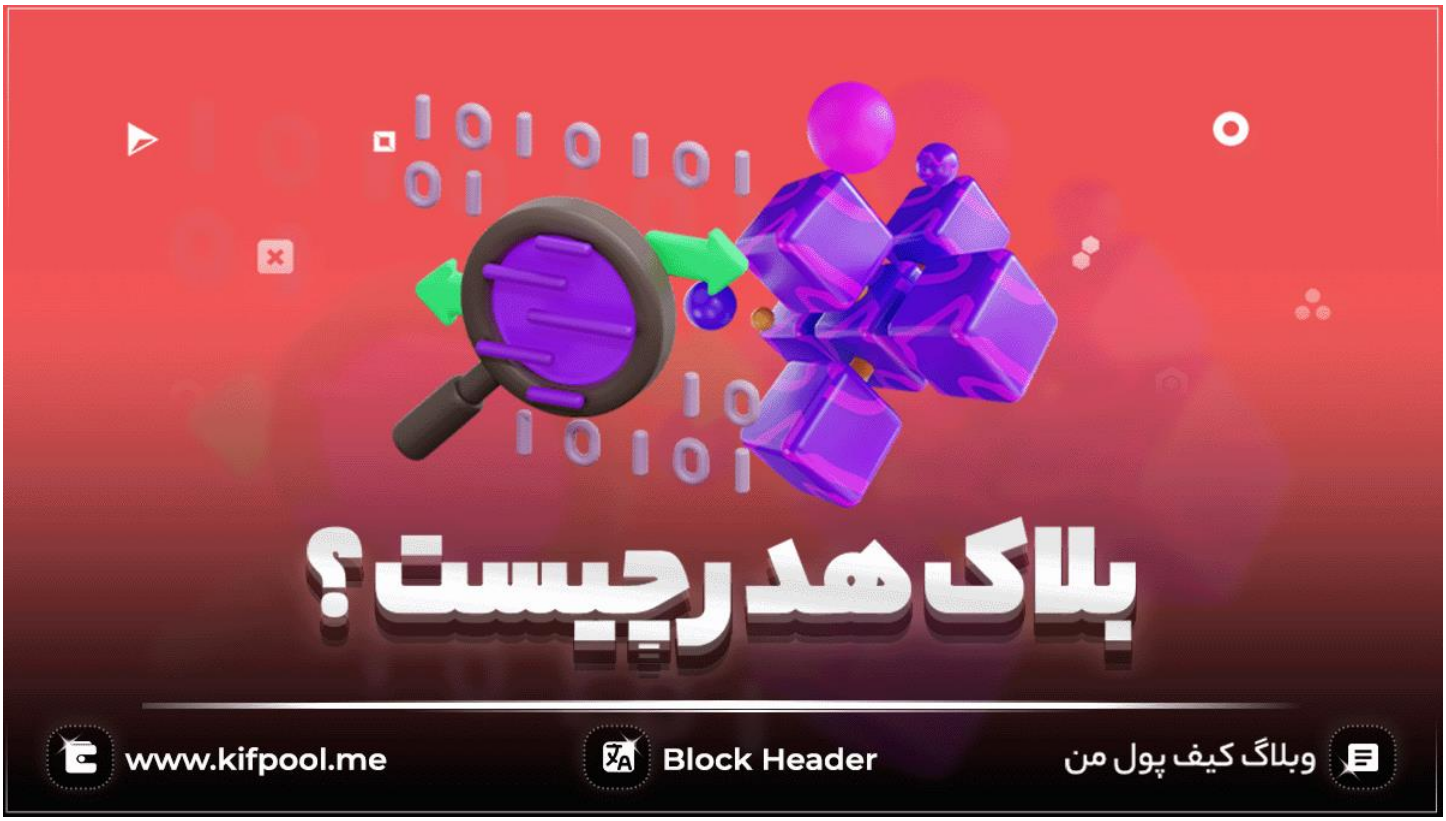


بلاک هدر (Block Header) چیست؟

آشنایی با هدر بلاک رمزارز به زبانی ساده

از هدر بلاک برای شناسایی یک بلاک خاص در کل زنجیره بلاکی استفاده می‌شود و نشانه‌ای برای شناسایی هر بلاک است. Block Header به‌طور مکرر هش می‌شود تا اثبات کار برای پاداش‌های استخراج یا همان ماینینگ برای ماینرها ایجاد گردد. به عبارتی دیگر، می‌توان گفت که ماینرها با هش کردن هدر بلاک به آن اعتبار می‌دهند. هش کردن هدر بسیار بهتر از هش کردن کل بلوکی است که می‌تواند هزاران تراکنش گوناگون داشته باشد و کار را سخت‌تر و طولانی‌تر کند. یک بلاک چین، مجموعه‌ای از بلاک‌های مختلف را شامل می‌شود که برای ذخیره اطلاعات مرتبط با تراکنش‌های رخ داده در شبکه به کار می‌رود. هر کدام از بلاک‌ها یک هدر منحصربه‌فرد را شامل می‌شوند و هر بلاک از طریق هدر بلاک خود به‌صورت جداگانه و منفرد شناسایی می‌گردد.

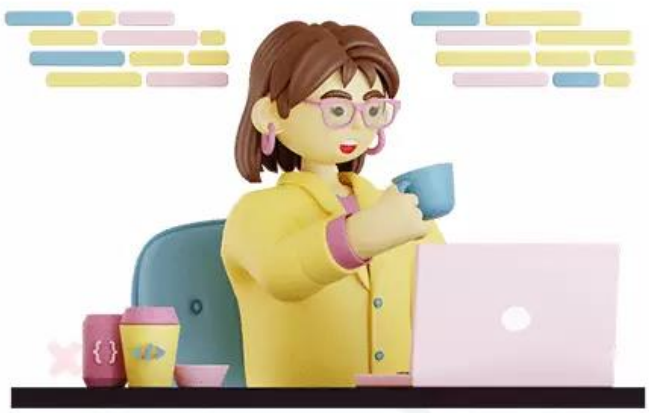
اجزای تشکیل دهنده هدر بلاک

هدر بلاک هر رمزارزی از سه مجموعه ابرداده بلوک تشکیل یافته است. این مجموعه، یک رشته ۸۰ بایتی را تشکیل می‌دهد و میانگین تراکنش‌ها حداقل ۲۵۰ بایت و بلوک متوسط بیش از ۵۰۰ تراکنش است. در ادامه جدول ساختار هدر بلاک را بررسی کرده و آشنایی بیشتری با هر یک پیدا می‌کنیم:

فیلد	توضیح	سایز
مهر زمانی (Timestamp)	زمان تقریبی ایجاد بلوک در یونیتکس را نشان می‌دهد.	٤ بایت
شماره نسخه یا ورژن (Version)	برای ردیابی ارتقاء نرم‌افزار یا پروتکل به کار می‌رود.	٤ بایت
ریشه مرکل	هش ریشه درخت مرکل با تراکنش‌های این بلوک ارتباط دارد.	۳۲ بایت
سختی شبکه (Difficulty Target)	دشواری الگوریتم اثبات کار برای این بلوک است.	٤ بایت
نانس (Nonce)	شمارنده‌ای است که ماینرها برای الگوریتم اثبات کار از آن استفاده می‌کنند.	٤ بایت
هش بلاک قبلی	هش بلوک قبلی در زنجیره را نشان می‌دهد.	۳۲ بایت

مهر زمان (Timestamp)

مهر زمانی در زنجیره بلوک نشان می‌دهد که یک بلوک در چه زمانی اجرا شده است. این اجزا به عنوان پارامتری برای تایید صحت هر بلوک نیز شناخته می‌شود.



با استفاده از شماره نسخه یا ورژن هدر بلاک می‌توانید به تغییرات و به‌روزرسانی‌ها دسترسی داشته باشید. نسخه‌های که بلاک‌ها از آن استفاده می‌کنند عبارتند از:

نسخه بلاک چین ۱٫۰ (ارز رمزنگاری شده): این نسخه همانند بیت کوین از یک دفتر کل عمومی برای ذخیره داده‌ها استفاده می‌کند.
بلاک چین نسخه ۲٫۰ (قرارداد هوشمند): در این نسخه که به آن قراردادهای هوشمند نیز گفته می‌شود، شامل برنامه‌هایی است که به خود شبکه اجرا کننده مانند اتریوم ربط دارند.
بلاک چین نسخه ۳٫۰ (DAPPS): این نسخه برای ایجاد یک ساختار غیرمتمرکز مانند مرورگر tor به کار می‌رود.
بلاک چین نسخه ٤٫۰ (بلاک چین برای صنعت): این نسخه برای ایجاد شبکه بلاک چین مقیاس پذیر و مقرون‌به‌صرفه به کار می‌رود تا افراد بیشتری بتوانند از آن استفاده کنند.

ریشه مرکل

ریشه مرکل از فرمول‌های ریاضی برای تشخیص داده‌های خراب، هک و دستکاری شده مطلع می‌شود. این اجزا، تمامی تراکنش‌ها را در هدر بلاک به‌صورت هش شده نگهداری می‌کند که مهر زمانی نیز شامل این بخش است. مهر زمانی امکان اینکه بتوان از زمان وقوع یک رویداد خاص را یک رکورد دائمی و رمزنگاری شده مطلع کند را نشان می‌دهد. اطلاعاتی مانند تاریخ و زمان این موضوع را نمایش می‌دهد و میزان دقت بالا با خطایی کمتر از ثانیه را داراست. تصور کنید که یک بلاک دارای ۲۰ تراکنش است و برای شناسایی این بلاک، به ۲۰ تراکنش نیاز داریم تا مقداری هش را با هم ترکیب کنیم؛ بنابراین به مقدار آن ریشه Merkle یا درخت مرکل گفته می‌شود.

دشواری هدف یا سختی شبکه

سختی شبکه یا دشواری هدف، پیچیدگی و قدرت محاسباتی مورد نیاز برای استخراج شبکه را نشان می‌دهد. دشواری هدف، باری تنظیم میزان سختی ماینرهایی که برای حل یک بلاک فعالیت می‌کنند، به کار می‌رود. اگر هدفی میزان سطح دشواری قابل توجهی داشته باشد، باید برای استخراج آن از یک ماشین محاسباتی گران‌تر استفاده کرد.

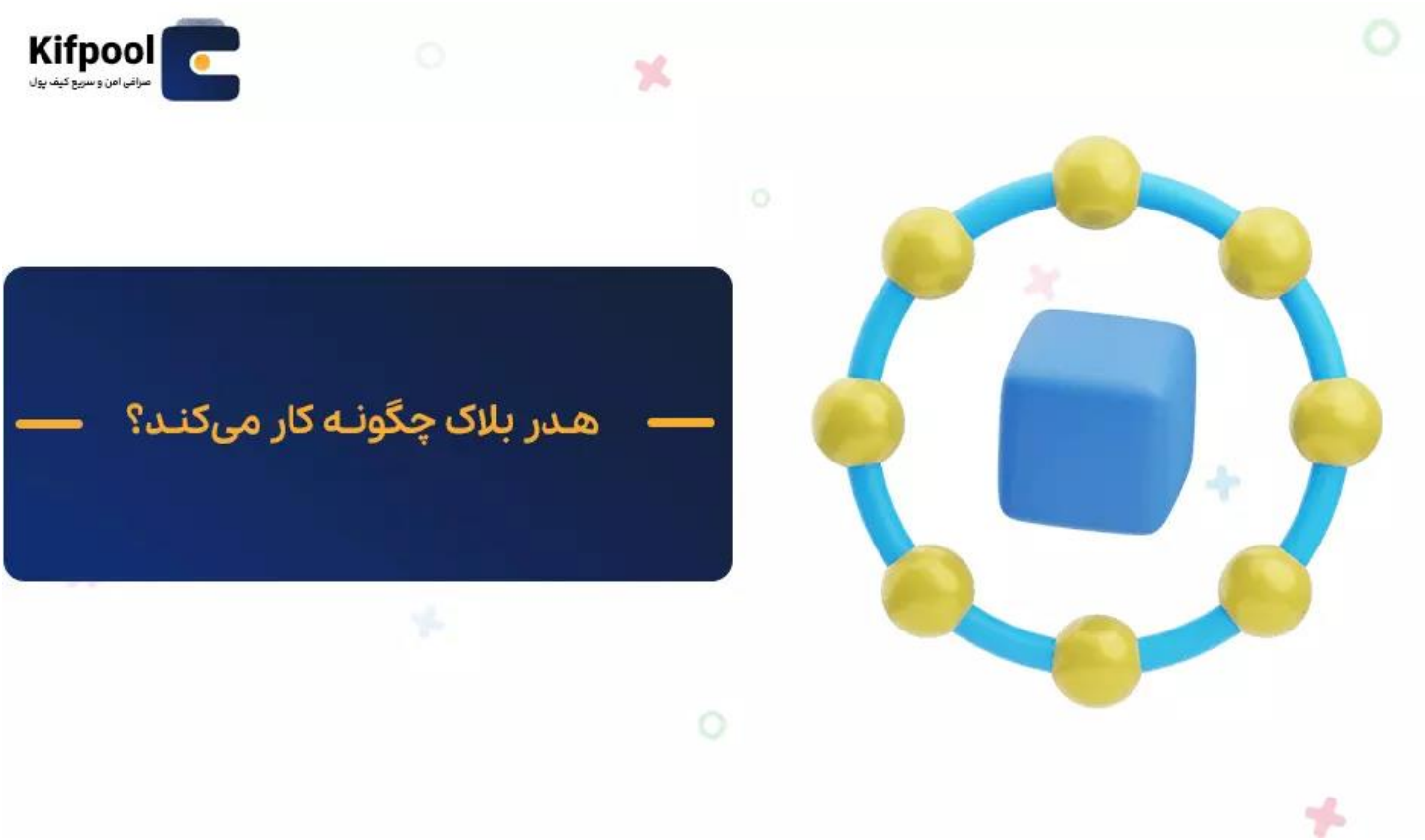
هش بلاک قبلی

از آنجایی که بلاک چین از چندین گره به نام بلوک یا بلاک تشکیل شده که به هم پیوسته هستند، هش قبلی مقدار هش شده آدرس گره قبلی را ذخیره می‌نماید. ناگفته نماند که اولین بلاک در بلاک چین، Genesis Block یا بلاک پیدایش است و هیچ مقدار هش قبلی ندارد. هش بلاک قبلی، آدرس گره قبلی یا والد را نگهداری می‌کند و می‌توان گفت که این بخش، باعث اتصال بلاک فعلی به بلاک والد می‌شود و از این طریق زنجیره‌ای ایمن به وجود می‌آورد.

نانس (Nonce)

Nonce مقداری است که ماینرها می‌توانند برای ایجاد جایگشت‌های گوناگون، آن را تغییر داده و یک هش درست در دنباله ایجاد نمایند. این مقدار به عدد فقط یک بار استفاده می‌شود مشهور است و عددی را شامل می‌شود که ماینرهای بلاک چین آن را پیدا می‌کنند و به‌طور مستقیم حدود ۱۰ بار طول می‌کشد تا به غیرصحیح بودن مقدار آن پی ببرند. ناگفته نماند که مقدار نانس از لحاظ محاسباتی، گران محسوب می‌شود.

هدر بلاک چگونه کار می‌کند؟



Block Header معمولا در اسناد توسعه دهندگان بیت کوین به کار می‌رود و باعث می‌شود تا وظایف هر بلاک به راحتی و با سرعت ذخیره شود. با کمک هدر بلاک می‌توان تمامی بلاک چین را در یک پایگاه ساده یا در حالت یک فایل ذخیره کرد. بلاک‌ها به‌طور لایه لایه طراحی می‌شوند و تا زمانی که به انتهای زنجیره بلاک برسند و توالی کامل شود، در همان ارتفاع رشد می‌کنند. اولین بلاک در زنجیره، بلاک پیدایش است و بلاک پایه در بالاترین سطح قرار می‌گیرد. همین طراحی لایه‌ای است که باعث می‌شود تا امنیت بیت کوین با نگهداری تاریخچه آن افزایش پیدا کند.

برای آشنایی با یک تمرین استخراج استاندارد، یک Block Header را در نظر بگیرید که به‌صورت مکرر توسط ماینرها با استفاده از تغییر مقدار نانس (nonce) هش می‌شود. ماینرها تلاش می‌کنند تا با انجام این کار، یک مدرک اثبات کار ایجاد نمایند تا به ماینرها کمک کنند که برای مشارکت‌های خود پاداش دریافت کرده و عملکرد یکپارچه و کارآمد سیستم بلاک چین حفظ شود. هش رمزنگاری، شناسه اصلی هر بلاکی است و مانند اثر انگشت دیجیتال آن بلاک محسوب می‌شود. هدر بلاک می‌تواند توسط الگوریتم‌های هش رمزگشایی شود و دوباره قابل خواندن و اجرا باشد.

ساختار هدر بلاک برای لایت کلاینت

هنگام خرید بیت کوین، خوب است بدانید که بلاک چین این رمزارز برای ذخیره‌سازی دستگاه‌هایی مانند گوشی‌های هوشمند بسیار بزرگ مناسب است. اگر زنجیره ۱۰۰۰۰۰ بلوک ۱ مگابایتی داشته باشد، شما باید ۱۰۰ گیگابایت فضا مصرف کنید؛ اما با استفاده از هدرهای بلوک، تنها به ۰٫۰۰۸ گیگابایت یا به عبارتی ۸ مگابایت

اشغال‌سازی فضا نیاز دارید. دستگاه‌هایی که فضای ذخیره‌سازی کمتری داشته باشند، می‌توانند درجاتی از اعتبارسنجی را به روال سابق انجام دهند. ریشه مرکل تمامی تراکنش‌ها را نگهداری می‌کند و از این طریق می‌توانید بررسی کنید که آیا تراکنش در یک بلوک خاص وجود دارد یا نه. البته انجام این کار هزینه‌ای هم دارد؛ چراکه به تکیه بر شخص ثالثی برای ارائه اطلاعات لازم نیاز است. در حالت کلی و باتوجه به نکات ذکر شده می‌توان گفت که کلاینت‌های لاین به سیستمی برتری دارند که در آن سیستم کاربران هیچ تاییدی انجام نمی‌دهند.

هدر بلاک؛ راه‌حل و نشانه‌ای برای شناسایی هر بلاک

هدر بلاک راه‌حل و نشانه‌ای برای شناسایی هر بلاک در زنجیره بلاک چین است و به‌صورت مکرر هش می‌شود تا اثبات کار برای پاداش‌های ماینرها ایجاد شود. هیچ بلاکی در بیت کوین بدون هدر وجود ندارد و هیچ زمانی هم وجود نخواهد داشت. اگر قصد دارید با عملکرد بلاک چین اطلاعات بیشتری پیدا کنید و به خوبی با نحوه کارکرد آن آشنا شوید، باید یادگیری هدر بلاک را در اولویت قرار دهید. هدف نهایی Block Header ایجاد یک ساختار امن، شفاف و غیرقابل تغییر و دستکاری برای ثبت تراکنش‌ها است تا از این طریق اعتماد کاربران در سیستم تامین شود. با علم بر این نکته که هدر بلاک چقدر برای اکوسیستم بیت کوین مهم است، اما بسیاری اوقات به آن بی‌توجهی می‌شود. به نظر شما دلیل این بی‌توجهی چیست؟ چرا در دنیای ارزها اغلب مسائل مهم در پشت پرده قرار می‌گیرند و بررسی نمی‌شوند؟ می‌توانید پاسخ‌های خود را در بخش نظرات کیف پول من با ما در میان بگذارید.