کد خبر: ۲۲۹۵۳۰
شنبه ۴ بهمن ۱۳۹۹ ۱۳:۰۱

# کوین دسک: هیچ دوبار خرج کردنی روی بیت کوین رخ نداده است

پس از انتشار اخبار و حواشی بسیار پیرامون خرج دوباره (Double Spend) روی شبکه بیت کوین، رسانه کوین دسک با بررسی شواهد موجود و اتفاقات مختلف، اعلام کرده است که هیچ دوباره خرج کردنی رخ نداده است. نباید فراموش کرد که یکی از اصولی که شبکه بیت کوین بر پایه آن کار می‌کند، توانایی شبکه در جلوگیری از این اتفاقات است.<;br&#۴۷;><br&#۴۷;>

به گزارش سایت خبری پرسون از کوین دسک، خرج دوباره روی شبکه بیت کوین، به آن مفهوم که عموم مردم باور دارند، رخ نداده است. نباید فراموش کرد که یکی از اصولی که شبکه بیت کوین بر پایه آن ایجاد شده، جلوگیری از خرج دوباره است.

جیسیون لاو (Jason Lau)، از مدیران ارشد صرافی اوکی کوین (OKCoin)، در مصاحبه‌ای گفت: تیتر خرج دوباره رسانه‌ها باعث اضطراب سرمایه‌گذاران شد، اما این اتفاق سوءتفاهمی از نحوه کارکرد شبکه بیت کوین بود. در این مورد، یک سازماندهی دوباره در یک بلاک بود که امری نسبتاً طبیعی در شبکه بیت کوین به حساب می‌آید.

به‌عبارت دیگر، هیچ بیت کوینی دوباره خرج «نشده» است؛ چراکه هیچ ارز تازه‌ای به عرضه بیت کوین اضافه نشده است. در این مورد، تنها ارزهایی از یک کیف پول مشابه، در دو بلاک متفاوت ثبت شده‌اند. این اتفاق ناشی از دوشاخه‌شدن معمولی بلاک چین بیت کوین است که در موارد بسیاری رخ می‌دهد.

از آنجایی که تنها یکی از این تراکنش‌ها (تراکنش موجود روی زنجیره بلندتر) معتبر است و امکان خرج‌کردن بیت کوین‌ها در زنجیره کوتاه‌تر وجود ندارد، نمی‌توان آن را یک خرج دوباره نامید.

سازماندهی دوباره بلاک در بیت کوین

به‌دلیل ذات توزیع‌شده شبکه بیت کوین و رقابت بالای ماینرها در این شبکه، گاهی اوقات، استخرهای استخراج در یک زمان، یک بلاک مشابه را استخراج می‌کنند. این اتفاق باعث می‌شود که زنجیره بیت کوین به دو زنجیره تقسیم شود. در این حالت، در هر دو شاخه بلاک چین، ماینرها به فعالیت خود ادامه می‌دهند و به بلاک‌های زنجیره اضافه می‌کنند. این اتفاق تا زمانی که یک زنجیره طول بیشتری پیدا کند، ادامه خواهد یافت.

فرض کنید استخر الف و استخر ب، در یک زمان، یک بلاک مشابه را استخراج کنند. در این حالت، بلاک چین بیت کوین به دو زنجیره الف و ب تقسیم می‌شود. ماینرها باید انتخاب کنند که استخراج خود را روی کدام شبکه ادامه خواهند داد. فرض می‌گیریم بلاک بعدی در زنجیره الف ساخته می‌شود، اما ۲ یا ۳ بلاک بعدی، در زنجیره ب قرار می‌گیرند. در این صورت، زنجیره ب، زنجیره طولانی‌تر است و ماینرها تصمیم می‌گیرند تأیید بلاک‌ها را در زنجیره ب ادامه دهند.

زنجیره الف در این مثال، فاقد اعتبار است و بلاک‌هایی هم که روی آن ماین شوند، بلاک کهنه نام دارند.

در بلاک شماره ۶۶۳,۸۳۳ هم همین اتفاق افتاد و ۲ بلاک توسط استخرهای استخراج مختلف ایجاد شدند. لاو می‌گوید در نتیجه این اتفاق یک سازماندهی مجدد در یک بلاک اتفاق افتاد. به همین دلیل است ساتوشی ناکاموتو در وایت پیپر بیت کوین اشاره می‌کند که تراکنش‌ها بعد از دریافت ۶ تأییدیه، نهایی می‌شوند؛ این یعنی تأیید نهایی یک تراکنش، مستلزم ایجاد ۶ بلاک دیگر، پس از بلاکی که تراکنش در آن قرار دارد، است.

خبری از خرج دوباره نبود

خرج دوباره مشکوک و پرحاشیه توسط بیتمکس (BitMEX) و در بلاک ۶۶۶,۸۳۳ گزارش شد. به‌گفته بیتمکس، بلاک کهنه یا بلاک یتیم (Orphaned Block)، حاوی یک تراکنش بود که در زنجیره معتبر هم وجود داشت؛ یعنی یک تراکنش حاوی بیت کوین‌هایی بود که هم در زنجیره معتبر و هم در زنجیره نامعتبر وجود داشت.

چیزی که بیتمکس از خرج دوباره مشکوک از آن یاد کرد، شبیه به یک تراکنش است که از طریق جایگزینی کارمزد (RBF) برگشت خورده است. تراکنش‌های RBF به تراکنش‌هایی اطلاق می‌شود که پیش از تأیید تراکنش اول (با کارمزد پایین‌تر)، یک تراکنش با کارمزد بالاتر ثبت و تأیید می‌شود. از این تکنیک معمولاً برای لغو تراکنش استفاده می‌شود.

چه اتفاقی افتاد؟

یک نفر ۰.۰۰۰۶۲۰۶۳ بیت کوین را با کمترین کارمزد ممکن (۱ ساتوشی به ازای هر بایت یا کمتر از ۱ سنت برای هر بایت) منتقل می‌کند.

از آنجایی که کارمزد تراکنش بسیار پایین بود، تأیید تراکنش زمانی طولانی طول کشید؛ از همین رو، ارسال‌کننده تراکنش سعی کرد تا با جایگزین‌کردن تراکنش با یک تراکنش با کارمزد بیشتر، آن را لغو کند.

اما در کمال تعجب، تراکنشی که کارمزد کمتری داشت (تراکنش اول) زودتر از تراکنش بعدی تأیید شد. این تراکنش در بلاکی قرار گرفت که در زنجیره بلندتر قرار داشت.

در سوی دیگر، تراکنشی که کارمزد بالاتری داشت، به بلاک کهنه رفت. در نتیجه ۰.۰۰۰۶۲۰۶۳ بیت کوین در آدرس ۱D۶aebVY۵DbS۱v۷rNTnX۲xeYcfWM۳os۱va روی زنجیره نامعتبر قرار داشت و ۰.۰۰۰۱۴۴۹۹ بیت کوین در آدرس مشابه روی زنجیره معتبر بود.

اهمیت شش تأیید

از نقطه‌نظر فنی، در سناریوی فعلی بیت کوین‌های مشابه، دو بار خرج شده‌اند؛ اما خرج دوباره روی زنجیره‌ای انجام گرفته است که معتبر تلقی نمی‌شود. برای تأیید این ادعا کافی است شناسه تراکنش نامعتبر را در یک کاوشگر بلاک بیت کوین جستجو کنید و ببینید که هیچ نتیجه‌ای برای شما نشان نمی‌دهد.

بن کارمن (Ben Carman)، از توسعه‌دهندگان بیت کوین در شوردبیتز (Suredbits)، در مصاحبه‌ای گفت: این اتفاق به‌نوعی یک خرج دوباره به حساب می‌آید ولی خرج دوباره واقعی نیست. معمولاً خرج دوباره به حالتی گفته می‌شود که شما عمداً تراکنشی که به شخص دیگر ارسال شده است را با تراکنشی با مقصد خودتان جایگزین کنید.

لوکاس نوزی (Lucas Nuzzi)، تحلیل‌گر داده‌های بیت کوین در کوین مترکیس (Coin Metrics)، در این باره می‌گوید: در این سناریو، مهم است که بدانیم ممکن است نسخه‌های مختلفی از یک تراکنش مشابه وجود داشته باشد، اما در نهایت [تنها] یکی از آنها برای نودها و کاربران شبکه بیت کوین معتبر است.

خرج دوباره معمولاً به این معنی است که ارسال‌کننده تراکنش، دریافت‌کننده را مجاب می‌کند که تراکنش را ارسال کرده است، اما در حقیقت تراکنش را به خودش هم فرستاده است؛ به همین دلیل، کسب‌وکارهای مختلف، تا ۶ تأیید صبر می‌کنند تا تراکنش نهایی شود. نباید فراموش کرد که در این مورد خاص، گزارشی از کلاهبرداری انجام نگرفته است. احتمالا دریافت‌کننده و ارسال‌کننده تراکنش یک نفر یا نهاد بوده است.

نیک کارتر (Nick Carter)، از بنیان‌گذاران کوین متریکس، در توییتر خود با اشاره به اینکه هیچ ادعایی مبنی بر کلاهبرداری وجود ندارد، معتقد است که فرضیه خرج دوباره فاقد اعتبار است. او در ادامه نوشت: در گذشته شاهد خرج دوباره بوده‌ایم؟ به احتمال زیاد بله. آیا این بدان معناست که شبکه بیت کوین اشکال دارد؟ نه! این اتفاقات در شرایطی رخ داده‌اند که امروز وجود ندارد.