Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۳ از ۱۳

پیش از بیت‌کوین: آزمایش‌های پول دیجیتال

بیست‌وپنج سال تلاش، شکست و چیزی نمانده به موفقیت، و قطعه‌ای که هر کدام برای بیت‌کوین به جا گذاشت

۸ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۳ از ۱۳

پیش از بیت‌کوین: آزمایش‌های پول دیجیتال

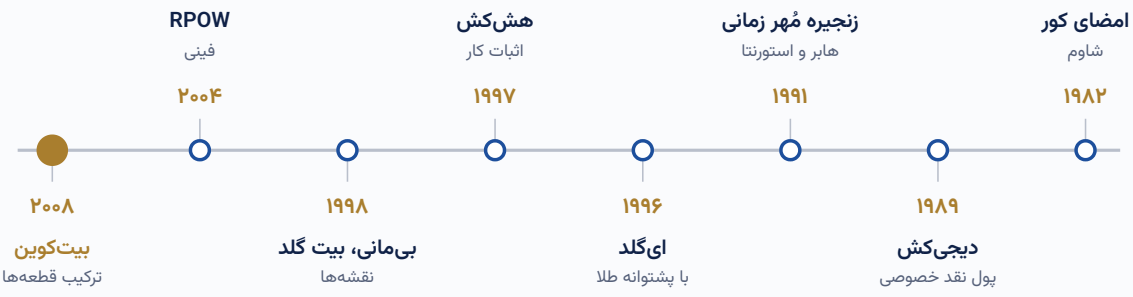
در یک جمله

بیت‌کوین از هیچ به وجود نیامد. ایده‌های پروژه‌های قدیمی‌تر پول دیجیتال را با هم ترکیب کرد و طوری طراحی شد که از همان یک ضعفی که بیشتر آن‌ها را از پا درآورد دوری کند.

رؤیایی قدیمی‌تر از مرورگر وب

در درس‌های ۱ و ۲ با دو مشکل آشنا شدیم: پول دیجیتال را می‌توان کپی کرد، و سیستمی که یک طرف آن را اداره می‌کند می‌تواند مسدود، تعطیل یا فاسد شود. مدت‌ها پیش از بیت‌کوین، رمزنگاران و کارآفرینان در تلاش بودند هر دو را حل کنند.

پروژه‌های آن‌ها از اوایل دهه ۱۹۸۰ تا میانه دهه ۲۰۰۰ ادامه داشت. بعضی به کسب‌وکارهای واقعی با مشتریان واقعی تبدیل شدند. بعضی هرگز از روی کاغذ فراتر نرفتند. هیچ‌کدام به‌طور کامل موفق نشدند، اما تقریباً هر کدام چیزی اضافه کردند که بعدها بیت‌کوین از آن استفاده کرد. دنبال کردن داستان آن‌ها بهترین راه برای فهمیدن این است که چرا بیت‌کوین این‌گونه ساخته شده است.



شکل ۱. بیش از ۲۵ سال آزمایش پول دیجیتال پیش از بیت‌کوین انجام شد. هر کدام قطعه‌ای از طرح نهایی را به جا گذاشت.

دیجی‌کش: خصوصی، اما در دست یک شرکت

در سال ۱۹۸۲، رمزنگاری به نام دیوید شاوم روشی به نام **امضای کور** را شرح داد. این روش به بانک اجازه می‌دهد یک سکه دیجیتال را امضا کند و معتبر بودنش را تأیید کند، بدون اینکه ببیند کدام سکه را امضا می‌کند. نتیجه، پول دیجیتالی است که می‌شود آن را مثل پول نقد به‌صورت خصوصی خرج کرد، چون بانک نمی‌تواند یک پرداخت را به کسی که سکه را برداشت کرده ربط دهد.

شاوم در سال ۱۹۸۹ شرکت دیجی‌کش (DigiCash) را تأسیس کرد تا این ایده را به محصول تبدیل کند، و در سال ۱۹۹۵ بانک مارک تواین در سنت‌لوئیس ارائه eCash آن را به مشتریانش آغاز کرد. فناوری کار می‌کرد. کسب‌وکار نه: بانک‌ها و فروشگاه‌های خیلی کمی به آن پیوستند و دیجی‌کش در سال ۱۹۹۸ اعلام ورشکستگی کرد.

ضعف عمیق‌تر در ساختار آن بود. هر سکه همچنان باید توسط یک بانک یا شرکت مرکزی صادر می‌شد، و همان طرف مرکزی خرج دوباره را بررسی می‌کرد. وقتی شرکت شکست خورد، پول هم همراه آن از بین رفت.

ای‌گلد: پشتوانه واقعی، یک نقطه شکست

ای‌گلد (e-gold) که در سال ۱۹۹۶ راه‌اندازی شد، مسیر دیگری را انتخاب کرد. هر واحد آن با طلای فیزیکی نگهداری‌شده در خزانه‌ها پشتیبانی می‌شد، و کاربران می‌توانستند موجودی‌های طلاپشتوانه را در چند ثانیه به هر جای دنیا برای هم بفرستند. سریع رشد کرد: تا سال ۲۰۰۶ سالانه بیش از ۲ میلیارد دلار پرداخت را پردازش می‌کرد.

اما ای‌گلد یک شرکت بود، و همین آن را به یک هدف تبدیل می‌کرد. نبود احراز هویت آن را برای مجرمان جذاب کرده بود، و در سال ۲۰۰۷ مقامات آمریکا شرکت و مدیرانش را متهم کردند. در سال ۲۰۰۸ آن‌ها به تبانی برای پولشویی و اداره کسب‌وکار انتقال پول بدون مجوز اعتراف کردند، و در سال ۲۰۰۹ انتقال‌ها متوقف شد. صاحبان حساب‌ها سال‌ها منتظر روندی برای پس گرفتن دارایی‌هایشان ماندند.

درس ۲ در دنیای واقعی اتفاق افتاد: یک نقطه کنترل، یک نقطه شکست هم هست، چه دلیلش یک هکر باشد، چه ورشکستگی و چه حکم دادگاه.

هش‌کش: گران کردن عمدی

در سال ۱۹۹۷، رمزنگاری به نام آدام بک **هش‌کش** (Hashcash) را برای مقابله با ایمیل‌های اسپم پیشنهاد کرد. پیش از ارسال یک پیام، کامپیوتر فرستنده باید یک معمای کوچک را حل می‌کرد که لحظه‌ای کار محاسباتی می‌برد. برای یک ایمیل، این هزینه دیده نمی‌شود. برای اسپمری که میلیون‌ها پیام می‌فرستد، به‌سرعت سنگین می‌شود.

نکته هوشمندانه، عدم تقارن آن است: حل کردن معما کند است اما بررسی آن آنی است. هر کسی که ایمیل را دریافت می‌کند می‌تواند بدون تکرار کار، مطمئن شود که کار انجام شده است. این ایده **اثبات کار** (proof of work) نام دارد، و وایت‌پیپر بیت‌کوین از هش‌کش به‌عنوان یک الهام مستقیم نام می‌برد.

تشبیه: آزمون سودوکو

حل یک سودوکوی سخت ممکن است یک ساعت طول بکشد، اما بررسی یک جدول کامل‌شده یک دقیقه وقت می‌گیرد. اگر کسی یک جدول حل‌شده به شما بدهد، می‌دانید که زحمتش را کشیده، حتی اگر هرگز ندیده باشید که چطور آن را حل کرده است. اثبات کار این ایده را به یک مُهر دیجیتال تلاش تبدیل می‌کند که هر کامپیوتری می‌تواند آن را تأیید کند.

بی‌مانی، بیت گلد و RPOW: نقشه‌ها

در سال ۱۹۹۸، دو طرح روی کاغذ به‌طرز شگفت‌آوری به بیت‌کوین نزدیک شدند. مهندس کامپیوتر وی دای طرح **بی‌مانی** (b-money) را شرح داد که در آن هر شرکت‌کننده نسخه‌ای از اینکه چه کسی مالک چه چیزی است نگه می‌دارد، و پول جدید با حل مسائل محاسباتی ساخته می‌شود. تقریباً در همان زمان، حقوق‌دان و دانشمند کامپیوتر نیک سابو **بیت گلد** (Bit Gold) را پیشنهاد کرد که راه‌حل‌های اثبات کار را همراه با مُهر زمانی به هم زنجیر می‌کرد تا چیزی کمیاب و پرهزینه برای تولید بسازد، نوعی طلای دیجیتال.

هیچ‌کدام هرگز راه‌اندازی نشدند. هر دو یک پرسش مهم را بی‌پاسخ گذاشتند: اگر افراد مستقل زیادی سوابق را نگه دارند، بدون اینکه کسی رئیس باشد چطور بر سر اینکه کدام سابقه درست است توافق کنند؟

در سال ۲۰۰۴، رمزنگاری به نام هال فینی **RPOW** (اثبات‌های کار قابل استفاده مجدد) را ساخت که اجازه می‌داد توکن‌های اثبات کار از فردی به فرد دیگر منتقل شوند. این سیستم واقعاً کار کرد، اما برای جلوگیری از خرج دوباره به یک سرور مورد اعتماد روی سخت‌افزار امن ویژه متکی بود. هنوز یک طرف مورد اعتماد در مرکز قرار داشت. پنج سال بعد، فینی نخستین بیت‌کوینی را دریافت کرد که از یک نفر برای نفر دیگر فرستاده شد.

زنجیره مُهرهای زمانی

یک قطعه دیگر از بیرون دنیای پول آمد. در سال ۱۹۹۱، پژوهشگرانی به نام‌های استوارت هابر و دبلیو. اسکات استورنتا به این پرداختند که چطور می‌شود ثابت کرد یک سند دیجیتال چه زمانی ساخته شده و از آن موقع تغییر نکرده است.

پاسخ آن‌ها این بود که سوابق را در یک زنجیره به هم وصل کنند. هر سابقه جدید اثر انگشت دیجیتال سابقه قبلی را با خود دارد، پس تغییر هر سابقه قدیمی همه حلقه‌های بعدی را می‌شکند. تاریخچه **دست‌کاری‌آشکار** می‌شود: هنوز می‌توانید برای بازنویسی آن تلاش کنید، اما همه می‌بینند که این کار را کرده‌اید. وایت‌پیپر بیت‌کوین سه بار به کار آن‌ها ارجاع می‌دهد، و ایده پیوند دادن سوابق به این شکل همان «زنجیره» (chain) در کلمه بلاک‌چین شد. درس ۶ دقیقاً توضیح می‌دهد که این اثر انگشت‌ها چطور کار می‌کنند.

> **یک نمونه واقعی**
>
> برای اینکه زنجیره‌شان را نتوان بی‌سروصدا بازنویسی کرد، شرکت هابر و استورنتا از سال ۱۹۹۵ اثر انگشت جدیدترین سوابقش را در آگهی‌های طبقه‌بندی‌شده روزنامه نیویورک تایمز منتشر می‌کرد. هر کسی می‌توانست روزنامه چاپی را با زنجیره مقایسه کند، و هیچ‌کس نمی‌توانست هزاران نسخه چاپ‌شده را بعداً تغییر دهد.

قطعه گمشده

تا میانه دهه ۲۰۰۰، تقریباً همه قطعه‌ها وجود داشتند. چیزی که هنوز کم بود، سخت‌ترین قطعه بود:

پروژه	چه چیزی اضافه کرد	چه چیزی هنوز کم بود
دیجی‌کش (۱۹۸۹)	پرداخت‌های دیجیتال خصوصی	وابسته به یک صادرکننده مرکزی
زنجیره مُهر زمانی (۱۹۹۱)	سوابق به هم پیوسته تا تاریخچه بی‌سروصدا تغییر نکند	برای پول طراحی نشده بود
ای‌گلد (۱۹۹۶)	انتقال‌های جهانی در مقیاس بزرگ	یک شرکت که می‌شد تعطیلش کرد
هش‌کش (۱۹۹۷)	اثبات کار: ساختنش پرهزینه، بررسی‌اش ارزان	پول نبود، فقط یک مُهر بود
بی‌مانی، بیت گلد (۱۹۹۸)	سوابق مشترک و پولی که با کار ساخته می‌شود	راهی برای توافق بدون رهبر نداشتند؛ هرگز راه‌اندازی نشدند
RPOW (۲۰۰۴)	توکن‌های اثبات کار که می‌شد دست‌به‌دست کرد	متکی به یک سرور مورد اعتماد

هر تلاشی یا به کسی وابسته بود که حرف آخر را بزند، یا هرگز حل نکرد که چطور غریبه‌ها بدون چنین کسی روی یک تاریخچه توافق کنند. در سال ۲۰۰۸، نویسنده‌ای ناشناس قطعه‌ها را کنار هم گذاشت و قطعه گمشده را اضافه کرد. این داستان درس ۴ است.

چرا این برای تریدرها مهم است

- **صادرکنندگان مرکزی به شیوه‌های آشنا شکست می‌خورند.** دیجی‌کش ورشکست شد و ای‌گلد را دادستان‌ها تعطیل کردند. همین الگو در سال ۲۰۱۳ تکرار شد، وقتی مقامات آمریکا لیبرتی رزرو (Liberty Reserve)، یک ارز دیجیتال متمرکز دیگر، را تعطیل کردند. هر دارایی که به یک صادرکننده وابسته است، ریسک تجاری و حقوقی همان صادرکننده را با خود دارد.
- **استیبل‌کوین‌های امروز یادآور ای‌گلد هستند.** یک استیبل‌کوین با پشتوانه دلار از مدلی مشابه پیروی می‌کند: یک شرکت ذخایر را نگه می‌دارد و در برابر آن توکن صادر می‌کند. به همین دلیل، پیش از تکیه بر یک استیبل‌کوین بهتر است ذخایر، مجوزها و وضعیت حقوقی صادرکننده‌اش را بشناسید.
- **روایت «طلای دیجیتال» ریشه‌های عمیقی دارد.** ایده بیت گلد درباره چیزی که چون ساختنش پرهزینه است کمیاب است، هنوز بر نحوه مقایسه بیت‌کوین با طلا از سوی بسیاری از سرمایه‌گذاران اثر می‌گذارد. دانستن اینکه یک روایت از کجا آمده کمک می‌کند قضاوت کنید وقتی بازار را حرکت می‌دهد، چقدر باید به آن وزن داد.

اصطلاحات کلیدی

امضای کور	روشی که با آن بانک یا صادرکننده یک سکه دیجیتال را تأیید می‌کند بدون اینکه ببیند کدام سکه است، تا پرداخت‌ها خصوصی بمانند.
اثبات کار	شاهدی بر اینکه یک کامپیوتر برای حل یک معما تلاش واقعی صرف کرده است. تولیدش کند است، بررسی‌اش آنی.
دارای پشتوانه	پول یا توکنی که ارزشش با یک دارایی واقعی، مثل طلا یا دلار، در اختیار صادرکننده پشتیبانی می‌شود.
مُهر زمانی	اثبات اینکه یک سابقه دیجیتال چه زمانی ساخته شده و از آن موقع تغییر نکرده است.
دست‌کاری‌آشکار	طوری ساخته شده که هر تغییری در سوابق گذشته برای همه آشکار باشد، حتی اگر نشود جلوی آن را به‌طور فیزیکی گرفت.
کمیابی دیجیتال	عرضه محدود چیزی دیجیتال که نمی‌توان آن را به‌سادگی کپی کرد یا رایگان ساخت.

نکات کلیدی

1. آزمایش‌های پول دیجیتال از اوایل دهه ۱۹۸۰ آغاز شد، بیش از ۲۵ سال پیش از بیت‌کوین.
2. دیجی‌کش حریم خصوصی و ای‌گلد مقیاس جهانی را آورد، اما هر دو به یک شرکت وابسته بودند و همراه آن از بین رفتند.
3. هش‌کش اثبات کار را معرفی کرد: تلاشی که تولیدش کند است اما تأییدش آنی.
4. بی‌مانی، بیت گلد و RPOW طرح سوابق مشترک و پول مبتنی بر کار را کشیدند، اما هیچ‌کدام حل نکردند که غریبه‌ها چطور بدون یک طرف مورد اعتماد توافق کنند.
5. مُهرهای زمانی به هم پیوسته نشان دادند چطور می‌شود تاریخچه را دست‌کاری‌آشکار کرد. بیت‌کوین این قطعه‌ها را ترکیب کرد و قطعه گمشده را اضافه 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. نوآوری کلیدی دیجی‌کش چه بود؟

A طلای نگهداری‌شده در خزانه
B امضاهای کور که پرداخت‌های دیجیتال را خصوصی می‌کرد
C اثبات کار برای جلوگیری از اسپم
D دفترکلی که هر کاربر یک نسخه از آن را دارد

۲. چرا ای‌گلد به پایان رسید؟

A اقدام قانونی علیه تنها شرکتی که آن را اداره می‌کرد
B ذخایر طلایش دزدیده شد
C یک باگ اجازه می‌داد کاربران سکه‌ها را کپی کنند
D کاربرانش به بیت‌کوین کوچ کردند

۳. هش‌کش در اصل برای چه کاری طراحی شده بود؟

A خصوصی کردن پرداخت‌های آنلاین
B نگهداری موجودی‌های طلاپشتوانه
C پرهزینه کردن ارسال ایمیل اسپم
D مُهر زمانی زدن بر اسناد حقوقی

۴. کدام ویژگی اثبات کار را مفید می‌کند؟

A هر کسی می‌تواند آن را فوراً تولید کند
B فقط یک سرور مرکزی می‌تواند آن را بررسی کند
C کپی کردنش آسان است
D تولیدش کند است اما تأییدش آنی

۵. کار هابر و استورنتا در سال ۱۹۹۱ چه چیزی اضافه کرد؟

A پول دیجیتال با پشتوانه طلا
B پیوند دادن سوابق در یک زنجیره تا تغییر تاریخچه آشکار شود
C ایمیل ناشناس
D نخستین صرافی رمزارز

۶. پیش از ۲۰۰۸، کدام قطعه هنوز کم بود؟

A اینترنت سریع‌تر

B راهی برای خصوصی کردن پرداخت‌ها

C راهی برای اینکه غریبه‌ها بدون هیچ مسئولی روی یک تاریخچه مشترک توافق کنند

D کامپیوترهایی به اندازه کافی قدرتمند برای اثبات کار

کلید پاسخ‌ها

۱ — B

امضاهای کور که پرداخت‌های دیجیتال را خصوصی می‌کرد

امضاهای کور دیوید شاوم به بانک اجازه می‌داد سکه‌ای را تأیید کند بدون اینکه ببیند کدام سکه است، پس پرداخت‌ها می‌توانستند مثل پول نقد خصوصی بمانند.

۲ — A

اقدام قانونی علیه تنها شرکتی که آن را اداره می‌کرد

ای‌گلد را یک شرکت اداره می‌کرد. پس از اتهام دادستان‌ها، شرکت و مدیرانش در سال ۲۰۰۸ اعتراف کردند و در سال ۲۰۰۹ انتقال‌ها متوقف شد. یک شرکت یعنی یک نقطه شکست.

۳ — C

پرهزینه کردن ارسال ایمیل اسپم

آدام بک هش‌کش را برای مبارزه با اسپم پیشنهاد کرد. هر ایمیل کمی کار محاسباتی لازم داشت: برای یک پیام هیچ، برای میلیون‌ها پیام بسیار پرهزینه.

۴ — D

تولیدش کند است اما تأییدش آنی

مثل یک سودوکوی حل‌شده، ساختن اثبات کار زحمت دارد اما بررسی‌اش فقط یک لحظه طول می‌کشد. به این ترتیب هر کسی می‌تواند بدون تکرار کار، از انجام شدن آن مطمئن شود.

۵ — B

پیوند دادن سوابق در یک زنجیره تا تغییر تاریخچه آشکار شود

هر سابقه اثر انگشت سابقه قبلی را دارد، پس تغییر یک سابقه قدیمی همه حلقه‌های بعدی را می‌شکند. این ایده همان «زنجیره» در بلاک‌چین شد.

۶ — C

راهی برای اینکه غریبه‌ها بدون هیچ مسئولی روی یک تاریخچه مشترک توافق کنند

سیستم‌های قبلی یا به یک طرف مورد اعتماد متکی بودند یا هرگز حل نکردند که شرکت‌کنندگان مستقل زیاد چطور روی یک سابقه توافق کنند. بیت‌کوین این قطعه گمشده را اضافه کرد، همان‌طور که درس ۴ توضیح می‌دهد.

منابع

- وزارت دادگستری آمریکا، اعتراف به جرم در پرونده ای‌گلد (ژوئیه ۲۰۰۸): https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
- ویکی‌پدیا، DigiCash: https://en.wikipedia.org/wiki/DigiCash
- ویکی‌پدیا، e-gold: https://en.wikipedia.org/wiki/E-gold
- Satoshi Nakamoto Institute، هال فینی: RPOW: https://nakamotoinstitute.org/finney/rpow/
- Cointelegraph، هم‌مخترع بلاک‌چین درباره اینکه چرا ساتوشی ناکاموتو نیست: https://cointelegraph.com/news/co-inventor-of-blockchain-on-why-he-is-not-satoshi-nakamoto

Market Talks

ادامه یادگیری

درس بعدی: درس ۴ سال ۲۰۰۸ و تولد بیت‌کوین

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.