



شاید شما نوسان گیر هستید و منتظرید تا قیمت بیت کوین بالا رفته و آن را بفروشید، اما برخی دیگر به فکر نگهداری بیت کوین نیستند. مگر نه اینکه داشتن ارز برای خرج کردن آن است؟ در این مطلب از درآمد سازان به این می‌پردازیم که وقتی بیت کوین را خرج می‌کنیم یا برای کسی می‌فرستیم، تراکنش چگونه اتفاق می‌افتد؟

تراکنش‌های بیت کوین از طریق کیف پول بیت کوین به کیف پولی دیگر انتقال داده می‌شوند و برای امنیت، به صورت دیجیتالی امضاء می‌شوند. همه افراد در شبکه بیت کوین از این تراکنش مطلع می‌گردند و تاریخچه تراکنش می‌تواند تا منبع و جایی که بیت کوین تولید شده ردیابی شود.

چیز جالب درباره بیت‌کوین این است که بیت کوین هیچ جا وجود ندارد، حتی روی یک هارد. وقتی گفته می‌شود شخصی ۱ بیت کوین دارد، به یک آدرس خاص بیت کوین نگاه می‌کنیم تا بیت کوین را در آن ببینیم، اما هیچ بیت کوینی به صورت دیجیتال در آن نیست. شما نمی‌توانید به یک شی فیزیکی یا حتی یک فایل اشاره کنید و بگویید این یک بیت کوین است. به جای این، فقط سوابق تراکنش‌ها هستند که وجود دارند، با موجودی‌شان که کاهش یا افزایش یافته است. با خرید بیت‌کوین از شخص دیگر یا هر تراکنشی که انجام می‌شود، اطلاعات در یک دفتر کل عمومی به نام بلاک چین (زنجیره بلوکی) نگهداری می‌شود. اگر می‌خواهید موجودی هر آدرس (کیف پول بیت کوین) را بدانید، این اطلاعات در آدرس آن ذخیره نشده؛ شما باید با نگاه کردن به بلاک‌چین، آن آدرس را دوباره‌سازی کنید.

تراکنش بیت کوین شبیه چیست؟

اگر x کمی بیت کوین به y بفرستد، این تراکنش ۳ قسمت از اطلاعات را دارا خواهد بود:

- ورودی: این سابقه‌ای است که نشان می‌دهد کدام آدرس بیت کوین، برای ارسال بیت کوین به y استفاده شده است.

- مقدار: این همان مقدار بیت کوین است که x به y می‌فرستد.

- خروجی: این، آدرس بیت کوین y است.

چگونه ارسال می‌شود؟

برای ارسال بیت کوین، شما به دو چیز نیاز دارید: یک آدرس بیت کوین و یک کلید اختصاصی. آدرس بیت کوین به صورت تصادفی ایجاد می‌شود و ترکیبی از اعداد و حروف است. کلید اختصاصی نیز ترتیبی از حروف و اعداد دیگر است که برخلاف آدرس کیف پول شما، به صورت محرمانه نگهداری می‌شود. آدرس بیت کوین خودتان مانند یک گاوصندوق با درب شیشه‌ای است. همه می‌بینند چه چیزی داخل گاوصندوق است (مقدار بیت کوین) اما فقط با کلید اختصاصی می‌توان آن را باز کند تا چیزی را از آن برداشت یا چیزی به آن اضافه کند.

وقتی x می‌خواهد به y بیت کوین بفرستد، از کلید اختصاصی خودش برای امضای یک پیام همراه با ورودی (منبع تراکنش‌های بیت کوین)، مقدار و خروجی استفاده می‌کند. سپس x بیت کوین را از کیف پول خود به یک شبکه بیت کوین گسترده‌تر ارسال می‌کند. از آنجا، استخراج‌کنندگان بیت کوین، تراکنش را تأیید می‌کنند، آن را در یک بلوک تراکنش قرار می‌دهند و در نهایت آن را حل می‌کنند.

چرا گاهی اوقات باید منتظر بمانیم تا تراکنش انجام شود؟

زیرا تراکنش شما باید توسط استخراج‌کنندگان بیت کوین تأیید شود، گاهی اوقات مجبور می‌شوید تا آن‌ها کار استخراج را به پایان رسانند. پروتکل بیت کوین طوری است که هر بلاک، حدوداً ۱۰ دقیقه طول می‌کشد تا استخراج شود. برخی فروشندگان ممکن است شما را مجبور کنند تا زمانی که بلاک فعلی تأیید شود منتظر بمانید، به این معنی که شاید نیاز باشد یک فنجان قهوه بخورید و پس از مدتی برگردید تا بتوانید از محصولات آنلاین یا خدماتی که با بیت کوین خریده‌اید استفاده کنید. در سمت دیگر، برخی فروشندگان شما را مجبور نمی‌کنند تا زمان تأیید تراکنش منتظر بمانید. آن‌ها فرض را بر این می‌گیرند که قبل از تأیید شدن تراکنش، شما تلاش نخواهید کرد بیت کوین را در جای دیگری خرج کنید. این معمولاً برای تراکنش‌هایی با ارزش کم اتفاق می‌افتد، زیرا ریسک کلاهبرداری پایین است.

اگر مقدار ورودی و خروجی با هم یکسان نشد چه اتفاقی می‌افتد؟

به خاطر اینکه بیت کوین به‌عنوان سوابقی از تراکنش‌ها وجود دارد، احتمال این هست که با تراکنش‌های مختلف بسیاری که مرتبط با یک کیف پول بیت کوین است مواجه شوید. مثلاً x ۲ بیت کوین، y ۳ بیت کوین و z ۱ بیت کوین به b می‌فرستند و این تراکنش‌ها جداگانه در زمان‌های جداگانه ارسال می‌شوند.

این‌ها به‌صورت خودکار و به‌عنوان یک فایل که شامل ۶ بیت کوین است در حساب X قرار نمی‌گیرند، بلکه آن‌ها به‌عنوان سابقه ۳ تراکنش جداگانه مشخص می‌شوند.

احتمال این وجود دارد که b بعداً بخواهد به یک نفر دیگر با نام C بیت کوین بفرستد و این مقدار بیت کوین دقیقاً به همان مقدار تراکنش‌های قبلی نباشد. فرض کنید b قصد دارد ۱,۵ بیت کوین به C بفرستد؛ اما مشکل اینجاست هیچ‌کدام از تراکنش‌هایی که b در آدرس بیت کوین خود دارد به این مقدار نیست و هیچ‌کدام از تراکنش‌ها را اگر جمع کنیم به این مقدار نمی‌رسد. تکلیف چیست؟ b نمی‌تواند یک تراکنش را به مقادیر کوچک‌تر تقسیم کند و فقط می‌تواند خروجی کامل یک تراکنش را خرج کند.

پس b ۲ بیت کوینی را که از X گرفته به C می‌فرستند. X ورودی است و C خروجی؛ اما مقدار موردنیاز فقط ۱,۵ بیت کوین است و b فقط همین مقدار را می‌خواهد خرج کند؛ بنابراین کیف پول او به‌صورت اتوماتیک ۲ خروجی برای b ایجاد می‌کند: ۱,۵ بیت کوین به C و ۰,۵ بیت کوین به آدرس جدید ارسال می‌شود. این آدرس جدید برای b ایجاد شده تا مقدار باقیمانده از ۲ بیت کوین (۰,۵ بیت کوین) را نگهداری کند.

آیا کارمزدی برای انتقال بیت کوین وجود دارد؟

اکثر اوقات بله. کارمزد انتقال بر اساس فاکتورهای متعددی محاسبه می‌شود. برخی از کیف پول‌ها به شما اجازه می‌دهند کارمزد انتقال را به‌صورت دستی وارد کنید. هر بخشی از بیت کوین که توسط دریافت‌کننده برداشته نشود یا به‌عنوان مابقی برگردانده شود به‌عنوان کارمزد تراکنش در نظر گرفته می‌شود. این مقدار سپس به‌عنوان یک پاداش اضافی، به استخراج‌کننده خوش‌شانسی می‌رسد که بلوک تراکنش را حل می‌کند.

رسید ارسال بیت کوین را می‌توان دریافت کرد؟

بیت کوین باهدف ارائه رسید طراحی نشده است. گرچه در آینده تغییراتی ایجاد می‌شود که اصلاحاتی برای کاربرپسند بودن بیت کوین در پی خواهد داشت. الان سیستم‌های پرداختی مانند Bitpay ویژگی‌های اختصاصی ارائه می‌دهند که معمولاً در کیف پول‌های ساده وجود ندارد، مانند رسید و صفحه تأیید سفارش که ارائه می‌دهند.

اگر بخواهم فقط مقدار کمی بیت کوین ارسال کنم تکلیف چیست؟

تراکنش‌های بیت کوین قابل تقسیم هستند. یک ساتوشی صدمیلیونم بیت کوین است و می‌توان یک تراکنش به کوچکی ۵۴۳۰ ساتوشی در شبکه بیت کوین ارسال کرد.