Market Talks
مرکز آموزش

بلاک‌چین · مبتدی · درس ۱۰ از ۱۳

نگهداری دارایی: حساب صرافی یا کیف پول خودتان

چه کسی واقعاً سکه‌های شما را نگه می‌دارد، تاریخ درباره هر دو انتخاب چه می‌گوید، و بیشتر تریدرها چطور حد وسط را انتخاب می‌کنند

۵ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۱۰ از ۱۳

نگهداری دارایی: حساب صرافی یا کیف پول خودتان

در یک جمله

نگه داشتن کریپتو در صرافی یعنی کلیدها دست صرافی است و شما فقط یک قول در دست دارید. نگه داشتن آن در کیف پول خودتان یعنی کلیدها و تمام مسئولیت با شماست. هر انتخاب شما را در برابر ریسک‌های متفاوتی محافظت می‌کند.

دو راه برای نگه داشتن یک بیت‌کوین

نگهداری دارایی (custody) به زبان ساده یعنی کلیدهای خصوصی دست چه کسی است. دو مدل اصلی وجود دارد:

- **امانی (کاستودیال).** یک صرافی یا شرکت دیگر کلیدها را نگه می‌دارد. شما با رمز عبور وارد می‌شوید و موجودی‌تان عددی در پایگاه داده خود شرکت است، همان‌طور که در درس ۵ دیدیم. وقتی برداشت می‌کنید، شرکت تراکنش را به جای شما امضا می‌کند.
- **نگهداری شخصی.** کلیدها دست خودتان است، معمولاً در کیف پولی که با عبارت بازیابی درس ۹ پشتیبان‌گیری شده. هیچ‌کس نمی‌تواند سکه‌های شما را جابه‌جا کند یا جلوی جابه‌جا کردنشان را بگیرد، اما اگر کلیدها را گم کنید هم هیچ‌کس نمی‌تواند نجاتتان دهد.

روی بلاک‌چین چیزی به نام «حساب شما» در صرافی وجود ندارد. آدرس‌های صرافی سکه‌های همه را با هم نگه می‌دارند و پایگاه داده‌اش ثبت می‌کند چه سهمی از این انبوه به هر مشتری تعلق دارد.



شکل ۱. با حساب صرافی، شرکت کلیدها را نگه می‌دارد و شما از طریق آن به بلاک‌چین می‌رسید. با کیف پول خودتان، کلیدها دست شماست و مستقیماً با بلاک‌چین سروکار دارید.

تشبیه: رخت‌کن

در یک مراسم شلوغ، کتتان را به رخت‌کن می‌دهید و یک ژتون شماره‌دار می‌گیرید. راحت است و معمولاً کتتان برمی‌گردد. اما در طول شب، چیزی که در دست دارید ژتون است، نه کت. اگر رخت‌کن دزد بزند، زودتر تعطیل شود یا یواشکی کت‌ها را به دیگران قرض داده باشد، ژتون شما فقط به اندازه آدم‌های پشت پیشخوان ارزش دارد. پوشیدن کت راحتی کمتری دارد، اما هیچ‌کس دیگری نمی‌تواند گمش کند.

تاریخ درباره صرافی‌ها چه می‌گوید

بیشتر صرافی‌ها هرگز ورشکست نمی‌شوند. اما وقتی صرافی‌های بزرگ سقوط کرده‌اند، مشتریان سال‌ها منتظر مانده‌اند و اغلب بخش بزرگی از پولشان را از دست داده‌اند:

صرافی	چه اتفاقی افتاد	مشتریان با چه روبه‌رو شدند
Mt. Gox (۲۰۱۴)	بزرگ‌ترین صرافی بیت‌کوین زمان خودش حدود ۸۵۰٬۰۰۰ بیت‌کوین را بر اثر سرقت و سوءمدیریت از دست داد	بازپرداخت باقی‌مانده دارایی‌ها تازه در ژوئیه ۲۰۲۴، ده سال بعد، آغاز شد
QuadrigaCX (۲۰۱۹)	بنیان‌گذار درگذشت و کیف پول‌های سردی که فقط خودش کنترل می‌کرد تقریباً خالی از آب درآمدند	حدود ۷۶ هزار کاربر حدود ۲۱۵ میلیون دلار کانادا طلبکار بودند
FTX (۲۰۲۲)	پول مشتریان را یک شرکت ترید وابسته خرج کرده بود و برداشت‌ها در عرض چند روز متوقف شد	میلیاردها دلار از دارایی مشتریان ناپدید شده بود و بنیان‌گذار بعدها به کلاهبرداری محکوم شد

در هر سه مورد، صفحه‌ها تا آخرین لحظه موجودی‌های عادی نشان می‌دادند. موجودی در صرافی یک طلب از شرکت است، نه مدرکی بر اینکه سکه‌ها واقعاً آنجا هستند.

ریسک‌های نگهداری شخصی

نگهداری شخصی شرکت را از ماجرا حذف می‌کند، اما همه کارها را به شما می‌سپارد. رایج‌ترین راه‌هایی که آدم‌ها خودشان سکه‌هایشان را از دست می‌دهند این‌هاست:

- **گم کردن نسخه پشتیبان.** عبارت بازیابی گم‌شده و دستگاه خراب یعنی سکه‌ها برای همیشه قفل شده‌اند. پژوهشگران Chainalysis در سال ۲۰۱۷ تخمین زدند که بین حدود ۲٫۸ تا ۳٫۸ میلیون بیت‌کوین به همین شکل از دست رفته، یعنی تقریباً یک‌پنجم همه سکه‌هایی که تا آن زمان استخراج شده بود.
- **لو رفتن نسخه پشتیبان.** عبارت بازیابی‌ای که در یک سایت یا برنامه جعلی وارد شود، همه چیز را به دزد تحویل می‌دهد، همان‌طور که درس ۹ نشان داد.
- **اشتباه در ارسال.** آدرس یا شبکه اشتباه را نمی‌شود برگرداند، همان‌طور که درس ۸ نشان داد.

نه پشتیبانی هست و نه بازیابی رمز عبور. این بهای نداشتن شرکتی است که بتواند ورشکست شود یا دارایی شما را مسدود کند.

بیشتر آدم‌ها چطور تقسیمش می‌کنند

برای خیلی‌ها پاسخ این یا آن نیست. یک رویکرد رایج این است که با صرافی مثل کیف پول جیبی رفتار کنید و با نگهداری شخصی مثل گاوصندوق خانه:

	حساب صرافی	کیف پول خودتان
کلیدها دست کیست	صرافی	شما
اگر رمز عبور را فراموش کنید	پشتیبانی معمولاً می‌تواند دسترسی را برگرداند	فقط عبارت بازیابی می‌تواند
اگر شرکت ورشکست شود	سکه‌هایتان ممکن است مسدود شوند یا از دست بروند	هیچ چیز تغییر نمی‌کند
مناسب برای	ترید فعال و مبالغی که به‌زودی لازم دارید	سرمایه‌های بلندمدت و پس‌انداز
ریسک اصلی	شرکت: هک، کلاهبرداری، مسدودسازی، ورشکستگی	خودتان: پشتیبان گم‌شده، کلاهبرداری، اشتباه

اگر دارایی‌ای در صرافی نگه می‌دارید، پلتفرم‌های بزرگ و دارای مجوز با سابقه طولانی را ترجیح دهید، همه امکانات امنیتی‌شان را فعال کنید و بررسی کنید که آیا به‌طور منظم اثبات ذخایر (proof of reserves) منتشر می‌کنند یا نه. یادتان باشد که اثبات ذخایر دارایی‌های صرافی را در یک لحظه مشخص نشان می‌دهد، اما همیشه همه بدهی‌هایش را نشان نمی‌دهد.

چرا این برای تریدرها مهم است

- **فیوچرز و مارجین به نگهداری امانی نیاز دارند.** برای ترید قراردادهای دائمی (پرپچوال)، وثیقه شما باید در صرافی باشد. به اندازه‌ای که پوزیشن‌هایتان لازم دارند آنجا نگه دارید، نه کل دارایی‌تان را، و سودهایی را که برای ترید لازم ندارید مرتب به کیف پول خودتان منتقل کنید.
- **علائم هشدار را زیر نظر بگیرید.** کند شدن یا توقف برداشت‌ها، تغییر ناگهانی سقف برداشت و خروج‌های بزرگ سکه از یک صرافی روی بلاک‌چین، بارها پیش از بروز مشکل دیده شده‌اند. در اوایل نوامبر ۲۰۲۲، برداشت‌ها از FTX کند شد و در عرض چند روز متوقف شد. واکنش به نخستین نشانه‌ها آسان‌تر از واکنش به آخرین نشانه‌هاست.
- **نگهداری شخصی هزینه‌ای از جنس سرعت دارد.** انتقال سکه از کیف پولتان به صرافی زمان و کارمزد شبکه لازم دارد و در بازار سریع دقیقه‌ها مهم‌اند. پیش از رسیدن نوسان، نه وسط آن، برنامه‌ریزی کنید که چه مقدار در هر طرف نگه دارید.

اصطلاحات کلیدی

نگهداری دارایی (custody)	کنترل کلیدهای خصوصی و در نتیجه کنترل سکه‌هایی که آن کلیدها باز می‌کنند.
امانی (کاستودیال)	حالتی که یک شرکت کلیدها را به جای شما نگه می‌دارد، مثل حساب صرافی.
نگهداری شخصی	نگه داشتن کلیدهای خودتان در کیف پولی که کنترلش با شماست، معمولاً با پشتیبان عبارت بازیابی.
ریسک طرف مقابل	ریسک اینکه شرکتی که دارایی شما را نگه می‌دارد ورشکست شود، آن را مسدود کند یا پس ندهد.
اثبات ذخایر	بررسی منتشرشده‌ای که دارایی‌های یک صرافی را در یک لحظه مشخص نشان می‌دهد و ممکن است همه بدهی‌هایش را نشان ندهد.
Not your keys, not your coins	جمله معروف «کلید مال تو نیست، سکه هم مال تو نیست». اگر کلیدها دست دیگری باشد، شما فقط قول او برای پس دادن سکه‌ها را دارید.

نکات کلیدی

1. نگهداری دارایی یعنی کلیدها دست کیست. در صرافی دست شرکت است و در نگهداری شخصی دست شما.
2. موجودی صرافی عددی در پایگاه داده شرکت و طلبی از آن است، نه سکه‌هایی تحت کنترل شما.

3. Mt. Gox، QuadrigaCX و FTX نشان می‌دهند که ورشکستگی صرافی می‌تواند دارایی مشتریان را سال‌ها مسدود کند یا به‌کلی از بین ببرد.
4. نگهداری شخصی ریسک شرکت را حذف می‌کند اما ریسک شخصی اضافه می‌کند: پشتیبان گم‌شده، عبارت بازیابی لورفته و اشتباه در ارسال.
5. بسیاری از افراد دارایی ترید را در یک صرافی معتبر و سرمایه‌های بلندمدت را در کیف پول خودشان 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. نگهداری دارایی (custody) در کریپتو یعنی چه؟

A. کلیدهای خصوصی دست چه کسی است
B. کدام صرافی کمترین کارمزد را دارد
C. چه مدت قصد دارید یک سکه را نگه دارید
D. کدام کشور بر یک سکه نظارت دارد

۲. ۱ بیت‌کوین در حساب صرافی‌تان دارید. در واقع چه چیزی در اختیار دارید؟

A. یک کلید خصوصی به نام خودتان
B. طلبی از صرافی که در پایگاه داده‌اش ثبت شده
C. سکه‌هایی در آدرسی شخصی که فقط شما کنترلش می‌کنید
D. یک کیف پول سخت‌افزاری که صرافی نگه می‌دارد

۳. دلیل اصلی اینکه مشتریان QuadrigaCX نتوانستند پولشان را پس بگیرند چه بود؟

A. شبکه بیت‌کوین از کار افتاد
B. مشتریان عبارت بازیابی‌شان را گم کردند
C. فقط بنیان‌گذار کیف پول‌ها را کنترل می‌کرد و وقتی درگذشت تقریباً خالی بودند
D. یک دولت همه صرافی‌های کانادا را مصادره کرد

۴. نگهداری شخصی کدام ریسک را حذف می‌کند؟

A ریسک گم کردن عبارت بازیابی
B ریسک ارسال به آدرس اشتباه
C ریسک فیشینگ
D ریسک اینکه صرافی سکه‌هایتان را مسدود کند یا از دست بدهد

۵. یک روش رایج برای تقسیم دارایی بین این دو مدل چیست؟

A همه چیز در صرافی برای راحتی
B دارایی ترید در یک صرافی معتبر، سرمایه بلندمدت در کیف پول خودتان
C همه چیز در نگهداری شخصی، حتی وثیقه فیوچرز
D تقسیم مساوی میان هر چه بیشتر صرافی

۶. اثبات ذخایر ممکن است چه چیزی را نشان ندهد؟

A کدام سکه‌ها را صرافی نگه می‌دارد
B آدرس‌های کیف پول صرافی
C همه آنچه صرافی به مشتریان و وام‌دهندگان بدهکار است
D تاریخ انجام بررسی

کلید پاسخ‌ها

۱ — A

کلیدهای خصوصی دست چه کسی است

هر کسی کلیدهای خصوصی را داشته باشد، سکه‌ها را کنترل می‌کند. نگهداری دارایی فقط همین پرسش است که آن شخص کیست.

۲ — B

طلبی از صرافی که در پایگاه داده‌اش ثبت شده

صرافی کلیدهای آدرس‌های مشترک را نگه می‌دارد. موجودی شما سابقه‌ای است از اینکه صرافی چقدر به شما بدهکار است.

۳ — C

فقط بنیان‌گذار کیف پول‌ها را کنترل می‌کرد و وقتی درگذشت تقریباً خالی بودند

وقتی فقط یک نفر کلیدها را کنترل می‌کرد و دارایی‌ها نادرست خرج شده بود، پس از مرگ او راهی برای بازگرداندن بیشتر پول‌ها وجود نداشت.

۴ — D

ریسک اینکه صرافی سکه‌هایتان را مسدود کند یا از دست بدهد

با کلیدهای خودتان، هیچ شرکتی نمی‌تواند سکه‌هایتان را مسدود کند، قرض بدهد یا از دست بدهد. ریسک‌های باقی‌مانده اشتباه‌های خودتان و کلاهبرداری‌ها هستند.

۵ — B

دارایی ترید در یک صرافی معتبر، سرمایه بلندمدت در کیف پول خودتان

ترید به دارایی در صرافی نیاز دارد، اما پس‌انداز در کیف پول خودتان از ریسک شرکت در امان‌تر است. هر طرف کاری را می‌کند که در آن بهتر است.

۶ — C

همه آنچه صرافی به مشتریان و وام‌دهندگان بدهکار است

اثبات ذخایر دارایی‌ها را در یک لحظه نشان می‌دهد. بدون تصویر کامل از بدهی‌ها، نمی‌تواند ثابت کند صرافی می‌تواند طلب همه را بپردازد.

منابع

- The Block، آغاز بازپرداخت بیت‌کوین Mt. Gox از ژوئیه ۲۰۲۴: https://www.theblock.co/post/301448/mt-gox-to-distribute-9-billion-of-bitcoin-bitcoin-cash-repayments-from-beginning-of-july
- Crowdfund Insider، گزارش امین QuadrigaCX: زیان ۲۱۵ میلیون دلاری ۷۶ هزار کاربر: https://www.crowdfundinsider.com/2019/05/147401-quadrigacx-trustees-final-report-finds-not-much-left-for-76-000-exchange-users-who-lost-215-million/
- ویکی‌پدیا، ورشکستگی FTX: https://en.wikipedia.org/wiki/Bankruptcy_of_FTX
- 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 ۱۱
مسیر یک تراکنش

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.