

# بلاک چین:

## هش چیست؟

آرشیو نموده

این روزها در دنیای فناوری مفاهیم تازه‌ای به وجود آمده که پیوسته خبرهای مربوط به آن‌ها و تغییر و تحولاتی را که در دنیای امروزی به وجود آورده‌اند، می‌شنویم. از جمله این مفاهیم می‌توان هوش مصنوعی، وب ۳، بلاک چین و متاورس را نام برد. در این مقاله می‌خواهیم به‌طور گسترده درباره بلاک چین بگویم.

بارشدر مزارها در دنیای اقتصاد دیجیتال، دیگر کمتر کسی وجود دارد که اسم بیت کوین را نشنیده باشد. بیت کوین معروف‌ترین ارز دیجیتال است که فردی ناشناس به نام ساتوشی ناکاموتو در سال ۲۰۰۹ میلادی

آن را معرفی کرد و بعدتر به یکی از انقلابی‌ترین ایده‌های دنیای اقتصاد تبدیل شد. اما ارتباط بیت کوین به بلاک چین چیست؟

پاسخ این است که بلاک چین فناوری‌ای است که بیت کوین بر بستر آن ساخته شده و مدیریت می‌شود. بلاک چین از دو واژه بلاک و چین تشکیل شده و به معنی زنجیره‌ای از بستک‌های (بلوک‌های) بهم وابسته و پشت سرهم است. این بستک‌ها برای ذخیره‌سازی اطلاعات دیجیتال

استفاده می‌شوند و نوعی پایگاه داده هستند. مفهوم بلاک چین را نخستین بار در سال ۱۹۹۱ دو دانشمند به نام‌های استوارت هابر

و اسکات استورنتا به‌عنوان روشی برای جلوگیری از دست‌کاری و تغییر اسناد الکترونیکی معرفی کردند، اما تا دهه اخیر و ظهور رمزارزها شهرت کافی پیدا نکرده بود. خاصیت‌های اصلی بلوک‌های بلاک چین، غیرمتمرکز بودن، تغییرناپذیری، امنیت بالا و شفافیت است که درباره هر کدام کمی بحث می‌کنیم.

سامانه متمرکز و غیرمتمرکز

شما می‌توانید بانک را به‌عنوان یک سامانه متمرکز در نظر بگیرید. وقتی به یک فروشگاه اینترنتی مراجعه می‌کنید و به پرداخت هزینه کالا می‌رسید، به یک صفحه پرداخت منتقل می‌شوید که به کارسازهای (سرورهای) بانک متصل است. شما مشخصات خود را مانند شماره کارت و رمز عبور، وارد می‌کنید. بانک بررسی می‌کند

**بلاک چین در لغت از دو کلمه بلاک و چین تشکیل شده و به معنی زنجیره‌ای از بستک‌های بهم پیوسته و پشت سرهم است. این بستک‌ها برای ذخیره‌سازی اطلاعات دیجیتال ما استفاده می‌شوند و نوعی پایگاه داده هستند.**

## « به هم پیوستگی و امنیت بلاک چین به کمک هش

در هر بستک، علاوه بر اطلاعاتی که ما وارد می‌کنیم، هش بستک قبلی هم ذخیره می‌شود که دلیل زنجیره نامیدن بلاک چین هم همین است. حال فرض کنید یک رخنه‌گر (هکر) قصد داشته باشد اطلاعات داخل یک بلوک را دست کاری کند و مثلاً مبلغ ثبت شده برای یک تراکنش را کم یا زیاد کند. در این صورت، حتی با عوض شدن یک رقم، هش آن بستک تغییر می‌کند و

تطابق نداشتنش با هش ثبت شده در بستک بعدی، دست کاری شدن آن را لو می‌دهد. بنابراین، رخنه‌گر برای تغییر اطلاعات یک بستک باید هش‌های ذخیره شده در تمام بستک‌های بعدی را هم تغییر دهد. این کار نیازمند توان پردازشی و انرژی بسیار زیادی است که در عمل غیرممکن است و نتیجه آن تغییر ناپذیری بستک‌ها و امن شدن بسیار بالای بلاک چین است. به همین شکل از این خاصیت تغییر ناپذیر بودن می‌توان در سایر حوزه‌ها هم استفاده کرد و هر جا که امنیت اطلاعات

ذخیره شده در اولویت است، آن را در یک بلاک چین ذخیره کرد. مثلاً برای ثبت فهرست اموال انبار یک شرکت، ثبت رأی‌های افراد در یک انتخابات یا ثبت تاریخچه مالیاتی یک مجموعه بزرگ.

در شماره‌های بعدی سعی می‌کنیم صحبت درباره بلاک چین را ادامه بدهیم و سایر موضوعات مربوط به آن، مانند رمزارزها، قراردادهای هوشمند، بهامهر (توکن)ها و «ان اف تی»ها را ارائه کنیم.

**هش هر بلوک برای آن مانند اثر انگشت برای انسان هاست و به عنوان ابزاری برای متمایز کردن آن‌ها از هم به کار می‌رود. کوچک‌ترین تغییر در اطلاعات یک بلوک باعث می‌شود هش آن کاملاً تغییر کند.**

ببیند آیا شما در حسابتان به اندازه مبلغ قیمت کالای مورد نظر پول دارید یا خیر. اگر مشکلی وجود نداشته باشد و شما پرداخت خود را نهایی کنید، بانک مبلغ مورد نظر را از حساب شما کم و به حساب فروشگاه اینترنتی انتقال می‌دهد. در این موقعیت، بانک در مرکز تمام تراکنش‌ها قرار گرفته و وظیفه مدیریت تراکنش‌ها و صورت حساب‌ها را بر عهده دارد و تنها خود بانک است که از موجودی حساب هر فرد آگاهی دارد. نکته منفی در این روش آن است که اگر روزی کارسازهای بانک بیش از حد شلوغ شوند یا به مشکل برخوردند، تراکنش‌های کاربران هم به مشکل بر می‌خورند. یا مثلاً اگر روزی فردی بتواند به کارسازهای بانک نفوذ و به آن‌ها را رخنه (هک) کند، اطلاعات حساب تمام مشتریان لو می‌رود. در مقابل این سامانه، بلاک چین وجود دارد که یک سامانه غیر متمرکز است. ما داخل بستک‌ها اطلاعات تمام تراکنش‌ها مانند تاریخ تراکنش، مبلغ، نشانی مبدأ و نشانی مقصد را ثبت می‌کنیم. به این ترتیب، بلاک چین ما یک دفتر کل برای صورت حساب‌ها بوده که به وسیله آن می‌توان با جمع و تفریق مبالغی که به کیف پول فرد داخل و خارج شده‌اند، موجودی فعلی آن کیف پول را محاسبه کرد. یک رونوشت دقیقاً یکسان از این بستک‌ها در دسترس هر کدام از اعضا قرار گرفته است و هر زمان که اطلاعات جدیدی در یک بلوک ثبت شود و قرار باشد آن بلوک به بلاک چین اضافه شود، به انتهای آن در رونوشت همه اعضا افزوده می‌شود. تمام پردازش‌ها و محاسبات مربوط به بلاک چین، مانند ساخت و تأیید بستک‌ها، توسط میلیون‌ها رایانه و پردازشگر متصل به شبکه در سراسر جهان انجام و بین آن‌ها تقسیم می‌شود. به این ترتیب، بلاک چین یک شبکه غیر متمرکز را به وجود می‌آورد تا به جای قرار داشتن مدیریت در دست یک نفر خاص، توسط تمامی اعضاء مدیریت صورت گیرد.

## « هش چیست؟

هش نوعی عملگر ریاضی است که روی داده‌هایی با هر حجم دلخواه اعمال می‌شود و در خروجی نوشته‌ای با طول ثابت را به ما می‌دهد. هش هر بلوک برای آن مانند اثر انگشت برای انسان هاست و به عنوان ابزاری برای متمایز کردن آن‌ها از هم به کار می‌رود. کوچک‌ترین تغییر در اطلاعات یک بستک باعث می‌شود هش آن کاملاً تغییر کند. بنابراین، از هش می‌توان به عنوان ابزاری برای بررسی صحت و درستی اطلاعات بستک‌ها استفاده کرد.