سختی استخراج چیست؟ + بررسی سختی استخراج کریپتو

سختی شبکه به زبان ساده

سختی شبکه یا سختی استخراج واحدی برای اندازه گیری نسبی شرایط لازم، جهت ایجاد یک بلاک جدید در بلاک چین است. سختی شبکه سختی پیدا کردن تابع هش بلاک یا حل بلاک در مدت زمان مدنظر را نشان می‌دهد و مقدار سختی توابع هش، سختی شبکه نام دارد.

به عبارتی سختی شبکه تعیین می‌کند که یک ماینر در چه مدت زمانی می‌تواند تابع هش بلاک را پیدا کرده و با این کار بلاک جدید را تولید و به زنجیره قبلی اضافه کند.با استفاده از سختی شبکه می‌توان شرایط ایجاد بلاک را به‌طور نسبی بررسی کرد.

به عنوان مثال هنگامی که گفته می‌شود **سختی شبکه بلاک چین** ارزدیجیتالی مانند بیت کوین (16,549BTC) زیاد است، این مسئله نشان می‌دهد که برای تایید تراکنش‌های وارد شده در یک بلاک چین به قدرت محاسباتی بیشتری نیاز است.

از سختی استخراج به عنوان یکی از مهم‌ترین معیارها در ارزیابی بلاک چین یاد می‌شود، چراکه که هرچه سختی شبکه بیشتر باشد، شبکه بلاک چین در برابر حملات مخرب مقاوم‌تر عمل می‌کند.

نحوه عملکرد سختی استخراج

در بلاک چین رمزارزهای مبتنی بر اثبات کار مانند بیت کوین، هش ریت باید با سختی استخراج همخوانی داشته باشد و یک هش زمانی معتبر است که برابر و یا کمتر از مقدار هش هدف تعیین شده باشد.

هش به‌صورت خودکار توسط پروتکل هر ارز محاسبه می‌گردد و هرچه مقدار فاصله مجاز میان هش به دست آمده توسط ماینرها و هش هدف کمتر باشد، ماینرها باید تابع هش را با دفعات بیشتری اجرا کنند تا به مقدار مناسبی برسند.

با افزایش سختی استخراج، ماینرها مجبور هستند که به‌صورت متوسط برای هر بلاک، توان رایانشی بیشتری مصرف نمایند تا موفق به یافتن هش معتبری شوند. توان هش یک شبکه ارزی، تمامی هش ریت دستگاه‌های استخراج ارز دیجیتال را نشان می‌دهد.

هر هش به‌صورت تصادفی تولید می‌شوذ و پیش از یافتن هش معتبر، ممکن است میلیون‌ها هش تولید گردد. پس از یافتن هش معتبر، کوین‌های جدید ایجاد شده و در قالب پاداش به ماینر برنده اعطا می‌شود.

اهمیت سختی استخراج

اگر سختی شبکه وجود نداشته باشد با افزایش تعداد ماینرها، میانگین مدت زمان پیدا شدن هر بلاک به کمتر از ده دقیقه کاهش پیدا می‌کند و به این صورت هیچ‌گونه محدودیتی برای ماینرها ایجاد نمی‌شود و بلاک‌ها در زمانی کمتر از مدت زمان تعیین شده ایجاد می‌گردند.

البته لازم به ذکر است که امکان دارد این زمان به ثانیه‌ها نیز کاهش پیدا کند و منجر به خلق مشکل تورم و تولید بی رویه ارزهای دیجیتال شود. اگر سختی شبکه ثابت باشد، هرچه ماینر جدید به شبکه افزوده گردد زمان کمتری برای اضافه کردن بلاک‌های جدید به بلاک چین صرف می‌شود.

سختی استخراج یا شبکه از این نظر اهمیت دارد که با افزایش یا کاهش ماینرها، شبکه به‌طوری تعادل پیدا می‌کند که در نهایت برای ایجاد هر بلاک، 10 دقیقه زمان صرف می‌شود و به این وسیله می‌توان میانگین زمان تولید هر بلاک در بلاک چین را بدون تغییر نگهداری کرد.

سختی استخراج ارزهای دیجیتال

هر رمزارزی که از اثبات کار برای تایید و اعتبارسنجی تراکنش‌ها استفاده کند، برای کنترل افزایش و کاهش تعداد ماینرها به سختی شبکه نیازمند است. البته اغلب افراد تنها بیت کوین را به عنوان ارز قابل استخراج می‌دانند اما ارزهای دیگری نیز وجود دارند که گزینه مناسبی برای استخراج هستند. از میان این رمزارزهای متعدد می‌توان به مونرو (138.2XMR)، زی کش (41.70ZEC)، گرین (0.0382GRIN)، لایت کوین (74.8LTC)، بیت کوین کش (113.3BCH)، دوج کوین (0.0889DOGE) اشاره کرد.

سختی شبکه بیت کوین (Bitcoin)

سختی شبکه بیت کوین با هر 2016 بلاک جدید و هر دو هفته تغییر می‌یابد؛ یعنی هر بار که 2016 بلاک جدید در زنجیره بلاک‌ها ساخته شود، برای تولید هر بلاک زمانی حدود 10 دقیقه صرف می‌گردد. با افزایش تعداد ماینرها، زمان استخراج بلاک در شبکه کم می‌شود و بلاک‌های بیشتری در مدت زمان کم استخراج می‌گردند.

مطلب پیشنهادی : هاوینگ چیست؟

البته بیت کوین‌ها محدود هستند و تنها 21 میلیون واحد از بیت کوین وجود دارد؛ به همین دلیل ساتوشی ناکاموتو**سازنده بیت کوین** برای جلوگیری از این رویداد، برای استخراج بیت کوین مقدار مشخصی سختی مشخص کرد تا یک ماینر بتواند معادلات را حل کرده و بلاک را تولید و به زنجیره بلاک قبلی اضافه کند.

مونرو (Monero)

یکی از بهترین و محبوب‌ترین ارزهای دیجیتال در بازار کریپتوکارنسی‌ها مونرو است. این ارز در سال‌های اخیر با سرعت زیادی پیشرفت کرده و نام آن در میان بیست ارز دیجیتال برتر بازار به چشم می‌خورد.

مونروایمنی زیادی دارد و توانسته با تمرکززدایی محبوبیت زیادی به دست بیاورد و بسیار از افراد را ترغیب به خرید مونرو کند. بیشترین کاربرد این ارز به دلیل آدرس‌های پنهان و پیگیر گریز بودن تراکنش‌ها در موقعیت‌هایی است که به حداکثر محرمانگی نیاز دارند.

زی کش (Zcash)

این ارز را می‌توان یک شبکه پرداخت غیر متمرکز P2P دانست که به کاربران این امکان را می‌دهد تا به‌طور خصوصی تراکنش‌های خود را انجام دهند.

در حقیقت زی کش از یک شبکه پرداخت غیرمتمرکز همتابه‌همتا و مبتنی بر ماینینگ است و امکام تراکنش‌های خصوصی را برای کاربران خود ایجاد می‌کند. کارکرد این ارز به‌صورت اثبات کار (تایید تراکنش‌ها با ماینینگ) است و زی کش با الگوریتم Equihash استخراج می‌شود.

گرین (Grin)

برخلاف بیت کوین، در تولید گرین هیچ محدودیتی وجود ندارد و گرین را می‌توان اولین پیاده سازی از پروتکل میمبل ویمبل دانست. این ارز با استاندارد اثبات کار فعال است و در دسته بندی ارزهای قابل استخراج قرار می‌گیرد.

مزایای افزایش سختی استخراج

شاید در مرحله اول به نظر برسد که افزایش سختی استخراج ویژگی منفی برای بلاک چین است اما افزایش سختی استخراج مزایای مهمی نیز دارد:

ثابت نگه داشتن نرخ ایجاد بلوک‌های جدید

ساتوشی ناکاموتو در وایت پیپر بیت کوین می‌گوید که سختی شبکه به چه شکلی باعث تولید پایدار و مداوم بلوک‌های جدید با نرخی ثابت می‌شود. الگوریتم اثبات کار به شکلی تعریف شده که در صورت افزایش بیش از اندازه سرعت تشکیل بلوک‌ها، سختی شبکه نیز به‌صورت خودکار بیشتر می‌شود.

این مسئله باعث شده تا زمان تشکیل هر بلوک در بلاک چین بیت کوین حدود 10 دقیقه طول بکشد. الگوریتم اثبات کار برای ثابت نگه داشتن این زمان به‌صورت خودکار هش بولک را تنظیم می‌نماید و سختی بیشتر یا کمتر می‌شود که زمان یافتن بلوک در مقایسه با عدد پیش فرض کمتر شود.

برای اینکه این اتفاق نیوفتد، شبکه به‌طور خودکار سختی استخراج را افزایش می‌دهد و این موضوع تا زمان پیدا کردن بلوک به همان عدد پیش فرض ادامه پیدا می‌کند. هنگامی که ناکاموتو اولین بلوک را در **زنجیره بیت کوین** استخراج کرد، تنها یک دستگاه احتمالا ساده در شبکه وجود داشت اما امروزه ده‌ها هزار دستگاه پیشرفته با نام

ASIC در سراسر دنیا فعال هستندو با تغییر سختی شبکه عملا نرخ ایجاد بلوک‌های جدید در زنجیره ثابت باقی می‌ماند.

حفظ امنیت شبکه

افزایش سختی قدرت شبکه، همان افزایش قدرت هش کلی در بلاک چین است که این اتفاق امنیت شبکه بلاک چین را ارتقا می‌دهد. در حقیقت هکرها برای موفقیت در دستیابی به بلوک‌های یک زنجیره، باید بر قدرت هش آن شبکه غلبه نمایند.

با افزایش یافتن سختی استخراج، دسترسی هکرها نیز دشوارتر می‌شود؛ به عنوان مثال هزینه حمله هکری به شبکه بیت کوین در حال حاضر به حدی زیاد است که انجام آن تقریبا برای هیچ فردی امکان پذیر نیست.

سختی استخراج؛ کلیدی برای بقای بلاک چین

سختی شبکه یا سختی استخراج واحدی برای اندازه گیری نسبی شرایط لازم، جهت ایجاد یک بلاک جدید در بلاک چین است. بدون شک اگر سختی استخراج وجود نداشته باشد، شبکه از کار می‌افتد و اگر مقدار این سختی کنترل نگردد و میزان سختی صرفه اقتصادی نداشته باشد دیگر هیچ کاربری حاضر به ادامه استخراج نمی‌شود و تمامی تراکنش‌ها بدون تایید باقی می‌مانند.

تمامی این موارد باعث می‌شوند عمر بلاک چین به پایان برسد؛ بنابراین **اهمیت سختی استخراج** یا سختی شبکه غیرقابل انکار است. هر رمزارزی که از اثبات کار برای تایید و اعتبارسنجی تراکنش‌ها استفاده کند، برای کنترل افزایش و کاهش تعداد ماینرها به سختی شبکه نیازمند است که از این رمزارزها می‌توان به بیت کوین، مونرو، زی کش، گرین، لایت کوین، بیت کوین کش و دوج کوین و اشاره کرد.

در این مطلب از وبلاگ کیف پول من به مفهوم سختی استخراج پرداختیم؛ برای آشنایی بهتر با مفاهیم دنیای ارزهای دیجیتال می‌توانید به وبلاگ کیف پول من مراجعه نمایید.