Market Talks

مرکز آموزش

بلاک‌چین · مبتدی · درس ۱۱ از ۱۳

مسیر یک تراکنش

از لحظه‌ای که دکمه ارسال را می‌زنید تا رسیدن سکه‌ها چه اتفاقی می‌افتد، و چرا گاهی بیشتر از انتظارتان طول می‌کشد

۶ دقیقه مطالعه ۶ سؤال آزمون همراه با کلید پاسخ

بلاک‌چین · مبتدی · درس ۱۱ از ۱۳

مسیر یک تراکنش

در یک جمله

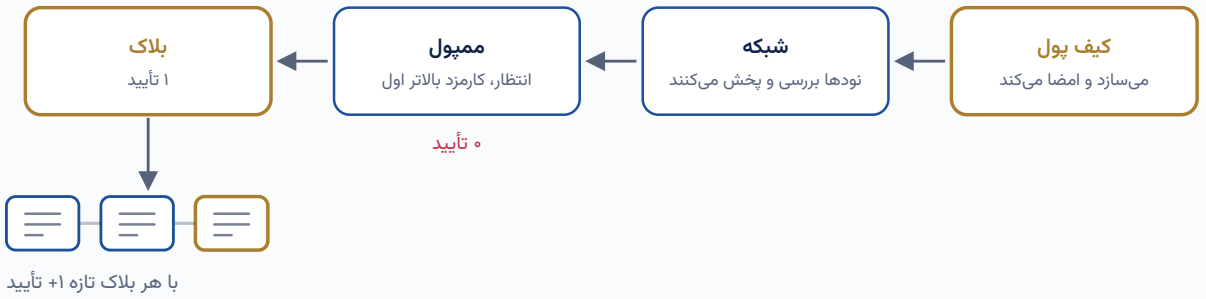
یک تراکنش کریپتو در کیف پول شما ساخته و امضا می‌شود، از نودی به نود دیگر می‌رود، در یک محل انتظار می‌ماند، ماینر یا اعتبارسنج آن را برمی‌دارد، و سپس زیر بلاک‌های تازه دفن می‌شود. کارمزدی که می‌پردازید تعیین می‌کند چقدر زود از صف خارج شود.

گام ۱: کیف پول تراکنش را می‌سازد و امضا می‌کند

وقتی دکمه ارسال را می‌زنید، هنوز چیزی به بلاک‌چین نمی‌رسد. اول کیف پول یک پیام کوچک آماده می‌کند که سه چیز را می‌گوید: کدام سکه‌ها خرج می‌شوند، به کجا می‌روند، و چقدر کارمزد پیشنهاد می‌دهید.

در بیت‌کوین، موجودی شما یک عدد واحد نیست. مجموعه‌ای از تکه‌های جداگانه سکه است که قبلاً دریافت کرده‌اید و به آن‌ها **خروجی‌های خرج‌نشده** می‌گویند. برای فرستادن ۰٫۳ BTC از تکه‌ای به ارزش ۰٫۵ BTC، کیف پول کل آن تکه را خرج می‌کند: ۰٫۳ به گیرنده می‌رسد، مقدار کمی صرف کارمزد می‌شود، و بقیه به‌عنوان **باقی‌مانده** (change) به یکی از آدرس‌های خودتان برمی‌گردد. اتریوم بیشتر شبیه یک حساب بانکی کار می‌کند، اما ایده امضا همان است.

در پایان، کیف پول پیام را با کلید خصوصی شما امضا می‌کند، همان‌طور که در درس ۸ دیدیم. امضا ثابت می‌کند که صاحب سکه دقیقاً همین پرداخت را تأیید کرده است. اگر بعداً حتی یک رقم تغییر کند، امضا دیگر با آن جور درنمی‌آید.



شکل ۱. تراکنش در کیف پول امضا می‌شود، نودها آن را بررسی و پخش می‌کنند، در ممپول منتظر می‌ماند، و وقتی ماینری آن را در بلاک قرار دهد اولین تأیید را می‌گیرد. هر بلاک بعدی یک تأیید دیگر اضافه می‌کند.

نمونه: ۰٫۵ BTC کجا می‌رود

شما یک تکه به ارزش ۰٫۵ BTC دارید و می‌خواهید ۰٫۳ BTC برای دوستتان بفرستید. کیف پول تراکنشی با دو خروجی می‌نویسد: ۰٫۳ BTC به دوستتان و ۰٫۱۹۹۹ BTC به آدرس باقی‌مانده خودتان. آن ۰٫۰۰۰۱ BTC کسری به‌عنوان خروجی در هیچ جا نوشته نمی‌شود. هر چه باقی بماند همان کارمزد است و ماینری که تراکنش را در بلاک قرار می‌دهد آن را برمی‌دارد.

گام ۲: پخش در شبکه و اتاق انتظار

تراکنش امضاشده به یک نود سپرده می‌شود و نود آن را بررسی می‌کند: امضاها معتبرند؟ سکه‌ها وجود دارند؟ قبلاً خرج نشده‌اند؟ اگر همه‌چیز درست باشد، نود آن را برای همتاهایش می‌فرستد و در عرض چند ثانیه در کل شبکه پخش می‌شود، همان‌طور که درس ۷ نشان داد.

هر نود تراکنش‌های معتبری را که دریافت کرده در محلی به نام **ممپول** (mempool، کوتاه‌شده memory pool) نگه می‌دارد. ممپول واحدی وجود ندارد. هر نود ممپول خودش را دارد و برای همین محتوای آن‌ها کمی با هم فرق دارد. تا وقتی تراکنش شما آنجاست، **صفر تأیید** دارد: شبکه از آن خبر دارد، اما هنوز روی بلاک‌چین نیست و در موارد نادر هنوز ممکن است جایگزین شود.

گام ۳: کارمزد تعیین می‌کند چه کسی اول برود

تقریباً هر ده دقیقه یک بلاک بیت‌کوین ساخته می‌شود و جای آن محدود است. وقتی تراکنش‌های منتظر بیشتر از ظرفیت یک بلاک باشند، ماینرها بلاک را با تراکنش‌هایی پر می‌کنند که برای جایی که اشغال می‌کنند بیشترین پول را می‌پردازند. به همین دلیل کارمزد بیت‌کوین به‌صورت نرخ اعلام می‌شود، بر حسب **ساتوشی به ازای هر بایت مجازی** (sat/vB)، نه درصدی از مبلغ. اگر اندازه دو تراکنش یکی باشد، فرستادن ۱۰ دلار یا ۱۰ میلیون دلار هزینه یکسانی دارد.

وضعیت شبکه	معمولاً چه اتفاقی می‌افتد
ممپول خلوت	حتی کارمزد کم هم به بلاک بعدی یا بلاک پس از آن می‌رسد
ممپول شلوغ	تراکنش‌های کم‌کارمزد منتظر می‌مانند، گاهی چند ساعت یا چند روز
هجوم ناگهانی	کارمزدها ممکن است در عرض یک ساعت چند برابر شوند

این هجوم می‌تواند شدید باشد. در ۲۰ آوریل ۲۰۲۴، بلاک ۸۴۰٬۰۰۰، یعنی همان بلاکی که پاداش استخراج بیت‌کوین را نصف کرد، بیش از ۳۷ BTC کارمزد جمع کرد که در آن زمان حدود ۲٫۴ میلیون دلار ارزش داشت، چون کاربران زیادی برای جا گرفتن در آن بلاک تاریخی با هم رقابت می‌کردند.

تشبیه: آخرین قایق شب

یک قایق کوچک هر ده دقیقه با تعداد ثابتی صندلی حرکت می‌کند. در شب‌های خلوت همه سوار می‌شوند. در تعطیلات آخر هفته صف طولانی است و خدمه کسانی را سوار می‌کنند که بالاترین قیمت را برای هر صندلی پیشنهاد می‌دهند. اگر حداقل قیمت را پیشنهاد داده باشید، وقتی قایق بعدی می‌رسد هنوز در صف هستید، و قایق بعد از آن هم.

گام ۴: تأییدها و تسویه

وقتی یک ماینر تراکنش شما را در بلاکی قرار می‌دهد که شبکه آن را می‌پذیرد، تراکنش **یک تأیید** می‌گیرد. هر بلاکی که روی آن اضافه شود یک تأیید دیگر اضافه می‌کند. هر بلاک اضافه، برگرداندن پرداخت را سخت‌تر می‌کند، چون مهاجم باید همه آن بلاک‌ها را از نو بسازد، همان‌طور که درس ۶ توضیح داد.

تعداد تأیید (بیت‌کوین)	معنای رایج
۰	شبکه آن را دیده، اما هنوز در بلاک نیست
۱	در بلاک است و برای مبالغ کوچک روزمره کافی است
چند تأیید	تعدادی که صرافی‌ها معمولاً پیش از واریز به حساب منتظرش می‌مانند و به پلتفرم بستگی دارد
۶	یک قاعده سرانگشتی قدیمی برای مبالغ بزرگ، حدود یک ساعت

شبکه‌های دیگر ریتم خودشان را دارند. اتریوم هر ۱۲ ثانیه یک بلاک اضافه می‌کند و بلاک را پس از حدود ۱۳ دقیقه نهایی می‌داند، یعنی زمانی که دیگر نمی‌توان آن را برگرداند مگر با از بین بردن مقدار عظیمی اتر استیک‌شده.

وقتی تراکنش گیر می‌کند

اگر در دوره‌ای شلوغ کارمزد را خیلی پایین بگذارید، تراکنش شما ممکن است مدت زیادی در ممپول‌ها منتظر بماند. چیزی از دست نمی‌رود: سکه‌ها جابه‌جا نشده‌اند. تراکنش‌های خیلی قدیمی در نهایت از بیشتر ممپول‌ها حذف می‌شوند و سکه‌ها همان‌جا که بودند می‌مانند. دو راه‌حل رایج وجود دارد:

- **جایگزینی با کارمزد بالاتر (Replace-by-fee یا RBF).** کیف پول نسخه جدیدی از همان پرداخت را با کارمزد بالاتر می‌فرستد که جای نسخه قبلی را می‌گیرد.
- **فرزند هزینه والد را می‌پردازد (Child pays for parent یا CPFP).** گیرنده، یا خود شما از طریق باقی‌مانده، سکه‌های گیرکرده را در تراکنش تازه‌ای با کارمزد بالا خرج می‌کند تا ماینر دلیلی داشته باشد که هر دو را با هم در بلاک بگذارد.

راه‌حل هر چه باشد، می‌توانید کل مسیر را خودتان دنبال کنید. هر تراکنش یک شناسه به نام **txid** دارد که می‌توانید آن را در یک بلاک‌اکسپلورر وارد کنید و ببینید منتظر است، تأیید شده، یا چقدر عمیق زیر بلاک‌ها قرار گرفته است.

چرا این برای تریدرها مهم است

- **واریزها آنی نیستند.** صرافی فقط پس از تعداد تأییدی که لازم می‌داند بیت‌کوین شما را به حساب واریز می‌کند. اگر قصد دارید روی یک حرکت سریع معامله کنید، سکه‌ها باید پیش از حرکت در صرافی باشند، نه در راه.
- **وقتی بازار حرکت می‌کند کارمزدها بالا می‌روند.** نوسان‌های تند قیمت، عده زیادی را هم‌زمان به سمت بلاک‌چین می‌کشاند و کارمزدها همراه آن‌ها جهش می‌کنند. پیش از ارسال نرخ کارمزد فعلی را بررسی کنید و وقتی زمان مهم است پایین‌ترین گزینه را انتخاب نکنید.
- **txid را نگه دارید.** اگر واریز یا برداشتی دیر شد، txid دقیقاً نشان می‌دهد کجاست. این همچنین اولین چیزی است که پشتیبانی صرافی از شما می‌خواهد.

اصطلاحات کلیدی

ممپول	محل انتظاری که هر نود تراکنش‌های معتبرِ منتظرِ ورود به بلاک را در آن نگه می‌دارد.
کارمزد تراکنش	مبلغی که فرستنده می‌پردازد تا تراکنشش در بلاک قرار بگیرد. در بیت‌کوین، هر چیزی است که پس از کم کردن خروجی‌ها از ورودی‌ها باقی می‌ماند.
sat/vB	ساتوشی به ازای هر بایت مجازی، نرخی که برای مقایسه کارمزدهای بیت‌کوین به کار می‌رود. هر ساتوشی یک صدمیلیونیم بیت‌کوین است.
تأیید	یک بلاک روی زنجیره که تراکنش شما را در بر دارد یا پس از آن آمده است. هر چه تأییدها بیشتر باشد، برگرداندن پرداخت سخت‌تر است.
خروجی باقی‌مانده	بخشی از سکه خرج‌شده که کیف پول آن را به آدرس خود فرستنده برمی‌گرداند.
شناسه تراکنش (txid)	کد یکتایی که یک تراکنش را مشخص می‌کند و به شما امکان می‌دهد آن را در بلاک‌اکسپلورر جست‌وجو کنید.

نکات کلیدی

1. تراکنش پیش از آنکه چیزی به شبکه فرستاده شود، در کیف پول شما ساخته و امضا می‌شود.
2. نودها آن را بررسی می‌کنند، به دیگران می‌فرستند و در ممپول خود نگه می‌دارند، جایی که صفر تأیید دارد.

3. جای بلاک محدود است، پس ماینرها تراکنش‌هایی را انتخاب می‌کنند که بالاترین نرخ کارمزد را می‌پردازند، نه بیشترین مبلغ را.
4. هر بلاکی که پس از بلاک شما اضافه شود یک تأیید دیگر است و صرافی‌ها پیش از واریز منتظر تعداد مشخصی از آن‌ها می‌مانند.
5. تراکنش گیرکرده را می‌توان با جایگزینی با کارمزد بالاتر یا روش فرزند هزینه والد را می‌پردازد سرعت داد و با txid آن را دنبال کرد.

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. تراکنش کجا امضا می‌شود؟

A. توسط اولین نودی که آن را دریافت می‌کند
B. در کیف پول فرستنده، پیش از ارسال
C. توسط ماینری که آن را در بلاک قرار می‌دهد
D. در کیف پول گیرنده، هنگام رسیدن

۲. برای فرستادن ۰٫۳ BTC یک سکه ۰٫۵ BTC خرج می‌کنید. بقیه آن چه می‌شود؟

A. برای همیشه از بین می‌رود
B. تا هاوینگ بعدی قفل می‌ماند
C. بیشترش به‌عنوان باقی‌مانده به شما برمی‌گردد و مقدار کم باقی‌مانده همان کارمزد است
D. گیرنده آن را به‌عنوان انعام نگه می‌دارد

۳. ممپول چیست؟

A. محل انتظار هر نود برای تراکنش‌های معتبری که منتظر بلاک هستند
B. یک سرور جهانی واحد که توسعه‌دهندگان بیت‌کوین اداره می‌کنند
C. کیف پولی که سکه‌های صرافی‌ها را نگه می‌دارد
D. بخشی از بلاک که کارمزدها در آن ثبت می‌شوند

۴. دو تراکنش بیت‌کوین هم‌اندازه‌اند. یکی ۱۰ دلار می‌فرستد و دیگری ۱۰ میلیون دلار. کدام برای اینکه سریع در بلاک قرار بگیرد کارمزد بالاتری لازم دارد؟

A تراکنش ۱۰ میلیون دلاری، چون کارمزد درصدی است

B هیچ‌کدام، هر دو به نرخ کارمزد یکسانی نیاز دارند

C تراکنش ۱۰ دلاری، چون پرداخت‌های کوچک عقب می‌افتند

D کارمزد را صرافی تعیین می‌کند، نه شبکه

۵. تراکنش شما در یک بلاک است و پس از آن دو بلاک دیگر اضافه شده است. چند تأیید دارد؟

A یک

B دو

C سه

D شش

۶. تراکنش کم‌کارمزد شما در یک دوره شلوغ چند ساعت است منتظر مانده. راه‌حل معمول چیست؟

A همان سکه‌ها را دوباره به یک آدرس جدید بفرستید

B با ماینرها تماس بگیرید و از آن‌ها بخواهید آن را در بلاک بگذارند

C کیف پول را از عبارت بازیابی بازگردانی کنید

D با جایگزینی با کارمزد بالاتر، نسخه‌ای تازه با کارمزد بیشتر بفرستید

کلید پاسخ‌ها

۱ **B**

در کیف پول فرستنده، پیش از ارسال

کیف پول پیش از پخش در شبکه، با کلید خصوصی امضا می‌کند. نودها و ماینرها فقط امضا را بررسی می‌کنند و نمی‌توانند آن را بسازند.

۲ **C**

بیشترش به‌عنوان باقی‌مانده به شما برمی‌گردد و مقدار کم باقی‌مانده همان کارمزد است

بیت‌کوین سکه‌ها را کامل خرج می‌کند. کیف پول تفاوت را به آدرس باقی‌مانده خودتان می‌فرستد و مقدار کمی را بدون تخصیص می‌گذارد تا کارمزد شود.

۳ **A**

محل انتظار هر نود برای تراکنش‌های معتبری که منتظر بلاک هستند

هر نود ممپول خودش را دارد، پس ممپول واحدی وجود ندارد. ممپول تراکنش‌هایی را نگه می‌دارد که معتبرند اما هنوز در بلاک نیستند.

۴ **B**

هیچ‌کدام، هر دو به نرخ کارمزد یکسانی نیاز دارند

ماینرها کارمزد را به ازای هر بایت مجازی از جا مقایسه می‌کنند. مبلغ ارسالی اهمیتی ندارد و فقط اندازه تراکنش مهم است.

۵ **C**

سه

بلاکی که تراکنش را در بر دارد اولین تأیید حساب می‌شود و هر بلاک پس از آن یک تأیید اضافه می‌کند، پس یک به‌علاوه دو می‌شود سه.

۶ **D**

با جایگزینی با کارمزد بالاتر، نسخه‌ای تازه با کارمزد بیشتر بفرستید

جایگزینی با کارمزد بالاتر، تراکنش منتظر را با نسخه‌ای با کارمزد بیشتر عوض می‌کند. گزینه رایج دیگر روش فرزند هزینه والد را می‌پردازد است.

منابع

- Bitcoin Developer Guide، تراکنش‌ها: https://developer.bitcoin.org/devguide/transactions.html
- Cointelegraph، کاربران بیت‌کوین رکورد ۲٫۴ میلیون دلار کارمزد در بلاک هاوینگ پرداختند: https://cointelegraph.com/news/bitcoin-halving-users-spend-record-millions-block-space-runes-rare-satoshis
- ethereum.org، اثبات سهام و نهایی شدن: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Bitcoin Optech، Replace-by-fee: https://bitcoinops.org/en/topics/replace-by-fee/

Market Talks

ادامه یادگیری

درس بعدی: درس ۱۲ بلاک‌چین‌های عمومی، خصوصی و کنسرسیومی

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.