پارسا رهبران × هنرجوی هنرستان سمپاد امیرکبیر مشهد ×

قسمت سوم

اجماعی برای محیط‌زیست

در قسمت‌های اول و دوم با مفهوم دفتر کل توزیع‌شده و اجماع آشنا شدیم. دانستیم که در واقع اجماع توافقی است بین اعضای شبکه، برای تأیید و ثبت تراکنش‌ها در شبکهٔ بلاک‌چین. با الگوریتم اجماع بیت‌کوین آشنا شدیم که همان الگوریتم اثبات کار است. الگوریتم اثبات کار با وجود امنیت بالای خود، مشکلاتی محیط زیستی را سبب می‌شود و برق و انرژی زیادی مصرف می‌کند؛ همان‌طور که در سال گذشته شاهد مشکلات فراوانی برای کمبود برق در کشورمان بودیم.

در این قسمت الگوریتم اجماع دیگری را معرفی می‌کنیم که تا حدود زیادی این مشکلات را حل خواهد کرد.

الگوریتم اجماع اثبات سهام[1]

به‌طور کلی، الگوریتم‌های اجماع دو هدف کلی را دنبال می‌کنند:

۱. ایجاد بلاک

۲. امنیت

ماینرها با قدرت پردازش خـــود، برای حل یک جورچین ریاضی با یکدیگر رقابت می‌کنند و هر ماینری که قدرت پردازش بالاتری داشته باشد، شانســـش برای یافتن بلاک افزایش خواهد یافت. ماینر برنده، علاوه بر ایجاد بلاک، جایزهٔ ثبت تراکنش را در بلاک دریافت می‌کند. همچنین، امکان دست‌کاری و رخنه(هک) در شبکهٔ بلاک‌چین تقریباً غیرممکن است. برای آسیب‌رساندن به امنیت این شبکه، کافی است افراد بخش زیادی از قدرت پردازشی شبکه را در اختیار بگیرند که به آن حملهٔ ۵۱ درصد نیز گفته می‌شود. اما هزینهٔ چنین حملاتی بسیار بالاست و توجیه اقتصادی ندارد.

ما در الگوریتم اثبات سهام (pos) ماینری نداریم. پس بلاک‌ها چگونه ایجاد می‌شـــوند؟ همچنین، چگونه می‌توانیم در این الگوریتم امنیت را برقرار کنیم؟

در ساختار POS ماینر نداریم و به‌جای ماینر از اعتبارسنج‌ها استفاده می‌شود. اما این اعتبارسنج‌ها[2] چگونه کار می‌کنند؟

با یک مثال این عملکرد را بررسی می‌کنیم. کارخانه‌ای را فرض کنید که ســـهام‌داران بسیاری دارد. اگر بخواهید شما در تصمیم‌گیری‌های ادارهٔ این کارخانه حق رأی داشـــته باشید، باید حتماً بخشی از سهام کارخانه را دارا باشید. هر چقدر تعداد سهام بالاتری داشته باشید، قدرت و رأی شما قدرت و وزن بالاتری دارد.

عملکرد اثبات ســـهام مشابه چنین عملکردی است. اگر قرار است فردی جزو اعتبارسنج‌های شبکهٔ بلاک چین با الگوریتم POS باشد، باید حتماً رمز ارز بومی شبکه را خریداری و در شبکه، به‌عنوان وثیقه، سپرده‌گذاری کند که به‌اصطلاح به آن استیک[3] گفته می‌شود. زمانی که دارایی خود را وثیقه‌گذاری کند، رمز ارز خریداری‌شده در شبکه قفل می‌شود و فرد حق برداشت از آن را ندارد، مگر زمانی که قصد خروج از اعتبارسنجی را داشته باشد.

نحوهٔ ثبت بلاک جدید و دریافت پاداش بلاک در این الگوریتم به چه صورت است؟

در الگوریتم اثبات کار ماینرها برای حل یک جورچین ریاضی رقابت می‌کنند، اما در این روش رقابتی بین اعتبارسنج‌ها نیست و نود اعتبارسنج طی یک فرایند تصادفی انتخاب می‌شوند. با این توضیح که برای این انتخاب عوامل (فاکتورهای) خاصی در نظر گرفته می‌شوند که مهم‌ترین‌های آن‌ها مقدار دارایی سپرده‌گذاری شده و مقدار سپرده‌گذاری‌شده[4] است. هر چقدر میزان دارایی سپرده‌گذاری‌شده بیشتر باشد، اعتبارسنج برای انتخاب از شانس بالاتری برخوردار است. برگ خرید دوم مدت‌زمان سپرده‌گذاری دارایی است، که هر چه فرد زمان بیشتری دارایی خود را سپرده‌گذاری کرده باشد، اعتبارسنج شانس بیشتری برای انتخاب دارد.

چگونه به اعتبارسنج تبدیل شویم؟

برای تبدیل‌شدن به اعتبارسنج، داشتن یک رایانهٔ کیفی و اتصال دائم به اینترنت برای این شبکه‌ها کافی است. همچنین، فرد باید مقداری از رمز ارزهای آن شبکه را خریداری و در شبکه سپرده‌گذاری کند. پس از سپرده‌گذاری، این دارایی قفل می‌شود و قابل استفاده نخواهد بود، مگر زمانی که فرد تصمیم بگیرد دارایی خود را از شبکه خارج کند. پس از گذشت مدتی مشخص، این دارایی آزاد می‌شود و قابل استفاده خواهد بود.

به‌عنوان مثال، اتریوم برای سپرده‌گذاری، حداقل ۳۲ رمز ارزِ اتر درخواست کرده است که رقم بسیار بالایی محسوب می‌شود. عموماً یک مجموعه استخرهای سپرده‌گذاری (استیکینگ) وجود دارد که می‌توان هر مقدار دارایی را در آن‌ها قرار داد و با در اختیارِ یک استخر استیکینگ قراردادنِ دارایی خود، در سود آن استخر سهیم شد.

معایب و مزایای الگوریتم اثبات سهام

در روش اثبات سهام به تجهیزات پیچیده برای حل توابع ریاضی و رسیدن به هش معتبر برای ایجاد بلاک جدید نیاز نیست. در واقع استفاده از روش PoS ۹۹ درصد از مصرف انرژی را در مقایسه با روش PoW صرفه‌جویی می‌کند.

یکی دیگر از تفاوت‌های مهم، هزینهٔ ابتدایی بسیار پایین برای ورود، در مقایسه با شبکه‌های PoW مانند بیت‌کوین است که به سرمایهٔ اولیهٔ بالایی نیاز دارد. خرید دستگاه‌های ماینر، تأمین انرژی برای راه‌اندازی آن‌ها و همچنین تعمیرات و نگهداری از این تجهیزات حساس، به‌طور عمده هزینه‌بر است و همهٔ افراد به مشارکت در این شبکه‌ها قادر نیستند. اما در مورد PoS این‌طور نیست. تقریباً در این روش به سرمایهٔ اولیه نیاز نیست و در نتیجه افراد بیشتری می‌توانند در شبکه مشارکت کنند.

یکی دیگر از مزایا، امنیت در این شبکه است. هرچند در الگوریتم PoS احتمال حملهٔ ۵۱ درصد به‌صورت کامل از بین نمی‌رود، با این‌حال احتمال آن بسیار کاهش می‌یابد. زیرا در این روش فرد یا گروه مهاجم باید بخش قابل‌توجهی از دارایی خود را در معرض خطر قرار دهند. همچنین، پس از وقوع این حمله، قیمت رمز ارز این شبکه قطعاً کاهش جدی می‌یابد و این افراد از این حیث نیز متضرر خواهند شد. در نتیجه، این حمله توجیه اقتصادی ندارد و افراد انگیزهٔ اقتصادی انجام این کار را ندارند.

اما با این حال این الگوریتم معایبی هم دارد. به دلیل سپرده‌گذاری رمز ارز در شبکه، گردش آن محدود می‌شود و کاربری آن پایین می‌آید. همچنین، از آنجا که همه نمی‌توانند حداقل میزان رمز ارز را برای اعتبارسنجی فراهم کنند (برای مثال ۳۲ اتر در شبکهٔ اتریوم)، برای اعتبار سنجی باید رمز ارز خود را در اختیار بعضی استخرها قرار دهند که این نیز زمینه‌های کلاه‌برداری در این زمینه را فراهم می‌کند و ممکن است افراد دارایی خود را از دست بدهند. همچنین، با قفل‌شدن دارایی در شبکه، دسترسی به دارایی کاهش می‌یابد و کاربران، در صورت نیاز به دارایی خود، با مشکلاتی روبه‌رو می‌شوند.

با این حال، الگوریتم اثبات سهام در مقایسه با الگوریتم اثبات کار قطعاً فایده‌های بیشتری دارد که اتریوم به‌عنوان یکی از مهم‌ترین بلاک‌چین‌های حال حاضر، الگوریتم اجماع خود را از اثبات کار به اثبات سهام تبدیل کرد.

پی‌نوشت‌ها

1. Proof Of Stake
2. Validator
3. stake
4. stake