Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۱۳ از ۱۳

باورهای نادرست و واقعیت‌ها

شش چیزی که مردم اغلب درباره بلاک‌چین اشتباه می‌کنند، هم در جهت بزرگ‌نمایی و هم در جهت کوچک‌شماری، و آنچه شواهد واقعاً نشان می‌دهند

۵ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۱۳ از ۱۳

باورهای نادرست و واقعیت‌ها

در یک جمله

بلاک‌چین نه جادوست و نه کلاهبرداری. در چند کار مشخص بسیار خوب است، مانند تسویه ارزش بدون واسطه و نگه داشتن سابقه‌ای مشترک که تغییر دادنش سخت است، و در کارهای دیگر ضعیف است. دانستن اینکه کدام به کدام است، شما را هم از هیاهو و هم از رد کردن یکسره در امان نگه می‌دارد.

باور نادرست ۱: «بیت‌کوین ناشناس است»

واقعیت: بیت‌کوین شبه‌ناشناس است، همان‌طور که درس ۵ توضیح داد. آدرس‌ها نام ندارند، اما هر پرداختی میان آن‌ها برای همیشه عمومی می‌ماند. همین که یک آدرس به یک شخص مرتبط شود، مثلاً از طریق صرافی‌ای که هویت او را بررسی کرده، بخش بزرگی از سابقه‌اش قابل ردیابی می‌شود.

نمونه روشنی در ژوئن ۲۰۲۱ پیش آمد. پس از حمله باج‌افزاری به Colonial Pipeline که عرضه سوخت در ساحل شرقی آمریکا را مختل کرد، وزارت دادگستری آمریکا باج را روی بلاک‌چین دنبال کرد و ۶۳٫۷ بیت‌کوین از ۷۵ بیت‌کوین پرداخت‌شده را پس گرفت. معلوم شد که یک دفتر کل عمومی جای خوبی برای پنهان شدن نیست.



شکل ۱. بلاک‌چین در چند کار مشخص قوی و در کارهای دیگر ضعیف است. بیشتر باورهای نادرست از فراموش کردن یکی از دو کفه این ترازو می‌آیند.

تشبیه: نام مستعار در خانه‌ای شیشه‌ای

فرض کنید همه نامه‌هایتان را با یک نام مستعار امضا می‌کنید، اما همه آن‌ها به دیوار ساختمانی شیشه‌ای در خیابانی شلوغ چسبانده شده‌اند. در ابتدا هیچ‌کس نام واقعی‌تان را نمی‌داند. اما به محض اینکه کسی ببیند شما یکی از نامه‌ها را می‌چسبانید، می‌تواند همه نامه‌های دیگری را که با همان نام مستعار امضا شده‌اند بخواند.

باور نادرست ۲: «کریپتو بیشتر برای جرم استفاده می‌شود»

واقعیت: جرم واقعی است، اما سهم کوچکی از فعالیت را تشکیل می‌دهد. شرکت تحلیلی Chainalysis برآورد کرد که آدرس‌های غیرقانونی در سال ۲۰۲۵ دست‌کم ۱۵۴ میلیارد دلار دریافت کرده‌اند. این رقم بسیار بزرگی است، اما همچنان کمتر از ۱٪ کل حجم تراکنش‌های کریپتویی است که این شرکت دنبال می‌کند. بخش زیادی از این مبلغ از دور زدن تحریم‌ها و سرقت‌هایی بود که گروه‌های مورد حمایت دولت‌ها انجام دادند.

هر دو نیمه مهم‌اند. سهم کوچک است، اما مبالغ آن‌قدر بزرگ‌اند که نهادهای ناظر، صرافی‌ها و بانک‌ها جرایم کریپتویی را جدی بگیرند، و به همین دلیل صرافی‌ها احراز هویت می‌خواهند.

باور نادرست ۳: «بلاک‌چین هک‌شدنی نیست»

واقعیت: خود دفتر کل بیت‌کوین هرگز بازنویسی نشده، اما تقریباً هر چیزی پیرامون آن قابل حمله است. بزرگ‌ترین زیان‌ها از لبه‌ها می‌آیند: صرافی‌ها، کیف پول‌ها، قراردادهای هوشمند و **پل‌ها** که توکن‌ها را میان زنجیره‌ها جابه‌جا می‌کنند. در مارس ۲۰۲۲، مهاجمان پس از به دست گرفتن کنترل بیشتر کلیدهایی که برداشت‌ها را تأیید می‌کردند، حدود ۶۲۵ میلیون دلار از پل Ronin که بازی Axie Infinity از آن استفاده می‌کرد بیرون کشیدند. وزارت خزانه‌داری آمریکا بعدها این سرقت را به گروه Lazarus کره شمالی نسبت داد.

زنجیره‌های کوچک دومین نقطه ضعف‌اند. اگر پشت یک شبکه توان استخراج یا سهام اندکی باشد، بازنویسی بلاک‌های اخیر ممکن است مقرون‌به‌صرفه باشد، همان چیزی که حمله ۵۱٪ نامیده می‌شود. امنیت به این بستگی دارد که تقلب چقدر هزینه داشته باشد، و این هزینه از زنجیره‌ای به زنجیره دیگر بسیار متفاوت است.

باور نادرست ۴: «اگر روی بلاک‌چین باشد، درست است»

واقعیت: بلاک‌چین ثابت می‌کند که یک سابقه از زمان نوشته شدن تغییر نکرده است. ثابت نمی‌کند که آن سابقه از اول درست بوده. اگر یک تأمین‌کننده کنار جعبه‌ای از سبزیجات معمولی بنویسد «ارگانیک»، زنجیره همان ادعای نادرست را صادقانه برای همیشه نگه می‌دارد.

به این گاهی **مسئله اوراکل** می‌گویند: هر بار که واقعیت‌های دنیای واقعی مانند قیمت‌ها، تحویل کالا یا مالکیت وارد بلاک‌چین می‌شوند، کسی باید آن‌ها را گزارش کند و باید به آن کس اعتماد کرد. زنجیره وقتی قوی‌ترین حالت را دارد که دارایی کاملاً روی خودش زندگی کند، مانند خود بیت‌کوین.

باورهای نادرست ۵ و ۶: «بیت‌کوین انرژی را هدر می‌دهد» و «بلاک‌چین سریع و رایگان است»

واقعیت درباره انرژی: استخراج بیت‌کوین واقعاً برق زیادی مصرف می‌کند، طبق پژوهشی از دانشگاه کمبریج در سال ۲۰۲۵ حدود ۱۳۸ تراوات‌ساعت در سال، یعنی تقریباً ۰٫۵٪ مصرف برق جهان. همان پژوهش نشان داد که ۵۲٫۴٪ آن از

منابع پایدار تأمین می‌شد، عمدتاً برق‌آبی، باد و انرژی هسته‌ای. شبکه‌های اثبات سهام مانند اتریوم تنها کسر بسیار کوچکی از این مقدار را مصرف می‌کنند. اینکه این انرژی می‌ارزد یا نه، همچنان بحثی واقعی است.

واقعیت درباره سرعت: بلاک‌چین‌های عمومی ذاتاً کندند، چون هزاران رایانه باید به توافق برسند. بیت‌کوین روی زنجیره اصلی خود تنها چند تراکنش در ثانیه را پردازش می‌کند و وقتی تقاضا جهش می‌کند کارمزدها بالا می‌روند، همان‌طور که درس ۱۱ نشان داد. سیستم‌های سریع‌تری روی آن ساخته می‌شوند، اما هر کدام معاوضه‌های خودش را دارد.

جاهایی که بلاک‌چین قوی است	جاهایی که ضعیف است
جابه‌جایی ارزش بدون واسطه	سرعت و هزینه در مقیاس بزرگ
سوابقی که تغییرشان بسیار سخت است	بررسی درستی داده‌های دنیای واقعی
باز برای همه و سانسورش دشوار	اشتباه‌ها و سرقت‌ها برگشت‌پذیر نیستند
همه می‌توانند قواعد را بررسی کنند	حریم خصوصی، چون همه‌چیز عمومی است

چرا این برای تریدرها مهم است

- **باورهای نادرست قیمت‌ها را جابه‌جا می‌کنند.** در ۱۲ مه ۲۰۲۱، تسلا با اشاره به انرژی مصرفی استخراج، پذیرش بیت‌کوین برای خرید خودرو را متوقف کرد و بیت‌کوین در آن روز حدود ۱۲٪ افت کرد. داستان‌هایی درباره انرژی، جرم و هک بارها و بارها برمی‌گردند و بازارها اغلب پیش از بررسی واقعیت‌ها واکنش نشان می‌دهند.
- **هک‌ها به توکن‌ها ضربه می‌زنند، نه همیشه به زنجیره.** وقتی یک پل یا صرافی خالی می‌شود، توکن‌های مربوط ممکن است سقوط کنند در حالی که شبکه زیربنایی به‌طور عادی کار می‌کند. پیش از اینکه تصمیم بگیرید این اتفاق برای سکه‌ای که دارید چه معنایی دارد، بپرسید دقیقاً به چه چیزی حمله شده است.
- **هیاهو از هر دو طرف می‌آید.** «بلاک‌چین همه‌چیز را درست می‌کند» و «بلاک‌چین بی‌فایده است» هر دو تیترهای ساده‌ای‌اند. پرسش مفید همیشه دقیق‌تر است: آیا این پروژه به یک سابقه باز و مشترک نیاز دارد و آیا واقعاً از آن استفاده می‌کند؟

اصطلاحات کلیدی

شبه‌ناشناس	استفاده از آدرس به جای نام. فعالیت‌ها عمومی‌اند و هویت فقط تا وقتی پنهان می‌ماند که آدرس به شخصی مرتبط نشده باشد.
پل	سرویسی که توکن‌ها را میان دو بلاک‌چین جابه‌جا می‌کند و اغلب مبالغ زیادی را در یک جا نگه می‌دارد، و همین آن را به هدفی رایج تبدیل می‌کند.

حمله ۵۱٪	حمله‌ای که در آن کسی بیشتر توان استخراج یا سهام یک زنجیره را در اختیار دارد و از آن برای بازنویسی بلاک‌های اخیر استفاده می‌کند.
مسئله اوراکل	دشواری وارد کردن اطلاعات دنیای واقعی به بلاک‌چین بدون نیاز به اعتماد به کسی که آن را گزارش می‌کند.
حجم غیرقانونی	ارزش کریپتویی که آدرس‌های مرتبط با جرم دریافت کرده‌اند، مانند کلاهبرداری، سرقت، باج‌افزار و دور زدن تحریم‌ها.
اثبات سهام	روشی برای ایمن کردن بلاک‌چین با قفل کردن سکه‌ها به جای استخراج، که برق بسیار کمتری لازم دارد.

نکات کلیدی

1. بیت‌کوین شبه‌ناشناس است، نه ناشناس، و پرداخت‌ها قابل ردیابی‌اند، همان‌طور که بازپس‌گیری باج Colonial Pipeline نشان داد.
2. فعالیت غیرقانونی به دلار بزرگ است، اما زیر ۱٪ حجم کریپتوی ردیابی‌شده مانده است.
3. دفتر کل بیت‌کوین هرگز بازنویسی نشده، اما صرافی‌ها، پل‌ها، قراردادهای هوشمند و زنجیره‌های کوچک به‌طور منظم مورد حمله قرار می‌گیرند.
4. بلاک‌چین سوابق را بدون تغییر نگه می‌دارد، اما نمی‌تواند بررسی کند که داده‌های دنیای واقعی هنگام ورود درست بوده‌اند یا نه.
5. بیت‌کوین انرژی زیادی مصرف می‌کند و زنجیره‌های عمومی ذاتاً کندند. شناختن نقاط قوت و محدودیت‌های واقعی، شما را از هیاهو در هر دو جهت در امان نگه می‌دارد.

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. چرا بیت‌کوین را شبه‌ناشناس می‌دانند و نه ناشناس؟

- A) تراکنش‌ها از همه به جز ماینرها پنهان‌اند
- B) آدرس‌ها نام ندارند، اما هر تراکنش عمومی و قابل ردیابی است
- C) فقط صرافی‌ها می‌توانند بلاک‌چین را ببینند
- D) کاربران باید نامشان را روی بلاک‌چین ثبت کنند

۲. Chainalysis درباره فعالیت غیرقانونی کریپتو در سال ۲۰۲۵ به چه نتیجه‌ای رسید؟

A بیشتر کل حجم کریپتو را تشکیل می‌داد
B پس از مقررات تازه به صفر رسید
C دست‌کم ۱۵۴ میلیارد دلار بود، اما همچنان کمتر از ۱٪ حجم ردیابی‌شده
D فقط روی بیت‌کوین دیده شد

۳. در هک Ronin در مارس ۲۰۲۲، به چه چیزی حمله شد؟

A خود بلاک‌چین بیت‌کوین
B یک پل، با به دست گرفتن کنترل بیشتر کلیدهایی که برداشت‌ها را تأیید می‌کردند
C همه کیف پول‌های اتریوم به‌طور هم‌زمان
D سخت‌افزار یک ماینر

۴. یک تأمین‌کننده اطلاعات نادرستی روی بلاک‌چین ثبت می‌کند. بلاک‌چین چه چیزی را تضمین می‌کند؟

A اطلاعات به‌طور خودکار اصلاح می‌شود
B اطلاعات درست است چون روی بلاک‌چین است
C این سابقه بعداً تغییر نمی‌کند، هرچند نادرست است
D ماینرها داده‌های نادرست را رد می‌کنند

۵. طبق پژوهش ۲۰۲۵ کمبریج، استخراج بیت‌کوین تقریباً چه سهمی از برق جهان را مصرف می‌کند؟

A حدود ۰٫۵٪
B حدود ۵٪
C حدود ۲۵٪
D بیش از نیمی

۶. پلی که یک توکن محبوب را نگه می‌دارد هک شده است. معقول‌ترین پرسش اول برای یک تریدر چیست؟

A آیا کل بلاک‌چین از کار افتاده است؟
B آیا باید همین حالا همه سکه‌هایم را بفروشم؟
C آیا درست است که حالا همه بلاک‌چین‌ها ناامن‌اند؟
D دقیقاً به چه چیزی حمله شده و کدام توکن‌ها را تحت تأثیر قرار می‌دهد؟

کلید پاسخ‌ها

۱ — B

آدرس‌ها نام ندارند، اما هر تراکنش عمومی و قابل ردیابی است

دفتر کل کاملاً عمومی است. همین که یک آدرس به شخصی مرتبط شود، پرداخت‌های گذشته‌اش را می‌توان دنبال کرد، همان کاری که بازرسان با باج Colonial Pipeline کردند.

۲ — C

دست‌کم ۱۵۴ میلیارد دلار بود، اما همچنان کمتر از ۱٪ حجم ردیابی‌شده

مبلغ دلاری بزرگ بود، اما در مقایسه با کل فعالیت ردیابی‌شده، سهم آن زیر ۱٪ ماند.

۳ — B

یک پل، با به دست گرفتن کنترل بیشتر کلیدهایی که برداشت‌ها را تأیید می‌کردند

مهاجمان کلیدهایی را که برداشت از پل را تأیید می‌کردند تصاحب کردند. بلاک‌چین‌های زیربنایی به‌طور عادی به کار خود ادامه دادند.

۴ — C

این سابقه بعداً تغییر نمی‌کند، هرچند نادرست است

بلاک‌چین سوابق را از تغییرات بعدی محافظت می‌کند. نمی‌تواند بداند که ادعایی درباره دنیای واقعی هنگام ورود درست بوده یا نه. این همان مسئله اوراکل است.

۵ — A

حدود ۰٫۵٪

این پژوهش مصرف را حدود ۱۳۸ تراوات‌ساعت در سال برآورد کرد، یعنی تقریباً ۰٫۵٪ مصرف برق جهان، که کمی بیش از نیمی از آن از منابع پایدار بود.

۶ — D

دقیقاً به چه چیزی حمله شده و کدام توکن‌ها را تحت تأثیر قرار می‌دهد؟

بیشتر هک‌ها به سرویس‌هایی ضربه می‌زنند که پیرامون یک زنجیره ساخته شده‌اند، نه به خود زنجیره. دانستن اینکه به چه چیزی حمله شده، نشان می‌دهد کدام دارایی‌ها واقعاً در خطرند.

منابع

- NPR، آمریکا میلیون‌ها دلار از باج پرداخت‌شده به هکرهای Colonial Pipeline را پس گرفت (ژوئن ۲۰۲۱): https://www.kunc.org/npr-news/2021-06-07/u-s-has-recovered-some-of-the-millions-paid-in-ransom-to-colonial-pipeline-hackers
- The Block، جرایم کریپتویی در ۲۰۲۵ از ۱۵۰ میلیارد دلار گذشت (Chainalysis): https://www.theblock.co/post/384753/crypto-crime-150-billion-usd-2025-state-actors-scale-onchain-chainalysis
- TechCrunch، مقام‌های آمریکایی هکرهای Lazarus کره شمالی را به سرقت ۶۲۵ میلیون دلاری Ronin مرتبط دانستند: https://techcrunch.com/2022/04/15/us-officials-link-north-korean-lazarus-hackers-to-625m-axie-infinity-crypto-theft
- دانشکده کسب‌وکار جاج کمبریج، افزایش انرژی پایدار در استخراج بیت‌کوین (آوریل ۲۰۲۵): https://jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/
- SiliconANGLE، سقوط قیمت بیت‌کوین پس از توقف پرداخت با بیت‌کوین در تسلا (مه ۲۰۲۱): https://siliconangle.com/2021/05/12/bitcoin-price-plunges-elon-musk-pulls-support-citing-environmental-concerns/

Market Talks

ادامه یادگیری

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.