Market Talks
مرکز آموزش

کریپتو · مبتدی · درس ۱۵ از ۱۵

واقعاً چطور شروع کنیم: صرافی‌ها، احراز هویت و کیف پول‌ها

نخستین قدم‌های عملی چه شکلی دارند: انتخاب صرافی، گذراندن احراز هویت (KYC)، ایمن کردن حساب، نخستین خرید، راه‌اندازی کیف پول با نگهداری شخصی و انتقال دارایی به آن

۱۲ دقیقه مطالعه ۸ سؤال آزمون همراه با کلید پاسخ

کریپتو · مبتدی · درس ۱۵ از ۱۵

واقعاً چطور شروع کنیم: صرافی‌ها، احراز هویت و کیف پول‌ها

در یک جمله

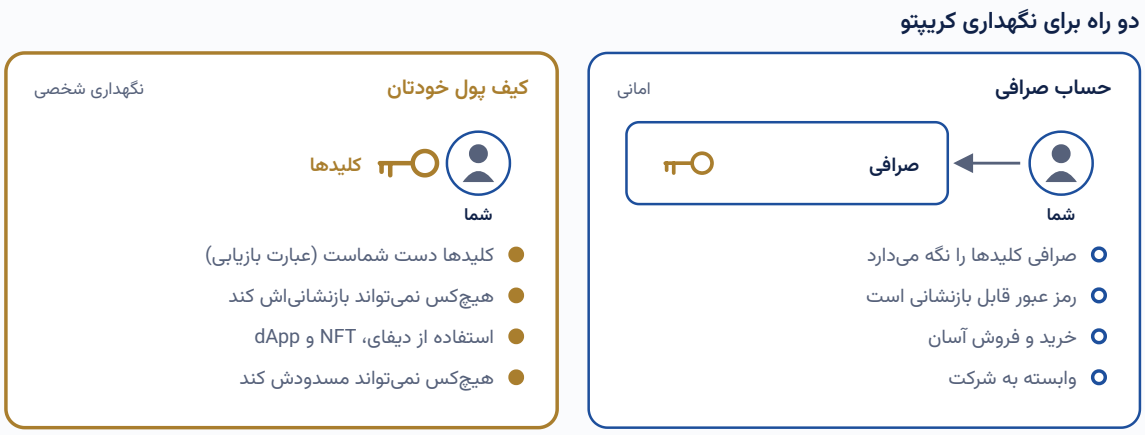
بیشتر افراد کریپتو را با یک صرافی متمرکز شروع می‌کنند و بعدها کیف پولی هم اضافه می‌کنند که کنترلش دست خودشان است. این درس قدم به قدم نشان می‌دهد هر مرحله شامل چه کاری است و اشتباه‌های رایج کجا رخ می‌دهند.

دو راه برای نگهداری کریپتو

پیش از باز کردن هر حسابی، بهتر است دو راه اصلی نگهداری کریپتو را بشناسید:

- **در صرافی (امانی یا کاستودیال):** در شرکتی مثل Binance یا Coinbase حساب باز می‌کنید. صرافی کلیدهای خصوصی را نگه می‌دارد و موجودی شما عددی در پایگاه داده آن است، مثل پول در حساب بانکی. این روش ساده است و اگر رمز عبورتان را فراموش کنید، صرافی می‌تواند کمک کند دوباره وارد حساب شوید.
- **در کیف پول خودتان (نگهداری شخصی):** کیف پولی مثل MetaMask یا یک دستگاه سخت‌افزاری مثل Ledger نصب می‌کنید. کلیدها از راه عبارت بازیابی دست خودتان است. هیچ‌کس نمی‌تواند کوین‌هایتان را مسدود کند یا به جای شما گمشان کند، اما هیچ‌کس هم نمی‌تواند آن‌ها را برایتان بازیابی کند.

جمله‌ای معروف این تفاوت را خلاصه می‌کند: **«کلید دست تو نیست، پس کوین هم مال تو نیست»** (not your keys, not your coins). بسیاری از افراد از هر دو استفاده می‌کنند: صرافی برای خرید و فروش، و کیف پول برای نگهداری و استفاده از کریپتو روی بلاک‌چین‌ها (درس‌های ۹ و ۱۲، و درس ۹ دوره بلاک‌چین).



شکل ۱. در صرافی کلیدها دست شرکت است؛ در کیف پول با نگهداری شخصی، دست خودتان.

مثال: وقتی صرافی‌ها زمین می‌خورند

در نوامبر ۲۰۲۲ صرافی FTX فروپاشید و مشتریان تا مدت‌ها نمی‌توانستند دارایی‌شان را برداشت کنند. در فوریه ۲۰۲۵ هکرهایی که FBI آن‌ها را به کره شمالی مرتبط دانست حدود **۱٫۵ میلیارد دلار** اتر از Bybit دزدیدند. Bybit برداشت‌ها را باز نگه داشت و اعلام کرد زیان مشتریان را جبران می‌کند، اما هر دو مورد یک نکته را نشان می‌دهند: کوین‌هایی که در صرافی‌اند به امنیت و صداقت همان شرکت وابسته‌اند.

انتخاب صرافی

صرافی متمرکز (درس ۹) راه معمول ورود است، جایی که پول معمولی به کریپتو تبدیل می‌شود. مواردی که افراد معمولاً مقایسه می‌کنند:

- **دسترسی و مجوز:** این‌که صرافی اجازه دارد به کاربران کشور شما خدمات بدهد یا نه، و کدام نهاد ناظر بر آن نظارت می‌کند.
- **روش‌های واریز:** انتقال بانکی، کارت یا روش‌های پرداخت محلی، و این‌که کدام ارزها پشتیبانی می‌شوند.
- **کوین‌ها و شبکه‌ها:** کدام کوین‌ها فهرست شده‌اند و کدام شبکه‌ها برای واریز و برداشت پشتیبانی می‌شوند (درس ۵).
- **کارمزدها:** کارمزد معامله، کارمزد کارت، اسپرد در «خرید فوری» و کارمزد برداشت.
- **سابقه:** تاریخچه هک یا مسدود شدن برداشت‌ها، و این‌که صرافی اثبات ذخایر منتشر می‌کند یا نه.

صرافی	ویژگی شناخته‌شده
Binance	بزرگ‌ترین صرافی جهانی از نظر حجم معاملات، با فهرست بسیار گسترده کوین‌ها
Coinbase	شرکت آمریکایی پذیرفته‌شده در بورس، اپلیکیشن ساده، پرکاربرد در آمریکا و اروپا
OKX	صرافی جهانی با کیف پول داخلی با نگهداری شخصی
Bybit	صرافی جهانی محبوب برای معاملات مشتقه
Kraken	یکی از قدیمی‌ترین صرافی‌ها، پرکاربرد در آمریکا و اروپا
Upbit	بزرگ‌ترین صرافی کره جنوبی، با معامله به وون کره

این نام‌ها نمونه‌هایی از خدمات پرکاربردند، **نه توصیه**. خدمات و قوانین تغییر می‌کنند و هر صرافی در همه کشورها در دسترس نیست. در برخی کشورها، مثل کره جنوبی، صرافی‌های داخلی افزون بر این، حساب بانکی با نام واقعی در یک بانک همکار را هم الزامی می‌کنند.

ثبت‌نام و احراز هویت (KYC)

صرافی‌های تحت نظارت باید بررسی کنند مشتریانشان چه کسانی هستند. به این کار **KYC** می‌گویند، کوتاه‌شده عبارت «مشتری‌ات را بشناس» (know your customer)، که در بیشتر کشورها بخشی از قوانین مبارزه با پولشویی (AML) است. یک ثبت‌نام معمول این‌طور پیش می‌رود:

1. **حساب:** ایمیل یا شماره تلفن و رمز عبور.
2. **اطلاعات شخصی:** نام کامل، تاریخ تولد، نشانی و ملیت.
3. **مدرک شناسایی:** عکس گذرنامه، کارت ملی یا گواهینامه رانندگی.
4. **سلفی یا احراز ویدیویی:** اپلیکیشن بررسی می‌کند که چهره با مدرک شناسایی یکی باشد و فردی واقعی پشت دوربین باشد.
5. **تأیید:** اغلب در چند دقیقه، گاهی چند روز. برخی صرافی‌ها بعداً برای سقف‌های بالاتر مدرک نشانی یا منشأ وجوه می‌خواهند.

طبق قاعده‌ای مرتبط به نام **قانون سفر** (Travel Rule)، صرافی‌ها در بسیاری از کشورها برای انتقال‌های بزرگ‌تر میان یکدیگر اطلاعات فرستنده و گیرنده را هم به اشتراک می‌گذارند و ممکن است بپرسند کیف پولی که به آن برداشت می‌کنید متعلق به چه کسی است.

KYC یعنی صرافی اطلاعات شخصی حساسی را نگه می‌دارد. این یکی از دلایلی است که واقعی بودن سایت اهمیت دارد: سایت‌های صرافی جعلی هم عکس مدارک شناسایی جمع می‌کنند (درس ۱۴).



شکل ۲. مراحل معمول KYC هنگام باز کردن حساب صرافی.

ایمن کردن حساب

حساب صرافی هدف حمله است، به همین دلیل صرافی‌ها چند لایه محافظت ارائه می‌کنند. این‌ها مواردی‌اند که معمولاً زودتر از بقیه فعال می‌شوند:

- **احراز هویت دومرحله‌ای (2FA):** کد دومی که برای ورود و برداشت لازم است. اپلیکیشن‌های احراز هویت مثل Google Authenticator، و پس‌کی‌ها (passkey) یا کلیدهای امنیتی، سخت‌تر از کدهای پیامکی دزدیده می‌شوند، چون کد پیامکی را می‌توان از راه سیم‌سواپ (SIM swap) ربود.
- **کد ضد فیشینگ:** کلمه‌ای که خودتان انتخاب می‌کنید و صرافی آن را در هر ایمیل واقعی که می‌فرستد درج می‌کند. ایمیلی که این کد را ندارد از طرف صرافی نیامده است.
- **فهرست سفید برداشت:** برداشت فقط به آدرس‌هایی مجاز است که از پیش ذخیره کرده‌اید، و برای آدرس‌های تازه اغلب یک دوره انتظار وجود دارد.
- **هشدار ورود و دستگاه:** اعلان‌هایی که وقتی کسی از دستگاه یا مکانی تازه وارد حساب می‌شود فرستاده می‌شوند.
- **رمز عبوری قوی و یکتا** که در هیچ جای دیگری استفاده نشده باشد.



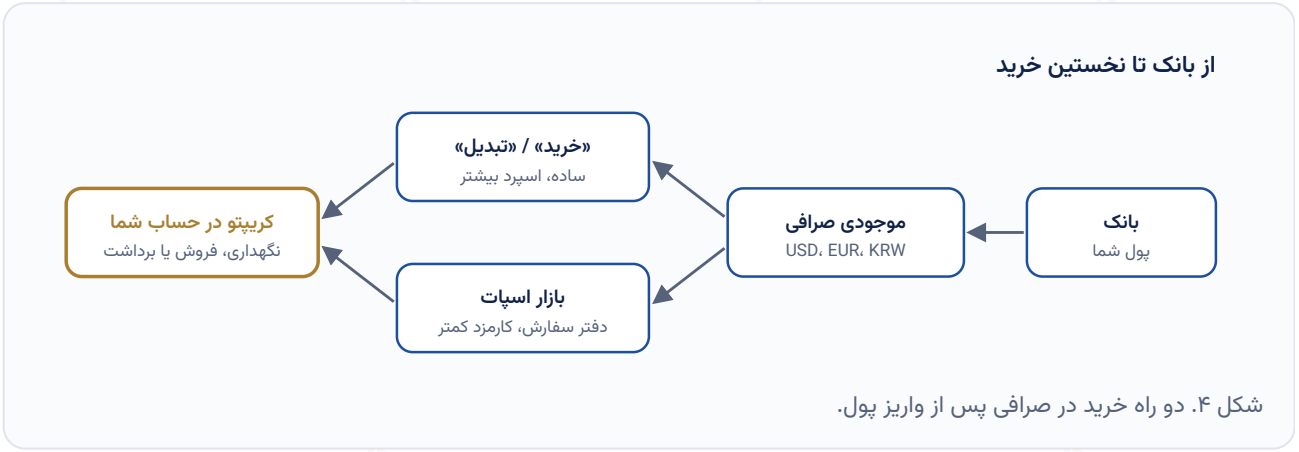
شکل ۳. صرافی‌ها چند لایه محافظت برای حساب ارائه می‌کنند.

نخستین خرید

وقتی حساب تأیید شد، پول واریز می‌شود و با کریپتو مبادله می‌شود:

- **واریز:** انتقال بانکی معمولاً ارزان‌ترین راه است. کارت سریع‌تر است اما اغلب چند درصد هزینه دارد. برخی صرافی‌ها بازار P2P (همتا به همتا) هم دارند که در آن کاربران از طریق صرافی مستقیم با یکدیگر معامله می‌کنند.
- **دکمه «خرید» یا «تبدیل»:** ساده‌ترین راه. مبلغی وارد می‌کنید و یک قیمت پیشنهادی می‌گیرید. کارمزد اغلب در اختلاف قیمت بیشتر (اسپرد) پنهان است.
- **بازار اسپات:** صفحه معامله با دفتر سفارش (درس ۹). سفارش بازار با بهترین قیمت موجود می‌خرد؛ سفارش محدود منتظر قیمت مورد نظر شما می‌ماند. کارمزدها در این‌جا معمولاً کمترند.

پس از خرید، کوین‌ها در حساب صرافی شما قرار می‌گیرند. از آن‌جا می‌توانند بمانند، فروخته شوند یا به یک کیف پول برداشت شوند.



شکل ۴. دو راه خرید در صرافی پس از واریز پول.

مثال: دو راه برای خرید

سوفی ۵۰۰ دلار با انتقال بانکی واریز می‌کند. با دکمه ساده «خرید» ۲۵۰ دلار بیت‌کوین می‌خرد و کمی کمتر از انتظارش دریافت می‌کند، چون قیمت پیشنهادی اسپردی حدود ۱٪ داشت. برای ۲۵۰ دلار دیگر از بازار اسپات با سفارش بازار استفاده می‌کند و ۰٫۱٪ کارمزد معامله می‌پردازد، یعنی حدود ۲۵ سنت. هر دو روش‌هایی عادی برای خریدند؛ تفاوت بیشتر در هزینه است و این‌که چقدر بخواهد با صفحه معامله سروکار داشته باشد.

کیف پول‌ها: گرم، سرد و نام‌های رایج

کیف پول با نگهداری شخصی اپلیکیشن یا دستگاهی است که کلیدهای شما را نگه می‌دارد و تراکنش‌ها را امضا می‌کند (درس ۹ دوره بلاک‌چین). انواع اصلی:

- **کیف پول‌های گرم** به اینترنت وصل‌اند: اپلیکیشن‌های موبایل و افزونه‌های مرورگر. رایگان‌اند و برای استفاده روزمره و اتصال به اپلیکیشن‌های دیفای راحت‌اند.

- **کیف پول‌های سرد** کلیدها را آفلاین نگه می‌دارند، معمولاً روی یک دستگاه سخت‌افزاری کوچک. تراکنش‌ها با فشار دادن دکمه‌های خود دستگاه تأیید می‌شوند، پس بدافزار روی کامپیوتر نمی‌تواند به‌تنهایی امضا کند.

کیف پول	نوع	شبکه‌های اصلی
MetaMask	افزونه مرورگر و اپلیکیشن موبایل	Ethereum و دیگر شبکه‌های EVM مثل Base، BNB Chain و Arbitrum، و اکنون Solana و Bitcoin هم
Trust Wallet	اپلیکیشن موبایل و افزونه	شبکه‌های فراوان، از جمله Ethereum، BNB Chain و Bitcoin
Phantom	اپلیکیشن موبایل و افزونه	در درجه اول Solana، و همچنین Base، Ethereum و Bitcoin
Ledger	کیف پول سخت‌افزاری	شبکه‌های فراوان، همراه با اپلیکیشن Ledger Live یا کیف پول‌های دیگر
Trezor	کیف پول سخت‌افزاری	شبکه‌های فراوان، همراه با اپلیکیشن Trezor Suite یا کیف پول‌های دیگر

باز هم، این‌ها نمونه‌های رایج‌اند، نه توصیه. اپلیکیشن‌های کیف پول از هدف‌های محبوب نسخه‌های جعلی‌اند، به همین دلیل افراد معمولاً آن‌ها را فقط از وب‌سایت رسمی یا لینکی در همان سایت دانلود می‌کنند. کیف پول‌های سخت‌افزاری معمولاً مستقیم از سازنده خریداری می‌شوند، چون دستگاه دست‌دوم یا دست‌کاری‌شده ممکن است امن نباشد.



شکل ۵. کیف پول‌های گرم آنلاین و راحت‌اند؛ کیف پول‌های سرد کلیدها را آفلاین نگه می‌دارند. نام‌ها نمونه‌اند، نه توصیه.

راه‌اندازی کیف پول و عبارت بازیابی

وقتی کیف پول تازه‌ای ساخته می‌شود، یک **عبارت بازیابی** (seed phrase، که «کلمات بازیابی» هم نامیده می‌شود) از ۱۲ یا ۲۴ کلمه نشان می‌دهد. این کلمه‌ها می‌توانند همه کلیدهای کیف پول را در هر اپلیکیشن یا دستگاه سازگاری دوباره بسازند. یعنی:

- هر کسی عبارت بازیابی را ببیند می‌تواند همه دارایی کیف پول را بردارد.

- اگر گوشی گم شود و عبارت بازیابی هم گم شده باشد، دارایی برای همیشه از دست رفته است. شرکت سازنده کیف پول نسخه‌ای از آن ندارد و نمی‌تواند بازنشانی‌اش کند.

روش رایج این است که کلمه‌ها روی کاغذ نوشته یا روی فلز حک شوند، با دقت بررسی شوند و آفلاین در جایی امن نگهداری شوند، گاهی در دو مکان. اسکرین‌شات، عکس، یادداشت‌های ابری، ایمیل و مدیر رمز عبوری که آنلاین همگام‌سازی می‌شود، راه‌های معمول دزدیده شدن عبارت بازیابی‌اند. هیچ کارمند پشتیبانی، اپلیکیشن یا وب‌سایت واقعی‌ای هرگز به آن نیاز ندارد (درس ۱۴).



شکل ۶. عبارت بازیابی کنترل کیف پول را در دست دارد. شیوه نگهداری آن تعیین می‌کند چه کسی می‌تواند دارایی را بردارد.

انتقال دارایی به کیف پول و نخستین سواپ

برداشت از صرافی به کیف پول خودتان همه آموخته‌های درس ۱۰ را به کار می‌گیرد:

1. **آدرس دریافت** را از کیف پول کپی کنید، برای شبکه درست.
2. در صرافی گزینه **«برداشت»** را انتخاب کنید، آدرس را جای‌گذاری کنید و **همان شبکه** را برگزینید. تگ ممو را فقط اگر طرف گیرنده لازم دارد اضافه کنید.
3. چند نویسه اول و آخر آدرس را بررسی کنید.
4. بسیاری از افراد اول یک **مبلغ آزمایشی کوچک** می‌فرستند و پس از رسیدنش، باقی را.

برای استفاده از کیف پول روی آن شبکه، کمی از **کوین بومی شبکه برای گس** هم لازم است، مثل ETH روی Ethereum، BNB روی BNB Chain یا SOL روی Solana (درس ۵).

نخستین سواپ در یک صرافی غیرمتمرکز (درس ۹) این‌طور انجام می‌شود: سایت رسمی DEX را باز کنید، کیف پول را **متصل** کنید، دو توکن را انتخاب کنید، تأثیر قیمت (price impact) و اسلیپیج را بررسی کنید، اگر خواسته شد به توکن **مجوز** (approve) بدهید (درس ۱۴ توضیح می‌دهد چرا مجوزها مهم‌اند)، سپس سواپ را در کیف پول **تأیید** کنید و کارمزد گس را بپردازید.

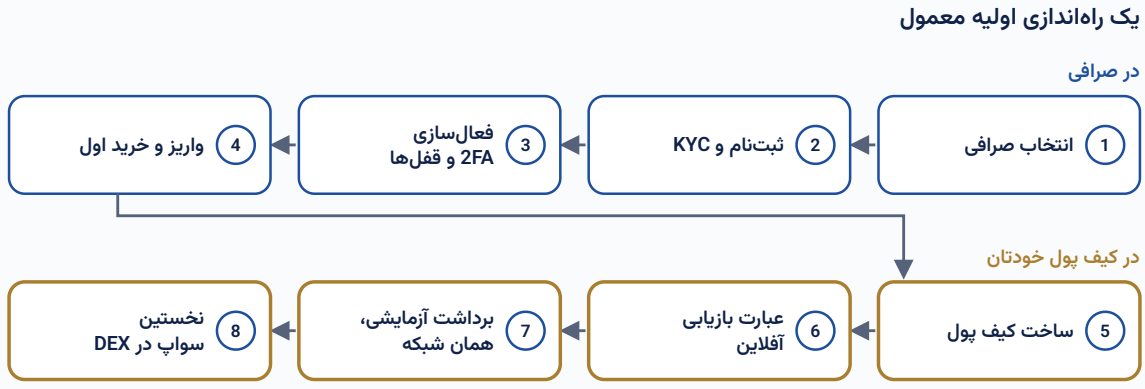


شکل ۷. انتقال دارایی از صرافی به کیف پول با نگهداری شخصی، سپس نخستین سواپ در یک DEX.

کل مسیر در یک نگاه

با کنار هم گذاشتن مطالب این درس، یک راه‌اندازی اولیه معمول هشت مرحله دارد. همه افراد همه مرحله‌ها را انجام نمی‌دهند: بسیاری فقط از صرافی استفاده می‌کنند و برخی دیگر پس از مدتی به نگهداری شخصی روی می‌آورند.

این درس سطح مبتدی دوره کریپتو را به پایان می‌رساند. اکنون می‌دانید کریپتو چیست، کوین‌ها، توکن‌ها و شبکه‌ها چه تفاوتی دارند، کجا معامله می‌شوند، قیمت‌ها چطور حرکت می‌کنند، ریسک‌های اصلی کدام‌اند و نخستین قدم‌های عملی چطور برداشته می‌شوند. سطح‌های متوسط و پیشرفته کریپتو، که ویژه اعضا هستند، عمیق‌تر به معامله، داده‌های آن‌چین و دیفای می‌پردازند.



شکل ۸. یک راه‌اندازی اولیه معمول، از حساب صرافی تا نخستین سواپ در DEX.

چرا این برای معامله‌گران مهم است

- **انتخاب صرافی بر هزینه‌ها اثر می‌گذارد.** کارمزد معامله، اسپرد، نرخ فاندینگ و کارمزد برداشت در طول معاملات زیاد روی هم جمع می‌شوند. سطح‌های کارمزد اغلب به حجم معاملات بستگی دارند.
- **ریسک طرف مقابل واقعی است.** دارایی‌ای که برای معامله در صرافی نگه داشته می‌شود به آن صرافی وابسته است. بسیاری از معامله‌گران فقط به اندازه نیاز معاملاتشان آن‌جا نگه می‌دارند و بقیه را جای دیگری نگهداری می‌کنند.
- **تنظیمات امنیتی از حساب معاملاتی محافظت می‌کنند.** 2FA، کد ضد فیشینگ و فهرست سفید برداشت باعث می‌شوند رمز عبور دزدیده‌شده برای مهاجم بسیار کم‌فایده‌تر باشد.
- **جابه‌جایی میان صرافی‌ها و کیف پول‌ها کاری روزمره است.** انتخاب شبکه درست و بررسی آدرس‌ها برای معامله‌گران فعال به عادت‌های هرروزه تبدیل می‌شوند.

اصطلاحات کلیدی

امانی (کاستودیال)	حالتی که در آن یک شرکت، مثلاً یک صرافی، کلیدهای خصوصی را از طرف شما نگه می‌دارد.
نگهداری شخصی (self-custody)	نگه داشتن کلیدهای خودتان در کیف پولی که کنترلش دست شماست، بی‌آن‌که هیچ شرکتی بتواند دارایی را مسدود یا بازیابی کند.
KYC	«مشتری‌ات را بشناس»: بررسی‌های هویتی که صرافی‌های تحت نظارت باید پیش از ارائه خدمات به مشتری یا در طول آن انجام دهند.
قانون سفر (Travel Rule)	قاعده‌ای که صرافی‌ها را ملزم می‌کند برای برخی انتقال‌ها اطلاعات فرستنده و گیرنده را به اشتراک بگذارند.
2FA	احراز هویت دومرحله‌ای: اثبات دوم هویت، مثل کدی از اپلیکیشن احراز هویت، علاوه بر رمز عبور.
کد ضد فیشینگ	کلمه‌ای شخصی که صرافی در ایمیل‌های واقعی‌اش درج می‌کند تا کاربران بتوانند ایمیل‌های جعلی را تشخیص دهند.
فهرست سفید برداشت	فهرستی از آدرس‌های ذخیره‌شده که تنها آدرس‌هایی‌اند که اجازه دریافت برداشت از یک حساب را دارند.
کیف پول گرم (hot wallet)	کیف پولی که کلیدهایش روی دستگاهی متصل به اینترنت است، مثل اپلیکیشن گوشی یا افزونه مرورگر.
کیف پول سرد (cold wallet)	کیف پولی که کلیدها را آفلاین نگه می‌دارد، معمولاً روی یک دستگاه سخت‌افزاری.

عبارت بازیابی (seed phrase)	فهرستی از ۱۲ یا ۲۴ کلمه که می‌تواند همه کلیدهای یک کیف پول را دوباره بسازد.
شبکه EVM	بلاک‌چینی که ماشین مجازی اتریوم (EVM) را اجرا می‌کند و به همین دلیل با همان کیف پول‌ها، آدرس‌ها و اپلیکیشن‌های Ethereum کار می‌کند. Arbitrum، Base، BNB Chain و Polygon نمونه‌هایی از آن‌اند.

نکات کلیدی

1. کریپتو را می‌توان در صرافی (امانی) یا در کیف پول خودتان (نگهداری شخصی) نگه داشت. بسیاری از افراد از هر دو استفاده می‌کنند.
2. صرافی‌ها در دسترس‌پذیری، روش‌های واریز، کوین‌ها، شبکه‌ها، کارمزدها و سابقه با هم فرق دارند. نام‌های این درس نمونه‌اند، نه توصیه.
3. KYC یعنی بررسی مدرک شناسایی و سلفی که قوانین مبارزه با پولشویی الزامی کرده‌اند.
4. 2FA با اپلیکیشن احراز هویت یا پس‌کی، کد ضد فیشینگ و فهرست سفید برداشت محافظت‌های اصلی حساب‌اند.
5. کیف پول‌های گرم راحت‌اند؛ کیف پول‌های سرد کلیدها را آفلاین نگه می‌دارند. عبارت بازیابی همه چیز را کنترل می‌کند و بازنشانی‌شدنی نیست.
6. برداشت به کیف پول به آدرس درست، همان شبکه و مقداری کوین بومی برای گس نیاز دارد. سواپ در DEX یعنی اتصال، مجوز و تأیید.

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. جمله «کلید دست تو نیست، پس کوین هم مال تو نیست» یعنی چه؟

- A کوین‌های داخل صرافی همیشه از دست می‌روند
- B اگر کس دیگری کلیدها را نگه دارد، کوین‌های شما به او وابسته‌اند
- C کلید خصوصی فقط برای بیت‌کوین لازم است
- D برای خرید کریپتو باید کیف پول سخت‌افزاری داشته باشید

۲. چرا صرافی‌های تحت نظارت مدرک شناسایی و سلفی می‌خواهند؟

A برای تعیین کارمزد معاملات شما
B به دلیل KYC و قوانین مبارزه با پولشویی
C برای انتخاب شبکه شما
D برای ساختن عبارت بازیابی شما

۳. کد ضد فیشینگ چیست؟

A رمز عبوری برای برداشت
B کلمه‌ای که صرافی در ایمیل‌های واقعی‌اش درج می‌کند
C کدی که همه ورودها را مسدود می‌کند
D نوعی کیف پول سخت‌افزاری

۴. کدام شکل 2FA آسان‌تر از همه دزدیده می‌شود؟

A اپلیکیشن احراز هویت
B کلید امنیتی سخت‌افزاری
C کد پیامکی
D پس‌کی

۵. تفاوت اصلی کیف پول گرم و کیف پول سرد چیست؟

A کیف پول‌های گرم فقط بیت‌کوین نگه می‌دارند
B کیف پول‌های سرد کلیدها را آفلاین نگه می‌دارند
C کیف پول‌های گرم عبارت بازیابی ندارند
D کیف پول‌های سرد نمی‌توانند تراکنش بفرستند

۶. آنا گوشی‌اش را گم می‌کند و هرگز عبارت بازیابی‌اش را یادداشت نکرده بود. چه بر سر کیف پول با نگهداری شخصی او می‌آید؟

A شرکت سازنده کیف پول آن را بازنشانی می‌کند
B صرافی‌اش می‌تواند آن را بازگرداند
C دیگر نمی‌توان به دارایی دسترسی داشت
D بلاک‌چین کوین‌ها را پس می‌فرستد

۷. لوکاس USDT را از یک صرافی به کیف پولش روی BNB Chain برداشت می‌کند. در صرافی کدام شبکه را باید انتخاب کند؟

A هر شبکه‌ای، همه یکسان‌اند

B Ethereum، چون بزرگ‌ترین است

C BNB Chain، همان شبکه آدرس کیف پولش

D Bitcoin

۸. USDT لوکاس می‌رسد، اما سواپ انجام نمی‌شود چون نمی‌تواند کارمزد را بپردازد. چه چیزی کم است؟

A عبارت بازیابی

B کمی BNB برای گس

C تأیید KYC

D کد ضد فیشینگ

کلید پاسخ‌ها

۱ B

اگر کس دیگری کلیدها را نگه دارد، کوین‌های شما به او وابسته‌اند

در صرافی، شرکت کلیدها را نگه می‌دارد، پس موجودی شما به امنیت و صداقت آن وابسته است.

۲ B

به دلیل KYC و قوانین مبارزه با پولشویی

بررسی‌های KYC در بیشتر کشورها برای صرافی‌های تحت نظارت الزام قانونی است.

۳ B

کلمه‌ای که صرافی در ایمیل‌های واقعی‌اش درج می‌کند

اگر ایمیلی که ادعا می‌کند از طرف صرافی است کد شما را نشان ندهد، واقعی نیست.

۴ C

کد پیامکی

کدهای پیامکی را می‌توان با سیم‌سواپ ربود، یعنی وقتی مهاجم شماره تلفن شما را به سیم‌کارت خودش منتقل می‌کند.

۵ B

کیف پول‌های سرد کلیدها را آفلاین نگه می‌دارند

کیف پول‌های گرم کلیدها را روی دستگاه‌های متصل به اینترنت نگه می‌دارند؛ کیف پول‌های سرد آن‌ها را آفلاین نگه می‌دارند و تراکنش‌ها را روی خود دستگاه تأیید می‌کنند.

۶ C

دیگر نمی‌توان به دارایی دسترسی داشت

فقط عبارت بازیابی می‌تواند کلیدها را دوباره بسازد. بدون آن، هیچ‌کس نمی‌تواند دارایی را بازیابی کند.

۷ C

BNB Chain، همان شبکه آدرس کیف پولش

شبکه ارسال و دریافت باید یکی باشد، وگرنه ممکن است دارایی از دست برود یا بازیابی‌اش دشوار شود (درس ۱۰).

۸ B

کمی BNB برای گس

هر تراکنش روی یک شبکه با کوین بومی همان شبکه پرداخت می‌شود، که این‌جا BNB روی BNB Chain است.

منابع

- TRM Labs، هک Bybit: ردگیری بزرگ‌ترین حمله کره شمالی: https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit
- TechTarget، FBI: گروه Lazarus پشت سرقت ۱٫۵ میلیارد دلاری از Bybit است: https://www.techtarget.com/cybersecurity/news/366619872/FBI-Lazarus-Group-behind-15-billion-Bybit-heist
- The Block، MetaMask چندزنجیره‌ای می‌شود: یک حساب برای EVM، Solana و به‌زودی Bitcoin: https://theblock.co/post/376450/metamask-multichain-account
- Cointelegraph، MetaMask پشتیبانی از Bitcoin را اضافه کرد: https://cointelegraph.com/news/metamask-adds-bitcoin-support-after-teasing-february

- Tiger Research، بازار رمزارز کره در ۲۰۲۶: https://reports.tiger-research.com/p/2026-korea-cryptocurrency-market-eng

Market Talks

ادامه یادگیری

این درس بخشی از دوره کریپتو در مرکز آموزش MARKET TALKS است. درس‌های سطح مبتدی رایگان‌اند و هر کدام یک آزمون و یک فایل PDF قابل دانلود دارند. درس‌های سطح متوسط و پیشرفته ویژه اعضا هستند.

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.