اجماع در بلاک‌چین

قسمت دوم

در قسمت اول بلاک‌چین را به‌عنوان یک فناوری انقلابی شناختیم و دانستیم که بلاک‌چین به خاطر ویژگی‌های منحصربه‌فردش تا چه اندازه موردتوجه قرارگرفته است. مهم‌ترین ویژگی‌های بلاک‌چین غیرمتمرکزبودن،غیرقابل‌دست‌کاری‌بودن،شفاف‌بودن، اجماع و توزیع را بررسی کردیم. در این مقاله قصد داریم به‌صورت دقیق‌تر روی ویژگی اجماع بلاک‌چین و چگونگی رسیدن به توافق و همچنین نحوهٔ کارکرد ماینرها توضیح دهیم.

شهری را در نظر بگیرید که هرکدام از مردم آن مشغول فعالیت‌های روزمرهٔ خود هستند. شهرداری به‌عنوان نهاد تصمیم‌گیر در این شهر، تمامی فعالیت‌ها را زیر نظر خود دارد و دستورات لازم را اتخاذ می‌کند. هرگونه تغییراتی در این شهر، به‌عنوان مثال تزیین شهر یا افتتاح فضای سبز عمومی، با دستور این نهاد انجام خواهد شد. این نهاد را به‌عنوان یک نهاد متمرکز در قسمت قبل شناختیم و به جای تمرکز قدرت در یک نقطه، از توزیع قدرت بین تمامی اعضای آن سخن گفتیم

در این بین نهادی قدرتمند وجود دارد که تصمیم‌های لازم را می‌گیرد، اما اگر این نهاد کنار برود، شهر چگونه بدون نهاد مرکزی به فعالیت خود ادامه دهد؟ مردم شهر با هزاران سلیقهٔ متنوع چگونه می‌توانند با یکدیگر به توافق برسند؛ طوری که شهر دچار هرج‌ومرج و آشوب نشود؟ با فرض رسیدن به توافق، چه‌کسی مسئول اجرای توافق موردنظر و چه‌کسی مسئول نظارت بر اجرای فعالیت موردنظر است؟

جواب از طریق اجماع. اما چگونه؟

اجماع در واقع توافقی است که میان اعضای شبکه وجود دارد و هیچ‌گونه تغییری در دفتر کل توزیع شده انجام نمی‌شود، مگر با رضایت و اجماع نظر حداقل ۵۱ درصد اعضای شبکه. در واقع، اگر تراکنشی در شبکه فرستاده شود، اصالت و درستی آن از طریق اجماع سنجیده می‌شود و این تراکنش با رأی اکثریت به دفتر کل توزیع‌شده اضافه می‌شود.

در بلاک‌چین الگوریتم‌های رسیدن به توافق‌های بسیارند و مهم‌ترین آن‌ها الگوریتم اثبات کار[1] و الگوریتم اثبات سهام[2] هستند.

در این قسمت قصد داریم به یکی از مهم‌ترین الگوریتم‌های اجماع یعنی الگوریتم اثبات کار بپردازیم. الگوریتم اجماع بسیاری از بلاکچین‌ها و سازوکار و نقش ماینرها را در این سامانه بررسی می‌کنیم.

دانستیم که بلاک‌چین در واقع یه دفتر کل توزیع شده است که همهٔ اعضای شبکه رونوشت(کپی) واحدی از این دفتر کل دارند. هر زمان که تراکنشی (منظور درخواست انتقال پول از شخص الف به ب) در شبکه فرستاده شود، تمامی اعضای شبکه (گره‌های شبکه) باید به اصالت یا نبود اصالت این تراکنش رأی بدهند. سپس موجودی حساب شخص الف بررسی می‌شود و در صورت بدون اشکال‌بودن، به‌درستی این تراکنش رأی می‌دهند. دفتر کل توزیع‌شده در واقع شامل موجودی حساب هر نشانی نیست، بلکه هر تراکنشی را که در شبکه فرستاده می‌شود ذخیره می‌کند.

برای مثال، شخص الف قصد ارسال پنج بیت‌کوین به شخص ب را دارد. ابتدا ورودی و خروجی‌های حساب شخص الف بررسی می‌شود. در صورتی که در تاریخچهٔ تراکنش‌ها، تعداد بیت‌کوین‌های دریافت‌شده منهای بیت‌کوین‌های ارسال‌شده، همچنان بیشتر از پنج بیت‌کوین باشد، تأیید نهایی انجام می‌شود و در صف اجرای تراکنش قرار می‌گیرد.

حال نقش ماینرها را بررسی می‌کنیم. تراکنش‌های تأییدشده در صف انتظار را ماینرها برای اجرا انتخاب می‌کنند. ماینرها برای حل یک جورچین ریاضی با یکدیگر به رقابت می‌پردازند و هر ماینری که زودتر جورچین را حل کند، برای اجرای تراکنش برگزیده خواهد شد. تراکنش در دفتر کل ثبت خواهد شد. یک نسخه از آن در اختیار تمامی اعضای شبکه قرار می‌گیرد و از آن پس توسط تمامی اعضای شبکه قابل‌رؤیت خواهد بود. در انتها ماینر پاداش ثبت تراکنش در بلاک را خواهد گرفت. برای مثال، در شبکهٔ بلاک‌چین بیت‌کوین پاداش مقداری بیت‌کوین است که به ماینر انجام‌دهندهٔ تراکنش فرستاده خواهد شد.

مزایای اثبات کار

استفاده از گواهی اثبات کار، هک و دست‌کاری بلاک‌چین را تقریباً غیرممکن می‌کند، چرا که برای هک باید قدرتی بالاتر از قدرت ۵۱ درصد شبکه را به دست آورد. به همین علت، هزینهٔ ازبین‌بردن بلاک‌چین بسیار بالاتر از منافع آن است.

همچنین، با استفاده از این روش اجماع، امکان دو بار خرج‌کردن یک کوین از بین می‌رود. منظور از دو بار خرج‌کردن این است که در صورتی که فرد الف یک بیت‌کوین داشته باشد که بخواهد به فرد ب بفرستد، فرد الف امکان فرستادن همان یک بیت‌کوین به شخص دیگر را ندارد.

معایب اثبات کار

بزرگ‌ترین چالش پیش روی اثبات کار، به قدرت محاسباتی حل جورچین ریاضی برای اجرای تراکنش مربوط است، چرا که برای داشتن این قدرت به داشتن سخت‌افزار و تجهیزات پیشرفته نیاز است.

و این تجهیزات و رایانه‌های پیشرفته ذاتاً برق و انرژی زیادی مصرف می‌کنند. علاوه بر این، این ماشین‌ها برای عملیاتی‌ماندن و جلوگیری از گرمای بیش‌ازحد و همچنین آسیب‌های مربوط به قطعات سخت‌افزاری به دلیل ایجاد حرارت داخلی، به مدیریت گرما یا دستگاه خنک‌کنندهٔ مؤثر نیاز دارند. طبق گزارش‌ها، در سال ۲۰۲۱، ماینرهای بیت‌کوین مسئول مصرف حدود ۹۰ تراوات ساعت برق در سال بودند. این بیشتر از برق مصرفی سالانه برای تأمین انرژی فنلاند است که کشوری با ۵٫۵ میلیون نفر جمعیت است. همچنین، تقریباً ۰٫۵ درصد از مصرف جهانی برق در سراسر جهان است. کارمزدهای بالای شبکهٔ اثبات کار از معایب بزرگ این شبکه است.

اشکال‌های اثبات کار دلیل مهمی را نشان می‌دهد که چرا دیگر برنامه‌های بلاک‌چین از سازوکارهای اجماع جایگزین مانند اثبات سهام استفاده کرده‌اند. اثبات کار، روش اجماع مهم‌ترین بلاک‌چین‌هایی چون بیت‌کوین، لایت‌کوین و اتریوم ۱٫۰ است. و اتریوم، با توجه به این مشکلات، به سمت روش اثبات سهام حرکت کرد که در مبحث آینده به آن می‌پردازیم.

پی‌نوشت‌ها

1. Proof of Work
2. Proof of Stake