Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۴ از ۱۳

۲۰۰۸ و تولد بیت‌کوین

یک مقاله نُه‌صفحه‌ای، تیتر روزنامه‌ای که در نخستین بلاک پنهان شد، و خالقی که کنار رفت

۸ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۴ از ۱۳

۲۰۰۸ و تولد بیت‌کوین

در یک جمله

در سال ۲۰۰۸، نویسنده‌ای ناشناس با نام ساتوشی ناکاموتو قطعه‌های آزمایش‌های قبلی را کنار هم گذاشت و مشکلی را حل کرد که هیچ‌کدام از آن‌ها نتوانسته بودند: اینکه غریبه‌ها بدون هیچ مسئولی روی یک تاریخچه واحد توافق کنند.

نُه صفحه در میانه یک بحران

در سپتامبر ۲۰۰۸، بانک سرمایه‌گذاری لمن برادرز سقوط کرد و دولت‌ها در سراسر جهان با عجله و با پول عمومی به نجات بانک‌هایشان رفتند. اعتماد به نظام مالی به پایین‌ترین حد خود رسیده بود.

شش هفته بعد، در ۳۱ اکتبر ۲۰۰۸، پیامی در یک فهرست پستی که رمزنگاران آن را می‌خواندند منتشر شد. نویسنده‌اش که با نام **ساتوشی ناکاموتو** امضا کرده بود، از نوع تازه‌ای از پول الکترونیکی خبر داد که مستقیماً بین کاربران کار می‌کرد، بدون هیچ واسطه مورد اعتماد. پیوستِ پیام، لینک یک مقاله کوتاه بود: *Bitcoin: A Peer-to-Peer Electronic Cash System*. این مقاله فقط نُه صفحه داشت.

مقاله ریشه‌هایش را پنهان نمی‌کرد. به بی‌مانی، هش‌کش و پژوهش‌های مُهر زمانی که در درس ۳ با آن‌ها آشنا شدید ارجاع می‌داد. چیزی که اضافه کرد، راهی بود برای اینکه این قطعه‌ها بدون شرکت، بانک یا سرور مورد اعتماد در مرکز، با هم کار کنند. بسیاری از خوانندگان آن فهرست تردید داشتند. بعضی می‌گفتند هرگز نمی‌تواند به اندازه کافی پرداخت پردازش کند. بعضی هم اصلاً اعتنایی نکردند.

حل قطعه گمشده

درس ۳ با یک پرسش بی‌پاسخ تمام شد: اگر هزاران کامپیوتر مستقل هر کدام نسخه‌ای از سوابق را نگه دارند، وقتی هیچ‌کس مسئول نیست چطور بر سر اینکه کدام نسخه درست است توافق کنند؟ پاسخ بیت‌کوین سه بخش دارد.

اول، پرداخت‌ها در دسته‌هایی به نام **بلاک** جمع می‌شوند و هر بلاک به بلاک قبلی پیوند می‌خورد، درست مثل زنجیره مُهرهای زمانی در درس ۳. دوم، حق افزودن بلاک بعدی با **اثبات کار** به دست می‌آید، همان ایده‌ای که نخستین بار هش‌کش به کار برد. کامپیوترهایی به نام **ماینر** برای حل یک معما رقابت می‌کنند و بلاک برنده را همه بررسی می‌کنند و بعد روی آن ادامه می‌دهند. سوم، اگر روزی دو نسخه از تاریخچه با هم رقابت کنند، هر کامپیوتر از زنجیره‌ای پیروی می‌کند که بیشترین کار پشت آن است.

این قواعد در کنار هم تقلب را بسیار گران می‌کنند. برای بازنویسی پرداختی که دیگر در عمق زنجیره قرار گرفته، مهاجم باید کارِ آن بلاک و همه بلاک‌های بعد از آن را دوباره انجام دهد، آن هم سریع‌تر از مجموع بقیه شبکه. ماینر برنده

همچنین بیت‌کوین‌های تازه‌ساخته را به‌عنوان پاداش دریافت می‌کند، پس همان کاری که از سوابق محافظت می‌کند، پول را هم صادر می‌کند. برای هیچ‌کدام از این دو کار به شرکتی نیاز نیست.



شکل ۱. گاهی دو ماینر تقریباً هم‌زمان یک بلاک پیدا می‌کنند. شبکه روی زنجیره‌ای که بیشترین کار را دارد ادامه می‌دهد و بلاک رقیب کنار گذاشته می‌شود.

تشبیه: قرعه‌کشی گران

دفتری مشترک را تصور کنید که هر بار فقط یک نفر می‌تواند در آن بنویسد. برای اینکه مشخص شود چه کسی صفحه بعد را می‌نویسد، همه بلیت قرعه‌کشی می‌خرند و هر بلیت هزینه برق واقعی دارد. تقریباً هر ده دقیقه یک برنده انتخاب می‌شود. کسی که بخواهد صفحه‌های قدیمی را جعل کند، باید بارها و بارها برنده شود، یعنی بیشتر از مجموع همه بلیت بخرد. نویسندگان درستکار همچنان برنده می‌شوند، چون تعدادشان خیلی بیشتر است.

۳ ژانویه ۲۰۰۹: نخستین بلاک

در ۳ ژانویه ۲۰۰۹، ساتوشی نخستین بلاک زنجیره بیت‌کوین را ساخت که با نام **بلاک پیدایش** (genesis block) شناخته می‌شود. پاداش آن ۵۰ بیت‌کوین بود و به دلیل یک ویژگی خاص در کد، این سکه‌ها هرگز قابل خرج کردن نیستند. شش روز بعد، نرم‌افزار برای دانلود و اجرا در اختیار همه قرار گرفت.

در ۱۲ ژانویه ۲۰۰۹، ساتوشی ۱۰ بیت‌کوین برای هال فینی فرستاد، همان رمزنگاری که RPOW را در درس ۳ ساخته بود. این نخستین پرداخت از یک نفر به نفر دیگر در شبکه بود. تا ماه‌ها پس از آن، کاربران گروه کوچکی از علاقه‌مندان بودند که برنامه را روی کامپیوترهای خانگی‌شان اجرا می‌کردند.

پیامی در نخستین بلاک

ساتوشی یک خط متن در بلاک پیدایش نوشت: *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* («وزیر دارایی در آستانه دومین نجات مالی بانک‌ها»). این تیتر صفحه اول آن روزنامه بریتانیایی در همان روز بود. درست مثل اثر انگشت‌های چاپ‌شده در روزنامه در درس ۳، ثابت می‌کند که این بلاک نمی‌توانسته پیش از آن تاریخ ساخته شده باشد. بسیاری آن را اشاره‌ای به دلیل ساخته شدن بیت‌کوین هم می‌دانند.

قواعدی که از روز اول نوشته شد

برخلاف دیجی‌کش یا ای‌گلد، بیت‌کوین صادرکننده‌ای ندارد که تصمیم بگیرد چقدر پول ساخته شود. عرضه از قواعدی پیروی می‌کند که از ابتدا در نرم‌افزار گنجانده شده‌اند:

- **تقریباً هر ۱۰ دقیقه یک بلاک جدید.** هر ۲۰۱۶ بلاک، یعنی حدوداً هر دو هفته، معما به‌طور خودکار سخت‌تر یا آسان‌تر می‌شود تا این سرعت حفظ شود، چه ماینرها دستگاه اضافه کنند و چه کم کنند.
- **پاداشی که کوچک‌تر می‌شود.** پاداش هر بلاک از ۵۰ بیت‌کوین شروع شد و هر ۲۱۰٬۰۰۰ بلاک، تقریباً هر چهار سال، نصف می‌شود. این رویداد **هاوینگ** (halving) نام دارد. پس از هاوینگ آوریل ۲۰۲۴، پاداش ۳٫۱۲۵ بیت‌کوین است.
- **یک سقف ثابت.** چون پاداش مدام نصف می‌شود، کل عرضه هرگز از ۲۱ میلیون بیت‌کوین فراتر نمی‌رود. انتظار می‌رود آخرین کسرها حدود سال ۲۱۴۰ استخراج شوند.

تغییر این قواعد کاری نیست که یک نفر بتواند به تنهایی انجام دهد. هر کامپیوتر در شبکه هر بلاک را با قواعدی که اجرا می‌کند می‌سنجد، پس بلاکی که آن‌ها را زیر پا بگذارد به‌سادگی رد می‌شود. درس ۷ این کامپیوترها را دقیق‌تر بررسی می‌کند.

از سرگرمی تا نخستین قیمت

در بیشتر سال ۲۰۰۹، بیت‌کوین هیچ قیمتی نداشت. در اکتبر ۲۰۰۹، کاربری با نام مستعار New Liberty Standard نخستین نرخ تبدیل به دلار را منتشر کرد: ۱۳۰۹٫۰۳ بیت‌کوین در برابر یک دلار آمریکا. او این عدد را با محاسبه برقی که کامپیوترش برای استخراج سکه مصرف می‌کرد به دست آورد.

در ۲۲ مه ۲۰۱۰، برنامه‌نویسی در فلوریدا به نام لازلو هانیچ ۱۰٬۰۰۰ بیت‌کوین برای دو پیتزا پرداخت، یکی از نخستین خریدهای کالای واقعی با این پول. در طول سال ۲۰۱۰ نخستین صرافی‌ها پدید آمدند و بیت‌کوین قیمتی بازاری پیدا کرد که هر روز تغییر می‌کرد. یک بازار معاملاتی متولد شده بود.

خالقی که کنار رفت

ساتوشی هرگز نام واقعی، چهره یا محل زندگی‌اش را فاش نکرد و فقط از طریق پست‌های انجمن و ایمیل ارتباط داشت. در طول سال ۲۰۱۰، ساتوشی کم‌کم کنترل کد را به توسعه‌دهندگان داوطلب دیگر سپرد. آخرین پیام تأییدشده، ایمیلی به تاریخ ۲۳ آوریل ۲۰۱۱، می‌گفت ساتوشی «سراغ کارهای دیگری رفته است». هویت پشت این نام هنوز ناشناخته است.

پژوهشگرانی که نخستین بلاک‌ها را بررسی کرده‌اند تخمین می‌زنند یک ماینر واحد، که بسیاری او را همان ساتوشی می‌دانند، در سال اول حدود ۱٫۱ میلیون بیت‌کوین جمع کرده است. شواهد غیرمستقیم است و این سکه‌ها هرگز جابه‌جا نشده‌اند.

این ناپدید شدن اهمیت زیادی پیدا کرد. دیجی‌کش و ای‌گلد هر کدام یک بنیان‌گذار و یک شرکت داشتند که می‌توانستند ورشکست شوند، متهم شوند یا زیر فشار قرار بگیرند. بیت‌کوین هیچ‌کدام را ندارد. نه دفتر مرکزی‌ای هست که تعطیل شود و نه رهبری که همه مجبور به پیروی از تصمیم‌هایش باشند.

ضعف قبلی	پاسخ بیت‌کوین
پول دیجیتال قابل کپی بود	هر پرداخت با یک تاریخچه مشترک واحد سنجیده می‌شود
یک شرکت تعیین می‌کرد چقدر پول وجود داشته باشد	سکه‌های جدید فقط از قواعد ثابت در نرم‌افزار به وجود می‌آیند
یک سرور مورد اعتماد جلوی خرج دوباره را می‌گرفت	هزاران کامپیوتر مستقل هر بلاک را بررسی می‌کنند
راهی برای توافق بدون رهبر نبود	اثبات کار تعیین می‌کند چه کسی بلاک بعدی را اضافه کند و زنجیره با بیشترین کار برنده است
بنیان‌گذاری که می‌شد متهمش کرد یا تحت فشارش گذاشت	خالقی ناشناس که کنار رفت

چرا این برای تریدرها مهم است

- **بحران بخشی از داستان است.** بیت‌کوین در میانه یک بحران بانکی راه‌اندازی شد، با تیتری درباره نجات بانک‌ها در نخستین بلاکش. این داستان هر بار که بانک‌ها تحت فشار قرار می‌گیرند دوباره زنده می‌شود. در مارس ۲۰۲۳، وقتی چند بانک آمریکایی ورشکست شدند، بیت‌کوین به‌شدت بالا رفت چون برخی سرمایه‌گذاران دنبال دارایی‌هایی بیرون از نظام بانکی بودند. چنین روایت‌هایی می‌توانند قیمت را حرکت دهند، حتی اگر دوام نیاورند.
- **برنامه عرضه علنی است.** تاریخ هر هاوینگ را می‌توان سال‌ها از قبل تخمین زد و بسیاری از تریدرها چرخه‌ای تقریباً چهارساله را حول آن‌ها دنبال می‌کنند. یادتان باشد که یک رویداد شناخته‌شده ممکن است از قبل در قیمت لحاظ شده باشد و چرخه‌های گذشته تضمینی برای چرخه بعدی نیستند.
- **سکه‌های قدیمی زیر ذره‌بین هستند.** سکه‌های سال‌های نخست هر بار که جابه‌جا می‌شوند خبرساز می‌شوند. در سپتامبر ۲۰۲۶، ۶۰۰ بیت‌کوین استخراج‌شده در سال ۲۰۱۰ پس از ۱۶ سال جابه‌جا شد و تحلیلگران خیلی زود دریافتند که پیوند روشنی با ساتوشی ندارد. بررسی شواهد درون‌زنجیره‌ای پیش از واکنش به یک تیتر می‌تواند شما را از معامله بر اساس شایعه نجات دهد.

اصطلاحات کلیدی

وایت‌پیپر	سندی کوتاه که توضیح می‌دهد یک سیستم یا پروژه جدید قرار است چطور کار کند. وایت‌پیپر بیت‌کوین نُه صفحه بود.
بلاک پیدایش	نخستین بلاک یک بلاک‌چین. بلاک پیدایش بیت‌کوین در ۳ ژانویه ۲۰۰۹ ساخته شد.
ماینر	کامپیوتر یا گرداننده آن که با انجام اثبات کار برای افزودن بلاک بعدی رقابت می‌کند و در ازای آن پاداش می‌گیرد.
پاداش بلاک	بیت‌کوین‌های تازه‌ای که ماینر برنده برای افزودن یک بلاک دریافت می‌کند. همه بیت‌کوین‌های جدید این‌گونه ساخته می‌شوند.
هاوینگ	نصف شدن پاداش بلاک در هر ۲۱۰,۰۰۰ بلاک، تقریباً هر چهار سال.
زنجیره با بیشترین کار	قاعده‌ای که می‌گوید وقتی نسخه‌های تاریخچه رقابت می‌کنند، شبکه از نسخه‌ای پیروی می‌کند که بیشترین اثبات کار پشت آن است.

نکات کلیدی

1. ساتوشی ناکاموتو وایت‌پیپر نُه‌صفحه‌ای بیت‌کوین را در ۳۱ اکتبر ۲۰۰۸، در میانه یک بحران بانکی، منتشر کرد.

2. بیت‌کوین بلاک‌های به هم زنجیرشده، اثبات کار و قاعده بیشترین کار را ترکیب کرد تا غریبه‌ها بدون هیچ مسئولی روی یک تاریخچه توافق کنند.
3. بلاک پیدایش ۳ ژانویه ۲۰۰۹ تیتر روزنامه‌ای درباره نجات بانک‌ها را در خود دارد که تاریخ ساخته شدنش را ثابت می‌کند.
4. بیت‌کوین‌های جدید فقط از پاداش بلاک‌ها به وجود می‌آیند که تقریباً هر چهار سال نصف می‌شوند، و کل آن‌ها هرگز از ۲۱ میلیون فراتر نمی‌رود.
5. ساتوشی در سال ۲۰۱۱ بدون فاش کردن هویتش کنار رفت و هیچ بنیان‌گذار یا شرکتی باقی نماند که بتوان تعطیلش کرد.

خودتان را محک بزنید

برای هر سؤال دور یک گزینه را خط بکشید. کلید پاسخ‌ها همراه با توضیح در صفحه بعد آمده است. این آزمون را می‌توانید به‌صورت آنلاین هم در markettalks.info انجام دهید و نتیجه را فوراً ببینید.

۱. وایت‌پیپر بیت‌کوین چه زمانی منتشر شد؟

A ژانویه ۲۰۰۹
B ۳۱ اکتبر ۲۰۰۸
C مه ۲۰۱۰
D آوریل ۲۰۱۱

۲. اگر دو نسخه از بلاک‌چین با هم رقابت کنند، شبکه از کدام پیروی می‌کند؟

A نسخه‌ای که قدیمی‌ترین کامپیوتر ساخته
B نسخه‌ای که با رأی صرافی‌ها انتخاب شده
C نسخه‌ای که بیشترین اثبات کار پشت آن است
D نسخه‌ای که بیشترین پرداخت را دارد

۳. تیتر روزنامه در بلاک پیدایش چه چیزی را ثابت می‌کند؟

A اینکه بلاک نمی‌توانسته پیش از ۳ ژانویه ۲۰۰۹ ساخته شده باشد
B اینکه یک بانک بیت‌کوین را تأیید کرده
C اینکه ساتوشی در بریتانیا زندگی می‌کرد
D اینکه نخستین بیت‌کوین‌ها پشتوانه پوند داشتند

۴. بیت‌کوین‌های جدید چطور ساخته می‌شوند؟

A یک بانک مرکزی هر وقت لازم باشد چاپشان می‌کند

B ساتوشی هر سال آن‌ها را آزاد می‌کند

C صرافی‌ها وقتی تقاضا بالا می‌رود آن‌ها را می‌سازند

D ماینرها آن‌ها را به‌عنوان پاداش افزودن بلاک دریافت می‌کنند

۵. در هاوینگ چه اتفاقی می‌افتد؟

A قیمت بیت‌کوین نصف می‌شود

B پاداش افزودن یک بلاک نصف می‌شود

C نیمی از همه بیت‌کوین‌ها از بین می‌رود

D بلاک‌ها دو برابر سریع‌تر اضافه می‌شوند

۶. چرا ناپدید شدن ساتوشی به بیت‌کوین کمک کرد؟

A استخراج بیت‌کوین را ارزان‌تر کرد

B همه قواعد را از سیستم حذف کرد

C هیچ بنیان‌گذار یا شرکتی باقی نگذاشت که بشود تعطیلش کرد یا تحت فشارش گذاشت

D به ساتوشی اجازه داد سکه‌ها را مخفیانه بفروشد

کلید پاسخ‌ها

۱ **B**

۳۱ اکتبر ۲۰۰۸

ساتوشی مقاله نُه‌صفحه‌ای را در ۳۱ اکتبر ۲۰۰۸ در یک فهرست پستی رمزنگاری منتشر کرد، حدود شش هفته پس از سقوط لمن برادرز.

۲ **C**

نسخه‌ای که بیشترین اثبات کار پشت آن است

هر کامپیوتر از زنجیره‌ای پیروی می‌کند که بیشترین کار پشت آن است. برای جایگزین کردن آن، مهاجم به قدرت محاسباتی بیشتر از مجموع بقیه شبکه نیاز دارد.

۳ **A**

اینکه بلاک نمی‌توانسته پیش از ۳ ژانویه ۲۰۰۹ ساخته شده باشد

این تیتر در ۳ ژانویه ۲۰۰۹ چاپ شد، پس بلاک نمی‌تواند قدیمی‌تر از آن باشد. اینکه ساتوشی چه کسی بود و کجا زندگی می‌کرد هنوز ناشناخته است.

۴ **D**

ماینرها آن‌ها را به‌عنوان پاداش افزودن بلاک دریافت می‌کنند

پاداش بلاک تنها راهی است که بیت‌کوین جدید به وجود می‌آید. این پاداش از قواعد ثابت نرم‌افزار پیروی می‌کند، پس هیچ‌کس نمی‌تواند تصمیم بگیرد بیشتر صادر کند.

۵ **B**

پاداش افزودن یک بلاک نصف می‌شود

هر ۲۱۰,۰۰۰ بلاک، تقریباً هر چهار سال، پاداش بلاک نصف می‌شود. به همین دلیل کل عرضه هرگز از ۲۱ میلیون فراتر نمی‌رود.

۶ **C**

هیچ بنیان‌گذار یا شرکتی باقی نگذاشت که بشود تعطیلش کرد یا تحت فشارش گذاشت

دیجی‌کش و ای‌گلد همراه شرکت‌هایشان از بین رفتند. بدون رهبری شناخته‌شده، بیت‌کوین نه دفتر مرکزی‌ای دارد که تعطیل شود و نه یک نفر که همه مجبور به پیروی از تصمیم‌هایش باشند.

منابع

- ساتوشی ناکاموتو، (۲۰۰۸) Bitcoin: A Peer-to-Peer Electronic Cash System :https://bitcoin.org/bitcoin.pdf
- فهرست پستی رمزنگاری، Bitcoin P2P e-cash paper (۳۱ اکتبر ۲۰۰۸): https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
- Cointelegraph، ده‌سالگی بیت‌کوین در سالگرد بلاک پیدایش: https://cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block
- Bitcoin Magazine، رشد ۶٫۵ میلیارد درصدی بیت‌کوین از نخستین قیمت دلاری: https://bitcoinmagazine.com/culture/bitcoin-is-up-6-5-billion-percent-since-it-was-first-priced-in-usd
- The Defiant، آخرین ایمیل ساتوشی ناکاموتو به مایک هرن (۲۳ آوریل ۲۰۱۱): https://thedefiant.io/news/people/bitcoin-creator-satoshi-nakamoto-sent-final-email-to-mike-hearn-on-april-23-2011-6735013c

- Cointelegraph، آیا ساتوشی واقعاً ۱ میلیون بیت‌کوین دارد؟: https://cointelegraph.com/news/big-questions-does-satoshi-actually-own-1-million-bitcoin

Market Talks

ادامه یادگیری

درس بعدی: درس ۵
بلاک‌چین واقعاً چیست

این درس بخشی از دوره رایگان بلاک‌چین در مرکز آموزش MARKET TALKS است: درس‌هایی در سطح مبتدی، متوسط و پیشرفته که هر کدام یک آزمون و یک فایل PDF قابل دانلود دارند.

مرکز آموزش
درس‌هایی از اصول پایه تا موضوعات پیشرفته

تحلیل بازارها
تحلیل تکنیکال و بنیادی بازارهای اصلی

گزارش‌ها
بیت‌کوین، طلا، نقره، SPX و بیشتر

markettalks.info

تلگرام @MARKET_TALKS

فقط برای آموزش. هیچ‌یک از مطالب این سند توصیه مالی نیست. © ۲۰۲۶ MARKET TALKS. می‌توانید این PDF را بدون تغییر به اشتراک بگذارید.