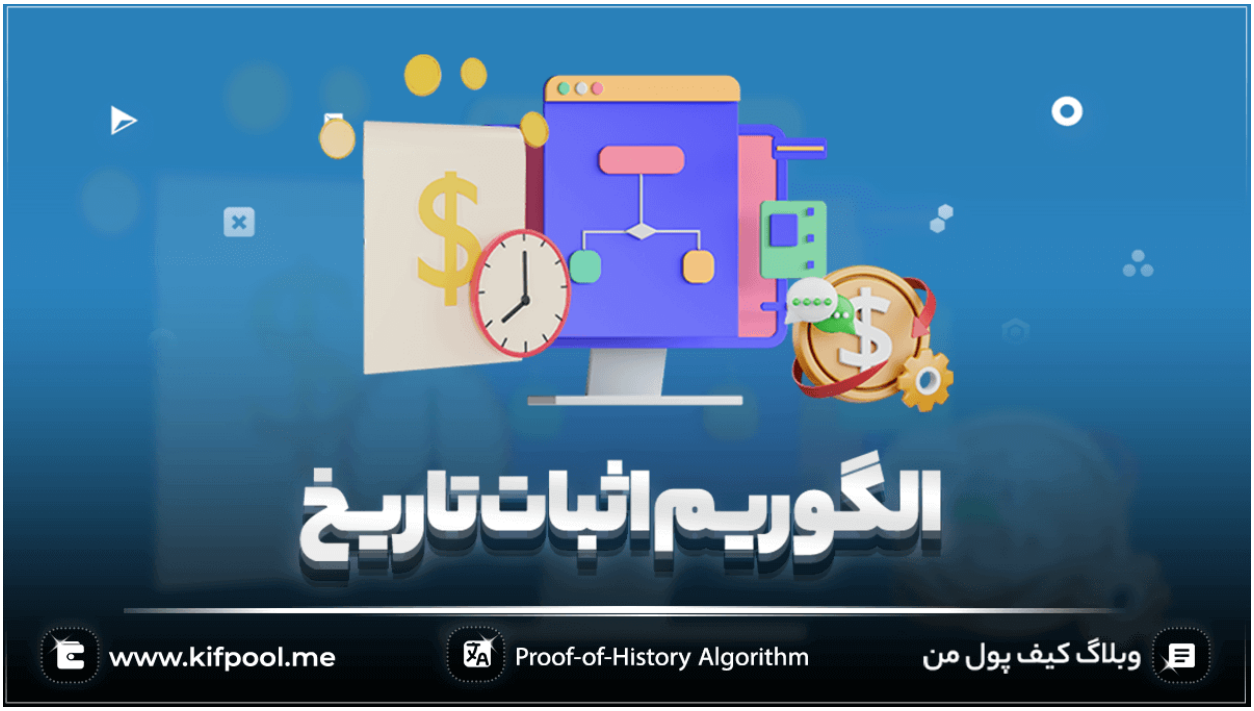


الگوریتم اثبات تاریخ

الگوریتم‌های اجماع در بازار کریپتوکارنسی برای حفظ امنیت شبکه مورد استفاده قرار می‌گیرند. **الگوریتم اجماع اثبات تاریخ** (الگوریتم اثبات) یا همان **proof of history** یکی از الگوریتم‌های جدیدی است که در سال 2017 شروع به کار کرده و رویدادها را در مدت زمان خاص، مشخص می‌کند. اجماع اثبات تاریخ الگوریتمی برای بلاک چین سولانا است. برای آشنایی بیشتر با این الگوریتم و نحوه کارکرد آن تا انتهای این مقاله از **کیفپولمن** ما را همراهی کنید.

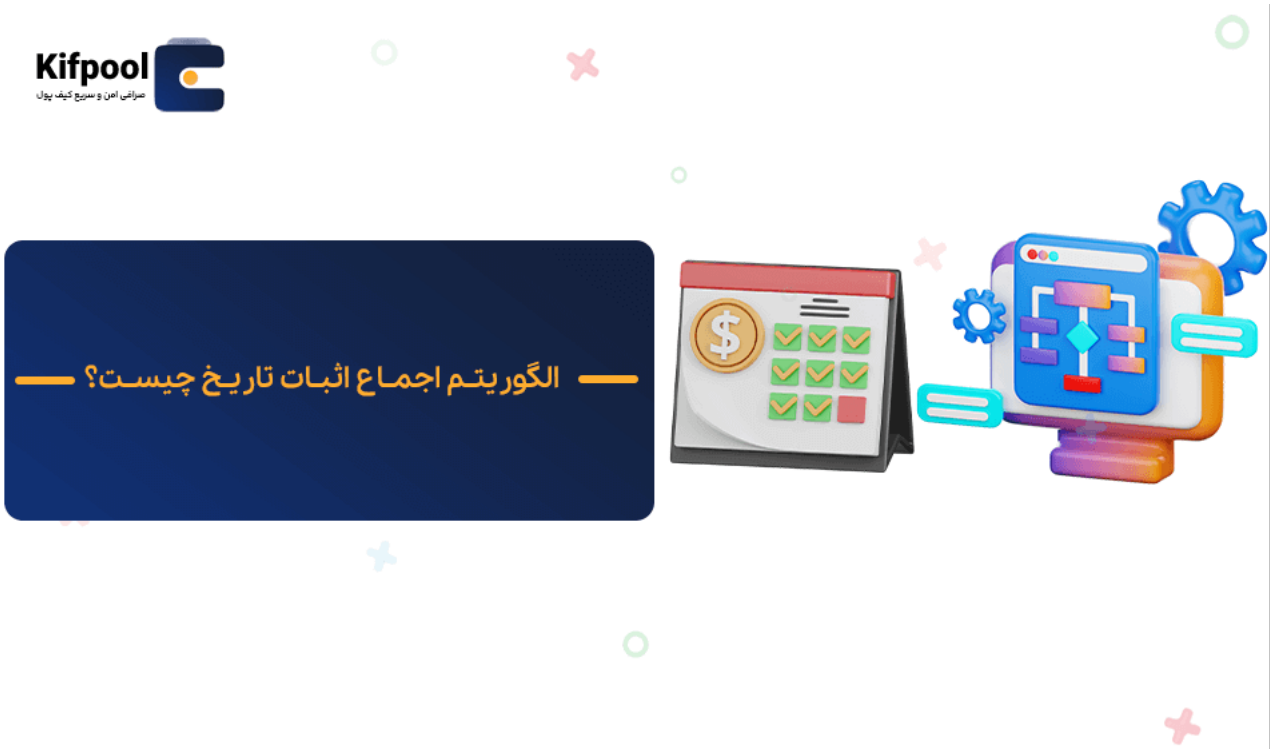
الگوریتم اجماع چیست؟

قبل از معرفی الگوریتم اجماع اثبات تاریخ لازم است ابتدا با نحوه عملکرد الگوریتم‌های اجماع آشنایی کلی داشته باشیم. شبکه بلاکچین یک دفتر کل توزیع شده است و برای ذخیره داده‌ها و اطلاعات به صورت خصوصی و عمومی مورد استفاده قرار می‌گیرد. هر شبکه بلاکچین از چندین گره یا نود تشکیل شده که هرکدام هویت منحصربه‌فردی داشته و برای امنیت و نظم شبکه خود از یک الگوریتم اجماع بهره می‌برد.

دریافت و ارسال درخواست کاربران شبکه، اعتبارسنجی و تایید درخواست‌های کاربران در قالب یک تراکنش، از نقش‌های مهم نودها در شبکه بلاکچین شمره می‌شود. تصور کنید هر کدام از نودها رفتار منحصربه‌فرد خود را داشته باشند؛ در این صورت نظم بلاکچین برهم خورده و منجر به ایجاد هرج‌ومرج خواهد شد. همچنین در چنین شرایطی اسپم‌ها و هکرها به راحتی می‌توانند باعث ایجاد خرابکاری در شبکه شوند.

برای جلوگیری از این بی‌نظمی و برای پیشگیری از خرابکاری‌های احتمالی، نیازمند ایجاد الگوریتمی با چهارچوب مشخص خواهیم بود تا نودها به دلخواه خود عمل نکنند. الگوریتمی که منجر به توافق نودها بر سر درستی یا نادرستی یک تراکنش و جلوگیری از بی‌نظمی آن‌ها می‌شود، الگوریتم اجماع نام دارد. لازم به ذکر است که تمام شبکه‌های بلاکچین دارای الگوریتم اجماع هستند ولی نحوه اجرای آن‌ها در شبکه‌های مختلف متفاوت خواهد بود.

الگوریتم اجماع اثبات تاریخ چیست؟



الگوریتم‌های اجماع، سازوکاری برای ایمن کردن شبکه بلاکچین و دفترکل توزیع شده هستند که توسط ارزهای دیجیتال مورد استفاده قرارر می‌گیرند. رمز ارزها از گروه بسیار گسترده‌ای از ارزهای دیجیتال، با مزایا و معایب خاص هرکدام استفاده می‌کنند. **الگوریتم اجماع اثبات تاریخ** مبتنی بر

شبکه بلاکچینی سولانا(SOL 23.48) بوده و توسط آناتولی یاکوونکو طراحی شده است. از این الگوریتم برای استخراج دارایی‌ها و حفظ امنیت شبکه بلاکچین استفاده می‌کنند. الگوریتم اجماع اثبات تاریخ که به اختصار الگوریتم PoH نیز خوانده می‌شود سهم زیادی در موفقیت سولانا داشته و باعث رشد 11 هزاردرصدی ارزش این شبکه شده است.
این الگوریتم برای سبک کردن نودهای شبکه مورد استفاده قرار گرفته و با استفاده از کدگذاری زمان در بلاک‌ها، میزان پردازش نودها را کاهش می‌دهد. الگوریتم اجماع اثبات تاریخ روشی را ایجاد می‌کند تا با کمک رویدادها در 2 تاریخ مختلف، یک سری محاسبات انجام شود.

مطلب پیشنهادی: مفهوم نود (گره) در بلاک چین

طریقه کارکرد الگوریتم اجماع اثبات تاریخ به چه صورت است؟

در شبکه بلاکچین سولانا رویدادهای بسیاری در زمان‌های متفاوت به وقوع می‌پیوندند. مرتب کردن این رویدادها با توجه به زمان، از جمله وظایف بسیار مهم الگوریتم اجماع اثبات تاریخ است. الگوریتم اثبات، معیار زمانی مشخصی برای مرتب کردن رویدادها داشته و هر تراکنش را در زمان مربوط به خود دسته‌بندی می‌کند.

در این الگوریتم در صورتی که چندین تراکنش انجام شود هر کدام از تراکنش‌ها در جایگاه مخصوص خود قرار خواهند گرفت؛ برای مثال تراکنش اول در جایگاه اول، تراکنش دوم در جایگاه دوم، تراکنش سوم در جایگاه سوم و به همین ترتیب تا آخر ادامه خواهد داشت.

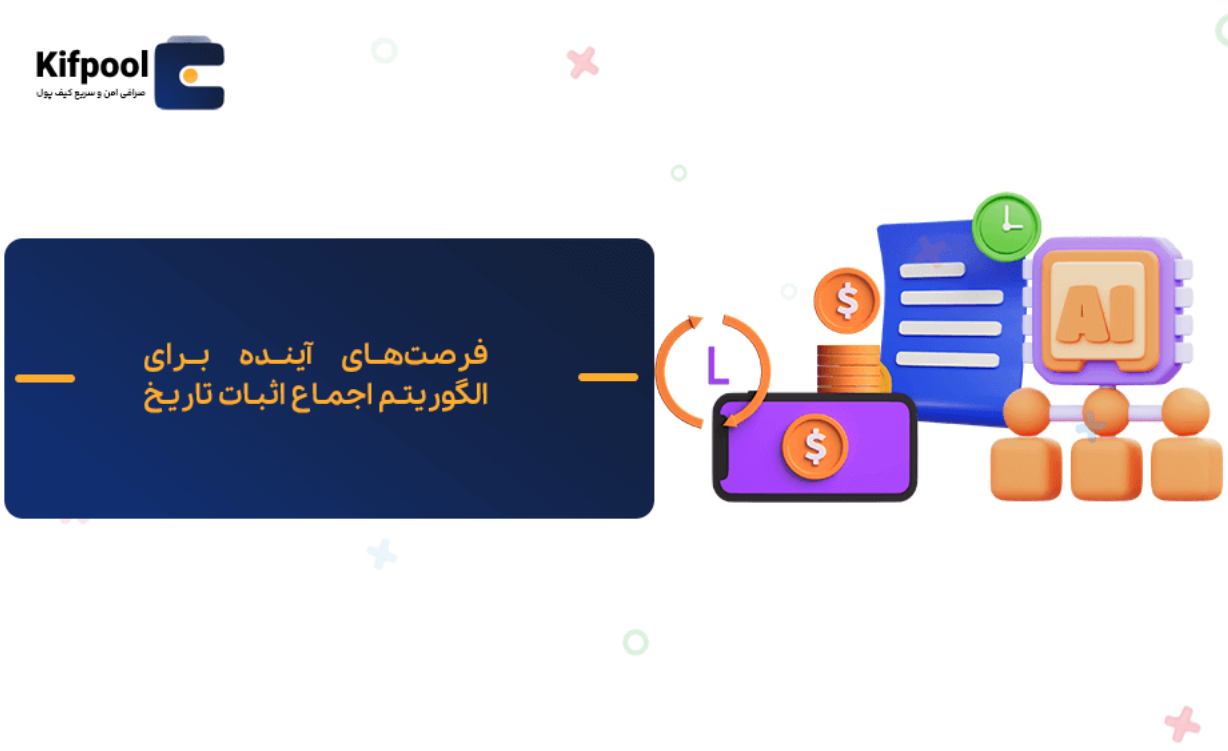
در الگوریتم‌های قبل از اجماع اثبات تاریخ، نودها با استفاده از برچسب زمانی به اجماع می‌رسیدند؛ اما در این الگوریتم خبری از اجماع نبوده و تراکنش‌ها با استفاده از اعتبارسنج‌ها یا همان ولیدیتورها (Validator) به مجموع بلاک‌های بلاکچین اضافه می‌شوند. بعد از ورود الگوریتم اثبات به این عرصه، دیگر نیازی به تایید مداوم رویدادها بوسیله نودها نبود. همچنین شبکه‌هایی که با استفاده از این الگوریتم کار می‌کنند، با استفاده از تابع SHA256 هش شده و باعث می‌شوند خروجی هش غیرقابل تشخیص باشد.

ویژگی‌های الگوریتم اثبات

الگوریتم اجماع اثبات تاریخ یکی از الگوریتم‌های بسیار خوب در شبکه‌های بلاکچینی شمرده می‌شود. انجام 65 هزار تراکنش در هر ثانیه با سرعت بسیار بالا، امنیت بالا در مقایسه با حریفان و توزیع منطقی ثروت از جمله ویژگی‌های مثبت این الگوریتم شمرده می‌شود.

با وجود ویژگی‌های خوبی که الگوریتم اجماع اثبات تاریخ دارد، نمی‌توان از نقاط ضعف آن چشم‌پوشی کرد. ناشناخته بودن الگوریتم، عملکرد ضعیف‌تر در مقابل الگوریتم‌هایی همچون فضا، عملکرد ضعیف‌تر در بهینه کردن حجم داده‌ها در مقابل الگوریتم‌های دیگر و کارکرد غیرمتمرکزتر الگوریتم اثبات سهام در مقابل الگوریتم اجماع اثبات تاریخ، از جمله نقاط ضعف این الگوریتم شمرده می‌شود.

فرصت‌های آینده برای الگوریتم اجماع اثبات تاریخ



الگوریتم اثبات یا همان **اجماع اثبات تاریخ** یکی از الگوریتم‌هایی به شمار می‌رود که بسیاری از سرمایه‌گذاران آینده روشنی برای آن پیشبینی می‌کنند و معتقدند این الگوریتم احتمال پیشرفت بسیار زیادی در آینده دارد. البته لازم به ذکر است که اثبات تاریخ یکی از الگوریتم‌هایی شمرده می‌شود که چالش‌هایی هم دارد؛ برای مثال این الگوریتم در مقیاس وسیع مورد آزمایش قرار نگرفته و نمی‌توان با اطمینان صد درصدی از بی‌عیب‌ونقص بودن آن سخن گفت.

همچنین ایجاد برخی از حملات و آسیب‌پذیری‌هایی که در سولانا کشف شده‌اند، به دلیل اثبات تاریخ بوده است. با این گفته‌ها هنوز نمی‌توان با اطمینان از اجماع امن بودن اثبات تاریخ صحبت به میان آورد.

الگوریتم اثبات؛ راهی برای پیشرفت‌های بزرگ

الگوریتم اجماع اثبات تاریخ (الگوریتم اثبات) یا به عبارتی همان proof of history، پیشرفت‌های بزرگی را برای سولانا به همراه داشته و نقشی اساسی در موفقیت آن داشته است. امنیت، سرعت و رویکرد غیرمتمرکز از جمله دستاوردهای الگوریتم اثبات برای سولانا به شمار می‌رود.

تابع هش یکطرفه این الگوریتم باعث بوجود آمدن امنیت بسیار بالایی برای حفظ اطلاعات شده است. به بیان ساده‌تر این الگوریتم با مکانیزمی بسیار هوشمند و در عین حال ساده، اقدام به منظم و یکپارچه سازی داده‌های شبکه می‌کند تا نودها درجه و ترتیب هر تراکنش را تشخیص

دهند. همچنین این الگوریتم کمک می‌کند فرایند فورک راحت‌تر در شبکه انجام شده و سرعت تولید بلاک‌های جدید افزایش یابد. در این مقاله سعی کردیم آشنایی کاملی با الگوریتم اجماع اثبات تاریخ در اختیار شما قرار دهیم، در صورت تمایل می‌توانید سوالات خود را با کارشناسان ما در میان بگذارید تا بهترین راهنمایی‌ها را در اختیار شما قرار دهند.