Market Talks
مرکز آموزش

کریپتو · مبتدی · درس ۱۰ از ۱۵

ارسال و دریافت امن: شبکه‌ها، آدرس‌ها و تگ‌های ممو

هر فیلد صفحه برداشت چه معنایی دارد، چرا شبکه باید در دو طرف یکی باشد، کی به ممو یا تگ نیاز دارید، و چطور از خودتان در برابر آدرس‌های مشابه محافظت کنید

۱۰ دقیقه مطالعه ۸ سؤال آزمون همراه با کلید پاسخ

کریپتو · مبتدی · درس ۱۰ از ۱۵

ارسال و دریافت امن: شبکه‌ها، آدرس‌ها و تگ‌های ممو

در یک جمله

انتقال کریپتو برگشت‌پذیر نیست، پس هر برداشت به درست بودن چهار چیز وابسته است: کوین، شبکه، آدرس و، در صورت نیاز، ممو یا تگ.

دکمه بازگشتی وجود ندارد

انتقال بانکی‌ای که به حساب اشتباه فرستاده شود گاهی قابل برگشت است. تراکنش بلاک‌چینی نه. وقتی تأیید شد، هیچ‌کس، نه شبکه، نه کیف پول شما و معمولاً نه صرافی، نمی‌تواند آن را برگرداند. این همان ویژگی‌ای است که کریپتو را در برابر سانسور مقاوم می‌کند، و یعنی هر جزئیاتی باید پیش از زدن دکمه ارسال درست باشد.

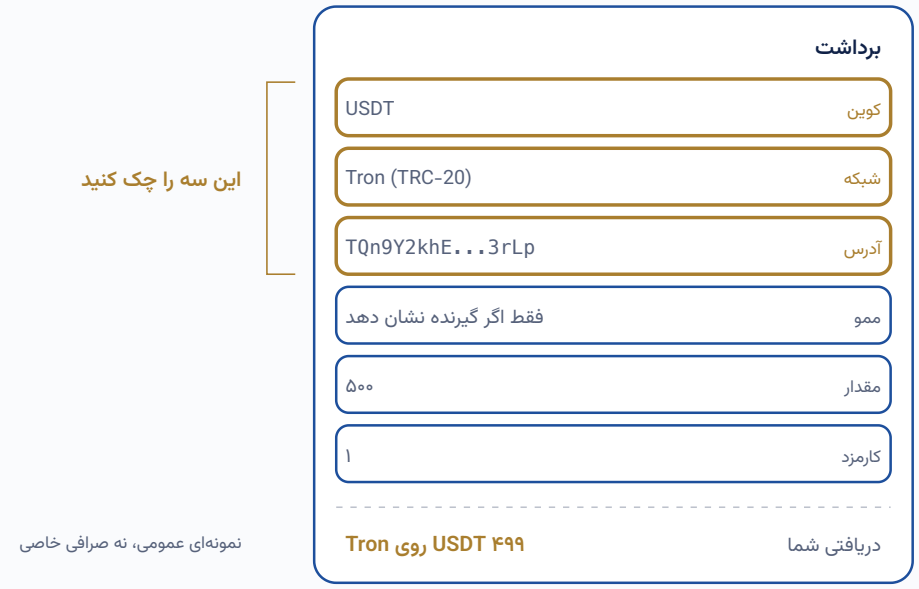
خبر خوب این است که تقریباً همه اشتباه‌های پرهزینه از چند فیلد در یک صفحه می‌آیند. این درس آن‌ها را یکی‌یکی مرور می‌کند.

کالبدشکافی یک برداشت

چه از صرافی برداشت کنید و چه از کیف پول خودتان ارسال کنید، همین نوع فیلدها را پر می‌کنید:

- **کوین:** چیزی که می‌فرستید، مثل USDT.
- **شبکه:** بلاک‌چینی که انتقال از آن انجام می‌شود، مثل Tron (TRC-20) یا Ethereum (ERC-20).
- **آدرس:** مقصد انتقال. باید آدرسی روی همان شبکه باشد.
- **ممو یا تگ:** یک عدد یا متن اضافی، که فقط برای برخی کوین‌ها و برخی گیرندگان لازم است.
- **مقدار:** چقدر می‌فرستید.
- **کارمزد:** کارمزد شبکه یا برداشت، که از مقدار کم یا به آن اضافه می‌شود.

بیشتر صرافی‌ها پیش از تأیید، خلاصه‌ای از آن‌چه به مقصد می‌رسد نشان می‌دهند. آهسته خواندن این خلاصه مفیدترین عادت این درس است.



شکل ۱. یک صفحه برداشت عمومی. کوین، شبکه و آدرس سه فیلدی‌اند که اشتباه در آن‌ها بیشترین هزینه را دارد.

شبکه باید در دو طرف یکی باشد

درس ۵ نشان داد که USDT به‌صورت توکن‌های جداگانه روی Solana، BNB Chain، Ethereum، Tron و شبکه‌های دیگر وجود دارد. هنگام ارسال، شبکه‌ای که انتخاب می‌کنید باید شبکه‌ای باشد که گیرنده برای آن کوین پشتیبانی می‌کند، و آدرس باید متعلق به همان شبکه باشد.

همیشه از سمت گیرنده شروع کنید. در صرافی یا کیف پول گیرنده، اول کوین و سپس شبکه را انتخاب کنید و آدرس واریزی را که نشان می‌دهد کپی کنید. سپس در سمت ارسال، دقیقاً همان شبکه را انتخاب کنید.

اگر یکی نباشند چه می‌شود؟

- اگر قالب آدرس متفاوت باشد، مثلاً آدرس Tron روی شبکه Ethereum، اپلیکیشن معمولاً انتقال را نمی‌پذیرد. این حالتِ خوش‌شانسی است.
- اگر هر دو شبکه از قالب آدرس یکسان **0x** استفاده کنند، مثل Ethereum و BNB Chain، انتقال انجام می‌شود، اما به شبکه‌ای که شاید گیرنده آن را زیر نظر نداشته باشد. دارایی‌ای که به کیف پول خودتان فرستاده شده اغلب با افزودن آن شبکه به کیف پول پیدا می‌شود. دارایی‌ای که به صرافی فرستاده شده ممکن است به درخواست بازیابی نیاز داشته باشد، که می‌تواند هفته‌ها طول بکشد، کارمزد داشته باشد یا رد شود.



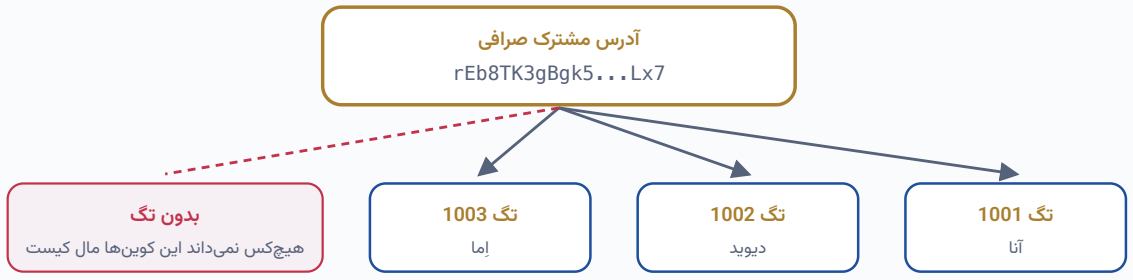
شکل ۲. شبکه باید در دو طرف یکی باشد. قالب آدرس متفاوت معمولاً پذیرفته نمی‌شود، اما شبکه‌هایی که قالب 0x مشترک دارند انتقال را می‌پذیرند، و همین می‌تواند دارایی را سرگردان کند.

ممو و تگ

صرافی‌ها برای برخی کوین‌ها یک آدرس واریز مشترک برای مشتریان زیادی به کار می‌برند. برای این‌که بدانند هر واریز متعلق به کدام مشتری است، یک عدد یا متن کوتاه به نام **ممو**، **تگ** یا **تگ مقصد** (destination tag) اضافه می‌کنند. نمونه‌های رایج XRP است که از تگ مقصد استفاده می‌کند، و TON، Stellar (XLM) و Cosmos (ATOM) که از ممو یا کامنت استفاده می‌کنند.

اگر صرافی گیرنده کنار آدرس یک ممو یا تگ نشان می‌دهد، هنگام ارسال **حتماً** باید آن را در فیلد ممو کپی کنید. بدون آن، کوین‌ها به آدرس مشترک صرافی می‌رسند اما هیچ‌کس نمی‌تواند تشخیص دهد که مال شماست. بازیابی آن‌ها معمولاً یعنی تماس با پشتیبانی همراه با مدرک، و تضمینی هم ندارد.

وقتی به کیف پول شخصی خودتان می‌فرستید، معمولاً ممو لازم نیست، چون آدرس فقط به شما تعلق دارد.



شکل ۳. صرافی‌ها برای کوین‌هایی مثل XRP اغلب به مشتریان زیادی یک آدرس واحد می‌دهند و با تگ آن‌ها را از هم جدا می‌کنند. واریزی که تگ ندارد به هیچ‌کس قابل انتساب نیست.

محافظت از آدرس

آدرس‌های کریپتو طولانی‌اند و به خاطر سپردنشان ناممکن است، و مهاجمان از دو راه اصلی از این سوءاستفاده می‌کنند:

- **مسموم‌سازی آدرس:** مهاجم آدرسی می‌سازد که نویسه‌های اول و آخرش با آدرسی که شما استفاده می‌کنید یکی است، سپس یک تراکنش بسیار کوچک یا جعلی برایتان می‌فرستد تا در تاریخچه‌تان دیده شود. بعداً شما به اشتباه آدرس نادرست را از تاریخچه کپی می‌کنید. در مه ۲۰۲۴ یک معامله‌گر از همین راه ۱٫۱۵۵ WBTC به ارزش حدود ۶۸ میلیون دلار از دست داد، پس از کپی کردن آدرسی که ابتدا و انتهایش با آدرس واقعی یکی بود. مهاجم بعدها پس از مذاکره دارایی را برگرداند، که بسیار نادر است.
- **بدافزار کلیپ‌بورد:** نرم‌افزاری مخرب روی کامپیوتر یا گوشی که در لحظه چسباندن، آدرس کپی‌شده را با آدرس مهاجم عوض می‌کند.

چند عادت ساده از شما در برابر هر دو محافظت می‌کند: آدرس را از صفحه واریز گیرنده کپی کنید، نه از تاریخچه تراکنش‌هایتان؛ هرگز آدرس را دستی تایپ نکنید؛ پس از چسباندن، نویسه‌های ابتدا، وسط و انتها را بررسی کنید؛ و برای آدرس‌هایی که زیاد به آن‌ها می‌فرستید از **فهرست سفید آدرس** (whitelist) صرافی یا دفترچه آدرس کیف پولتان استفاده کنید.



شکل ۴. مسموم‌سازی آدرس: ابتدا و انتهای آدرس مهاجم با آدرس واقعی یکی است، پس فقط وسط آن را لو می‌دهد. آدرس‌ها ساختگی‌اند.

اول آزمایش، بعد پیگیری

برای نخستین انتقال به یک آدرس تازه، بسیاری از کاربران باتجربه اول یک **تراکنش آزمایشی** کوچک می‌فرستند، صبر می‌کنند تا برسد و تنها پس از آن بقیه را می‌فرستند. کارمزد اضافی معمولاً در مقایسه با هزینه یک اشتباه ناچیز است.

پس از ارسال، یک **هش تراکنش** یا TxID می‌گیرید: کدی یکتا که انتقال شما را مشخص می‌کند. چسباندن آن در بلاک اکسپلورر همان شبکه، مثل Etherscan برای Ethereum یا Tronscan برای Tron، نشان می‌دهد انتقال تأیید شده یا

نه و به کجا رفته است. صرافی‌ها واریزها را فقط پس از تعداد مشخصی **تأیید** (confirmation) به حساب می‌گذارند، پس ممکن است یک انتقال چند دقیقه پیش از نمایش در حساب شما، روی بلاک‌چین کامل‌شده دیده شود.

اگر مشکلی پیش آمد، سریع اقدام کنید: هش تراکنش را نگه دارید، از طریق وب‌سایت یا اپلیکیشن رسمی پلتفرم گیرنده با پشتیبانی آن تماس بگیرید، و به هر کسی که پیام می‌دهد و پیشنهاد بازیابی دارایی می‌کند اعتنا نکنید. این پیشنهادها تقریباً همیشه کلاهبرداری دوم‌اند.



شکل ۵. چک‌لیستی کوتاه برای هر انتقال.

چرا این برای معامله‌گران مهم است

- **جابه‌جایی دارایی بخشی از معامله است.** معامله‌گران اغلب پول را میان صرافی‌ها و کیف پول‌ها جابه‌جا می‌کنند، گاهی با عجله. بیشتر اشتباه‌های پرهزینه انتقال زیر فشار زمان رخ می‌دهند.
- **انتخاب شبکه سرعت و هزینه را تغییر می‌دهد.** USDT روی Tron یا Solana معمولاً در چند دقیقه و با کارمزد کم می‌رسد. همین انتقال روی Ethereum می‌تواند گران‌تر باشد، و بیت‌کوین ممکن است برای تأییدها یک ساعت یا بیشتر لازم داشته باشد.
- **صرافی‌ها گاهی یک شبکه را متوقف می‌کنند.** هنگام ارتقا یا شلوغی، واریز یا برداشت روی یک شبکه ممکن است معلق شود. بررسی وضعیت شبکه پیش از ارسال از گیر کردن دارایی در مسیر جلوگیری می‌کند.
- **فهرست سفید یک لایه امنیتی اضافه می‌کند.** بسیاری از صرافی‌ها اجازه می‌دهند برداشت را به آدرس‌های ذخیره‌شده محدود کنید، که اگر روزی حسابتان به خطر بیفتد کمک می‌کند.

اصطلاحات کلیدی

شبکه برداشت	بلاک‌چینی که برای انتقال انتخاب می‌شود. گیرنده باید آن را برای آن کوین پشتیبانی کند.
آدرس واریز	آدرسی که گیرنده برای یک کوین مشخص روی یک شبکه مشخص به شما می‌دهد.

ممو، تگ، تگ مقصد	کدی اضافی که به صرافی می‌گوید واریز به یک آدرس مشترک متعلق به کدام مشتری است.
مسموم‌سازی آدرس	کلاهبرداری‌ای که آدرسی مشابه را در تاریخچه تراکنش‌هایتان می‌کارد، به این امید که آن را به اشتباه کپی کنید.
بدافزار کلیپ‌بورد	نرم‌افزاری مخرب که آدرس کریپتوی کپی‌شده را با آدرس مهاجم عوض می‌کند.
تراکنش آزمایشی	انتقالی کوچک که اول فرستاده می‌شود تا درست بودن آدرس و شبکه تأیید شود.
هش تراکنش (TxID)	کدی یکتا که یک تراکنش را مشخص می‌کند و می‌توان آن را در بلاک اکسپلورر جست‌وجو کرد.
فهرست سفید آدرس	تنظیمی در صرافی که برداشت را فقط به آدرس‌هایی که از پیش ذخیره کرده‌اید مجاز می‌کند.

نکات کلیدی

1. انتقال‌های کریپتویی تأییدشده برگشت‌پذیر نیستند، پس جزئیات باید پیش از ارسال درست باشند.
2. هر برداشت به کوین، شبکه و آدرس درست و، در صورت نیاز، ممو یا تگ نیاز دارد.
3. از سمت گیرنده شروع کنید: کوین و شبکه را آن‌جا انتخاب کنید، آدرس واریز را کپی کنید، سپس هنگام ارسال همان شبکه را برگزینید.
4. اگر گیرنده ممو یا تگ نشان می‌دهد، باید آن را وارد کنید، وگرنه ممکن است دارایی به حسابتان نشیند.
5. مسموم‌سازی آدرس و بدافزار کلیپ‌بورد کپی کردن بی‌دقت را هدف می‌گیرند. از صفحه واریز کپی کنید، هرگز از تاریخچه، و ابتدا، وسط و انتها را بررسی کنید.
6. یک تراکنش آزمایشی کوچک، هش تراکنش و بلاک اکسپلورر به شما اجازه می‌دهند انتقال را قدم‌به‌قدم تأیید کنید.

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. چرا جزئیات هنگام ارسال کریپتو این‌قدر مهم‌اند؟

- A) کارمزدها بسیار بالاست
- B) تراکنش‌های تأییدشده برگشت‌پذیر نیستند
- C) صرافی‌ها هر انتقال را دستی بررسی می‌کنند
- D) آدرس‌ها پس از یک بار استفاده منقضی می‌شوند

۲. امن‌ترین ترتیب مراحل برای انتقال USDT به صرافی دیگر کدام است؟

A در سمت ارسال هر شبکه‌ای را انتخاب کنید و بعد دنبال آدرس بگردید

B در سمت گیرنده کوین و شبکه را انتخاب کنید و آدرس واریز را کپی کنید، سپس هنگام ارسال همان شبکه را انتخاب کنید

C آدرس را از حافظه تایپ کنید

D از آدرس آخرین تراکنشتان استفاده کنید

۳. USDT از نوع BEP-20 را به آدرس کیف پول Ethereum خودتان می‌فرستید. چرا ممکن است انتقال باز هم انجام شود؟

A USDT خودکار روی همه شبکه‌ها کار می‌کند

B BNB Chain و Ethereum از قالب آدرس یکسان 0x استفاده می‌کنند

C صرافی آن را برایتان تبدیل می‌کند

D در هیچ حالتی انجام نمی‌شود

۴. کی ممو یا تگ مقصد لازم است؟

A برای هر انتقال بیت‌کوین

B وقتی صرافی گیرنده آن را کنار آدرس واریزش نشان می‌دهد، برای کوین‌هایی مثل XRP، XLM یا TON

C فقط برای انتقال‌های بالای ۱۰،۰۰۰ دلار

D هرگز، اختیاری است

۵. اگر ممو لازم را وارد نکنید چه می‌شود؟

A انتقال خودکار برگشت داده می‌شود

B کوین‌ها به صرافی می‌رسند اما بدون تماس با پشتیبانی نمی‌توان آن‌ها را به حساب شما ربط داد

C کوین‌ها نابود می‌شوند

D هیچ، ممو فقط برای اطلاع است

۶. مسمومسازی آدرس چطور کار می‌کند؟

A بلاک‌چین را به ویروس آلوده می‌کند

B آدرسی مشابه با ابتدا و انتهای یکسان در تاریخچه‌تان می‌کارد تا آن را به اشتباه کپی کنید

C کلید خصوصی شما را تغییر می‌دهد

D کارمزد شبکه را بالا می‌برد

۷. امن‌ترین جا برای کپی کردن آدرس گیرنده کجاست؟

A تاریخچه تراکنش‌هایتان

B پیامی از یک غریبه

C صفحه واریز خود گیرنده یا دفترچه آدرس ذخیره‌شده شما

D اسکرین‌شاتی از شبکه‌های اجتماعی

۸. با هش تراکنش چه می‌توانید بکنید؟

A تراکنش را برگردانید

B آن را در بلاک اکسپلورر جست‌وجو کنید تا ببینید انتقال تأیید شده یا نه و به کجا رفته است

C آدرس گیرنده را تغییر دهید

D کارمزد را پس بگیرید

کلید پاسخ‌ها

۱ B

تراکنش‌های تأییدشده برگشت‌پذیر نیستند

انتقال بلاک‌چینی پس از تأیید قطعی است. هیچ‌کس نمی‌تواند آن را برایتان برگرداند.

۲ B

در سمت گیرنده کوین و شبکه را انتخاب کنید و آدرس واریز را کپی کنید، سپس هنگام ارسال همان شبکه را انتخاب کنید

شروع از سمت گیرنده تضمین می‌کند شبکه از آن‌هایی است که پشتیبانی می‌کند و آدرس به همان شبکه تعلق دارد.

۳ B

BNB Chain و Ethereum از قالب آدرس یکسان 0x استفاده می‌کنند

همان آدرس 0x روی هر دو شبکه وجود دارد. در کیف پول خودتان اغلب با افزودن BNB Chain آن را می‌بینید؛ در صرافی، بازیابی ممکن است کند باشد یا رد شود.

۴ B

وقتی صرافی گیرنده آن را کنار آدرس واریزش نشان می‌دهد، برای کوین‌هایی مثل XRP، XLM یا TON

صرافی‌ها برای این کوین‌ها یک آدرس مشترک برای مشتریان زیادی به کار می‌برند. ممو به آن‌ها می‌گوید واریز مال شماست.

۵ B

کوین‌ها به صرافی می‌رسند اما بدون تماس با پشتیبانی نمی‌توان آن‌ها را به حساب شما ربط داد

دارایی به آدرس مشترک می‌رسد اما هیچ‌کس نمی‌داند مال شماست. بازیابی از طریق پشتیبانی در برخی موارد ممکن است، اما تضمینی ندارد.

۶ B

آدرسی مشابه با ابتدا و انتهای یکسان در تاریخچه‌تان می‌کارد تا آن را به اشتباه کپی کنید

مهاجمان نویسه‌های اول و آخر آدرسی را که استفاده می‌کنید تقلید می‌کنند. در مه ۲۰۲۴ یک معامله‌گر از این راه حدود ۶۸ میلیون دلار از دست داد.

۷ C

صفحه واریز خود گیرنده یا دفترچه آدرس ذخیره‌شده شما

کپی کردن از تاریخچه دقیقاً همان چیزی است که مسموم‌سازی آدرس از آن سوءاستفاده می‌کند. از صفحه واریز رسمی یا آدرسی ذخیره‌شده و تأییدشده استفاده کنید.

۸ B

آن را در بلاک اکسپلورر جست‌وجو کنید تا ببینید انتقال تأیید شده یا نه و به کجا رفته است

هش، انتقال شما را مشخص می‌کند. بلاک اکسپلورر همان شبکه وضعیت و تعداد تأییدهای آن را نشان می‌دهد.

منابع

- CoinDesk، سرقت ۶۸ میلیون دلار کریپتو با مسموم‌سازی آدرس: https://www.coindesk.com/business/2024/05/03/exploiter-steals-68m-worth-of-crypto-through-address-poisoning
- Cointelegraph، مهاجم مسموم‌سازی آدرس WBTC پس از مذاکره دارایی را بازگرداند: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

- Stablecoin Insider، گزارش USDT در سه‌ماهه دوم ۲۰۲۶ (USDT به تفکیک شبکه): https://stablecoininsider.org/usdt-q2-2026-report-supply-regulation-and-the-two-tier-market/

Market Talks

ادامه یادگیری

درس بعدی: درس ۱۱
اسپات در برابر مشتقات: نگاه اول به فیوچرز، قراردادهای دائمی و اهرم

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.