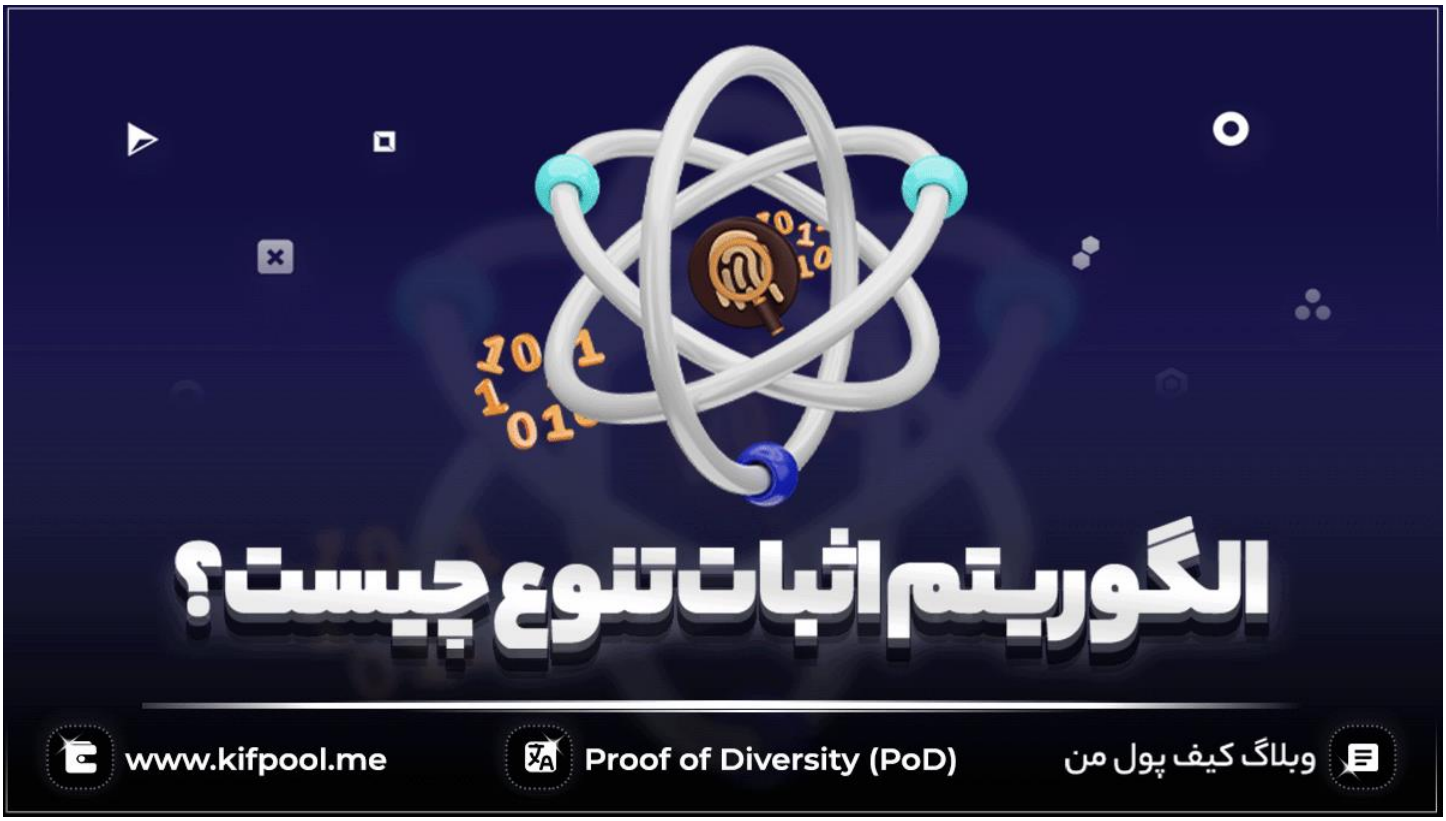
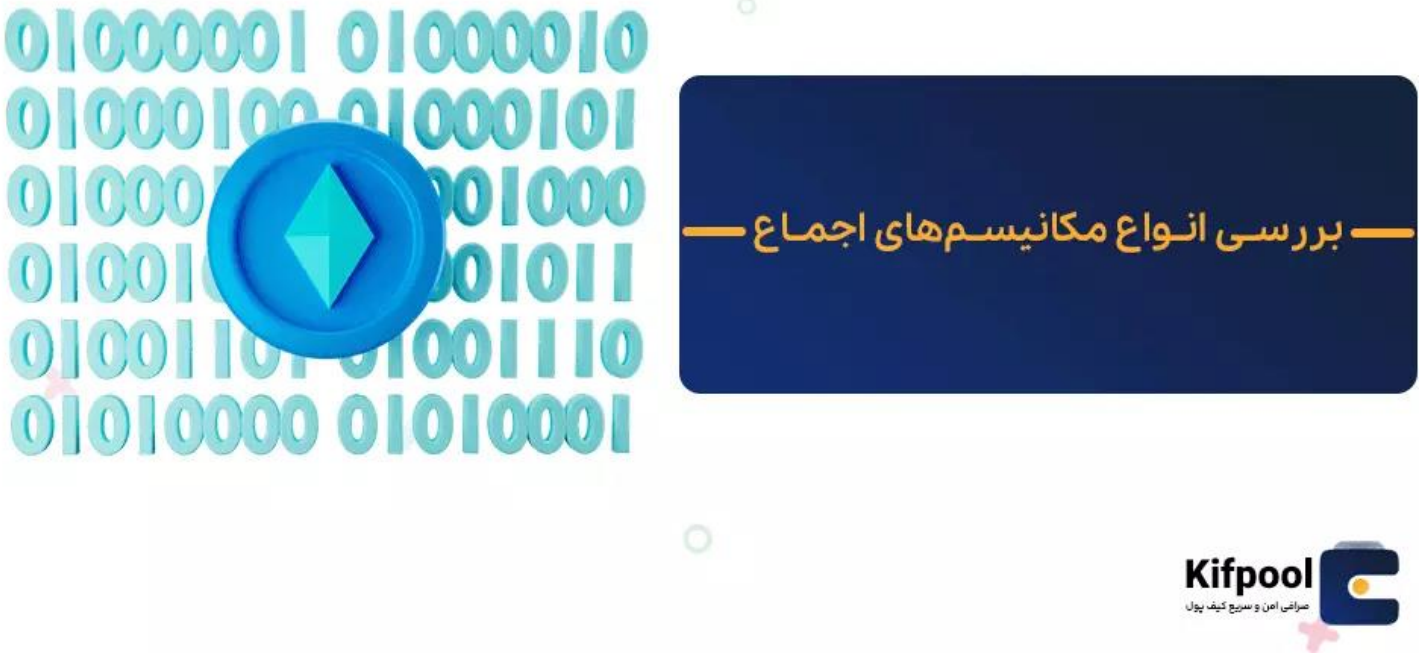


الگوریتم اجماع اثبات تنوع(PoD)

اهمیت الگوریتم اجماع اثبات تنوع

بیش از یک دهه از زمانی که بیت کوین به وجود آمد، می‌گذرد. در طول این زمان، خرید بیت کوین افزایش یافته و کاربران بسیاری با دنیای ارزها و به ویژه بیت کوین آشنا شده‌اند؛ با این حال، هنوز هم رشد گسترده قیمت BTC و مشارکت همراه با بهبود شبکه منعکس نشده است. پیشرفت‌های جدیدی مانند طرح سگویت بیت کوین (Segregated Witness) جهت فراهم کردن شرایطی برای محافظت از انعطاف‌پذیری (Malleability) تراکنش‌ها و همچنین افزایش ظرفیت بلاک (Capacity Block) در شبکه بلاک چین بیت کوین و شبکه لایتنینگ (Lightning Network) برای کمک به انجام معاملات کوچک به‌صورت سریع‌تر و موثرتر انجام شده‌اند. در حالت کلی، می‌توان گفت که این عوامل باعث بهبود عملکرد تراکنش‌ها و کاهش هزینه‌ها شده است؛ اما این پیشرفت‌ها به طور کامل نتوانسته‌اند مشکلات کاربران و علاقه‌مندان به بیت کوین را برطرف سازند. شبکه بیت کوین در تلاش است تا مقیاس پذیری خود را افزایش دهد و راه حل‌های موجود در این زمینه را برای دستیابی به این آرزوی بزرگ خود بررسی می‌کند.

بررسی انواع مکانیسم‌های اجماع برای آشنایی با الگوریتم اجماع اثبات تنوع



الگوریتم اثبات تنوع یکی از جدیدترین راه حل‌ها برای مقیاس پذیری دنیای بلاک چین است؛ مشکلی که بسیاری از کاربران شبکه‌های غیرمتمرکز با آن دست و پنجه نرم می‌کنند و همواره به دنبال راهکارهایی برای بهبود آن هستند. مقیاس پذیری (Scalability) در بلاک چین را می‌توان توانایی پاسخگویی یک شبکه به میزان تقاضا دانست که باید برای تعداد تراکنش در ثانیه (Second TPS: Transactions Per)، حجم مورد نیاز برای ذخیره این شبکه و سرعت انتقال در اطلاعات شبکه بلاک چین پاسخگو باشند؛ اما چرا باید از الگوریتم اجماع اثبات تنوع (PoD) استفاده کرد؟ در ادامه از طریق آشنایی با دو نمونه از الگوریتم‌های اجماع به پاسخ پرسش‌های خود دست پیدا می‌کنید.

انتقادات گسترده از اجماع اثبات کار (PoW) به دلیل ناکارآمدی مصرف انرژی

مکانیسم اجماع اثبات کار (PoW) بیت‌کوین را ساتوشی ناکاموتو در سال ۲۰۰۸ به وجود آورد که کشف موفقیت‌آمیزی بود و سرانجام توانست یک ارز دیجیتال محدود و غیرمتمرکز را فعال کند. در این الگوریتم، استخراج‌کننده‌های ارز با یکدیگر به رقابت می‌پردازند تا هر بلوک پرداخت را استخراج کنند؛ در حالی که به‌صورت هم‌زمان برای تایید تراکنش‌ها و یا دفاع در برابر حملات مضاعف دو بار خرج کردن (Double Spending) و خنثی‌سازی سایر فعالیت‌های مخرب کار می‌کنند. هر چقدر که ماینرها هش ریت بیشتری ارائه کنند، شبکه‌های ارز دیجیتال نیز امن‌تر و قوی‌تر می‌شوند. البته دستاوردهای قدرت ماینینگ را نمی‌توان با افزایش توان عملیاتی را کارایی تراکنش‌ها یکی دانست؛ چراکه هر ماینری برای ارائه‌دهی همان خدمات مشترک رقابت می‌کند. نکات

گفته شده نشان می‌دهند که بیت کوین به دلیل ناکارآمدی انرژی خود با انتقادات گسترده‌ای از طرف کاربران دنیای ارزهای دیجیتال مواجه شده است و وجود الگوریتمی مانند اجماع اثبات تنوع پیش از گذشته احساس می‌شود.

الگوریتم اثبات سهام نمی‌تواند محدودیت‌های مقیاس پذیری را کاهش دهد!

مکانیسم اثبات سهام (PoS) یکی دیگر از الگوریتم‌های اجماع است که به عنوان جایگزینی برای مکانیستم اثبات کار در نظر گرفته می‌شود. در این الگوریتم، مشارکت کنندگان با قرار دادن کوین‌های خود در انتشار شبکه مشارکت می‌کنند و یک نسخه متفاوت از PoS را به کار می‌برند که به آن اثبات سهام واگذار شده (Delegated Proof of Stake) می‌گویند. با وجود کشف تمامی این مکانیسم‌های اثبات سهام و اثبات کار برای عوامل مختلفی نظیر مصرف انرژی، هنوز هم نگرانی‌های مهمی در رابطه با مقیاس پذیری وجود دارد. وجود سرمایه گذاران فراوان در یک شبکه‌ای لزوما توان بالای یک شبکه را نشان نمی‌دهد. بر خلاف مکانیسم اجماع اثبات کار، سایر مکانیسم‌های اجماع (Consensus Mechanism) از لحاظ مشارکت محدود هستند؛ چراکه تعداد زیادی کوین در گردش وجود دارد و می‌توان گفت شبکه‌های اثبات سهام مشکل مقرون‌به‌صرفه‌تری دارند. همان طور که گفته شد، اکثر آلت کوین‌های اصلی از الگوریتم‌های اثبات سهام و اثبات کار یا ترکیب این دو استفاده می‌کنند؛ اما با توجه به قابلیت‌های کاربردی خود، نمی‌توانند محدودیت‌های مقیاس‌پذیری طولانی‌مدت شبکه‌ها را در زمان پذیرش انبوه کاهش داده یا برطرف سازند و به همین دلیل باید از الگوهای جدیدی مانند الگوریتم اجماع اثبات تنوع (PoD) روی کار بیایند.

مطلب پیشنهادی: الگوریتم تحمل خطای بیزانس چیست؟

Nyzo mainnet؛ نمونه‌ای از مکانیسم اجماع اثبات تنوع

mainnet Nyzo شبکه‌ای است که اخیرا راه‌اندازی شده و از یک مکانیسم جدید اجماع به نام اثبات تنوع در اولین نوع خود استفاده می‌کند. این الگوریتم به کیفیت Nyzo اشاره دارد که این شبکه با مشارکت بیشتر رشد پیدا کرده و بهبود پیدا می‌کند. شبکه Nyzo به جای ماینرها و سهامداران از یک چرخه یا دوره تایید کننده تشکیل شده است. در این چرخه، هر تایید کننده‌ای به نوبت بلوک‌ها را ضرب می‌کند و به جای اینکه هر یک از شرکت کنندگان به رقابت با تایید کننده دیگری بپردازند، برای ایجاد بلوک‌ها تا حد ممکن با یکدیگر همکاری کرده و ارتباط برقرار می‌کنند.

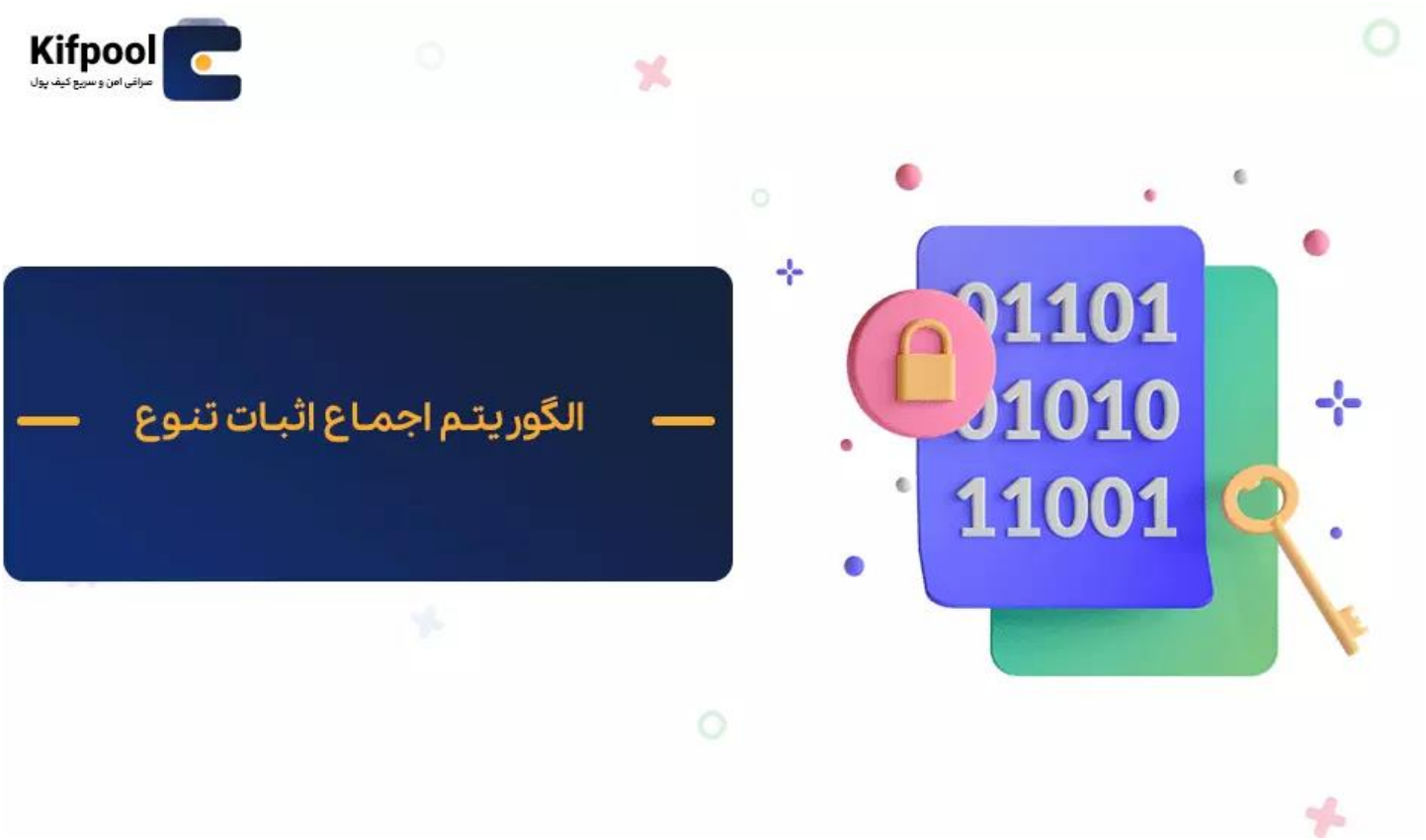
شبکه Nyzo mainnet چگونه کار می‌کند؟

هر دوره زمانی که به اتمام می‌رسد، کاندیداهای برتر به عنوان تایید کنندگان فعال در دوره بعدی انتخاب می‌شوند. این پروسه انتخاب تایید کنندگان می‌تواند بر اساس یک الگوریتم از پیش تعیین شده یا معیارهایی مانند شهرت، سهام یا ترکیبی از عوامل مختلف باشد. زمانی که تایید کنندگان فعال برای دوره بعدی مشخص شدند، آن‌ها به عنوان مسئول ضرب بلوک‌ها در آن دوره مشخص شناخته می‌شوند و هر تایید کننده‌ای در مجموعه، پیش از کامل شدن دوره باید از فرصت خود استفاده کند. پس از اینکه دوره به پایان رسید، چرخه جدیدی آغاز می‌شود و این فرآیند به‌طور مداوم تکرار می‌شود و این اطمینان حاصل می‌شود که در هر زمانی مجموعه‌ای از تایید کنندگان فعال مسئول حفظ امنیت بلاک چین و اعتبارسنجی تراکنش‌ها هستند. قرار گرفتن در صف برای کاندیدای دوره بعدی، به شرکت کنندگان این امکان را می‌دهد تا به یک تایید کننده فعال تبدیل شوند و برای ضرب بلوک‌ها پاداش قابل توجهی به دست بیاورند. انتخاب تایید کنندگان برا دوره بعدی، معمولا به مکانیسم اجماع بلاک چین و قوانین خاص آن وابسته است. به عبارتی دیگر، در پایان دوره، همانطور که شرکت کنندگان فعلی به تایید کنندگان رای داده‌اند، آن‌ها نیز می‌توانند به چرخی بعدی ملحق شوند و برای کار خود به عنوان پاداش، NYZO دریافت نمایند.

شبکه NYZO و حملات ۵۱ درصدی

این سیستم باعث می‌شود که NYZO در برابر حملات ۵۱ درصدی که از رایج‌ترین حملات سازمان‌دهی شده در کریپتو هستند، به شدت مقاومت کند. در این نوع حملات، یک عامل مخرب به منابعی که بخش قابل توجهی از کل شبکه را تشکیل می‌دهند، اجازه می‌دهد تا اجماع را به انحصار خود در بیاورند و شبکه را از مدار خود خارج کنند. در شبکه NYZO، یک حمله ۵۱ درصدی به آماده‌سازی قابل توجهی نیاز دارد؛ چراکه تایید کنندگان جدید به تدریج می‌توانند در دوره زمانی مشخص ادغام شوند. معمولا یک حمله چند دقیقه طول می‌کشد؛ اما یک حمله ۵۱ درصدی به NYZO ماه‌ها زمان می‌برد وحتی در مرحله نوپای فعلی شبکه نیز به میلیون‌ها دلار هزینه برای اجرا و به بررسی دقیق شرکت کنندگان شبکه و تمامی جزئیات مربوط به مکانیسم ورود عمومی نیاز دارد.

الگوریتم اجماع اثبات تنوع؛ یک راه حل جدید برای مقیاس پذیری بلاک چین



Nyzo تنها شبکه در بلاک چین است که با حداکثر کارایی خود عمل می‌کند و پتانسیل لازم برای گسترش و پیشرفت دارد. فعالان دنیای ارزها با محدودیت‌های مقیاس‌پذیری طولانی‌مدت شبکه‌ها در زمان پذیرش انبوه مواجه هستند و در جستجوی مکانیسم اجماع بهینه برای حل این مشکل، الگوریتم اجماع اثبات تنوع می‌تواند یکی از بهترین راه حل‌های موجود در این زمینه باشد. Nyzo که از الگوریتم اثبات تنوع استفاده می‌کند، در تضاد شدید با بیت کوین است و بیش از حد لازم از برق و انرژی مصرف نمی‌کند. همچنین این شبکه به دلیل مقاومت بالای خود در برابر حمله ۵ درصدی، آماده است تا جایگاه خود را در ارزهای دیجیتال ایمن و محکم نماید. تمامی این مزیت‌ها با وجود الگوریتم اجماع اثبات تنوع به عنوان یک راه حل جدید برای مقیاس پذیری بلاک چین امکان پذیر است. نظر شما درباره این الگوریتم جدید چیست؟ به نظر شما آینده الگوریتم اثبات تنوع چگونه خواهد بود؟ می‌توانید پاسخ‌های خود را در بخش نظرات با ما در میان بگذارید.

منبع: Micky