چرا بیت‌کوین برای بانک‌داران اهمیت دارد؟

از آلن لین (Alan Lane) بپرسید؛ در ماه اکتبر 2013 رئیس و مدیرعامل «سیلورگیت بانک» در ساحل تپه‌ای «لا هویا» در کالیفرنیا، برای برگزاری نشستی با انجمن بانک‌داران کالیفرنیا و دپارتمان ایالتی نظارت بر بازرگانی رهسپار ساکرامنتو بود. جان لین اوون (Jan Lynn Owen)، رئیس کمیسیون مربوطه، ضمن مطالعه فهرستی اجمالی از میان تعداد زیادی موضوع و مسئله، درخصوص سیستم نظارتی این دپارتمان، درباره بیت‌کوین سخن گفت؛ همان واحد پول اینترنتی، سامانه و فناوری پرداختی که به تیتر خبرها تبدیل شده، بحث‌های زیادی را شعله‌ور کرده و در جهان الهام‌بخش نوآوری شده است. لین گوش‌هایش را تیز کرد، چون اتفاقاً مجموعه 616 میلیون دلاری سیلورگیت نیز حمایت بانکی از یک استارت‌آپ بیت‌کوینی را در دست بررسی داشت.

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

لین با یادآوری آن نشست می‌گوید: «دستم را بلند کردم و گفتم، آیا شخص دیگری هم هست که با مشتریان بالقوه بیت‌کوینی در حال گفت‌وگو باشد؟ خیلی از حضار هاج و واج به در و دیوار اتاق چشم دوختند. بسیاری از بانک‌داران حاضر در جلسه حتی اسم بیت‌کوین را هم نشنیده بودند... یکی از آن‌ها که یادم نیست چه کسی بود گفت: فکر می‌کنم اعتبار قانونی بیت‌کوین را از آن سلب کنند.»
لین پاسخ داد: «خب، اگر اعتبارش را از آن بگیرند من حدود 1200 دلار ضرر می‌کنم، چون این اواخر 10 بیت‌کوین خریده‌ام.» سپس یکی از بانک‌داران حاضر که رفیق لین بود برای این که سربه‌سرش بگذارد گفت: «آلن، تو نباید این موضوع را رو می‌کردی. حالا خودت را آماج حمله رگولاتورها قرار دادی.»
لین آن بیت‌کوین‌ها را با پول خودش خریده بود، نه به‌خاطر سرمایه‌گذاری، بلکه بیش‌تر به‌این خاطر که می‌خواست بداند این سیستم چگونه کار می‌کند. همان‌طور که خود لین می‌گوید، «اگر به درون (این سیستم) گام نگذارید چگونه می‌توانید درباره‌اش چیزی یاد بگیرید؟»
از زمان دیدار بانک‌داران کالیفرنیا به‌این سو، به‌نظر می‌رسد کنج‌کاوی و یادگیری درباره بیت‌کوین بیش‌تر و بیش‌تر از پیش ارزش خود را نمایان کرده است. نشست مشترک سنای امریکا، رگلاتورها، قانون‌گذاران و ناظران رسمی و حقوقی در ماه نوامبر سال گذشته نشان داد که بیت‌کوین به‌عنوان سیستم پرداخت‌ها، کاربردهای قانونی و خلاقانه‌ای دارد. به‌تازگی و پس از آن نیز تجارت‌خانه‌های نام‌آشنای این کشور مانند Overstock.com، زینگا و حتی تیم بسکتبال

ساکرامنتو کینگز پذیرش پرداخت‌های بیت‌کوین را آغاز کرده‌اند. حتی کاندیداهای سیاسی نیز کمک‌های انتخاباتی را از طریق این سیستم دریافت می‌کنند. با افزایش شمار کاربران بیت‌کوین تراکنش‌های جهانی آن نیز رو به افزایش است.
لین می‌گوید: «اگر بیت‌کوین به شیوه‌ای معتبر برای معاوضه پول تبدیل شود، آن گاه شرم بر ما بانک‌داران باد اگر آن را نفهمیم.»

فهم درست بیت‌کوین به معنی نگاه به ورای توان‌مندی‌های آن به‌عنوان جایگزینی برای پول است. تصور می‌شود که روزی این شبکه بتواند بسیار بیش‌تر از پول‌های الکترونیک و بدون مرز برای معاوضه پول مورد استفاده قرار بگیرد.

فهم درست بیت‌کوین (Bitoin با B برای اشاره به سیستم پرداخت و فناوری بیت‌کوین به‌کار می‌رود و با b برای اشاره به واحد پول بیت‌کوین) به معنی نگاه به ورای توان‌مندی‌های آن به‌عنوان جایگزینی برای پول است. تصور می‌شود که روزی این شبکه بتواند بسیار بیش‌تر از پول‌های الکترونیک و بدون مرز برای معاوضه پول مورد استفاده قرار بگیرد (به کاربردهای آن در ارتباط با اسناد مالیکت سهام یا حقوق مالکیت دارایی‌ها فکر کنید). اما چشم‌انداز درازمدت این سیستم برای آینده از نظر صاحبان سرویس‌های مالی سنتی که از دیرباز در سازوکارهای‌شان به اعتماد خود بر واسطه‌های طرف سوم (third party) متکی بوده‌اند، گیج‌کننده و سرسام‌آور است.
تاکنون بیش‌تر داستان‌های خبری درباره بیت‌کوین به بخش‌های جنجالی و ژورنالیستی آن پرداخته‌اند، از جمله: کاربردهای غیرمجاز این پول در بازارهای سیاه آنلاین؛ بنیان‌گذار مرموز آن که پیش از ناپدید شدنش در سال 2011 با نام مستعار ساتوشی ناکاموتو شناخته می‌شد؛ نرخ پر فراز و نشیب و دیوانه‌وار آن در معاوضه با دلار و استقبال آدم‌های مشهوری مانند دوقلوهای وینکلووس[1] از آن.
برآیند دیدگاه‌های آنلاین و گفت‌وگوهای توییتری سؤالی را فراروی‌مان قرار داده است: این‌که آیا بیت‌کوین ارزش ذاتی دارد؟ این بحث پایانی ندارد. روزنامه‌نگارانی که در حیطه‌های مالی قلم می‌زنند، این پدیده را از روزنه‌ای کوچک می‌نگرند و بانگ برمی‌آورند که ارزش بیت‌کوین مانند حبابی است که به‌زودی خواهد ترکید، متنفران حرفه‌ای فضای وبلاگ‌نویسی نیز گرایش‌های آزادی‌خواهانه و پیش‌بینی‌های تقریباً عجیب بیش‌تر هواداران مشتاق بیت‌کوین را به سخره می‌گیرند.
اما ناظران خردمندتر شایستگی‌های بیت‌کوین را در این می‌بینند که سامانه‌ای جهانی است و ناسازگاری ندارد؛ سیستمی که به بسیاری از پرسش‌های مقاله منتشر شده از سوی Federal Reserve در سال گذشته، پاسخی درخور و عالی می‌دهد؛ مقاله‌ای که در آن از همه خواسته شده بود درباره نحوه مدرن‌سازی زیرساخت‌های این کشور برای جابه‌جایی پول نظر بدهند.

جیمز وستر، از تحلیل‌گران محقق در IDC Financial Insights می‌گوید: «یکی از علت‌هایی که باعث شد با پرسش‌های زیادی روبه‌رو شویم و از ما سؤال شود که چرا آن نهاد فدرال بر مرمت سیستم کنونی و سنتی پرداخت تأکید دارد، این است که این سیستم در وضعیت فعلی کاستی‌هایی دارد. اما به‌نظر می‌رسد بیت‌کوین، تقریباً به‌صورت شانسی و تصادفی (بدون برنامه‌ریزی قبلی برای تحقق این هدف خاص) می‌تواند آن مشکلات را حل کند.» برای مثال، بیت‌کوین پرداخت‌ها را تقریباً بی‌درنگ انجام می‌دهد، چیزی که به گفته همین نهاد فدرال، آرزوی فزاینده کاربران عادی است و عموماً بسیاری از سیستم‌های کنونی پرداخت، از آن بی‌بهره‌اند.»
جرمی آلیر، مؤسس و مدیرعامل Circle internet Financial [2]، می‌گوید، این پول حداکثر در 60 دقیقه و اغلب حتی کم‌تر از آن پرداخت و در حساب مقصد مستقر می‌شود و روند کار هم به‌خوبی انجام می‌پذیرد. چنین سرعتی بسیار فراتر از سرعت جابه‌جایی پول با استفاده از تراکنش‌های اعتباری و نقدی (credit و debit) در سازوکارهای امروز است. از دید فروشندگان، جابه‌جایی پول با سامانه بیت‌کوین حتی بهتر است، زیرا، آن‌ها می‌دانند که پول را دریافت کرده‌اند و آن پول کجا است. بیت‌کوین یکی از خواسته‌های دیگر بانک مرکزی ایالات متحده (Federal Reserve) را هم برآورده می‌کند و آن کاهش هزینه‌ها به‌ویژه برای تراکنش‌های برون‌مرزی است. در سامانه بیت‌کوین انتقال از یک آدرس بیت‌کوین به آدرس دیگر رایگان است، مگر این‌که فرستنده بخواهد تراکنش خاصی را داشته باشد و هزینه‌اش را هم بپردازد که حتی در این‌صورت نیز هزینه‌ها به‌طور معمول چند پنی بیش‌تر نیستند و اغلب برای تأیید سریع‌تر تراکنش دریافت می‌شوند. البته، خرید و فروش بیت‌کوین در ازای پول قانونی به‌وسیله معاوضه آنلاین می‌تواند هزینه‌های بیش‌تری داشته باشد. اما، حتی در این‌صورت نیز استفاده از بیت‌کوین برای انتقال، می‌تواند ارزان‌تر از شیوه‌های پرداخت‌های سنتی تمام شود.
تحلیل آدام شایرو از Promontory Financial Group در سال گذشته، نشان داد که فرستادن یک هزار دلار از ایالات‌متحده به اروپا برای صرفه‌جویی در هزینه اجاره اقامت‌گاه‌های سفری با استفاده از شبکه بیت‌کوین (و با احتساب درصد دستمزدی که برای این مبادله اخذ می‌شود) با 15 دلار تمام می‌شود. این رقم اندک را با هزینه 50 دلاری انتقال برون‌مرزی پول با استفاده از کارت اعتباری و هزینه 40 تا 80 دلاری آن با شبکه‌های بین‌بانکی مقایسه کنید.
وستر می‌گوید: «نمی‌شود به بیت‌کوین چشم دوخت و گفت خب، معرکه است.» اگر بیت‌کوین می‌تواند در بعضی از این موارد کمک‌مان کند، پس شاید حتی بتواند بعضی از مشکلات را از سر راه بردارد و آن‌گاه شاید لازم باشد که دیگر به حرف‌هایی مانند این‌که بیت‌کوین حباب است و... پایان دهیم.
اما حتی این‌گونه تعریف و قدردانی‌ها از مزیت‌های سیستم پرداختی بیت‌کوین هم کافی نیست و قدیمی شده است. توان‌مندی بیت‌کوین در پرداخت‌ها حتی نیمی از قابلیت‌های آن هم نیست و مزیت‌های آن را باید بسیار فراتر از این‌ها دانست.

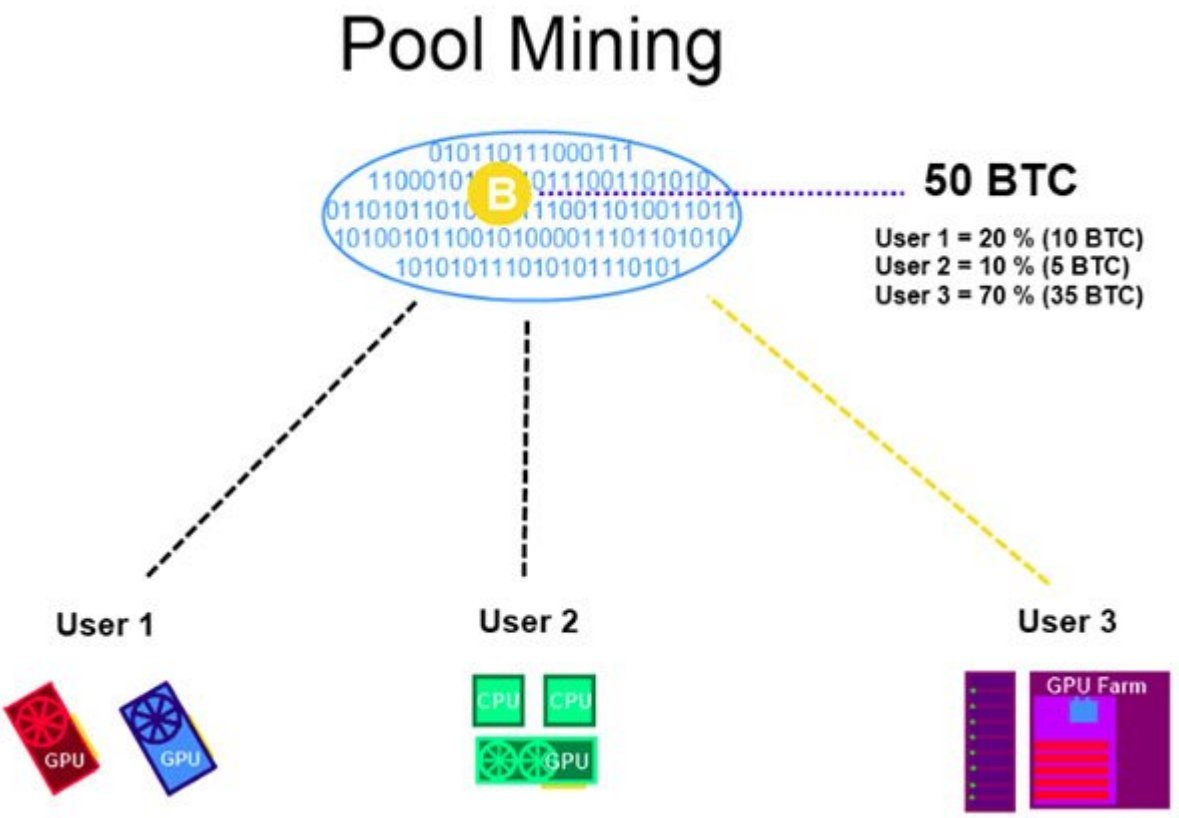
خرید و فروش بیت‌کوین در ازای پول قانونی به‌وسیله معاوضه آنلاین می‌تواند هزینه‌های بیش‌تری داشته باشد. اما، حتی در این‌صورت نیز استفاده از بیت‌کوین برای انتقال، می‌تواند ارزان‌تر از شیوه‌های پرداخت‌های سنتی تمام شود.

برای این‌که کاملاً مشخص شود چرا بیت‌کوین مهم است، نباید آن را فقط یک واحد پول و نه فقط یک سیستم پرداخت قلمداد کنید، بلکه باید آن را یک پروتکل بدانید. (هر پروتکل مجموعه‌ای از قوانین برای مبادله اطلاعات بین کامپیوترها در یک شبکه است. کاربردهایی که همه ما می‌شناسیم و عاشقشان هستیم، روی این پروتکل‌ها شکل گرفته‌اند. برای مثال، تار جهان گستر یا WWW روی پروتکل TCP/IP ایجاد شده است؛ پروتکلی که لایه زیرساختی اینترنت را تشکیل می‌دهد.)
قلب بیت‌کوین شبکه تراکنشی آن است، سیستمی نامتمرکز که به‌سرعت و به‌صورت عمومی به‌روز می‌شود و جزئیات تاریخ همه تراکنش‌ها روی شبکه را، از زمان پیدایش، در سال 2009 تاکنون، در خود دارد. این شبکه تراکنشی روی یک یا چند سرور محدود نشده است؛ بلکه زندگی خود را روی هزاران کامپیوتر در سراسر جهان پی می‌گیرد.
شاید شما درباره Bitcoin mining یا «بیت‌کوین‌کاوی» / «استخراج بیت‌کوین» چیزهایی شنیده باشید. این اصطلاح نام بی‌مسمایی است. کاری که در بیت‌کوین انجام می‌شود، بیش‌تر شبیه آن چیزی است که مقامات محلی یک ناحیه انجام می‌دهند. اما، چون استخراج معدن فرآیندی رقابتی است که درخلال آن هر معدن‌چی می‌کوشد ماده معدنی بیش‌تری را استخراج کند، برای به‌دست آوردن بیت‌کوین از عبارت mining یا معدن‌کاوی استفاده می‌شود.
کامپیوترهای بیت‌کوین‌کاوان در واقع با یکدیگر مسابقه می‌دهند تا مسئله ریاضی پیچیده‌ای را حل کنند که برای ثبت تازه‌ترین بلوک‌های تراکنش‌ها در Blockchain [3] لازم است. در این مسابقه که تقریباً هر10 دقیقه یک‌بار از نو آغاز

می‌شود، جایزه برنده 25 بیت‌کوین است که به تازگی صادر یا به‌عبارتی ضرب شده است. (همچنین، هزینه ناچیز تراکنش‌هایی که ارسال‌کنندگان برای جابه‌جایی سریع‌تر پول‌شان پرداخته‌اند و در بالا به‌آن اشاره شد). به همین سبب است که این فرآیند را کاویدن یا استخراج نامیده‌اند، زیرا، بیت‌کوین‌ها با این شیوه به چرخه اضافه می‌شوند؛ فرآیندی همچون استخراج طلا یا نقره از زمین، البته با این استثنا که معدن‌چیان بیت‌کوین برای این منظور به‌جای انجام دادن کارهای سخت، از برق و قدرت پردازش تراشه‌ها استفاده می‌کنند.

کامپیوترهای بیت‌کوین‌کاوان در واقع با یکدیگر مسابقه می‌دهند تا مسئله ریاضی پیچیده‌ای را حل کنند که برای ثبت تازه‌ترین بلوک‌های تراکنش‌ها در Blockchain لازم است. در این مسابقه که تقریباً هر10 دقیقه یک‌بار از نو آغاز می‌شود، جایزه برنده 25 بیت‌کوین است که به تازگی صادر یا به‌عبارتی ضرب شده است

اما یک پرسش این است که این مسابقه هیچ داوری ندارد، پس چه‌کسی مشخص می‌کند که آیا فلان بیت‌کوین‌کاو برنده شده است یا نه؟ پاسخ: بیت‌کوین‌کاوان دیگر! آن‌ها تنها درصورتی بلوک جدیدی را می‌پذیرند که همه تراکنش‌های آن معتبر باشد (یعنی هیچ‌کس تلاش نکرده باشد بیت‌کوینی را که آن‌ها ندارند، خرج کند) و آن‌ها با معطوف کردن توجه‌شان به محاسبه بلوک بعدی پذیرش خود را به همه اعلام می‌کنند. در این سیستم، رأی اکثریتی جایگزین تصمیم‌گیری متمرکز می‌شود.
در واقع، ناکاموتو کار ثبت رکوردها را به یک رقابت با انگیزه مالی تبدیل کرد که در آن شرکت‌کنندگان در هر جایی از جهان که باشند می‌توانند به خواست خود از مسابقه بیرون آیند یا به آن وارد شوند. ناکاموتو می‌خواست کاری کند که هر دو نفر در هر جای زمین بتوانند به‌صورت همتا به همتا (P2P) و بدون نیاز به نظارت و داوری یک میانجی یا طرف سوم مطمئن، تراکنش را به انجام برسانند. اگر یک بیت‌کوین‌کاو در اوکلند از گردونه کار خارج شود، همتایان او از ایسلند تا استرالیا می‌توانند ادامه کار را به‌دست بگیرند.
آندریاس ام آنتونوپولوس، از تکنولوژیست‌ها و کارآفرینان منطقه خلیج سان فرانسیسکو (Bay Area) که یکی از مشتاق‌ترین تبلیغ‌کنندگان دوآتشه بیت‌کوین است، می‌گوید: «نبود یک مرکز واحد برای بیت‌کوین به‌این معنی است که هیچ هدفی برای حمله وجود ندارد و قدرت در یک‌جا متمرکز نیست. قدرت بین کل این جامعه پراکنده و توزیع شده است. هیچ اهرمی وجود ندارد که کشیده شود (و بیت‌کوین را از حرکت باز دارد)، نقطه‌های خاصی وجود ندارند که آسیب‌آفرین باشند و این برای همه اطمینان‌بخش است.»
اما، چرا باید مردم به نرم‌افزاری اعتماد کنند که حتی پدیدآورنده‌اش شخصی مرموز و ناشناس است؟ نکته مهم این است که بیت‌کوین یک سیستم منبع باز است و کد زیرساختی آن نیز در دسترس همگان است. بنابراین، هر کسی می‌تواند آن را بررسی کند.



گاوین آندرسن، دانشمند ارشد بنیاد بیت‌کوین که رویکرد بنیاد متبوعش در ارتباط با بیت‌کوین تجاری است، می‌گوید: «خوره‌ای مثل من می‌تواند کد منبع آن‌را بررسی کند. برای ما مهم نیست چه کسی آن را نوشته است.» او می‌افزاید: «ریاضی‌دانی را تصور کنید که به تئوری شخصی استناد می‌کند که از او متنفر است. شما واقعاً اهمیتی نمی‌دهید که این ایده از کجا آمده است؛ برای شما خود این ایده اهمیت دارد.»

آندرسن می‌گوید: «در عمر پنج ساله بیت‌کوین صدها آدم فنی ماهر آن را بررسی کرده‌اند، هم هکرهای کلاه‌سپید و هم هکرهای کلاه‌سیاه این فرصت را داشته‌اند تا شانس خود را برای رخنه در آن بیازمایند و هیچ‌کس موفق نشده است.» اندرسن در جایگاه توسعه‌دهنده ارشد هسته نرم‌افزار بیت‌کوین می‌گوید:«درست است که او و بنیاد بیت‌کوین که در سال 2012 شکل گرفت، بر آن تأثیر می‌گذارند اما مدل راهبری بیت‌کوین مانند مدل رهبری خود اینترنت بسیار توزیع‌شده و بسیار گسترده است.»

او می‌افزاید: «کل این سیستم شلوغ و بی‌نظم است و مانند سیستم‌های متمرکز ساختار بالا به پایین ندارد. هیچ‌کسی نیست که 100 درصد در رأس آن باشد.» و درست همان‌طور که چیدمان نامتمرکز اینترنت به تیم برنرزلی اجازه داد تا وب را بدون اجازه کسی پدید آورد، پروتکل بیت‌کوین نیز این امکان را فراهم‌آورده است تا در حاشیه blockchain کاربردهای نوآورانه‌ای شکل بگیرند.

نمونه ساده‌ای از آن سرویس Proof of Existence است؛ سرویسی برای ثبت رسمی که توسط مانوئل آرائوز، توسعه‌دهنده نرم‌افزار در آرژانتین پدید آمده است. این سایت به همه اجازه می‌دهد تا اثرانگشت رمزنگاری‌شده و تاریخ‌داری را (که نوعی رشته hash یا درهم‌ریخته است)، از هر سندی به blockchain ضمیمه کند. کاربر می‌تواند بعدها ثابت کند که آن سند در فلان زمان موجود بوده است، حال آن سند چه یک درخواست مکتوب باشد، چه یک سند مالکیت، پتنت، فیلمنامه، نامه عاشقانه یا هر چیز دیگری. ذخیره این اسناد در blockchain به این معنی است که رکورد ثبت‌شده‌ای از آن به‌صورت عمومی همیشه و همه‌جا در دسترس است. البته، برای توضیح دقیق‌تر موضوع باید افزود، این به‌معنی علنی کردن خود سند نیست. درهم‌سازی یا hash تابعی یک‌سویه است؛ اگر همه آن‌چه که دارید یک hash یا داده‌های رمزشده از سند باشد، نمی‌توانید آن را مهندسی معکوس کنید تا به داده‌های اصلی دست بیابید. اما اگر هر دو را داشته باشید (هم سند و هم hash را) می‌توانید ثابت کنید که آن hash خاص متعلق به مجموعه داده‌های خاصی است. در واقع کسی که به هر دوی آن‌ها دسترسی دارد، صاحب سند است. حتی کوچک‌ترین تغییرها در این داده‌ها به پدیدآمدن یک hash یا رشته درهم‌ریخته کاملاً متفاوت منجر می‌شود. برای مثال، با اعمال تابع SHA-256(الگوریتم درهم‌ساز رایج در بیت‌کوین)روی واژه pickle، رشته‌ای 64 حرفی به‌صورت زیر ساخته می‌شود:

6d08a4e630e4aa0d5cd873e65aea0a23df42de61073ecb49ef17158fe6a9dcea.

اما، اگر به آخر این واژه حرف s را بیافزایید رشته درهم‌ریخته شما به‌صورت زیر درمی‌آید که رشته‌ای با همان تعداد حرف است اما بسیار متفاوت از مورد نخست خواهد بود:

3614e3639c0a98b1006a50ffe5744f054cf4499592fe8ef1b339601208e80066

[illegible] *FDIC* [illegible]

[illegible] *(FDIC)* [illegible] *FDIC* [illegible]

[illegible] *Elliptic* [illegible] *wallet* [illegible] 9 [illegible] *(Lloyd)* [illegible] *Inscrypto* [illegible] *(Derivatives)* [illegible] *Founder Shield* [illegible]

[illegible]

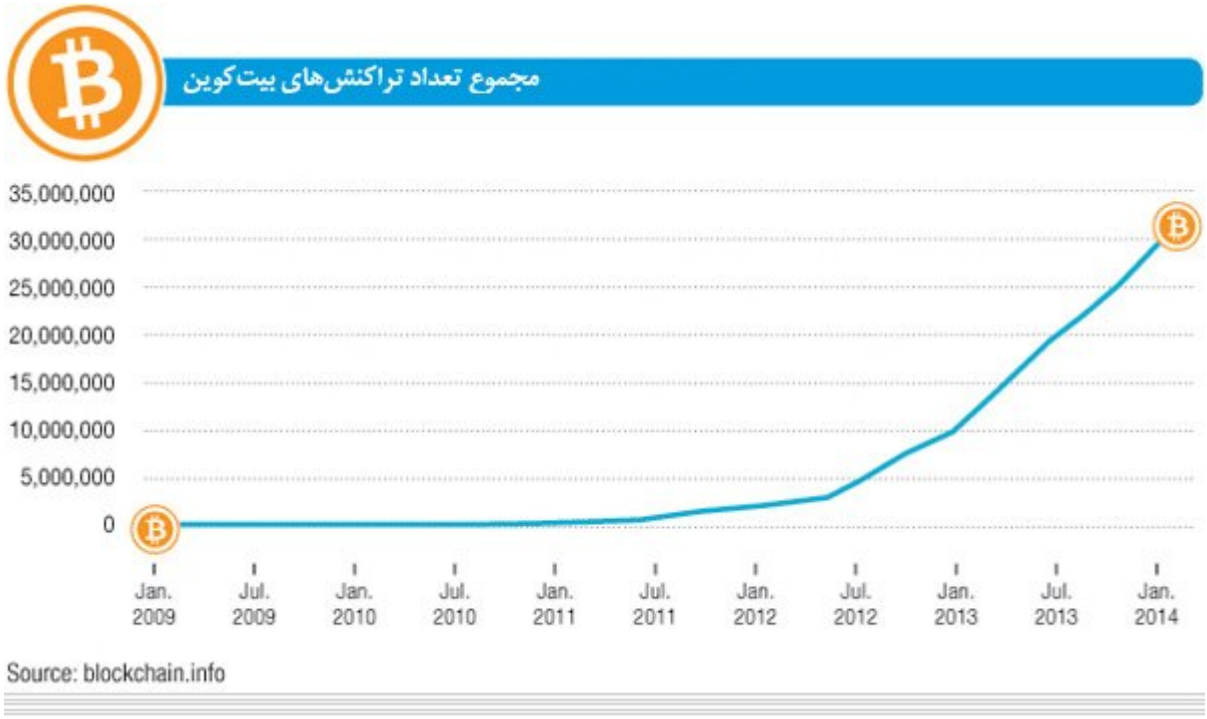
[illegible] *(SIPC)* [illegible]

[illegible] *Nesenoff & Miltenberg LLP* [illegible] *FDIC* [illegible] *FDIC* [illegible]

[illegible] *Coinbase* [illegible] *wallet* [illegible] *Mercatus* [illegible]

وقتی می‌گوییم فناوری بیت‌کوین راه‌کار نامتمرکزی را ارائه می‌دهد، معنی‌اش این است که می‌توانید مطمئن باشید اهمیتی ندارد برای این‌کار از چه برنامه‌ای استفاده می‌کنید زیرا در هر صورت می‌توانید به داده‌ها اعتماد کنید. به این دلیل‌که توسط هیچ شخص/نهاد/مرکز میانجی و طرف سومی تغییر نخواهند یافت.
ایده پیشرفته‌تری نیز که روند توسعه خود را می‌پیماید، ایده سکه‌های رنگی است. سکه‌های رنگی بیت‌کوین‌هایی هستند که به‌صورت دیجیتال در blockchain نشانه‌گذاری شده‌اند و ارزش ثانویه‌ای دارند که چیزی جدا از ارزش نقدی بیت‌کوین است. یک سکه رنگی می‌تواند مالکیت یک سهم، وام‌برگه یا دیگر گونه‌های سرمایه را نشان دهد. روی کاغذ، بیت‌کوین می‌تواند به‌عنوان ستون فقرات بازار جهانی سرمایه خدمت کند؛ جایی که شرکت‌ها می‌توانند اوراق بهادار صادر کنند و بر واسطه‌هایی مانند مراکز مبادله بانکی کم‌تر متکی باشند.
باری سیلبرت، مدیرعامل شرکت کارگزاری SecondMarket در نیویورک، می‌گوید، سرشت نامتمرکز بیت‌کوین در

کنار درهای گشوده فهرست حساب‌هایش و این‌که دو شخص روی شبکه که نه یکدیگر را می‌شناسند و نه به واسطه‌ای نیاز دارند، می‌توانند تراکنش خود را به انجام برسانند به‌راستی امکاناتی را به‌روی بیت‌کوین می‌گشاید که می‌توان از آن‌ها به‌عنوان شیوه‌های خاص و منظم تراکنش‌های مالی بهره برد.
این بازار صرف‌نظر از به‌کارگیری واسطه‌ها و حسابرسان ویژه باید سازگاری‌اش را بیش از این‌ها افزایش دهد. گیل لوریا، از تحلیل‌گران Wedbush Securities که چرخه بیت‌کوین را مورد مطالعه قرار داده است، می‌گوید، این چرخه به سیستم مبادله سهام نیویورک یا بازار بورس نزدک (NASDAQ) که ممکن است دچار رکود شود و چنین هم می‌شود، وابسته نیست. بلکه به سازوکاری متکی است که نقطه آسیب‌پذیری ندارد.
جاناتان موهان، مؤسس BitcoinNYC، (یک گروه شبکه‌ساز بیت‌کوین در نیویورک) سکه‌های رنگی را به پاکت‌های نامه تمبردار تشبیه می‌کند (در این‌جا بیت‌کوین رنگی نقش تمبری را بازی می‌کند که با وجود آن محتوای پاکت می‌تواند در سیستم پستی جابه‌جا شود.) باتوجه به نرخ کنونی بیت‌کوین شاید بگویید که چندصددلار برای یک تمبر پستی خیلی زیاد است. اما، بیت‌کوین‌ها تا هشتمین رقم اعشار نیز بخش‌پذیر هستند. بنابراین، صادرکننده عملاً می‌تواند حتی یک هزارم بیت‌کوین را نیز در ازای 80 سنت (بسته به قیمت روز) تصاحب کند، آن را به‌صورت یک سهم یا وام برگه برچسب‌گذاری و سپس برای توزیع میان سرمایه‌گذاران به بیت‌های کوچک‌تری تقسیم کند.
حتی کاربردهای فرضی بیش‌تری از بلاک‌چین درباره مفاهیم مرتبط با دارایی‌های هوشمند، قراردادهای هوشمند، و پول‌های برنامه‌پذیر مطرح است. در ابتدایی‌ترین شکل تراکنش بیت‌کوین، اگر برای مثال باب بخواهد برای آلیس یک بیت‌کوین بفرستد، به دو قطعه اطلاعات نیاز دارد: کلید خصوصی خودش و یک آدرس تولیدشونده از کلید عمومی آلیس. هر کسی می‌تواند به نشانی بیت‌کوین پول بفرستد، اما تنها کسی می‌تواند این پول را برداشت کند که کلیدخصوصی را دراختیار داشته باشد و تراکنش مربوطه را با این کلید امضا کرده باشد.
تصور کنید که آن کلید خصوصی کلید یک خودرو می‌بود، در این‌صورت چه اتفاقی می‌افتاد؟ در چنین سناریویی، دارنده خودرو می‌توانست وسیله نقلیه را طوری پیکربندی کند که تنها درصورت دریافت پیغامی روشن شود که توسط کلیدخصوصی (و دارای سکه رنگی) امضا شده بود.
لوریا با ذکر مثالی می‌گوید، اگر بخواهد برای خرید خودروی تسلا از بانک وام بگیرد (شرکت خودروسازی تسلا پرداخت‌های بیت‌کوین را می‌پذیرد) تا زمانی که قسط‌های وامش را پرداخت کند، بانک این موضوع را در blockchain منعکس می‌کند و او می‌تواند از خودروی خود استفاده کند. اما اگر لوریا پرداخت قسط‌ها را متوقف کند (و درنتیجه blockchain نیز پیغامی دریافت نکند که نشان دهد او در آن ماه قسط بانکش را پرداخته است)، به‌جای این‌که وکلا و مسئولان جمع‌آوری قرض‌ها و ضبط‌کنندگان دارایی از طرف بانک وارد عمل شوند، خود بانک می‌تواند خودروی تسلای لوریا را تقریباً به‌طور مستقیم از کار بیاندازد طوری که او نتواند از آن استفاده‌کند.
از آنجا که همه‌چیز در blockchain ضبط می‌شد، هر دو طرف می‌توانستند ببینند که دقیقاً چه اتفاقی افتاده است و هیچ‌یک از دو طرف نمی‌توانست دیگری را فریب دهد. بدهکاران بانک نمی‌توانستند بهانه بیاورند که ایمیل‌شان را چک نکرده‌اند و دست بعضی از بستان‌کاران نیز از انجام کارهای غیرمسئولانه کوتاه می‌شد (مثل مواقعی که شما قسط را تحویل مأمور مربوطه می‌دهید اما او پرداخت آن‌را به‌موقع ثبت نمی‌کند و دیرکردش به‌پای شما نوشته می‌شود.) علاوه‌بر این، بدهکار هم نیازی نداشت حریم خصوصی خود را قربانی کند. از آن‌جا که نشانی‌های بیت‌کوین رشته‌های حرفی-عددی مستعار هستند، دیگرانی که به بلاک‌چین می‌نگرند الزاماً نمی‌دانند دو طرف دادوستد چه کسانی هستند. همه آن‌چه که می‌توان دید این است که چگونه و چه زمانی انبوهی از بیت‌کوین‌ها از مبدأ A به مقصد B منتقل می‌شوند.



پیش‌بینی آنتونوپولوس این است که سرانجام بیت‌کوین حیطه جدیدی را به‌روی قانون محاسبات خواهدگشود که ضمن آن قراردادها (اعم از وام‌ها، فروش دارایی‌ها یا توافق‌نامه‌های خدماتی و...) اغلب به‌صورت برنامه‌های کامپیوتری «خود اجرا» نوشته می‌شوند و بسیاری از خطرهای تجاری به‌سادگی از میان برداشته می‌شود.
آنتونوپولوس می‌گوید، در این‌صورت وکلا (در نوشتن و تنظیم سندها) بیش‌تر بر خواسته‌های دو طرف قرارداد متمرکز خواهند شد تا بر فرونشاندن دعاوی یا داوری کردن درباره دعاوی کاربران. البته تا رسیدن به چنین جایگاهی راه زیادی در پیش است. همان‌طور که لین در نشست بانک‌داران کالیفرنیا شاهد بود، بیش‌تر بانک‌های امریکا هنوز درخصوص مشارکت در اقتصاد بیت‌کوین حتی در عادی‌ترین شکل آن (باز کردن حساب سپرده برای مبادله ارزهای مجازی) دست به عصا راه می‌روند.
تونی گالیپی، مدیرعامل BitPay در آتلانتا، شرکتی که کارش پردازش پرداخت‌ها است، تابستان پارسال در کنفرانسی گفت، هر کسب‌وکار بیت‌کوین دست‌کم باعث شده است تا یک حساب بانکی بسته شود. برای بسیاری از بانک‌داران، آیین‌نامه منتشر شده در سال گذشته توسط شبکه نظارت بر جرائم مالی(وابسته به وزارت خزانه‌داری امریکا)، برای این‌که استارت‌آپ‌ها را به همگان بشناساند کافی نبوده است. این آیین‌نامه، شرکت‌های فعال در بخش پول‌های مجازی را نیز همچون همکاران‌شان در بخش تجارت پول‌های سنتی، به رعایت همان قوانین معروف شناخت مشتری (know-your-customer) [5] ملزم می‌کند.
بروس والاس، مدیر ارشد عملیاتی SVB Financial Group، (شرکت مادر «سیلیکون ولی بانک» در سانتا کلارای کالیفرنیا) می‌گوید، چالش فعلی و بسیاری از بی‌میلی‌های مؤسسه‌های مالی به ارائه سرویس‌های بانکی برای شرکت‌های بیت‌کوین به‌این علت است که آن‌ها به راهنمایی رگلاتورها نیاز دارند.
این بانک با سرمایه 22 میلیارد دلاری خود در مقایسه با مؤسسه دیگر برای شرکت‌های نوآور جاذبه بیش‌تری دارد و تعداد معدودی هم مشتری پول مجازی دارد که البته دیگر مشتریان بیش‌تری را نمی‌پذیرد. والاس می‌گوید: «در حال حاضر، مشکلاتی داریم. ما باید برای کمک به رگلاتورها بیش‌تر زمان بگذاریم و باید بکوشیم مؤسسه‌ها و بانک‌هایی را که نمی‌خواهند برای پی‌بردن به نحوه پشتیبانی بانکی از شرکت‌های فعال در حیطه پول مجازی زمان بیش‌تری بگذارند درست راهنمایی کنیم.»
او همچنین می‌گوید یکی از مشکلاتی که رگلاتورهای فدرال باید حل کنند این است که مشخص کنند یک بانک پس از آن‌که مشتریان ِ مشتریانشان، دلارهای خود را به پول‌های مجازی یا برعکس تبدیل کردند عملکرد آن‌ها تا کجا باید تحت نظارت قرار بگیرد. او می‌افزاید امروز، اگر یک مشتری به بانک برود و 5000 دلار به‌صورت نقد از حساب برداشت کند، بانک به یقین باید بداند که او 5000 دلار به‌صورت نقد گرفته است. اما از آن‌جا به بعد برای بانک ممکن نیست بداند مشتری با پولی که گرفته است چه‌کار می‌کند. موضوع بدیهی این است که بیت‌کوین که ویژگی‌هایی از انتقال پول نقد و سرمایه الکترونیک را همزمان یک‌جا دارد در هیچ‌یک از این‌دو شاخه نمی‌گنجد.
والاس می‌گوید، وقتی نمی‌توانید بدانید بیت‌کوین را با چه کسانی دادوستد می‌کنند، وقتی تمام آن‌چه که می‌دانید

نشانی کیف‌پول (wallet) است، برای یک مؤسسه مالی سخت است که بگوید، بله، ما می‌توانیم با اطمینان گزارش بدهیم که وقوع آن تراکنش را دیدیم و طرف دیگر تراکنش یک third party قانونی بوده است که هویتش را می‌دانیم و از علت انجام این تراکنش هم آگاه هستیم.
اما، چون گستره امکاناتی که بلاک‌چین در اختیارمان می‌گذارد وسیع و گوناگون است هنوز این پرسش مطرح است که آیا بانک‌ها خرید بیت‌کوین را ردگیری و دنبال کنند یا این‌که آن‌را فرآیندی همچون برداشت پول از ماشین‌های خوردپرداز به‌حساب آورند. (والاس می‌گوید شخصاً برایش مهم نیست رگلاتورها به‌کدام سو متمایل شوند، آن‌چه که در حال حاضر اهمیت دارد این است که آن‌ها ابعاد گوناگون بیت‌کوین را تشریح کنند و آن‌را به همگان بشناسانند.)
اما سامان‌دهی بیش‌تر در این حیطه، چه تضمینی باشد و چه نه، بیت‌کوین را در دستیابی به حداکثر توان‌مندی‌های خود با خطر مواجه خواهدکرد. لوریا در ودبوش می‌گوید: «هیچ دولتی نمی‌تواند بیت‌کوین را نابود کند. هیچ رگولاتوری نمی‌تواند بیت‌کوین را خاموش کند. اما آن‌ها می‌توانند از پیشرفت و نوآوری بیت‌کوین، به‌ویژه در کشور خودشان جلوگیری کنند.»
مورد دیگری که گسترش بیت‌کوین را، به‌عنوان سیستم پرداخت، با مشکل مواجه می‌کند نرخ گریزپا و دائماً متغیر آن است. البته چند سرویس پردازشگر بیت‌کوین مانند BitPay و Coinbase با تبدیل بی‌درنگ پرداخت‌های بیت‌کوین به دلار این مشکل را برای صاحبان کسب‌وکار آسان کرده‌اند. اما چون کسی نمی‌داند تفاوت بهای بیت‌کوین از یک روز تا روز دیگر چقدر است، مشتریانی که غیر از گروه هسته بازرگانان، کنجکاوان و هواداران دو آتشه این پول هستند، تمایل‌شان نسبت به‌این پول کند خواهد بود.

سازوکار کاویدن و استخراج بیت‌کوین هنوز با چشم‌انداز بنیادی و مدنظر ناکاموتو که می‌گفت، «یک سی‌پی‌یو، یک رأی»، فاصله دارد. با رقابتی‌تر شدن این تجارت، کاوندگان بیت‌کوین به‌هم پیوستند و گروه‌های کاونده تشکیل دادند، تولیدکنندگان سخت‌افزار تراشه‌های قدرتمندی را معرفی کردند که به‌آن‌ها ASIC گفته می‌شود و به‌طور ویژه برای استخراج بیت‌کوین طراحی شده‌اند

اندرسن، از بنیاد بیت‌کوین، می‌گوید «گریزپایی» یا نرخ دائماً متغیر بیت‌کوین مسئله و مشکلی روشن است. اگر قرار است بیت‌کوین به‌راستی به یک سیستم پرداخت ماندگار تبدیل شود، باید نرخ آن بسیار پایدارتر از آنی باشد که اینک شاهدش هستیم. اما، آیا ممکن است پولی که برخلاف بسیاری از پول‌های دیگر جهان، از سوی هیچ دولتی و هیچ مالیاتی پشتیبانی نمی‌شود به چنین ثباتی برسد؟ آلیر، از Circle Financial، می‌گوید که اگر سرمایه‌گذاران بزرگ (مانند بانک‌ها، شرکت‌های بیمه و...) وارد ماجرا شوند، ارزش بیت‌کوین می‌تواند به ثبات برسد. برای مثال، شرکت متبوع سیلبرت موسوم به (SecondMarket)، سال گذشته برای سرمایه‌گذاران شایسته و مخاطره‌پذیر، شرکت ویژه‌ای را راه‌اندازی کرد که (Bitcoin Investment Trust) نام دارد؛ برادران وینک‌لووس نیز، که به‌خاطر کشمکش‌هایشان با مارک‌زاکربرگ بر سر پیدایش فیس‌بوک به شهرت رسیدند، هنوز برای طرح خود درخصوص صندوق بازرگانی معاوضه بیت‌کوین منتظر تأییدیه کمیسیون بورس و اوراق بهادار امریکا (SEC) هستند. بیت‌کوین به‌عنوان سیستم پرداخت یک ویژگی جذاب امنیتی دارد: این‌که در واقع یک سیستم Push است و نه Pull.از این‌رو، هرگاه فرآیند پرداخت در این سیستم آغاز می‌شود، دارنده حساب نقشی فعال بازی می‌کند. این درحالی است که در سیستم‌های پرداخت Pull، مشتری کارت اعتباری یا شماره حساب بانکی خود را به فروشنده یا حسابرس می‌دهد و به او اعتماد می‌کند که در واقع یک واسطه یا طرف سوم (third party) است و امیدوار است که اطلاعات او را امن نگاه دارند. در واقع در سیستم‌های Pull مشتری نقش فعالی ندارد، بلکه پسیو یا منفعل است. تجربه‌های گوناگون امنیتی نشان داده‌اند که سیستم Push در مقایسه با سیستم‌های Pull یا سیستم‌های ترکیبی Push & Pull مزیت بیش‌تری دارند.
اما ضعف‌های بالقوه دیگری هم در شبکه بیت‌کوین وجود دارد. شاید بزرگ‌ترین مخاطره این سیستم در درازمدت امکان بروز حمله‌های به‌اصطلاح «51 درصدی» باشد. در چنین وضعیتی یکی از اعضای شبکه کنترل بیش‌تر امکانات استخراج بیت‌کوین را به‌دست می‌گیرد و شرایط نابسامانی به‌بار می‌آورد. از جمله این‌که می‌تواند سکه‌ها را با دوبرابر ظرفیت متعارف پرداخت کند یا از پردازش تراکنش‌های کاربران دیگر جلوگیری کند.
در حال حاضر، سازوکار کاویدن و استخراج بیت‌کوین هنوز با چشم‌انداز بنیادی و مدنظر ناکاموتو که می‌گفت، «یک سی‌پی‌یو، یک رأی»، فاصله دارد. با رقابتی‌تر شدن این تجارت، کاوندگان بیت‌کوین به‌هم پیوستند و گروه‌های کاونده تشکیل دادند، تولیدکنندگان سخت‌افزار تراشه‌های قدرتمندی را معرفی کردند که به‌آن‌ها ASIC گفته می‌شود و به‌طور ویژه برای استخراج بیت‌کوین طراحی شده‌اند و علاوه‌بر این‌ها، مسئله‌های ریاضی نیز که استخراج بیت‌کوین تنها با حل آن‌ها ممکن می‌شود سخت‌تر شدند. سال گذشته اتفاق جالب و در خور توجهی روی داد و خطر از بیخ گوش

بیت‌کوین گذشت، زیرا نزدیک بود یکی از گروه‌های کاونده بیت‌کوین (بدون قصد قبلی و بی‌آن‌که درصدد خرابکاری باشد) کنترل 51 درصد از کل قدرت پردازشی این شبکه را به انحصار خود درآورد. اما چون همه و از جمله خود این گروه می‌دانستند و می‌دانند که ارزش بالای بیت‌کوین به‌خاطر استقلال و غیرانحصاری بودن آن است گروه یادشده هر بار خردمندانه پس نشست و خودش منابع را آزاد کرد.
لوریا می‌گوید، مشارکت‌کنندگان به‌حدی نسبت به موفقیت بیت‌کوین مشتاق و علاقه‌مند هستند که حتی وقتی مواردی همچون رویداد فوق بروز می‌یابد خود این سیستم (مجموعه کاربران و مشارکت‌کنندگان) خودش را تصحیح می‌کند تا کل شبکه زیر سؤال نرود. البته بدیهی است که چنین مکانیسمی و مزیتی می‌تواند در بعضی موقعیت‌ها به یک ضعف تبدیل شود، اما دست‌کم فعلاً اشخاص ذی‌نفع در این شبکه می‌کوشند خطر یادشده را مدیریت کنند و از آن به‌دور باشند.
اندرسن پیش‌بینی می‌کند که در آینده تولیدکنندگان تراشه‌های کاونده بیت‌کوین آن‌ها را به کوچک‌ترین و باصرفه‌ترین شکل ممکن مهندسی خواهندکرد و درنتیجه این تراشه‌ها هم ارزان خواهندشد و هم به‌صورت انبوه در دسترس خواهندبود. او می‌گوید: «تراشه‌های کاونده روزی چنان همه‌گیر خواهندشد که شاید وقتی یک بسته خوراکی یا تنقلات می‌خرید، به‌همراه آن یک دستگاه تراشه ASIC هم جایزه بگیرید. در این‌صورت سازوکار کاوش و استخراج بیت‌کوین بسیار و بسیار بیش‌تر از آن‌چه که امروز می‌بینیم نامتمرکز خواهدشد و این‌جا است که دیدگاه مدنظر ناکاموتو می‌تواند به واقعیت تبدیل شود؛ «یک تراشه کاونده، یک رأی.»
در چنین سیستمی حتی اگر روزی برنامه‌ای مخرب کنترل بیت‌کوین را به‌دست بگیرد، یا دولت یک کشور (در محدوده خود) آن‌را از کار بیاندازد، یا ارزش آن سقوط کند، می‌توان در برابرش ایستاد.
هم‌اکنون رمزپول‌های مبتنی‌بر Blockchain دیگری نیز سر درآورده‌اند. تا اواسط ژانویه امسال سایت Cryptsy تعداد 117 پول مشابه دیگر را فهرست کرده‌بود. به‌نظر می‌رسد بسیاری از آن‌ها همچون Dogecoin و Coinye West یا بازارگرمی یا حقه‌هایی فرصت‌طلبانه برای سود بردن از وضعیت پدیدآمد باشد. اما این‌طور که پیدا است بعضی از رمزپول‌ها مانند Ethereum که در مقایسه با بیت‌کوین از زبان برنامه‌نویسی زیرساختی کارآمدتری بهره برده‌اند، تلاشی جدی دارند و برای کاربردهای پیشرفته‌ای همچون پول هوشمند طراحی شده‌اند.
آنتونوپولوس اختراع Blockchain را با شکافت هسته‌ای مقایسه می‌کند. او می‌گوید، ابتدا شکافت هسته‌ای کشف می‌شود، بعد ساختمانی که یک راکتور هسته‌ای در درونش جای گرفته، ساخته می‌شود و سپس برقی که از آن تولید می‌شود، پدید می‌آید. اما همه در اندیشه قیمت برق تمام‌شده‌ای هستند که از این راکتور بیرون می‌آید و توجه نمی‌کنند که شکافت هسته‌ای به‌خودی خود تا چه‌اندازه مهم است و به‌راستی فیزیک و انرژی و همه‌چیز را تغییر داده است. شاید شما بتوانید جلوی برق را بگیرید، شاید بتوانید راکتورها را تحت مدیریت و کنترل خود درآورید. اما بدیهی است نمی‌توانید مردم را وا دارید تا وجود پدیده شکافت هسته‌ای را از یاد ببرند و نمی‌توانید این کشف را از میان ببرید.
لین، مدیرعامل بانک سیلورگیت، هنوز هیچ استارت‌آپی را که در حیطه بیت‌کوین فعال است، پشتیبانی نمی‌کند، اما می‌گوید با Coinsetter، از سرویس‌های معاوضه پول مجازی، در حال گفت‌وگو است و این سرویس برنامه‌ای را ارائه کرده که از نظر لین فوق‌العاده دقیق است. لین می‌گوید، اگر بتوانیم راهی پیدا کنیم تا این برنامه به مرحله اجرا دربیاید و اگر بتوانیم کاری کنیم که رگلاتورهای‌مان با آن کنار بیایند، همه هوادار آن خواهیم بود.
لین انتظار ندارد که بسیاری از همتایان بانک‌دار او خیلی زود به بررسی بیت‌کوین علاقه‌مند شوند که چه‌بسا حتی بررسی آن در گذر زمان نیز به‌سختی و کندی پیش برود. خود او نیز هنوز با بیت‌کوین‌هایی که خریده است کلی کار دارد. به‌گفته لین، مدیرعامل بانک باید نگران خیلی چیزها باشد. او می‌گوید، اگر همکاران بانک‌دارش علاقه‌مند شوند درباره بیت‌کوین بیش‌تر بدانند اما همزمان با ایده‌های غیرمسئولانه در این‌خصوص مخالفت کنند، آن‌ها را سرزنش نمی‌کند.
با این‌حال، او می‌گوید، از میان تمام چیزهایی که شاید روزی به آن‌ها علاقه‌مند شوید، چه مالی باشد، چه فنی، چه درباره سیستم پرداخت‌ها و...، بیت‌کوین برای او از همه‌شان بالاتر ایستاده‌است و او مایل است درباره‌اش بیش‌تر بیاموزد. از همین‌رو است که می‌گوید: «هرچه بیش‌تر (درباره‌اش) آموختم، بیش‌تر گفتم عجب، این خیلی عالیه.»

پانویس

1. منظور از دوقلوهای وینکلووس (Winklevoss twins)، کامرون و تایلر وینکلووس، ورزشکاران حرفه‌ای رشته قایقرانی، کارآفرین و مؤسس ConnectU (پیش‌تر HarvardConnection) است که ارائه دادخواست آن‌ها علیه مارک زاکربرگ، مؤسس فیس‌بوک، و ادعای این‌که او ایده فیس‌بوک را از ConnectU ربوده است، مشهورشان کرد.
2. استارت‌آپی واقع در بوستون که هدفش کسب بیت‌کوین به‌شیوه‌ای ساده‌تر برای خرید و کاربردهای روزانه است
3. Blockchain فایلی کامپیوتری و عمومی است که همه تراکنش‌ها در آن ثبت می‌شوند و همه کاربران می‌توانند

آن‌را بررسی کنند. برای مطالعه تعریف برخی از واژه‌های کلیدی در سیستم بیت‌کوین به اینفوگرافی «راهنمای مفاهیم پایه بیت‌کوین» مراجعه کنید.
4. این آدرس
5. قانون شناخت مشتری یا know your costumer؛ این آدرس را ببینید.

فایل پیوست:

پیوست	اندازه
اینفوگرافی مبانی بیت کوین را از اینجا دانلود کنید	83.59 کیلوبایت

منبع:
امریکن بانکر
تاریخ انتشار:
25 مرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/cover-story/1263