیین استاندارد برای این فناوری نوظهور هستند. یکی از آنها به نام UBS، پیشنهاد ایجاد «سکه حل‌فصل» 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 «تریوم» که به جرات می‌توان گفت که جاه‌طلبانه‌ترین پروژه در زمینه دفترهای حساب توزیع شده است، قصد حل آن را دارد. دفترهای حساب

نشان دادند. عجیب‌تر اینکه، یکی از دلایل وجود چنین علاقه‌ای این است که این فناوری از لیبرالیزم ضد دولتی به دنیا آمد که تطابق با مقررات ضد پولشویی 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 به وجود آیند، توسعه داده می‌شوند. وقتی موتورهای الکتریکی برای اولین بار 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 ارزش‌های دیجیتال، چیزی مشابه همین موضوع را می‌بیند. 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 صورت حساب‌ها نیز کاری زمان‌بر است که باعث افزایش ریسک و هزینه می‌شود.

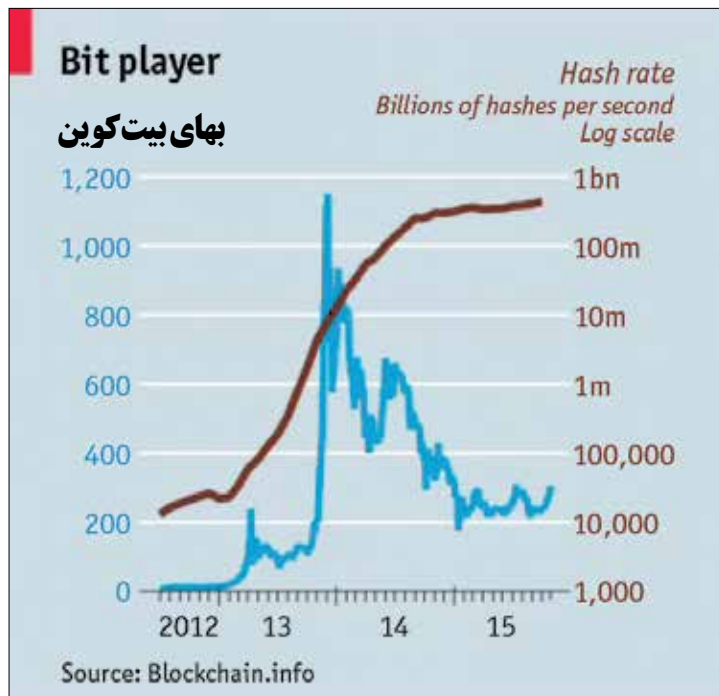
راه‌حل‌های پیشنهادی را مشکل می‌کند. اعمال تغییرات باید با توافق بخش اعظمی از جامعه بیت‌کوینی صورت گیرد که به وجود آوردن نقطه مشترک تفکر برای این افراد کار راحتی نیست. جنگ داخلی را فرض کنید که دلیل آن حجم بلوک‌ها باشد. یک طرف دعوا، ادعا می‌کند که افزایش سریع اندازه بلوک‌ها به تجمع بیشتر در صنعت کاوش منجر 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 به طول خواهد انجامید به‌طور کلی نابود خواهد شد.

وقفهای در جنگ

همین و گاوبین اندرسون از دیگر بزرگان بیت‌کوین، رهبران کمپ حامیان افزایش اندازه بلوک‌ها هستند. آنها از شرکت‌های کاوشگری خواست‌اند 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 به‌انجام 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 دفتر حساب‌های توزیع شده بهینه‌سازی شده‌اند و نه برای ارز دیجیتال بودن بیت‌کوین. «مولتی‌چین» پلتفرم ساختن زنجیره بلوک خود ارائه شده توسط «کوین‌ساینسز»، نشان می‌دهد که چه چیزی امکان‌پذیر است. در کنار ارائه امکان ساخت یک زنجیره بلوک عمومی همانند آن چه 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



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



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 باز هم می‌توان آن را مورد سؤال قرار داد. با اینکه این سیستم در دوران رنسانس در ایتالیا شروع شد، رشدش به اندازه رشد سرمایه‌داری در دنیا سریع نبود و تنها در اواخر قرن نوزدهم، خارج از ایتالیا به کار 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 حسابداری که دیگر نیازی به حفظ شدن توسط شرکت یا یک دولت ندارند، می‌توانند به مرور زمان تغییراتی را در چگونگی کارکرد شرکت‌ها و دولت‌ها به وجود آورند؛ اینکه چه چیزی از آنها انتظار می‌رود و چه چیزی بدون حضور آنها می‌توان انجام داد. رسیدن به این نکته که سیستم‌های غیر متمرکز ثبت وقایع به اندازه هم‌تایان مرکز‌گرایشان قابل اعتماد 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 است با مقاومت نیز روبه‌رو شوند. برخی از منتقدان بیت‌کوین آن را به صورت آخرین ابزاری برای گسترش «ایدئولوژی کالیفرنایی» که با وعده موفقیت با عدم مرکز‌گرایی مبتنی بر فناوری و در عین حال نادیده گرفتن واقعیت‌های قدرت‌ها عملاً 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، به خودی خود ایده جذاب و قدرتمندی نیست. در عین حال، 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.

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

رسو چه گفته بود؟

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

توزیع شده اترיום که محصول کار ویتالیک بوتترین، برنامه‌نویس ۲۱ ساله 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 بوتترین، چنین هوشی به ایجاد «سازمان‌های غیر مرکز‌گرای مستقل» - شرکت‌های مجازی وضع‌کننده قانون برای اجرا بر روی زنجیره بلوکی اترיום - کمک می‌کند.

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



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