Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۹ از ۱۳

عبارت بازیابی و نسخه پشتیبان

۱۲ یا ۲۴ کلمه‌ای که می‌توانند کل کیف پول شما را دوباره بسازند، چطور امن نگهشان دارید، و چه کسانی برای به دست آوردنشان تلاش می‌کنند

۶ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۹ از ۱۳

عبارت بازیابی و نسخه پشتیبان

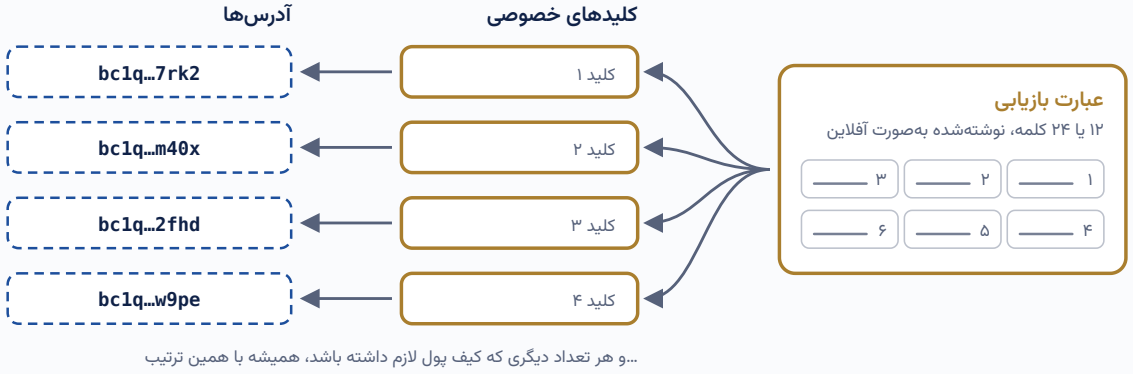
در یک جمله

عبارت بازیابی (seed phrase) فهرستی از ۱۲ یا ۲۴ کلمه معمولی است که می‌تواند همه کلیدهای خصوصی کیف پول شما را دوباره بسازد. اگر نگهش دارید، می‌توانید پس از گم شدن یا خرابی دستگاه همه چیز را بازیابی کنید. اگر لو برود، هر کسی می‌تواند همه چیز را ببرد و راه برگشتی هم وجود ندارد.

یک نسخه پشتیبان برای همه کلیدها

در درس ۸ دیدیم که کیف پول برای هر پرداخت یک آدرس تازه می‌سازد و هر آدرس از کلید خصوصی خودش می‌آید. پشتیبان گرفتن از ده‌ها کلید جداگانه کابوس می‌شد. کیف پول‌های امروزی این مشکل را این‌طور حل می‌کنند که همه کلیدهایشان را از یک عدد آغازین واحد می‌سازند که به آن **سید** (seed، به معنای بذر) می‌گویند.

سید فقط یک بار، هنگام راه‌اندازی اولیه کیف پول، به شکل فهرستی از ۱۲ یا ۲۴ کلمه به شما نشان داده می‌شود. این همان **عبارت بازیابی** شماست که به آن سید فریز هم می‌گویند. همان کلمه‌ها را تقریباً در هر برنامه کیف پول امروزی وارد کنید، دقیقاً همان کلیدها را با همان ترتیب دوباره می‌سازد و همان سکه‌ها را پیدا می‌کند. گوشی یا دستگاه سخت‌افزاری ممکن است گم شود، دزدیده شود یا خراب شود. تا وقتی کلمه‌ها را دارید، بیت‌کوین‌هایتان از دست نرفته‌اند.



شکل ۱. یک عبارت بازیابی همه کلیدهای خصوصی کیف پول را می‌سازد و هر کلید یک آدرس می‌دهد. عبارت را در هر کیف پول سازگاری بازیابی کنید، همان کلیدها و سکه‌ها برمی‌گردند.

تشبیه: نگاتیو عکس

در دوران دوربین‌های فیلمی، نگاتیو از هر عکس چاپی ارزشمندتر بود. اگر عکسی گم می‌شد، می‌شد از روی نگاتیو هر چند بار که بخواهید و در هر عکاسی دوباره چاپش کرد. عبارت بازیابی نگاتیو کیف پول شماست. برنامه روی گوشی‌تان فقط یکی از چاپ‌هاست. اما هر کس دیگری هم که نگاتیو را داشته باشد می‌تواند چاپ‌های خودش را بگیرد.

چرا کلمه، و چرا همین کلمه‌ها

در پشت صحنه، سید فقط یک عدد تصادفی بسیار بزرگ است. نوشتن آن به شکل ۶۴ کاراکتر از ارقام و حروف یعنی دعوت به اشتباه، پس یک استاندارد پرکاربرد آن را به کلمه‌هایی از یک فهرست ثابت شامل ۲۰۴۸ کلمه ساده انگلیسی تبدیل می‌کند. هر کلمه نماینده بخشی از آن عدد است.

این فهرست با دقت ساخته شده است. در نسخه انگلیسی، هیچ دو کلمه‌ای چهار حرف اولشان یکسان نیست، پس حتی اگر انتهای کلمه پاک شده باشد هنوز خوانا است. کلمه آخر هم مثل یک بررسی داخلی عمل می‌کند: اگر یک کلمه را اشتباه بنویسید، کیف پول معمولاً هشدار می‌دهد که عبارت نامعتبر است، به جای اینکه بی‌صدا یک کیف پول خالی باز کند.

کلمه‌ها را کیف پول به‌طور تصادفی انتخاب می‌کند، نه شما. نکته اصلی همین است. یک عبارت ۱۲ کلمه‌ای می‌تواند یکی از حدود ۳۴۰ میلیارد میلیارد میلیارد میلیارد ترکیب باشد، عددی ۳۹ رقمی. عبارتی که خودتان ساخته باشید، یا بیتی از یک ترانه، به‌سرعت توسط برنامه‌هایی که میلیون‌ها عبارت رایج را امتحان می‌کنند حدس زده می‌شود.

بعضی کیف پول‌ها اجازه می‌دهند یک رمز اضافه اختیاری هم اضافه کنید که اغلب به آن passphrase می‌گویند. با آن، ۱۲ یا ۲۴ کلمه به‌تنهایی برای باز کردن کیف پول کافی نیستند. این کار محافظت را بیشتر می‌کند، اما اگر این رمز را فراموش کنید، کلمه‌ها هم کمکی نمی‌کنند.

نگهداری: آفلاین، بادوام، قابل پیدا کردن

یک نسخه پشتیبان خوب باید از سه خطر جان سالم به در ببرد: دزدها، حوادثی مثل آتش یا آب، و حافظه خودتان سال‌ها بعد. گزینه‌های رایج این‌طور با هم مقایسه می‌شوند:

کجا	در برابر چه مقاوم است	در برابر چه آسیب‌پذیر است
نوشته روی کاغذ، در خانه	هکرها، چون هرگز به اینترنت وصل نمی‌شود	آتش، آب و هر کسی که پیدایش کند
حک‌شده روی صفحه فلزی	هکرها، آتش و آب	هر کسی که پیدایش کند، مگر اینکه خوب پنهان شده باشد
نسخه دوم در جای دیگر، مثل صندوق امانات بانک	از دست رفتن تنها نسخه در یک حادثه	نسخه‌های بیشتر یعنی جاهای بیشتر برای لو رفتن
عکس، اسکرین‌شات، یادداشت، ایمیل یا فضای ابری	هیچ چیزی که کاغذ بهتر از عهده‌اش برنیاید	هک شدن حساب‌ها، پشتیبان‌های همگام‌شده و بدافزارهایی که تصاویر را می‌کاوند

هر کدام را که انتخاب کنید، کلمه‌ها را به ترتیب بنویسید، شماره‌گذاری کنید و تک‌تک را با صفحه نمایش مقایسه کنید. بعد یک تمرین بازیابی انجام دهید: در حالی که فقط مبلغ کمی در کیف پول است، آن را پاک کنید یا از دستگاه دیگری استفاده کنید، کلمه‌ها را دوباره وارد کنید و مطمئن شوید همان آدرس‌ها ظاهر می‌شوند. پیدا کردن اشتباه در این مرحله ارزان است. پیدا کردنش در شرایط اضطراری نه.

هیچ آدم درستکاری آن را از شما نمی‌خواهد

چون عبارت بازیابی همه چیز را باز می‌کند، هدف اصلی کلاهبرداری‌های کریپتویی است. ترفندها متفاوت‌اند، اما درخواست همیشه یکی است: کلمه‌هایتان را جایی وارد کنید. ممکن است به شکل یک پشتیبان در پیام‌هایتان بیاید، یک پنجره بازشو که می‌گوید کیف پولتان باید «همگام‌سازی» یا «تأیید» شود، یک برنامه کیف پول جعلی در فروشگاه برنامه‌ها، یا سایتی که وعده ایردراپ رایگان می‌دهد.

قاعده ساده است و هیچ استثنایی ندارد. عبارت بازیابی فقط و فقط در کیف پول خودتان، و وقتی خودتان در حال بازیابی آن هستید، وارد می‌شود. هیچ شرکت کیف پول، صرافی، برنامه‌نویس یا ادمین کانالی هرگز به آن نیاز ندارد.

یک نمونه واقعی: کیف پول‌های «جایگزین» جعلی

در سال ۲۰۲۰ به پایگاه داده شرکت سازنده کیف پول سخت‌افزاری Ledger نفوذ شد و در دسامبر نام، آدرس منزل و شماره تلفن حدود ۲۷۲ هزار مشتری در اینترنت منتشر شد. ماه‌ها بعد، برخی مشتریان بسته‌ای با بسته‌بندی‌ای شبیه بسته‌بندی اصلی Ledger دریافت کردند، همراه با نامه‌ای که می‌گفت دستگاهشان ناامن است و یک «جایگزین» داخل بسته است. دستورالعمل از آن‌ها می‌خواست عبارت بازیابی‌شان را وارد کنند. دستگاه دستکاری شده بود و کلمه‌ها مستقیم به دست دزدها می‌رسید.

چرا این برای تریدرها مهم است

- **گروه‌های ترید شکارگاه هستند.** کلاهبرداران وارد گروه‌های شلوغ کریپتو می‌شوند، نام و عکس ادمین‌ها را کپی می‌کنند و به افراد پیام خصوصی می‌دهند و کمک یا «بررسی کیف پول» پیشنهاد می‌کنند. MARKET TALKS هرگز عبارت بازیابی، کلیدهای خصوصی یا رمزهای عبور شما را نمی‌خواهد و هیچ تیم واقعی دیگری هم نمی‌خواهد.
- **حساب صرافی شما هم رازهای مشابه خودش را دارد.** حساب‌های صرافی عبارت بازیابی ندارند، اما کدهای پشتیبان احراز هویت دومرحله‌ای نقش مشابهی دارند. اگر کسی آن‌ها را همراه با رمز عبورتان به دست بیاورد، می‌تواند حساب را تصاحب کند. آن‌ها را هم مثل عبارت بازیابی آفلاین نگه دارید.
- **به کسانی که بعد از شما می‌مانند فکر کنید.** پژوهشگران تخمین می‌زنند میلیون‌ها بیت‌کوین برای همیشه از دست رفته‌اند، بسیاری به این دلیل که تنها کسی که کلیدها را می‌دانست فوت کرد یا فراموششان کرد. اگر مبالغ قابل توجهی دارید، فکر کنید یک فرد مورد اعتماد چطور می‌تواند روزی آن‌ها را بازیابی کند، بدون اینکه امروز به کسی دسترسی بدهید.

اصطلاحات کلیدی

سید	عدد تصادفی بزرگ و واحدی که کیف پول همه کلیدهای خصوصی‌اش را از آن می‌سازد.
عبارت بازیابی	سید که به شکل ۱۲ یا ۲۴ کلمه نوشته شده است. می‌تواند همه کلیدهای کیف پول را دوباره بسازد. به آن سید فریز هم می‌گویند.
فهرست کلمات	فهرست ثابت ۲۰۴۸ کلمه‌ای که عبارت‌های بازیابی از آن انتخاب می‌شوند، تا هر کیف پول سازگاری بتواند آن‌ها را بخواند.
چک‌سام	بررسی داخلی‌ای که در کلمه آخر قرار دارد و به کیف پول کمک می‌کند بفهمد عبارت اشتباه نوشته شده است.
Passphrase	رمز اضافه اختیاری که به عبارت بازیابی افزوده می‌شود. بدون آن، کلمه‌ها به‌تنهایی کیف پول را باز نمی‌کنند.
تمرین بازیابی	امتحان کردن بازیابی با عبارت بازیابی نوشته‌شده، پیش از اینکه پول قابل توجهی در کیف پول بگذارید.

نکات کلیدی

1. کیف پول‌های امروزی همه کلیدها را از یک سید می‌سازند که به شکل عبارت بازیابی ۱۲ یا ۲۴ کلمه‌ای به شما نشان داده می‌شود.

2. با عبارت بازیابی می‌توانید کیف پولتان را روی دستگاه جدیدی دوباره بسازید، حتی اگر دستگاه قبلی گم یا خراب شده باشد.
3. کلمه‌ها از فهرستی ثابت شامل ۲۰۴۸ کلمه می‌آیند، کیف پول آن‌ها را تصادفی انتخاب می‌کند و کلمه آخر برای کشف اشتباه‌ها به کار می‌رود.
4. عبارت را آفلاین و روی چیزی بادوام نگه دارید، هرگز در عکس، یادداشت، ایمیل یا فضای ابری، و بازیابی را با مبلغی کم امتحان کنید.
5. هر کسی عبارت بازیابی‌تان را بخواهد قصد دزدی دارد. این عبارت فقط در کیف پول خودتان وارد می‌شود.

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. عبارت بازیابی چه کاری می‌تواند انجام دهد؟

A. رمز عبور صرافی را بازنشانی کند
B. همه کلیدهای خصوصی کیف پولتان را دوباره بسازد
C. تراکنش‌هایتان را سریع‌تر کند
D. پرداختی را که فرستاده‌اید لغو کند

۲. گوشی‌ای که برنامه کیف پولتان روی آن است دزدیده می‌شود. عبارت بازیابی را نوشته‌اید. چه باید بکنید؟

A. کیف پول را با عبارت بازیابی روی دستگاه دیگری بازیابی کنید
B. با پشتیبانی بیت‌کوین تماس بگیرید
C. بپذیرید که سکه‌ها از دست رفته‌اند
D. از صرافی بخواهید دزدی را برگرداند

۳. چرا نباید عبارت بازیابی را از جمله محبوبتان بسازید؟

A. کیف پول‌ها نمی‌توانند جمله بخوانند
B. تراکنش‌ها را کندتر می‌کند
C. عبارت‌هایی که آدم‌ها می‌سازند را برنامه‌ها به‌راحتی حدس می‌زنند
D. جمله‌ها حق نشر دارند

۴. امن‌ترین روش نگهداری عبارت بازیابی کدام است؟

A اسکرین‌شات در گالری عکس
B یادداشتی در پیش‌نویس‌های ایمیل
C فایلی در فضای ابری
D نوشته یا حک‌شده به‌صورت آفلاین، در جایی امن از آتش و دزدی

۵. کلمه آخر عبارت بازیابی به چه کاری می‌آید؟

A رمز عبور کیف پول را تعیین می‌کند
B مثل یک بررسی عمل می‌کند که بیشتر اشتباه‌های نوشتن را می‌گیرد
C تعیین می‌کند کیف پول کدام رمزارز را نگه دارد
D موجودی کیف پول را نشان می‌دهد

۶. کسی در یک گروه ترید به شما پیام می‌دهد و پیشنهاد می‌کند اگر عبارت بازیابی را بدهید کیف پولتان را درست کند. چه خبر است؟

A این یک روال عادی پشتیبانی است
B برای بررسی موجودی شما به آن نیاز دارد
C کلاهبرداری است، چون هیچ کمک‌کننده واقعی‌ای به عبارت بازیابی شما نیاز ندارد
D دارد هویت شما را تأیید می‌کند

کلید پاسخ‌ها

۱ **B**

همه کلیدهای خصوصی کیف پولتان را دوباره بسازد

عبارت بازیابی شکل نوشته‌شده سیدی است که همه کلیدهای شما از آن ساخته می‌شوند. هر کیف پول سازگاری می‌تواند با آن همان کلیدها را دوباره بسازد و همان سکه‌ها را پیدا کند.

۲ **A**

کیف پول را با عبارت بازیابی روی دستگاه دیگری بازیابی کنید

سکه‌ها روی بلاک‌چین هستند، نه در گوشی. بازیابی با عبارت بازیابی کنترل را به شما برمی‌گرداند و انتقال فوری دارایی به یک کیف پول جدید از آن محافظت می‌کند.

۳ **C**

عبارت‌هایی که آدم‌ها می‌سازند را برنامه‌ها به‌راحتی حدس می‌زنند

امنیت از اینجا می‌آید که کلمه‌ها به‌طور تصادفی از میان تعداد عظیمی ترکیب انتخاب می‌شوند. عبارت‌هایی که آدم‌ها انتخاب می‌کنند بسیار قابل پیش‌بینی‌ترند.

۴ **D**

نوشته یا حک‌شده به‌صورت آفلاین، در جایی امن از آتش و دزدی

هر چیزی که روی حساب یا دستگاهی متصل به اینترنت باشد، در دسترس هکرها یا بدافزار است. یک نسخه آفلاین و بادوام این خطر را از بین می‌برد.

۵ **B**

مثل یک بررسی عمل می‌کند که بیشتر اشتباه‌های نوشتن را می‌گیرد

بخشی از کلمه آخر از روی بقیه کلمه‌ها محاسبه می‌شود، پس اگر یک کلمه اشتباه نوشته شود، کیف پول معمولاً می‌گوید عبارت نامعتبر است.

۶ **C**

کلاهبرداری است، چون هیچ کمک‌کننده واقعی‌ای به عبارت بازیابی شما نیاز ندارد

با عبارت بازیابی شما می‌شود همه چیز را از کیف پول برد. تیم‌های پشتیبانی واقعی هرگز آن را نمی‌خواهند، پس خود این درخواست ثابت می‌کند کلاهبرداری است.

منابع

- پیشنهاد بهبود بیت‌کوین ۳۹، کد یادیار برای ساخت کلیدها (GitHub): https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- BleepingComputer، ارسال دستگاه‌های دستکاری‌شده Ledger برای سرقت رمزارز: https://www.bleepingcomputer.com/news/cryptocurrency/criminals-are-mailing-altered-ledger-devices-to-steal-cryptocurrency
- Cointelegraph، تا چهار میلیون بیت‌کوین ممکن است برای همیشه از دست رفته باشد (تخمین Chainalysis): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

ادامه یادگیری

درس بعدی: درس ۱۰
نگهداری: حساب صرافی یا کیف پول شخصی

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.