الگوریتم اثبات ذخیره چیست؟

پس از رویداد شکه کننده فروپاشی صرافی FTX که یک صرافی ارزهای دیجیتال و صندوق تامینی رمزارز بود، عملکرد صرافی‌ها و تامین کنندگان امنیت ارزها زیر سوال رفت. همه ما می‌دانیم که استفاده از صرافی‌های متمرکز، ریسک‌های خاص خود را به همراه دارد و این نهادها و پروتکل‌های نیمه متمرکز و غیرمتمرکز، حضانت از دارایی افراد را بر عهده می‌گیرند. بسیاری از کارشناسان، معتقدند که صرافی‌های متمرکز برای در امان ماندن دارایی افراد، باید از **الگوریتم اثبات ذخیره (Proof of Reserve)** استفاده نمایند. اگر صرافی‌ها بدون اطلاع سرمایه گذاران از دارایی آن‌ها برای تحقق اهداف خود استفاده کنند، بحران‌های شدیدی کل اکوسیستم را تهدید می‌کند. Proof of Reserve شفافیت را افزایش می‌دهد و چارچوبی برای حسابرسی ایجاد می‌کند و به عنوان روشی نوین در حال پیشرفت است. اما الگوریتم اثبات ذخیره چیست؟ اثبات ذخیره چگونه کار می‌کند و چرا اهمیت بسیار زیادی دارد؟ برای پاسخ به سوالات خود در ادامه این مطلب از وبلاگ کیف پول من با ما همراه باشید.

آشنایی با اثبات ذخیره به زبانی ساده

برای اینکه دنیای ارزهای دیجیتال و امور مالی غیرمتمرکز بتوانند با سرعت زیادی رشد و پیشرفت خود را گسترش دهند، به اعتماد کامل میان کاربران و پروتکل‌های مختلف نیاز دارند. به زبانی ساده، می‌توان گفت وظیفه اثبات ذخیره یا Proof of Reserve است تا نشان دهد که نهادها و پروتکل‌های متمرکز یا نیمه متمرکز، وجوهی که برای مشتریان خود نگه می‌دارند را واقعا در اختیار دارند یا تظاهر به داشتن آن می‌کنند. در حقیقت این پروتکل نشان می‌دهد که مشتریان

می‌توانند در زمان دلخواه، وجوه خود را برداشت کنند و از شفافیت در دسترس بودن وجوه خود اطمینان حاصل کنند. صرافی‌ها و کسب‌وکارهایی که در زمینه کریپتو فعال هستند، با استفاده از Proof of Reserve به مشتریان خود ثابت می‌کنند که مبالغ واریزی توسط این افراد در حساب موجود است و در این پروسه، فرآیند حسابرسی توسط شخص ثالثی انجام می‌شود تا هیچ شک و جعلی در اطلاعات ذخیره شده ایجاد نگردد.

اثبات ذخیره چگونه کار می‌کند؟

درخت مرکل که به درخت درهم‌سازی نیز معروف است، به عنوان ابزاری بسیار کارآمدی برای تایید داده‌ها شناخته می‌شود. در این ساختار، ابتدا از کلیه داده‌ها هش گرفته و در مرحله بعدی، به‌صورت دو به دو هش داده‌ها با هم ادغام شده و مجددا از آن‌ها هش گرفته می‌شود. این روند تا زمان رسیدن به آخرین مقدار ریشه درخت مرکل ادامه پیدا می‌کند. با در نظر گرفتن ویژگی‌های توابع هش، هرگونه تغییری که در داده‌ها رخ دهد، ریشه درخت مرکل نیز تغییر می‌کند؛ بنابراین کوچک‌ترین تغییرها نیز به راحتی مشخص می‌شوند. در طی فرآیند اثبات ذخیره، فردی که وظیفه حسابرسی را بر عهده دارد (Auditor)، وضعیت لحظه‌ای داده‌ها (اسنپ‌شات) را تهیه می‌کند. با قرار گرفتن این داده‌ها در درخت مرکل، ریشه درخت محاسبه می‌شود و حسابرس به تغییرات ایجاد شده دسترسی پیدا می‌کند.

چرا الگوریتم اثبات ذخیره اهمیت دارد؟

اثبات ذخیره به چند دلیل بسیار اهمیت دارد و از پروتکل‌های حیاتی است. Proof of Reserve این اطمینان را به کاربران دنیای ارزها می‌دهد تا تایید نمایند دارایی‌هایی را که در یک صرافی نگهداری می‌کنند، دارای پشتوانه هستند و صرافی می‌تواند وجوه کاربران را در صورت درخواست برداشت، پرداخت کند. همچنین اثبات ذخیره صرافی‌ها و کسب‌وکارهای فعال در این زمینه را مجبور به رعایت استانداردهای شفافیت می‌کند و از اینکه این کسب‌وکارها درگیر فعالیت‌های غیرقانونی شوند، اقدامات لازم را برای جلوگیری فراهم می‌کند. همچنین می‌توان گفت که حجم دارایی‌های دیجیتالی که موسسات مختلف و بانک‌ها برای مردم نگهداری می‌کنند، در حال افزایش است؛ بنابراین باید اقداماتی پیرامون کاهش ریسک‌های سیستماتیک انجام شود تا از کافی بودن این دارایی‌ها در صرافی‌های متمرکز، توکن‌های رپد شده و غیره اطمینان حاصل گردد. اثبات ذخیره هم به نفع کاربران عمل می‌کند و هم به نفع پلتفرم‌ها و این موضوع به حفظ کاربر و توسعه پلتفرم کمک‌های شایانی می‌کند. برای درک بیشتر، بهتر است بگوییم که Proof of Reserve یک موقعیت برد برد برای تمامی طرف‌های درگیر معامله را ایجاد می‌کند و برای کل اکوسیستم ارزهای دیجیتال مهم است.

مطلب پیشنهادی: الگوریتم اثبات اعتبار

مزایای اثبات ذخیره

POR راه‌حلی متمایز در شبکه‌های بلاک چین است و مزایای زیادی به همراه دارد که در ادامه هر یک را بررسی می‌کنیم:

سوابق معاملات را ارائه می‌کند!

یکی از وظایف اثبات ذخیره، ارائه سوابق معاملاتی به مشتریان است. برنامه‌هایی که دارای الگوریتم Proof of Reserve هستند، امور مالی یک موسسه را به‌صورت شفاف و واضح ارائه می‌کنند و در صورتی که این پروسه به درستی انجام شود، کاربران این پروتکل می‌توانند سوابق معاملات و تراکنش‌های شخصی خودشان را پیگیری کنند و بهترین تصمیم را برای سرمایه گذاری اتخاذ نمایند.

حضانت و نگهداری مناسب دارایی‌ها را تایید می‌کند!

یکی دیگر از مزایای **الگوریتم اثبات ذخیره**، تایید حضانت و نگهداری مناسب از دارایی‌ها است. این الگوریتم به کاربران اجازه می‌دهد تا رمزارزهای نگهداری شده توسط موسسه‌ها را تایید نمایند و سرمایه گذاران از این فرآیند برای شناسایی تغییرات ایجاد شده در حساب‌های شخصی خود استفاده می‌کنند تا دید بهتری برای مدیریت وجوه خود داشته باشند. همچنین وجود استانداردهای Proof of Reserve که برای عموم کاربران قابل مشاهده است، می‌تواند از تقلب جلوگیری کند و در نهایت از حملات هکرها جلوگیری می‌شود. همچنین صرافی‌ها ترغیب می‌شوند

تا مرتکب اشتباهی نگردند؛ چراکه این اشتباهات به سرعت رو می‌شوند و این مسئله می‌تواند برای صرافی خطاکار بسیار گران تمام شود.

مطلب پیشنهادی: الگوریتم اثبات سوختن

بررسی‌های لازم درباره پروتکل‌های حضانتی را انجام می‌دهد!

الگوریتم اثبات ذخیره، بررسی‌های لازم درباره پروتکل‌های حضانتی را انجام می‌دهد. کاربران پیش از اینکه حساب خود را در صرافی‌های ارز دیجیتال ایجاد کنند، می‌توانند تحقیقاتی ابتدایی درباره آن پلتفرم انجام دهند. ابزارهای Proof of Reserve یکی از روش‌های مناسب برای آغاز این تحقیقات است و استفاده از آن امکان بروز حوادث ناشی از مدیریت ضعیف وجوه را توسط موسسه‌ها و پروتکل‌های حضانتی کاهش می‌دهد.

نواقص اثبات ذخیره

اگرچه **الگوریتم اثبات ذخیره** دارای مزایای منحصربه‌فردی است، اما برخی نواقص و اشکالات ذاتی نیز دارد. در این الگوریتم، صرافی‌ها تنها آدرس‌های مربوط به کیف پول خود را ارائه می‌کنند و راهی وجود ندارد تا بتوان مطمئن شد که این آدرس واقعا متعلق به صرافی است یا نه. همچنین الگوریتم Proof of Reserve در برخی اوقات، اطلاعات شخصی و موجودی کاربران را فاش می‌کند. صرافی‌های ارز دیجیتال وظیفه دارند تا اطلاعات احراز هویت کاربران را نزد خود باامنیت بالا نگهداری کنند و به جز مواقع خاص و مواجه شدن با مشکلات، اطلاعات کاربران را تفتیش نکنند.

اثبات ذخیره؛ پروتکلی مهم برای اثبات درستکاری صرافی‌های ارز دیجیتال

سو استفاده از وجوه کاربران توسط پلتفرم‌های مالی حضانتی، فضای کرپیتو را با مشکلاتی مواجه کرده و این بازار را در وضعیت تاسف‌باری قرار داده است. با وجود الگوریتم‌هایی مانند **اثبات ذخیره**، کورسوی امیدی در میان این رویدادهای شوکه کننده نظیر فروپاشی صرافی FTX به وجود آمده و باعث شده تا فضای ایمن‌تری برای سرمایه گذاران دنیای رمزارزها ایجاد شود. این الگوریتم علاوه بر مزایای بی‌نظیری که دارد، دارای معایبی است که نمی‌توان آن‌ها را نادیده گرفت؛ به همین دلیل باید در انتخاب صرافی و کیف پول ارزهای دیجیتال خود نهایت دقت را به خرج دهید و چه کیف پولی بهتر از **کیف پول من** که بارها حسن نیت و درستکاری خود را به کاربران نشان داده است و بیش از 1 میلیون کاربر فعال دارد؟

شما درباره الگوریتم اثبات ذخیره چه نظری دارید؟ آیا فکر می‌کنید این الگوریتم می‌تواند با سایر الگوریتم‌ها مانند اثبات سهام رقابت کند؟ به نظر شما کدام الگوریتم برتر است؟ می‌توانید پاسخ به این سوالات را در قسمت نظرات با ما در میان بگذارید.