بلاکچین، رمزارز و اقتصاد توکن چگونه دنیای مالی را دگرگون می‌کنند

اقتصاد کریپتو

آریس وان لین وانگ

مترجمان: علیرضا نواب پور، محمدرضا قدوسی

INDEPENDENTLY PUBLISHED


بسم الله
الرحمن
الرحيم

سرشناسه: وانگ، آریس وانلین. Wang, Aries Wanlin
عنوان و نام پدید آور: اقتصاد کریپتو: بلاکچین، رمزارز و اقتصاد توکن چگونه دنیای مالی را دگرگون می کنند
نویسنده: آریس وان لین وانگ
مترجمان: علیرضا نواب پور، محمدرضا قدوسی
مشخصات نشر: تهران: راه پرداخت، ۱۴۰۱.
مشخصات ظاهری: ۱۱۶ص.
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۳۲-۳
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: عنوان اصلی: Crypto economy: how blockchain, cryptocurrency, and token-economy are disrupting the financial world, 2018.
عنوان دیگر: بلاکچین، رمزارز و اقتصاد توکن چگونه دنیای مالی را دگرگون می کنند.
موضوع: بانکداری اینترنتی
موضوع: پول - نوآوری
موضوع: رمزارز
شناسه افزوده: قدوسی، محمدرضا، ۱۳۶۷ -، مترجم
شناسه افزوده: نواب پور، علیرضا، ۱۳۷۰-
رده بندی کنگره: HG۱۷۰۸/۷
رده بندی دیویی: ۳۳۲/۱۰۲۸۵
شماره کتابشناسی ملی: ۸۹۰۷۰۴۰

بلاکچین، رمزارز و اقتصاد توکن چگونه دنیای مالی را دگرگون می‌کنند

اقتصاد کریپتو

آریس وان لین وانگ

مترجمان: علیرضا نواب‌پور، محمدرضا قدوسی

INDEPENDENTLY PUBLISHED

انتشارات
راه‌پرداخت

عنوان : اقتصاد کریپتو
ناشر : تهران: راه پرداخت، ۱۴۰۱.
نویسنده: آریس‌وان‌لین وانگ
مترجمان: علیرضا نواب‌پور، محمدرضا قدوسی
ویراستار ارشد : مینا والی
ویراستار محتوایی : قاسم سرافرازی
ویراستار فنی: یلدا شایسته‌فر
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا : علیرضا کیوان
ناظر چاپ : قادر شهبازی
نوبت چاپ:اول ۱۴۰۱
شمارگان : ۱۰۰ نسخه
شابک: ۳-۳۲-۷۷۰۲-۶۲۲-۹۷۸
تلفن : ۰۲۱-۴۴۴۳۹۶۶
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 press Way2Pay.press @Way2Pay_Network

فهرست

پیش‌گفتار

پیش‌گفتار از کوین‌بری[1]، مدیرعامل شرکت مینتوم[2]

«هیچ چیز قدرتمندتر از ایده‌ای نیست که زمان آن فرا رسیده باشد.»

ویکتور هوگو

ما در نقطه تحول تراکنش‌های مالی در سراسر جهان هستیم. چه کسی تغییر را در آغوش می‌گیرد و چه کسی آن را پشت سر می‌گذارد؟ تمرکززدایی، اعتماد، حریم شخصی و دموکراتیزه‌کردن معاملات مالی همه ایده‌هایی هستند که زمان تحقق‌شان فرا رسیده است. فناوری بلاکچین قطعا این ایده‌ها را طی چند سال آینده هدایت خواهد کرد. سوال این است: این اتفاق کجا خواهد افتاد؟ برخی دولت‌ها فناوری آینده را در آغوش خواهند گرفت و سایرین در برابر وضع موجود مقاومت خواهند کرد. چه کسی برنده می‌شود و چه کسی می‌بازد؟

در کتاب «اقتصاد کریپتو[3]: بلاکچین، رمزارز و اقتصاد توکن چگونه دنیای مالی را دگرگون می‌کنند» اریس وانلین وانگ[4] تشریح کرده که چگونه این اقتصاد مانند انقلابی جدید عمل خواهد کرد. او به‌عنوان یک شخص فعال که هم‌بنیان‌گذار یک صرافی رمزارز بوده و عملکرد موفقی در اقتصاد کریپتو طی چند سال داشته است، یک راهنمای نهایی به سمت چیزی است که گاهی اقتصاد جدید را دچار سردرگمی می‌کند. خوانندگان بی‌شک از چشم‌انداز وی و درکش از نگرانی‌ها و انگیزه‌های افرادی که کارهای اقتصادی می‌کنند، بهره خواهند برد.

در طول تجربه حرفه‌ای‌ام، بینشی در مورد نگرانی‌ها و انگیزه‌های ملت‌های گوناگون و رگولاتورهای این فناوری جدید حاصل کردم. به‌عنوان یک نماینده سازمان غیرانتفاعی (NGO) در ایالات متحده در شهر نیویورک، من نگرانی‌های وزیران فناوری اطلاعات را از چند کشور در سراسر جهان شنیدم. من یک وکیل مدافع دولت ایالات متحده هستم، بنابراین در مورد اینکه چگونه رگولاتورهای دولتی در زمان مواجهه با فناوری‌های جدید واکنش نشان می‌دهند، بینشی دارم. من همچنین مدیرعامل یک استارت‌آپ به نام «مینتوم» هستم که در

1. Kevin Barry
2. Myntum Limited
3. Crypto Economy
4. Aries Wanlin Wang

حال ساخت خزانه آنلاین[1] برای تامین امنیت دارایی‌های دیجیتالی بااهمیت (مانند توکن‌ها و رمزارزها) است. به همین دلیل، من از نزدیک شاهد توسعه اقتصاد کریپتو در دو دهه گذشته بودم. در نهایت، من موسس یک سازمان غیرانتفاعی به نام «اولین آزادی‌ها»[2] هستم که باعث پیشرفت پنج آزادی فهرست‌شده در اولین اصلاحیه برای قانون اساسی ایالات متحده شد (آزادی مذهب، گفتار، مطبوعات، تجمعات و جبران نارضایتی[3]). چه پیوندی بین این اصلاحیه و اقتصاد کریپتو وجود دارد؟

مبنای هر دوی آنها «آزادی» است. در اواخر قرن ۱۸، ایده‌ها و ایده‌آل‌های اولین اصلاحیه به بخشی از بستر تاکید آمریکا بر آزادی فردی تبدیل شد. حال زمان ایده‌ها و ایده‌آل‌های بلاکچین و اقتصاد کریپتو فرا رسیده است. هم‌اکنون سوالاتی به وجود می‌آیند که باید بررسی شوند:

- متمرکزسازی یا تمرکززدایی؟
- اعتماد بین طرفین یا یک شخص ثالث برای تضمین اعتماد؟
- شفافیت معاملات یا معاملات پنهان و مبهم؟
- یک جهان بدون مرز با تاثیر سیاسی کمتر یا یک جهان دارای مرز با تاثیر سیاسی بیشتر؟
- تامین مالی جمعی[4] برای کسب‌وکارهای جدید یا فقط سرمایه‌گذاری جسورانه[5]، بانک‌های سرمایه‌گذاری (شرکت‌های تامین سرمایه) و دولت‌ها؟

اینها تنها چند ایده‌ای هستند که شهروندان، کسب‌وکارها و تنظیم‌گران دولت مجبور به بررسی آنها هستند. چگونه دولت‌ها در مورد فناوری جدید تصمیم می‌گیرند؟ در کل، دولت‌ها سه گزینه دارند؛ پشتیبانی، مخالفت، بدون هیچ موضعی. اقتصاد کریپتو، موضع پشتیبان یا بی‌طرفی نسبت به دولت‌ها را ترجیح می‌دهد. برای انجام این کار، بیشتر افراد در اقتصاد کریپتو می‌دانند برای کمک به رشد اقتصاد جدید جهت تنظیم مقررات هوشمندانه نیازمند کار با دولت‌های دارای حوزه‌های قضایی مختلف هستند. کار با حوزه‌های قضایی دوستانه برای ایجاد رشد در اقتصاد کریپتوی جدید، احتمال متقاعدکردن دولت‌هایی را فراهم می‌کند که

1. Online vaults
2. First Freedoms
3. Redress of grievances
4. Crowdfunding
5. Venture capital

با تغییر سیاست‌های خود مخالف هستند. پس، تمرکززدایی یا متمرکزسازی؟ قرن‌هاست، معاملات مالی نیازمند بانک‌های متمرکز، نهادهای مالی یا سرمایه‌دارانی همانند بانک‌های ملی، بانک‌های تجاری و صادرکنندگان کارت اعتباری است تا به‌عنوان «شخص ثالث مورد اعتماد» برای تسهیل معاملات طرفین ایفای نقش کنند. زمانی که فناوری بلاکچین در سال ۲۰۰۸ به وجود آمد، هیچ‌کس روش معقول و امنی را برای دورزدن بانک‌ها نداشت. با فناوری بلاکچین، افراد و کسب‌وکارها برای اولین بار قدرتی برای معامله مستقیم با یکدیگر پیدا کردند. این ایده‌آل به نظر می‌رسد، اما جای مطالعه و بررسی بیشتری دارد و من باور دارم که گاهی داشتن یک شخص ثالث مورد اعتماد گزینه خوبی است. آیا برای تضمین اعتماد، به یک شخص ثالث یا اعتماد طرفین نیاز داریم؟ اقتصاد کریپتو این امکان را برای افراد و کسب‌وکارها فراهم می‌کند که یا به‌طور مستقیم با یکدیگر معامله کنند یا به‌طور سنتی از سیستم پولی حاکمیتی (فیات[1]) یعنی با وجود یک شخص ثالث استفاده کنند. من باور دارم که در آینده، رمزارز برای خریدهای نسبتا کوچک و پول فیات برای اهداف نسبتا بزرگ استفاده خواهد شد. در این زمان، هیچ متد خوبی برای حل اختلاف در بازارهای رمزارز وجود ندارد. در دنیای رمزنگاری جای اعتراض وجود ندارد. اگر یک معامله بد پیش برود، هیچ‌کسی وجود ندارد که بتوان به او شکایت کرد. به کدام حوزه قضایی شکایت خود را اعلام می‌کنید؟ باور دارم که در آینده نزدیک افراد درگیر در معاملات بزرگ استفاده از اقتصاد سنتی را ادامه می‌دهند، اما این هنوز یک خبر خوب برای دنیای کریپتو است! بیشتر معاملات روتین هر روز، معاملات کوچکی‌اند که برای رمزارزها مناسب هستند.

شفافیت معاملات یا معاملات مبهم و نهان؟

معاملات رمزارزها در دفاتر عمومی[2] برای دید عموم، شفاف هستند. هر بیت‌کوین[3] تنها یک بار می‌تواند استفاده شود. این مساله یک خروج اساسی از اقتصاد سنتی فیات که از یک دلار چند بار استفاده می‌کند، به سمت اقتصاد کریپتو است. ری دالیو[4] از همکاران Bridgewater

1. Fiat
2. Public ledger
3. Bitcoin
4. Ray Dalio

در مقاله «ماشین اقتصاد چگونه کار می‌کند» مورد زیر را تشریح کرده است:

«تقریبا همه آنچه فدرال رزرو، پول می‌نامد در حقیقت «اعتبار» است (یعنی وعده تحویل پول). مجموع کل بدهی در آمریکا حدود ۵۰ تریلیون دلار و مجموع مقدار پول (ارز و ذخایر) در حال حاضر سه تریلیون دلار است. بنابراین اگر ما از این اعداد به‌عنوان یک شاخص استفاده کنیم، مقدار وعده‌ها برای ارائه پول (مانند بدهی) تقریبا ۱۵ برابر مقدار پول ارائه‌شده است.

تا زمانی که چرخ‌های این ماشین اقتصادی می‌چرخد، موسیقی نواخته می‌شود و هیچ‌کس برای آن تقلا نمی‌کند، اما اگر زمانی موسیقی متوقف شود، ۵۰ نفر برای این سه کرسی به مبارزه می‌پردازند. این چیزی است که در بحران‌های اقتصادی رخ می‌دهد، اما به‌دلیل اینکه هر بیت‌کوین فقط یک بار می‌تواند استفاده شود، این مساله رخ نمی‌دهد.»

یک جهان بدون مرز با تاثیر سیاسی کمتر یا یک جهان دارای مرز با تاثیر سیاسی بیشتر؟

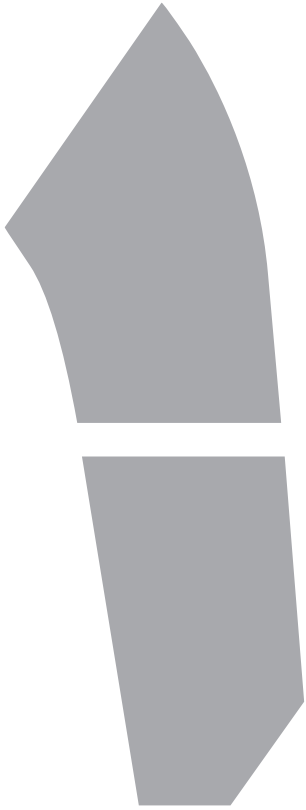
من یک ایده‌آلیست هستم. من بسیار به ایده جهان بدون مرز توجه کرده‌ام. فناوری بدون مرز است و معاملات مالی به صورت تئوری می‌توانند بدون مرز باشند. در اقتصاد فیات سنتی و در اقتصاد کریپتو، دارایی‌ها می‌توانند با یک کلیک به هر جایی ارسال شوند. با این وجود، این حقیقت نیست. دولت‌ها گاهی اوقات به اختلاف و مشکل برمی‌خورند و شهروندان را از انجام کسب‌وکار با یکدیگر منع می‌کنند. کسب‌وکارها و افراد باید به تحریم‌هایی که بر کشور آنها اعمال شده است، احترام بگذارند. این یک اصل تجاری کوچک است: به هر رگولاتوری که می‌تواند شما را تعطیل کند، محاکمه کند، جریمه یا زندانی کند، احترام بگذارید.

رمزارزها به‌عنوان یک جهان بدون مرز کمتر تحت تاثیر سیاست هستند. بنابراین الگوریتم‌ها به رقابت‌های سیاسی منفی با یکدیگر منجر نمی‌شوند. الگوریتم‌ها به جنگ‌های تجاری وارد نمی‌شوند. الگوریتم‌ها رقابت‌های تاریخی، جاه‌طلبی‌های نظامی یا رهبرانی در جست‌وجوی شکوه و عظمت ندارند. جهان بدون مرز و رمزارزها پتانسیل زیادی برای دموکراتیزه‌کردن معاملات اقتصادی و فرصت اقتصادی برای بهره‌مندی همه افراد جهان را دارند.

آیا تامین مالی جمعی، فقط برای کسب‌وکارهای جدید یا سرمایه‌گذاری جسورانه، بانک‌های سرمایه‌گذاری و دولتی است؟

عرضه اولیه سکه[1] که معمولا آن را رویدادهای تولید توکن (TGE[2]) می‌نامیم، یک نوع تامین مالی جمعی است. من باور دارم که این دموکراتیزه‌کردن افزایش سرمایه کسب‌وکارها اگر با مقررات هوشمندانه‌ای همراه باشد، موفقیت‌های بزرگی را به همراه خواهد داشت. دولت‌ها علاقه‌مند به توقف تقلب‌ها هستند. این یک دغدغه صحیح هم در اقتصاد سنتی و هم اقتصاد کریپتو است. مقررات در TGE از کشوری به کشور دیگر متفاوت است. کشورهای G20 با بزرگ‌ترین اقتصاد، معمولا مراقب وضع موجود هستند. بسیاری از ۱۸۰ کشور که در G20 نیستند به آزمایش و تجربه تمایل دارند. ۲۰ اقتصاد برتر در جهان ۸۰ درصد ثروت جهان را دارند. ۱۷۲ کشور دیگر نسبت به شرایط فعلی کمتر هیجان‌زده‌اند و اقتصاد کریپتو را متفاوت می‌بینند. این یک موضوع تکراری مکالمات در ایالات متحده است. جهان در حال توسعه؛ اقتصاد کریپتو و فناوری بلاکچین را به‌عنوان یک روش بالقوه برای بهبود زندگی شهروندان از طریق TGE می‌بینند. اقتصاد کریپتو و رهبران بلاکچین نیاز دارند که با تنظیم‌گران حاکمیتی برای شناساندن پتانسیل فناوری به آنها همکاری کنند. مهم است درک کنیم که کشورها ارز خود را جدی می‌گیرند. برنامه‌ریزان دولتی در ایالات متحده، چین و اتحادیه اروپا در مورد پتانسیل سرمایه‌گذاری نگران هستند. اقتصاددانان در کشورهای G20 اگر نتوانند در مورد چگونگی ردیابی هر معامله تصمیم بگیرند، ممکن است پروژه‌ها را بر اساس اطلاعات ناقص انجام دهند. مالیات دولتی مشکل بزرگی است. اقتصاد کریپتو نیازمند کار با دولت‌ها با توجه به مالیات‌بندی با بلوغ بازار است. این همکاری یک برخورد فرهنگی پیچیده است، اما من فکر می‌کنم این ضروری است و همه احزاب در بلندمدت از آن بهره‌مند می‌شوند. کشورها نمی‌خواهند در مقابل پیشرفت بهترین شهروندان خود که قصد راه‌اندازی کسب‌وکار و ایجاد شغل‌هایی فراتر از مرزها دارند، بایستند. اصلاحیه اول قانون اساسی ایالات متحده، آزادی فردی را تشویق می‌کند و به ایجاد قراردادی بین شهروندان و دولت در بیش از ۲۰۰ سال کمک می‌کند. من باور دارم که اقتصاد کریپتو و فناوری بلاکچین می‌تواند آزادی اقتصادی را برای افراد تقویت کرده و روش تجارت فعلی را بازنویسی کند.

1. Initial Coin Offerings
2. Token Generating Events



فصل اول

چگونه چیزی شبیه بیت‌کوین رخ می‌دهد؟

در اواخر سال ۲۰۰۸، در سایه شدیدترین بحران‌های اقتصادی عصر حاضر، یک انقلاب جدید در شکل پول پدید آمد. ابتدا، هیچ نشانه‌ای مبنی بر اینکه فرم مبهم پول الکترونیکی مهم‌ترین نوآوری مالی قرن بیست‌ویکم است، یک ابزار که می‌تواند توسط افراد، اقتصاد و شرکت‌ها در سراسر جهان توسعه یابد، وجود نداشت. در اکتبر همان سال، یک وایت‌پیپر توسط یک شخص یا گروه گمنامی که خود را ساتوشی ناکاموتو نامیدند، منتشر شد که ارز دیجیتالی را تحت عنوان بیت‌کوین به همراه فناوری پایه آن، برای اولین‌بار معرفی کرد. چند نکته در این تشریح ابتدایی وجود دارد که هر کسی که در مورد بیت‌کوین فکر می‌کند، قدرت پیشرفت و انقلاب در نظام مالی جهانی را نیز احساس می‌کند. آن زمان موفقیت بیت‌کوین کاملا محرز نبود.

در روزهای اولیه آن، بیت‌کوین عجیب و غریب دیده شد؛ چیزی که فقط به‌منظور متقاعدکردن متخصصان رمزنگاری بود. ۱۰ سال پیش، عموم مردم با رمزارز آشنا نبودند. تنها برای متخصصان قابل فهم بود. البته امروزه، نام «بیت‌کوین» به‌عنوان نماینده کلیه رمزارزها به کار می‌رود؛ چراکه دارای بالاترین ارزش در بازار رمزارزهاست. علاوه بر این، مقدار زیادی از توجهات را به فناوری «بلاکچین» جلب کرده است؛ فناوری که بر اساس آن ساخته شده است (اگر در یک کنفرانس بلاکچین شرکت کرده باشید، به‌درستی انتظارات بزرگ مردم از آینده فناوری بلاکچین را احساس می‌کنید...). بیت‌کوین بالا و پایین زیادی را تجربه کرده، اما این شور و اشتیاق کاهش نیافته است. بلاکچین از ابتدا به‌عنوان «فضای ذخیره» برای بیت‌کوین توسعه یافته است؛ چیزی که معاملات را ثبت می‌کند و از احتمال اینکه ارز به‌صورت نامناسبی استفاده شود، جلوگیری می‌کند. تمرکز این کتاب بر پشتوانه تکنیکال رمزارزهاست و اقتصاد کریپتو آن را ممکن می‌سازد. اما قبل از اینکه به اهمیت آن برسیم، نیاز داریم که دقایقی را به بیت‌کوین و تاریخچه آن بپردازیم، چراکه بیت‌کوین محرک اقتصاد کریپتو است و به همین دلیل بسیار مهم است.

فاجعه بحران وام مسکن در سال ۲۰۰۸ اعتماد عموم مردم به بانک‌ها، دولت‌ها و دیگر موسسات قدرتمند را از بین برد؛ همان نهادهایی که به‌عنوان یک نهاد منسجم دیده می‌شدند و برای همه نسل‌ها قابل اطمینان به نظر می‌رسیدند. حال، جهان به‌دنبال راه‌حل‌های جدید است. در این موقعیت، بیت‌کوین مانند یک توپ جادویی به نظر می‌رسد

که برای حل بسیاری از مسائلی که از بحران مالی ناشی شده‌اند، طراحی شده است. بیت‌کوین قدرت را تمرکززدایی می‌کند و هیچ داور یا تنظیم‌گر خارجی که بتواند ما را شکست دهد، وجود ندارد. در مقابل، قدرت به‌درستی در دست مردم ـ کاربران رمزارزها ـ است.

اما شاید بیت‌کوین به‌دلیل اینکه در زمان درست پا به عرصه ظهور گذاشت، موفقیت‌آمیز بود. باید اعتراف کرد بیت‌کوین رمز و رازی دارد؛ جذابیتی که بسیاری از آنها عاشقانه و جسورانه بودند. بیت‌کوین در ابتدا منحصربه‌فرد بود، مانند یک کلوپ که افراد می‌خواهند به آن بپیوندند. بیت‌کوین در وهله اول توسط گروه‌های بسیار کوچک ـ کارشناسان رمزنگاری و شیفتگان فناوری که به آزادی فردی حساس بودند ـ شناخته شد. درست مانند آنچه در مسیر هر برند انحصاری است، بیت‌کوین نیز به‌تدریج خود را به توده‌های مختلف مردم شناساند. هم‌اکنون همان‌طور که مصرف‌کنندگان رمزارز برای گرفتن آن تقلا می‌کنند، به‌درستی درک نمی‌کنند که ارز چیست و چه قدرت انتقالی را داراست. اما بر ماست که در این‌باره بحث کنیم، بنابراین نیاز داریم که نگاهی به تاریخچه پول بیندازیم.

سومر یک تمدن کهن است که در مسوپوتامیا[1] حدود سه‌هزار سال قبل از میلاد تاسیس شد. سومریان به‌عنوان اولین کسانی که از پول به‌عنوان واسطه‌ای برای تسهیل در مبادلات استفاده می‌کردند، شناخته می‌شوند. قبل از سومریان، انسان‌ها اغلب از یک سیستم دادوستد کالایی برای مبادلات استفاده می‌کردند؛ تبادل چیزهای فیزیکی با یکدیگر که مشکلات زیادی را برای یک سیستم دادوستد به همراه داشت.

برای مثال، فرض کنید زمستان است و شما برای گرمایش منزل خود چوب می‌خواهید. شما گاو و گوسفند دارید. همسایه شما درخت دارد و برای خانواده خود گوشت نیاز دارد. شما و همسایه شما باید از یک ترتیب دادوستد استفاده کنید؛ یک گوسفند در ازای ۲۰ بسته چوب. شما به وی گوسفند می‌دهید و او به شما چوب می‌دهد. مطمئنا، این کار صورت می‌گیرد، اما نه به آسانی استفاده از پول.

تبادل کالا به کالا بدون یک واسطه پذیرفته‌شده جهانی مشکلات و مسائل بسیاری را با خود به همراه دارد. اگر شما هیچ‌یک از کالاهایی را که همسایه‌تان نیاز دارد، نداشته باشید، معامله نمی‌تواند به‌طور مستقیم شکل بگیرد. برای برطرف‌کردن این مشکلات، پول و اعتبار

1. Mesopotamia

را ابداع کردیم که مبنایی برای اقتصاد امروز است. امروزه، اگر شما چوب بخواهید، می‌توانید از اعتبار یا پول برای قرض گرفتن ۲۰ بسته چوب از همسایه خود استفاده کنید، این کار شاید شما را مقروض کند، اما اجازه می‌دهد که در آینده پرداخت را انجام دهید. همچنین می‌توانید پول چوب‌ها را نقدی بپردازید و می‌توانید از هر راه دیگری که می‌خواهید استفاده کنید. در هر مبادله پولی، همسایه شما باید به شما و ارزی که به وی می‌دهید، اعتماد داشته باشد. اعتبار و پول، معامله را امکان‌پذیر می‌سازند و آن را کارآمدتر می‌کنند.

حال، بعد از سه هزار سال از تکامل مالی و فناورانه، اینترنت یک نسخه دیجیتال از روش دادوستد سومریان را برای ما به ارمغان آورده است. از زمانی که اینترنت اولین‌بار در سال ۱۹۶۹ اختراع شد، نیم‌قرن گذشته است و اینترنت بخش جدایی‌ناپذیر زندگی ما شده است. بسیاری از افراد می‌توانند بدون هیچ دوستی زندگی کنند، اما بدون دسترسی به اینترنت نمی‌توانند. اینترنت افراد را به‌صورت بی‌سیم و بلافصل از طریق ایمیل‌ها، شبکه‌های اجتماعی، کسب‌وکار آنلاین و... با یکدیگر مرتبط می‌سازد. میزان مشارکت اجتماعی و مالی که از طریق اینترنت انجام می‌دهیم، نشان می‌دهند که چگونه در هر جنبه زندگی خود بر اینترنت تکیه می‌کنیم.

مزایای اینترنت واضح هستند، اما جنبه‌های منفی نیز وجود دارد. برخی از بزرگ‌ترین جنبه‌های منفی آن این است که ما حقیقتا نمی‌توانیم از موارد مربوط به امنیت و حریم شخصی چشم‌پوشی کنیم. چگونه می‌توانیم زمانی که همه اطلاعات شخصی و عکس‌های ما در وب است، حریم شخصی خود را حفظ کنیم؟

برای بیشتر ما، پاسخ این است که تنها به افراد مورد اعتماد و شناخته‌شده اجازه دهیم که فعالیت‌های آنلاین ما را مشاهده کنند. این امر به‌نوعی، مشابه این است که چگونه تصمیم می‌گیریم دولت‌ها و بانک‌ها، معاملات اقتصادی ما را نظارت، مدیریت و کنترل کنند. شرکت‌هایی مانند فیس‌بوک، گوگل، مایکروسافت و آی‌بی‌ام به بخشی از نهادهایی تبدیل شده‌اند که برای ارائه امنیت آنلاین به آنها اعتماد می‌کنیم. به‌طوری که اطلاعاتی که استفاده می‌کنیم در سرورهای مرکزی متعلق به شرکت‌های اینترنتی قدرتمند ذخیره می‌شوند. این شرکت‌ها خدمات ارزشمندی برای ما فراهم می‌کنند و در مقابل با ارائه اطلاعات شخصی، به آنها اعتماد می‌کنیم. زمانی که اطلاعات ما در دستان آنهاست، ما کنترل کمی

در مورد اینکه چگونه ممکن است از آن استفاده کنند، داریم. فکر کنید که تاکنون چند بار یکی از شرکت‌های وب، اطلاعات کاربران را بدون اجازه فروخته است. فکر کنید که چند بار وب‌سایت‌ها شرایط خدماتی خود را تغییر و اجازه دادند که داده‌های مشتریان فروخته شود یا به روش دیگری استفاده شوند.

رسوایی اخیر فیس‌بوک یک مثال عالی از نقض حریم شخصی و سوءاستفاده از قدرت است که بسیاری از کاربران احساس کردند ماه‌هاست که ناعادلانه از آنها سوءاستفاده شده است.

هم‌اکنون اهمیتی ندارد که در مورد اینترنت چه احساسی دارید، قطعا به طرز غیرقابل انکاری نیروی اصلی است که ما را به سمت آینده می‌کشاند. بسیاری از بانک‌ها، غول‌های مبتنی بر اینترنت هستند که برای شکست‌دادن بسیار بزرگ‌اند[1]. گوگل از طریق ترویج موتور جست‌وجوی خوبش، بر تبادل اطلاعات تسلط یافت. پلتفرم‌های شبکه‌های اجتماعی غالب، مانند فیس‌بوک نیز ارتباطات شخصی و تبادل اطلاعات عمومی را کنترل می‌کنند. بنابراین تجارت الکترونیک به بخشی از زندگی ما تبدیل شده است، مانند استفاده از آمازون و علی‌بابا که در این زمینه شکست‌ناپذیر هستند.

سرقت اطلاعات شخصی یک چیز است، اما پتانسیل برای سرقت اطلاعات مالی آنلاین چیزی بسیار مهم‌تر است. برای بسیاری از افراد در سراسر جهان، انجام تراکنش‌های مالی آنلاین جایگزین مراجعه حضوری به بانک‌ها شده است. همان‌طور که خرده‌فروشی روزگار سختی را تجربه کرده است، حال ما کالاهایی را به‌صورت آنلاین با افزایش دفعات خرید‌وفروش می‌کنیم و به جای اینکه تلفن را برداریم و برای سفارش غذا به رستوران زنگ بزنیم، در وب‌سایت، منو را می‌گیریم و سفارش می‌دهیم. این افزایش در فعالیت‌های مالی آنلاین خواستار امنیت و کارایی بهتر است. رمزارز به همین دلیل ایجاد شده است؛ چراکه امنیت بهتری را فراهم می‌کند و ساده‌تر استفاده می‌شود. ما نیاز نداریم که در زمانی که با استفاده از رمزارز خرید می‌کنیم، هویت خود را آشکار کنیم و در حقیقت، همچنان گمنام می‌مانیم.

1. Too big to fail

طرفداری از آزادی فردی[1]، سایفرپانک‌ها[2] و پول دیجیتال

این مساله مردم را بر آن می‌داشت که یک روزی از پول دیجیتال (انتقال آنلاین دلار دیجیتال) به استفاده از رمزارز؛ پولی که با استفاده از رمزنگاری ایجاد شده است، روی بیاورند. این مهاجرت همین الان در حال وقوع است. امروزه پدیده این‌چنینی را به‌درستی درک کردیم و نیاز است که بپرسیم چرا این اتفاق رخ داده است. چرا افراد می‌خواهند یک ارز، جدا از پول فیات کنترل‌شده توسط دولت‌های مرکزی و بانک‌های مرکزی ایجاد کنند؟

عموما داینرز کلاب[3] به‌عنوان منشاء تولد کارت‌های اعتباری شناخته می‌شود. در سال ۱۹۷۴، رول‌اند مونرو[4] کارت آی‌سی[5] را به‌عنوان واسطه‌ای برای ذخیره ارز دیجیتال ابداع کرد. در سال ۱۹۸۲، ایالات متحده سیستم انتقال وجوه الکترونیک[6] را ایجاد کرد، بریتانیا و آلمان نیز موسسات مشابهی را کمی بعد ایجاد کردند. کارت‌های اعتباری صادرشده توسط بانک‌ها یک موفقیت بزرگ بود که با افزایش تقاضا به‌صورت نمایی رشد کردند. این اولین دیجیتالی‌سازی پول فیات بود. این اتفاق از این رو مهم بود که درک ما از پول را به روشی که طی چند قرن استفاده می‌شد، تغییر داد. برای اولین‌بار، اکثر ما نیازمند حمل پول نقد نبودیم و این یعنی هر کاری می‌تواند به‌صورت مجازی انجام شود.

حتی اگر پول دیجیتال خیلی از پول فیات متفاوت باشد، هنوز متکی بر اعتماد به بانک‌ها و دولت‌های قدرتمند مرکزی است. هرکسی این مساله را به‌دلیل مقررات و الزامات ذاتی آن نمی‌پسندد. یعنی، بر خلاف پول نقد، نمی‌توانید از کارت اعتباری خود به‌صورت ناشناس استفاده کنید؛ با یک نرخ خاص کارت اعتباری خود را در کشور دیگر شارژ می‌کنید. البته برخی کارت‌ها در همه کشورها پذیرفته نیستند و واسطه‌ها- مانند بانک‌ها و شرکت‌های مالی- نقش اصلی را در معاملات بازی می‌کنند. پی‌پال و علی‌پی خود را به‌عنوان «گزینه‌های مورد اعتماد پرداخت شخص ثالث» دیده‌اند و حضور آنها توانایی ما برای انجام معاملات

---

1. Libertarianism

۲. سایفرپانک هر فرد فعالی است که از فناوری‌های رمزنگاری قوی و تقویت حریم خصوصی به عنوان مسیری برای تغییرات اجتماعی و سیاسی حمایت می‌کند.

3. Diners Club
4. Roland Moreno
5. IC card
6. Electronic funds transfer system (EFTS)

به‌صورت مخفیانه یا ناشناس را مختل کرده است. گفتنی است معاملات پولی بین‌المللی از یک بانک به بانک دیگر بدون ثبت عمومی، امکان‌پذیر نیست.

واسطه‌های آنلاین همچنین برای گردآوری بهتر اطلاعات مشتری و خریدار، تلاش کرده‌اند فناوری‌های نقض‌کننده حریم خصوصی مثل کلید عمومی را ارائه کنند. این فناوری‌ها خریدار و فروشنده را ملزم می‌کنند که برای هر تراکنش، فرایندهای پیچیده‌ای را از سر بگذرانند تا هویت‌شان را تایید کنند. با این حال ظهور بیت‌کوین تا حد زیادی از گسترش این سیستم‌های جدید جلوگیری کرده است.

توانایی پرداخت و انجام تراکنش آنلاین به‌صورت گمنام همواره از طرف جوامع خاصی مانند نخبگان فناوری و اطلاعات، سایفرپانک‌ها، طرفداران غیرمتمرکزسازی و طرفداران آزادی فردی از جنبه سیاسی، مورد حمایت قرار می‌گیرد. در تمامی گروه‌های مذکور یک هویت و جهان‌بینی مشترک وجود دارد؛ آنها احساس می‌کنند که بخشی از یک خانواده بزرگ تحت تاثیر نظرات متفکرانی همچون فریدریش آوگوست فون هایک[1] هستند. زمانی که موانعی برای تجارت آزاد مانند کلید عمومی ظاهر شد، سایفرپانک‌ها و رهروان‌شان، به ایجاد روشی جدید برای تبادل اطلاعات (مالی و غیر آن) روی آوردند که شامل مداخله بسیار محدود نهادهای تنظیم‌گر جدید می‌شد یا اصلا مداخله آنها را نمی‌پذیرفت. آنها می‌خواهند حریم شخصی را ارتقا بخشند و از آزادی فردی حمایت کنند. آنها تلاش می‌کنند به‌صورت فعالی دولت و مقررات را سرنگون کنند.

به نظر می‌رسد همه این خواسته‌ها در بیت‌کوین تحقق پیدا کرده است.

قبل از دهه ۱۹۸۰، تیموتی می[2] ایده‌ای را برای پول دیجیتال مطرح کرد که «اعتبار کریپتو»[3] نام گرفت. دیوید چام[4] اولین کسی بود که از علم رمزنگاری برای E-cash استفاده کرد. یکی از مسائل اصلی که پول نقد الکترونیکی با آن مواجه بود «دو بار خرج کردن»[5] بود. «دو بار خرج کردن» تقریبا همان معنای ظاهری لغوی را دارد. یعنی پولی یکسان دو بار خرج شود؛ تراکنشی

1. Friedrich August von Hayek
2. Timothy May
3. Crypto Credits
4. David Chaum
5. Double Spend

یکسان دو بار اجرا شود. مثل این است که چکی را به بانکی ببرید و نقدش کنید و بعد همان چک را به بانکی دیگر ببرید و دوباره نقدش کنید. برای مثال فرض کنید کاربر الف، یک دلار «ای‌کش» را از طریق امضای الکترونیک به کاربر ب ارسال کند. ریسکی که وجود دارد این است که کاربر ب امضای الکترونیک کاربر الف را کپی کند تا به جای یک دلار، دو دلار بگیرد.

یکی از اولین راهکارهای حل مساله دو بار خرج‌کردن درج شماره سریال منحصربه‌فرد روی اسناد بهادار بود. وقتی کاربر الف سند بهادار را ارسال می‌کرد، کاربر ب امضا را بررسی می‌کرد و با کاربر الف تماس می‌گرفت و از او شماره سریال را جویا می‌شد و می‌پرسید آن سند بهادار ای‌کش قبلا استفاده شده است یا خیر. اگر آن سند بهادار قبلا نقد نشده بود، کاربر ب پول را می‌پذیرفت. بعد کاربر الف ثبت می‌کرد که آن سند بهادار استفاده شده است.

وای! عجیب نیست که چنین سیستمی فراگیر نشده است؟

در دنیای دیجیتال امروز سرورها تمام کارها از جمله ثبت همه امضاها و شماره‌سریال‌های مربوط به تراکنش‌های مالی را انجام می‌دهند. استفاده از شماره سریال مساله دو بار خرج‌کردن را حل کرد، اما امکان انجام تراکنش گمنام را به افراد نداد؛ چراکه از طریق شماره‌سریال می‌شد همه تراکنش‌ها (و اطلاعات شخصی متناظر آن) را رهگیری کرد.

دیوید چام در راستای گمنام‌کردن تراکنش‌ها، روش دور زدنی با عنوان «امضای کور»[1] را پیشنهاد داد. این روش با یک تیر دو نشان می‌زد و هر دو مساله گمنامی و دو بار خرج‌کردن را حل می‌کرد. کاربر با این روش می‌تواند هر گونه تبادل پولی را انجام دهد که از طریق پول فیزیکی امکان‌پذیر است (البته به‌جز شیر یا خط فیزیکی). امضای کور چطور عمل می‌کند؟ همه اتفاقات در یک «پاکت» روی می‌دهد. کاربر الف سند بهاداری با شماره‌سریال را در پاکتی می‌گذارد که هیچ‌کس جز کاربر ب به آن دسترسی ندارد. اما کاربر ب چطور بدون افشای هویتش سند بهادار را امضا می‌کند؟ پاسخ قرار دادن کاغذ کاربن در پاکت است، با این کار امضا از طریق کاغذ کاربن روی سند بهادار ثبت می‌شود. در این حالت کاربر ب شماره‌سریال را نمی‌داند و کاربر الف نمی‌داند چه کسی سند بهادار را امضا کرده است.

خلاصه اینکه تراکنش انجام می‌شود، بدون آنکه دو طرف از هویت یکدیگر آگاه باشند.

---

1. Blind Signature

دیوید چام با استفاده از این فناوری دو شرکت تاسیس کرد. یکی دیجی‌کش[1] که به‌منظور ارائه خدمات پرداخت دیجیتال آنلاین با استفاده از ای‌کش ایجاد شد و دیگری سایبرباکس[2] که برای پشتیبانی از بانک‌ها طراحی شد.

ای‌کش راه‌حل تازه و خوشایندی بود، اما مانند نوشیدنی خنکی که زود تمام می‌شود، این تازگی هم زیاد ماندگار نبود! و با وجود مزیت‌هایش هرگز در بین افراد عادی پذیرفته نشد. اگرچه برای کمک به خریداران و فروشنده‌ها در تسهیل تراکنش‌ها طراحی شده بود، اما فروشنده‌های کمی معتقد بودند استفاده از آن منفعتی برای آنها دارد.

زمانی که بیت‌کوین به میان آمد، داستان عوض شد که در ادامه کتاب در مورد این تفاوت‌ها بحث خواهیم کرد، اما صرف‌نظر از شکست ای‌کش در تجاری‌سازی، مفهوم امضای کور نقطه عطفی مهم و حیاتی در تاریخ ارز دیجیتال بود.

دیوید چام پتنت‌هایی را برای فناوری‌های مربوط به ای‌کش از جمله امضای کور ثبت کرد، اقدامی که به‌دلیل ایجاد مانع در پیشرفت پرداخت‌های الکترونیک انتقادهایی را به‌دنبال داشت. با این حال این مساله سایفرپانک‌ها را متوقف نکرد و آنها به استفاده از امضای کور برای توسعه راه‌حل‌های پرداخت ادامه دادند. ۱۰ سال بعد از اینکه دیجی‌کش ورشکست شد، ساتوشی تولد بیت‌کوین را به جهانیان اعلام کرد. اغلب افرادی که این خبر را اولین‌بار از طریق ایمیل ساتوشی دریافت کردند، همین سایفرپانک‌ها بودند.

بیایید زمان بیشتری را برای تفکر در مورد سایفرپانک‌ها و اینکه دقیقا چه کاری می‌خواهند انجام دهند، تخصیص دهیم. جولیان آسانژ[3] ممکن است مثال خوبی از یک سایفرپانک متمایز باشد، اما تنها مثال نیست. سایفرپانک‌ها علاقه شدیدی به آزادی فردی دارند. آسانژ به‌وضوح در مورد در دسترس بودن اطلاعات و قابل دسترس بودن برای عموم، حساس بود. سایفرپانک‌ها همین احساس را نسبت به رمزارز هم دارند. آنها اعتقاد دارند تراکنش‌های مالی خصوصی باید برای عموم در دسترس قرار گیرد، از سیستم بانکی موجود تمرکززدایی شود، جلوی تورم گرفته شود و امنیت بهبود یابد. سایفرپانک‌ها نیز به‌دنبال اجتناب از

1. DigiCash
2. Cyberbucks
3. Julian Assange

فاجعه‌هایی هستند که در سال‌های اخیر اقتصاد جهانی را تحت تاثیر قرار داده است. بحران سال ۲۰۰۸ اعتماد جهان به توانایی دولت‌ها و موسسات مالی بزرگ در کنترل موثر اقتصاد را از بین برد. از نظر سایفرپانک‌ها بیت‌کوین با ارائه راه‌حلی که به کاربران این امکان را می‌داد که از همه اشتباهات گذشته اجتناب کنند، امیدی تازه ایجاد کرد.

با این حال با وجود آرزوهای دور و دراز جماعت سایفرپانک در سال ۲۰۰۸، بیت‌کوین و دیگر رمزارزها هنوز نتوانسته‌اند به اندازه پول فیات با اقبال گسترده مردم روبه‌رو شوند. در عین حال بیت‌کوین به‌واسطه ماهیت تحول‌آفرین و افزایش قیمت نجومی‌اش، آگاهی جهانی زیادی ایجاد کرده است. از آنجایی که مزیت‌هایش کاملا مشهود و برای بسیاری از افراد به‌شدت جذاب است، بنابراین دولت‌های زیادی فعالانه به‌دنبال ایجاد روش‌هایی برای استفاده از آن هستند.

در مطالب بعدی دوست دارم رمزارز را از لحاظ نحوه انتشار و عرضه در برابر ارزهای متداول کنونی قرار دهم.

تکامل علم رمزنگاری

برای صدها سال، بانک‌های مرکزی با مدیریت مقدار پولی که به بازار وارد می‌شود و کنترل زمان ورود این پول، یکی از مهم‌ترین نقش‌ها را در سیستم مالی و به‌ویژه در مورد پول فیات و همچنین پول دیجیتال مرسوم ایفا کرده‌اند. برای اینکه پول دیجیتال به‌عنوان ارزی موجه و واقعی پذیرفته شود، باید نماینده ارزش باشد و بتواند ارزش را منتقل کند. همان‌طور که پیش از این اشاره کردم، پول دیجیتال صرفا شکلی دیگر از پول فیات است. ذاتا فرقی با هم ندارند. پول دیجیتال برای تایید همه تراکنش‌ها به شخص ثالث مورد اعتماد وابسته است، اما رمزارزها هیچ نیازی به شخص ثالث ندارند. به عبارت دیگر رمزارزها واسطه را حذف می‌کنند. رمزارزها همچنین از این لحاظ با پول فیات متفاوت هستند که پشتوانه رمزنگاری دارند. رمزنگاری در رمزارزها دو کارکرد اساسی دارد؛ اولی رمزنگاری[1] و دومی تایید اصالت[2] است که از طریق فرایند کدگذاری و کدگشایی صورت می‌پذیرد.

1. Encryption
2. Verification

رمزنگاری به‌عنوان یک علم در جنگ جهانی دوم کاربرد گسترده‌ای داشت. در کنار سربازان متفقین، ریاضیدانان و مهندسانی بودند که با استفاده از رمزنگاری به نبرد در جنگ پنهان اطلاعات مشغول بودند. وقتی آلمانی‌ها از ماشین معروف انیگما[1] برای انتقال فرمان‌های رمزگذاری‌شده استفاده می‌کردند، رمزنگارهای متفقین به‌سختی تلاش می‌کردند تا در زمانی کم آن فرمان‌ها را رمزگشایی کنند.

امروزه رمزنگاری در کارکردها و موقعیت‌های اقتصادی کاربرد گسترده‌ای دارد. رمزنگاری به‌طور خاص در علوم کامپیوتر و به‌ویژه در حوزه امنیت اینترنت کاربرد پیدا کرده است. با هر کلیک بر مرورگر، با صفحات در حال اجرا بر یک سیستم پیچیده از کدها در تعامل هستیم. رمزنگاری، ورودی و خروجی اطلاعات را در این صفحات امن می‌سازد.

در دهه ۱۹۷۰، علم رمزنگاری نوآوری‌های بزرگی را به خود دید. ویتفیلد دیفی[2] و مارتی هلمن[3] در سال ۱۹۷۶، پروتکلی به نام «تبادل کلید دیفی و هلمن» را اختراع کردند که تجارت الکترونیک مدرن و ارتباطات رمزنگاری‌شده امروزی را ممکن ساخت. در سال ۱۹۷۷، ران ریوست[4]، آدی شامیر[5] و لئونارد آدلمن[6]، RSA را ایجاد کردند که یک موتور رمزنگاری قوی با ارزش تجاری زیاد بود و در سال ۱۹۸۵، نیل کوبلیت[7] و ویکتور میلر[8]، رمزنگاری منحنی بیضوی[9] را ارائه کردند که رویکردی به رمزنگاری کلید عمومی بر مبنای ساختار جبری منحنی‌های بیضوی روی میدان‌های متناهی است.

رمزنگاری رکن اصلی امنیت اینترنت، ارتباطات و همچنین رمزارزهایی مانند بیت‌کوین است. دولت آمریکا در مراحل اولیه پیدایش الگوریتم‌های رمزگذاری روی آنها کنترل کاملی داشت. آژانس امنیت ملی، کاربران آنها را با دقت تحت نظر داشت. تازه در دهه ۱۹۹۰ بود که این الگوریتم‌ها در دسترس مردم قرار گرفت. جالب است که گفته می‌شود آژانس امنیت ملی

1. Enigma
2. Whitfield Diffie
3. Marty Hellman
4. Ron Rivest
5. Adi Shamir
6. Leonard Adelman
7. Neal Koblit
8. Victor Miller
9. ECC

با تعبیه درهای پشتی[1] در فناوری‌های عرضه‌شده به مردم این امکان را ایجاد کرده است تا هر وقت خواست محتواهای خاصی را تضعیف یا منحرف کند.

بیت‌کوین به اندازه کافی برای اجتناب از راه‌های دررو ایجادشده توسط آژانس امنیت ملی خوش‌شانس بوده است. الگوریتمی که ساتوشی ناکاموتو، مبدع بیت‌کوین انتخاب کرد، آن‌قدر پرطرفدار نبود که زیر نظر آژانس امنیت ملی قرار بگیرد. همان‌طور که توسط ویتالیک بوترین[2]، موسس اتریوم تایید شد، ساتوشی هنگام طراحی بیت‌کوین تصمیم‌های زیادی گرفته است که با خوش‌شانسی همراه بوده‌اند و یکی از آنها انتخاب الگوریتم مناسب برای نیفتادن در دام‌های آژانس امنیت ملی بوده است. در حال حاضر فقط چند برنامه وجود دارند که با موفقیت از دام‌های آژانس امنیت ملی گریخته‌اند. شاید احساس امنیتی که این مساله به کاربران می‌بخشد، دلیل دیگری برای موفقیت بیت‌کوین باشد.

بیت‌کوین بهترین مثال برای ارزش فناوری بلاکچین است. در وایت‌پیپری[3] که ساتوشی در سال ۲۰۰۸ منتشر کرد، به‌وضوح مشخص شده که بلاکچین ستون اصلی سیستم تبادل برای کاربران بیت‌کوین است. همان‌طور که ساتوشی می‌گوید این سیستم «نسخه‌ای کاملا همتابه‌همتا از پول الکترونیک است که امکان ارسال مستقیم پرداخت‌های آنلاین از طرفی به طرفی دیگر بدون عبور از نهادی مالی را فراهم می‌کند». استفاده از فناوری رمزنگاری برای امن‌کردن پرداخت‌ها نیاز به نقش‌آفرینی بانک‌ها (یا دیگر نهادها) به‌عنوان واسطه را حذف کرده است.

سازوکار بیت‌کوین به چه شکل است؟

فردی که با بیت‌کوین معامله را انجام می‌دهد، از یک کیف پول الکترونیکی استفاده می‌کند که یک آدرس IP دارد که شامل «کلید» عمومی فرد و یک مدرک شناسایی دیگر است. این همان کیف پولی است که به فرد اجازه می‌دهد بیت‌کوین‌ها را ارسال و دریافت کند و هر معامله را مستند سازد. کاربران بیت‌کوین علاوه بر کلید عمومی، کلید خصوصی اختصاصی دارند که فقط در دسترس خودشان است. این رمزنگاری دوگانه به کاربران بیت‌کوین کمک

1. Back door
2. Vitalik Buterin
3. White Paper

می‌کند که گمنام بمانند. به‌منظور اعتبارسنجی معامله بیت‌کوین، کاربران برای رسیدن به اجماع نظر باید از قدرت کامپیوتر برای بلاکچین استفاده کنند. بعد از این، تراکنش‌ها در بلوک‌های مختلف و گسترده در تمام زنجیره مستند می‌شوند. می‌توان گفت بلاکچین امکان نگهداری سابقه‌ای دائمی از هر تراکنش بیت‌کوین را فراهم می‌کند و احتمال وقوع به‌اصطلاح خرج‌های دوگانه را از بین می‌برد. بلاکچین مولفه‌ای ضروری برای بیت‌کوین است و بدون آن غیرمتمرکزسازی این رمزارز و واسطه‌زدایی از آن امکان‌پذیر نیست. در همه بلوک‌های روی زنجیره، اطلاعاتی تغییرناپذیر ذخیره می‌شوند و فناوری و شفافیت کاملی که فناوری فراهم می‌کند، به ایجاد اعتماد منجر می‌شود.

احتمالا این پرسش مطرح می‌شود که بلاکچین دقیقا چطور از تقلب یا کلاهبرداری افراد جلوگیری می‌کند؟ این سوال خوبی است.

نمی‌خواهم خیلی فنی صحبت کنم؛ اما کلید اصلی در علم رمزنگاری نهفته است. در زنجیره بلوک‌ها یا همان بلاکچین، هر بلوک چیزی به نام اشاره‌گر هش[1] دارد که به بلوک جلودار زنجیره اشاره می‌کند و ارزش هش ذخیره‌شده در آن را آشکار می‌کند. با وجود این اشاره‌گر هش، هک‌کردن بلاکچین امکان‌پذیر نیست. وقتی بلوکی ایجاد و پذیرفته می‌شود، ایجاد تغییر در آن تقریبا غیرممکن است. در سطح بنیادین و فنی بلوک‌ها و تراکنش‌هایی که آنها ثبت می‌کنند، در عمل تغییرناپذیر هستند.

پیش از این به چند مورد از مشکلات گمنام‌ماندن هنگام انجام تراکنش با پول دیجیتال اشاره کردیم. هر تراکنش واقعا گمنام باید کلیدی عمومی و کلیدی خصوصی داشته باشد. چنین تراکنشی همچنین شامل امضای دیجیتال و رمزنگاری نامتقارن می‌شود که در ادامه بررسی می‌کنیم.

شاید این عبارت‌ها پیچیده به‌نظر برسند، اما توضیح این مفاهیم دشوار نیست. رمزنگاری نامتقارن به هر کاربر دو کلید می‌دهد؛ یک کلید عمومی و یک کلید خصوصی. کلید عمومی شناسه و آدرس IP دارنده حساب را ارائه می‌دهد. این کلید می‌تواند اطلاعات را رمزنگاری کند. اطلاعاتی را که کلید عمومی رمزگذاری کند، فقط با کلید خصوصی متناظرش می‌توان رمزگشایی کرد. اگر یک کاربر از کلید خصوصی برای امضای هر اطلاعاتی استفاده کند، تنها

1. Hash Pointer

تطبیق کلید عمومی می‌تواند صحت امضا را اعتبارسنجی کند. در این جهان غیرمتمرکز، هیچ نیازی به قدرت متمرکز (مانند بانک، شرکت نرم‌افزاری، یا نهاد دولتی) برای مدیریت یا تامین امنیت اطلاعات کاربران نیست. کاربران حساب خود را باز می‌کنند و کلید خصوصی خود را حفظ می‌کنند. کاربران بیت‌کوین (و کاربران هر رمزارز دیگر) اغلب از واژه آدرس[1] برای اشاره به مقدار هش کلید عمومی استفاده می‌کنند و کلید خصوصی در کنترل هر کاربر باقی می‌ماند. به این ترتیب دولت و هر نهاد دیگری که در دنیای واقعی اطلاعات هویتی ما را برای راستی‌آزمایی تراکنش‌ها جمع‌آوری و مدیریت می‌کند، با رمزنگاری نامتقارن حذف می‌شود.

فناوری شبکه همتابه‌همتا آخرین عنصری بود که برای قطعی‌شدن ایجاد بیت‌کوین، باید به‌درستی محقق می‌شد. اغلب افراد وقتی به این نوع فناوری فکر می‌کنند، موردی مثل نپستر[2] را در نظر می‌گیرند.

نپستر، توسط شان فنینگ و شان پارکر در سال ۱۹۹۹ تاسیس شد و اولین نرم‌افزار موسیقی بود که افراد را قادر می‌ساخت فایل‌های موسیقی را از طریق اینترنت و مستقیم از کامپیوتری به کامپیوتر دیگر ارسال کنند. مشکلات کپی‌رایت و شکایت‌های حقوقی باعث شدند که نپستر در اولین سال قرن بیست‌ویکم تعطیل شود. با این حال اگرچه نپستر در نهایت شکست خورد، اما پروژه مهمی بود؛ چراکه نشان داد فناوری همتابه‌همتا عملی است و می‌توان آن را در مقیاس انبوه استفاده و پیاده‌سازی کرد.

پیدایش بیت‌کوین

وایت‌پیپر ۹ صفحه‌ای که ساتوشی ناکاموتو در اکتبر ۲۰۰۸ منتشر کرد، با این عبارت شروع شده بود: «نسخه‌ای کاملا همتابه‌همتا از پول الکترونیک که امکان ارسال مستقیم پرداخت‌های آنلاین از طرفی به طرفی دیگر بدون عبور از نهادی مالی را فراهم می‌کند». ساتوشی با این سخنان وارد گود شده بود، مشکل را شناسایی کرده و راه‌حل را هم پیشنهاد داده بود. بیت‌کوین با دیگر پول‌های دیجیتال تفاوت داشت؛ چراکه به قدرت مرکزی وابسته نبود.

---

1. Address
2. Napster

برای آنکه این پروژه به موفقیت برسد، ساتوشی باید کاری می‌کرد که جهان ایده قدرت غیرمتمرکز را بپذیرد. مرعوب‌کننده به‌نظر می‌رسد، اما آیا واقعا تغییری بنیادین است؟ خیر، هر روز در زندگی روزمره غیرمتمرکزسازی را تجربه می‌کنیم. برای مثال زیاد از ایمیل استفاده می‌کنیم و پروتکل ساده نامه‌رسانی[1]، سیستمی غیرمتمرکزساز است.

ساتوشی می‌دانست که برای رسیدن به هدف ترویج سیستمی مبتنی بر غیرمتمرکزسازی باید مساله «اجماع توزیع‌شده»[2] را هم حل کند.

اجماع توزیع‌شده دقیقا چیست؟ برای تشریح این مفهوم اغلب از داستان ژنرال‌های بیزانس استفاده می‌شود.

داستان این است: بیزانس زمانی قدرتمندترین امپراتوری جهان و بسیار پهناور بود. قلمروی تحت فرمان بیزانس در سرتاسر اروپا و آسیا گسترش یافته و بزرگ‌تر از ایالات متحده کنونی بود. هر وقت جنگی آغاز می‌شد، نیروهای نظامی از دولت مرکزی به جنگ اعزام می‌شدند. فرماندهی هر کدام از نیروها بر عهده ژنرالی بود که مستقل عمل می‌کرد. مساله این بود که این امپراتوری چطور وفاداری ژانرال‌ها در میدان جنگ را تضمین کند و اگر ژنرالی خیانت کرد، چگونه از این مساله آگاه شود. مساله زمانی به نقطه بحرانی رسید که به ژنرال‌ها دستور داده شد یا همه با هم حمله کنند یا همه عقب‌نشینی کنند. اگر نیمی از ژنرال‌ها حمله می‌کردند و نیمی دیگر عقب‌نشینی، فاجعه روی می‌داد. وقتی ژنرال‌ها با هم ارتباط برقرار می‌کردند و یکی از دیگری می‌شنید که دستور حمله یا عقب‌نشینی صادر شده است، چطور مطمئن می‌شدند که با فردی خائن در ارتباط نیستند؟

رمزنگارها هم با همین مساله برخورد کردند. بدین معنی که وقتی «ژنرال‌های» زیادی وجود دارند که اطلاعات همتا‌به‌همتا را در بلاکچین پخش می‌کنند، چطور می‌توان به نظری واحد رسید؟ ساتوشی مساله اجماع توزیع‌شده را از طریق مقوله‌ای به نام «اثبات کار»[3] حل کرد. اثبات کار به بیان ساده یعنی کار صادقانه پاداش می‌گیرد.

اثبات کار را اولین‌بار رمزنگاری بریتانیایی به نام «آدام بک»[4] آزمایش کرد که در سال ۱۹۹۶

1. Simple Mail Transfer Protocol
2. Distributed consensus
3. Proof of Work
4. Adam Back

نرم‌افزاری برای مقابله با ایمیل‌های اسپم توسعه داده بود. در سیستمی که او طراحی کرد، همراه هر ایمیل باید اطلاعاتی ارسال می‌شد که اثبات می‌کرد برای ایجاد آن ایمیل چقدر زمان صرف شده و چقدر تلاش شده است. این مساله فرستندگان ایمیل‌های اسپم را دچار دردسر کرد؛ زیرا برای آنکه ایمیل‌هایشان در آزمون قبول شوند و در صندوق ایمیل گیرنده هدف قرار بگیرند، باید با تلاش زیادی به استاندارد مورد نیاز می‌رسیدند، اما از آنجایی که در سال ۱۹۹۶ (دست‌کم در مقایسه با الان) افراد زیادی از ایمیل استفاده نمی‌کردند، مساله ایمیل‌های اسپم به اندازه اکنون جلب توجه نکرد. در نتیجه سیستم آدام بک فرصتی برای پذیرش گسترده پیدا نکرد. با این حال نوآوری نرم‌افزارش در آینده بسیار کاربردی شد.

اثبات کار از لحاظ اقتصادی هزینه ورود اطلاعات غلط را افزایش می‌دهد. اضافه‌کردن یک بلوک به بلاکچین نیازمند قدرت رایانش قابل توجهی است. اولین نفری که بلوکی را وارد سیستم می‌کند، باید زمان و انرژی زیادی صرف کند. وقتی می‌شنوید ماینرها «بیت‌کوین استخراج می‌کنند»، در واقع منظور این است که بلوک‌های جدید ایجاد می‌کنند یا تراکنش‌های جدید زنجیره را راستی‌آزمایی می‌کنند. گفتنی است بلاکچین بیت‌کوین به کمک اثبات کار و به تناسب تلاش‌های این ماینرها به آنها پاداش می‌دهد.

اگر برای مثال بگوییم ۱۰ هزار ساعت مطالعه و آموزش، فردی را در رشته‌ای خاص متخصص می‌کند، در دنیای بیت‌کوین هم چنین شرایطی برقرار است و ماینرها باید از طریق تابع هش[1] کارشان را اثبات کنند. این فرایند علاوه بر طولانی‌بودن، بسیار پیچیده است. ماینرها باید مسائل ریاضی مختلفی را حل کنند. نتیجه حل موفقیت‌آمیز این مسائل دریافت بیت‌کوین است. وقتی بلوکی جدید در بلاکچین ایجاد می‌شود، ماینر مقدار مشخصی بیت‌کوین را به‌عنوان پاداش دریافت می‌کند و وقتی تراکنشی جدید در بلوک‌ها ثبت می‌شود، ماینر بسته به اینکه چه کسی تراکنش را آغاز کرده، مقدار مشخصی بیت‌کوین پاداش می‌گیرد.

اثبات کار در فضایی اجرا می‌شود که نیازی به «اعتماد» به شکل مرسوم وجود ندارد؛ چراکه سیستم همه اتفاقات را راستی‌آزمایی می‌کند؛ تا زمانی که فرد کارش را انجام دهد، پاداش دریافت می‌کند و تقلب در این فرایند تقریبا غیرممکن است. در حال حاضر انواع زیادی از رمزارزها از جمله بیت‌کوین، لایت‌کوین، دوج‌کوین و مونرو وجود دارند که برای اعتبارسنجی

1. Hash Function

تراکنش‌ها و ایجاد بلوک‌های جدید از اثبات کار استفاده می‌کنند.

هرچه بلوک‌های یک زنجیره بیشتر باشند، اطلاعات بیشتری که به بلوک‌ها وارد می‌شوند، سیستم را منسجم‌تر و امن‌تر می‌کنند، اما در عین حال انرژی بیشتری هم مصرف می‌شود. این چرخه معیوب مصرف انرژی باعث می‌شود اثبات کار برای محیط زیست زیان‌آور باشد. در نتیجه بسیاری از افراد در پی راهکارهای جایگزین عملی برای آن هستند. در همین راستا اثبات سهام[1] به‌عنوان روش بسیار محبوب دیگری برای رسیدن به توافق توزیع‌شده ظهور پیدا کرده است.

اثبات سهام روش دیگری برای محاسبه ارزش است، اما هزینه ورودی بسیار کمتری دارد. به بیان ساده، این رویکرد را این‌طور می‌توان خلاصه کرد: «ثروتمند، ثروتمندتر می‌شود.» در اثبات سهام هرچه بیت‌کوین بیشتری داشته باشید، احتمال بیشتری وجود دارد که حل کردن بلوک به شما سپرده شود. در اثبات سهام، ماینرها اعتبارسنج خوانده می‌شوند. اعتبارسنج‌ها در ابتدا باید مقدار مشخصی رمزارز سپرده‌گذاری کنند. هرچه مقدار بیشتری سپرده‌گذاری کنند، شانس بیشتری برای حل کردن بلوک جدید دارند. اثبات سهام به اندازه فرایند استخراج مرسوم، برق نیاز ندارد و به‌مرور طرفدارانش بیشتر می‌شوند. برای مثال اتریوم به‌تازگی از روش اثبات کار به اثبات سهام روی آورده است.

چرا ارز دیجیتال مهم است

تاکنون به جزیره یپ[2] در میکرونزی[3] نرفته‌ام، اما شنیده‌ام پول آنجا منحصر به‌فرد است. جزیره‌نشین‌های یپ از دیسک‌های ساخته‌شده از سنگ آهک به‌عنوان ارز استفاده می‌کنند. اگر دیسکی آن‌قدر بزرگ باشد که جابه‌جایی آن سخت باشد (همان‌طور که اغلب هستند) مالک آن فقط کافی است نشانه‌ای روی آن بگذارد تا نشان دهد برای تسویه‌حساب تراکنشی استفاده شده است. این مفهوم دست‌کم از لحاظ نحوه ثبت هر تراکنش تا حدی شبیه بیت‌کوین است.

نشانه‌گذاری روی دیسک‌های سنگی یپ با حفظ اطلاعات تراکنش در بلاکچین آنچنان

1. Proof of Stake
2. Yap
3. Micronesia

تفاوتی ندارد. اطلاعات معاملات بیت‌کوین (و دیگر رمزارزها) در سروری مرکزی نگهداری نمی‌شود. بلاکچین در سطح میلیون‌ها کامپیوتر گسترده شده و روی آنها اجرا می‌شود، بنابراین از آنجایی که بلاکچین تنها در یک پایگاه داده بزرگ نگهداری نمی‌شود، هک کردن آن دشوار است. در واقع اطلاعات همزمان همه جا هستند. از این رو بلاکچین همواره روی اینترنت در دسترس همه است و همه می‌توانند از آن استفاده کنند. از حریم خصوصی (دست‌کم در زمینه ارسال و دریافت پول) با استفاده از کلیدهای عمومی و خصوصی حفاظت می‌شود؛ بنابراین بیت‌کوین دارایی برگزیده در اینترنت و بلاکچین ستون اصلی آن است که با مستند و امن کردن همه تراکنش‌ها از آن محافظت می‌کند.

از زمانی که ساتوشی چشم‌اندازش برای بیت‌کوین و بلاکچین را مطرح کرد، یک دهه می‌گذرد. از آن روزهای اولی که سایفرپانک‌ها و خوره‌های فناوری، ارز جدید مد روزی را فقط برای خودی‌ها ترویج می‌کردند تا امروز که رمزارزها با ارائه روشی جدید برای مشارکت در تراکنش‌ها و اجرای آنها عموم مردم را توانمند می‌سازند، مسیر زیادی طی شده است. احتمالا هنوز هم با زمانی که شاهد رقابت رمزارزها با ارزهای متعارف باشیم، فاصله داریم، اما این ایده دیگر علمی-تخیلی نیست. واقعا امکان دارد که در طول زندگی ما اتفاق بیفتد و اگر این‌طور بشود با حذف اشخاص ثالث، هزینه کمتر برای تراکنش‌ها، صرفه‌جویی در زمان، امنیت بهتر و گمنامی تقریبا کامل، در همه انواع تراکنش‌ها به بهره‌وری‌های جدیدی دست می‌یابیم.

بلاکچین جدا از بیت‌کوین و به‌عنوان فناوری، اینترنت بعدی است.

اینترنت با ایجاد دسترسی لحظه‌ای به همه چیز با یک کلیک موس، ما را به عصر کامپیوتر (یا عصر اطلاعات) آورد. اینترنت جهان را هم‌سطح کرده است. همه می‌توانند از فاصله‌های دور با هم ارتباطی سریع برقرار کنند. بلاکچین ما را قادر می‌سازد که دنیای بهتر و متصل‌تری را تجربه کنیم. این دنیا به کمک شفافیت قابل اعتماد خواهد شد، اطلاعات در آن همیشه در دسترس خواهند بود و آزادی دسترسی در آن بیشتر خواهد بود که مشارکت همه را امکان‌پذیر می‌کند. بلاکچین راه را برای ابداع‌ها و نوآوری‌های جدید، کاربردهای جدید و انرژی جوانی نسل بعدی باز می‌کند. بلاکچین برای بسیاری از ما هنوز تازه و در عین حال بسیار هیجان‌انگیز است. معتقدم با کمی صبر خواهیم دید که بلاکچین در آینده خیلی نزدیک کاربردهای مهم و گسترده‌تری پیدا می‌کند.

هیچ ندیده‌ای هنوز

انتشارات راه‌پرداخت

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

ما در نقطه تحـول در سراسـر جهان هسـتیم. چه کسـی تغییـر را در آغوش می‌گیرد و چه کسـی نه؟ تمرکززدایی، اعتماد، حریم شـخصی و دموکراتیزه کـردن معاملات مالـی همه ایده‌هایی هسـتند که زمان تحقق‌شان فرا رسیده اسـت. فناوری بلاکچین قطعا این ایده‌ها را طی چند سال آینده هدایت خواهد کرد. سـوال این است: این اتفاق کجا خواهد افتاد؟ برخی دولت‌ها فناوری آینده را در آغوش خواهند گرفت و سـایرین مقاومت خواهند کرد. چه کسی برنده می‌شـود و چه کسی می‌بازد؟

درکتـاب «اقتصاد کریپتـو: بلاکچین، رمـزارز و اقتصـاد توکن چگونه دنیای مالی را دگرگـون می‌کنند» آریس وان‌لین‌وانگ تشـریح کرده که چگونه این اقتصاد مانند انقلابی جدید عمل خواهـد کرد. او به‌عنوان یک شـخص فعال که هم‌بنیان‌گذار یک صرافی رمزارز بوده و عملکرد موفقی در اقتصاد کریپتو طی چند سال داشته است، یک راهنمای نهایی به سمت چیزی است که گاهی اقتصاد جدید را دچار سردرگمی می‌کند. خوانندگان بی‌شک از چشـم‌انداز وی و درک او از نگرانی‌ها و انگیزه‌های فعالان اقتصادی، بهره خواهند برد.

INDEPENDENTLY
PUBLISHED

کتاب اقتصـاد کریپتو با حمایت کارخانه نوآوری رسانه راه‌کار منتشر شده و نسخه اصلی آن به شکل مستقل منتشر شده است

راه‌کار

انتشارات راه‌پرداخت
ناشـر فنـاوری و نـوآوری
way2pay.press

ISBN 978-622-7702-32-3
۶۹ هـزار تومـان