بلاک‌چین: هش چیست؟

آرش نعمت‌زاده

۱

این روزها در دنیای فناوری مفاهیم جدیدی به وجود آمده‌اند که به‌طور دائم خبرهای مربوط به آن‌ها و تغییر و تحولاتی را که در دنیای امروزی به وجود آورده‌اند، می‌شنویم. از جملهٔ این مفاهیم می‌توان هوش مصنوعی، وب ۳، بلاک‌چین و متاورس را نام برد. در این مقاله می‌خواهیم به‌طور مفصل دربارهٔ بلاک چین بگوییم.

با رشد رمزارزها در دنیای اقتصاد دیجیتال، دیگر کمتر کسی وجود دارد که اسم بیت‌کوین را نشنیده باشد. بیت‌کوین معروف‌ترین ارز دیجیتال است که فردی ناشناس به نام ساتوشی ناکوموتو در سال ۲۰۰۹ میلادی آن را معرفی کرد و بعدتر به یکی از انقلابی‌ترین ایده‌های دنیای اقتصاد تبدیل شد. اما ارتباط بیت‌کوین به بلاک‌چین چیست؟ پاسخ این است که بلاک‌چین فناوری‌ای است که بیت‌کوین بر بستر آن ساخته شده است و مدیریت می‌شود. بلاک‌چین در لغت از دو کلمهٔ بلاک و چین تشکیل شده و به معنی زنجیره‌ای از بستک‌های (بلوک‌های) متصل و پشت سرهم است. این بستک‌ها برای ذخیره‌سازی اطلاعات دیجیتال استفاده می‌شوند و نوعی پایگاه داده هستند. مفهوم بلاک‌چین 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 دههٔ اخیر و ظهور رمزارزها شهرت کافی پیدا نکرده بود. خاصیت‌های اصلی بلوک‌های بلاک‌چین، غیرمتمرکزبودن، تغییرناپذیری، امنیت بالا و شفافیت است که دربارهٔ هر کدام کمی بحث می‌کنیم.

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

سامانهٔ متمرکز و غیرمتمرکز

شما می‌توانید بانک را به‌عنوان یک سامانهٔ متمرکز در نظر بگیرید. وقتی به یک فروشگاه اینترنتی مراجعه می‌کنید و به پرداخت هزینهٔ کالا می‌رسید، به یک صفحهٔ پرداخت منتقل می‌شوید که به کارسازها(سرورهای) بانک متصل است. شما مشخصات خود را مانند شمارهٔ کارت و رمز عبور، وارد می‌کنید. بانک بررسی می‌کند ببیند آیا شما

در حسابتان به اندازهٔ مبلغ کالای موردنظر پول دارید یا خیر. اگر مشکلی وجود نداشته باشد و شما پرداخت خود را نهایی کنید، بانک مبلغ موردنظر را از حساب شما کم و به حساب فروشگاه اینترنتی انتقال می‌دهد. در این موقعیت، بانک در مرکز تمام تراکنش‌ها قرار گرفته و وظیفهٔ مدیریت تراکنش‌ها و صورت‌حساب‌ها را بر عهده دارد و تنها خود بانک است که از موجودی حساب هر فرد آگاهی دارد. نکتهٔ منفی در این روش آن است که اگر روزی کارسازهای بانک بیش از حد شلوغ شوند یا به مشکل بر بخورند، تراکنش‌های کاربران هم به مشکل بر می‌خورند. یا مثلاً اگر روزی فردی بتواند به کارسازهای بانک نفوذ و آن‌ها را رخنه (هک) کند، اطلاعات حساب تمام مشتریان لو می‌رود.

در مقابل این سامانه، بلاک‌چین وجود دارد که یک سامانهٔ غیرمتمرکز است. ما داخل بستک‌ها اطلاعات تمام تراکنش‌ها مانند تاریخ تراکنش، مبلغ، نشانی مبدأ و نشانی مقصد را ثبت می‌کنیم. به این ترتیب، بلاک‌چین ما یک دفتر کل برای صورت‌حساب‌ها است که به وسیلهٔ 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 بلاک‌چین اضافه شود، به انتهای آن در رونوشت همهٔ اعضا اضافه می‌شود. تمام پردازش‌ها و محاسبات مربوط به بلاک‌چین، 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، بلاک‌چین یک شبکهٔ غیرمتمرکز را به وجود می‌آورد که به جای اینکه مدیریت به دست یک فرد خاص، توسط همهٔ اعضا مدیریت می‌شود.

هش چیست؟

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

به‌هم‌پیوستگی و امنیت بلاک‌چین به کمک هش

در هر بستک، علاوه بر اطلاعاتی که ما وارد می‌کنیم، هش بستک قبلی هم ذخیره می‌شود که دلیل زنجیره نامیدن بلاک‌چین هم همین است. حال فرض کنید یک هکر قصد داشته باشد اطلاعات داخل یک بلوک را دست‌کاری کند و مثلاً مبلغ ثبت‌شده برای یک تراکنش را کم یا زیاد کند. در این صورت، حتی با عوض‌شدن یک رقم، هش آن بستک تغییر می‌کند و تطابق نداشتنش با هش ثبت‌شده در بستک بعدی، دست‌کاری‌شدن آن را لو می‌دهد. بنابراین، رخنه‌گر برای تغییر اطلاعات یک بستک باید هش‌های ذخیره‌شده در تمام بستک‌های بعدی را هم تغییر دهد. این کار نیازمند توان پردازشی و انرژی بسیار زیادی است که در عمل غیرممکن است و نتیجهٔ آن تغییرناپذیری بستک‌ها و امن‌شدن بسیار بالای بلاک‌چین است. به همین شکل از این خاصیت تغییرناپذیربودن می‌توان در سایر حوزه‌ها هم استفاده کرد و هر جا که امنیت اطلاعات ذخیره‌شده در اولویت است، آن را در یک بلاک‌چین ذخیره کرد. مثلاً برای ثبت فهرست اموال انبار یک شرکت، ثبت رأی‌های افراد در یک انتخابات یا ثبت تاریخچهٔ مالیاتی یک مجموعهٔ بزرگ.

هشِ هر بلوک برای آن مانند اثر انگشت برای انسان‌هاست و به‌عنوان ابزاری برای متمایزکردن آن‌ها از هم به کار می‌رود. کوچک‌ترین تغییر در اطلاعات یک بلوک باعث می‌شود هش آن کاملاً تغییر کند.

در شماره‌های بعدی سعی می‌کنیم صحبت دربارهٔ بلاک‌چین را ادامه بدهیم و دربارهٔ سایر موضوعات مربوط به آن، مانند رمزارزها، قراردادهای هوشمند، بهامهر (توکن)ها و «ان‌اف‌تی» ها را ارائه کنیم.