Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۸ از ۱۳

# کلیدها، آدرس‌ها و کیف پول‌ها

چه چیزی واقعاً مالکیت یک بیت‌کوین را ثابت می‌کند، برای دریافت پول چه چیزی را به اشتراک می‌گذارید، و یک کیف پول واقعاً چه نگه می‌دارد

۶ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۸ از ۱۳

# کلیدها، آدرس‌ها و کیف پول‌ها

در یک جمله

مالک بیت‌کوین بودن یعنی داشتن یک کلید خصوصی، عددی مخفی که اجازه می‌دهد پرداخت‌ها را امضا کنید. از آن یک کلید عمومی و یک آدرس به دست می‌آید که می‌توانید به اشتراک بگذارید. کیف پول اصلاً سکه نگه نمی‌دارد: کلیدها را نگه می‌دارد و با آن‌ها امضا می‌کند.

## یک راز و دو چیز که می‌توانید به اشتراک بگذارید

در درس ۵ دیدیم که بلاک‌چین هیچ نامی را نگه نمی‌دارد، فقط آدرس‌ها را. پس شبکه از کجا می‌داند یک سکه مال شماست؟ پاسخ، مجموعه‌ای از سه بخش به هم پیوسته است:

- **کلید خصوصی.** عددی مخفی که به‌طور تصادفی از میان بازه‌ای چنان بزرگ انتخاب می‌شود که ۷۸ رقم دارد، هم‌مقیاس هش‌های درس ۶. هر کسی آن را بداند می‌تواند سکه‌های مرتبط با آن را خرج کند.
- **کلید عمومی.** عددی که با نوع خاصی از ریاضیات از کلید خصوصی محاسبه می‌شود. می‌توان آن را به هر کسی نشان داد.
- **آدرس.** کدی کوتاه‌تر که از هش کردن کلید عمومی ساخته می‌شود و یک بررسی داخلی دارد که اشتباه‌های تایپی را تشخیص می‌دهد. این همان چیزی است که به دیگران می‌دهید تا به شما پول بپردازند.

هر گام فقط در یک جهت کار می‌کند. تبدیل کلید خصوصی به کلید عمومی، و کلید عمومی به آدرس، برای کامپیوتر کسری از ثانیه طول می‌کشد. برگشتن به عقب عملاً ناممکن است. به همین دلیل می‌توانید آدرستان را هر جایی منتشر کنید، بدون اینکه سکه‌هایتان در خطر بیفتند.




هر فلش کسری از ثانیه طول می‌کشد. برگشتن در جهت مخالف عملاً ناممکن است.

شکل ۱. کلید خصوصی کلید عمومی را می‌سازد و کلید عمومی آدرس را. هر گام فقط در یک جهت کار می‌کند، پس به اشتراک گذاشتن آدرس هرگز کلید خصوصی شما را فاش نمی‌کند.

## خرج کردن یعنی امضا کردن

برای خرج کردن بیت‌کوین، کیف پول شما یک تراکنش می‌سازد و یک **امضای دیجیتال** را که با کلید خصوصی‌تان ساخته شده به آن اضافه می‌کند. هر نودی می‌تواند با کلید عمومی شما آن امضا را بررسی کند و مطمئن شود که با کلید خصوصی متناظر ساخته شده، بدون اینکه هرگز خود کلید خصوصی را ببیند.

امضا همچنین به جزئیات دقیق همان یک تراکنش گره خورده است. اگر کسی مبلغ یا مقصد را حتی به اندازه یک کاراکتر تغییر دهد، امضا دیگر جور نیست و همه نودها آن را رد می‌کنند. به همین دلیل هیچ‌کس نمی‌تواند پرداخت شما را در مسیرش در شبکه رهگیری کند و به جای دیگری بفرستد.

این همان تفاوت بزرگ با بانکداری است. بانک با بررسی اینکه شما چه کسی هستید تصمیم می‌گیرد اجازه خرج کردن دارید یا نه. بیت‌کوین فقط بررسی می‌کند که امضا معتبر است یا نه. نه نامی، نه بازیابی رمز عبوری، نه پشتیبانی مشتری؛ فقط ریاضیات.

**تشبیه: صندوق پستی با شکاف**

آدرس را مثل صندوق پستی‌ای تصور کنید که جلویش یک شکاف دارد. هر کسی بداند صندوق کجاست می‌تواند نامه‌ای در آن بیندازد، و همه اهالی کوچه می‌بینند چند نامه می‌رسد. اما فقط کسی که کلید دارد می‌تواند صندوق را باز کند و نامه‌ها را بیرون بیاورد. اگر کلید را گم کنید، نامه‌ها برای همیشه داخل صندوق قفل می‌مانند. اگر کسی از کلید کپی بگیرد، می‌تواند صندوق را خالی کند.

## آدرس‌های بیت‌کوین چه شکلی دارند

بیت‌کوین چند بار قالب آدرس‌هایش را تغییر داده است. همه آن‌ها هنوز کار می‌کنند و می‌توان آن‌ها را از روی نخستین کاراکترهایشان از هم تشخیص داد:

| شروع با | نوع | سال معرفی |
|---|---|---|
| **1** | Legacy، قالب اولیه | ۲۰۰۹ |
| **3** | آدرس اسکریپتی، اغلب برای کیف پول‌های مشترک یا چندامضایی | ۲۰۱۲ |
| **bc1q** | Native SegWit، تراکنش‌های کوچک‌تر و کارمزد کمتر | ۲۰۱۷ |
| **bc1p** | Taproot، جدیدترین قالب، با حریم خصوصی و انعطاف بیشتر | ۲۰۲۱ |

بلاک‌چین‌های دیگر سبک‌های خودشان را دارند. برای مثال، آدرس‌های اتریوم با *0x* و پس از آن ۴۰ کاراکتر شروع می‌شوند. نمی‌توانید آدرس بیت‌کوین را با آدرس اتریوم عوض کنید، حتی اگر یک برنامه هر دو را نشان دهد.

یک کیف پول خوب هر بار که می‌خواهید پولی دریافت کنید، آدرس جدیدی می‌سازد. همه این آدرس‌ها متعلق به همان کیف پول هستند و آدرس‌های قدیمی هم کار می‌کنند. استفاده از آدرس‌های تازه باعث می‌شود غریبه‌ها سخت‌تر

بتوانند همه پرداخت‌های شما را به هم ربط دهند.

## کیف پول واقعاً چه چیزی نگه می‌دارد

برخلاف اسمش، کیف پول هرگز سکه نگه نمی‌دارد. سکه‌ها فقط به شکل ورودی‌هایی روی بلاک‌چین وجود دارند. **کیف پول** ابزاری است که کلیدهای شما را نگه می‌دارد، بلاک‌چین را می‌خواند تا موجودی‌تان را نشان دهد، تراکنش می‌سازد و آن‌ها را امضا می‌کند.

کیف پول‌ها به دو گروه کلی تقسیم می‌شوند:

- **کیف پول‌های گرم** کلیدها را روی دستگاهی متصل به اینترنت نگه می‌دارند، مثل یک برنامه موبایل یا نرم‌افزار دسکتاپ. برای استفاده روزمره راحت‌اند، اما کلیدها در معرض هر چیزی هستند که بتواند به آن دستگاه حمله کند.
- **کیف پول‌های سرد** کلیدها را آفلاین نگه می‌دارند. **کیف پول سخت‌افزاری** دستگاه کوچکی است که کلیدها را درون خودش نگه می‌دارد و تراکنش‌ها را بدون اینکه هرگز کلیدها را به کامپیوترتان نشان دهد امضا می‌کند. استفاده از آن کندتر است، اما هک کردنش بسیار سخت‌تر است.

اگر سکه‌هایتان در صرافی است، کلیدها دست صرافی است، نه شما. درس ۱۰ این دو انتخاب را مقایسه می‌کند و درس ۹ به نسخه پشتیبانی می‌پردازد که همه کلیدهای شما را یک‌جا محافظت می‌کند.

یک نمونه واقعی: هارد دیسکی در زباله‌دان

در سال ۲۰۱۳، جیمز هاولز، مهندس کامپیوتری در ولز، به‌اشتباه هارد دیسک قدیمی‌ای را دور انداخت که کلید خصوصی ۸۰۰۰ بیت‌کوینی را که سال‌ها قبل استخراج کرده بود در خود داشت. هارد به زباله‌دان شهر رسید. او بیش از یک دهه تلاش کرد تا اجازه حفاری آن را بگیرد. در ژانویه ۲۰۲۵ یک دادگاه بریتانیا دعوای او را رد کرد و درخواست تجدیدنظرش هم در مارس همان سال رد شد. سکه‌ها هنوز روی بلاک‌چین هستند؛ همه آن‌ها را می‌بینند و هیچ‌کس نمی‌تواند خرجشان کند.

## چرا این برای تریدرها مهم است

- **هر بار کل آدرس را بررسی کنید.** در کلاهبرداری مسموم‌سازی آدرس، مهاجمان یک تراکنش بسیار کوچک از آدرسی می‌فرستند که تقریباً شبیه آدرسی است که شما استفاده می‌کنید، به این امید که دفعه بعد آن را از تاریخچه‌تان کپی کنید. در مه ۲۰۲۴، یک تریدر ۱۱۵۵ بیت‌کوین رپ‌شده (WBTC) به ارزش حدود ۶۸ میلیون دلار به چنین آدرسی فرستاد. مهاجم بعدها پس از مذاکره بیشتر آن را برگرداند، که اتفاقی بسیار نادر است.
- **شبکه را هم چک کنید، نه فقط آدرس را.** صرافی‌ها اغلب یک رمزارز را روی چند شبکه پشتیبانی می‌کنند. فرستادن روی شبکه‌ای که طرف گیرنده از آن پشتیبانی نمی‌کند می‌تواند بازگرداندن دارایی را بسیار سخت یا ناممکن کند. پیش از تأیید، شبکه و هر مِمو یا تگ لازم را بررسی کنید.
- **اول یک مبلغ آزمایشی کوچک بفرستید.** برای انتقال‌های بزرگ یا نخستین انتقال، یک پرداخت آزمایشی کوچک کمی کارمزد دارد اما می‌تواند کل مبلغ را نجات دهد. بسیاری از تریدرها همچنین در حساب صرافی‌شان از فهرست سفید آدرس‌های برداشت استفاده می‌کنند.

## اصطلاحات کلیدی

| | |
|---|---|
| **کلید خصوصی** | عددی تصادفی و مخفی که به دارنده‌اش اجازه می‌دهد تراکنش امضا کند و سکه‌های مرتبط با آن را خرج کند. |
| **کلید عمومی** | عددی که از کلید خصوصی محاسبه می‌شود، می‌توان آن را به اشتراک گذاشت و برای بررسی امضاها به کار می‌رود. |
| **آدرس** | کدی کوتاه‌تر که از کلید عمومی ساخته می‌شود و آن را به اشتراک می‌گذارید تا دیگران برایتان سکه بفرستند. |
| **امضای دیجیتال** | مدرکی که با کلید خصوصی ساخته می‌شود و یک تراکنش مشخص را تأیید می‌کند، و هر کسی می‌تواند آن را با کلید عمومی بررسی کند. |
| **کیف پول** | ابزاری که کلیدهای شما را نگه می‌دارد، موجودی‌تان را از روی بلاک‌چین نشان می‌دهد و تراکنش می‌سازد و امضا می‌کند. |
| **کیف پول سخت‌افزاری** | دستگاه کوچکی که کلیدهای خصوصی را آفلاین نگه می‌دارد و بدون نشان دادن کلیدها به کامپیوتر، تراکنش امضا می‌کند. |

## نکات کلیدی

1. مالک بیت‌کوین بودن یعنی کنترل یک کلید خصوصی. هر کسی کلید را داشته باشد می‌تواند سکه‌ها را خرج کند.

2. کلید عمومی و آدرس از کلید خصوصی محاسبه می‌شوند و هیچ‌کدام را نمی‌توان دوباره به آن برگرداند.
3. خرج کردن به امضای دیجیتالی نیاز دارد که به همان تراکنش دقیق گره خورده و هر نودی بدون دیدن کلید خصوصی می‌تواند بررسی‌اش کند.
4. آدرس‌های بیت‌کوین بسته به نوعشان با 1، 3، bc1q یا bc1p شروع می‌شوند و کیف پول می‌تواند برای هر پرداخت آدرس تازه‌ای بسازد.
5. کیف پول‌ها کلید نگه می‌دارند، نه سکه. کیف پول‌های گرم راحت‌اند، اما کیف پول‌های سرد کلیدها را آفلاین و بسیار امن‌تر نگه می‌دارند.

## 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. چه چیزی به کسی قدرت خرج کردن بیت‌کوین را می‌دهد؟**

A دانستن آدرس
B داشتن کلید خصوصی
C داشتن حساب در یک صرافی
D دانستن شناسه تراکنش

**۲. چرا به اشتراک گذاشتن عمومی آدرس امن است؟**

A چون آدرس‌ها پس از یک بار استفاده منقضی می‌شوند
B چون شبکه آدرس را از دیگران پنهان می‌کند
C چون هیچ‌کس نمی‌تواند از آدرس به کلید خصوصی برسد
D چون آدرس‌ها رمزگذاری شده‌اند

**۳. اگر کسی مبلغ یک تراکنش امضاشده را تغییر دهد چه می‌شود؟**

A امضا دیگر جور نیست و نودها آن را رد می‌کنند
B تراکنش با مبلغ جدید انجام می‌شود
C امضا خودکار به‌روز می‌شود
D ماینر تصمیم می‌گیرد کدام مبلغ استفاده شود

**۴. یک کیف پول کریپتو در واقع چه چیزی را نگه می‌دارد؟**

A سکه‌های شما را

B یک نسخه از کل بلاک‌چین را

C اطلاعات بانکی شما را

D کلیدهای شما را

**۵. یک آدرس بیت‌کوین با bc1q شروع می‌شود. از چه نوعی است؟**

A Legacy

B Native SegWit

C اتریوم

D Taproot

**۶. مزیت اصلی کیف پول سخت‌افزاری چیست؟**

A تراکنش‌ها را سریع‌تر می‌کند

B همه کارمزدها را حذف می‌کند

C کلیدهای خصوصی را آفلاین نگه می‌دارد و بدون فاش کردنشان امضا می‌کند

D اجازه می‌دهد سکه‌هایی را که به آدرس اشتباه فرستاده‌اید پس بگیرید

# کلید پاسخ‌ها

۱ B

**داشتن کلید خصوصی**

کلید خصوصی است که پرداخت‌ها را امضا می‌کند. هر کسی آن را داشته باشد می‌تواند سکه‌ها را خرج کند، به همین دلیل باید مخفی بماند.

۲ C

**چون هیچ‌کس نمی‌تواند از آدرس به کلید خصوصی برسد**

هر گام از کلید خصوصی به کلید عمومی و به آدرس یک‌طرفه است. دیگران می‌توانند به آدرس شما پول بفرستند، اما نمی‌توانند از آن برای پیدا کردن کلید خصوصی‌تان استفاده کنند.

۳ A

**امضا دیگر جور نیست و نودها آن را رد می‌کنند**

امضا به جزئیات دقیق یک تراکنش گره خورده است. هر تغییری، حتی یک کاراکتر، آن را نامعتبر می‌کند.

۴ D

**کلیدهای شما را**

سکه‌ها فقط روی بلاک‌چین وجود دارند. کیف پول کلیدهای شما را نگه می‌دارد، موجودی‌تان را از زنجیره می‌خواند و تراکنش‌هایتان را امضا می‌کند.

۵ B

**Native SegWit**

آدرس‌هایی که با bc1q شروع می‌شوند Native SegWit هستند و در ۲۰۱۷ معرفی شدند. آدرس‌های Taproot با bc1p و آدرس‌های Legacy با 1 شروع می‌شوند.

۶ C

**کلیدهای خصوصی را آفلاین نگه می‌دارد و بدون فاش کردنشان امضا می‌کند**

کیف پول سخت‌افزاری کلیدها را درون دستگاه نگه می‌دارد و فقط تراکنش‌های امضاشده را بیرون می‌فرستد، پس بدافزار روی کامپیوتر شما نمی‌تواند کلیدها را بخواند.

منابع


- ساتوشی ناکاموتو، (۲۰۰۸) Bitcoin: A Peer-to-Peer Electronic Cash System :https://bitcoin.org/bitcoin.pdf
- ویکی‌پدیا، بیت‌کوین‌های دفن‌شده در زباله‌دان نیوپورت: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph، تریدری که ۶۸ میلیون دلار در کلاهبرداری مسموم‌سازی آدرس از دست داد (مه ۲۰۲۴): https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph، بازگرداندن دارایی‌ها پس از مذاکره: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

ادامه یادگیری

# درس بعدی: درس ۹
# عبارت بازیابی و نسخه پشتیبان

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.