اثبات سهام چیست؟

آشنایی با مکانیزم اجماع (Consensus Mechanism)

مکانیزم اجماع، مکانیسم تحمل خطا است که در سیستم‌های رایانه‌ای و بلاک چین به‌منظور دستیابی به توافق لازم بر روی مقداری داده، وضعیت واحد شبکه در میان فرآیندهای توضیع شده یا سیستم‌های چندعاملی مثل رمزارزهای دیجیتال استفاده می‌شود.

این مکانیزم به روش‌های مورد استفاده برای دستیابی به توافق، امنیت و اعتماد در شبکه کامپیوتری غیرمتمرکز اشاره می‌کند. الگوریتم اثبات سهام (**PoS**) و اثبات کار (**PoW**) دو نمونه از رایج‌ترین مکانیسم‌های اجماع هستند که می‌توان به آن اشاره کرد. همچنین مکانیزم اجماع به روش‌های مورد استفاده برای دستیابی به توافق، اعتماد و امنیت در یک شبکه کامپیوتری غیرمتمرکز اشاره می‌کند.

آشنایی با الگوریتم اثبات سهام (Proof of Stake)

الگوریتم اثبات سهام یکی از روش‌های حفظ امنیت شبکه بلاک چین است و از چاپ سکه‌های اضافی توسط کاربران جلوگیری می‌کند. این الگوریتم نوع متفاوتی از مکانیزم اجماع است و بلاک چین‌ها می‌توانند به‌منظور توافق برای یک ثبت واقعی، از تاریخچه داده استفاده کنند.

بر اساس الگوریتم اثبات سهام گروهی از افراد جامعه بلاک چین، به عنوان اعتبار سنجی (Validator) عمل می‌کنند و وظیفه دارند با اجرای قوانینی در ارتباط با اثبات از طریق سهام، تراکنش‌ها را اعتبار سنجی کرده و امنیت شبکه را تامین کنند.

این الگوریتم تمرکززدایی در قلب فناوری بلاک چین و رمزارزها محسوب می‌شود و هیچ سازمان مرکزی برای مدیریت تراکنش‌ها و داده‌های موجود در بلاک چین وجود ندارد. هدف این الگوریتم حل مشکل وابستگی به انرژی برق برای تولید بلاک‌های جدید در مکانیسم اثبات کار است.

این مکانیسم با استفاده از قوانینی مشخص، نود بعدی تولید کننده بلاک جدید را به‌صورت تصادفی انتخاب می‌کند و نقش نود انتخاب شده، تراکنش بلاک، تایید اعتبار و امضای آن برای شبکه اعتبارسنجی است.

عملکرد الگوریتم اجماع اثبات سهام (PoS)

در اثبات سهام، کاربران به مقدار دلخواه خود سهام یا سرمایه به شبکه پرداخت می‌نمایند و باتوجه به سهامی که به شبکه سپرده‌اند، می‌توانند در اثبات سهام شرکت کرده و بلاک‌های جدید را به شبکه اضافه کنند.

سهامی که کاربران به شبکه سپرده‌اند، قابلیت بازگشت دارد و هر زمانی که بخواهند می‌توانند وجوه خود را از شبکه باز پس بگیرند. اثبات سهام از فرایند انتخاباتی شبه تصادفی استفاده می‌کند تا هر بار یک نود را برای تایید بلاک بعدی انتخاب کند.

فرآیند انتخاب کردن گره‌های تایید کننده به این دلیل شبه تصادفی است که علی رغم انتخاب رندوم، معیارهایی مثل مقدار رمزارز استیک شده توسط آن‌ها و مدت زمان استیکینگ ارز دیجیتال اهمیت زیادی دارند.

بزرگتر بودن این موارد، احتمال انتخاب نودها را افزایش می‌دهد و احتمال انتخاب شدن یک گره به عنوان تایید کننده هنگامی که 1000 توکن بومی آن شبکه به مدت یک ماه استیک شده، بیشتر از کره دیگر با 100 توکن قفل شده در مدت یک هفته می‌شود.

استفاده از استخراج ارز دیجیتال یا ماینینگ در شبکه‌های مبتنی بر الگوریتم اثبات سهام رایج نیست و به جای آن از تایید کردن و یا ساخت بلاک استفاده می‌شود. فورج (Forge) در این مکانیسم به معنی تایید بلاک‌ها و فورجر (Forger) به معنی اعتبار سنج یا همان ولیدتور تراکنش‌ها و تایید کننده بلاک است.

تفاوت PoS و PoW

الگوریتم‌های اثبات سهام و اثبات کار هر دو در انتشار ارزهای رمزنگاری کاربرد دارند اما الگوریتم اثبات کار با وقت و انرژی کمتری این کار را انجام می‌دهد. در اثبات سهام (PoS) بلاک‌ها تولید می‌شوند اما در اثبات کار، بلاک‌ها را از شبکه بلاک چین استخراج می‌کنند.

در الگوریتم اثبات کار در ازای کارکرد ماینرها، کوین‌هایی به عنوان پاداش در اختیار استخراج کنندگان قرار می‌گیرد اما در الگوریتم اثبات سهام از کارمزد تراکنش به اعتبارسنج‌ها پاداش داده می‌شود. توان سخت افزاری در اثبات سهام اهمیتی ندارد و باتوجه به کارکرد بهتر آن نسبت به اثبات کار، قیمت انتشار کوین‌ها کمتر بوده و مصرف انرژی آن نیز پایین‌تر می‌شود.

در الگوریتم اثبات کار استخراج ارزها از طریق سخت افزارهای پیشرفته برای جل معادلات ریاضی استفاده می‌کنند اما در اثبات سهام، تعداد کوین‌ها عامل موثری برای انتخاب به‌منظور ماینر منتخب است.

مزایای استفاده از الگوریتم اثبات سهام

الگوریتم اثبات سهام مزایای زیادی دارد که آن را به عنوان الگوریتمی بهتر و جایگزین تبدیل می‌کنند. در ادامه در مورد مزایای این الگوریتم توضیح می‌دهیم:

مصرف انرژی پایین

اصلی‌ترین مزیت **الگوریتم اثبات سهام درمقایسه با الگوریتم اثبات کار**، صرفه جویی در مصرف انرژی است. الگوریتم اثبات کار انرژی زیادی برای تایید تراکنش‌ها و حفظ امنیت شبکه مصرف می‌کند که این مسئله باعث شده برخی از کشورها فعالیت ماینر ارز دیجیتال را ممنوع کنند.

در اثبات سهام برای تایید تراکنش‌ها به ماینرهای بزرگ نیازی نیست؛ بنابراین برق بسیار کمتری مصرف می‌شود و گرمایش کمتری برای کرده زمین اتفاق می‌افتد. به همین دلیل است که از این روش به عنوان روشی سبز برای ماین ارزهای دیجیتال یاد می‌شود.

سرعت پردازش بالا

تجربه‌های کسب شده نشان می‌دهند که شبکه‌های بلاک چینی که از الگوریتم اثبات سهام استفاده می‌کنند، توان پردازش بیشتری دارند. همچنین در این شبکه‌ها زمان تشکیل هر بلوک به مراتب کاهش می‌یابد و تعداد تراکنش‌هایی که در یک ثانیه پردازش می‌یابند نیز بیشتر می‌شود.

قیمت توکن بومی شبکه

در شبکه‌هایی که از الگوریتم اثبات سهام استفاده می‌شود، بخش قابل توجهی از توکن‌ها قفل می‌گردند. این اتفاق به حفظ ارزش توکن در طولانی مدت کمک می‌کند؛ چراکه فرایند عرضه و تقاضای توکن‌ها در بازار به خوبی کنترل می‌شوند.

مطلب پیشنهادی : فارکس چیست؟

معایب استفاده از الگوریتم اثبات سهام

علاوه بر مزایای منحصربه‌فرد الگوریتم اثبات کار، این گواه معایبی نیز دارد که در ادامه به آن‌ها اشاره می‌کنیم:

اعتبارسنجانی با دارایی زیاد

درباره تمرکززدایی، عملکرد الگوریتم اثبات سهام بسیار بهتر از الگوریتم اثبات کار است اما یکی از تردیدهای موجود در این زمینه، در رابطه با افرادی است که حجم زیادی از کوین‌ها را در اختیار دارند. این افراد می‌توانند با اختصاص دادن کوین‌های خود به شبکه، به یک نود قوی تبدیل شده و بر روی عملیات تایید تراکنش‌ها تاثیر بگذارند.

قفل کردن سرمایه اعتبار سنجان

برخی از شبکه‌های بلاک چینی که با گواه اثبات سهام فعالیت می‌کنند، سرمایه کاربران برای مدت مشخصی قفل می‌کنند. در این شبکه‌های بلاک چین اعتبارسنجان نمی‌توانند زودتر از موعد مشخص، سرمایه خود را خارج نمایند. این موضوع باتوجه به نوسانات زیاد قیمت ارزهای دیجیتال، نارضایتی برخی از اعتبارسنجان را ایجاد کرده است.

رمزارزهای مبتنی بر الگوریتم اثبات سهام

Peercoin اولین ارزی است که در سال 2012 به وجود آمد و از گواه اثبات سهام برای تایید تراکنش‌های خود استفاده می‌کرد. Sunny King و Scott Nadal دو مخترع این روش بودند که برای حل مشکلات اثبات کار، روشی خلاقانه ایجاد کردند.

چندین سال از آن زمان می‌گذرد و امروزه صدها ارز از اثبات سهام استفاده می‌کنند. به عنوان مثال در اتریوم 2 مشارکت کنندگان باید 32 اتر را برای تبدیل شدن به یک ولیدیتور استیک کنند و اگر یک گره به عنوان ولیدیتور انتخاب شده و مدتی آفلاین شود، مقداری از دارایی قفل شده خود را از دست می‌دهد.

کاردانو (0.3256ADA)، پولکادات (5.710DOT)، ایاس (0.9000EOS)، الگورند (0.2666ALGO) ترون (0.0501TRX)، تزوس (0.9803XTZ)،کازموس (9.973ATOM) و غیره از روش‌های منحصربه‌فردی برای رسیدن به اجماع در شبکه خود استفاده می‌کنند که همه آن‌ها نوعی الگوریتم اثبات سهام هستند.

الگوریتم اثبات سهام و دلیل اهمیت آن

الگوریتم اثبات سهام، یک الگوریتم اجماع است که بر اساس این الگوریتم، سهام گروهی از افراد جامعه بلاک چین، به عنوان اعتبار سنجی (Validator) عمل می‌کنند و وظیفه دارند با اجرای قوانینی در ارتباط با اثبات از طریق سهام، تراکنش‌ها را اعتبار سنجی کرده و امنیت شبکه را تامین کنند.

در اثبات سهام، کاربران به مقدار دلخواه خود سهام یا سرمایه به شبکه پرداخت می‌نمایند و باتوجه به سهامی که به شبکه سپرده‌اند، می‌توانند در اثبات سهام شرکت کرده و بلاک‌های جدید را به شبکه اضافه کنند. سهامی که کاربران به شبکه سپرده‌اند، قابلیت بازگشت دارد و هر زمانی که بخواهند می‌توانند وجوه خود را از شبکه باز پس بگیرند.

مطلب پیشنهادی : توکن سوزی چیست؟

این الگوریتم مزایای منحصربه‌فردی مانند مصرف انرژی پایین و سرعت پردازش بالایی دارد و به دلیل این ویژگی‌ها بسیاری از بلاک چین‌ها و ارزهای دیجیتال، بر این الگوریتم مبتنی هستند.

البته این الگوریتم معایب مخصوص خود را مانند هر چیز دیگری دارد اما هنوز هم به عنوان روشی جایگزین برای الگوریتم اثبات کار محسوب می‌شود.

در این مطلب از وبلاگ کیف پول من با الگوریتم اثبات سهام آشنا شده و نحوه کارکرد و مزایای استفاده از آن را توضیح دادیم. برای آشنایی با الگوریتم اثبات کار و سایر مطالب مرتبط می‌توانید به وبلاگ کیف پول من مراجعه کنید.