کریپتوکارنسی

چاپ سوم

پول دیجیتال چطور می‌تواند فایننس را متحول کند

جیان وُلپیسلی

محمد رهبان

WIRED

فایل نمونه


بسم الله
الرحمن
الرحيم

سرشناسه: وُلپیسلی، جیان-Volpicelli, Gian
عنوان و نام پدیدآور: کریپتوکارنسی: پول دیجیتال چطور می‌تواند فایننس را متحول کند/ جیان وُلپیسلی
مشخصات نشر: تهران: راه پرداخت، ۱۴۰۰.
مشخصات ظاهری: ۱۱۱ص.؛۱۴/۵×۲۱/۵ س‌م.
شابک: ۶-۱۵-۷۷۰۲-۶۲۲-۹۷۸
وضعیت فهرست‌نویسی: فیپا
یادداشت: عنوان اصلی: Cryptocurrency (WIRED guides): How Digital Money Could Transform Finance
عنوان دیگر: پول دیجیتال چطور می‌تواند فایننس را متحول کند.
موضوع: بیتکوین-Bitcoin
موضوع: انتقال الکترونیکی وجوه- Electronic funds transfers
موضوع: بلاک‌چین (پایگاه‌های اطلاعاتی)-Blockchains (Databases)
شناسه افزوده: رهبان، محمد، ۱۳۶۷-، مترجم
شناسه افزوده: والی، مینا، ۱۳۶۳-، ویراستار
شناسه افزوده: سرافرازی، قاسم، ۱۳۶۶-، ویراستار
رده بندی کنگره: HG۱۷۱۰
رده بندی دیویی: ۳۳۲/۱۷۸
شماره کتابشناسی ملی: ۸۷۲۱۵۳۵

کریپتوکارنسی

پول دیجیتال چطور می‌تواند فایننس را متحول کند

جیان وُلپیسلی

محمد رهبان

WIRED

عنوان : کریپتوکارنسی؛ پول دیجیتال چطور می‌تواند فایننس را متحول کند
ناشر : راه پرداخت
نویسنده: جیان وُلپیسلی
مترجم: محمد رهبان
ویراستار ارشد : مینا والی
ویراستار محتوایی : قاسم سرافرازی
ویراستار فنی: محدثه گودرزنیا
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا : بهناز سعیدی
ناظر چاپ : قادر شهبازی
نوبت چاپ: سوم ۱۴۰۲
شمارگان : ۱۰۰۰ نسخه
شابک: ۶-۱۵-۷۷۰۲-۶۲۲-۹۸۷
تلفن : ۰۲۱-۴۴۴۳۹۶۶۶
دورنگار: ۸۹۷۸۴۹۰۲
ایمیل : info@way2pay.press
وب‌سایت : way2pay.shop
لیتوگرافی: هنر اشکان
چاپ و صحافی: واژه

فروشگاه انتشارات راه‌پرداخت نشانی: تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

@Way2Pay Books Way2Pay.press @Way2Pay_Network

فهرست

[یادداشت ناشر]

رضا قربانی / انتشارات راه پرداخت

در زمینه رمزارزها کتاب‌های بی‌شماری منتشر شده است؛ خوشبختانه کتاب‌های خوبی به زبان فارسی در مورد این موضوع مهم در دسترس علاقه‌مندان است و امیدواریم این روندْ مستمر و با افزایش کیفیت ادامه داشته باشد. ما در مجموعه راه پرداخت تلاش کرده‌ایم منابع خوب و قابل قبولی برای مخاطب فارسی‌زبان تهیه کنیم. استقبال مخاطبان هم نشان‌دهنده تشنگی جامعه برای دانستن و دسترسی به محتوای با کیفیت است. ما از انتشار کتاب‌های متعدد از سوی سایر ناشران استقبال می‌کنیم و اکنون که رمزارزها نوید دنیایی دیگر را داده‌اند امید است بتوانیم با آگاهی قدم در دنیای قشنگ نو بگذاریم. کسب دانش، راز غلبه بر چالش‌های جدید دنیای نو است؛ اگر برای آموزش خودمان زمانی کافی اختصاص ندهیم نمی‌توانیم بر چالش‌ها غلبه کنیم. جهان جدید از بسیاری جهات نسبت به گذشته جذاب‌تر شده است و زیبایی‌ها خودش را دارد اما چالش‌های مخصوص خودش را هم سر راه‌مان می‌گذارد که نمی‌توانیم بدون دانش و آگاهی بر این موانع غلبه کنیم.

رمزارز یا کریپتوکارنسی حوزه جدیدی است که در سال‌های اخیر توجه بسیاری را به خودش جلب کرده است و بسیاری از رسانه‌های مهم جهان نیز پیوسته روندهای این دنیای

نو را پوشش داده‌اند. برای غلبه بر چالش‌های کریپتوکارنسی و بهره‌برداری از فرصت‌هایی که این محصولات نوآورانه به ما عرضه می‌کنند، باید تاریخچه جهان جدید را بی‌کم‌وکاست بدانیم.

کتاب کریپتوکارنسی، که وایرد و انتشارات پنگوئن منتشرش کرده‌اند، با بیانی روان و شیوا تلاش می‌کند تاریخ چندساله دنیای رمزارزها را روایت کند. این تاریخچه از بیت‌کوین شروع می‌شود و همه ماجراهای جذاب متعاقب و پشت‌پرده‌اش را شرح می‌دهد؛ در ادامه اتریوم و دیگر دستاوردهای این حوزه را برمی‌شمرد. بیان کتاب به اندازه‌ای مطلوب است و چنان ریتم آهنگینی دارد که می‌شود آن را دستمایه ساخت یک مستند قرار داد. این کتاب برای مخاطبی است که دانش چندانی در زمینه بلاکچین و دارایی دیجیتال ندارد ولی قصد دارد تاریخچه کریپتوکارنسی را بداند و بتواند بر مبنای این تاریخچه درباره آینده قضاوت کند.

ما در راه پرداخت به عنوان مخاطب از مطالعه این کتاب لذت بردیم و امیدواریم مخاطبان فارسی‌زبان هم مانند ما از مطالعه این کتاب لذت کافی ببرند. در سال‌های گذشته نیز تلاش کردیم خلأ آموزش رسمی در حوزه فین‌تک را پر و بتوانیم شرایطی را فراهم کنیم که بسیاری از هم‌میهنان ما با دانش و آگاهی دست به انتخاب بزنند. جمله‌ای که همیشه گفته‌ایم این است که «بازار کریپتوکارنسی بازار پرنوسانی است» و هرچند به آینده آن امید بسته‌ایم ولی این احتمال را نباید دور از نظر داشت که ممکن است آینده، به هر دلیلی، به گونه دیگری رقم بخورد.

امیدواریم تلاش‌هایی که انجام می‌دهیم به اندازه کافی اثربخش باشد.

مقدمه

شاید بپرسید رمزارز (کریپتوکارنسی) چیست؟ این پرسش مانند بسیاری از پرسش‌های دیگری که به تعریف مربوط می‌شوند، چند پاسخ دارد. رمزارز بخش پررونقی در حوزه استارتاپ‌های فناوری است. در عین حال نوعی پول دیجیتال، یا کوینی مثل «بیت‌کوین»، «اتر» یا «مونرو» است. رمزارز می‌تواند ابزار و روشی برای نقد کردن پول‌های ناشی از فعالیت‌های مجرمانه و بزهکاری نیز باشد.

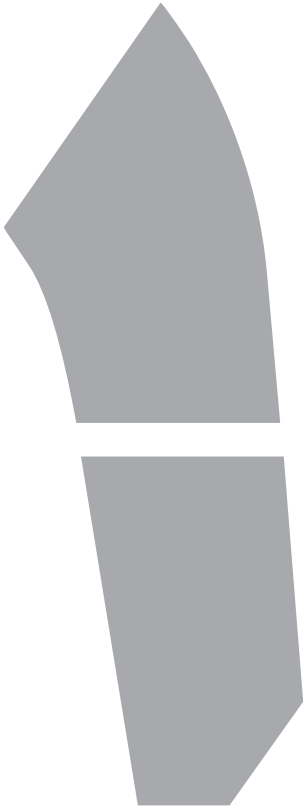
در واقع رمزارز نوعی فناوری است که با استفاده از روش‌های رمزنگاری، تبادل واحدهای ارزش در بستر اینترنت را بدون وابستگی به هرگونه واسطه‌ای ممکن می‌کند. فردی با نام مستعار می‌تواند با استفاده از رمزارز، بدون دخالت بانک‌ها، شرکت‌های پرداخت یا هر نوع مرجع دیگری، یک واحد ارزش را به فرد دیگری با نام مستعار ارسال کند. درستی این انتقال با مجموعه توزیع‌شده‌ای از کامپیوترها تأمین می‌شود که هیچ‌کدام‌شان نمی‌توانند به‌تنهایی آن پرداخت را متوقف کنند یا تغییر دهند.

رمزارز چالشی برای سازوکار متعارف سیستم مالی در چند قرن اخیر و کانال‌هایی است که ایجاد و نگهداری آن‌ها بر عهده واسطه‌ها و موجودیت‌های شخص ثالثی بوده که درستی تراکنش‌ها را ضمانت می‌کرده‌اند. همچنین تلاشی برای آسان‌تر کردن انتقال پول دور از چشم و دسترسی دولت‌هاست. هدف نهایی واسطه‌زدایی، حذف بیشترین لایه‌های انسانی ممکن از تراکنش‌ها و ارتباطات و مستقیم و همتابه‌همتا کردن رابطه‌هاست (دست‌کم نیت این بوده، اما واقعیت فنی در بسیاری از موارد به‌هیچ‌وجه بی‌نقص نبوده است).

در حال حاضر موضوع به‌آرامی از حیطه فناوری خارج و به حیطه فلسفه سیاسی وارد می‌شود و حقیقت این است که رمزارز همان‌طور که برنامه‌ای مالی است، برنامه‌ای سیاسی هم هست. یکی دیگر از اهداف کلیدی رمزارز غیرمتمرکزسازی است. مفهوم غیرمتمرکزسازی می‌گوید سیستم را نباید فقط یک یا چند نقش‌آفرین کنترل کنند. غیرمتمرکزسازی مانند واسطه‌زدایی یکی از مشخصه‌های عصر اینترنت است، عصری که در آن سیاست‌مداران تلاش می‌کنند رسانه‌ها و راستی‌آزمایان را دور بزنند و با توییت‌های‌شان نظر رأی‌دهندگان را به نفع خود تغییر دهند و عصری که در آن تجارت الکترونیکی بسیاری از فروشگاه‌های سنتی را به ورطه نابودی کشانده است. به همین دلیل است که گاهی تعریف «پول اینترنتی» برای رمزارز بسیار منطقی به نظر می‌رسد.

این کتاب می‌خواهد با بررسی دوباره گام‌هایی که رمزارز برداشته است، به جزئیات این پاسخ‌های گوناگون بپردازد. همچنین تاریخ رمزارز را از ابتدا، یعنی سه دهه پیش تا آخرین تحولاتش، تعریف می‌کند. این کتاب رویدادنگاری سیر تکامل رمزارز، اصول پیش‌برنده آن و اقدامات مخترعان و سازندگانش است. در پنج فصل که هرکدام بر دوره خاصی از رمزارز تمرکز می‌کنند (در این صنعت دوره‌ها هرکدام فقط چند ماه طول می‌کشند)، تلاش می‌کنم پاسخی تا حد ممکن مفصل به این پرسش بدهم که «رمزارز چیست و چرا باید به آن اهمیت بدهیم؟»

برای سفری چالش‌برانگیز آماده شوید.



فصل اول

بیت‌کوین

رمزارز از کجا شروع شد؟

رمزارز به‌عنوان پروژه‌ای سیاسی پا به جهان گذاشت. این موضوع خیلی راحت به فراموشی سپرده می‌شود چراکه اخبار مربوط به بیت‌کوین یا اتریوم بیشتر در صفحات مالی، رسانه‌های مربوط به فناوری و وب‌سایت‌های ویژه‌ای مشاهده می‌شود که درمورد هر تغییر کوچکی در ارزش توکن‌های دیجیتال گزارش می‌دهند. به‌سختی می‌توان در گمانه‌زنی‌های نسنجیده درمورد ارزهای خیالی، فرازونشیب‌های نامعقول بازار و توییت‌های خشمگینانه مبلغان رمزارز ایدئولوژی فراگیری پیدا کرد.

با این حال می‌توان رمزارز را نقطه پایانی دهه‌ها آزمایش برای ساختن فناوری‌ای دانست که می‌تواند مفهوم دولت را به چالش بکشد؛ این فناوری، پول دیجیتال بدون پشتیبانی و حمایت دولت است.

افرادی که این هدف را دنبال می‌کردند، خودشان را «سایفرپانک» (cypherpunk) می‌خواندند که ائتلافی نه‌چندان محکم از متخصصان فناوری، پژوهشگران و اندیشمندانی بود که اولین بار در اوایل دهه ۱۹۹۰ جلساتی را در منطقه خلیج «سان فرانسیسکو» برگزار و بعد روابط‌شان را با تشکیل «انجمن اینترنتی سایفرپانک‌ها» محکم‌تر کردند. سایفرپانک‌ها نتیجه تلفیق فناوری دیجیتال با لیبرترینیسم (libertarianism) هستند. از نظر سایفرپانک‌ها اینترنت ناگزیر باید فضایی برای آزادی، استقلال، ارتباط و اشتراک‌گذاری بی‌قیدوشرط دانش می‌شد.

تهدید اصلی برای این آرمان، دولت‌ها بودند که تلاش می‌کردند اینترنت را قانون‌گذاری کنند، از آن برای جاسوسی از کاربرانش استفاده کنند و در نهایت آن را به چیزی تبدیل کنند که آزادی و حقوق شهروندی را به مسلخ می‌برد. اینجا بود که رمزنگاری قدرتمند مطرح شد. سایفرپانک‌ها امیدوار بودند ابزارهایی مثل ایمیل رمزنگاری‌شده، شبکه‌های گمنام و سیستم‌های امن تعیین هویت بتوانند کاربران اینترنت را از چشم دولت‌ها دور نگه دارند و مانع هرگونه نظارت الکترونیکی شوند. قرار بود در بلندمدت عمومی شدن رمزنگاری، قوانین و مقررات دولت‌ها برای فضای مجازی را بیهوده و بی‌استفاده کند، اطلاعات آزادانه در گردش باشند و بازارهای آنلاین که

همه‌چیز می‌فروختند، از فایل‌های موسیقی دارای کپی‌رایت گرفته تا اسرار صنعتی، قارچ‌گونه همه‌جای اینترنت سبز شوند.

سناریوی نهایی مطلوب، «کریپتو آنارشی» بود، عبارتی که اولین بار سایفرپانک برجسته و دانشمند اینتل، «تیموتی می» (Timothy May) در سال ۱۹۹۲ در مقاله‌ای با عنوان مانیفست کریپتو آنارشیست (The Crypto Anarchist Manifesto) مطرح کرد. آن‌طور که می بعداً در مقاله‌ای طولانی‌تر توضیح داد، کریپتو آنارشی شامل سقوط دولت و ظهور نظمی سیاسی می‌شد که در آن «هیچ قانون خارجی و حاکمی وجود ندارد و توافق‌های داوطلبانه با پشتیبانی نهادهای تشکیل‌شده به‌صورت داوطلبانه تنها شکل حاکمیت خواهند بود». واژه «کریپتو» در «کریپتو آنارشی»، هم اشاره‌ای شوخ‌طبعانه به توهین‌های سیاسی مانند «کریپتو فاشیست» بود و هم تأیید جدی نقشی که رمزنگاری در شکل‌گیری حرکتی مطلوب به سمت سیستمی ایفا می‌کرد که «با مهم‌تر شدن فضای سایبری توسعه می‌یافت. سیستمی که قرار بود مرزهای ملی را کنار بزند و مبتنی بر تجارت آزاد داوطلبانه (و حتی گمنام) باشد. وجود چنین سیستمی به‌معنی پایان دولت‌ها به‌شکل کنونی خواهد بود». نه مرزی، نه مالیاتی، نه قانونی.

همه سایفرپانک‌ها به شدت تیموتی می مخالف دولت نبودند. می آرمان‌گرایی افراطی بود که دیدگاه سیاسی‌اش در طبقه‌بندی راست تندرو قرار می‌گرفت. اما در میان بیش از ۷۰۰ عضو انجمن اینترنتی سایفرپانک‌ها (از جمله افرادی مثل «آدام بَک» (Adam Back)، بیزینس‌من بریتانیایی، «ریچارد استالمن» (Richard Stallman)، نظریه‌پرداز نرم‌افزار آزاد و «جولیان آسانژ»، بنیان‌گذار «ویکی‌لیکس») بیشتر آن‌ها معتقد بودند حریم خصوصی باید حفظ شود، نظارت الکترونیکی خطرناک است و در آرزوی اینترنتی عاری از هرگونه نظارت دولتی بودند.

وقتی سایفرپانک‌ها شروع کردند به ترسیم طرحی کلی از چشم‌اندازشان، برخی از اجزای این چشم‌انداز در جایگاه خودشان قرار گرفته بودند. «پرتی گود پرایوسی» (Pretty Good Privacy)، برنامه‌ای که می‌توان از آن برای رمزنگاری ارتباطات آنلاین استفاده کرد، در سال ۱۹۹۱ راه‌اندازی شده بود، ایمیل‌رسان‌های گمنام (سیستم‌هایی

که ایمیل‌ها را به گیرنده‌های موردنظر ارسال می‌کردند، اما هویت فرستنده را پنهان نگه می‌داشتند) در حال فراگیرتر شدن بودند و لایه‌های گمنامی بیشتری را اضافه می‌کردند. اما دستیابی به یک خواسته، یعنی پول نقد دیجیتال گمنام، همچنان دشوار بود.

هدف نهایی لیبرترین‌های سایفرپانک بدون رکن اساسی لیبرترینیسم، یعنی بازار آزاد، محقق نمی‌شد. از نظر تیموتی می فضای مجازی نه‌فقط به انجمنی برای ارتباطات گمنام بدون محدودیت تبدیل می‌شد، بلکه قرار بود به بازاری بزرگ تبدیل شود که بتوان در آن انواع کالاها، خدمات و اطلاعات (قانونی و به‌ویژه غیرقانونی) را معامله کرد. مانعی که در این راه وجود داشت این بود که این تراکنش‌ها باید با چه ارزی معامله می‌شدند. بدیهی بود که سیستم‌های پرداخت الکترونیکی بانک‌ها یا شرکت‌های کارت اعتباری نمی‌توانستند جزئی از انتخاب‌ها باشند.

این سیستم‌ها، پرداخت‌کننده و دریافت‌کننده را ملزم به استفاده از نام‌های واقعی‌شان می‌کردند؛ الزامی که در تضاد با اعتقاد سایفرپانک‌ها به گمنامی بود. مهم‌تر اینکه سیستم‌ها سوابقی را ثبت می‌کردند که دولت‌ها می‌توانستند آن‌ها را برای نظارت الکترونیکی یا درمورد تجارت غیرقانونی، برای پیگرد قانونی به دادگاه فراخوانی کنند. آن‌طور که «اریک هیوز» (Eric Hughes)، یکی دیگر از بنیان‌گذاران جنبش سایفرپانک، در مقاله‌ای با عنوان مانیفست سایفرپانک (A Cypherpunk Manifesto) که در سال ۱۹۹۳ منتشر شد، نوشته بود: «برای حفظ حریم خصوصی در جامعه باز به سیستم‌های تراکنش گمنام نیاز داریم.» هیوز افزوده بود که در حالت عادی این کارکرد را پول نقد محقق می‌کند.

اما پول نقد هم به دلایل بی‌شماری نامناسب به شمار می‌رفت. برخی از این دلایل مادی بودند: به‌هیچ‌وجه معقول نبود که بازارهای گمنام مبتنی بر فضای مجازی به ارسال پستی اسکناس یا (بدتر) انتقال آن در جلسات حضوری وابسته باشند. دلایل دیگر مفهومی بودند: حتی اگر همه سایفرپانک‌ها به دنبال حذف کامل دولت نبودند، بسیاری از آن‌ها پیرو «مکتب اقتصادی اتریش» بودند که در اواخر قرن نوزدهم و اوایل قرن بیستم در «وین» مطرح شد و «فریدریش فون هایک» (Friedrich von Hayek)،

اندیشمند موردعلاقه «مارگارت تاچر» از اعضای آن بود. اعضای این مکتب ارز دولتی را نکوهش می‌کردند و معتقد بودند پول باید مانند طلا و نقره نوعی ارزش پایدار و ذاتی داشته باشد. اعضای مکتب اتریش می‌ترسیدند که وقتی پول ارزش پایدار نداشته باشد (مانند ارزهای مدرن که ارزش‌شان نه از قابلیت تبدیل آن‌ها به فلزات گران‌بها بلکه از حرف دولت‌ها ناشی می‌شود)، بانک‌های مرکزی با سیاست‌های‌شان به‌دل‌خواه ارزش ارز را افزایش یا کاهش دهند و با این کار، با تورم به بستانکاران و با تورم منفی به بدهکاران زیان برسانند. هایک در کتاب ملیت‌زدایی از پول (The Denationalisation of Money) استدلال می‌کند که راه خلاصی از این معضل این است که شهروندان و سازمان‌های خصوصی ارزهای خودشان را در رقابت با پول قانونی دولت منتشر کنند و به کاربران اجازه دهند خودشان انتخاب کنند که می‌خواهند با کدام معامله کنند. طبق استدلال هایک، این اتفاق به فراگیری مناسب‌ترین پول‌هایی منجر می‌شود که ارزش‌شان با اقدامات تورم‌زای دولت‌ها کاهش نمی‌یابد.

بنابراین، سایفرپانک‌ها به چیزی ورای پول نقد یا پول الکترونیکی بانکی نیاز داشتند؛ پدیده‌ای جدید که گمنامی اسکناس را با سرعت و نفوذ جهانی انتقال پول و در عین حال با پایداری موردنظر مکتب اتریش تلفیق می‌کرد. این کار آسان نبود.

اولین چالش در مسیر ابداع چنین ارزی با عنوان «مسئله دو بار خرج کردن» شناخته می‌شود. اگر بخواهید واحد ارز دیجیتالی ایجاد کنید، احتمالاً به چیزی شبیه فایل کامپیوتری می‌رسید که شامل رشته‌ای از کاراکترها به‌عنوان شناسه منحصربه‌فرد می‌شود که شبیه شماره‌سریال اسکناس‌هاست. اما اسکناس‌ها از اتم تشکیل شده‌اند، در حالی که اسکناس‌های دیجیتال فرضی ما از بیت‌ها تشکیل می‌شوند و این موضوع مشکلی ایجاد می‌کند.

در حالی که اسکناس کاغذی در لحظه‌ای که بین طرفین جابه‌جا می‌شود، به‌آسانی سرنوشت آن مشخص می‌شود (شما یک اسکناس ۱۰ دلاری دریافت می‌کنید و یا پرداخت می‌کنید)، یک فایل دیجیتال را می‌توان چند بار به چند دریافت‌کننده فرستاد. کاربر متقلب پول نقد دیجیتال می‌تواند تصمیم بگیرد واحد یکسانی از یک ارز را چند بار خرج کند. این مسئله تهدیدی برای موجودیت هر سیستم پرداختی

است. سرراست‌ترین راه‌حل این است که واسطه شخص ثالثی وجود داشته باشد که از سوابق تراکنش‌ها نگهداری و تراکنش‌های درست و مشروع را تسویه کند و تراکنش‌هایی را حذف کند که شامل پولی می‌شوند که پرداخت‌کننده بیش از یک بار آن را خرج کرده است. این همان کاری است که بانک‌ها انجام می‌دهند.

اما این راه‌حل مسئله دیگری ایجاد می‌کرد که متمرکزسازی بود. وجود یک واسطه یا بانک در مرکز شبکه پرداخت نه‌فقط برخلاف اصول کریپتو آنارشیستی سایفرپانک‌ها بود، بلکه مسئله‌ای ایجاد می‌کرد که متخصصان کامپیوتر «تک‌نقطه شکست» (single point of failure) می‌خوانند و تأثیری حیاتی بر موجودیت یک سیستم می‌گذارد. قدرت‌های مرکزی ممکن است هک شوند، نقش‌آفرینان متخاصم آن‌ها را به کنترل خود درآورند یا دولت‌ها مجبورشان کنند تراکنش‌هایی را مسدود کنند که شامل برخی کالاها می‌شوند (البته شاید مسدود کردن تراکنش‌های مربوط به مواد مخدر و سلاح بی‌اشکال به نظر برسد، اما عربستان سعودی و چین تراکنش‌های مربوط به برخی کتاب‌ها را هم مسدود می‌کنند).

چنین وضعیتی در تضاد با آرمان‌شهر بازار آزاد مدنظر تیموتی می بود. راه‌حل دیگر این مسئله واگذاری اداره سیستم نه به یک طرف بلکه به شبکه‌ای بزرگ‌تر از داوران مستقل است که ملحق شدن به آن برای همه آزاد باشد. در این مدل غیرمتمرکز، داورها مقدار پول نقد دیجیتال متعلق به هر کاربری را رصد می‌کنند و اجازه می‌دهند تراکنش‌های درست و مشروع انجام شوند و جلوی انجام تراکنش‌هایی را می‌گیرند که موجودی پرداخت‌کننده را منفی می‌کنند.

با این حال این راه‌حل هم مشکل دیگری ایجاد می‌کند. در فضای سایبری، یا دست‌کم در نسخه سایفرپانکی آن، همه گمنام هستند و نمی‌توانید هویت داورها را بررسی کنید. در نتیجه نمی‌توان فهمید چه زمانی یک مهاجم ارتشی از کاربران جعلی را رهبری می‌کند تا اکثریت لازم برای تأیید پرداخت‌هایی را به دست آورد که نباید تأیید شوند. چنین کاری به اعتبار سیستم آسیب می‌زند. اجتناب از این مسئله نیازمند یک پیچیدگی و در عین حال دسترسی همگانی است. می‌خواهید پیوستن به شبکه داوران برای همه آزاد باشد تا غیرمتمرکز بودن را افزایش دهید و حمله به

سیستم را برای مراجع قدرت دشوارتر کنید؛ در عین حال می‌خواهید پای منافع مالی افراد مشارکت‌کننده در سیستم نیز در میان باشد تا مجرم یا سازمانی دولتی نتواند به‌سادگی با وارد کردن افرادی به سیستم، عملکرد آن را منحرف کند. در عین حال داوری در این سیستم نباید بیش از حد گران باشد یا دست‌کم باید مشوق‌هایی داشته باشد چراکه در غیر این صورت هیچ‌کس برای داور شدن داوطلب نخواهد شد. پرسش این است که آیا می‌توان به این تعادل ظریف دست یافت؟

از اواسط دهه ۱۹۸۰ سایفرپانک‌ها با این مسائل (و مسائل گوناگون دیگر) دست‌وپنجه نرم می‌کردند و قدم‌قدم به راه‌حل نزدیک‌تر می‌شدند. رمزنگاری به نام «دیوید چام» (David Chaum) (که به‌عنوان پدر سایفرپانک‌ها شناخته می‌شود، اما عضو انجمن اینترنتی سایفرپانک‌ها نبود) و «آدام بک»، «نیک زابو» (Nick Szabo)، «هال فینی» (Hal Finney) (یکی از توسعه‌دهندگان کلیدی «پرتی گود پرایوسی») و «وی دای» (Wei Dai) که همه سایفرپانک بودند، به بحث‌ها درمورد نحوه ایجاد پول نقد دیجیتال یا رمزارز غنا بخشیدند. پول نقد دیجیتال به این دلیل رمزارز خوانده می‌شد که رمزنگاری خدشه‌ناپذیری‌اش را تضمین می‌کرد. در برخی موارد ایده‌های‌شان روی کاغذ ماندند، اما در موارد دیگر به پروژه‌ها یا حتی شرکت‌هایی واقعی، البته با طول عمر کوتاه، تبدیل شدند. اما هیچ‌کدام از این پروژه‌ها و شرکت‌ها آن نقطه عطفی نبودند که بتواند پول نقد دیجیتال را به جریان اصلی بازار بیاورد. این وضعیت در سال ۲۰۰۸ تغییر کرد.

وایت‌پیپر

یکی از متن‌های بسیار تأثیرگذار در تاریخ اینترنت، در هالووین سال ۲۰۰۸ منتشر شد، زمانی که جهان هنوز در گیرودار بحران وام مسکن بود.

«در حال کار روی سیستم پول نقد دیجیتال جدیدی هستم که کاملاً همتابه‌همتا و بی‌نیاز به شخص ثالث قابل‌اعتماد است». این جمله در ایمیلی آمده بود که به انجمن اینترنتی رمزنگاری ارسال شده بود که چند نفر از اولین سایفرپانک‌ها عضو آن بودند (مقاله کامل را می‌توانید در http://www.bitcoin.org/bitcoin.pdf مشاهده

کنید). فرستنده، ایمیل را با نام **«ساتوشی ناکاموتو»** امضا کرده بود.

ساتوشی ناکاموتو نامی مستعار بود. به‌رغم تلاش‌های خبرنگاران، تحقیقات اینترنتی و پیدا شدن افرادی که مدعی نام ناکاموتو شده‌اند، هویت واقعی این فرد یا افراد پشت این لقب پنهان مانده است. اکنون ناکاموتو سال‌ها بعد از نوشتن آخرین متنش به اسطوره اینترنت یا حتی پیامبر اینترنت تبدیل شده است، تا جایی که در سال ۲۰۲۰ مقاله‌ای در مجله آتلانتیک، وی را با «جان تایتر» (John Titor) و «کیو» (Q) مقایسه کرد. جان تایتر مسافر زمان خودخوانده‌ای بود که پیش‌بینی‌های آخرالزمانی‌اش در اوایل دهه ۲۰۰۰ دنبال‌کنندگان آنلاین قابل‌توجهی را به سمت وی جلب کرد و کیو نظریه‌پرداز تئوری‌های توطئه پشت جنبش «کیوانان» (Qanon) است که طرف‌داران زیادی در اینترنت دارد. اما تفاوتی میان این چهره‌ها با ساتوشی ناکاموتو وجود دارد: جان تایتر و کیوانان داستان‌سراهایی هستند که معروف شدن برای‌شان وسیله‌ای است تا با سرهم کردن داستان‌های خیالی ذهن دنبال‌کنندگان‌شان را به تسخیر درآورند (و درمورد کیوانان به انجام کارهای خشونت‌آمیز ترغیب‌شان کنند). ساتوشی ناکاموتو مخترعی است که میراثش ابزاری بسیار ملموس است، هرچند که این ابزار روایتی را درباره آنچه اینترنت و پول باید باشد ترویج می‌کند. اگر بخواهیم به تشبیه پیامبرگونه متوسل شویم، تایتر و کیوانان دو رهبر فرقه‌های کوچک هستند، در حالی که ناکاموتو «موسی» است که ده فرمان را برای سایفرپانک‌هایی آورده که از سال‌ها پیش منتظر ظهور پول نقد دیجیتال بودند. ده فرمان ناکاموتو در واقع همان وایت‌پیپر بیت‌کوین است.

این سند ۹ صفحه‌ای که ناکاموتو به انجمن اینترنتی رمزنگاری فرستاده بود «بیت‌کوین: یک سیستم پول نقد الکترونیکی همتابه‌همتا» (Bitcoin: A Peer-to-Peer Electronic Cash System) نام داشت و نقشه راه فنی و در عین حال مختصر و مفیدی برای ایجاد پول اینترنتی بدون پشتوانه دولت بود. ناکاموتو کاملاً با رمزنگاری آشنایی داشت و آثار سایفرپانک‌های کلیدی را مطالعه کرده بود (ناکاموتو در این متن به آثار آدام بک و وی دای ارجاع داده بود). حال باید پرسید طرحش چه بود؟ بیت‌کوین چیست؟

بیت‌کوین نام شبکه پرداخت دیجیتال پیشنهادی ناکاموتو، نام پول نقد دیجیتالی که در این شبکه مبادله می‌شود و نام نرم‌افزاری است که وجود این شبکه را ممکن می‌کند. بعداً از این واژه به‌طور کلی به‌عنوان بدل واژه رمزارز یا تعریف ذهنیتی ویژه درباره ظرفیت این فناوری استفاده شد.

بیایید روی همان تعریف اول متمرکز شویم و با تشبیهی پیش‌پاافتاده اما مؤثر شروع کنیم: بیت‌کوین را ایمیل برای پول در نظر بگیرید. البته نه ایمیل عادی، بلکه ایمیل با رمزنگاری کلید عمومی، نوعی ایمیل که در حفظ حریم خصوصی قدرتمندتر است. برای ارسال ایمیل با این روش، فرستنده به دو کد طولانی نیاز دارد.

کد اول که برای جلوگیری از هک و جعل هویتش توسط دیگران است و باید پنهان نگهش دارد، «کلید خصوصی» فرستنده است؛ رمز عبوری که می‌تواند از آن برای امضا کردن پیام به‌صورت جعل‌نشدنی استفاده و اثبات کند که نویسنده این پیام است. کد دوم «کلید عمومی» گیرنده است؛ قفلی دیجیتال که همه می‌توانند با استفاده از آن محتوای ایمیل‌های ارسالی به آن گیرنده خاص را پنهان کنند و فقط کلید خصوصی آن گیرنده می‌تواند آن را باز کند. پروژه ناکاموتو نیز سازوکاری مشابه دارد. صاحب مقدار مشخصی از پول نقد دیجیتال (بیت‌کوین) برای خرج کردن آن‌ها به کلید خصوصی خودش و کلید عمومی دریافت‌کننده (در واقع اغلب به نسخه‌ای کوتاه‌شده از آن) نیاز دارد تا مبلغ را به حساب آن فرد منتقل کند. این جابه‌جایی‌ها معمولاً از طریق دستگاه، نرم‌افزار یا اپلیکیشنی با نام «کیف پول» مدیریت می‌شود که حاوی کلیدهای عمومی و خصوصی کاربر است.

هم‌راستا با هنجارهای سایفرپانک، هرکسی می‌تواند بدون افشای هویتش از بیت‌کوین استفاده کند، البته که این کار با گذشت زمان دشوارتر شده است. از طرف دیگر، همه پرداخت‌ها در معرض دید عموم قرار دارند. هرکسی می‌تواند ببیند کیف پول گمنام مشخصی چقدر به کیف پول گمنام دیگری پرداخت کرده است. احتمالاً در این مورد دیگر بیت‌کوین شباهتی به ایمیل ندارد. بیت‌کوین‌ها برخلاف ایمیل‌ها از پرداخت‌کننده به دریافت‌کننده ارسال نمی‌شوند. بلکه پرداخت‌کننده یک «تراکنش» ایجاد می‌کند. تراکنش بسته داده‌ای است که در طراحی ناکاموتو شامل

اطلاعاتی درباره پرداخت‌کننده و دریافت‌کننده، مقدار بیت‌کوینی که مالکیتش تغییر می‌کند و کدی می‌شود که به تراکنشی ارجاع می‌دهد که در آن پرداخت‌کننده، مبلغ را دریافت کرده است (که نوعی سند دیجیتال است). تراکنش‌ها به‌صورت عمومی به شبکه‌ای از داوران مخابره می‌شوند که مشابه شبکه‌ای است که سایفرپانک‌ها به‌عنوان راهی برای جلوگیری از دو بار خرج کردن بدون حضور قدرت مرکزی مطرح کرده بودند. درمورد بیت‌کوین گروه بزرگی از کامپیوترها به نام «نود» (Node) وجود دارند که نرم‌افزار بیت‌کوین را اجرا می‌کنند. هر فردی با یک لپ‌تاپ، دسترسی به اینترنت و علاقه به رمزارز می‌تواند نودی ایجاد کند. همه نودها کپی یکسانی از دفترکلی آنلاین در اختیار دارند که جزئیات همه تراکنش‌های بیت‌کوین از ابتدا تاکنون را ثبت کرده است. این دفترکل در واقع زنجیره‌ای از مالکیت‌هاست که نشان می‌دهد هر کاربر در هر زمان چقدر بیت‌کوین داشته است. وقتی تراکنش جدیدی اعلام می‌شود، در تمام شبکه حرکت می‌کند و نودها یکی پس از دیگری با توجه به دفترکل بررسی می‌کنند که پرداخت‌کننده مالک بیت‌کوین‌هایی که خرج می‌کند هست یا خیر. اگر باشد، تراکنش می‌تواند انجام شود، اما هنوز نمی‌تواند تأیید شود.

تأیید این تراکنش‌ها و ثبت تغییرات مالکیت در دفترکل وظیفه زیرمجموعه‌ای از نودها به نام «نودهای استخراج» یا «ماینرها» است. این واژه فقط یک بار در وایت‌پیپر بیت‌کوین به‌عنوان نام مستعاری برای افرادی مطرح شده است که نودهایی را اداره می‌کنند. به‌گفته ناکاموتو، آن‌ها «شبیه استخراج‌کنندگان طلا هستند که منابع‌شان را برای افزایش طلاهای در گردش صرف می‌کنند». برای درک این موضوع به مسئله‌ای فکر کنید که سایفرپانک‌ها هنگام در نظر گرفتن ساختار داوری غیرمتمرکز به‌جای واسطه صرف با آن برخورد کرده بودند. می‌خواهید دسترسی به شبکه داوران را تا حد ممکن باز نگه دارید. هرچه نودهای بیشتری در شبکه بیت‌کوین باشند، هدف گرفتن یکی از آن‌ها و مسدود کردن تراکنش‌ها برای دولت‌ها دشوارتر می‌شود. اما اگر پیوستن به شبکه خیلی آسان باشد، ممکن است خراب‌کارها سیستم را به کنترل خودشان درآورند.

بنابراین ناکاموتو به این نتیجه رسید که تأیید تراکنش‌ها باید هزینه‌بر باشد. ماینرها

باید صدها تراکنش معتبر را در دسته‌هایی (به نام «بلوک») جمع‌آوری و برای اضافه کردن آن‌ها به دفترکل با یکدیگر رقابت کنند. ماینر برای به دست آوردن این مزیت باید یک مسئله ریاضی مبتنی بر تابع هش را حل کند. تابع هش الگوریتمی است که می‌تواند هر قطعه داده‌ای (از عبارت ساده «سلام، دنیا» تا تمام سه‌گانه ارباب حلقه‌ها) را به هش یا رشته‌ای از ارقام با اندازه‌ای استاندارد تبدیل کند. هش‌ها در رمزنگاری پرطرفدارند زیرا تبدیل داده‌ها به هش آسان است، اما مهندسی معکوس و رسیدن به داده‌ها با استفاده از هش تقریباً غیرممکن است. ماینرهای بیت‌کوین باید داده‌های تراکنش بلوک را به هشی ۲۵۶ بیتی تبدیل کنند که با تعداد مشخصی صفر شروع شود. ماینرها، برای رعایت کردن این شرط، عددی به نام «نانس» را به داده‌های تراکنش اضافه می‌کنند با این امید که به نتیجه درست برسند. چطور این عدد را پیدا می‌کنند؟ با حدس زدن. نود استخراج سریع، پشت‌سر هم و خودکار، اعداد تصادفی را امتحان می‌کند تا به پاسخ برسد.

انجام این کار نیازمند کامپیوترهای قدرتمند و برق برای تأمین توان موردنیازشان است. به همین دلیل است که ناکاموتو گفته بود ماینرها «منابع صرف می‌کنند» و به همین دلیل است که این سیستم «اثبات کار» (proof-of-work) خوانده می‌شود. البته افرادی که نودهای استخراج را اداره می‌کنند، پول‌شان را به‌خاطر نوع‌دوستی خرج نمی‌کنند؛ با این کار می‌توانند برنده جایزه‌ای بشوند. اولین نود استخراجی که مسئله را حل کند، بی‌درنگ به ماینرهای دیگر اطلاع می‌دهد و این ماینرها هم بررسی می‌کنند که آیا تراکنش‌های بلوک معتبرند یا خیر و اگر این‌طور باشد، دفترکل‌های‌شان را بر همان اساس به‌روز می‌کنند.

نودهای ساده نیز همین به‌روزرسانی را انجام می‌دهند و دفترکل در تمام شبکه به‌روز می‌شود. ماینر برنده، تعداد مشخصی بیت‌کوین یا طبق تشبیه ناکاموتو «طلا» پاداش می‌گیرد. این پاداش هر چهار سال نصف می‌شود (این ویژگی «هاوینگ» (halving) خوانده می‌شود) چراکه ناکاموتو تعیین کرد که کل موجودی بیت‌کوین باید متناهی و ۲۱ میلیون واحد باشد. ماینرها همچنین می‌توانند از کاربرانی که می‌خواهند تراکنش‌های‌شان سریع‌تر پردازش شوند، کارمزدهای کمی در قالب بیت‌کوین دریافت

کنند (وقتی آخرین بلوک در حدود سال ۲۱۴۰ استخراج شود، تنها مشوق ماینرها فقط کارمزد تراکنش‌ها خواهد بود). این امر یکی از شواهدی است که نشان می‌دهد کدهای ناکاموتو رابطه‌ای درهم‌تنیده با سیاست دارند. بیت‌کوین هم‌سو با مکتب اتریش ابداع شده است؛ استاندارد طلا را به بازی می‌گیرد، از پول ملیت‌زدایی می‌کند و مهم‌تر اینکه به الگوریتم انتشار پول خودکار رنگ واقعیت می‌بخشد، در حالی که معمولاً بانکی مرکزی وجود داشته که می‌توانسته موجودی پول را افزایش یا کاهش دهد.

ناکاموتو در اوایل سال ۲۰۰۹ در مطلبی در انجمن «بنیاد همتابه‌همتا» (P2P Foundation) نوشته بود: «مشکل ریشه‌ای ارزهای متعارف اعتمادی است که برای عملی کردن آن‌ها باید وجود داشته باشد. باید به بانک مرکزی اعتماد کرد که ارزش ارز را کاهش نمی‌دهد، اما تاریخ ارزهای فیات مملو از خدشه‌دار شدن این اعتماد است» و پیش‌بینی کرد که «اعتماد» نقشی محوری در بحث‌های مربوط به رمزارز خواهد داشت. ناکاموتو در پیامی به انجمن اینترنتی رمزنگاری با لحنی طعنه‌آمیز گفته بود: «اگر بتوانیم بیت‌کوین را به‌شکل مناسب توضیح بدهیم، برای دیدگاه لیبرترینیسم خیلی جذاب خواهد بود. اما من بیش از کلمات در استفاده از کدها مهارت دارم.»

اما کد (اگرچه از لحاظ شفافیت ایدئولوژیک بسیار واضح است) مبتنی بر اصل فایده‌گرایی و در معرض آسیب است. «جایا کلارا برک» (Jaya Klara Brekke)، استادیار و پژوهشگر فناوری‌های غیرمتمرکز در دانشگاه «دورهام»، می‌گوید هرچند استخراج بیت‌کوین بر «نظریه کالایی پول» دلالت می‌کند (طبق این نظریه پول چیزی با ارزش ذاتی مانند طلاست)، عنصر دفترکل در این سیستم که در آن دارایی‌های هر فرد به‌صورت مدخل‌هایی در ترازنامه جهانی شبکه وجود دارند، بر دیدگاهی متضاد دلالت می‌کند که برک آن را «نظریه اعتباری پول» می‌خواند.

علاوه بر این، کد تکامل می‌یابد. به‌عنوان مثال مقوله استخراج را در نظر بگیرید. وایت‌پیپر تمایزی میان نودها و ماینرها قائل نمی‌شود؛ همه نودها استخراج می‌کنند. امروزه بیشتر نودها استخراج نمی‌کنند، بلکه صرفاً از نسخه‌ای از دفترکل نگهداری می‌کنند، تراکنش‌ها را بازپخش می‌کنند و پایداری و قدرت را افزایش می‌دهند. به

همین دلیل است که مسائل ریاضی‌ای که ماینرها باید حل کنند با گذشت زمان دشوارتر و حل‌شان پرهزینه‌تر می‌شوند. زمانی که شبکه بیت‌کوین تازه راه‌اندازی شده بود، تازه‌کارها می‌توانستند با یک لپ‌تاپ استخراج کنند. امروزه استخراج کسب‌وکاری است که تعداد زیادی از سرورهای بسیار تخصصی انجام می‌دهند که در کشورهایی واقع شده‌اند که برق در آن‌ها ارزان است. هرچند پایبندی به «چشم‌انداز ساتوشی» به‌مرور به نوعی علاقه وسواس‌گونه تبدیل شده، این مورد فقط یکی از نمونه‌هایی است که نشان می‌دهد قوانین بیت‌کوین از هالووین سال ۲۰۰۸ تاکنون بارها به بحث گذاشته شده، به‌روز شده و تغییر کرده‌اند.

البته این کشمکش‌ها اجتناب‌ناپذیر بودند. بیت‌کوین باید تکامل می‌یافت. اما هم‌زمان ایده تغییرناپذیری از همان ستون اصلی سیستم، یعنی دفترکل، یا به‌عبارت دیگر «بلاکچین»، در این سیستم تعبیه شده است. ناکاموتو در وایت‌پیپر بیت‌کوین بلاکچین را صرفاً «زنجیره» (chain) می‌خواند. به این دلیل زنجیره خوانده می‌شود که هر بلوکی که استخراج می‌شود و اکثریت ماینرها و نودها آن را اعتبارسنجی می‌کنند به دفترکل اضافه می‌شود و پیوندی ناگسستنی و زنجیروار با بلوک قبلی خواهد داشت. همان‌طور که داده‌های یک تراکنش به تراکنشی ارجاع می‌دهند که در آن پرداخت‌کننده آن مقدار بیت‌کوین را دریافت کرده، همه بلوک‌ها نیز حاوی ارجاعی رمزنگاری‌شده به بلوک قبلی‌شان و بلوک قبلی به بلوک قبل‌تر از خود و همین‌طور تا اولین بلوک استخراج‌شده هستند.

این معماری به مهاجمان اجازه نمی‌دهد تراکنش‌های قبلی را تغییر دهند و راه را برای دو بار خرج کردن باز بگذارند. هرکسی که بخواهد تراکنش قبلی را دستکاری کند، باید نه‌فقط بلوک حاوی آن تراکنش، بلکه همه بلوک‌های بعد از آن را که داده‌های‌شان به آن بلوک هک‌شده ارجاع می‌دهند دوباره استخراج کند. این کار بسیار دشوار است. میانگین زمان موردنیاز برای استخراج هر بلوک ده دقیقه است. وقتی مهاجم تلاش می‌کند یک بلوک را دوباره استخراج کند، سایر ماینرها احتمالاً هم‌زمان بلوک جدیدی را به بلاکچین اضافه کرده‌اند. هر ده دقیقه که مهاجم به‌سختی تلاش می‌کند همه بلوک‌های موردنیاز برای بازنویسی تاریخچه بلاکچین را تغییر دهد، بلوک

استخراج‌شده جدیدی ظاهر می‌شود که تلاش‌های مهاجم را پیچیده‌تر می‌کند. اما برای اینکه این سازوکار سخت‌تر شود، ناکاموتو یک شرط را نیز در کد تعیین کرد؛ اینکه نودهای استخراج همیشه باید بلوک‌های جدید را به طولانی‌ترین زنجیره اضافه کنند. در غیر این صورت هکرها می‌توانستند به‌آسانی بلوک موردنظرشان را دوباره استخراج کنند و سایر ماینرها را برای پیروی از خودشان در زنجیره کوتاه‌تر و دست‌کاری‌شده فریب دهند (هکرها همچنین ممکن است با استفاده از قدرت رایانش کافی برای به دست گرفتن اکثریت نودهای استخراج در دفترکل اختلال ایجاد کنند. چنین سناریویی با نام «حمله ۵۱ درصد» شناخته می‌شود. اما اثبات کار باید این نوع حمله را بیش از حد دشوار و دستاوردش را تقریباً ناچیز کند). همه عناصر پروژه ناکاموتو می‌خواستند اطمینان حاصل کنند که تراکنش‌ها را نمی‌توان مسدود، سانسور یا معکوس کرد. چنین مشخصه‌ای به زیان افرادی است که قربانی کلاهبرداری می‌شوند، اما برای سایفرپانک‌ها پیروزی بزرگی محسوب می‌شود.

چه چیزی بیت‌کوین را ارزشمند کرد؟ برخلاف دلار پیش از سال ۱۹۷۱، طلا پشتوانه ارزش بیت‌کوین نیست و برخلاف دلار پس از سال ۱۹۷۱ نیز حرف دولت و پذیرش آن به‌عنوان ابزار پرداخت مالیات، تضمین‌کننده ارزش بیت‌کوین نیست. از دیدگاه عینی، ارزش امروز بیت‌کوین نتیجه برخورد عرضه و تقاضا در صرافی‌های آنلاین است، جایی که بیت‌کوین در ازای دریافت ارزهای دولتی فروخته می‌شود. هر صرافی با توجه به میانگین حجم معاملات پلتفرمش قیمت معادل دلاری متفاوتی تعیین می‌کند. به همین دلیل است که هرچند قیمت بیت‌کوین معمولاً در همه پلتفرم‌ها تقریباً یکسان است، معامله‌گران می‌توانند از کمی آربیتراژ (بهره گرفتن از تفاوت قیمت بین دو یا چند بازار برای کسب سود) بین صرافی‌های متفاوت بهره ببرند.

اما این توضیح فنی به این پرسش پاسخ نمی‌دهد که چرا افراد برای خرید بیت‌کوین هزینه می‌کنند. با توجه به اینکه بیت‌کوین و نحوه استفاده از آن از ابتدا تاکنون تغییر کرده، بحث در این مورد داغ و همچنان در حال تکامل است. اما مطلب آنلاینی که ناکاموتو در سال ۲۰۱۰ نوشت، تا حدی به ما نشان می‌دهد که نظر احتمالی او درباره ارزش بیت‌کوین چه بوده است. ناکاموتو در این مطلب وجود فلز کمیابی را فرض

می‌گیرد که از همه جهات به‌جز یک ویژگی بی‌فایده و بی‌استفاده است. آن ویژگی امکان انتقال آسان آن از فردی به فرد دیگر است. ناکاموتو در ادامه استدلال می‌کند که «اگر این فلز به‌نحوی و به هر دلیلی ارزش پیدا کند، هرکسی که بخواهد ثروت را به مسافت دوری بفرستد، می‌تواند مقداری از آن را بخرد، منتقلش کند و از گیرنده بخواهد آن را بفروشد. شاید وقتی افراد متوجه فایده احتمالی آن برای تبادل شوند، ارزش گردشی اولیه‌ای پیدا کند».

به‌عبارت دیگر، ارزش بیت‌کوین به ویژگی‌های آن وابسته است. همان‌طور که انتخاب طلا به‌عنوان ابزار تبادل در کمیابی، درخشندگی، انعطاف‌پذیری و مقاومت آن در برابر فرسایش و ویژگی‌های دیگر این فلز ریشه داشت، ارزش بیت‌کوین نیز از توانایی انتقال آن بدون ریسک مسدودی یا برگشت‌پذیری ناشی می‌شود. در این تفسیر تا زمانی که افرادی باشند که بیت‌کوین را (برای آرمان‌های لیبرترین، اهداف مجرمانه یا اهداف ضد نظارت الکترونیکی) مفید بدانند، بیت‌کوین ارزش خواهد داشت و سفته‌بازی هم اثر مکمل مهمی خواهد گذاشت.

اوج گرفتن

واکنش‌های اولیه به وایت‌پیپر بیت‌کوین سراسر انتقاد بودند و به ایرادهای ابعاد مختلف پیشنهاد ناکاموتو اشاره می‌کردند. ناکاموتو با بردباری به همه این انتقادها پاسخ داد و همین‌طور که بحث‌ها پیش می‌رفتند، شور و اشتیاق اعضای انجمن اینترنتی رمزنگاری مشهود و ملموس می‌شد. اعضای این انجمن چنان مشغول بحث درمورد بیت‌کوین شده بودند که در ۱۷ نوامبر ۲۰۰۸، ادمین این انجمن، «پری ای متزگر» (Perry E. Metzger)، پیامی با عنوان «فعلاً، پایان بحث درمورد بیت‌کوین» فرستاد که از جامعه در حال گسترش حامیان بیت‌کوین می‌خواست بحث‌های‌شان را در جای دیگری ادامه دهند. همین کار را کردند.

ابتدا بحث را به انجمن دیگری و بعد به تالار گفت‌وگویی اختصاصی به نام «بیت‌کوین‌تاک» (Bitcointalk) منتقل کردند که ناکاموتو در نوامبر ۲۰۰۹ تأسیس کرده بود. صدها ایمیل، مطلب، گفت‌وگو و پیام خصوصی، بیت‌کوین را از مانیفستی

فنی به پروژه منبع‌باز پویایی تبدیل کرد. شبکه بیت‌کوین، در سوم ژانویه ۲۰۰۹ راه‌اندازی شد. ناکاموتو اولین بلوک بیت‌کوین را استخراج کرد و به‌عنوان برچسب زمانی اضافه گزاره کوتاهی را به این بلوک پیوست کرد: «روزنامه تایمز سوم ژانویه ۲۰۰۹؛ وزیر خزانه‌داری در آستانه عرضه دومین طرح نجات بانک‌ها». این گزاره عنوانی واقعی از روزنامه تایمز لندن بود که به برنامه «آلیستر دارلینگ» (Alistair Darling)، وزیر خزانه‌داری بریتانیا، برای نجات بانک «لویدز» و «رویال بانک اسکاتلند» از بحران مالی اشاره می‌کرد. بیت‌کوین با نیش و کنایه‌ای به بانک‌ها و هزینه‌کرد دولت‌ها پا به جهان گذاشت.

دلیل موفقیت بیت‌کوین (که حتی سخت‌گیرترین منتقدان این پروژه تأیید می‌کنند در نهایت ایده پول نقد دیجیتال را به جریان اصلی بازار آورده است) در درجه نخست توانایی ساتوشی ناکاموتو در استفاده از فناوری موجود برای دستیابی به رؤیای سایفرپانک بود. مسئله دیگری هم نقش داشت: در سال ۲۰۰۸ به نظر می‌رسید دوران بیت‌کوین فرارسیده است، زیرا ابزاری بود که با روح زمانه هم‌خوانی داشت. وعده اصلی بیت‌کوین واسطه‌زدایی به نفع تبادل مستقیم میان همتایان بود.

اقتصاددان‌ها ایده واسطه‌زدایی را اولین‌بار در دهه ۱۹۶۰ مطرح کردند تا روند کاهش وابستگی به واسطه‌های مالی، مثل بانک‌های تجاری و صندوق‌های بازنشستگی را با آن توصیف کنند. اما با ظهور اینترنت، این عبارت به‌عنوان پدیده‌ای که می‌تواند روی صنایع بسیاری تأثیر بگذارد، بار معنایی فراگیر و تحول‌آفرینی پیدا کرد. واسطه‌زدایی به اسم رمزی در عصر حباب دات‌کام تبدیل شد و بعد از ترکیدن این حباب در دهه ۲۰۰۰ شاهد تحقق ملموس آن بودیم. تا زمانی که ناکاموتو خبر راه‌اندازی شبکه بیت‌کوین را اعلام کرد، افراد زیادی (علاوه بر سایفرپانک‌ها) برای آشنایی با پدیده‌ای مانند بیت‌کوین آماده شده بودند. این افراد دیده بودند که چطور اینترنت، آژانس‌های مسافرتی را به‌عنوان کانال‌های خرید بلیت هواپیما و رزرو هتل بی‌مصرف کرده است، چطور تجارت الکترونیکی به تولیدکننده و خریدار امکان معامله مستقیم داده و عمده‌فروش و خرده‌فروش را حذف کرده است و چطور شبکه‌های اجتماعی به سیاست‌مداران و چهره‌های سیاسی این امکان را داده‌اند که رسانه‌های متعارف را دور

بزنند و بی‌واسطه با مخاطبان‌شان ارتباط برقرار کنند.

بیت‌کوین وعده می‌داد که همین کار را برای پول انجام می‌دهد؛ شرکت‌های پرداخت، نهادهای مالی و بانک‌های مرکزی حذف می‌شدند و فقط با کدهای ریاضی سروکار داشتیم. حذف لایه‌های واسطه‌گری اضافه (واسطه‌هایی که رانت‌خوار بی‌فایده یا دردسر امنیتی در نظر گرفته می‌شدند) مبنای تعریف بیشتر پروژه‌های رمزارزی بعد از بیت‌کوین بود.

با این حال نفوذ بیت‌کوین به جریان اصلی تدریجی بود. در اواسط سال ۲۰۱۰، قیمت بیت‌کوین در چند صرافی موجود در آن زمان کمتر از ۰٫۱ دلار بود. این دوره گمنامی دوام نداشت. کلارا جایا برک، استاد دانشگاه دورهام، می‌گوید: «نقطه عطف مهم در تاریخ بیت‌کوین ویکی‌لیکس بود.» در نوامبر ۲۰۱۰، این وب‌سایتِ افشاگری که جولیان آسانژ، عضو سابق جامعه سایفرپانک، بنیان‌گذارش بود، در فهرست سیاه قرار گرفت و نتوانست از طریق پلتفرم‌های پرداخت متعارف سرمایه جذب کند.

اعضای انجمن بیت‌کوین‌تاک شروع به بحث در این مورد کردند که آیا بهتر است به آسانژ توصیه کنند که کمک‌های مالی بیت‌کوینی را بپذیرد. مگر نه اینکه یکی از موارد استفاده شاخص بیت‌کوین مقابله با مسدودسازی پرداخت‌ها از طرف دولت بود؟ ناکاموتو که هنوز در آن انجمن فعال بود، با نگرانی از توجهی که ارتباط با ویکی‌لیکس به بیت‌کوین معطوف می‌کرد، به‌شدت با این ایده مخالفت کرد. افراد نظر ناکاموتو را پذیرفتند و با ویکی‌لیکس تماس نگرفتند. اما خبرنگاران متوجه این ماجرا شدند و با انتشار مقاله‌هایی در فضای آنلاین استدلال کردند که بیت‌کوین دست‌کم روی کاغذ می‌تواند راه‌حلی برای معضل ویکی‌لیکس فراهم کند. آن‌طور که یکی از کاربران بیت‌کوین‌تاک به‌شوخی گفته بود: «مرغ از قفس پرید.» نظر ناکاموتو هم شبیه به همین بود. او در ۱۱ دسامبر ۲۰۱۰، یک روز بعد از گزارش‌های رسانه‌ای اولیه درباره بیت‌کوین و ویکی‌لیکس نوشته بود: «ویکی‌لیکس به لانه زنبورها لگد زد و حالا زنبورها به سمت ما می‌آیند.» ناکاموتو فقط یک مطلب دیگر، آن هم یک روز بعد نوشت و بعد دیگر در آن انجمن چیزی ننوشت. بعداً در ارتباطی ایمیلی با یکی از توسعه‌دهندگان ارشد بیت‌کوین توضیح داده بود که «سراغ مسائل دیگری رفته است». ویکی‌لیکس

در ژوئن ۲۰۱۱ پذیرش بیت‌کوین به‌عنوان کمک مالی را شروع کرد.

فقط پس‌لرزه‌های موضوع ویکی‌لیکس نبودند که سال ۲۰۱۱ را به سالی حساس و کلیدی برای بیت‌کوین تبدیل کردند. اولین اتفاق از راه رسیدن نسخه‌های بدلی بیت‌کوین بود. توسعه‌دهندگان با استفاده از بیت‌کوین به‌عنوان طرح اولیه و اضافه کردن قابلیت‌های جدید، انواع جدیدی از پول دیجیتال را ساختند (که گاهی «آلت‌کوین» خوانده می‌شوند). «نیم‌کوین» (Namecoin) و «لایت‌کوین» (Litecoin)، دو نمونه برجسته بودند که هر دو در سال ۲۰۱۱ عرضه شدند. تقریباً انگار طبق دکترین فریدریش فون هایک، این فضا به‌مرور به فضای رقابت رمزارزهای مختلف تبدیل شده بود. به‌علاوه، سال ۲۰۱۱ همان سالی بود که «ویتالیک بوترین» (Vitalik Buterin)، برنامه‌نویس ۱۷ ساله روسی-کانادایی شیفته ایده بیت‌کوین شد و کار برای راه‌اندازی مجله‌ای تخصصی به نام «مجله بیت‌کوین» (Bitcoin Magazine) را شروع کرد. دو سال بعد بوترین نقشی حیاتی در ایجاد رمزارز دیگری به نام «اتریوم» ایفا کرد که همان‌طور که در ادامه خواهیم دید، منشأ تغییر پارادایمی در تمام این حوزه شد. سال ۲۰۱۱ همچنین سالی بود که «راس اولبریکت» (Ross Ulbricht)، لیبرترین متولد ایالت تگزاس، «سیلک‌رود» (Silk Road) را راه‌اندازی کرد.

سیلک رود بازار آنلاینی برای خریدوفروش مواد مخدر بود که در دارک‌وب قرار داشت و از بیت‌کوین به‌عنوان ابزار پرداخت استفاده می‌کرد. آرمان‌شهر کریپتو آنارشیستیِ مدنظر تیموتی می در نهایت به حقیقت پیوسته بود و در این میان برچسب ناخوشایند پول مجرمان به بیت‌کوین زده شد، برچسبی که بیت‌کوین بعد از یک دهه هنوز نتوانسته از شر آن خلاص شود.

اگر بگوییم سیلک‌رود بیت‌کوین را میان جماعتی جدید (جماعت خریدار مواد مخدر) محبوب کرد، می‌توان این استدلال را نیز مطرح کرد که تعطیلی بسیار پرسروصدای این بازار در سال ۲۰۱۳ به جهانی‌شدن کاربرد بیت‌کوین کمک کرد. تحلیلی درمورد تغییرات قیمت بیت‌کوین در صرافی‌های آنلاین در فاصله سال‌های ۲۰۱۲ تا ۲۰۱۸ که در سال ۲۰۱۹ در رویال سوسایتی (Royal Society) منتشر شد، نشان می‌دهد که دستگیری اولبریکت احتمالاً یکی از محرک‌های حباب بیت‌کوینی

بود که در نیمه دوم سال ۲۰۱۳ شروع شد و چهارم دسامبر با ۱۱۳۲ دلاری شدن قیمت بیت‌کوین به اوج رسید. در این مقاله نوشته شده بود: «تعطیلی سیلک‌رود باعث شد سرمایه‌گذاران محتاط، بیت‌کوین را به‌عنوان ابزار سرمایه‌گذاری مناسب در نظر بگیرند، سرمایه‌گذارانی که تا آن زمان به‌واسطه کاربرد غیرقانونی بیت‌کوین به‌عنوان پولی مجرمانه از آن دوری می‌کردند.» چند عامل دیگر نیز در ایجاد این حباب نقش داشتند، از جمله گرایش فزاینده به بیت‌کوین در چین و بحران بدهی منطقه یورو که باعث شده بود بسیاری از مردم اروپا به دنبال ذخیره ارزشی خارج از قلمروی دولت باشند. حباب‌های بسیار دیگری هم بعد از آن ایجاد شدند (مقاله مذکور از ۱۳ مورد نام می‌برد) که بزرگ‌ترین آن‌ها در سال ۲۰۱۷ قیمت بیت‌کوین را به نزدیک ۲۰ هزار دلار به‌ازای هر واحد رساند. این حباب‌ها تا حدی خالی شده‌اند، اما کاملاً نترکیده‌اند. در ژوئیه ۲۰۲۰ ارزش همه بیت‌کوین‌های جهان حدود ۱۱۸ میلیارد دلار برآورد می‌شد. سقوط سیلک‌رود به‌نوعی ناقوس مرگ بیت‌کوین به‌عنوان ارز و آغاز عصر بیت‌کوین به‌عنوان ابزار سرمایه‌گذاری سفته‌بازانه بود که تا امروز همچنان ادامه دارد (البته شاید بعد از اینکه شرکت سازنده خودروهای برقی «تسلا» در اوایل سال ۲۰۲۱ اعلام کرد پرداخت با بیت‌کوین را می‌پذیرد، این وضعیت نیز دوباره تغییر کرد).

کار ناتمام

دنیایی که بیت‌کوین در زمان رشد انفجاری‌اش در سال ۲۰۱۳ در آن قرار داشت، خیلی با دنیای سال ۲۰۰۸، یعنی زمان پیدایش بیت‌کوین، متفاوت بود. افکار ناکاموتو در خلأیی فنی واقعیت یافته بودند. بیت‌کوین در آن زمان تنها رمزارز موجود بود. اما چهار سال بعد، با توجه به ظهور موجی از پروژه‌های پول نقد دیجیتال که به‌نحوی از الگوی بیت‌کوین الهام گرفته بودند، «رمزارز» به واژه‌ای تبدیل شده بود که اغلب به‌صورت جمع استفاده می‌شد. از آن زمان به بعد بیشتر نوآوری‌ها (و در عین حال تبهکاری‌ها، دغل‌کاری‌ها و طرح‌های نابخردانه) در این حوزه در پروژه‌هایی غیر از بیت‌کوین اتفاق افتادند. یکی از دلایل این وضعیت این بود که جامعه بیت‌کوین به‌قدری به وایت‌پیپر بیت‌کوین دل‌بسته است که هرگونه انحرافی از آن به منازعات

آتشین و دودستگی گاه‌وبیگاه منجر می‌شود. از سویی جامعه بیت‌کوین شاهد قدرت گرفتن قبیله پرسروصدای «ماکسیمالیست‌های بیت‌کوین» بوده که هر توکنی به‌غیر از بیت‌کوین را با نامعقول یا کلاهبرداری خواندن رد می‌کنند.

البته منظور این نیست که جامعه بیت‌کوین تغییرناپذیر یا فسیل شده است. اتفاقاً برعکس، برتری بیت‌کوین، این جامعه (شامل توسعه‌دهندگان، ماینرها، گردانندگان نودها، صرافی‌ها و مفسران مطرح در شبکه‌های اجتماعی) را مجبور کرده است با چند مسئله روبه‌رو شوند که اگر به آن‌ها رسیدگی نشود، می‌توانند موفقیت بلندمدت این پروژه را به خطر بیندازند.

شاید اساسی‌ترین مسئله چیستی بیت‌کوین باشد. دوگانه بیت‌کوین به‌عنوان پول در برابر بیت‌کوین به‌عنوان یک کالای سرمایه‌گذاری، مسئله‌ای نظری نیست و پیامدهای فنی زیادی دارد. اگر بیت‌کوین یک کالای سرمایه‌گذاری باشد، چیزی مانند شمش طلاست که می‌خرید و ذخیره می‌کنید. اگر بیت‌کوین پول باشد، رقیب‌هایش شرکت‌های پرداختی مثل «ویزا» خواهند بود.

ویزا ادعا می‌کند از ظرفیت پردازش ۵۶٬۰۰۰ تراکنش در ثانیه برخوردار است. در حالی که بیت‌کوین در سال ۲۰۲۰ می‌توانست هفت تراکنش را در ثانیه پردازش کند که برای یک شبکه پرداخت بسیار کم است. یکی از دلایل این مسئله به بلوک‌های تشکیل‌دهنده بلاکچین مربوط می‌شود. ناکاموتو طوری این بلوک‌ها را طراحی کرده است که حداکثر اندازه آن‌ها یک مگابایت باشد. این محدودیت باعث می‌شود تعداد تراکنش‌هایی که می‌توان در هر بلوک جا داد و در ده دقیقه به دفترکل اضافه کرد، محدود باشد. به همین دلیل است که بحث درمورد مقیاس‌پذیری بیت‌کوین اغلب حول بزرگ‌تر کردن بلوک‌ها می‌چرخد، راه‌حلی که مشکلات خودش را به همراه دارد چراکه بلوک‌های بزرگ‌تر فضای بیشتری را روی دیسک سخت دستگاه اشغال می‌کنند و این مسئله نیز باعث افزایش هزینه اداره نود و در نتیجه تمرکز قدرت در چند ماینر محدود می‌شود. این بحث در سال ۲۰۱۷ به زورآزمایی میان هواداران بلوک‌های بزرگ‌تر و حامیان «سگویت» (SegWit) یا «سگرگیتد ویتنسن» (Segregated Witness) منجر شد.

هواداران بلوک‌های بزرگ‌تر بیشتر ماینرهای آسیایی به رهبری «راجر ور» (Roger Ver) که به «مسیح بیت‌کوین» (Bitcoin Jesus) معروف است، بودند. راجر ور لیبرترینی افراطی بود که در سال ۲۰۰۵ به دلیل فروش مواد منفجره در فروشگاه اینترنتی «ای‌بی» ۱۰ ماه به زندان افتاد و بعداً حق شهروندی آمریکا از او گرفته شد. سگویت راه‌حلی نرم‌افزاری بود که امکان جای دادن تراکنش‌های بیشتر در بلوک‌ها بدون افزایش اندازه‌شان را می‌داد. در اوت ۲۰۱۷ جماعتی که راجر ور رهبری‌شان را بر عهده داشت راه خودشان را رفتند و زنجیره را دو تکه (یا «فورک») کردند تا نسخه‌ای جایگزین برای بیت‌کوین یا «بیت‌کوین کش» (Bitcoin Cash) راه‌اندازی کنند که می‌توانست در هر ثانیه تا ۱۱۶ تراکنش را پردازش کند. برک می‌گوید: «این دو تکه شدن بازتابی از دو نسخه متفاوت ماهیت بیت‌کوین بود.» بعد از این فورک‌های دیگری هم رخ دادند.

مسئله اساسی در بسیاری از این اختلاف‌نظرهای ایدئولوژیک موضوع غیرمتمرکزسازی بود. با تبدیل شدن استخراج به کسب‌وکاری شرکتی، یکی از ارکان اعلام‌شده الگوی بیت‌کوین (یعنی پایداری آن) زیر ذره‌بین رفته است. در اوایل سال ۲۰۲۰ معادل ۴۹٫۹ درصد استخراج شبکه بیت‌کوین از طریق پنج شرکت استخراج انجام می‌شد. این شرکت‌ها همه «استخرهای» استخراج مستقر در چین بودند که به ماینرهای خرد این امکان را می‌دادند که منابع‌شان را در کنار هم قرار دهند و بعد عواید را با هم تقسیم کنند.

این تمرکز قدرت زنگ خطری برای شیفتگان غیرمتمرکزسازی است و یکی از این افراد می‌گوید شاید همه این بحث‌های محافل بیت‌کوینی درباره غیرمتمرکزسازی، ظاهرسازی برای پنهان کردن ساختارهای قدرت معمول باشد. «انجلا والش» (Angela Walch)، استاد حقوق دانشگاه «سنت مری» در شهر «سن آنتونیو»ی ایالت «تگزاس» می‌گوید: «غیرمتمرکزسازی معمولاً بیش از آنکه توصیفی واقعی برای سیستم‌ها (در بخش رمزارز) باشد، اصطلاح بازاریابی یا آرمان‌گرایانه است. فکر می‌کنم پوششی برای افرادی است که می‌خواهند طوری جلوه دهند که انگار قدرتی ندارند.» از طرف دیگر، جامعه بیت‌کوین از چند گروه تشکیل شده که به‌نحوی

تأثیرگذاریِ خنثی‌کننده‌ای روی یکدیگر دارند. ماینرها قدرتمندند، اما گردانندگان نودهای کامل غیراستخراجی و همچنین توسعه‌دهندگانی که مخزن داده حاوی کد بیت‌کوین را کنترل می‌کنند (github.com/Bitcoin/Bitcoin) نیز همین‌طورند.

«اندرو میلر» (Andrew Miller)، استادیار دانشگاه «ایلینوی» و عضو هیئت‌مدیره چند شرکت رمزارزی، می‌گوید: «درمورد بیت‌کوین شبیه هر پروژه منبع‌بازی، نفوذها و مناسبات سیاسی وجود دارند. برخی افراد دوست دارند منکر وجود نوعی ساختار سیاسی و اجتماعی شوند که در واقعیت سازوکار بیت‌کوین را عملی می‌کند. این افراد به‌عنوان مثال می‌گویند «این شرایط باید برقرار باشد چون ریاضیات آن را تأیید می‌کند». این حرف‌ها کاملاً پرت‌وپلا هستند. بیت‌کوین در واقع مبتنی بر فرایند توافق اجتماعی است.»

مسئله کلیدی دیگر گمنامی است. سایفرپانک‌ها در آرزوی پول نقد دیجیتالی بودند که در آن هویت کاربر گمنام باشد، اما بیت‌کوین هرگز کاملاً گمنام نبوده است. تراکنش‌ها همه به‌صورت عمومی منتشر می‌شوند و فقط یک اشتباه می‌تواند هویت پشت هر آدرسی را فاش کند. به‌عنوان مثال اگر مظنونی منابع را از طریق کیف پول امانی جابه‌جا کند (کلیدهای رمزنگاری‌شده کیف پول‌های امانی را معمولاً صرافی‌ها نگهداری می‌کنند که اغلب هویت کاربران‌شان را احراز می‌کنند)، احتمال مشخص شدن هویتش بسیار زیاد خواهد بود. با ظهور شرکت‌های امنیتی مثل «چینالیسیس» (Chainalysis) یا «الیپتیک» (Elliptic) که برای برقراری ارتباط بین کیف پول‌ها و اطلاعات شخصی، از تکنیک‌های یادگیری ماشین استفاده می‌کنند، این احتمال بیشتر هم شده است. در چند سال گذشته رمزارزهایی با تمرکز بیشتر بر حریم خصوصی و گمنامی، مثل «مونرو» (Monero)، «زی‌کش» (Zcash) و «گرین» (Grin) عرضه شده‌اند.

مسئله زیست‌محیطی هم وجود دارد که در واقع گناه نخستین بیت‌کوین است. استخراج بیت‌کوین در یک سال به‌اندازه کشور سوئد برق مصرف می‌کند. در دنیایی که به‌شدت تحت‌تأثیر تغییرات اقلیمی قرار گرفته است، تشکیلاتی که عملکردش به مقوله اثبات کار با اتلاف بی‌دلیل مقادیر بسیار زیاد انرژی اتکا دارد، چقدر اخلاقی

است؟ به همین دلیل بیشتر پروژه‌های رمزارز جدید تلاش می‌کنند سازوکار اثبات کار را به‌کلی کنار بگذارند یا نقشه راهی برای کنار گذاشتن آن داشته باشند. اما این ماجرا به‌هیچ‌وجه فقط به بیت‌کوین محدود نمی‌شود.

فصل دوم

اتریوم

به سوی قلمروی ناشناخته اتر

بیت‌کوین حول پول می‌چرخد. ساتوشی ناکاموتو آن را به‌عنوان سیستمی برای جابه‌جایی واحدهای ارزش از فردی به فرد دیگر بدون اتکا به واسطه‌ها طراحی کرد. اما تقریباً بلافاصله بعد از عرضه بیت‌کوین، توسعه‌دهندگان و علاقه‌مندان شروع کردند به جست‌وجو برای پیدا کردن راه‌های استفاده از بلاکچین بیت‌کوین برای کاربردهایی به‌غیر از پول.

ابتدایی‌ترین استفاده، افزودن نظر به تراکنش‌ها بود (همان‌طور که ناکاموتو عنوان روزنامه تایمز را به بلوک جنسیس (اولین بلوک بلاکچین بیت‌کوین) اضافه کرده بود) تا افراد بتوانند پیام‌های سانسورنشدنی و در عین حال عمومی برای یکدیگر بفرستند. این کاربرد می‌توانست پیامدهایی ناخوشایند داشته باشد. مطالعه‌ای در سال ۲۰۱۸ نشان می‌داد که نظرهای روی بلاکچین مملو از صدها لینک به تصاویر پورنوگرافی کودکان‌اند.

اما بیشتر موارد استفاده پیشنهادی «بیت‌کوین ۲.۰» کمتر مخرب و بیشتر خلاقانه بودند. در سال ۲۰۱۱ پروژه‌ای به نام نیم‌کوین مطرح شد که پیشنهاد می‌داد از شبکه بیت‌کوین برای ایجاد سامانه نام دامنه (Domain Name System) غیرمتمرکز استفاده شود. توسعه‌دهندگان در سال ۲۰۱۲ مفهوم «سکه‌های رنگی» (coloured coins) را مطرح کردند: سکه‌های رنگی مقادیر کمی بیت‌کوین بودند که با روش‌هایی متمایزکننده برچسب‌گذاری می‌شدند و بدل‌های قابل‌معامله آسان برای دارایی‌هایی مثل اوراق قرضه، شمش طلا یا سند ملک بودند.

این ایده‌ها در تقابل با این واقعیت بودند که بیت‌کوین سیستمی تک‌بعدی بود که با مشکلات مقیاس‌پذیری دست‌وپنجه نرم می‌کرد و با بزرگ‌تر شدن جامعه‌اش مدام دچار تغییرات می‌شد. هر پروژه‌ای که روی این زیرساخت بنا می‌شد ممکن بود با این تغییرات به خطر بیفتد. وقتی بیت‌کوین در آوریل ۲۰۱۳ حداقل مقدار تراکنش را ۵.۴۳۰ ساتوشی تعیین کرد، حامیان کوین رنگی این اقدام را به‌عنوان عقب‌گرد نکوهش کردند.

راهی احتمالی برای برطرف کردن این معضل این بود که هر پروژه‌ای بلاکچین و کوین خودش را با کارکردی ویژه عرضه کند. مشکل این رویکرد این بود که در جهانی مملو از هزاران بلاکچین، قابلیت تعامل وجود نخواهد داشت؛ هر بلاکچین به جزیره کریپتویی محصوری با استانداردها و کوین انحصاری خودش تبدیل می‌شد و هیچ راه روشنی برای استفاده از هم‌افزایی با سایر بلاکچین‌های مشابه وجود نداشت. ناهم‌خوانی گسترش می‌یافت. گزینه جایگزین این بود که از چندپارگی اجتناب کنیم و بلاکچینی واحد بسازیم که به‌نحوی طراحی شده باشد که سایر پروژه‌ها (کوین‌ها) بتوانند در بستر آن ساخته شوند. یکی از حامیان این رویکرد دوم ویتالیک بوترین بود.

از آشنایی بوترین با بیت‌کوین در سال ۲۰۱۱ مدتی گذشته و تجربه‌های گوناگونی را از سر گذرانده بود. بعد از اینکه توسعه‌دهنده بازی آنلاین چندنفره «دنیای وارکرفت» (World of Warcraft) ناگهان توانایی ویژه‌ای را به یکی از شخصیت‌های این بازی اعطا کرد، این بازی را کنار گذاشته بود. بوترین می‌گوید این تجربه باعث شد بفهمد «خدمات متمرکز می‌توانند چه اتفاقات وحشتناکی را رقم بزنند». هنوز از این تجربه خشمگین بود. بوترین ابتدا به ایده ناکاموتو بدبین بود، اما به‌تدریج مجذوب آن شد. به همراه فردی که در محیط آنلاین با یکدیگر آشنا شده بودند، مجله بیت‌کوین را راه‌اندازی کرد و نویسنده ارشد این رسانه شد. اولین مقاله‌اش درباره این موضوع بود که چرا نوجوانانی مثل خودش باید از بیت‌کوین استفاده کنند.

بوترین در تصمیمی هوشمندانه قصد نداشت روزنامه‌نگاری کسب‌وکار را به‌عنوان شغل ادامه دهد. بوترین به‌عنوان برنامه‌نویس بااستعداد، علاقه‌مند به اقتصاد و فردی که بعداً بورس بنیاد «پیتر تیل» (Peter Thiel)، یکی از چهره‌های مطرح سیلیکون ولی، را دریافت کرد، از مجله بیت‌کوین برای آشنایی با پروژه‌های رمزارزی و مشارکت در آن‌ها و بستری برای گسترش ایده‌هایش درباره این حوزه استفاده کرد. تا سال ۲۰۱۳ به این جمع‌بندی رسید که این بخش در چرخه تکراری اشتباهی گرفتار شده است. همه می‌خواستند کارکردهایی را به بیت‌کوین اضافه کنند که برای انجام آن‌ها ساخته نشده بود. توسعه‌دهندگان تلاش می‌کردند اپلیکیشن‌های آنلاین را در بستری اجرا کنند که اساساً چیزی شبیه پروتکل ایمیل بود. برای ساخت سیستمی پیچیده‌تر از سیستم

ایمیل (چیزی شبیه خدمات آنلاین و اپلیکیشن‌های متصل به اینترنت) به پلتفرمی نیاز دارید که شبیه اینترنت رفتار کند. بوترین فکر می‌کرد می‌تواند این اینترنت غیرمتمرکز را برنامه‌نویسی کند و در وایت‌پیپری که در اواخر سال ۲۰۱۳ منتشر کرد، آن را اتریوم نامید.

رونمایی باشکوه اتریوم در ژانویه ۲۰۱۴ در همایش بیت‌کوین آمریکای شمالی (North American Bitcoin Conference) در شهر «میامی» انجام شد، جایی که بوترین برنامه‌اش را در یک ارائه طولانی ۲۸ دقیقه‌ای مفصل توضیح داد. همان‌جا مشخص شد که چهره‌ای کاریزماتیک خواهد شد. بسیار جوان بود، اما فوق‌العاده درمورد مسائل فنی به خودش اطمینان داشت، در استفاده از استعاره‌ها و شوخی‌های نامتعارف ماهر بود، در ارائه ناشی (گاهی تپق می‌زد و تیک‌های کلامی داشت)، در عین حال میخ‌کوب‌کننده بود. ویتالیک بوترین با قد بلند، اندام بسیار باریک و چشمان آبی نافذی که به دوردست خیره شده بودند، همان تصور گیک‌ها از منجی موعود را بازنمایی می‌کرد. تمام افسانه‌هایی که در سال‌های بعد درمورد او مطرح شدند (اینکه آی‌کیوی او ۲۵۷ است، ماندارین را در دو ماه یاد گرفته و آدم‌فضایی است)، از همان لحظه‌ای شکل گرفتند که سخنرانی‌اش در میامی را با تشویق پرهیجان حاضران به پایان رساند.

پیشنهاد بوترین بیت‌کوینی به همراه نتایج و پیامدها بود. در حالی که تراکنش بیت‌کوین شبیه این است که فردی سکه‌ای را به فردی دیگر بدهد، تراکنش اتریوم قرار بود شبیه وارد کردن سکه در دستگاه فروش خودکار و بلافاصله دریافت یک فنجان قهوه داغ در سینی باشد. در حالی که شبکه بیت‌کوین اطمینان حاصل می‌کرد که هیچ‌کس نمی‌تواند تغییر مالکیت پول را متوقف یا معکوس کند، اتریوم می‌توانست گام دیگری هم بردارد: اطمینان حاصل کند که پرداخت به نتیجه مورد انتظار پرداخت‌کننده، یعنی عرضه معادل دیجیتال همان فنجان قهوه، منجر می‌شود.

بلاکچین اتریوم که سرانجام در ژوئیه ۲۰۱۵ عملیاتی شد به‌نحوی طراحی شده که از دو نوع حساب پشتیبانی کند: آدرس‌های استاندارد شبیه بیت‌کوین که کاربران می‌توانند با استفاده از آن‌ها رمزارز اتریوم، یعنی اتر، را ارسال و دریافت کنند و

حساب‌های قرارداد که آدرس‌های خودکاری هستند که شبیه دستگاه‌های فروش خودکار عمل می‌کنند. حساب‌های قرارداد مبتنی بر مفهوم «قرارداد هوشمند» هستند. قرارداد هوشمند ایده‌ای بود که «نیک زابو»، سایفرپانک معروف، در مقاله‌ای در سال ۱۹۹۶ مطرح کرد که به بررسی این موضوع می‌پرداخت که فناوری دیجیتال چطور امکان ایجاد نوعی از توافق‌نامه‌های مالی را فراهم کرده که اجرای آن‌ها به وکلا یا واسطه‌ها وابسته نیست و در کدهای کامپیوتری تعبیه و به‌صورتی گریزناپذیر اجرا می‌شوند.

ارسال تراکنش پرداخت (یا هر ورودی دیگری مثل پیام) به حساب قرارداد اتریوم به‌طور خودکار به اجرای کد قرارداد منجر می‌شود. به‌عنوان مثال قرارداد را می‌توان به‌نحوی برنامه‌نویسی کرد که بلافاصله توکن دیجیتال نماینده یک سند ملکی (شبیه سکه‌های رنگی) را به هر فردی منتقل کند که با اتر هزینه آن را پرداخت می‌کند. همچنین ممکن است نقش حساب امانی بین دو طرف را ایفا کند، یعنی اترها را به‌صورت امن نگه دارد تا زمانی که پرداخت‌کننده خریدش را دریافت کند و اجازه ارسال مبلغ به دریافت‌کننده را بدهد. یا ممکن است قراردادی به‌نحوی طراحی شود که گزارش‌های هواشناسی را از منبعی خارجی (که در شبکه اتریوم «اوراکل» (oracle) خوانده می‌شود) دریافت و به‌صورت خودکار به کشاورزانی که احتمالاً به دلیل گرمای شدید یا باران سیل‌آسا زیان خواهند دید خسارت بیمه‌ای پرداخت کند.

بوترین اتریوم را با عبارت «تورینگ کامل» (Turing complete) توصیف کرد که یعنی قراردادهای هوشمند را می‌توان به‌نحوی طراحی کرد که تقریباً هر عملیات قابل‌تصوری را از طریق ترکیبی از تعداد زیادی فرمان متفاوت اجرا کنند (تا اوت ۲۰۲۰، درمجموع ۱۴۲ فرمان یا «آپ‌کد» (opcode) ایجاد شده است). در اتریوم هرکسی می‌تواند با قرار دادن کد منبع قرارداد در شبکه از طریق تراکنش، حساب قرارداد ایجاد کند.

به‌گفته معماران اتریوم، مزیت قراردادهای هوشمند (برخلاف بلاکچین ساده و ابتدایی بیت‌کوین) این است که علاوه بر اینکه امکان اجرای عملیات‌های پیچیده‌تر را فراهم می‌کنند، سطحی از قابلیت اعتماد را ایجاد می‌کنند که هیچ قرارداد ساخته بشری نمی‌تواند حتی به گرد پای آن برسد. در یلو پیپری (Yellow Paper) فنی که در

سال ۲۰۱۵ منتشر شد، «گوین وود» (Gavin Wood)، متخصص کامپیوتر بریتانیایی که به همراه بوترین و توسعه‌دهنده دیگری به نام «جفری ویکل» (Jeffrey Wilcke) بیشتر کدهای اتریوم را نوشته‌اند، این‌طور گفته بود: «فسادناپذیری قضاوت که اغلب کمیاب است، به‌آسانی در دسترس یک مفسر الگوریتمی بی‌طرف قرار دارد.»

در ادامه می‌نویسد: «شفافیت یا این توانایی که از طریق لاگ تراکنش و قوانین یا کدهای فرمان دقیقاً ببینیم وضعیت یا قضاوتی چطور اتفاق افتاده است، هیچ‌وقت به‌طور کامل در سیستم‌های متکی به انسان محقق نمی‌شود چراکه زبان طبیعی ناگزیر مبهم است، اطلاعات اغلب کامل نیستند و حذف سوگیری‌های متداول دشوار است.»

پیش‌زمینه‌ای بسیار سیاسی برای این موضعِ گوین وود وجود دارد. وود در سال ۲۰۱۹ گفته بود که پنج سال پیش، وقتی «ادوارد اسنودن»، پیمانکار سابق آژانس امنیت ملی، برنامه نظارت الکترونیکی جهانی ایالات متحده را برملا کرده بود، همدلی عمیقی نسبت به اسنودن احساس کرده بود. وود می‌گوید: «متوجه شدم پروژه‌ای که روی آن کار می‌کنم، یعنی اتریوم، اساساً بخشی از جنبشی است که اسنودن هم دنبال می‌کند.» هدف این جنبش که وود نامش را وب ۳.۰ گذاشته بود، جایگزینی مراکز قدرت غیرشفاف و سلطه‌جویانه با شبکه‌های شفاف بود. وود می‌گوید: «آرمان وب۳.۰ را این‌طور می‌توان خلاصه کرد: وابستگی کمتر به اعتماد و حقیقت بیشتر.»

از نقطه‌نظر اتریوم، سروکار داشتن با طرف‌های مقابل و سازمان‌های انسانی همیشه مستلزم وجود اعتماد است: اعتماد به اینکه حرف و نیت‌شان یکی است، اعتماد به اینکه منطقی عمل می‌کنند، اعتماد به اینکه شیاد نیستند و اعتماد به اینکه از شما جاسوسی نمی‌کنند. اما در طرف دیگر، قوانین زیربنایی قراردادهای هوشمند خوداجراشونده و بی‌نیاز به اعتمادند. این قراردادها در بلاکچین در دسترس همه هستند و دقیقاً همان کاری را می‌کنند که می‌گویند و نیاز به اعتماد کردن را از بین می‌برند. البته با این پیش‌فرض که اجرای کد قرارداد هوشمند برای تحقق آثارش کافی باشد. فرض خطرناکی است که بعداً برای جامعه اتریوم مشکل ایجاد می‌کند.

اینکه کدهای کامپیوتری مجموعه‌ای از فرمان‌ها را اجرا کنند، در واقع چندان

هیچ ندیده‌ای هنوز

انتشارات راه‌پرداخت

برای سفارش اینترنتی این کتاب به وبسایت انتشارات راه‌پرداخت مراجعه کنید
way2pay.shop

طی دهه گذشته رشد مداوم کریپتوکارنسی به عنوان شکل جایگزین ارز را شاهد بوده‌ایم. اما کریپتوکارنسی دقیقاً چیست و پتانسیلش برای تغییر دنیای پول چگونه است؟ در این کتاب جیان واپیسلی، از نشریه وایرد، هر چیزی را که باید درباره کریپتوکارنسی بدانید توضیح می‌دهد. او به شکل گیری و توسعه این نوع پول اشاره و توضیحی دقیق درباره کارکرد آن ارائه می‌دهد. همچنین ابهامات پیرامون اصطلاحات این حوزه، از بلاکچین، بیت کوین و استیبل کوین تا استخراج، قراردادهای هوشمند و فورک را از بین می‌برد. همین طور مروری بر ایدئولوژی‌های سیاسی و اقتصادی‌ای ارائه می‌دهد که محرک کریپتوکارنسی‌ها هستند و به سؤالی اساسی اشاره می‌کند: آیا کریپتوکارنسی تأثیر تحول آفرین اقتصادی و اجتماعی‌ای را که طرفدارانش ادعا می‌کنند، دارد؟

کتاب «کریپتوکارنسی» را می‌توان کتاب آموزش الفبای مهم‌ترین دوره‌ها در تاریخ کریپتوکارنسی تلقی کرد که از دهه ۱۹۹۰ شروع و تا به امروز می‌رسد. نویسنده دورنمایی را به تصویر می‌کشد که به ساخت بیت کوین توسط ساتوشی ناکاموتو منجر شد و به حباب عرضه اولیه سکه و استیبل کوین رسید و به لیبرا و دیفای ختم شد.

ISBN 978-622-7782-15-6
۱۱۶ هزار تومان
انتشارات راه پرداخت
ناشر فناوری و نوآوری
way2pay.press