Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۵ از ۱۳

بلاک‌چین واقعاً چیست

یک تعریف ساده، سه بخشی که هر بلاک‌چینی دارد، و ادعاهای رایجی که درست نیستند

۷ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۵ از ۱۳

بلاک‌چین واقعاً چیست

در یک جمله

بلاک‌چین دفتری از تراکنش‌هاست که کامپیوترهای مستقل زیادی با هم نگه می‌دارند. ورودی‌های جدید در دسته‌های به هم پیوسته اضافه می‌شوند، ورودی‌های قدیمی را نمی‌توان بی‌سروصدا تغییر داد، و قواعد مشترک، نه یک شرکت، تعیین می‌کنند چه چیزی وارد شود.

تعریفی که واقعاً به کار می‌آید

در چهار درس گذشته یک مشکل و جست‌وجوی طولانی برای حل آن را دنبال کردیم. حالا می‌توانیم نام درستی روی آن راه‌حل بگذاریم. اگر هیاهو را کنار بگذاریم، بلاک‌چین این است:

دفتری از تراکنش‌ها که کامپیوترهای مستقل زیادی با هم نگه می‌دارند؛ ورودی‌های جدید در دسته‌های به هم پیوسته اضافه می‌شوند، ورودی‌های قدیمی را نمی‌توان بی‌سروصدا تغییر داد، و قواعد مشترک تعیین می‌کنند چه چیزی اضافه شود.

هر بخش این جمله اهمیت دارد. «کامپیوترهای مستقل زیاد» همان چیزی است که واسطه درس ۱ را حذف می‌کند. «دسته‌های به هم پیوسته» زنجیره بلاک‌هایی است که از پژوهش‌های مُهر زمانی در درس ۳ بیرون آمد. «قواعد مشترک» روش توافقی است که در درس ۴ دیدید. هر کدام را حذف کنید، دیگر بلاک‌چینی به معنایی که بیت‌کوین معرفی کرد ندارید.

به این نوع سابقه **دفترکل** (ledger) می‌گویند: فهرستی از اینکه چه کسی چه چیزی را برای چه کسی و چه زمانی فرستاده است. بلاک‌چین یک روش خاص برای نگه داشتن دفترکل است که برای موقعیت‌هایی ساخته شده که طرف‌ها به‌طور کامل به هم اعتماد ندارند.

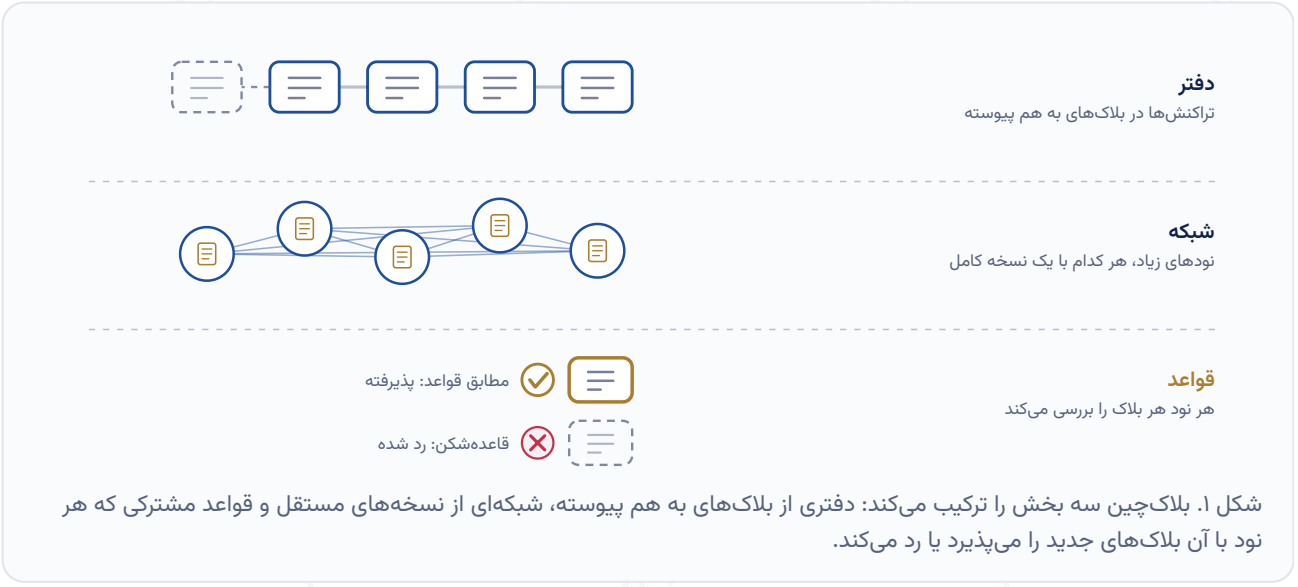
سه بخش که با هم کار می‌کنند

بهتر است هر بلاک‌چین عمومی را سه لایه روی هم در نظر بگیرید:

- **دفتر.** تراکنش‌ها در بلاک‌ها دسته‌بندی می‌شوند و هر بلاک به بلاک قبلی اشاره می‌کند، تا برسد به نخستین بلاک. درس ۶ نشان می‌دهد این پیوند دقیقاً چطور ساخته می‌شود.
- **شبکه.** هزاران کامپیوتر به نام **نود** (node) هر کدام یک نسخه کامل از دفتر را نگه می‌دارند و تراکنش‌ها و بلاک‌های جدید را به هم می‌رسانند. درس ۷ آن‌ها را با جزئیات بررسی می‌کند.

- **قواعد.** هر نود هر بلاک جدید را پیش از پذیرفتن با قواعد یکسانی بررسی می‌کند. بلاکی که قاعده‌ای را بشکند رد می‌شود، فرقی نمی‌کند چه کسی آن را فرستاده باشد. روش انتخاب کسی که بلاک بعدی را اضافه می‌کند **اجماع** (consensus) نام دارد، و نسخه بیت‌کوین همان اثبات کاری است که در درس ۴ با آن آشنا شدید.

هیچ‌کدام از این بخش‌ها به‌تنهایی تازه نیست. پایگاه داده، شبکه و بررسی قواعد مدت‌ها پیش از ۲۰۰۸ وجود داشتند. چیزی که بلاک‌چین را متفاوت می‌کند ترکیب آن‌هاست، و اینکه هیچ طرف واحدی هیچ‌کدام از این سه را کنترل نمی‌کند.



شکل ۱. بلاک‌چین سه بخش را ترکیب می‌کند: دفتری از بلاک‌های به هم پیوسته، شبکه‌ای از نسخه‌های مستقل و قواعد مشترکی که هر نود با آن بلاک‌های جدید را می‌پذیرد یا رد می‌کند.

درونش واقعاً چه هست

تصور رایج، یک خزانه بزرگ پر از سکه است. واقعیت بیشتر به یک فهرست خیلی طولانی از انتقال‌ها شبیه است. یک بلاک بیت‌کوین بیشتر شامل تراکنش‌هاست که هر کدام در اصل می‌گوید «این سکه‌ها از اینجا به آنجا می‌روند»، به‌علاوه یک سرآیند کوچک که آن را به بلاک قبلی وصل می‌کند.

هیچ‌جا خطی نیست که بگوید «آلیس ۲ بیت‌کوین دارد». کیف پول شما موجودی‌تان را با بررسی همه تراکنش‌های گذشته مربوط به آدرس‌هایتان محاسبه می‌کند. موجودی شما نتیجه تاریخچه است، نه عددی جداگانه که کسی نگه دارد و بتواند ویرایشش کند.

نام‌ها هم ذخیره نمی‌شوند. تراکنش‌ها به **آدرس‌ها** اشاره می‌کنند، رشته‌های طولانی از حروف و اعداد. همین بیت‌کوین را **شبه‌ناشناس** می‌کند، نه ناشناس: هر کسی می‌تواند ببیند هر آدرس چه کرده، اما به‌طور خودکار نمی‌داند چه کسی پشت آن است. درس ۸ توضیح می‌دهد آدرس‌ها از کجا می‌آیند.

خودتان بررسی کنید

نخستین پرداخت از یک نفر به نفر دیگر، یعنی ۱۰ بیت‌کوینی که ساتوشی در ژانویه ۲۰۰۹ برای هال فینی فرستاد، در بلاک ۱۷۰ است. هر وب‌سایت رایگان بلاک اکسپلورر را باز کنید، بلاک ۱۷۰ را جست‌وجو کنید، و آن را پس از بیش از ۱۷ سال بدون تغییر پیدا می‌کنید. همه نودهای کامل در دنیا هنوز همان تراکنش را نگه می‌دارند.

چهار ویژگی مهم

بلاک‌چین‌های عمومی مثل بیت‌کوین چهار ویژگی دارند که سیستم‌های معمولی معمولاً ندارند:

- **فقط افزودنی.** ورودی‌های جدید را می‌توان به انتها اضافه کرد. ورودی‌های قدیمی هرگز ویرایش یا حذف نمی‌شوند. اشتباه با یک تراکنش جدید اصلاح می‌شود، نه با پاک کردن تراکنش قبلی.
- **تکثیرشده.** همان دفتر کامل روی هزاران دستگاه در کشورهای مختلف وجود دارد. از دست رفتن بخشی از آن‌ها چیزی را تغییر نمی‌دهد.
- **شفاف.** هر کسی می‌تواند دفتر را دانلود کند و هر تراکنشی را که تا به حال انجام شده، بدون اجازه گرفتن، بخواند.
- **بدون نیاز به مجوز.** هر کسی می‌تواند بدون ثبت‌نام یا تأیید، تراکنش بفرستد یا نود اجرا کند. درس ۱۲ به بلاک‌چین‌های خصوصی می‌پردازد که این‌طور نیستند.

تشبیه: گروه چتی که هیچ‌کس نمی‌تواند ویرایشش کند

یک گروه چت را تصور کنید که گوشی هر عضو کل تاریخچه را نگه می‌دارد، پیام‌ها هرگز ویرایش یا حذف نمی‌شوند، و یک پیام جدید فقط وقتی نمایش داده می‌شود که بیشتر گوشی‌ها بررسی کرده باشند که با قوانین گروه می‌خواند. می‌توانید برنامه را از گوشی خودتان پاک کنید، اما گفت‌وگو در همه جای دیگر ادامه پیدا می‌کند. برای تغییر حرفی که پارسال زده شد، باید آن را هم‌زمان روی هزاران گوشی تغییر دهید.

بلاک‌چین چه چیزی نیست

بلاک‌چین‌ها ادعاهای بزرگی را به خود جذب می‌کنند. بهتر است چند تا از آن‌ها را از همین ابتدا اصلاح کنیم:

- **پایگاه داده‌ای سریع‌تر یا ارزان‌تر نیست.** هماهنگ نگه داشتن هزاران نسخه عمداً کند و پرهزینه است. برای بیشتر نرم‌افزارهای روزمره، یک پایگاه داده معمولی انتخاب بهتری است.
- **هک‌نشدنی نیست.** خود دفتر بیت‌کوین ثابت کرده که حمله به آن بسیار دشوار است، اما صرافی‌ها، کیف پول‌ها و برنامه‌هایی که حول بلاک‌چین‌ها ساخته شده‌اند مرتب هک می‌شوند. بیشتر زیان‌ها همان‌جا رخ می‌دهد، نه روی زنجیره.

- **ماشین حقیقت نیست.** بلاک‌چین ثابت می‌کند که یک ورودی ثبت شده و تغییر نکرده است. نمی‌تواند ثابت کند که آن ورودی از اول درست بوده. اگر اطلاعات نادرست وارد شود، زنجیره با وفاداری یک سابقه نادرست را نگه می‌دارد.

	پایگاه داده معمولی	بلاک‌چین عمومی
چه کسی می‌تواند سابقه اضافه کند	مالک و کسانی که او تأیید کند	هر کسی که قواعد را رعایت کند
ویرایش سوابق قدیمی	ممکن، اغلب بدون اینکه دیده شود	بدون اینکه همه ببینند ممکن نیست
چه کسی نسخه‌ها را نگه می‌دارد	مالک	هزاران نود مستقل
چه کسی می‌تواند آن را بخواند	هر کسی که مالک اجازه دهد	همه
سرعت و هزینه	سریع و ارزان	کندتر و گران‌تر
اگر گرداننده ناپدید شود	سیستم متوقف می‌شود	شبکه به کار خود ادامه می‌دهد

چرا این برای تریدرها مهم است

- **موجودی صرافی روی بلاک‌چین نیست.** وقتی در یک صرافی بیت‌کوین می‌خرید، معامله در پایگاه داده خود صرافی ثبت می‌شود. بلاک‌چین فقط واریز و برداشت را می‌بیند. وقتی FTX در نوامبر ۲۰۲۲ فروپاشید، صفحه‌های مشتریان موجودی‌هایی نشان می‌داد که شرکت نمی‌توانست پرداختشان کند. درس ۱۰ به اینکه چطور به این ریسک فکر کنید می‌پردازد.
- **داده عمومی، داده معاملاتی است.** چون دفتر شفاف است، هر کسی می‌تواند انتقال‌های بزرگ، ورود و خروج سکه‌ها به صرافی‌ها و کیف پول‌هایی را که سال‌ها بی‌حرکت بوده‌اند زیر نظر بگیرد. بسیاری از تریدرها از این داده‌های درون‌زنجیره‌ای استفاده می‌کنند و سطح پیشرفته یک درس کامل درباره آن دارد.
- **خود این کلمه می‌تواند بازار را حرکت دهد.** در دسامبر ۲۰۱۷، شرکت Long Island Iced Tea نامش را به Long Blockchain تغییر داد و قیمت سهامش در عرض چند ساعت چند برابر شد، بدون اینکه هیچ کسب‌وکار واقعی بلاک‌چینی پشتش باشد. بعدها SEC ثبت این سهام را لغو کرد و سه نفر را به معامله با اطلاعات نهانی متهم کرد. فهمیدن اینکه بلاک‌چین چیست کمک می‌کند هیاهو را وقتی می‌بینید تشخیص دهید.

اصطلاحات کلیدی

دفترکل سابقه‌ای از اینکه چه کسی چه چیزی را برای چه کسی و چه زمانی فرستاده. بلاک‌چین یکی از روش‌های نگه داشتن دفترکل است.

نود	کامپیوتری که یک نسخه از بلاک‌چین را نگه می‌دارد، بلاک‌های جدید را با قواعد بررسی می‌کند و آن‌ها را با دیگران به اشتراک می‌گذارد.
اجماع	روشی که شبکه بلاک‌چین با آن توافق می‌کند کدام بلاک بعدی اضافه شود. بیت‌کوین از اثبات کار استفاده می‌کند.
فقط افزودنی	سابقه‌ای که می‌توان به آن ورودی جدید اضافه کرد، اما ورودی‌های قدیمی هرگز ویرایش یا حذف نمی‌شوند.
شبه‌ناشناس	مرتبط با یک آدرس به جای نام واقعی. فعالیت‌ها عمومی است، اما فرد پشت آن به‌طور خودکار شناخته نمی‌شود.
بدون نیاز به مجوز	باز برای همه، بدون نیاز به ثبت‌نام یا تأیید برای فرستادن تراکنش یا اجرای نود.

نکات کلیدی

1. بلاک‌چین دفتری از تراکنش‌هاست که کامپیوترهای مستقل زیادی با هم نگه می‌دارند، در دسته‌های به هم پیوسته اضافه می‌شود و قواعد مشترک بر آن حاکم است.
2. هر بلاک‌چین عمومی سه بخش دارد: دفتر، شبکه نودها و قواعدی که تعیین می‌کنند چه چیزی اضافه شود.
3. بلاک‌ها شامل تراکنش‌ها هستند، نه موجودی یا نام. موجودی شما از کل تاریخچه آدرس‌هایتان محاسبه می‌شود.
4. بلاک‌چین‌های عمومی فقط افزودنی، تکثیرشده، شفاف و بدون نیاز به مجوز هستند.
5. بلاک‌چین پایگاه داده سریع‌تر، هک‌نشدنی یا ماشین حقیقت نیست. ثابت می‌کند یک ورودی تغییر نکرده، نه اینکه درست بوده است.

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. کدام توصیف از بلاک‌چین دقیق‌تر است؟

A خزانه‌ای امن که سکه‌های دیجیتال را نگه می‌دارد
B دفتری از تراکنش‌ها که کامپیوترهای مستقل زیادی با قواعد مشترک با هم نگه می‌دارند
C نوعی پایگاه داده سریع‌تر که یک شرکت فناوری اداره می‌کند
D وب‌سایتی که مردم در آن رمزارز معامله می‌کنند

۲. هر بلاک‌چین عمومی کدام سه بخش را با هم ترکیب می‌کند؟

A سکه‌ها، کیف پول‌ها و صرافی‌ها
B ماینرها، بانک‌ها و نهادهای نظارتی
C دفتر، شبکه نودها و قواعد
D رمزهای عبور، سرورها و نسخه‌های پشتیبان

۳. کیف پول شما از کجا موجودی بیت‌کوین‌تان را می‌داند؟

A همه تراکنش‌های گذشته مربوط به آدرس‌هایتان را جمع می‌زند
B خط موجودی ذخیره‌شده در هر بلاک را می‌خواند
C از شرکتی که بیت‌کوین را اداره می‌کند می‌پرسد
D نام شما را در بلاک‌چین جست‌وجو می‌کند

۴. «فقط افزودنی» یعنی چه؟

A فقط کاربران تأییدشده می‌توانند سابقه اضافه کنند
B سوابق پس از مدتی حذف می‌شوند
C فقط جدیدترین بلاک قابل خواندن است
D می‌توان ورودی جدید اضافه کرد، اما ورودی‌های قدیمی هرگز ویرایش یا حذف نمی‌شوند

۵. چرا بیت‌کوین را شبه‌ناشناس می‌دانند و نه ناشناس؟

A چون تراکنش‌ها از دید عموم پنهان است
B چون فعالیت‌ها عمومی و مرتبط با آدرس‌هاست، اما نه به‌طور خودکار با نام‌های واقعی
C چون کاربران باید با نام واقعی ثبت‌نام کنند
D چون فقط ماینرها می‌توانند تراکنش‌ها را ببینند

۶. کدام ادعا درباره بلاک‌چین‌ها درست است؟

A بلاک‌چین ثابت می‌کند اطلاعات درونش درست است

B بلاک‌چین‌ها از پایگاه‌های داده معمولی سریع‌تر و ارزان‌ترند

C بلاک‌چین ثابت می‌کند یک ورودی تغییر نکرده، اما نه اینکه هنگام ثبت درست بوده

D هیچ چیزی که حول بلاک‌چین ساخته شده هک نمی‌شود

کلید پاسخ‌ها

۱ **B**

دفتری از تراکنش‌ها که کامپیوترهای مستقل زیادی با قواعد مشترک با هم نگه می‌دارند

بلاک‌چین یک دفترکل مشترک است. کامپیوترهای مستقل زیادی نسخه‌ها را نگه می‌دارند، ورودی‌های جدید در بلاک‌های به هم پیوسته اضافه می‌شوند و قواعد مشترک تعیین می‌کنند چه چیزی وارد شود.

۲ **C**

دفتر، شبکه نودها و قواعد

دفتر بلاک‌های به هم پیوسته را نگه می‌دارد، شبکه نودها نسخه‌ها را نگه می‌دارد و به اشتراک می‌گذارد، و قواعد تعیین می‌کنند کدام بلاک‌ها پذیرفته شوند.

۳ **A**

همه تراکنش‌های گذشته مربوط به آدرس‌هایتان را جمع می‌زند

بلاک‌ها انتقال‌ها را نگه می‌دارند، نه موجودی‌ها را. موجودی شما از تاریخچه همه تراکنش‌های ورودی و خروجی آدرس‌هایتان محاسبه می‌شود.

۴ **D**

می‌توان ورودی جدید اضافه کرد، اما ورودی‌های قدیمی هرگز ویرایش یا حذف نمی‌شوند

در یک دفتر فقط افزودنی، تاریخچه فقط بزرگ‌تر می‌شود. اشتباه با یک تراکنش جدید اصلاح می‌شود، نه با تغییر یک تراکنش قدیمی.

۵ **B**

چون فعالیت‌ها عمومی و مرتبط با آدرس‌هاست، اما نه به‌طور خودکار با نام‌های واقعی

هر کسی می‌تواند همه تراکنش‌های یک آدرس را ببیند. چیزی که به‌طور خودکار نمی‌داند، فرد واقعی پشت آن آدرس است.

۶ **C**

بلاک‌چین ثابت می‌کند یک ورودی تغییر نکرده، اما نه اینکه هنگام ثبت درست بوده

بلاک‌چین از تغییر یک سابقه محافظت می‌کند. اگر اطلاعات نادرست وارد شود، آن سابقه نادرست را هم با همان وفاداری نگه می‌دارد.

منابع

- ساتوشی ناکاموتو، (۲۰۰۸) Bitcoin: A Peer-to-Peer Electronic Cash System :https://bitcoin.org/bitcoin.pdf
- رکوردهای جهانی گینس، نخستین تراکنش بیت‌کوین: https://guinnessworldrecords.com/world-records/696243-first-bitcoin-transaction
- Fortune، اتهام معامله با اطلاعات نهانی پس از تغییر نام به Long Blockchain (ژوئیه ۲۰۲۱): https://fortune.com/2021/07/09/sec-insider-trading-long-blockchain
- CoinDesk، حذف سهام Long Blockchain Corporation از سوی SEC: https://www.coindesk.com/long-blockchain-corporation-shares-delisted-sec

Market Talks

ادامه یادگیری

درس بعدی: درس ۶
بلاک‌ها و هش، به زبان ساده

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.