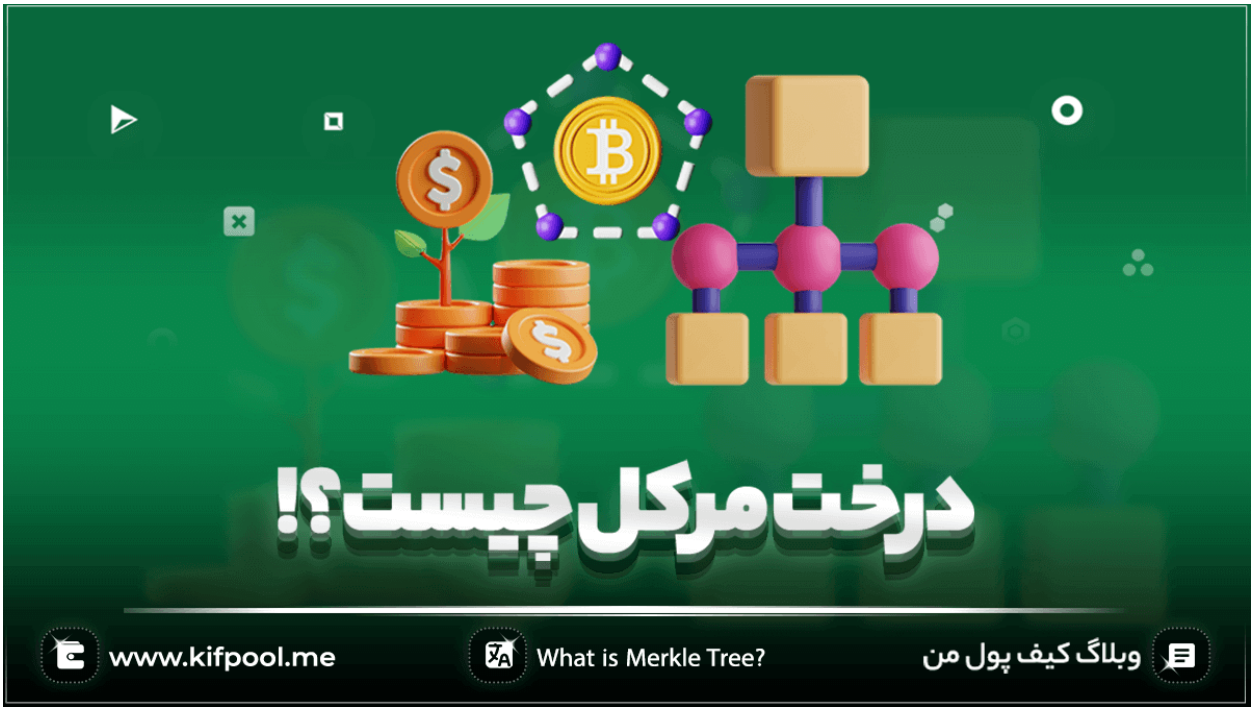
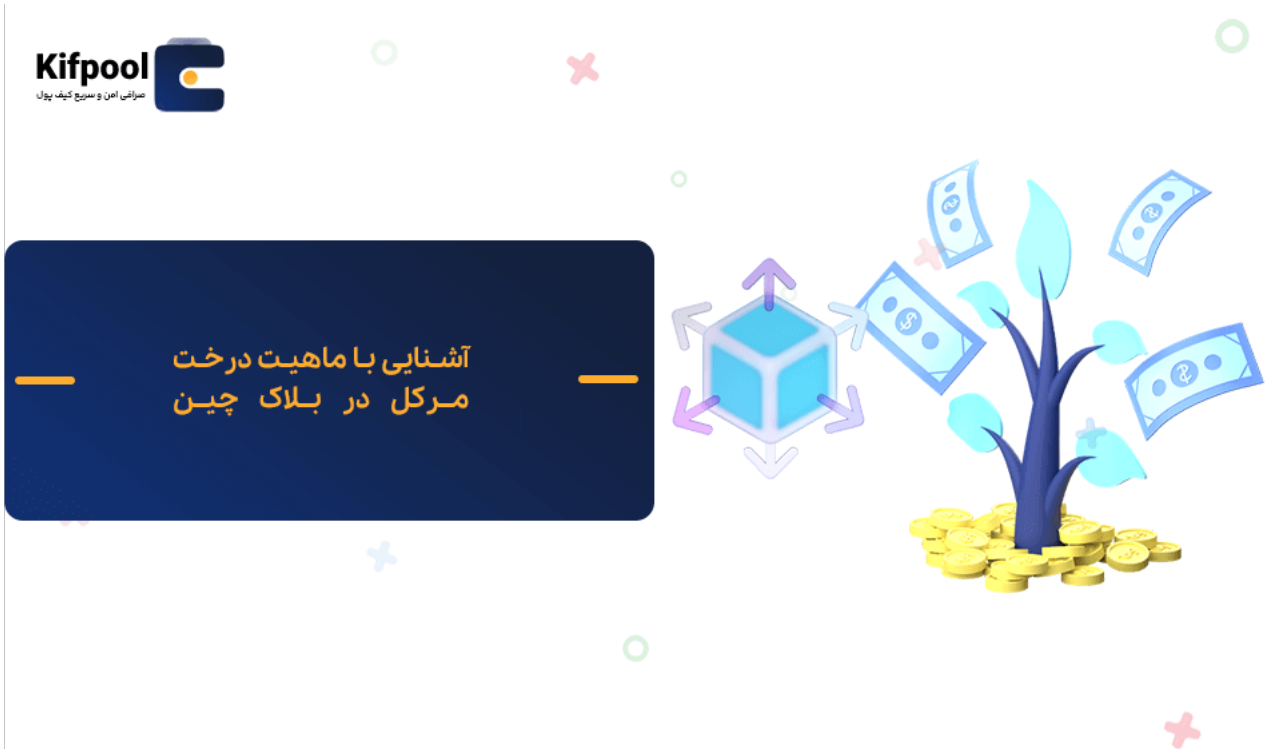


درخت مرکل چیست؟!

اگر جز تازه واردان دنیای کریپتوکارنسی به شمار می‌روید، احتمالا از حجم اصطلاحات تخصصی ارز دیجیتال موجود در این دنیای سودآور کلافه شده‌اید؛ اما واقعیت این است که هر بازار مالی متناسب با میزان اهمیت خویش دارای برخی اصطلاحات تخصصی است و از آنجایی که مارکت ارز دیجیتال و فناوری بلاک چین مفاهیم بسیار نوینی به شمار می‌روند، آشنایی با ساختار اصلی آن‌ها برای اطمینان یافتن از وضعیت امنیتی این دنیای نوظهور امری اجتناب ناپذیر به نظر می‌رسد. یکی از اصطلاحات بسیار مهم رایج در مکالمات روزمره تحلیل‌گران و صاحب نظران دنیای کریپتو به اصطلاح **درخت مرکل** (**Merkle Tree**) مربوط می‌شود؛ احتمالا با شنیدن این اصطلاح یک تصویر ذهنی در ارتباط با یک درخت با شاخ و برگ بسیار زیاد در ذهن شما شکل گرفته‌است ولی در حقیقت این اصطلاح به ساختار پلکانی و سلسه مراتبی اشاره دارد که در شبکه‌های بلاک چینی برای اعتبارسنجی در نظر گرفته شده است.

احتمالا با مطالعه این مطالب و مواجهه با برخی اصطلاحات تخصصی موجود آن نظیر اعتبارسنجی و بررسی صحت داده‌های یک پایگاه کمی گیج و سردرگم شده‌اید؛ اما با توجه به اهمیت ذاتی آشنایی با نحوه عملکرد شبکه‌های بلاک چینی در دستیابی به اطمینان خاطر بیشتر در انجام معاملات رمزارزی نظیر خرید بیت کوین که به سرمایه زیادی نیز نیاز دارد، ما این مقاله از بلاگ کیف پول من را به بررسی دقیق و ساده مفهوم درخت مرکل اختصاص داده‌ایم؛ اگر شما هم در این زمینه کنجکاو هستید، تا انتهای این مطلب با ما همراه باشید.

آشنایی با ماهیت درخت مرکل در بلاک چین



قدم اول در شناخت هر ماهیتی، به ارائه یک تعریف جامع و ساده از ماهیت مورد نظر اختصاص یافته است و آشنایی با مفهوم **درخت مرکل** (Merkle Tree) نیز از این قاعده مستثنی نمی‌باشد؛ اما اجازه دهید قبل از بیان چیستی و ویژگی‌های درخت مرکل، نگاهی به نقطه آغازین شکل‌گیری این اصطلاح داشته باشیم. جالب است بدانید که اصطلاح «درخت مرکل» برای اولین بار در سال 1980 میلادی از سوی فردی به نام رالف مرکل که در حقیقت یک دانشمند و پژوهشگر فعال در حوزه علوم کامپیوتر بود، مطرح گردید و عملا این اصطلاح صرفا به دنیای کریپتوکارنسی اختصاص نداشته و کاربردهای غیربلاک چینی نظیر تکثیر داده در پایگاه‌های داده توزیع شده غیر SQL، سیستم IPFS، Git (که یک نرم‌افزار کنترل پروژه است) و غیره را می‌توان برای آن متصور بود؛ اما با این وجود، اصطلاح درخت مرکل عمده شهرت خویش را وام‌دار رشد و توسعه دنیای کریپتوکارنسی بوده و هنگامی که کاربران در شبکه‌های بلاک چینی قصد اعتبارسنجی تراکنشی را داشته باشند، این درخت به سراغ آن‌ها می‌آید.

همین مسئله سبب شده تا امروزه هر فرد تازه‌واردی که قصد سرمایه‌گذاری بر روی ارزهای دیجیتال داشته و بخواهد به خرید رمزارزهای مختلف نظیر خرید اتریوم دست زند، باید در قدم اول به سراغ درک مفهوم و ساختار درخت مرکل رفته و پس از دستیابی به چشم‌اندازی دقیق و عمیق از عملکرد شبکه‌های بلاک چینی، معاملات خود را انجام دهد. درخت مرکل که به آن درخت هش نیز گفته می‌شود، در اصل یک ساختار بسیار قدرتمند و پیچیده است که در بررسی سریع و آنی داده‌ها در یک مجموعه و پایگاه بزرگ کاربرد دارد و در حقیقت شکل آن نیز یک نمودار درختی

است که هر برگ از آن یک **هش** (**Hash**) است. منظور از هش اطلاعات کلیدی بلاک است که به صورت هش رمزنگاری شده‌اند. برای درک بهتر مفهوم هش، باید با اصطلاحی تحت عنوان «تابع هش» آشنا باشید که با توجه به خروج موضوعی این مسئله از عنوان مقاله که بررسی مفهوم درخت مرکل است، صرفا نگاهی گذرا به آن کرده و از آن عبور می‌کنیم: منظور از تابع هش، تابعی است که به وسیله آن می‌توان هر مجموعه از داده‌ها (با ابعاد مختلف) را به یک خروجی با اندازه معین تبدیل کرد.

مطلب پیشنهادی: بررسی مفهوم رمزگذاری هش شده

به بیان بهتر، اطلاعات تراکنش‌ها در شبکه‌های بلاک چینی به صورت یک متن عادی در شبکه ذخیره نمی‌شوند، بلکه این اطلاعات را در ساختار داده‌ای به نام درخت مرکل جای می‌دهند و این درخت در برگیرنده خلاصه‌ای از کلیه تراکنش‌های انجام یافته در هر بلاک است. جالب است بدانید که درخت مرکل، در حقیقت یک درخت وارونه است که در آن هش‌های به دست آمده از تراکنش‌ها در قسمت پایینی که به عنوان «نودهای برگ» از آن‌ها یاد می‌شود قرار می‌گیرند و بخش میانی درخت به شاخه‌ها (Branches) و بخش بالایی به ریشه مرکل (Merkle Root) اختصاص یافته است و هر بلاک در شبکه‌های بلاک چینی دارای یک ریشه مرکل است. با توجه به ماهیت توزیع شدگی دفتر کل شبکه‌های بلاک چینی وجود درخت مرکل در این شبکه‌ها، فرآیند مدیریت و ذخیره‌سازی سیل عظیمی از تراکنش‌ها را بهبود بخشیده است.

بررسی یک مثال

برای آن که راحت‌تر بتوانید با اصطلاح کاربردی درخت مرکل ارتباط برقرار کنید، مثالی را مورد بررسی قرار می‌دهیم: تصور کنید که با چهار تراکنش به نام‌های A، S، H و K در یک بلاک روبه‌رو هستیم و سپس به کمک تابع هش، هر یک از این تراکنش‌های نام برده شده را به هش تبدیل می‌کنیم و حال هش A، هش S، هش H و هش K داریم؛ این هش‌های اولیه ما بخش نودهای برگ (Leaf Nodes) را شکل می‌دهند و سپس این هش‌های ایجاد شده را 2 به 2 و به صورت جفت با یکدیگر ترکیب کرده و به هش‌های جدید AS و HK می‌رسیم که این دو هش جدید، شاخه درخت مرکل را به وجود می‌آورند و سپس در مرحله نهایی این دو هش را نیز با هم ترکیب می‌کنیم تا هش ASHK شکل بگیرد که این هش ASHK همان ریشه درخت مرکل ما خواهد بود و عملا به این شکل امکان هرگونه دخل و تصرف و انجام تغییرات (حتی اصلاحات جزئی) از کاربران در شبکه سلب شده و امنیت شبکه بلاک چینی به لحاظ امنیت داده تامین می‌گردد.

در واقع هر بلاک از بخش‌های عنوان (Header) و بدنه (Body) شکل گرفته است که ریشه درخت مرکل در قسمت هدر هر بلاک ذخیره می‌شود. البته لازم به ذکر است که بخش هدر هر بلاک علاوه

بر ریشه درخت مرکل، اطلاعات دیگری نظیر مهر زمان (Timestamp)، هش بلاک قبلی، شماره نسخه بلاک، نانس و غیره را نیز شامل می‌شود و عملا ذکر هش بلاک قبلی در هر بلاک جدید و وجود درخت مرکل در هر بلاک، این اطمینان خاطر را برای کاربران دنیای کریپتوکارنسی فراهم می‌آورد که اطلاعات تراکنش آن‌ها بدون امکان تغییر و ویرایش اطلاعات به زنجیره شبکه وصل شده است و با خیال راحت می‌توانند با خرید تتر، بیت کوین، اتریوم و غیره از حق مالکیت غیرقابل سلب خویش بر روی این دارایی‌های دیجیتالی بهره ببرند.

کاربرد درخت مرکل در بلاک چین

به طور کلی استفاده از درخت مرکل در فناوری بلاک چین مزایای بسیار زیادی را به همراه داشته است که یکی از مهم‌ترین کاربردهای آن، مسئله یکپارچه‌سازی داده‌ها در بلاک‌هاست؛ در واقع این درخت این امکان را برای کاربران فراهم می‌سازد تا بدون نیاز به دانلود کامل بلاک چین که حجمی بالغ بر 350 گیگابایت دارد، یک تراکنش مشخص را به راحتی بررسی و تائید نمایند. برای درک بهتر این کاربرد، مجددا به مثل مطرح شده در بالا برمی‌گردیم؛ تصور کنید که شما به عنوان یک اعتبارسنج قصد تائید تراکنش H از بلاک فوق را دارید، در این صورت می‌توانید حرکت خود را از ریشه درخت مرکل آغاز کنید و به صورت دو دویی (Binary) به سمت برگ‌ها حرکت نمایید.

با چنین کاری بخشی از درخت مرکل که مربوط به هش AS بود در همان قدم اول حذف می‌شوند و عملا به کمک این درخت، دیگر نیازی به بررسی کلیه تراکنش‌ها برای تائید یک تراکنش مشخص نخواهید داشت و صرفا می‌توان با استفاده از اطلاعات ذخیره شده در بخش هدر هر بلاک، اعتبار تراکنش را مورد بررسی و ارزیابی قرار داد. حال که با این کاربرد آشنا شدید، تصور کنید که اگر در شبکه بلاک چین بیت کوین از درخت مرکل استفاده نمی‌شد، چه اتفاقی می‌افتاد؟ چنین خلایی سبب می‌شد تا هر نود در شبکه ملزم به حفظ نسخه کاملی از کلیه تراکنش‌های بیت کوینی انجام شده باشد، امری که به نظر می‌رسد کار چندان راحتی نیست؛ چراکه حجم این اطلاعات بسیار سرسام‌آور است و این در حالی است که با استفاده از درخت مرکل برای اثبات اعتبار یک تراکنش، صرفا به بخش کمی از اطلاعات موجود در سرتاسر شبکه نیاز داریم.

مزایای استفاده از درخت مرکل در بلاک چین

استفاده از **درخت مرکل** در تائید تراکنش‌های انجام یافته در شبکه دارای مزایای بسیار زیادی است که در ادامه به بررسی 3 مورد از مهم‌ترین مزایای وجودی درخت مرکل در شبکه‌های بلاک چینی می‌پردازیم:

- ساده‌تر شدن شناسایی هرگونه دستکاری: استفاده از ساختار هش، امکان تشخیص هرگونه دستکاری در تراکنش‌ها را برای اعتبارسنج‌ها و ولیدیتورها راحت‌تر می‌کند. همان طور که در مطالب فوق مشاهده کردید، هر تراکنش در بلاک به صورت یک هش در درخت مرکل ذخیره می‌شود و در صورتی که جزئیات یک تراکنش تغییر کند، این تغییر تا سطوح بالای درخت نیز می‌رسد و این درحالی است که ریشه درخت مرکل قبلا در هدر بلاک ذخیره شده است و به هنگامی که ریشه مرکل موجود در هدر بلاک با ریشه مرکل در داده‌ها مورد مقایسه قرار می‌گیرد، به راحتی می‌توان متوجه تغییرات انجام یافته در تراکنش‌ها گردید.
- کارآمدتر شدن فرآیند تائید داده‌ها: درخت مرکل با توجه به ویژگی‌های ذاتی خویش امکان تائید یکپارچه تراکنش‌ها را به صورت منظم و بی‌نقص فراهم کرده است.
- عدم تاخیر و سرعت بالا: استفاده از درخت مرکل در شبکه بلاک چینی سبب شده تا فرآیند انتقال داده‌ها در شبکه‌های بلاک چینی بدون کوچک‌ترین تاخیری انجام گیرد که چنین مسئله‌ای نقش کلیدی را در توسعه استفاده از فناوری بلاک چین در پرداخت‌های مالی روزمره کاربران ایفا می‌کند.

مطلب پیشنهادی: امور بانکی متمرکز (CeFi)

درخت مرکل؛ راه‌حلی امن برای کارآمدی فرآیند تائید تراکنش‌ها در بلاک چین

فرآیند تائید تراکنش‌ها و عدم امکان دستکاری اطلاعات آن‌ها از موارد مهمی است که هر پلتفرم فعال در حوزه نقل و انتقالات مالی بایستی توجه ویژه به آن داشته باشد. یکی از اصلی‌ترین راه‌حل‌های موجود در دنیای کریپتوکارنسی برای یکپارچه‌سازی داده‌ها، استفاده از **درخت مرکل (Merkle Tree)** است و با توجه به اهمیت این اصطلاح در مارکت ارز دیجیتال، ما این مقاله از بلاگ کیف پول من را به بررسی جامع مفهوم درخت مرکل در دنیای ارز دیجیتال اختصاص دادیم و همان طور که در مطالب فوق مشاهده کردید، این اصطلاح یکی از مفاهیم بسیار مهم علوم کامپیوتر به شمار رفته که در اصل نمایشگر ساختاری از داده‌هاست که در نمودار درختی جای گرفته‌اند.

در شبکه‌های بلاک چینی، از فناوری درخت مرکل به عنوان یک ابزاری کارآمد در زمینه سازماندهی داده‌های تراکنش‌ها استفاده می‌شود و در عمل کارآیی بیشتری را برای شبکه‌های بلاک چینی در ردیابی ساده هرگونه تغییر و دستکاری در داده‌های تراکنش‌ها را فراهم می‌آورد. ناگفته نماند که اگر در ارتباط با ماهیت و چیستی درخت مرکل در بازار رمزارزی و شبکه‌های بلاک چینی سوالی دارید که پاسخ آن را در مطالب فوق پیدا نکرده‌اید، می‌توانید سوال خویش را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.