ماهنامه اختصاصی مدیران فناوری های مالی ایران
ASRETARAKONESH.IR
ضمیمه ماهنامه عصرتراکنش در زمینه بلاکچین، رمزارز و دارایی دیجیتال | ۱۰۰ صفحه

عصرتراکنش

ماهنامه عصرتراکنش با افتخار تقدیم می‌کند

داستانِ رمزارز

راهنمای اینکه رمزارزها ازکجا می‌آیند، چه معنایی دارند و چرا مهم هستند

Bloomberg Businessweek

با حمایت

excoino

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 ۰/۱ بیت‌کوین دارم، گاهی اوقات دچار ترس عقب‌ماندن از این جهان موازی می‌شوم که بیشتر از یک دهه به رشد خود ادامه داده است؛ جهانی که طرفداران افراطی آن با اطمینان تمام در موردش صحبت می‌کنند 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 مدت‌هاست 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 نویسنده فایننس این روزها، «مَت لِوین»، نویسنده بلومبرگ اوپینیون (Bloomberg Opinion)، خواسته‌ایم به ما بگوید این فناوری اغلب دیوانه‌کننده، اکثراً عجیب و همیشه جذاب چیست و در آینده به کجا خواهد رسید. -*«جوئل وبر» (Joel Weber)، سردبیر بلومبرگ بیزینس‌ویک*

هفته‌نامه «بلومبرگ بیزینس‌ویک» را طی چند سال گذشته به‌صورت مداوم دنبال کرده‌ایم؛ این رسانه با اینکه بر دنیای کسب‌وکارها تمرکز دارد، ولی به‌صورت پیوسته از دیدگاه مالی به موضوعات نگاه می‌کند. اگر جلدهای این ماهنامه و مطالبش در این چند سال را دنبال کرده باشید، می‌دانید که فناوری‌های مالی و به‌طور خاص رمزارزها و بیت‌کوین مورد توجه این رسانه بوده‌اند. با اینکه این رسانه تا حد خوبی تخصصی محسوب می‌شود، ولی محتواهایش به زبان ساده بیان می‌شوند. زمانی که دیدیم این رسانه یک شماره کامل را به رمزارزها اختصاص داده، تصمیم گرفتیم کل شماره را ترجمه و صفحه‌آرایی و به‌عنوان ضمیمه ماهنامه عصر تراکنش منتشر و در اختیار مدیران فناوری‌های مالی ایران قرار دهیم. در این سال‌ها در انتشارات راه پرداخت و دیگر رسانه‌های راه‌کار به‌صورت پیوسته درباره رمزارزها و بیت‌کوین و اتریوم نوشته‌ایم؛ تلاش کرده‌ایم بیشتر از اینکه دیگران را به ورطه تریدینگ 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 جذاب‌تر از سودهای آنی است و تصور می‌کنیم آنهایی که فلسفه و فناوری پشت رمزارزهایی مانند بیت‌کوین و اتریوم را درک کنند، از این فضا لذت می‌برند. حالا و با گسترش ابزارها و کسب‌وکارها، شاهد این هستیم که عرصه رمزارز گسترده‌تر شده و این روزها مفاهیمی مانند متاورس و ان‌اف‌تی و دیفای به‌کرات شنیده می‌شود. در این شماره ویژه عصر تراکنش که ترجمه کامل شماره ویژه «بلومبرگ بیزینس‌ویک» است، با زبانی ساده همه آنچه را باید درباره رمزارزها بدانید، به شما آموزش می‌دهیم. امیدواریم این کار مفید باشد. - *رضا قربانی، سردبیر ماهنامه عصر تراکنش*

کریپتو به زبان آدمیزاد؛ من اگر می‌خواستم برای این ویژه‌نامه بلومبرگ تیتری بزنم، همین تیتر را به زبان انگلیسی انتخاب می‌کردم. یک روزنامه‌نگار که آشنایی چندانی هم با جهان کریپتو ندارد، تصمیم به نوشتن مطالبی درباره چیستی، کارکرد و ابعاد کریپتو و این بازار می‌گیرد. در واقع او سعی می‌کند با روایت‌گونه‌کردن 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 به‌دلیل 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 گل‌آلودِ 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 همه‌چیز به ما نشان می‌دهد که با یک ماهیگیر فصلی طرف نیستیم و نویسنده هر قصد و نیتی داشته باشد، نخواسته بر موج جهلِ مردمِ هجوم‌آورده 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 برنمی‌آورند، بلکه فارغ از هیاهوها به کندوکاو می‌پردازند. - *علی ورامینی، مشاور سردبیر*

Bloomberg Businessweek
excoino
عصر تراکنش

داستانِ رمزارز

نوشته مت لوین
ترجمه علیرضا کاظمی‌نیا، محمد رهبان، ثریا حقی

عصر تراکنش: شماره ویژه بلاکچین، رمزارز و دارایی دیجیتال | صاحب امتیاز: موسسه شبکه عصر تراکنش | مدیرمسئول و مدیرعامل: مینا والی | سردبیر: رضا قربانی | مشاوران سردبیر: رسول قربانی و علی وامینی | دبیر تحریریه: مینا حاجی | تحریریه: نیلوفر نادری، نسیم بنایی، طهورا آدینه‌وند، غزل یگانگی، فاطمه اکبا | تحریریه ویژه‌نامه: علیرضا کاظمی‌نیا، محمد رهبان، ثریا حقی | مدیرهنری: روح‌اله گیتی‌نژاد | صفحه‌آرا: علیرضا کیوان، حمید ابراهیمی، محمد قربانی | ویراستار زبان: شایسته‌فر | عکس: نسیم اعتمادی | اشتراک: محمد عبدالپور | نشانی: تهران، جنت‌آباد جنوبی، بلوار الله غربی، کوچه حدیث، بن‌بست حدیث ۲، پلاک ۸ | تلفن تحریریه: ۴۴۴۳۴۹۶۶ | وب‌سایت: AsreTarakonesh.ir | ایمیل: mag@way2pay.ir | چاپ: واژه (۸۸۳۱۶۶۱۳) | صحافی: واژه | ناظر چاپ: قادر شهبازی

I

دفترکل، بیت‌کوین و بلاکچین

الف
زندگی در دیتابیس‌ها

دنیای مدرن
از دیتابیس‌های
بزرگ تشکیل


VAX 11/780
تا حد زیادی
ی سازمان‌های
ی 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[1].

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، وسایل‌تان آنجاست، همسایگان‌تان از اینکه ببینند که از خانه خارج می‌شوید، شگفت‌زده نمی‌شوند، ولی اگر ببینند غریبه‌ای وارد خانه شده، تعجب خواهند کرد. با این حال، رکورد ثبت‌شده 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. نگه‌داشتن پول به‌صورت رکوردهایی در دیتابیس بسیار راحت‌تر از نگه‌داشتن آن به‌صورت 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[2]. 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.

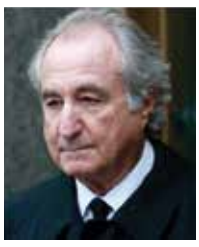
مالکیت پول هم تا حدی شبیه به همین موضوع است. کیسه طلا راهکار به‌نسبت ساده‌ای برای نشان‌دادن مالکیت پول است، ولی وزن زیادی دارد. در مقابل وقتی بانکداری وجود داشته باشد که از طلای افراد نگهداری می‌کند و رسیدی به آنها می‌دهد که می‌توانند آن را خرج کنند یا با مراجعه به بانک دیگری که مدیرش دوست مدیر بانک 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.

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 اطلاع‌داشتن 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 نگه‌دارندگان
دیتا بیس ها
اعتماد می‌کنیم

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 که اکثراً نادیده گرفته می‌شود.



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 هیچ‌وجه 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 حسابرسی‌شده ما نگاه کنید. ما تحت نظارت فدرال‌رزرو 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].

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 منبع‌باز و چنین مواردی وجود نداشت، افراد مجبور بودند هر روز میلیون‌ها ادعا را بدون دلیل و مدرک بپذیرند چون راه دیگری نداشتند.

۲. ترکیب‌پذیری

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 کوبول نوشته شده‌اند. هنوز افراد زیادی در آمریکا وجود دارند که با پست‌کردن 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 به‌صورت 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 به‌هرحال یک جعبه سیاه است.

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 به‌راحتی 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.

زندگی مدرن از اطلاعات درون دیتابیس‌های متعدد تشکیل شده است

اگر دیتابیس‌ها را به‌روز 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 به‌سادگی 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؟

چه می‌شد اگر فقط یک دیتابیس وجود داش


ت و همه در مدیریت آن مشارکت داشتند؟

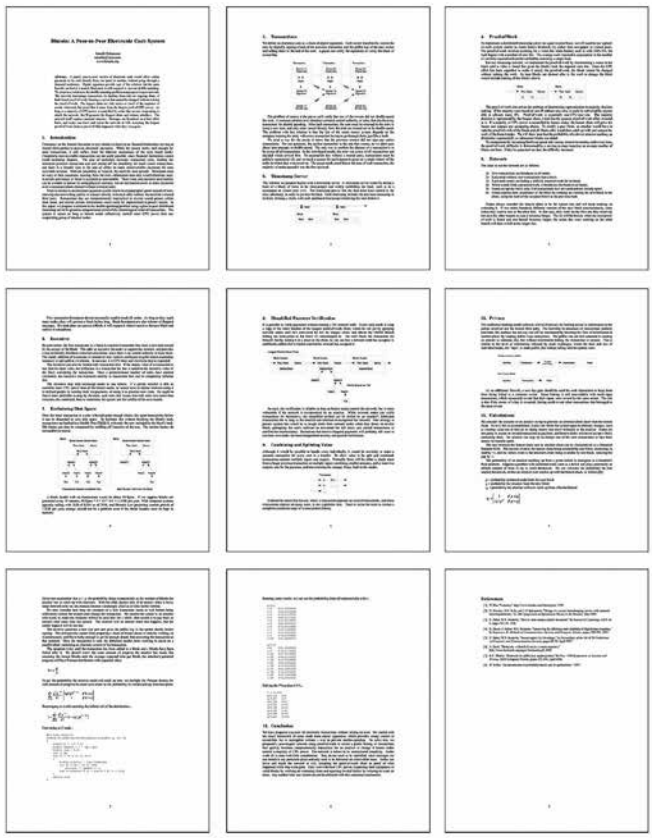
ج

پول نقد دیجیتال

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 همتابه‌همتا برای پول نقد الکترونیکی» (عنوان وایت‌پیپرش) 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.



وایت‌پیپر ساتوشی

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. همه‌چیز عجیب است و اغلب باید اطلاعات زیادی در مورد فعالیت‌های بازار و تاریخچه مالی داشت تا بتوان رفتار افراد را درک کرد.

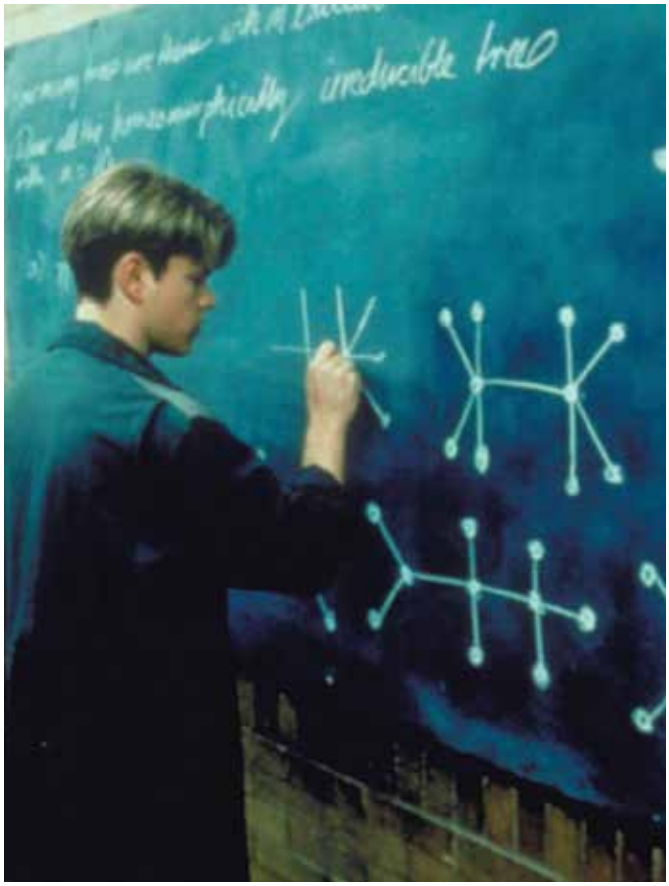
در چند سال گذشته، جنجالی‌ترین موضوع فایننس، «کریپتو» بوده است. کریپتو مجموعه‌ای از ایده‌ها، محصولات و فناوری‌هاست که از وایت‌پیپر بیت‌کوین نشئت گرفته‌اند، اما کریپتو به همان اندازه خطوطی است که طی این سال‌ها روی چارت‌های مالی شکل گرفته‌اند. زمانی که ساتوشی بیت‌کوین را اختراع کرد، هر بیت‌کوین صفر دلار 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، به‌سرعت ثروتمند شدند و توانستند خودروها و خانه‌های گران‌قیمت بخرند. آنها از عملکرد خود خشنود 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 این‌قدر 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 نه‌تنها 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

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 صحبت‌کردن 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 به‌دنبال بهبود یا متحول‌کردن 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.

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 کریپتو بی‌ارزش

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 آن‌قدرها 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 خریدوفروش 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، بازی‌کردن 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!

نمی‌خواهم 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 ارائه 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 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» بپردازیم 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 توزیع‌شده)

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 خواهم 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) به‌جز ساتوشی، تمام افراد مشهور دنیای

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 توضیح‌دادن 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 جایگزین‌کردن 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. ضرب‌کردن این دو عدد ساده است، ولی نمی‌توان از روی حاصل‌ضرب به‌سادگی فهمید کدام دو عدد در هم ضرب شده‌اند). شیفت سزار به‌سادگی قابل حدس‌زدن است، ولی برخی روش‌های کدگذاری وجود دارند که به‌سادگی قابل معکوس‌کردن 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 a تا f 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 آن‌قدر 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 ۶۴بیتی 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:

```
86d5e02e7e3d0a012df389f727373b1f0b1828e07eb757a2269fe73870bbd044
```

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 به‌دست‌آمده وجود ندارد؛ با اینکه ورودی‌ها شباهت بسیار زیادی به هم دارند. این امر یکی از ویژگی‌های اصلی یک‌طرفه‌بودن است. به عبارت دیگر، اگر دو ورودی، شباهت بسیار یکسانی به هم داشته باشند، خروجی آنها نباید با هم شباهت داشته باشند، زیرا معکوس‌کردن تابع را ساده می‌کند؛ بنابراین هر ورودی به یک خروجی تصادفی می‌رسد.[۷]

۴. یک‌طرفه‌بودن، 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، ماشین‌حساب‌های 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 ۱۰۱۰ به‌صورت 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 ۱۰۱۰ 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 به‌سادگی 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 ۶۴بیتی در مبنای ۱۶، حدود ۱۰ به توان ۷۷ دارد (که بیشتر از تعداد اتم‌های تشکیل‌دهنده کره زمین است)، احتمال چنین اتفاقی بسیار اندک است.

شاید بپرسید پیام سری‌ای که قابل معکوس‌شدن 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 هش‌شده آن را به‌صورت زیر ذخیره می‌کند:

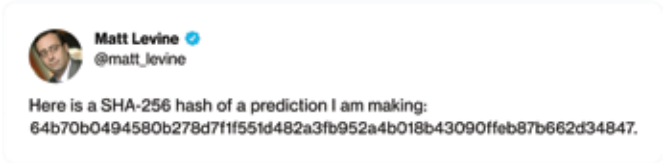
```
008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcba0f2e6abed3a9d601
```

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 توییتر اعلام عمومی کنید تا اگر پیش‌بینی اشتباه بود، آبروریزی نشود یا روی نتیجه نهایی اثر نگذارید. فرض کنید پیش‌بینی این است که «تیم فوتبال جتس، مسابقه سوپربول ۲۰۲۴ را برنده خواهد شد». می‌توانید همین عبارت را روی تکه‌کاغذی بنویسید، آن را در پاکتی بگذارید، پاکت را مهروموم کنید و آن را در اختیار یکی از دوستان‌تان قرار دهید تا پس از برگزاری 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.

```
008c70392e3abfbd0fa47bbc2ed96aa99bd49e159727fcba0f2e6abeb3a9d601
```

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



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

۸. پرداختن به جزئیات هش از محدوده این مقاله فراتر می‌رود، ولی مفاهیم متعدد دیگری مثل «جدول رنگین‌کمانی» و «سالت» برای شکست‌دادن 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.)

اگر کلیدی برای کدگذاری استفاده می‌شود، 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، می‌تواند پیام‌های تبادل‌شده را بخواند.

با استفاده از رمزنگاری کلید عمومی دیگر نیازی به ارسال کلیدهای سری نیست. کلید عمومی را می‌توان به‌راحتی 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 می‌کنید و برای گیرنده می‌فرستید.

گیرنده نیز الگوریتم رمزگشایی را با کلید خصوصی خودش اجرا می‌کند و پیام را رمزگشایی می‌کند. امکان رمزگذاری پیام با استفاده از کلید عمومی وجود دارد، ولی کسی نمی‌تواند با کمک کلید عمومی پیام را رمزگشایی کند. فقط گیرنده پیام می‌تواند این کار را با کمک کلید خصوصی خود انجام دهد (به این ترتیب تابع کلید عمومی از دید همه به‌جز صاحب کلید خصوصی یک‌طرفه به حساب می‌آید).

یک مفهوم مرتبط با این حوزه «امضای دیجیتال» است که آن هم کلید عمومی و خصوصی دارد. وقتی می‌خواهم پیامی برای کسی بفرستم و اثبات کنم آن را نوشته‌ام، پیام را با کمک کلید خصوصی خودم رمزگذاری می‌کنم و پیام اولیه را در کنار پیام رمزشده برای گیرنده ارسال می‌کنم. گیرنده هم آن پیام را با استفاده از کلید عمومی رمزگشایی می‌کند و نتیجه به‌دست‌آمده را با پیام اولیه مقایسه می‌کند. اگر این دو مقدار با هم یکسان باشند، اثبات می‌شود که من نویسنده آن پیام بوده‌ام.

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

دوستم آن پیام را با کلید عمومی مرتبط با آن حساب رمزگشایی می‌کند و به این ترتیب مشخص می‌شود که من صاحب آن حساب هستم.

این ایده اصلی بیت‌کوین است، ولی جزئیات پیچیده‌تری هم دارد.

۴. بیت‌کوین چگونه کار می‌کند

ساده‌ترین توصیف بیت‌کوین به این صورت است: فهرستی عمومی از آدرس‌هایی وجود دارد که هر کدام با مجموعه‌ای از اعداد و حروف تصادفی مشخص می‌شوند و مقداری بیت‌کوین در هر کدام وجود دارد. مثلاً ممکن است حسابی با آدرس 1A1zP1eP5QGefi2DMPTf TL5SLmv7DivfNa[10] حاوی ۶۸/۶ بیت‌کوین باشد. آدرس هر حساب در واقع کلید عمومی آن است.[11] اگر من صاحب آن بیت‌کوین‌ها 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، می‌توانم تراکنش ارسال بیت‌کوین را با کلید خصوصی خودم امضا کنم. گیرنده نیز می‌تواند با استفاده از آدرس‌های عمومی، امضای من را تأیید کند. با همین اطلاعات می‌توان تأیید کرد که من آن حساب را کنترل می‌کنم و بیت‌کوین‌ها متعلق به من است، ولی کسی نمی‌تواند کلید خصوصی من را در اختیار بگیرد. در نتیجه می‌توان بدون اعتماد بین طرفین یا اعتماد به بانک واسطه، پول تبادل کرد. ساتوشی در وایت‌پیپر بیت‌کوین نوشته است: «سکه الکترونیکی (Electronic coin) را زنجیره‌ای از امضاهای دیجیتال تعریف می‌کنیم.» ترکیب آدرس عمومی و کلید خصوصی برای تعریف سکه کافی است. رمزارز را «رمزارز» صدا می‌زنیم، زیرا ارزی است که از رمزنگاری به دست آمده است.

اگر با دقت نگاه کنید، می‌بینید که صرفاً پیامی بین دو طرف تبادل

۱۰. این اولین آدرسی است که بیت‌کوین دریافت کرده و گفته می‌شود متعلق به ساتوشی ناکاموتو است.

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

شـده و نتیجـه ایـن تبـادل را ارز نامیده‌ایـم. سیسـتم مالی سـنتی نیز تفاوت چندانی ندارد؛ چراکه بانک‌ها با یکدیگر طلا و اسـکناس تبادل نمی‌کنند، بلکه دیتابیس‌هایی را نگه می‌دارند و تبـادل ۱۰۰ دلار از یک بانک به بانک دیگر به معنی به‌روزرسانی این دیتابیس‌هاست.

بـه همیـن ترتیـب، در سیسـتم بیت‌کویـن هـم هـر تراکنشـی باعـث به‌روزرسـانی دیتابیـس (دفترکل) می‌شـود، ولـی چه کسـی متولی این دفترکل است؟ سـاده‌ترین پاسخ، کل شـبکه بیت‌کوین اسـت (هزاران نفری که از بیت‌کوین استفاده می‌کنند و نرم‌افزارش را در کامپیوترهای خود دارنـد). هـر یـک از ایـن اعضـا یـک نسـخه از دفتـرکل دارنـد؛ به عبارت دیگر هر نود (Node) در شـبکه فهرسـتی از تعداد حسـاب‌ها و بیت‌کوین‌های موجود در هر حسـاب دارد و همه نودها در به‌روزرسانی دفترکل همکاری می‌کنند.

تراکنش‌های بیت‌کویـن خصوصی نیسـتند، بلکه کل شـبکه از انجام آنها مطلع می‌شود تا نودها بتوانند فهرست‌های خود را به‌روز کنند. اگر امضای تراکنش انجام‌شده معتبر باشد، همه نودها دفترکل خود را به‌روز می‌کنند؛ به این ترتیب که مبلغ تراکنش از حساب فرستنده کسر و به حساب گیرنده اضافه می‌شود.[۱۲]

دفترکل بیت‌کویـن در واقع فقط فهرسـتی از آدرس‌ها و موجودی‌شـان نیسـت، بلکه فهرسـتی از تمام تراکنش‌های انجام‌شده اسـت.[۱۳] تمام اعضای شبکه دفترکل را نگهداری و تمام تراکنش‌ها را ثبت می‌کنند.

سیستم بیت‌کوین جالب اسـت، 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 نادرسـتی اسـتفاده شـده باشد، تقلبی‌بودن تراکنش مشخص خواهد شد و کسی آن را به دفترکل اضافه نخواهد کرد. همـه نودها از نرم‌افزارهای منبع‌باز بـرای تأیید تراکنش‌ها و مدیریت دفترکل اسـتفاده می‌کننـد و هر کس که بخواهـد، می‌تواند صحت هر یک از تراکنش‌ها را بررسـی کنـد؛ بنابراین نیـازی به اعتماد بیش از حد نیست.

تا اینجای مقاله گفته‌ام که همه اعضای شـبکه نسـخه‌ای از دفترکل را نگهداری می‌کنند و شـاید این امـر در اولین روزهای زندگـی بیت‌کوین درسـت بوده باشـد، ولی دیگر این‌گونه نیسـت. هزاران «نود کامل» در شبکه وجود دارد که تمام دفترکل بیت‌کوین را، با استفاده از نرم‌افزارهای منبع‌باز و رسـمی بیت‌کویـن، دانلـود و تأییـد می‌کنند، ولـی میلیون‌ها نـود هم وجـود دارد کـه چنیـن کاری انجـام نمی‌دهنـد و فقـط مقداری بیت‌کوین دارند؛ با این اعتماد که آن نودهای کامل، سـلامت شـبکه را حفظ خواهند کـرد. با این حال، مبنـای اعتماد به ایـن نودهای کامل با مبنای اعتماد به بانک‌ها کمی تفاوت دارد؛ این نودها می‌دانند که همه

ساتوشی بیت‌کوین را به‌عنوان زنجیره‌ای از امضاها تعریف کرده است. مفهوم رمزارز مبتنی بر پیام‌هایی اسـت که کاربـران بین یکدیگر ردوبـدل 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 وایت‌پیپر بیت‌کوین وجود دارد با عنوان «بازپس‌گیری 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 عبارت‌های پرکاربرد دنیای کریپتو است و بد نیست از کاربردش آگاه باشید.

چه دستاوردی داشته‌ایم؟

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 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 توزیع‌شده است و تضمینی وجود ندارد که همه نودها همزمان از رخ‌دادن تراکنش‌ها مطلع شوند و اگر همه نودها در مورد ترتیب تراکنش‌ها توافق نداشته باشند، اتفاق‌های ناگواری (دو بار خرج‌کردن پول) می‌تواند رخ دهد. ساتوشی می‌گوید: «تراکنش‌ها باید به‌صورت 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 به‌صورت گروه‌هایی به نام بلوک درمی‌آورند. پس از مدتی، نسخه‌ای از آن بلوک به‌صورت رسمی به فهرستی از بلوک‌ها تبدیل می‌شود که ترتیب رخ‌دادن تراکنش‌ها را نشان می‌دهد. به این ترتیب می‌گوییم بلوک مورد نظر «ماین» شده

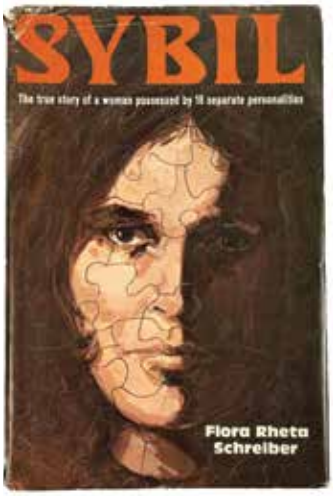
است.[۱۴] در بیت‌کوین، تقریباً ۱۰ دقیقه طول می‌کشد تا یک بلوک ماین شود.[۱۵]

ماینرها شروع به جمع‌آوری بلوک جدیدی می‌کنند که نهایتاً ماین و رسمی می‌شود. اینجاست که هشینگ اهمیت پیدا می‌کند. بلوک جدید به بلوکی که قبل از آن آمده، اشاره دارد و این کار را با استفاده از هشی انجام می‌دهد که صحیح و قابل پذیرش‌بودن بلوک قبلی و ترتیب بلوک‌ها را تأیید می‌کند. به این ترتیب، هر بلوک به بلوک قبلی خود اشاره دارد و بلاکچین به وجود می‌آید. بلاکچین رکوردی رسمی از تراکنش‌های مورد قبول شبکه و ترتیب آنها به وجود می‌آورد. هش‌ها نیز نوعی برچسب زمانی هستند که ترتیب تراکنش‌ها را نشان می‌دهند.

می‌توان سیستمی ساده برای انجام این کار متصور شد. هر ۱۰ دقیقه یک بار یکی از ماینرها فهرستی از تراکنش‌ها را ارائه می‌دهد و تمام کامپیوترهای روی شبکه بیت‌کوین در مورد آن فهرست رأی می‌دهند؛ اگر آن فهرست رأی اکثریت را به دست آورد، رسمی می‌شود و در بلاکچین ثبت خواهد شد.

متأسفانه چنین سیستمی بیش از حد ساده است، زیرا قانونی برای وارد شدن به شبکه بیت‌کوین وجود ندارد و هر کسی که کامپیوتری داشته باشد و نرم‌افزارهای منبع‌باز بیت‌کوین را نصب کند، می‌تواند بخشی از شبکه باشد. چنین شخصی نیازی ندارد که درستکار بودن خود را ثابت کند. حتی لازم نیست ثابت کند که انسان است. او اگر مایل باشد، می‌تواند هزاران کامپیوتر را به شبکه متصل کند.

این شرایط ریسکی را به وجود می‌آورد که با نام «حمله سیبیل» (Sybil) شناخته می‌شود؛ برگرفته از عنوان کتابی منتشرشده در سال ۱۹۷۳ که



شخصیت اصلی‌اش زنی بود که ادعا می‌کند چند شخصیت دارد. در سیستمی که گروهی از افراد، دفترکل را نگهداری می‌کنند و هر کسی می‌تواند بدون اجازه به این گروه اضافه شود، یک نفر می‌تواند هزاران نود را ایجاد و وانمود کند که هزاران نفر است. او در مرحله بعد می‌تواند تراکنش‌هایی نادرست ثبت کند و چون اکثریت شبکه را در اختیار دارد، سایر اعضا فریب می‌خورند. به این ترتیب آن شخص می‌تواند دارایی‌های دیگران را سرقت کرده یا حداقل شبکه را دچار هرج‌ومرج کند.

ماینرهای بیت‌کوین برای ماین‌کردن این رمزارز کاری عجیب و پرهزینه انجام می‌دهند که مبتنی بر هشینگ است. هر ماینر خلاصه‌ای از فهرست تراکنش‌های داخل بلوک به همراه هش بلوک قبلی را برمی‌دارد و عدد تصادفی (که نانس نامیده می‌شود) را به انتهای آن فهرست اضافه می‌کند. سپس نتیجه حاصله را به‌عنوان ورودی به الگوریتم SHA-256 می‌دهد که عددی ۶۴ بیت هگزا دسیمال را تولید می‌کند. اگر این عدد به اندازه کافی کوچک باشد، ماینر یک بلوک را ماین کرده، در غیر این صورت، ماینر دوباره با استفاده از یک نانس جدید تلاش می‌کند.

منظور از «کوچک‌بودن» حدی است که نرم‌افزار بیت‌کوین تعیین می‌کند و این حد می‌تواند تغییر کند تا ماین‌کردن بلوک سخت‌تر یا ساده‌تر شود (هدف این است که ماین‌کردن هر بلوک به‌طور متوسط ۱۰ دقیقه زمان ببرد؛ هرچه تعداد ماینرها بیشتر شود و از کامپیوترهای سریع‌تری استفاده کنند، ماین‌کردن سخت‌تر می‌شود). در حال حاضر عدد خروجی باید با ۱۹ صفر شروع شود. یکی از نتیجه‌های موفق در ذیل آمده شده است:

```
000000000000000000c9f1194ce7ff75c5f265d5520878e9e9392c3c8ff203
```

این روال شبیه بازی ۲۰سؤالی است و شرکت‌کنندگان باید مرتب عددهایی را حدس بزنند؛ بدون اینکه سرنخی داشته باشند و البته تعداد دفعات حدس‌زدن هم بسیار بیشتر از ۲۰ بار است. احتمال اینکه هر ترکیبی از فهرست تراکنش‌ها با یک نانس تصادفی به هشی با ۱۹ صفر منجر شود، بسیار کم است (۱ در ۷۵ سکتیلیون)؛ بنابراین

۱۴. در عمل یک بلوک زمانی رسمی می‌شود که پنج بار تأیید شده باشد؛ پس از ماین‌شدن، بعد از اینکه بلوک دیگری که ماین شده به آن اشاره کند، پس از اینکه بلوک بعدی ماین‌شده به بلوک قبلی اشاره کند و به همین ترتیب تا پنج بار این اتفاق رخ دهد و زنجیره‌ای از پنج بلوک شکل گیرد.

۱۵. می‌توانید بلوک‌های تمام‌شده را روی کاوشگر شبکه ببینید. مثلاً بلوک ۷۵۵۹۶۵ که در تاریخ ۲۷ سپتامبر ماین شده، فهرستی از ۲۴۶۶ تراکنش بین آدرس‌های مختلف است. مثلاً آدرسی که با bc1qns شروع شده، ۰/۰۰۵۲ بیت‌کوین برای آدرسی فرستاده که با ۱۶qZC۷ شروع می‌شود و آدرس ۳۹VgGL مقدار ۰/۰۱۲ بیت‌کوین را بین دو آدرس ۱۴NrDK و ۳۷o۱E۳ تقسیم کرده است.

عصر تراکنش؛ رسانه مدیران فناوری‌های مالی ایران

ماینرها الگوریتم هشینگ را تریلیون‌ها بار اجرا می‌کنند تا هشی پیدا کنند که با ۱۹ صفر شروع می‌شود.[۱۶]
در حال حاضر هش‌ریت شبکه بیت‌کوین کمی بیشتر از ۲۰۰ میلیون تراهش در ثانیه است (هرچند عدد بزرگی به حساب می‌آید، اما بسیار کوچک‌تر از ۷۵ سکتیلیون است). در این شرایط، به‌طور متوسط حدود ۶۰۰ ثانیه طول می‌کشد 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 می‌تواند یک بلوک را استخراج کند و آن ماینر برای پاداش بیت‌کوین می‌گیرد. ماین‌کردن هر بلوک به معنی ماین‌کردن بیت‌کوین 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 بیت‌کوین منتشر می‌کند، سپس سایر اعضا صحت آن بلوک را بررسی می‌کنند (به این معنی که تمام تراکنش‌های داخل فهرست معتبر باشند، هش درست باشد، تعداد صفرها صحیح باشد و غیره). اگر بلوک تأیید شود، همه کار روی بلوک بعدی را شروع می‌کنند؛ هش بلوک قبلی، تراکنش‌هایی که از آن زمان وارد شبکه شده‌اند و نانس جدیدی را کنار هم قرار می‌دهند و سعی می‌کنند هش جدیدی پیدا کنند. هر بلوک بر پایه بلوک قبلی ساخته می‌شود.

۶. ماینینگ

این فعالیت‌ها هزینه بسیار زیادی دارند. ماینرها به سخت‌افزارهای ویژه‌ای نیاز دارند تا بتوانند هش‌های متعدد را به‌سرعت محاسبه کنند و این روزها مزارع کامپیوتری بزرگی ایجاد کرده‌اند که همیشه در حال فعالیت هستند. برق لازم برای استخراج بیت‌کوین به اندازه مصرف برق کشورهای متوسط است؛ بنابراین به محیط زیست آسیب می‌زند. شاید بهترین توصیفی که برای بیت‌کوین ارائه شده، عبارت زیر باشد که شخصی در توییتر منتشر کرده است:

تصور کنید چه اتفاقی می‌افتاد اگر با روشن نگه‌داشتن خودرویتان می‌توانستید سودوکوهایی را حل کنید که قابل تبادل با هروئین بودند!

چنین شرایطی باعث هدررفت انرژی می‌شود. بعضی اوقات گفته می‌شود که ماینرها مجبور به حل مسائل پیچیده ریاضی هستند تا بتوانند بلوک‌های جدید را استخراج کنند، ولی این ادعا صحیح نیست. آنها صرفاً به روش «بروت فورس» در حال امتحان تک‌تک حالت‌های ممکن بین چندین عدد هستند تا بتوانند هش درست را به دست

۱۶. نقل قول دیگری از ویتالیک: «از آنجایی که الگوریتم SHA-256 شبه‌تصادفی و کاملاً غیرقابل پیش‌بینی است، تنها راه برای ایجاد بلوک‌های معتبر سعی‌وخطاست، به این معنی که نانس را یک عدد افزایش دهیم و ببینیم هش جدید نتیجه مطلوب را می‌دهد یا خیر.»

excoino

صرافی آنلاین اکسکوینو محیطی امن و راحت برای
خرید و فروش و معامله برترین رمزارزهای دیجیتال دنیا

- کمترین کارمزد
- پشتیبانی ۲۴ ساعته
- مدیریت کیف پول شخصی

آورند. هیچ مسئله ریاضی‌ای حل نمی‌شود و هیچ چیزی به دانش بشر اضافه نمی‌شود.

البته ماینرها مسئله مهمی را برای بیت‌کوین حل می‌کنند؛ مسئله امن نگه‌داشتن شبکه و دفترکل تراکنش‌های آن. مشخص است که تأیید تراکنش‌های بیت‌کوین 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 بلوک‌ها، «اثبات کار» می‌گویند. اگر کسی هش درست را به دست آورد، ثابت می‌کند که فعالیت محاسباتی سنگینی انجام داده است.

اثبات کار مکانیسمی برای توافق بین افرادی است که برای مشارکت در سیستم هزینه اقتصادی پرداخت کرده‌اند، بدون اینکه کسی اطلاعات هویتی این افراد را بداند. کسی که بیت‌کوین استخراج می‌کند، نمی‌خواهد این رمزارز ارزش خود را از دست بدهد. ماینرها سرمایه‌گذاری زیادی برای بیت‌کوین کرده‌اند؛ از جمله اینکه کامپیوترهای گران‌قیمت خریده‌اند و هزینه زیادی برای برق می‌پردازند. آنها با این کار اثبات کرده‌اند که صحیح‌بودن دفترکل برایشان اهمیت دارد و در ازای کارهایشان بیت‌کوین دریافت می‌کنند که باعث می‌شود سهم بیشتری در سیستم داشته باشند.

این بیت‌کوین‌ها از هیچ به وجود می‌آیند؛ فعالیت استخراج و نرم‌افزار هسته بیت‌کوین آنها را به وجود می‌آورد. در واقع تمام بیت‌کوین‌ها از طریق استخراج به دست آمده‌اند. نه ساتوشی و نه اولین اعضای شبکه، هیچ بیت‌کوینی بدون استخراج دریافت نکرده‌اند.

پاداش استخراج هر بلوک در ابتدا ۵۰ بیت‌کوین بود و اکنون به ۶/۲۵ رسیده است. نکته‌ای که باید در نظر داشت اینکه این پاداش‌ها برای کاربران بیت‌کوین هزینه‌بر هستند. هر ۱۰ دقیقه یک بار ۶/۲۵ بیت‌کوین جدید خلق می‌شود و در ازای ایمن‌کردن شبکه به ماینرها داده می‌شود. این عدد معادل حدود شش میلیارد دلار در سال است.[۱۷] این هزینه به‌صورت غیرمستقیم و مشابه نوعی تورم است؛ بنابراین اگر شرایط یکسان باشد، با اضافه‌شدن عرضه بیت‌کوین[۱۸]، ارزش هر بیت‌کوین کمی کاهش می‌یابد. در حال حاضر شبکه بیت‌کوین ۱/۵ درصد از ارزش خود را در هر سال به ماینرها منتقل می‌کند.

این عدد از تورم دلار آمریکا کمتر است، ولی هنوز هم بی‌اهمیت نیست. هر سال ماینرهایی که امنیت شبکه را حفظ می‌کنند، بخشی کوچک، ولی معنادار از کل ارزش بیت‌کوین را به خود اختصاص می‌دهند. کاربران بیت‌کوین هم در ازای این انتقال ارزش، پاداش دریافت می‌کنند.[۱۹]

امنیت و توزیع‌شدگی

اگر استخراج بیت‌کوین کسب‌وکار پردرآمدی باشد، افراد زیادی به‌دنبال آن خواهند رفت؛ در نتیجه یک نفر نمی‌تواند به‌راحتی اکثر قدرت استخراج را در اختیار داشته باشد. اگر یک نفر یا گروه اکثر قدرت استخراج را در اختیار داشته باشد، می‌تواند کارهای منفی انجام دهد؛ مثلاً تأیید بلوک‌های تقلبی، دو بار خرج‌کردن پول، معکوس‌کردن تراکنش‌های صحیح و غیره (به این شرایط حمله ۵۱ درصد گفته می‌شود). وقتی بتوان میلیاردها دلار از استخراج بیت‌کوین به دست آورد، افراد زیادی روی این کار سرمایه‌گذاری خواهند کرد، البته رقابت‌کردن هزینه زیادی دربر دارد. وقتی میلیاردها دلار جهت کسب قدرت استخراج سرمایه‌گذاری شود، برای سرمایه‌گذاران مهم خواهد بود که ارزش بیت‌کوین را حفظ کنند؛ بنابراین اقدام نادرستی در شبکه انجام نخواهند داد.

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

۱۸. اما نهایتاً فقط ۲۱ میلیون بیت‌کوین قابل استخراج است. این محدودیت بخشی از کد بیت‌کوین است و قابل افزایش نیست. وقتی تمام بیت‌کوین‌های ممکن استخراج شوند، ماینرها چه انگیزه‌ای برای امن نگه‌داشتن شبکه خواهند داشت؟ کارمزد تراکنش. کد بیت‌کوین به ماینرها اجازه می‌دهد علاوه بر استخراج، بخشی از مبلغ هر تراکنش را نیز به‌عنوان کارمزد خود بردارند و وقتی آخرین بیت‌کوین استخراج شود (حوالی سال ۲۱۴۰)، کارمزد تنها راه کسب پاداش در شبکه بیت‌کوین خواهد بود.

۱۹. ویتالیک بوترین در سال ۲۰۲۱ مطلبی در این رابطه نوشته که این‌گونه شروع می‌شود: «هزینه‌ای که اکوسیستم‌های بیت‌کوین و اتریوم برای امنیت می‌پردازند (هدف الگوریتم اثبات کار) بسیار بیشتر از تمام هزینه‌های آنها برای سایر بخش‌هاست. از ابتدای امسال، شبکه بیت‌کوین روزانه به‌طور 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.»

excoino

برای به روز بودن در دنیای کریپتو ما را دنبال کنید

یک گفتگوی کریپتویی
با حضور مهمان‌های جذاب

EXCONOMY

بررسی موضوعات مهم
اقتصاد کلان در ایران و جهان

اخبار روزانه دینای کریپتو

excoino

برنامه "آن ایر" اکسکوینو؛ بررسی به روز بازار رمزارزها
هر دوشنبه و چهارشنبه

- تحلیل ۳ رمزارز مهم بازار
- بررسی شاخص‌های تاثیرگذار آنچین
- تحلیل بازار در بخش فاندامنتال

II
چه معنایی دارد؟

با کمی جزئیات سازوکار بیت‌کوین، ابداع ساتوشی ناکاموتو را توضیح دادم، اما اجازه دهید کمی به عقب برگردیم؛ چیزی که ساتوشی ابداع کرده، دقیقاً چیست؟

ساده‌ترین پاسخ این است که ابداع ساتوشی بیت‌کوین بود. ◂