الگوریتم اثبات مشارکت (PoCo) چیست؟

مروری بر ماهیت الگوریتم اجماع در شبکه‌های بلاک چینی

قبل از آن که بتوانیم مطالبی را در ارتباط با چیستی الگوریتم اثبات مشارکت بیان کنیم، ضرورت دارد که نگاهی اجمالی بر ماهیت خود الگوریتم اجماع داشته باشیم تا از این طریق با دستیابی به یک درک صحیح از علت وجودی چنین الگوریتمی در شبکه‌های بلاک چینی، مطالبی که در ادامه به آن‌ها پرداخته خواهد شد را مطالعه نمائید. الگوریتم اجماع (Consensus Algorithm) در واقع همان پروتکلی است که مانع از ایجاد هرج و مرج در شبکه‌های غیرمتمرکز بلاک چینی می‌شود. به بیان بهتر، در شبکه‌های بلاک چینی، بر خلاف سیستم‌های متمرکز ما با یک دفتر کل مواجه نیستیم، بلکه دفتر کل شبکه‌های بلاک چینی در میان نودها توزیع شده و هر یک از آن‌ها یک نسخه از این دفتر کل را در اختیار دارند و دقیقا به همین علت است که امکان هرگونه تحریف اطلاعات در شبکه‌های بلاک چینی وجود ندارد.

اما به هنگامی که از توزیع شدگی شبکه بلاک چین و عدم تمرکز سخن می‌گوئیم، این بدان معنا خواهد بود که بازیگران فعال در حوزه تائید تراکنش افزایش یافته و به دلیل نبود یک نهاد مرکزی برای نظارت بر فعالیت آن‌ها (نظیر آنچه که در سیستم‌های متمرکز وجود دارد) احتمال اعمال سلیقه‌های متفاوت در تائید یا عدم تائید تراکنش‌ها افزایش می‌یابد که چنین مسئله‌ای می‌تواند در نهایت به فروپاشی کامل یک شبکه بلاک چینی منجر گردد. تیم‌های توسعه دهنده شبکه‌های بلاک چینی با تسلط بر این نکته از یک الگوریتم اجماع برای نظارت بر فعالیت ماینرها و ولیدیتورها کمک گرفته‌اند تا اشخاص یاد شده متناسب با قوانین بلاک چین تراکنش‌ها را تائید کنند و به بیان ساده‌تر، اعتبار سنج‌ها در تائید تراکنش‌ها و ایجاد بلاک جدید از اختیار و اعمال سلیقه

برخوردار نیستند و حتما باید از قوانین موجود در شبکه بلاک چینی تبعیت کنند؛ در غیر این صورت با مجازات‌هایی همچون جریمه اسلشینگ (Slashing Penalty) که در الگوریتم اجماع اثبات سهام (Proof of Stake) وجود دارد، مواجه خواهند شد.

آشنایی با چیستی الگوریتم اثبات مشارکت (PoCo)

یکی از الگوریتم‌های اجماع جدیدی که از سوی پلتفرم آی اگزک (iExec)، یکی از شبکه‌های وابسته به اتریوم، راه‌اندازی شده است، **الگوریتم اثبات مشارکت (Proof of Contribution)** نام دارد و در این الگوریتم اجماع، مبنای اصلی اعتماد شبکه‌های بلاک چینی به ولیدیتورها و اعتبارسنج‌ها، میزان مشارکت آن‌ها در نظر گرفته شده است. در واقع در الگوریتم اجماع اثبات مشارکت هم به مشارکت کاربران و هم به محاسبه نرخ هش (Hash Rate) نیاز داریم تا مرحله تائید صلاحیت کاربران را به درستی پشت سر بگذاریم و عملا کلیه نودها و گره‌های فعال در شبکه بلاک چینی که از الگوریتم اثبات مشارکت بهره می‌برند از طریق ارزیابی مولفه‌های خاصی انتخاب می‌شوند و در نهایت آن دسته از کاربرانی که بیشترین میزان مشارکت در شبکه را به خود اختصاص دهند، می‌توانند بلاک جدید را در بلاک چین استخراج نمایند.

اگر نگاهی موشکافانه به الگوریتم اثبات مشارکت داشته باشیم، متوجه خواهیم شد که این الگوریتم اجماع با وجود تمرکز بر روی مشارکت کاربران، همچنان رتبه خوبی را به لحاظ تمرکززدایی دریافت می‌کند و عملا در برابر هارد فورک نیز از انعطاف‌پذیری خوبی برخوردار است. در الگوریتم اثبات مشارکت، نودها قسمتی از توان و قدرت محاسباتی خویش را به امر اعتبارسنجی تراکنش‌ها اختصاص می‌دهند و سپس میزان مشارکت‌های گره‌ها مورد مقایسه قرار می‌گیرد و در صورتی که چندین گره نتایج کاملا یکسانی را ارائه کرده باشند، در این صورت پاداش اعتبارسنجی به طور مساوی در میان نودهای مشارکت کننده توزیع می‌گردد. به بیان بهتر، الگوریتم

اثبات مشارکت رویکردی مشابه الگوریتم اثبات کار دارد ولی تمرکز خویش را بر روی کاهش میزان انرژی مورد نیاز برای فرآیند ماین و استخراج گذاشته و از این طریق سود بیشتری را عاید ولیدیتورها می‌نماید. وجود چنین سطح از همکاری در میان اعضای شبکه، آن‌ها را به انجام صحیح وظایف و ایمن‌تر شدن شبکه تشویق می‌نماید.

مطلب پیشنهادی: استخر سیاه چیست؟

به طور خلاصه در الگوریتم اثبات مشارکت، علاقه‌مندان به شرکت در فرآیند اعتبارسنجی بلاک‌ها در قدم اول یک سپرده امنیتی را به اشتراک می‌گذارند و سپس در طول جلسه اجماع پروتکل‌های اثبات مشارکت کلیه مشارکت نودها در داخل شبکه را دنبال می‌کنند و در نهایت آن دسته از نودهایی که بیشترین میزان مشارکت در شبکه را به خود اختصاص داده‌اند، مجوز تولید بلاک جدید را دریافت می‌کنند و در ازای ایجاد بلاک جدید، پاداش دریافت می‌کنند. یکی از ویژگی‌های مهم الگوریتم اثبات مشارکت، فراهم شدن امکان ایجاد اعتماد کافی برای اجماع محاسباتی در خارج از محیط شبکه بلاک چین (جایی مثل فضای ابری که کلیه سازوکار الگوریتم اثبات مشارکت در آن اجرا می‌شود) است.

مقایسه الگوریتم اثبات مشارکت با سایر الگوریتم‌های اجماع

در الگوریتم‌های مشهور موجود در دنیای کریپتوکارنسی، یعنی الگوریتم‌های اثبات کار و اثبات سهام ما با یک ویژگی منفی روبه‌رو هستیم که این ویژگی منفی عبارت است از این که هر گره و کاربری که به منابع محاسباتی بیشتری دسترسی داشته باشد، برنده فرآیند استخراج خواهد بود و سایر نودها دارای شانس بسیار کمتری در دریافت پاداش شبکه هستند و این در حالی است که در الگوریتم اثبات مشارکت، امکان مشارکت در روند اعتبارسنجی تراکنش‌ها به کلیه نودها اعطا می‌شود و کلیه اعضای شبکه از شانس خوبی برای دریافت پاداش شبکه برخوردار هستند و عملا الگوریتم اثبات مشارکت با این هدف طراحی شده است که در دنیای کریپتوکارنسی نباید هیچگونه مشارکتی به هدر رود.

از سوی دیگر در کلیه الگوریتم‌های اجماع (بجز الگوریتم اثبات مشارکت PoCo) با همبستگی تصاعدی منابع محاسباتی و سرمایه‌گذاری اقتصادی روبه‌رو هستیم، که وجود چنین مسئله‌ای سبب می‌شود تا قدرت و منابع محاسباتی در ساختار آن‌ها متمرکز شده و در نهایت شبکه مورد تهدید قرار می‌گیرد که چنین مسئله‌ای می‌تواند در طولانی مدت بر قیمت رمزارزها تاثیر گذاشته و خرید بیت کوین یا خرید اتریوم را تحت تاثیر قرار دهد.

مزایای استفاده از الگوریتم اثبات مشارکت در شبکه بلاک چینی

به طور کلی به هنگامی که در مقام **مقایسه الگوریتم اثبات مشارکت** با سایر الگوریتم‌های اجماع برمی‌آییم، متوجه وجود برخی مزایای برجسته می‌شویم که بررسی آن‌ها در دستیابی به درکی روشن از ماهیت الگوریتم اثبات مشارکت چندان خالی از لطف نخواهد بود. از **مزایای الگوریتم اثبات مشارکت** می‌توان به موارد زیر اشاره کرد:

- در الگوریتم اثبات سهام با اتخاذ رویکردی متعادل مانع از هدر رفت انرژی مصرفی از سوی ولیدیتورها می‌شود.
- الگوریتم اثبات مشارکت از میزان انعطاف بیشتری در مقایسه با سایر الگوریتم‌های اجماع برخوردار است.
- از سطح امنیتی خوبی برخوردار است.

الگوریتم اثبات مشارکت؛ الگوریتمی بهینه و امن برای شبکه‌های بلاک چینی

الگوریتم اجماع همان پروتکلی است که در شبکه های بلاک چینی، وظیفه حفظ امنیت و درستی فعالیت نودها را بر عهده دارد و مانع اعمال خودسرانه اعتبارسنج‌ها در تائید تراکنش‌ها یانجام یافته در شبکه و ایجاد بلاک‌های جدید می‌گردد. از زمان ظهور دنیای کریپتوکارنسی تا به امروز الگوریتم‌های اجماع متعددی با هدف جلوگیری از انجام حملات دوبار خرج کردن و دابل اسپندینگ طراحی و اجرا شده است که یکی از این الگوریتم های نوپا، الگوریتم اثبات مشارکت نام دارد که به دلیل مزایای برجسته آن در مقایسه با سایر الگوریتم‌ها مورد توجه بسیاری از پروژه های رمزارزی قرار گرفته است و به همین علت ما این مقاله از بلاگ کیف پول من را به بررسی جامع این الگوریتم محبوب اختصاص دادیم.

همان طور که در مطالب فوق مشاهده کردید، این الگوریتم به لحاظ ماهیتی به الگوریتم اجماع اثبات کار شباهت دارد و تفاوت اصلی این الگوریتم با الگوریتم PoW در این نکته خلاصه شده است که در الگوریتم اثبات مشارکت صرفا توان محاسباتی ملاک اعطای پاداش بلاک نبوده و میزان مشارکت نودها نیز در نظر گرفته می‌شود و از این طریق نه تنها از هدر رفت انرژی جلوگیری به عمل می‌آید، بلکه سیستم اعطای پاداش نیز عادلانه میان کلیه نودهایی که میزان مشارکت بالایی در شبکه داشته‌اند، پخش می‌شود. ناگفته نماند که اگر در ارتباط با چیستی الگوریتم اثبات مشارکت سوالی دارید که به پاسخ آن در مطالب فوق اشاره‌ای نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.