Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۱ از ۱۳

مسئله اعتماد

چرا هر پرداخت دیجیتال به یک واسطه نیاز دارد و چرا بلاک‌چین برای تغییر این وضعیت ابداع شد

۷ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۱ از ۱۳

مسئله اعتماد

در یک جمله

امروزه هر پرداخت دیجیتال به واسطه‌ای مورد اعتماد وابسته است که حساب‌ها را نگه می‌دارد. بلاک‌چین تلاشی است برای نگه‌داشتن دفتری مشترک که لازم نیست به کسی اعتماد کرد.

پول یک رکورد است، نه یک شیء

بیشتر پولی که دارید اسکناسی در کشوی میز نیست، بلکه عددی در پایگاه داده یک بانک است. وقتی از حساب خود به کسی پول می‌دهید، هیچ چیز فیزیکی جابه‌جا نمی‌شود. بانک شما یک رقم را در سوابق خود کم می‌کند و بانک گیرنده رقم دیگری را زیاد می‌کند.

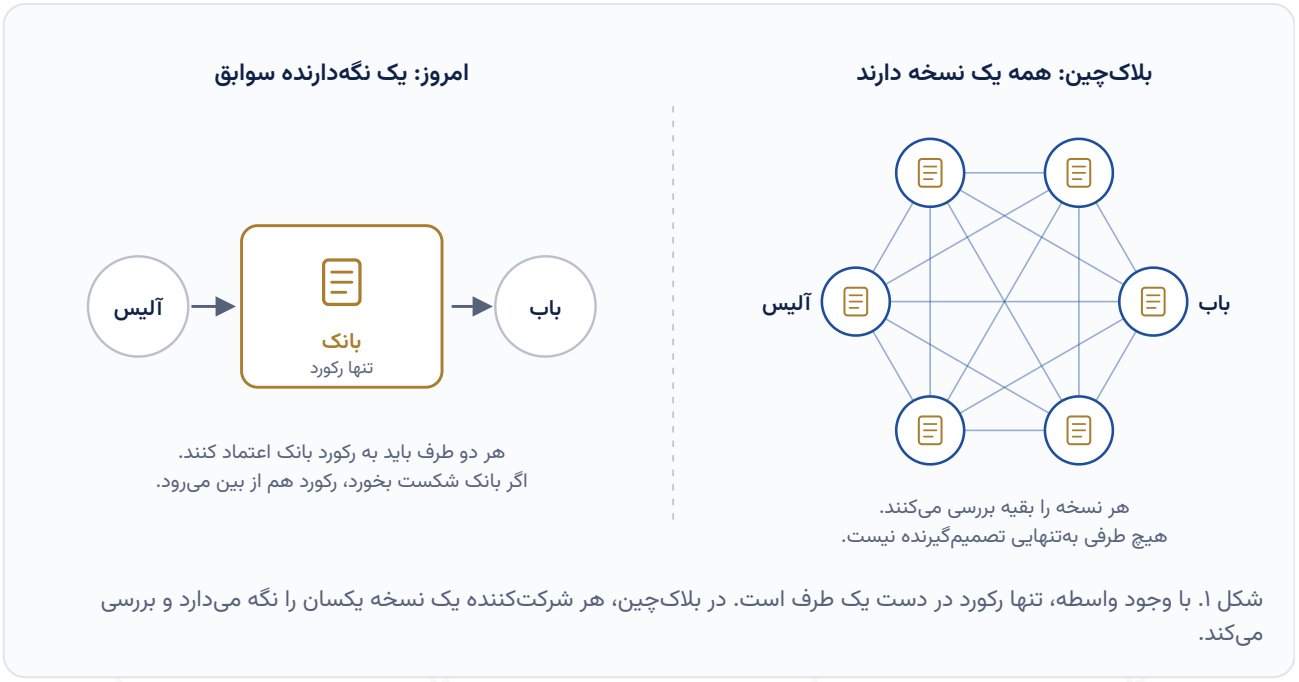
بنابراین آنچه واقعاً در اختیار دارید یک وعده است: وعده بانک که سوابقش درست است و هر وقت بخواهید به آن عمل می‌کند. همین موضوع درباره موجودی کارت، اپلیکیشن‌های پرداخت و دارایی‌هایی که در صرافی‌ها نگه می‌دارید هم صدق می‌کند. پول دیجیتال در اصل رکوردی است که کسی آن را نگه می‌دارد.

چرا به واسطه تکیه می‌کنیم

فرض کنید می‌خواهید به فروشنده‌ای در آن سوی دنیا پول بدهید که هرگز او را ندیده‌اید. شما نمی‌توانید سوابق او را بررسی کنید و او هم نمی‌تواند سوابق شما را بررسی کند. هیچ‌کدام دلیلی برای اعتماد به دیگری ندارید. واسطه این مشکل را با انجام هم‌زمان سه کار حل می‌کند:

- **نگه‌داشتن سوابق رسمی** درباره اینکه چه چیزی متعلق به چه کسی است.
- **بررسی هر پرداخت**، مثلاً اینکه واقعاً پولی را که می‌فرستید دارید.
- **حل اختلاف‌ها**، از جمله برگرداندن اشتباه‌ها و تقلب‌ها.

بانک‌ها، شبکه‌های کارت، اپلیکیشن‌های پرداخت و صرافی‌ها همگی این نقش را بازی می‌کنند. بیشتر وقت‌ها این سازوکار به‌خوبی کار می‌کند و دقیقاً به همین دلیل بر دنیای مالی مسلط است.



شکل ۱. با وجود واسطه، تنها رکورد در دست یک طرف است. در بلاک‌چین، هر شرکت‌کننده یک نسخه یکسان را نگه می‌دارد و بررسی می‌کند.

هزینه پنهان اعتماد به دیگران

تکیه بر واسطه راحت است، اما هیچ‌وقت رایگان نیست. این هزینه‌ها به چهار شکل خود را نشان می‌دهند:

- **کارمزد و تأخیر.** یک حواله بین‌المللی ممکن است از زنجیره‌ای از بانک‌ها عبور کند و هر کدام زمان و کارمزدی به آن اضافه کنند. طبق داده‌های بانک جهانی، در اوایل سال ۲۰۲۵ ارسال ۲۰۰ دلار به خارج از کشور به‌طور میانگین ۶٫۴۹٪ هزینه داشت، یعنی بیش از دو برابر هدف جهانی ۳٪.
- **کنترل دسترسی.** واسطه می‌تواند حساب را مسدود کند، ببندد یا از افتتاح آن خودداری کند. طبق داده‌های بانک جهانی، هنوز بیش از یک میلیارد بزرگسال در جهان هیچ حساب بانکی ندارند.
- **نقطه شکست واحد.** اگر واسطه هک شود، از کار بیفتد یا ورشکست شود، همه کسانی که به آن تکیه کرده بودند هم‌زمان آسیب می‌بینند.
- **سوابقی که نمی‌توانید بررسی کنید.** شما فقط موجودی‌ای را می‌بینید که واسطه تصمیم می‌گیرد نشان دهد. نمی‌توانید دفاتر آن را خودتان حسابرسی کنید.

هیچ‌کدام از این‌ها به این معنا نیست که بانک‌ها بد هستند. معنایش این است که اعتماد هزینه دارد و شما آن را می‌پردازید، چه متوجه شوید چه نه.

یک نمونه واقعی

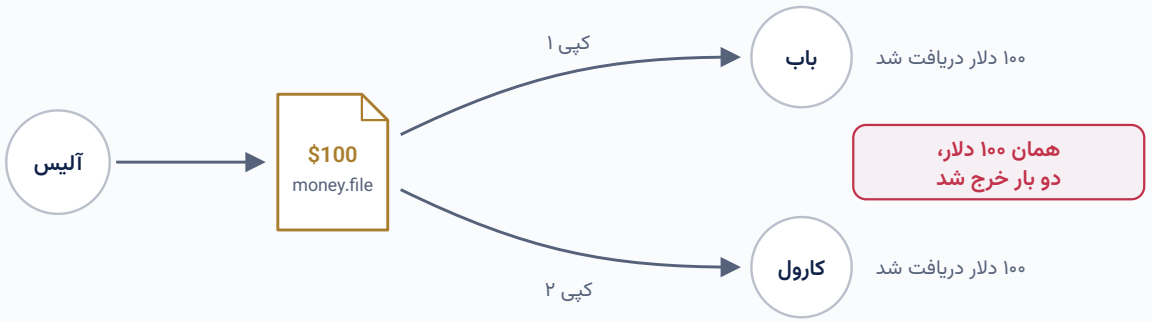
در نوامبر ۲۰۲۲، صرافی رمزارز FTX فروپاشید و اعلام ورشکستگی کرد. مشتریانی که فکر می‌کردند روی این پلتفرم بیت‌کوین و دلار دارند، فهمیدند که در واقع فقط طلبی از یک شرکت ورشکسته دارند. دارایی‌های آن‌ها تا روشن شدن روند ورشکستگی سال‌ها مسدود ماند.

چرا به‌سادگی پول دیجیتال نسازیم؟ مسئله خرج دوباره

چیزهای دیجیتال به‌طور کامل کپی می‌شوند. وقتی عکسی را برای دوستتان ایمیل می‌کنید، آن عکس را از دست نمی‌دهید. حالا هر دو آن را دارید. این برای عکس مشکلی ندارد، اما برای پول یک فاجعه است. اگر پول فقط یک فایل بود، می‌توانستید همان فایل را برای صد نفر بفرستید و با آن به همه‌شان پول بدهید.

یک سکه فیزیکی نمی‌تواند هم‌زمان در دو جیب باشد. اما پول دیجیتال می‌تواند، مگر اینکه چیزی جلوی آن را بگیرد. به این وضعیت **مسئله خرج دوباره** (Double Spending) می‌گویند و این اصلی‌ترین چالش پول دیجیتال است.

تا پیش از سال ۲۰۰۸، تنها راه‌حل قابل اتکا یک نگه‌دارنده مرکزی سوابق بود که تعیین کند کدام پرداخت اول انجام شده و کپی را رد کند. به همین دلیل هر تلاشی برای ساخت پول نقد دیجیتال همچنان به یک واسطه نیاز داشت و وقتی آن واسطه شکست می‌خورد یا تعطیل می‌شد، پول هم همراه با آن از بین می‌رفت. این تلاش‌های اولیه را در درس ۳ بررسی می‌کنیم.



شکل ۲. یک فایل دیجیتال قابل کپی است، بنابراین بدون یک سازوکار محافظتی، همان پول می‌تواند هم‌زمان برای دو نفر فرستاده شود.

پرسشی که بلاک‌چین برای پاسخ به آن ساخته شد

اگر همه آنچه گفتیم را کنار هم بگذاریم، به یک پرسش می‌رسیم:

> آیا گروهی از غریبه‌ها که به یکدیگر اعتماد ندارند می‌توانند یک رکورد مشترک را نگه دارند که همه آن را بپذیرند، بدون اینکه کسی مسئول آن باشد؟

این همان مسئله‌ای است که بلاک‌چین برای حل آن طراحی شد. در سال ۲۰۰۸ مقاله‌ای با نام ساتوشی ناکاموتو منتشر شد که راه‌حلی پیشنهاد می‌داد و چند ماه بعد بیت‌کوین راه‌اندازی شد. این ماجرا را در درس ۴ تعریف می‌کنیم.

ایده اصلی به‌طور خلاصه این است:

- به جای یک رکورد در دست یک نگه‌دارنده، **نسخه‌های یکسان فراوانی** در دست هر کسی است که بخواهد یک نسخه داشته باشد.

- هر ورودی جدید **توسط همه** و بر اساس قوانین عمومی یکسان **بررسی می‌شود**.
- تغییر ورودی‌های گذشته **بسیار پرهزینه** است، بنابراین می‌توان به تاریخچه اتکا کرد.

اعتماد از یک نهاد به سمت قوانین، ریاضیات و راستی‌آزمایی آشکار منتقل می‌شود. جامعه رمزارزها این را در یک جمله کوتاه خلاصه می‌کند: *اعتماد نکن، بررسی کن.*

تشبیه: صفحه‌گسترده مشترک

صفحه‌گسترده‌ای آنلاین را تصور کنید که یک شرکت میزبانی آن را بر عهده دارد. آن شرکت می‌تواند دسترسی شما را قطع کند، ردیف‌ها را ویرایش کند یا فایل را گم کند. حالا صفحه‌گسترده دیگری را تصور کنید: همه یک نسخه کامل از آن دارند، ردیف جدید فقط زمانی اضافه می‌شود که کل گروه تأیید کند طبق قوانین است و ردیف‌های قدیمی مُهر و موم شده‌اند و دیگر قابل ویرایش نیستند. هیچ‌کس مالک آن نیست و هر کسی می‌تواند آن را بررسی کند. این صفحه‌گسترده دوم، ایده اصلی بلاک‌چین است.

آنچه بلاک‌چین از بین نمی‌برد

مهم است که از همان ابتدا درباره محدودیت‌ها صادق باشیم. بلاک‌چین نیاز به اعتماد به *یک نگه‌دارنده واحد سوابق* را از بین می‌برد، اما اعتماد را به‌طور کامل حذف نمی‌کند. شما همچنان به درستی نرم‌افزار، به دقت خودتان در محافظت از کلیدها و اغلب به واسطه‌های تازه‌ای مثل صرافی‌ها و اپلیکیشن‌های کیف پول متکی هستید.

همچنین تور ایمنی را هم برمی‌دارد. معمولاً هیچ پشتیبانی وجود ندارد که پرداختی را که به اشتباه ارسال شده برگرداند. در درس‌های بعدی این دوره، هر دو روی این بده‌بستان‌ها را با جزئیات خواهید دید.

چرا این موضوع برای معامله‌گران مهم است

- **ریسک طرف مقابل همه‌جا هست.** وقتی دارایی شما در یک صرافی یا نزد یک کارگزار است، شما وعده آن شرکت را در دست دارید، نه خود دارایی را. فروپاشی FTX نشان داد این تفاوت در عمل چه معنایی دارد.
- **تسویه به شکل متفاوتی انجام می‌شود.** معاملات سهام در آمریکا یک روز کاری پس از معامله تسویه می‌شوند (T+1، از مه ۲۰۲۴) و فقط در روزهای کاری. اما انتقال بیت‌کوین طبق قوانین خود شبکه و به‌صورت شبانه‌روزی، حتی در تعطیلات آخر هفته، تسویه می‌شود.
- **اعتماد روایت‌های بازار را شکل می‌دهد.** بیت‌کوین در پی بحران بانکی ۲۰۰۸ متولد شد. وقتی در مارس ۲۰۲۳ چند بانک منطقه‌ای آمریکا ورشکست شدند، بیت‌کوین در هفته‌های بعد رشد شدیدی داشت و بسیاری از تحلیلگران بازار این حرکت را به تردیدهای تازه نسبت به بانک‌ها ربط دادند. درک مسئله اعتماد به شما کمک می‌کند بفهمید چرا چنین روایت‌هایی قیمت‌ها را حرکت می‌دهند.

اصطلاحات کلیدی

واسطه	طرفی میانی، مانند بانک یا صرافی، که سوابق را نگه می‌دارد و پرداخت‌ها را میان دو طرف انجام می‌دهد.
دفتر کل (Ledger)	سابقه‌ای از تراکنش‌ها و موجودی‌ها. بلاک‌چین نوع خاصی از دفتر کل است.
ریسک طرف مقابل	ریسک اینکه طرف دیگر یک توافق به تعهدات خود عمل نکند.
خرج دوباره	خرج کردن یک پول دیجیتال بیش از یک بار. جلوگیری از آن اصلی‌ترین چالش پول نقد دیجیتال است.
تسویه	لحظه‌ای که پرداخت یا معامله کامل می‌شود و تغییر مالکیت قطعی است.
بی‌نیاز از اعتماد (Trustless)	سیستمی که در آن لازم نیست به هیچ طرف واحدی اعتماد کنید، چون هر کسی می‌تواند قوانین را بررسی کند. معنایش این نیست که هیچ اعتمادی لازم نیست.

نکات کلیدی

1. پول دیجیتال یک رکورد است و امروزه یک واسطه این رکورد را برای ما نگه می‌دارد.
2. واسطه‌ها راحتی می‌آورند، اما کارمزد، تأخیر، کنترل دسترسی و نقطه شکست واحد هم به همراه دارند.
3. چون فایل‌های دیجیتال به‌طور کامل کپی می‌شوند، پول دیجیتال با مسئله خرج دوباره روبه‌رو است.
4. تا پیش از ۲۰۰۸، فقط یک نگه‌دارنده مرکزی سوابق می‌توانست جلوی خرج دوباره را بگیرد.
5. بلاک‌چین به طرف‌های مستقل فراوانی اجازه می‌دهد یک رکورد مشترک را نگه دارند که هر کسی می‌تواند بررسی کند، بدون اینکه کسی مسئول آن باشد.

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. وقتی از حساب بانکی خود به کسی پول می‌دهید، واقعاً چه اتفاقی می‌افتد؟

- (A) اسکناس بین خزانه‌های بانک‌ها جابه‌جا می‌شود
- (B) بانک ورودی‌های سوابق خود را به‌روز می‌کند
- (C) یک فایل سکه دیجیتال برای گیرنده فرستاده می‌شود
- (D) بانک مرکزی برای گیرنده پول تازه چاپ می‌کند

۲. مسئله خرج دوباره چیست؟

A پرداخت دو کارمزد برای یک تراکنش
B کسر شدن دو باره مبلغ به اشتباه
C خرج کردن یک پول دیجیتال بیش از یک بار، چون فایل‌های دیجیتال قابل کپی هستند
D ارسال هم‌زمان پول به دو بانک

۳. پیش از سال ۲۰۰۸، سیستم‌های پرداخت دیجیتال معمولاً چگونه جلوی خرج دوباره را می‌گرفتند؟

A با تکیه بر یک مرجع مرکزی که سوابق رسمی را نگه می‌داشت
B با محدود کردن پرداخت‌ها به مبالغ کوچک
C با استفاده از سکه‌های فیزیکی در کنار سکه‌های دیجیتال
D اصلاً نمی‌توانستند جلوی آن را بگیرند

۴. کدام یک از موارد زیر جزو هزینه‌های تکیه بر واسطه نیست؟

A کارمزد و تأخیر
B ریسک مسدود شدن حساب
C نقطه شکست واحد
D پرداخت‌هایی که هرگز قابل برگشت نیستند

۵. اگر دارایی خود را در یک صرافی نگه دارید، واقعاً چه چیزی در اختیار دارید؟

A خود دارایی‌ها که به نام شما روی بلاک‌چین ثبت شده‌اند
B طلبی از صرافی که به توان پرداخت آن بستگی دارد
C بیمه‌ای که بازپرداخت کامل را تضمین می‌کند
D نسخه‌ای از کلیدهای خصوصی صرافی

۶. در بلاک‌چین، «بی‌نیاز از اعتماد» (Trustless) به چه معناست؟

A هیچ‌کس به هیچ‌کس اعتماد ندارد، پس هیچ چیز کار نمی‌کند
B هیچ نوع اعتمادی لازم نیست
C لازم نیست به هیچ طرف واحدی اعتماد کنید، چون هر کسی می‌تواند قوانین و سوابق را بررسی کند
D فقط اعضای مورد اعتماد می‌توانند به شبکه بپیوندند

کلید پاسخ‌ها

۱ **B**

بانک ورودی‌های سوابق خود را به‌روز می‌کند

هیچ چیز فیزیکی جابه‌جا نمی‌شود. بانک در سوابق خود موجودی شما را کم و موجودی گیرنده را زیاد می‌کند. پول شما در واقع همان رکورد بانک و وعده آن برای عمل به آن است.

۲ **C**

خرج کردن یک پول دیجیتال بیش از یک بار، چون فایل‌های دیجیتال قابل کپی هستند

فایل‌های دیجیتال به‌طور کامل کپی می‌شوند، بنابراین بدون یک سازوکار محافظتی می‌شد همان پول دیجیتال را برای افراد زیادی فرستاد. جلوگیری از این، اصلی‌ترین چالش پول نقد دیجیتال است.

۳ **A**

با تکیه بر یک مرجع مرکزی که سوابق رسمی را نگه می‌داشت

یک نگه‌دارنده مرکزی سوابق تعیین می‌کرد کدام پرداخت اول بوده و کپی‌ها را رد می‌کرد. این روش کار می‌کرد، اما به این معنا بود که هر سیستمی به یک واسطه وابسته بود.

۴ **D**

پرداخت‌هایی که هرگز قابل برگشت نیستند

واسطه‌ها معمولاً می‌توانند اشتباه‌ها و تقلب‌ها را برگردانند. پرداخت‌های برگشت‌ناپذیر ویژگی و در عین حال ریسک بلاک‌چین‌ها هستند، نه واسطه‌های سنتی.

۵ **B**

طلبی از صرافی که به توان پرداخت آن بستگی دارد

شما وعده صرافی را در دست دارید. اگر صرافی مانند FTX در سال ۲۰۲۲ فرو بپاشد، این وعده ممکن است مسدود شود یا از بین برود. این همان ریسک طرف مقابل است.

۶ **C**

لازم نیست به هیچ طرف واحدی اعتماد کنید، چون هر کسی می‌تواند قوانین و سوابق را بررسی کند

یعنی لازم نیست به حرف یک نهاد واحد تکیه کنید. مقداری اعتماد باقی می‌ماند، مثلاً به نرم‌افزار و به شیوه‌ای که خودتان از کلیدهایتان محافظت می‌کنید.

منابع

- بانک جهانی، Remittance Prices Worldwide، گزارش سه‌ماهه اول ۲۰۲۵:
https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q125_1_0.pdf

Market Talks

ادامه یادگیری

درس بعدی: درس ۲
متمرکز، توزیع‌شده، غیرمتمرکز

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.