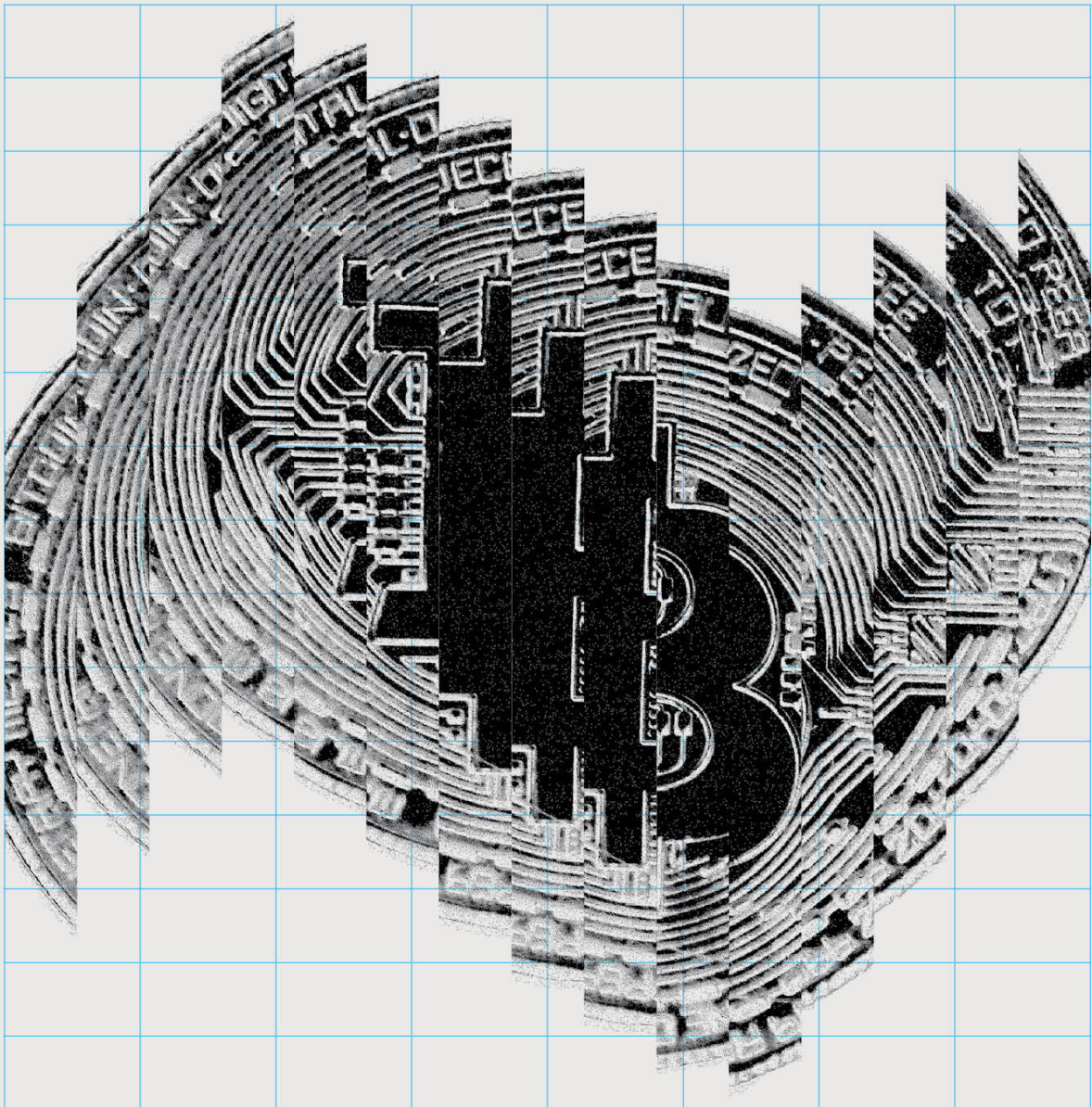


دانشتان رمزارز

مت لوین

با ترجمه: علیرضا کاظمی نیا | محمدرهبان | تریا حقی

رویداد ۹ ژانویه
Jan 9



بسم الله
الرحمن
الرحيم



The mark of
responsible forestry
FSC® C009732

سرشناسه: لوین، مت، Levine, Matt

عنوان و نام پدیدآور: داستان رمزارز/مت لوین؛ باترجمه علیرضا کاظمی نیا، محمد رهبان، ثریا حقی؛ ویراستار ارشد مینا والی؛ ویراستار محتوایی قاسم سرافرازی؛ ویراستار ادبی علی ورامینی.

مشخصات نشر: تهران: راه پرداخت، ۱۴۰۲.

مشخصات ظاهری: ۹۴ ص. مصور(رنگی).

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۹۱-۰

وضعیت فهرست نویسی: فیپا

یادداشت: کتاب حاضر به مناسبت رویداد ۹ ژانویه منتشر شده است.

یادداشت: عنوان اصلی: The crypto story ..., 2022.

یادداشت: بالای عنوان: کتاب راهنما برای درک اینکه رمزارزها از کجا آمده‌اند چه معنایی دارند و چرا مهم هستند.

عنوان دیگر: کتاب راهنما برای درک اینکه رمزارزها از کجا آمده‌اند چه معنایی دارند و چرا مهم هستند.

موضوع: رمزارز، Cryptocurrencies

موضوع: ارز مجازی، Digital currency

شناسه افزوده: کاظمی نیا، علیرضا، ۱۳۶۹-، مترجم

شناسه افزوده: رهبان، محمد، ۱۳۶۷-، مترجم

شناسه افزوده: حقی، ثریا، ۱۳۶۸-، مترجم

شناسه افزوده: والی، مینا، ۱۳۶۳-، ویراستار

شناسه افزوده: رویداد ۹ ژانویه (سومین: ۱۴۰۲: تهران)

رده بندی کنگره: HG۱۷۱۰/۳

رده بندی دیویی: ۳۳۲/۴

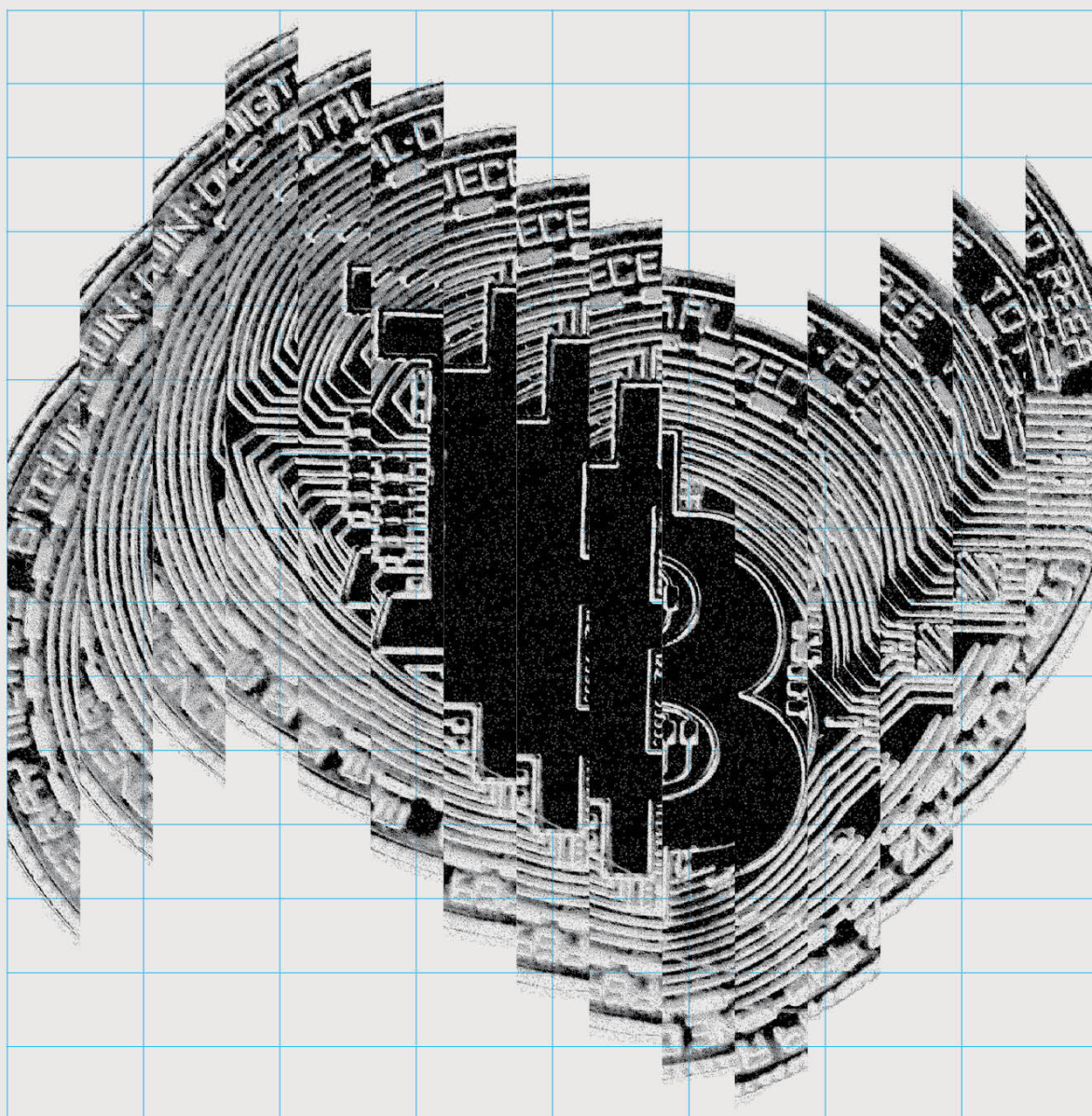
شماره کتابشناسی ملی: ۹۵۰۵۶۹۲

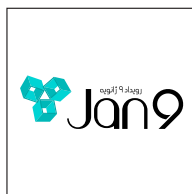
دانشنامه رمزارز

مجله

بترجمه: علیرضا کاظمی نیا | محمدرهبان | ثریا حقی

رویداد ۹ ژانویه
Jan9





عنوان: داستانِ رمزارز

ناشر: راه پرداخت

نویسنده: مت لوین

مترجمان: علیرضا کاظمی نیا، محمد رهبان، ثریا حقی

ویراستار ارشد: مینا والی

ویراستار محتوایی: قاسم سرافرازی

ویراستار ادبی: علی ورامینی

بازبینی نهایی متن: مینا حاجی

صفحه آرا: علیرضا کیوان، حمید ابراهیمی

ناظر چاپ: قادر شهبازی

نوبت چاپ: اول ۱۴۰۲

شمارگان: ۱۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۹۱-۰

تلفن: ۰۲۱-۴۴۴۳۹۶۶

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل: publisher@way2pay.press

وبسایت: way2pay.press

لیتوگرافی: هنراشکان

چاپ و صحافی: واژه

همه حقوق چاپ و نشر این اثر برای «انتشارات راه پرداخت» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتالی و ...) بدون اجازه کتبی ناشر ممنوع است.

فروشگاه انتشارات راه پرداخت نشانی: تهران، جنت آباد جنوبی، خیابان لاله غربی، روبه روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸



داستانِ رمزارز

نوشته مت لوین

ترجمه علیرضا کاظمی نیا، محمدرهبان، ثریا حقّی

۱. دفترکل، بیت کوین و بلاکچین

۵

بخش عمده‌ای از اطلاعات زندگی شما در دفتر کلی ثبت می‌شود که تحت کنترل سازمان‌هایی مانند بانک‌ها، کارپردازها یا اداره‌های دولتی قرار دارد و راهی جز اعتماد به آن سازمان‌ها ندارید. در سال ۲۰۰۸، نوع جدیدی از پول به وجود آمد که طرز تفکر افراد نسبت به اعتماد را تغییر داد.

۲. چه معنایی دارد؟

۲۹

بیت کوین دستاورد بزرگی از دیدگاه فناوری بود، ولی بیت کوین فقط بخشی از این ماجراست. موضوعات بسیار متنوعی وجود دارد که باید درک‌شان کنیم، از اتریوم و وب ۳٫۰ گرفته تا عکس‌های کارتونی گران‌قیمت میمون‌ها.

۳. سیستم مالی کریپتو

۶۲

مدت‌هاست که دنیای واقعی از روایی مشخص پیروی کرده، ولی این روای در دنیای کریپتو صدق نمی‌کند. در این قسمت به نحوه تکامل (و حتی پسرفت) شرایط می‌پردازیم.

۴. اعتماد، پول و جامعه

۸۸

کریپتو از اینجا به کجا می‌رود؟ زمانی که آماده بودید این قسمت را مطالعه کنید، بهتر است قبل از آن به معنی کلمات اعتماد، پول، جامعه و پانزی فکر کنید.

همین چند وقت پیش بود که با خودم فکر کردم: «نکنه در مورد کریپتو اشتباه کرده باشم؟!» حتی من هم که انسانی عادی (شاید هم کمی معتاد به دنیای فایننس) هستم و کمتر از ۱/۰ بیت کوین دارم، گاهی اوقات دچار ترس عقب ماندن از این جهان موازی می شوم که بیشتر از یک دهه به رشد خود ادامه داده است؛ جهانی که طرفداران افراطی آن با اطمینان تمام در موردش صحبت می کنند و معتقدند این بُعد جدید اقتصاد به آینده شکل خواهد داد، ولی از دید منتقدانش، صرفاً نوعی کلاهبرداری پانزی جدید است که پایان خوشی نخواهد داشت. برخی از این افراد حتی امیدوارند «زمستان کریپتویی» فعلی، همان پایانی باشد که مدت هاست منتظرش هستند. با این حال کریپتو برای خودش جایگاهی در فایننس، فناوری و مغز ما باز کرده و شاید بیشتر نزدیک به نقطه شروعش باشیم تا پایان. بنابراین اگر کریپتو قرار نیست از بین برود، بهتر است درک مناسبی از آن به دست آوریم. به همین دلیل از بهترین نویسندگان فایننس این روزها، «مَت لَوین»، نویسنده بلومبرگ اوپینین (Bloomberg Opinion)، خواسته ایم به ما بگوید این فناوری اغلب دیوانه کننده، اکثراً عجیب و همیشه جذاب چیست و در آینده به کجا خواهد رسید.

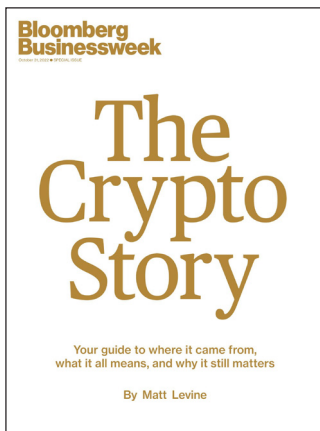
جوئل ویر

سرمدیر بلومبرگ بیزینس ویک

هفته نامه «بلومبرگ بیزینس ویک» را طی چند سال گذشته به صورت مداوم دنبال کرده ایم؛ این رسانه با اینکه بر دنیای کسب و کارها تمرکز دارد، ولی به صورت پیوسته از دیدگاه مالی به موضوعات نگاه می کند. اگر جلد های این ماهنامه و مطالبش در این چند سال را دنبال کرده باشید، می دانید که فناوری های مالی و به طور خاص رمزارزها و بیت کوین مورد توجه این رسانه بوده اند. با اینکه این رسانه تا حد خوبی تخصصی محسوب می شود، ولی محتواهایش به زبان ساده بیان می شوند. زمانی که دیدیم این رسانه یک شماره کامل را به رمزارزها اختصاص داده، تصمیم گرفتیم کل شماره را ترجمه و صفحه آرایی و به عنوان ضمیمه ماهنامه عصر تراکنش منتشر و در اختیار مدیران فناوری های مالی ایران قرار دهیم. در این سال ها در انتشارات راه پرداخت و دیگر رسانه های راه کار به صورت پیوسته درباره رمزارزها و بیت کوین و اتریوم نوشته ایم؛ تلاش کرده ایم بیشتر از اینکه دیگران را به ورطه تردینگ هل دهیم، به آنها آموزش دهیم که با این فضا آشنا شوند و بعد از اینکه راه را از بیراه شناختند، با اختیار خودشان و متکی بر دانش و عقل خودشان، وارد این فضا شوند. فناوری پشت رمزارزها برای ما جذاب تر از سودهای آنی است و تصور می کنیم آنهایی که فلسفه و فناوری پشت رمزارزهایی مانند بیت کوین و اتریوم را درک کنند، از این فضا لذت می برند. حالا و با گسترش ابزارها و کسب و کارها، شاهد این هستیم که عرصه رمزارز گسترده تر شده و این روزها مفاهیمی مانند متاورس و ان اف تی و دیفای به کرات شنیده می شود. در این شماره ویژه عصر تراکنش که ترجمه کامل شماره ویژه «بلومبرگ بیزینس ویک» است، با زبانی ساده همه آنچه را باید درباره رمزارزها بدانید، به شما آموزش می دهیم. امیدواریم این کار مفید باشد.

رضا قربانی

مدیرمسئول انتشارات راه پرداخت



کتاب داستان رمزارز ترجمه‌ای از یک شماره کامل نشریه بلومبرگ بیزینس ویک است که پیش از این به عنوان ضمیمه ماهنامه عصر تراکنش با حمایت مجموعه اکسکوینو منتشر شده است. با توجه به کیفیت محتوا، تصمیم گرفتیم این اثر به شکل یک کتاب مستقل نیز منتشر شود.



کریپتو به زبان آدمیزاد؛ من اگر می‌خواستم برای این ویژه‌نامه بلومبرگ تیتري بزنم، همین تیتري را به زبان انگلیسی انتخاب می‌کردم. یک روزنامه‌نگار که آشنایی چندانی هم با جهان کریپتو ندارد، تصمیم به نوشتن مطالبی درباره چپستی، کارکرد و ابعاد کریپتو و این بازار می‌گیرد. در واقع او سعی می‌کند با روایت‌گونه کردن یک پدیده زمخت، آن را چنان خواندنی کند که هر آدم دور از این داستانی را جذب داستان خودش کند. یکی از چیزهایی که به این ویژه‌نامه بلومبرگ و کاری که نویسنده‌اش کرده، اهمیت می‌بخشد، این است که او زمانی شروع به نوشتن و تحقیق درباره بازار کریپتو می‌کند که تقریباً می‌توان گفت هیچ زمان دیگری کریپتو چنین در محاق و استقبال مردمی از آن ناامیدکننده نبوده است. پرواضح است که این دوران بی‌فروغ به دلیل ریزش شدید بیت‌کوین و دیگر کوین‌هاست. کار «مت لوین» از این جهت اهمیت پیدا می‌کند که از قضا در این شرایط است که می‌توان یک پدیده را خوب شناخت. وقتی شور عامه مردم نسبت به چیزی زیاد می‌شود، همیشه ماهیگیرانی هستند که تور خود را برای آنان که سرمایه‌به‌دست، گیج و جاهل نسبت به موضوع دور خود می‌چرخند، پهن می‌کنند تا در آن گل‌آلود آب برای خود ماهی‌های سرگردان را به تور بیندازند؛ همان‌هایی که همیشه در دوران اوج بورس کارشناس بورس می‌شوند و در دوران اقبال کریپتو، متخصص بازار کریپتو. هنگامه افول و ریزش بازار هم هیچ نشانی از این متخصصان فصلی پیدا نخواهد شد. همین که نویسنده این مطالب در این مقطع سراغ چنین بحثی می‌رود پیش از همه چیز به ما نشان می‌دهد که با یک ماهیگیر فصلی طرف نیستیم و نویسنده هر قصد و نیتی داشته باشد، نخواسته بر موج جهل مردم هجوم آورده به بازاری سوار شود. شاید در نگاه اول، این موضوع بی‌ارزشی به نظر برسد، اما نکته این است که وقتی با چنین بازاری و پالودگی انواع مطالب، مقاله، تحلیل و... مواجه هستیم، یکی از راه‌های تشخیص سره از ناسره همین نکات است. اینکه تحلیلگران ریشه‌دار، همچون قارچ در روزهایی خاص سر بر نمی‌آورند، بلکه فارغ از هیاهوها به کندوکاو می‌پردازند.

علی ورامینی

مشاور انتشارات راه‌پروا

I

دفترکل، بیتکوین وبلاکچین

الف

زندگی در دیتابیس‌ها



دنیای مدرن ت از دیتابیس ه بزرگ تشک



ساحدزیادی

سای سازمان های

ل شده است

اگر پولی در بانک دارید، در واقع آنچه دارید رکوردی از دیتابیس بانک است که نشان می‌دهد چقدر پول دارید. اگر سهامی خریده باشید، در واقع دارایی شما رکوردی در دیتابیس شرکت یا نهادی واسطه و متمرکز است.^۱

اگر صاحب‌خانه باشید، شرایط کمی فرق می‌کند، چون خانه‌ای فیزیکی وجود دارد، ولی مالکیت شما روی آن خانه در دیتابیسی ثبت شده است. مثلاً اگر در آمریکا زندگی کنید، مدارکی وجود دارد که نشان می‌دهد شما آن خانه را خریده‌اید (سند مالکیتی که در کشویی در زیرزمین اداره ثبت کانتی محل زندگی شما قرار دارد). حضور فیزیکی شما در آن خانه اهمیت زیادی دارد؛ کلید آنجا را دارید، وسایل تان آنجاست، همسایگان تان از اینکه ببینند که از خانه خارج می‌شوید، شگفت‌زده نمی‌شوند، ولی اگر ببینند غریبه‌ای وارد خانه شده، تعجب خواهند کرد. با این حال، رکورد ثبت شده در دیتابیس از جهات زیادی اهمیت دارد. مثلاً اگر بخواهید وام بگیرید، بانک باید اطمینان حاصل کند که سند ملک به نام شماست. به همین ترتیب، اگر کسی بخواهد خانه‌تان را بخرد، باید مطمئن شود که نام شما روی سند است؛ صرف در اختیار داشتن کلید کافی نخواهد بود.

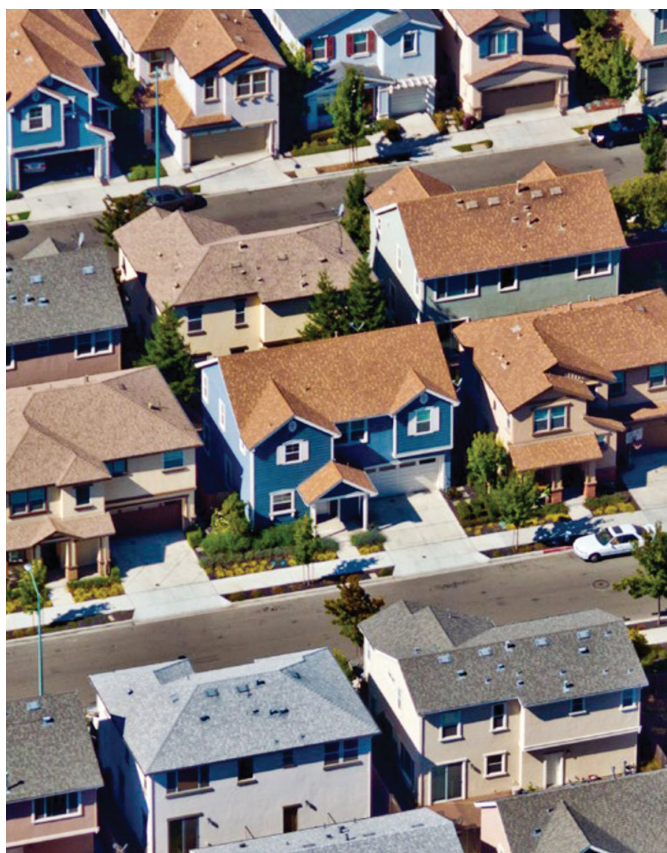
مثال‌های متعدد دیگری وجود دارد. بخش عمده‌ای از اتفاقات دنیای امروز در محیط آنلاین رخ می‌دهد. نمی‌توان گفت که زندگی اجتماعی و مسیر شغلی افراد به رکوردهایی تبدیل شده که در دیتابیس‌های گوگل، متا و مایکروسافت قرار دارند، ولی نمی‌توان هم گفت که این‌گونه نیست.

بخشی از این شرایط به خاطر فراگیر شدن کامپیوترهاست. نگاه داشتن پول به صورت رکوردهایی در دیتابیس بسیار راحت‌تر از نگاه داشتن آن به صورت طلا یا حتی اسکناس است، اما برخی موضوعات کمی پیچیده‌تر هستند. مثلاً صاحب‌خانه بودن اصلاً به چه معنی است؟ یک جواب برای این پرسش از دیدگاه طبیعت است؛ به این معنی که هر کس در خانه باشد، صاحب آن است و اگر کسی قدرت بیشتری داشته باشد و بتواند او را بیرون کند، صاحب جدید آن خانه خواهد شد.

گزینه دیگر این است که از دیدگاه روستا به مسئله نگاه کنیم. صاحب‌خانه بودن به این معنی است که فرد در آن خانه زندگی می‌کند و همسایگانش می‌دانند که در آن خانه زندگی می‌کند و اگر کسی تلاش کند وارد آن خانه شود، صاحب اول به همراه همسایگانش قدرت بیشتری دارند و جلوی ورود او را می‌گیرند. به این ترتیب مالکیت خانه به واسطه شبکه‌ای از هم‌رده‌ها که اعتماد زیادی به یکدیگر دارند، تضمین می‌شود. سومین دیدگاه هم دیدگاه «دولت» است؛ صاحب‌خانه بودن به این معنی است که دولت معتقد باشد کسی صاحب‌خانه است و اگر کسی تلاش کند وارد خانه شود، دولت او را

بیرون می‌کند.^۲ به این ترتیب، دولت عامل تضمین مالکیت است و دیتابیس هم ابزاری برای این کار است. در این شرایط اعتماد به شخص لازم نیست، بلکه باید به اعمال قانون اعتماد کرد.

مالکیت پول هم تا حدی شبیه به همین موضوع است. کیسه طلا راهکار به نسبت ساده‌ای برای نشان دادن مالکیت پول است، ولی وزن زیادی دارد. در مقابل وقتی بانکداری وجود داشته باشد که از طلای افراد نگهداری می‌کند و رسیدی به آنها می‌دهد که می‌توانند آن را خرج کنند یا با مراجعه به بانک دیگری که مدیرش دوست مدیر بانک اول است، طلای خود را بگیرند، کار بسیار ساده‌تر می‌شود؛ هرچند افراد باید به بانکداران اعتماد کنند و بانکدارانی که با هم دوست هستند نیز باید به یکدیگر اعتماد داشته باشند. در سیستمی که مبتنی بر رابطه شخصی نباشد، به نحوی که کارمندان باجه‌دار بانک با مشتریان آشنا نباشند و مشتریان حتی بتوانند از دستگاه خودپرداز پول دریافت کنند، اعتماد به سیستم لازم است؛ اعتماد به اینکه دولت، قوانین، تلاش برای حفظ وجهه یا نیروهای بازار، دست‌وپای بانک‌ها را می‌بندند؛ بنابراین آنها رفتار مناسبی خواهند داشت.



● همسایگی، جایی که هرکسی اسم شما را می‌داند

۱. یکی از این واسطه‌ها شرکت سپرده‌گذاری و تسویه وجوه است که به نیابت از افراد عادی صاحب سهام اکثر شرکت‌های آمریکایی است؛ بنابراین اگر صاحب سهامی هستید، در واقع دارای رکوردی در دیتابیس این شرکت هستید که نشان می‌دهد این شرکت چه تعدادی از سهم‌های کدام شرکت را به نیابت از شما در اختیار دارد.

۲. لازم نیست آنجا زندگی کنید، چون اطلاع داشتن دولت کافی است. می‌توانید خانه را اجاره دهید، به این معنی که شخص دیگری با اجازه شما آنجا زندگی کند، اگر آن اجازه را لغو کنید، می‌توانید با مراجعه به دولت بخواهید که آن شخص از خانه شما خارج شود.

ما به ننگه دارندگان دیتابیس‌ها اعتماد می‌کنیم

۱۳

پس وقتی می‌گوییم زندگی مدرن در دیتابیس‌ها ثبت می‌شود، به این معنی است که زندگی مدرن به اعتماد زیادی نیاز دارد. بعضی اوقات این اعتماد به خاطر شناخت است، ولی اکثر مواقع به خاطر اعتمادی است که به کل سیستم داریم؛ سیستمی از قوانین و دیتابیس‌ها و خود مفهوم اعتماد. ما فرض می‌کنیم که می‌توانیم به سیستم اعتماد کنیم، چون این کار زندگی را بسیار ساده‌تر می‌کند و این فرض در اکثر مواقع درست است. اعتماد کلی ما به نگه‌دارندگان دیتابیس‌ها و اینکه اکثرشان قابل اعتماد هستند یکی از مهم‌ترین دستاوردهای زندگی مدرن است،

ب

اگر کسی از این شرایط راضی نباشد، چه؟

۱. بی‌اعتمادی

همیشه هم به نگه‌دارندگان دیتابیس‌ها اعتماد نداریم و این افراد همیشه هم قابل اعتماد نیستند؛ گاهی اوقات به این خاطر که اصلاً قابل اعتماد نیستند. مثلاً بانک‌هایی وجود دارند که به هیچ وجه برای نگهداری پول قابل اعتماد نیستند و در برخی مناطق نمی‌توان اعتماد داشت که قانون توانایی نظارت کافی بر این بانک‌ها را دارد. دولت‌هایی وجود دارند که نمی‌توان به آنها اعتماد کرد که موجودی حساب افراد را توقیف نکرده، نتایج انتخابات را دستکاری نکنند و اسناد مالکیت را تغییر ندهند. شبکه‌های اجتماعی‌ای وجود دارند که نمی‌توان به آنها اعتماد کرد که به دلخواه خودشان حساب کاربری افراد را مسدود نکنند. اکثر ساکنان ایالات متحده در اکثر روزهای عمر خود در دنیایی با اعتماد زیاد زندگی می‌کنند؛ دنیایی که می‌توان به واسطه‌های نگه‌دارنده دیتابیس‌های مهم اعتماد کرد و انتظار داشت که رفتار مناسبی داشته باشند، ولی همه افراد در سراسر دنیا در چنین محیطی زندگی نمی‌کنند.

حتی در آمریکا نیز اعتماد می‌تواند مفهوم شکننده‌ای باشد. بحران مالی ۲۰۰۸ آسیبی جدی به اعتماد افراد نسبت به نظام بانکداری وارد کرد. افراد عادی فکر می‌کردند بانک‌ها فعالیت‌های خوب، امن و مفید انجام می‌دهند، ولی مشخص شد که اقداماتی پرریسک انجام داده‌اند که به بحران مالی منجر شده بود. پس از آن اتفاق‌ها افراد کمتری حاضر بودند پس‌انداز خود را به بانک‌ها بسپارند.

همچنین افرادی وجود دارند که از دیدگاه فلسفی با مفهوم اعتماد موافق نیستند. حتی بانک‌هایی که هیچ نوع سابقه نامناسبی ندارند هم قابل اعتماد نیستند؛ زیرا از نظرشان بانک نوعی جعبه سیاه است. چنین فردی به بانک می‌گوید: «از کجا می‌توانم مطمئن باشم که پولم را پس می‌دهید؟» و بانک در جواب می‌گوید: «می‌توانید به ترازنامه‌های حسابرسی شده ما نگاه کنید. ما تحت نظارت فدرال رزرو هستیم. شرکت بیمه سپرده فدرال هم ما را بیمه کرده و تاکنون پیش نیامده که پول کسی را پس ندهیم.» با وجود این توضیحات نمی‌توان مطمئن بود که بانک پول فرد را پس می‌دهد، چون وجود اعتماد یکی از الزامات این سیستم است، ولی شاید کسی «مدرک» بخواهد.^۳



که اکثراً نادیده گرفته می‌شود.



^۳ شاید چنین خواسته‌ای مربوط به عصر مدرن باشد یا حداقل خواسته‌ای باشد که در دنیای مدرن با سهولت بیشتری به دست می‌آید. در دنیایی که اینترنت، ویکی‌پدیا، نرم‌افزارهای منبع باز و چنین مواردی وجود نداشت، افراد مجبور بودند هر روز میلیون‌ها ادا را بدون دلیل و مدرک بپذیرند چون راه دیگری نداشتند.

زندگی مدرن از اطلاعات درون دیتابیس‌های متعدد تشکیل شده است:



حتی اگر برخی افراد حاضر باشند به نگه‌دارنده‌های دیتابیس اعتماد کنند، شاید از دیدگاه فنی اعتراض داشته باشند. این دیتابیس‌ها همیشه خوب نیستند. بسیاری از سیستم‌های بانکداری با زبان کامپیوتری بسیار قدیمی‌ای به نام کوپول نوشته شده‌اند. هنوز افراد زیادی در آمریکا وجود دارند که با پست کردن چک‌های کاغذی حساب‌های خود را پرداخت می‌کنند. تسویه‌شدن معاملات سهام در آمریکا دو روز زمان می‌برد. به عبارت دیگر، اگر من روز دوشنبه از کسی سهام بخرم، او روز چهارشنبه سهام را تحویل می‌دهد و من هم چهارشنبه هزینه را پرداخت می‌کنم. دلیل این تأخیر به این خاطر نیست که کارگزار من مجبور است پول کاغذی به کسی تحویل دهد یا کارگزار خریدار مجبور است سند کاغذی سهام را ارسال کند، ولی فرایندی که اتفاق می‌افتد از نوادگان همین فرایند است. این فرایند به صورت دستی رخ می‌دهد و برخی مواقع اشتباه‌هایی در آن رخ می‌دهد. به همین دلیل است که معاملات زیادی «ناموفق» می‌شوند. بهتر است دیگر سراغ بحث خرید ملک نرویم، چون فرایندش بیشتر شبیه مراسمی است که با حضور چند وکیل و کارمند و با خواندن عبارت‌هایی شبیه به طلسم انجام می‌شود.

• آیا می‌توانید این بانک
را نام ببرید؟ فرقی ندارد
که بتوانید یا نه! این بانک
به هر حال یک جعبه سیاه
است.



اگر دیتابیس‌ها را به روز کنیم، چه؟

چه اتفاقی رخ می‌داد اگر می‌توانستیم تمام دیتابیس‌های موجود را دوباره با زبان‌های برنامه‌نویسی، نرم‌افزارها و اصول مهندسی جدید ایجاد کنیم و هدفمان ایجاد ارتباط بین آنها باشد؟ اگر چنین اتفاقی رخ می‌داد، شبیه به این بود که یک دیتابیس بزرگ داریم؛ دیتابیس کل زندگی. کاربران می‌توانستند پول و ملک خود را به سادگی مبادله کنند یا در ازای شرکت در کلاس یا جلسه آنلاین به یکدیگر امتیاز و جایزه بدهند و همه این اتفاق‌ها روی یک سیستم کامپیوتری واحد رخ می‌داد.

وجود چنین سیستمی کارها را بسیار ساده می‌کند و قدرت بسیار زیادی دارد، ولی ترسناک هم هست، چون مفهوم اعتماد را تحت فشار بسیار بیشتری قرار می‌دهد. هر کس کنترل این دیتابیس را داشته باشد، عملاً دنیا را در کنترل خود دارد. به چه کسی می‌توان تا این حد اعتماد کرد؟

اگر از آن دست افرادی باشید که دیتابیس‌های کامپیوتری مدرن را تجربه کرده‌اند، این فرایندهای دستی و کُند به نظرتان عجیب خواهد بود. شاید فکر کنید باید دیتابیس‌ها از طریق رابط‌های برنامه‌نویسی با یکدیگر تعامل کنند تا سرعت کار بالا برود. مثلاً وقتی بانک می‌خواهد به مشتری خود وام مسکن بدهد، باید بتواند به راحتی به دیتابیس ثبت اسناد متصل شده و مطمئن شود که او صاحب واقعی خانه مورد نظر است (به جای اینکه مجبور باشد وکیل خود را به دفتر ثبت اسناد بفرستد). همچنین باید بتواند با اتصال به دیتابیس نهادهای انتظامی از هویت متقاضی وام مطمئن شود و با کمک دیتابیس کارگزاری بورس از دارایی‌های او اطمینان حاصل کند.

چه می‌شد اگر فقط یک دیتابیس مدیریت آن‌ها می‌شد

پیس وجود داشت و همه در ارکت داشتند؟

۱. حاشیه: اصلاً در حال خواندن چه چیزی هستید؟ چرا می‌خوانیدش؟ چرا من آن را نوشته‌ام؟

سلام! من مت هستم. قبلاً وکیل و سرمایه‌گذار بانکی بودم. اکنون برای مجله بلومبرگ اوپینیون مطلب می‌نویسم. شغلم نوشتن مطالب مرتبط با فایننس است. به فایننس علاقه دارم. نوشتن در موردش کار جذابی است. فایننس نگاه خاصی به دنیا دارد و در واقع مجموعه‌ای از ساختارهاست که انسان‌ها برای اقتصاد تعیین کرده‌اند. درک این ساختارها اغلب کار سختی است و حس لذت‌بخشی دارد که بتوانم آنها را بفهمم. همه اصول فایننس پیش‌فرض‌های متعددی دارند. همه چیز عجیب است و اغلب باید اطلاعات زیادی در مورد فعالیت‌های بازار و تاریخچه مالی داشت تا بتوان رفتار افراد را درک کرد.

در چند سال گذشته، جنجالی‌ترین موضوع فایننس، «کریپتو» بوده است. کریپتو مجموعه‌ای از ایده‌ها، محصولات و فناوری‌هاست که از وایت‌پیپر بیت‌کوین نشئت گرفته‌اند، اما کریپتو به همان اندازه خطوطی است که طی این سال‌ها روی چارت‌های مالی شکل گرفته‌اند. زمانی که ساتوشی بیت‌کوین را اختراع کرد، هر بیت‌کوین صفر دلار ارزش داشت، چون ایده‌ای خام بود، اما نوامبر سال گذشته قیمت بیت‌کوین تا ۶۷ هزار دلار هم اوج گرفت و کل ارزش کریپتوهای در گردش از سه تریلیون دلار فراتر رفت. بسیاری از افرادی که اوایل ظهور کریپتو، وارد بازار شده بودند، به سرعت ثروتمند شدند و توانستند خودروها و خانه‌های گران‌قیمت بخرند. آنها از عملکرد خود خوشنود بودند، چون فکر می‌کردند کریپتو آینده دنیاست و آنها نیز در حال ساختن آینده هستند و به همین دلیل پاداش مناسبی دریافت می‌کنند. آنها به افرادی که کریپتو نداشتند، می‌گفتند: «فقیر ماندن خوش بگذره.» این افراد حق را به خود می‌دادند و ثروتمند شده بودند و می‌خواستند همه این موضوع را بدانند.

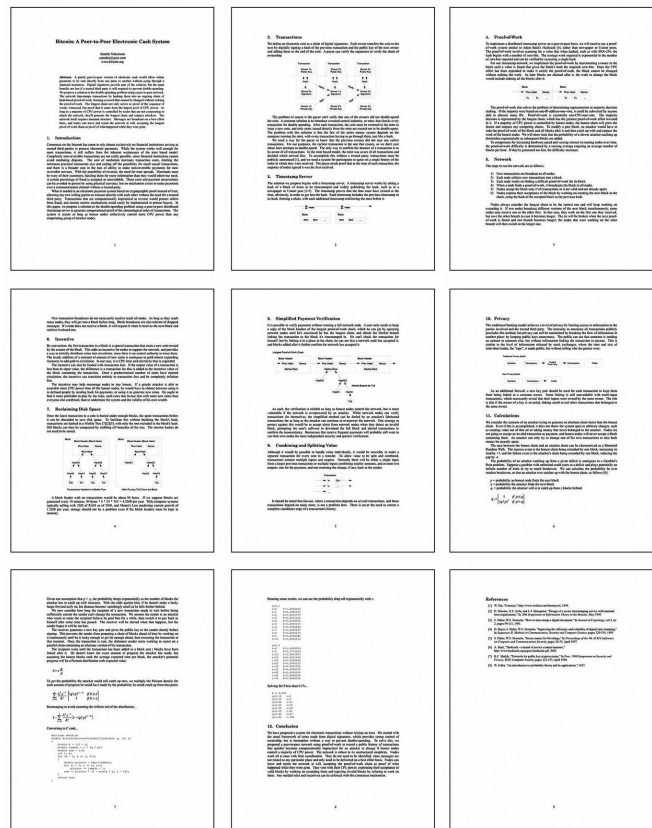
افراد بسیار زیادی هم بودند که وارد کریپتو نشده بودند. تصور این افراد (که خیلی هم اشتباه نبود) این بود که کریپتو راهکاری مناسب برای جرائم مالی و کلاهبرداری پانزی است. آنها می‌پرسیدند: «هدف این کارها چیست؟»، «این پول‌ها از کجا آمده است؟»، «اگر واقعاً در حال ساختن آینده هستید، دقیقاً چه کاری انجام می‌دهید؟» و «اگر واقعاً در حال ساختن آینده هستید، چرا آینده این قدر تاریک به نظر می‌آید؟» و پاسخ طرفداران کریپتو اغلب این بود: «فقیر ماندن خوش بگذره.»

امسال آن خط‌های روی نمودارها نزولی شدند، قیمت بیت‌کوین از ۲۰ هزار دلار هم پایین‌تر رفت و ارزش کل بازار به کمتر از یک تریلیون دلار رسید؛ در این میان برخی از بزرگ‌ترین شرکت‌های کریپتو ورشکست شدند. این موضوع نه تنها باعث خوشحالی مخالفان کریپتو شد، بلکه باعث می‌شد از اهمیت کریپتو در خبرها کاسته شود. در مقابل طرفداران کریپتو تأکید بیشتری روی ادعاهای خود کردند. آنها

ساتوشی ناکاموتو در سال ۲۰۰۸ راهکاری را ارائه داد تا همه افراد بتوانند دیتابیس خود را مدیریت کنند و به این ترتیب مفهوم «کریپتو» یا رمزارز را خلق کرد.

فکر نمی‌کنم ساتوشی در آن زمان فکر می‌کرد دارد چنین کاری می‌کند. او در آن زمان می‌خواست «بیت‌کوین؛ سیستمی هم‌تابه هم‌تابه برای پول نقد الکترونیکی» (عنوان وایت‌پیپر) را خلق کند. ساتوشی ادعا می‌کرد نوعی پول نقد برای تراکنش‌های اینترنتی ایجاد کرده است؛ «نوعی سیستم پرداخت الکترونیکی مبتنی بر اثبات رمزنگاری به جای اعتماد که به فرد اجازه می‌دهد پول جابه‌جا کند، بدون اینکه به شخص ثالث مورد اعتمادی نیاز باشد». به این ترتیب اگر من بخواهم کالایی از کسی بخرم، کافی است پول دیجیتال (بیت‌کوین) برای او بفرستم و او نیز کالا را برای من ارسال کند. هیچ شخص ثالث مورد اعتمادی مثل بانک در این تعامل نقش ندارد.

وقتی روال را این‌گونه توصیف می‌کنیم، به نظر می‌رسد ساتوشی سیستمی را ابداع کرده که دو طرف می‌توانند با هم تعامل کنند، بدون اینکه هیچ‌کس دخالت کند، ولی حقیقت این است که افراد متعددی در این تعامل نقش دارند.





می‌توان به مفاهیم کریپتو نگاه کرد و معادل‌هایی در دنیای فایننس برایشان پیدا کرد. با این کار می‌توان اطلاعات زیادی از هر دو طرف به دست آورد؛ از یک طرف می‌توان آینده مفاهیم جدید کریپتو را پیش‌بینی کرد (مثلاً اینکه چه اتفاق ناگواری برای پروژه‌ای رخ خواهد داد) و از طرف دیگر می‌توان دید جدیدی به مفاهیم قدیمی فایننس پیدا کرد.

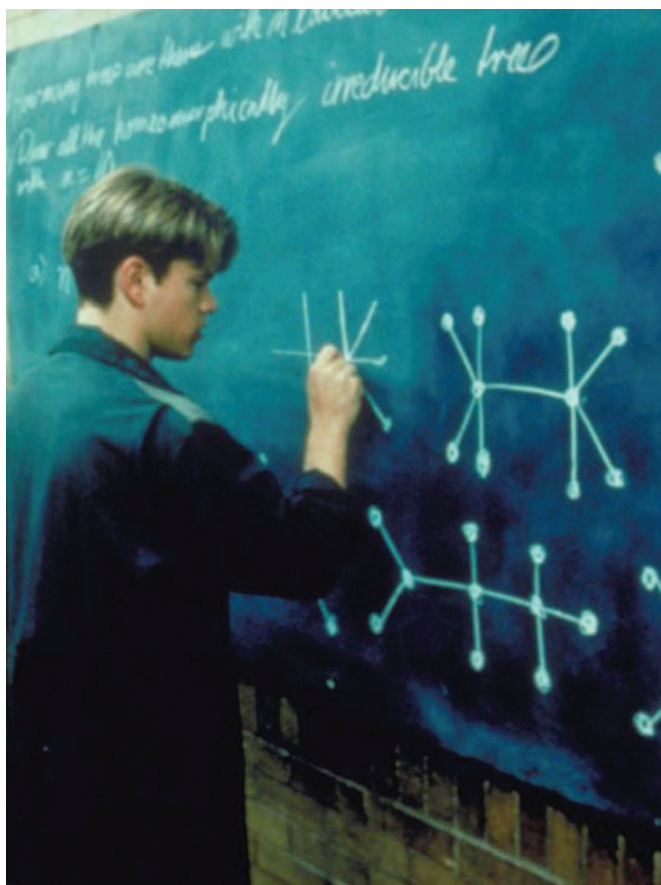


● جمعیتی در کنفرانسی مربوط به بیت‌کوین در میامی، آوریل ۲۰۲۲

همچنین، باید بگویم به‌عنوان کسی که در مورد فایننس می‌نویسد، علاقه خاصی به داستان‌های کلاهبرداری و فریب افراد باهوش دارم. این داستان‌ها معمولاً جالب، روشن‌گر و به‌ویژه خنده‌دار هستند. دنیای کریپتو از این داستان‌ها زیاد دارد؛ بنابراین این روزها زیاد در مورد کریپتو می‌نویسم. باید در رابطه با چند مورد هم هشدار بدهم؛ اول اینکه من متخصص ماهری در زمینه کریپتو نیستم و واقعاً به آن باور ندارم. تا قبل از نوشتن این مقاله کریپتو نداشتم و اکنون هم فقط یکصد دلار دارم؛ بنابراین هدفم از نوشتن در مورد کریپتو از دیدگاه کسی است که به **نبوغ و حماقت** انسان علاقه دارد و هر دوی این پدیده‌ها به‌وفور در دنیای کریپتو یافت می‌شوند. در مقابل، هدفم از نوشتن این مقاله این نیست که بگویم کریپتویی ارزش

معتقدند سقوط بازار باعث خروج طرفداران ضعیف خواهد شد و به طرفداران واقعی کریپتو اجازه می‌دهد که آینده را در کنار یکدیگر خلق کنند.

شاید برخی فکر کنند اکنون زمان مناسبی برای صحبت کردن در مورد کریپتو نیست، چون قیمت نزولی شده، ولی الان زمان مناسبی برای این کار است، زیرا هیجان بازار خوابیده و آنچه در بازار باقی مانده، محدود به سفته‌بازی و کلاهبرداری نیست. اکنون می‌توانیم به معنای واقعی کریپتو فکر کنیم (تا حدی بدون توجه به نمودارهای صعودی). من نه آنچنان طرفدار کریپتو هستم و نه آنچنان مخالفش. به فایننس علاقه دارم؛ از نظرم موضوع جالبی است و اگر کسی به فایننس (درک ساختارهایی که انسان‌ها برای نظم‌دادن به اقتصاد ایجاد می‌کنند) علاقه داشته باشد، کریپتو برایش جذابیت بسیار زیادی دارد. کریپتو شبیه آزمایشگاهی برای نهادهای مالی است که در ۱۴ سال گذشته توانسته یک سیستم مالی جدید را از صفر ایجاد کند. کریپتو در این مدت به دنبال بهبود یا متحول کردن فعالیت‌های استاندارد فایننس بوده و برخی مواقع توانسته راه‌های بهتری پیدا کند.



اما بسیاری از تلاش‌های کریپتو هم به بن‌بست‌هایی رسیده که فایننس سنتی دهه‌ها پیش کشف کرده بود. در بسیاری از موارد شاهد راهکارهایی بودیم که فایننس سنتی قبلاً ارائه کرده بود، ولی صرفاً نام‌ها و توضیحات جدیدی برای آنها انتخاب شده بود.

منجر شوند. علاوه بر آن، جنبه فایننس ماجرا بسیار جذاب است!

۲. حاشیه: اسامی و افراد

قبل از اینکه ادامه دهیم، خوب است چند نام و مفهوم را بررسی کنیم؛ اول به «کریپتو» پردازیم که موضوع این مقاله است. نام خوبی برای آن وجود ندارد، ولی اکثر متخصصان از کریپتو استفاده می‌کنند که مخفف کلمه «کریپتوکارنسی» [در فارسی رمزارز] است. این نام به دو دلیل خوب نیست؛ اول اینکه روی مفهوم «ارز» تأکید دارد، در حالی که بخش زیادی از دنیای کریپتو الزاماً ربطی به ارز ندارد و دوم اینکه روی مفهوم «کریپتوگرافی» [در فارسی رمزنگاری] تأکید دارد، ولی اکثر فعالان این حوزه مستقیماً فعالیت‌های مرتبط با رمزنگاری انجام نمی‌دهند. متخصصان، میلیاردرها و رهبران این حوزه الزاماً اطلاعاتی در مورد رمزنگاری ندارند و افرادی که متخصص رمزنگاری هستند، بعضی اوقات از اینکه دیگران پیشوند «کریپتو» را استفاده می‌کنند، دلخور می‌شوند.

«بلاکچین»

«توکن»

«وب ۳/۰»

«دیفای (فایننس توزیع شده)»

«متاورس»

نام‌های متعدد دیگری هم در کریپتو وجود دارند و بعضی اوقات برای اشاره به مفاهیم بسیار گسترده‌ای استفاده می‌شوند، ولی آن نام‌ها برتری خاصی نسبت به «کریپتو» ندارند؛ بنابراین از همین نام در ادامه مقاله استفاده خواهیم کرد. دومین نام و مفهوم، «ساتوشی ناکاموتو» است؛ نام مستعار کسی که وایت‌پیپر بیت‌کوین را نوشت و تاکنون توانسته هویت واقعی خود را مخفی نگه دارد (حدس و گمان‌های متعددی در مورد اینکه ساتوشی واقعی کیست، وجود دارد؛ از ایلان ماسک تا برنامه‌نویسی که اسم واقعی‌اش ساتوشی ناکاموتو است. در ادامه مقاله او را ساتوشی خطاب می‌کنم).

شایان ذکر است که (شاید) به جز ساتوشی، تمام افراد مشهور دنیای

و احمقانه است و به‌زودی از عرصه روزگار محو خواهد شد. چنین کاری مثل هدر دادن وقت است. هدفم این نیست که شما را قانع کنم که کریپتو در حال ساختن آینده است و اگر شما هم سوار این قطار نشوید، فقیر خواهید ماند. می‌خواهم قانع‌تان کنم که کریپتو جالب است و راهکارهای جدید برای مسائل قدیمی پیدا کرده و حتی اگر بعضی از این راهکارها اشتباه باشند، درس‌هایی برای ما دارند.

به نظر من کریپتو توانسته در ۱۴ سال گذشته سیستم مالی قابل قبولی به وجود آورد که در موردش بیشتر صحبت خواهم کرد، چون به فایننس علاقه دارم، ولی به نظرم لازم نیست افراد عادی آن قدرها هم به سیستم‌های مالی توجه داشته باشند. هر سیستم مالی در واقع مجموعه‌ای از دیتابیس‌هاست؛ راهی برای انتقال ادعای دارایی نسبت به کالاهای قابل لمس، نوعی مکمل دنیای واقعی. سیستم مالی‌ای که بتواند پرورش محصولات کشاورزان، خانه‌دار شدن خانواده‌ها و خلق محصول کسب‌وکارها را ساده کند، سیستم خوبی است. در مقابل سیستمی که باعث ثروتمند شدن معامله‌گران کالاهای انتزاعی شود، بدون اینکه به هیچ‌کس دیگر کمک کند، سیستمی ناکارآمد است.

یکی از برجسته‌ترین پرسش‌های دنیای کریپتو در ۱۴ سال گذشته این بوده که کریپتو چه کاربردی دارد. اکثر کسب‌وکارهایی که واقعاً از کریپتو استفاده می‌کنند، کسب‌وکارهای مالی هستند؛ مثلاً صرافی‌هایی که امکان خرید و فروش کریپتو را فراهم می‌کنند یا راهکارهایی که به مهاجران اجازه می‌دهد ساده و سریع به کشور خود پول ارسال کنند. در همین حال، جدی‌ترین طرفداران کریپتو معتقدند که هدف کریپتو خلق سیستم‌های واقعی و مفید است. کریپتو روابط اجتماعی، بازی کردن و کامپیوترها را تغییر خواهد داد و متاورس را به وجود خواهد آورد. کریپتو عنصری حیاتی در جهش بعدی اینترنت خواهد بود و وب ۳/۰ را جایگزین وب ۲/۰ خواهد کرد. اگر از این افراد بخواهیم که نمونه‌ای از کسب‌وکارهای واقعی مبتنی بر کریپتو ارائه دهند، چندین کسب‌وکار مالی بسیار جذاب را نام خواهند برد، ولی پس از آن اکثر کاربردهای کریپتو تئوری خواهند بود؛ مثلاً شبکه اجتماعی مبتنی بر کریپتو روی وب ۳/۰ (که هنوز به وجود نیامده است).

شاید هنوز برای به وجود آمدن چنین شبکه‌ای زود باشد. شاید تا ۱۰ سال دیگر کریپتو، بلاکچین و توکن‌ها اهمیت حیاتی برای همه فعالیت‌های اینترنتی داشته باشند، اینترنت هم (حتی بیشتر از امروز) در زندگی افراد نقش داشته باشد و افرادی که زودتر وارد کریپتو شده‌اند، بسیار ثروتمند شده باشند. شاید آن زمان حتی کودکان هم بدانند دوج‌کوین چیست!

منی‌خواهم احتمال شکل‌گیری چنین آینده‌ای را نادیده بگیرم، بلکه دوست دارم پیامدهای احتمالی آن را مدنظر قرار دهم. البته نقشه‌راهی برای به وجود آوردن این آینده نخواهم داد. من متخصص فناوری نیستم و به کریپتو هم ایمان واقعی ندارم، ولی خوب است که پیامدهای کریپتو برای آینده اینترنت را بررسی کنیم، چون هم می‌توانند بسیار مثبت باشند و هم بسیار منفی؛ شاید هم صرفاً به بهبودهایی ساده

کریپتو، کارهایی بسیار بزرگ و خنده‌دار انجام می‌دهند. در اکثر مقالات کریپتو با شخصیت‌هایی بی‌باک مواجه هستیم که شرط‌بندی‌ها و تراکنش‌های میلیارد دلاری انجام می‌دهند. البته در این مقاله این‌گونه نیست! هدف من توضیح دادن کریپتو است تا وقتی یکی از این شخصیت‌ها وارد دنیای کریپتو می‌شود، بتوانید هدف پشت فعالیت‌هایش را درک کنید.

۳. حاشیه: رمزنگاری در «کریپتو»

رمزنگاری علم مطالعه پیام‌های سری است؛ علم کدگذاری و کدگشایی. اکثر مطالب این مقاله ربطی به رمزنگاری ندارد، ولی مبانی کریپتو روی رمزنگاری استوار است؛ بنابراین خوب است که کمی در مورد این حوزه بدانیم.

ساده‌ترین توصیف رمزنگاری این است که ورودی‌ای (عدد، کلمه یا متن) را پس از اعمال یک تابع به عدد، کلمه یا متن دیگری تبدیل می‌کنیم. این تابع می‌تواند به سادگی جایگزین کردن حروف هر کلمه با حروف دیگری باشد (مشهور به شیفت سزار) یا پیچیدگی ریاضی بیشتری داشته باشد. یکی از ویژگی‌های تابع‌های رمزنگاری این است که یک‌طرفه^۴ عمل می‌کنند، یعنی با دانستن خروجی نمی‌توان ورودی را با قطعیت حدس زد. به عبارت دیگر، محاسبه خروجی از روی ورودی ساده است، ولی محاسبه ورودی با دانستن خروجی کار ساده‌ای نیست (ساده‌ترین مثال این ویژگی وقتی است که دو عدد اول بسیار بزرگ را در هم ضرب می‌کنیم. ضرب کردن این دو عدد ساده است، ولی نمی‌توان از روی حاصل ضرب به سادگی فهمید کدام دو عدد در هم ضرب شده‌اند). شیفت سزار به سادگی قابل حدس زدن است، ولی برخی روش‌های کدگذاری وجود دارند که به سادگی قابل معکوس کردن نیستند و به همین دلیل برای انتقال اطلاعات سری کاربرد دارند.

یکی از این روش‌ها «هش» نام دارد که هر ورودی‌ای را به عددی طولانی با تعداد رقم ثابت تبدیل می‌کند. یکی از محبوب‌ترین این تابع‌ها SHA-256 نام دارد که اختراع آژانس امنیت ملی آمریکاست.^۵ مثلاً می‌توان کل متن این مقاله را به تابع هش داد و عددی بسیار طولانی گرفت (معمولاً برای اینکه این اعداد طولانی کوتاه‌تر شوند، برای نمایش

آنها، به جای مبنای ۱۰ از مبنای ۱۶ استفاده می‌شود؛ به این معنی که علاوه بر رقم‌های ۰ تا ۹ از حروف f تا a هم برای نمایش این اعداد استفاده می‌شود). کسی که این عدد خروجی را داشته باشد، نمی‌تواند آن را به مقاله‌ای که من نوشته‌ام، تبدیل کند.

به این ترتیب می‌گوییم تابع هش یک‌طرفه است؛ دانستن هش هیچ اطلاعاتی در مورد مقاله به کسی نمی‌دهد؛ حتی اگر فرد بداند از چه تابعی استفاده شده است. تابع هش در عمل نوعی درهم‌سازی به حساب می‌آید؛ این تابع هر یک از حروف نوشته (معادل مجموعه صفر و یک) را دریافت می‌کند و آن قدر آنها را مخلوط می‌کند تا دیگر قابل تشخیص نباشند. تابع هش دستورات کاملاً مشخصی برای نحوه انجام این کار دارد، ولی معکوس این دستورات نتیجه‌ای نمی‌دهد.^۶ تابع هش مثل خامه‌ریختن داخل قهوه است، انجامش راحت است، ولی نمی‌توان آن را معکوس کرد.

الگوریتم SHA-256 به ازای هر ورودی یک خروجی ۶۴ بیتی ایجاد می‌کند. مثلاً هش کتاب ۷۳۰ صفحه‌ای رمان اولیس، خروجی زیر است:

```
3f120ea0d42bb6af2c3b858a08be9f737dd422f5e92c04f82cb9c40f06865d0e
```

همان‌طور که می‌بینید، طول این خروجی با طول هش عبارت «سلام. من مت هستم» یکسان است:

```
86d5e02e7e3d0a012df389f7273b1f0b1828e07eb757a2269fe73870bbd044
```

ولی اگر در عبارت بالا به جای نقطه از کاما استفاده کنم، خروجی کاملاً متفاوتی برای «سلام، من مت هستم» به دست خواهد آمد:

```
9f53386fc98a51b78135ff88d19f1ced2aa153846aa492851db84dc6946f558b
```

رابطه واضحی بین دو عدد به دست آمده وجود ندارد؛ با اینکه ورودی‌ها شباهت بسیار زیادی به هم دارند. این امر یکی از ویژگی‌های اصلی یک‌طرفه بودن است. به عبارت دیگر، اگر دو ورودی، شباهت بسیار یکسانی به هم داشته باشند، خروجی آنها نباید با هم شباهت داشته باشند، زیرا معکوس کردن تابع را ساده می‌کند؛ بنابراین هر ورودی به یک خروجی تصادفی می‌رسد.^۷

۴. یک‌طرفه بودن، جزئیات فنی بیشتری دارد که در این مقاله مطرح نمی‌کنم. آنچه در این مقاله تابع یک‌طرفه نامیده می‌شود، تابعی است که در واقع امیدواریم یک‌طرفه باشد، زیرا فناوری‌های کامپیوتری، ریاضی و رمزنگاری همیشه در حال تغییر و پیشرفت هستند.

۵. اگر می‌خواهید خودتان امتحان کنید، ماشین حساب‌های مختلفی برای SHA-256 آنلاین وجود دارد؛ یکی از آنها Xorbin.com است. اگر هم بخواهید خودتان برنامه این هش را بنویسید یا روی کاغذ امتحانش کنید، مقاله FIPS PUB 180-4 دولت ایالات متحده را بخوانید یا به ویکی‌پدیا مراجعه کنید.

۶. مثالی ساده: یکی از راه‌های ساده برای مخلوط کردن داده‌ها استفاده از تابع XOR است. خروجی این تابع زمانی که یکی از ورودی‌ها ۱ باشد، ۱ خواهد بود و در حالتی که هر دو ورودی ۰ یا ۱ باشند، ۰ خواهد بود. فرض کنید این تابع را روی دو عدد ۱۱۰۰ و ۰۱۰۱ به صورت بیت‌به‌بیت از چپ اعمال کنیم. خروجی ۱۰۰۱ خواهد بود. محاسبه خروجی با دانستن ورودی‌ها کار ساده‌ای است، ولی اگر ورودی‌ها را ندانیم، می‌توان از جفت‌های ۱۱۰۰ و ۰۱۰۱ یا ۰۰۱۱ و ۱۰۱۰ یا ۱۰۰۱ و ۰۰۰۰ نیز همین خروجی را به دست آورد. اگر نیمی از این مقاله را با نیمی دیگر از آن XOR کنید، مخلوطی به دست خواهید آورد که به سادگی قابل بازگرداندن به مقاله اولیه نیست. اگر همین کار را چند ده بار تکرار کنید، مقاله را رمزنگاری کرده‌اید.

۷. از آنجایی که طول خروجی تابع هش یک عدد مشخص است، این احتمال وجود دارد که دو ورودی متفاوت به خروجی یکسانی برسند. به این حالت، «تصادم» گفته می‌شود، ولی از آنجایی که یک عدد ۶۴ بیتی در مبنای ۱۶، حدود ۱۰ به توان ۷۷ دارد (که بیشتر از تعداد اتم‌های تشکیل دهنده کره زمین است)، احتمال چنین اتفاقی بسیار اندک است.

مسابقه در سال ۲۰۲۴ آن را باز کند. چنین راهکاری به اعتماد نیاز دارد، زیرا فرد پیش‌بینی‌کننده و مخاطبان آن پیش‌بینی همگی باید به نگه‌دارنده پاکت نامه اعتماد داشته باشند.

008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcbaf2e6abeb3a9d601

اما راه دیگری هم وجود دارد که نیازی به اعتماد ندارد؛ می‌توانید جمله مورد نظر را هش کنید و هش را توییت کنید:



Matt Levine
@matt_levine

Here is a SHA-256 hash of a prediction I am making:
64b70b0494580b278d71f1f551d482a3fb952a4b018b43090feb87b662d34847.

شاید فالوورهای شما از این کار گیج یا ناراحت شوند، ولی نمی‌توانند پیش‌بینی شما را کدگشایی کنند و اگر زمانی پیش‌بینی شما درست از آب دربیاید، می‌توانید توییت خود را ریتوییت کنید و جمله هش‌نشده را هم کنار آن قرار دهید. به این ترتیب، اگر کسی بخواهد می‌تواند هش جمله را حساب کرده و با هش اولیه مقایسه کند.



علاوه بر هش، یکی دیگر از تابع‌های یک‌طرفه، رمزنگاری کلید عمومی است. فرض کنید من دو عدد دارم که «کلید عمومی» و «کلید خصوصی» نامیده می‌شوند. این دو عدد طولانی هستند و به نظر می‌آید که تصادفی باشند، ولی با هم رابطه خاصی دارند؛ با استفاده از الگوریتم‌های عمومی می‌توان با کمک یکی از این اعداد پیامی را قفل کرد و با کمک عدد دیگر، قفل را باز کرد. این سیستم دوکلیدی یکی از مشکلات کلاسیک حوزه کدگذاری را برطرف می‌کند؛ بدین نحو که

شاید بپرسید پیام سری‌ای که قابل معکوس شدن نیست، چه کاربردی دارد؟ چنین پیامی قابلیت تأیید شدن دارد. اگر هش این مقاله را برای کسی بفرستم، او نمی‌تواند متن اصلی آن را به دست آورد.^۸ ولی اگر همان متن را داشته باشد، می‌تواند با استفاده از الگوریتم هش مشترک (مثلاً SHA-256) هشی را تولید کند که با هش من یکسان است؛ بنابراین نمی‌توان هش را کدگشایی کرد، ولی می‌توان تأیید کرد که طرف مقابل پیام را به‌درستی کدگذاری (هش) کرده است. شاید انجام چنین کاری برای یک مقاله مسخره باشد، ولی اصل قابل تأیید بودن، کاربردهای مختلفی دارد. یکی از کاربردهای روزمره آن رمز عبور در سیستم‌های کامپیوتری است. وقتی سیستمی از کاربر می‌خواهد که رمز عبورش را وارد کند، باید راهی برای تأیید درستی آن رمز وجود داشته باشد.

یک راه این است که رمز عبور کاربر را ذخیره کنیم و عبارت واردشده را با محتوای دیتابیس مقایسه کنیم، اما چنین کاری خطرناک است، زیرا اگر کسی بتواند به دیتابیس رمز عبورها دسترسی پیدا کند، رمز عبور همه کاربران را به دست خواهد آورد؛ بنابراین بهتر است هش رمز عبورها را ذخیره کنیم. کاربر هنگام ثبت‌نام رمز خود را وارد می‌کند (مثلاً password123) و سیستم هش شده آن را به صورت زیر ذخیره می‌کند:

008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcbaf2e6abed3a9d601

وقتی کاربر می‌خواهد وارد پروفایل خود شود، رمز واردشده دوباره هش می‌شود و با مقدار ذخیره شده مقایسه می‌شود. اگر دو هش یکسان بودند، کاربر رمز را درست وارد کرده و در غیر این صورت اجازه ورود به سیستم را نخواهد داشت. به این ترتیب، اگر کسی فهرست هش‌ها را سرقت کند، نمی‌تواند به رمز عبور کاربران دسترسی داشته باشد.^۹ کاربردهای دیگری نیز برای تابع هش وجود دارد؛ از جمله برچسب زمانی. فرض کنید اتفاقی را پیش‌بینی کرده‌اید که در زمان مشخصی رخ خواهد داد و می‌خواهید اعتبار این پیش‌بینی نصیب خودتان شود، ولی نمی‌خواهید پیش‌بینی خود را روی توییت‌های اعلام عمومی کنید تا اگر پیش‌بینی اشتباه بود، آبروریزی نشود یا روی نتیجه نهایی اثر نگذارد. فرض کنید پیش‌بینی این است که «تیم فوتبال جتس، مسابقه سوپر بول ۲۰۲۴ را برنده خواهد شد». می‌توانید همین عبارت را روی تکه کاغذی بنویسید، آن را در پاکتی بگذارید، پاکت را مهر و موم کنید و آن را در اختیار یکی از دوستان تان قرار دهید تا پس از برگزاری

۸. پرداختن به جزئیات هش از محدوده این مقاله فراتر می‌رود، ولی مفاهیم متعدد دیگری مثل «جدول رنگین کمانی» و «سالت» برای شکست دادن یا تقویت امنیت هش‌ها استفاده می‌شوند.

۹. تمرینی برای خواننده: در این مقاله هش چند عبارت را آورده‌ام و در مورد تابع هش هم صحبت کرده‌ام، ولی هش کل مقاله را ذکر نکرده‌ام. به نظر شما چرا؟ (باور کنید دلم می‌خواست این کار را انجام دهم.)



۴. بیت کوین چگونه کار می کند

ساده ترین توصیف بیت کوین به این صورت است: فهرستی عمومی از آدرس هایی وجود دارد که هر کدام با مجموعه ای از اعداد و حروف تصادفی مشخص می شوند و مقداری بیت کوین در هر کدام وجود دارد. مثلاً ممکن است حسابی با آدرس `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa` حاوی $68/6$ بیت کوین باشد. آدرس هر حساب در واقع کلید عمومی آن است.^{۱۱} اگر من صاحب آن بیت کوین ها باشم، به این معنی است که من کلید خصوصی متناظر با آن کلید عمومی را در اختیار دارم که عملاً رمز عبور آن حساب است. از آنجایی که من کلید خصوصی آن حساب را دارم، می توانم تراکنش ارسال بیت کوین را با کلید خصوصی خودم امضا کنم. گیرنده نیز می تواند با استفاده از آدرس های عمومی، امضای من را تأیید کند. با همین اطلاعات می توان تأیید کرد که من آن حساب را کنترل می کنم و بیت کوین ها متعلق به من است، ولی کسی نمی تواند کلید خصوصی من را در اختیار بگیرد.

در نتیجه می توان بدون اعتماد بین طرفین یا اعتماد به بانک واسطه، پول تبادل کرد. ساتوشی در وایت پیپر بیت کوین نوشته است: «سکه الکترونیکی (Electronic coin) را زنجیره ای از امضاهای دیجیتال تعریف می کنیم.» ترکیب آدرس عمومی و کلید خصوصی برای تعریف سکه کافی است. رمزارز را «رمزارز» صدا می زنیم، زیرا ارزی است که از رمزنگاری به دست آمده است.

اگر کلیدی برای کدگذاری استفاده می شود، با کلید کدگشایی یکسان باشد. همچنین یک طرف باید کلید را برای طرف دیگر ارسال کند و اگر کسی بتواند کلید را در مسیر سرقت کند، می تواند پیام های تبادل شده را بخواند.

با استفاده از رمزنگاری کلید عمومی دیگر نیازی به ارسال کلیدهای سری نیست. کلید عمومی را می توان به راحتی با همه به اشتراک گذاشت، ولی کلید خصوصی را نباید در اختیار کسی قرار داد. وقتی بخواهید پیامی سری ارسال کنید، آن را با استفاده از الگوریتم رمزگذاری و کلید عمومی به رمز تبدیل می کنید و برای گیرنده می فرستید.

گیرنده نیز الگوریتم رمزگشایی را با کلید خصوصی خودش اجرا می کند و پیام را رمزگشایی می کند. امکان رمزگذاری پیام با استفاده از کلید عمومی وجود دارد، ولی کسی نمی تواند با کمک کلید عمومی پیام را رمزگشایی کند. فقط گیرنده پیام می تواند این کار را با کمک کلید خصوصی خود انجام دهد (به این ترتیب تابع کلید عمومی از دید همه به جز صاحب کلید خصوصی یک طرفه به حساب می آید).

یک مفهوم مرتبط با این حوزه «امضای دیجیتال» است که آن هم کلید عمومی و خصوصی دارد. وقتی می خواهم پیامی برای کسی بفرستم و اثبات کنم آن را نوشته ام، پیام را با کمک کلید خصوصی خودم رمزگذاری می کنم و پیام اولیه را در کنار پیام رمز شده برای گیرنده ارسال می کنم. گیرنده هم آن پیام را با استفاده از کلید عمومی رمزگشایی می کند و نتیجه به دست آمده را با پیام اولیه مقایسه می کند. اگر این دو مقدار با هم یکسان باشند، اثبات می شود که من نویسنده آن پیام بوده ام.

نوعی سیستم بانکداری را تصور کنید که در آن همه افراد می توانند اطلاعات حساب های بانکی را ببینند. فهرستی عمومی از حساب ها وجود دارد و به ازای هر حساب، کلید عمومی و موجودی آن حساب مشخص است. من به دوستم می گویم: «حساب شماره ۰۰۱۲۳۴۵۶۷۸۹ متعلق به من است و ۲۵۰ دلار در آن دارم.» در ادامه پیامی را با کلید خصوصی خودم امضا می کنم و پیامی با مضمون «انتقال ۵۰ دلار» برای او می فرستم.

دوستم آن پیام را با کلید عمومی مرتبط با آن حساب رمزگشایی می کند و به این ترتیب مشخص می شود که من صاحب آن حساب هستم. این ایده اصلی بیت کوین است، ولی جزئیات پیچیده تری هم دارد.

۱۰. این اولین آدرسی است که بیت کوین دریافت کرده و گفته می شود متعلق به ساتوشی ناکاموتو است.

۱۱. این آدرس در واقع هش شده کلید عمومی است، ولی به گفته ویتالیک بوترین، خالق اتریوم؛ «در ادبیات رمزنگاری قابل قبول است که هش شده کلید عمومی را معادل کلید عمومی استفاده کنیم.» او در وایت پیپر خود در سال ۲۰۱۴ این موضوع را توضیح داده و اگر از نظر ویتالیک چنین کاربردی درست باشد، از نظر من هم درست است.

دفترکل بیت کوبین در واقع فقط فهرستی از آدرس ها و موجودی شان نیست، بلکه فهرستی از تمام تراکنش های انجام شده است.^{۱۳} تمام اعضای شبکه دفترکل را نگهداری و تمام تراکنش ها را ثبت می کنند.

ولی اکنون به جای اینکه بخواهیم

به بانک اعتماد کنیم، باید به

هزاران غریبه اعتماد کنیم.

شرایط به آن وخامتی هم که به نظر می‌رسد، نیست. صحت هر یک از تراکنش‌ها را می‌توان تأیید کرد؛ اگر تراکنشی با کلید خصوصی متناظر با حساب فرستنده رمزگذاری شود، همه اعضای شبکه می‌توانند درستی آن را تأیید کنند و اگر کلید خصوصی نادرستی استفاده شده باشد، تقلبی بودن تراکنش مشخص خواهد شد و کسی آن را به دفترکل اضافه نخواهد کرد. همه نودها از نرم‌افزارهای منبع‌باز برای تأیید تراکنش‌ها و مدیریت دفترکل استفاده می‌کنند و هر کس که بخواهد، می‌تواند صحت هر یک از تراکنش‌ها را بررسی کند؛ بنابراین نیازی به اعتماد بیش از حد نیست.

تا اینجاى مقاله گفته‌ام که همه اعضاى شبکه نسخه‌اى از دفترکل را نگهدارى مى‌کنند و شايد اين امر در اولين روزهاى زندگى بيت‌کوين درست بوده باشد، ولى ديگر اين گونه نيست. هزاران «نود کامل» در شبکه وجود دارد که تمام دفترکل بيت‌کوين را، با استفاده از نرم‌افزارهاى منبع باز و رسمى بيت‌کوين، دانلود و تأييد مى‌کنند، ولى ميليون‌ها

اگر با دقت نگاه کنید، می بینید که صرفاً پیامی بین دو طرف تبادل شده و نتیجه این تبادل را ارز نامیده ایم. سیستم مالی سنتی نیز تفاوت چندانی ندارد؛ چراکه بانک ها با یکدیگر طلا و اسکناس تبادل نمی کنند، بلکه دیتابیس هایی را نگه می دارند و تبادل ۱۰۰ دلار از یک بانک به بانک دیگر به معنی به روزرسانی این دیتابیس هاست.

[illegible]

● ساتوشی بیت‌کوین را به‌عنوان زنجیره‌ای از امضاها تعریف کرده است. مفهوم رمزارز مبتنی بر پیام‌هایی است که کاربران بین یکدیگر ردوبدل می‌کنند و شماره‌هایی را به یکدیگر اختصاص می‌دهند.

۱۲. در واقع دفترکل فهرستی از آدرس‌ها و موجودی حساب‌ها نیست. به این دلیل از این تشبیه استفاده می‌کنم که درک موضوع ساده‌تر شود، ولی دفترکل بیت‌کوین از دیدگاه فنی به این صورت نیست.

۱۳. بخشی در وایت پیپر بیت کوین وجود دارد با عنوان «باز پس‌گیری فضای دیسک» که راهکاری برای فشرده‌سازی اطلاعات مربوط به تراکنش‌های قدیمی با استفاده از درخت مرکل ارائه می‌دهد. صحبت از این موضوع فراتر از محدوده این مقاله است، ولی عبارت «درخت مرکل» یکی از عبارات رایج در دنیای کریپتو است و بد نیست از کار بردش آگاه باشید.

چه دستاوردی داشته ایم؟

برسد؟

این رویکرد استاندارد در دنیای کریپتو است. سیستم‌های کریپتو سعی می‌کنند با استفاده از انگیزه‌های اقتصادی افراد را به رفتار صادقانه تشویق کنند، به جای اینکه به آنها اعتماد کنند که کار درست را انجام می‌دهند.

توضیحاتی که دادم، بخش عمده‌ای از ماجرا را مشخص می‌کند، ولی یک نکته هنوز ناگفته مانده است. بیت‌کوین‌های موجود از کجا آمده‌اند؟ درکش ساده است که بگوییم همه اعضای شبکه دفترکلی حاوی تمام تراکنش‌های انجام‌شده دارند و می‌توان مبداء تمام تراکنش‌ها را شناسایی کرد، ولی مبداء اولین بیت‌کوین کجاست؟ دفترکل چگونه آغاز شده است؟

البته ترتیب تراکنش‌ها نیز اهمیت دارد. اگر یک بیت‌کوین در حساب من باشد و آن را برای دو نفر بفرستم، چه کسی صاحب آن بیت‌کوین است؟ شاید این مسئله ساده به نظر بیاید، ولی حل آن مشکل است، زیرا بیت‌کوین شبکه‌ای توزیع شده است و تضمینی وجود ندارد که همه نودها همزمان از رخ دادن تراکنش‌ها مطلع شوند و اگر همه نودها در مورد ترتیب تراکنش‌ها توافق نداشته باشند، اتفاق‌های ناگواری (دو بار خرج کردن پول) می‌تواند رخ دهد. ساتوشی می‌گوید: «تراکنش‌ها باید به صورت عمومی اعلام شوند و به سیستمی نیاز داریم که به اعضای شبکه اجازه دهد روی ترتیب واحدی از دریافت پیام‌ها توافق کنند.» این سیستم، بلاکچین نام دارد.

۵. بلاکچین

تک‌تک تراکنش‌های بیت‌کوین در کل شبکه اعلام می‌شوند. برخی از نودهای شبکه (که ماینر نامیده می‌شود) تراکنش‌های دریافتی را جمع‌آوری می‌کنند و آنها را به صورت گروه‌هایی به نام بلوک درمی‌آورند. پس از مدتی، نسخه‌ای از آن بلوک به صورت رسمی به فهرستی از بلوک‌ها تبدیل می‌شود که ترتیب رخ دادن تراکنش‌ها را

نمود هم وجود دارد که چنین کاری انجام نمی‌دهند و فقط مقداری بیت‌کوین دارند؛ با این اعتماد که آن نودهای کامل، سلامت شبکه را حفظ خواهند کرد. با این حال، مبنای اعتماد به این نودهای کامل با مبنای اعتماد به بانک‌ها کمی تفاوت دارد؛ این نودها می‌دانند که همه اعضای شبکه می‌توانند در هر لحظه که بخواهند، درست کار کردن آنها را تأیید کنند.

همچنین باید دقت داشت که همه اعضای شبکه از صداقت منفعت مالی به دست می‌آورند. اگر همه صادقانه عمل کنند، سیستم پرداختی‌ای به وجود می‌آید که می‌تواند ارزشمند باشد. در مقابل اگر افراد زیادی دروغ بگویند و تراکنش‌های تقلبی در دفترکل خود ثبت کنند، هیچ‌کس به بیت‌کوین اعتماد نخواهد کرد و ارزش آن از بین می‌رود؛ دزدیدن بیت‌کوین چه فایده‌ای دارد، اگر ارزش آن به صفر

استفاده از آن داشته باشند. کاربران بیت‌کوین از دیدگاه فلسفی بخشی از سیستمی هستند که می‌تواند تا حدی حس بهتری نسبت به استفاده از آن داشته باشند. این سیستم به گونه‌ای طراحی شده که به کاربران اجازه دهد تا به صورت عمومی تراکنش‌های خود را ثبت کنند و به این ترتیب به یک سیستم توزیع شده و غیرمتمرکز دست یابند.



منظور از «کوچک بودن» حدی است که نرم افزار بیت کوین تعیین می کند و این حد می تواند تغییر کند تا ماین کردن بلوک سخت تر یا ساده تر شود (هدف این است که ماین کردن هر بلوک به طور متوسط ۱۰ دقیقه زمان ببرد؛ هرچه تعداد ماینرها بیشتر شود و از کامپیوترهای سریع تری استفاده کنند، ماین کردن سخت تر می شود). در حال حاضر عدد خروجی باید با ۱۹ صفر شروع شود. یکی از نتیجه های موفق در ذیل آمده شده است:

این روال شبیه بازی ۲۰ سؤالی است و شرکت‌کنندگان باید مرتب عده‌هایی را حدس بزنند؛ بدون اینکه سرنخی داشته باشند و البته تعداد دفعات حدس زدن هم بسیار بیشتر از ۲۰ بار است. احتمال اینکه هر ترکیبی از فهرست تراکنش‌ها با یک نانس تصادفی به هشی

● ابن شریطہ کے راہ وجود میں آوری کہ نام «حملہ سیبیل» (Sybil)



می‌توانید بلوک‌های تمام‌شده را روی کاوشگر شبکه ببینید. مثلاً بلوک ۷۵۸۹۶۵ که در تاریخ ۲۷ سپتامبر ماین شده، فهرستی از ۲۴۶۶ تراکنش بین آدرس‌های مختلف است. مثلاً آدرسی که با `bci1qns` شروع شده، ۰/۰۰۵۲ بیت‌کوین برای آدرسی فرستاده که با `۱۶qZCV` شروع می‌شود و آدرس `۳۷vGGL` مقدار ۰/۰۱۲ بیت‌کوین را به دو آدرس `۱۴NfRDk` و `۳۷o1E۳` تقسیم کرده است.

بیت کوین منتشر می کند، سپس سایر اعضا صحت آن بلوک را بررسی می کنند (به این معنی که تمام تراکنش های داخل فهرست معتبر باشند، هش درست باشد، تعداد صفرها صحیح باشد و غیره). اگر بلوک تأیید شود، همه کار روی بلوک بعدی را شروع می کنند؛ هش بلوک قبلی، تراکنش هایی که از آن زمان وارد شبکه شده اند و نانس جدیدی را کنار هم قرار می دهند و سعی می کنند هش جدیدی پیدا کنند. هر بلوک بر پایه بلوک قبلی ساخته می شود.

۶. ماینینگ

این فعالیت ها هزینه بسیار زیادی دارند. ماینرها به سخت افزارهای ویژه ای نیاز دارند تا بتوانند هش های متعدد را به سرعت محاسبه کنند و این روزها مزارع کامپیوتری بزرگی ایجاد کرده اند که همیشه در حال فعالیت هستند. برق لازم برای استخراج بیت کوین به اندازه مصرف برق کشورهای متوسط است؛ بنابراین به محیط زیست آسیب می زند. شاید بهترین توصیفی که برای بیت کوین ارائه شده، عبارت زیر باشد که شخصی در توییتر منتشر کرده است:

**تصور کنید چه اتفاقی
می افتاد اگر باروشن
نگه داشتن خود رویتان
می توانستید
سود و کوهایی را حل
کنید که قابل تبادل با
هر وئین بودند!**

چنین شرایطی باعث هدررفت انرژی می شود. بعضی اوقات گفته

با ۱۹ صفر منجر شود، بسیار کم است (۱ در ۷۵ سکتیلیون)؛ بنابراین ماینرها الگوریتم هشینگ را تریلیون ها بار اجرا می کنند تا هشی پیدا کنند که با ۱۹ صفر شروع می شود.^{۱۶}

در حال حاضر هش ریت شبکه بیت کوین کمی بیشتر از ۲۰۰ میلیون تراشه در ثانیه است (هرچند عدد بزرگی به حساب می آید، اما بسیار کوچک تر از ۷۵ سکتیلیون است). در این شرایط، به طور متوسط حدود ۶۰۰ ثانیه طول می کشد تا بتوان نانس درست را حدس زد و یک بلوک را ماین کرد.



● جوینده طلا، حدود ۱۸۶۰

این شرایط نوعی مسابقه است. تنها یک ماینر می تواند یک بلوک را استخراج کند و آن ماینر برای پاداش بیت کوین می گیرد. ماین کردن هر بلوک به معنی ماین کردن بیت کوین جدید است که به فعالیت محاسباتی زیادی نیاز دارد؛ شبیه به پیدا کردن طلا پس از کندن دل کوه. ●

وقتی ماینر نانس مناسب را پیدا کند، بلوک و هش آن را روی شبکه

۱۶. نقل قول دیگری از ویتالیک: «از آنجایی که الگوریتم SHA-256 شبه تصادفی و کاملاً غیرقابل پیش بینی است، تنها راه برای ایجاد بلوک های معتبر سعی و خطاست، به این معنی که نانس را یک عدد افزایش دهیم و ببینیم هش جدید نتیجه مطلوب را می دهد یا خیر.»

می شود که ماینرها مجبور به حل مسائل پیچیده ریاضی هستند تا بتوانند بلوک های جدید را استخراج کنند، ولی این ادعا صحیح نیست. آنها صرفاً به روش «بروت فورس» در حال امتحان تک تک حالت های ممکن بین چندین عدد هستند تا بتوانند هش درست را به دست آورند. هیچ مسئله ریاضی ای حل نمی شود و هیچ چیزی به دانش بشر اضافه نمی شود.

البته ماینرها مسئله مهمی را برای بیت کوین حل می کنند؛ مسئله امن نگه داشتن شبکه و دفترکل تراکنش های آن. مشخص است که تأیید تراکنش های بیت کوین هزینه زیادی دارد؛ بنابراین تقلب در آن سخت است. در نتیجه حمله سیبیل کار سختی خواهد بود. به همین دلیل است که ساتوشی و دیگران به این روش تأیید بلوک ها، «اثبات کار» می گویند. اگر کسی هش درست را به دست آورد، ثابت می کند که فعالیت محاسباتی سنگینی انجام داده است.

اثبات کار مکانیسمی برای توافق بین افرادی است که برای مشارکت در سیستم هزینه اقتصادی پرداخت کرده اند، بدون اینکه کسی اطلاعات هویتی این افراد را بداند. کسی که بیت کوین استخراج می کند، نمی خواهد این رمزارز ارزش خود را از دست بدهد. ماینرها سرمایه گذاری زیادی برای بیت کوین کرده اند؛ از جمله اینکه کامپیوترهای گران قیمت خریده اند و هزینه زیادی برای برق می پردازند. آنها با این کار اثبات کرده اند که صحیح بودن دفترکل برایشان اهمیت دارد و در ازای کارهایشان بیت کوین دریافت می کنند که باعث می شود سهم بیشتری در سیستم داشته باشند.

این بیت کوین ها از هیچ به وجود می آیند؛ فعالیت استخراج و نرم افزار هسته بیت کوین آنها را به وجود می آورد. در واقع تمام بیت کوین ها از طریق استخراج به دست آمده اند. نه ساتوشی و نه اولین اعضای شبکه، هیچ بیت کوینی بدون استخراج دریافت نکرده اند.

پاداش استخراج هر بلوک در ابتدا ۵۰ بیت کوین بود و اکنون به ۶/۲۵ رسیده است. نکته ای که باید در نظر داشت اینکه این پاداش ها برای کاربران بیت کوین هزینه بر هستند. هر ۱۰ دقیقه یک بار ۶/۲۵ بیت کوین جدید خلق می شود و در ازای ایمن کردن شبکه به ماینرها داده می شود. این عدد معادل حدود شش میلیارد دلار در سال است.^{۱۷} این هزینه به صورت غیرمستقیم و مشابه نوعی تورم است؛ بنابراین اگر شرایط یکسان باشد، با اضافه شدن عرضه بیت کوین^{۱۸}، ارزش هر

بیت کوین کمی کاهش می یابد. در حال حاضر شبکه بیت کوین ۱/۵ درصد از ارزش خود را در هر سال به ماینرها منتقل می کند. این عدد از تورم دلار آمریکا کمتر است، ولی هنوز هم بی اهمیت نیست. هر سال ماینرهایی که امنیت شبکه را حفظ می کنند، بخشی کوچک، ولی معنادار از کل ارزش بیت کوین را به خود اختصاص می دهند. کاربران بیت کوین هم در ازای این انتقال ارزش، پاداش دریافت می کنند.^{۱۹}



اگر استخراج بیت کوین کسب و کار پردرآمدی باشد، افراد زیادی به دنبال آن خواهند رفت؛ در نتیجه یک نفر نمی تواند به راحتی اکثر قدرت استخراج را در اختیار داشته باشد. اگر یک نفر یا گروه اکثر قدرت استخراج را در اختیار داشته باشد، می تواند کارهای منفی انجام دهد؛ مثلاً تأیید بلوک های تقلبی، دو بار خرج کردن پول، معکوس کردن تراکنش های صحیح و غیره (به این شرایط حمله ۵۱ درصد گفته می شود). وقتی بتوان میلیاردها دلار از استخراج بیت کوین به دست آورد، افراد زیادی روی این کار سرمایه گذاری خواهند کرد، البته رقابت کردن هزینه زیادی دربر دارد. وقتی میلیاردها دلار جهت کسب قدرت استخراج سرمایه گذاری شود، برای سرمایه گذاران مهم خواهد بود که ارزش بیت کوین را حفظ کنند؛ بنابراین اقدام نادرستی در شبکه انجام نخواهند داد.

۱۷. اگر هر ۱۰ دقیقه ۶/۲۵ بیت کوین استخراج شود، ۳۷/۵ عدد در ساعت و ۹۰۰ عدد در روز استخراج خواهد شد که این عدد باید در ۳۶۵ و قیمت بیت کوین ضرب شود.

۱۸. اما نهایتاً فقط ۲۱ میلیون بیت کوین قابل استخراج است. این محدودیت بخشی از کد بیت کوین است و قابل افزایش نیست. وقتی تمام بیت کوین های ممکن استخراج شوند، ماینرها چه انگیزه ای برای امن نگه داشتن شبکه خواهند داشت؟ کارمزد تراکنش. کد بیت کوین به ماینرها اجازه می دهد علاوه بر استخراج، بخشی از مبلغ هر تراکنش را نیز به عنوان کارمزد خود بردارند و وقتی آخرین بیت کوین استخراج شود (حوالی سال ۲۱۴۰)، کارمزد تنها راه کسب پاداش در شبکه بیت کوین خواهد بود.

۱۹. ویتالیک بوتیرین در سال ۲۰۲۱ مطلبی در این رابطه نوشته که این گونه شروع می شود: «هزینه ای که اکوسیستم های بیت کوین و اتریوم برای امنیت می پردازند (هدف الگوریتم اثبات کار) بسیار بیشتر از تمام هزینه های آنها برای سایر بخش هاست. از ابتدای امسال، شبکه بیت کوین روزانه به طور متوسط ۳۸ میلیون دلار پاداش استخراج و پنج میلیون دلار کارمزد تراکنش پرداخت کرده است. بلاکچین اتریوم با ۱۹/۵ میلیون دلار پاداش استخراج در روز و ۱۸ میلیون دلار کارمزد تراکنش در روز، در رتبه دوم قرار دارد.»

II

چه معنایی دارد؟

۲۹

با کمی جزئیات سازوکار بیت کوین، ابداع ساتوشی ناکاموتورا توضیح دادم، اما اجازه دهید کمی به عقب برگردیم؛ چیزی که ساتوشی ابداع کرده، دقیقاً چیست؟

ساده ترین پاسخ این است که ابداع ساتوشی بیت کوین بود. ◀



پیت کوین پدپ



داده‌مهمی است