

بلاکچین چیست؟ و چه کاربردی دارد؟



بلاکچین چیست؟
و چه کاربردی دارد؟



نویسنده: مهران منصوری فر

اگر در دنیای ارزهای دیجیتال فعالیت می‌کنید، بدون شک بارها و بارها نام بلاکچین را شنیده‌اید. آیا دقیقا می‌دانید بلاکچین چیست و چگونه کار می‌کند؟ از اهمیت آن اطلاعی دارید؟ اگر شما نیز دوست دارید در این زمینه اطلاعات جامعی به دست آورید، خواندن این مقاله به شما کمک خواهد کرد.

بلاک چین به زبان ساده

بلاک چین دارای سیستمی غیر متمرکز بوده و در سراسر جهان قابل استفاده است. کلمه بلاک چین از دو کلمه block به معنای بلاک و chain به معنای زنجیره تشکیل شده است. علت انتخاب این نام آن است که اطلاعات داخل بلاک‌هایی ذخیره می‌شود که به صورت زنجیروار پشت سر یکدیگر قرار می‌گیرند.

شما برای هر تراکنش مالی به یک واسطه مانند بانک نیاز دارید، اما در خرید و فروش‌های ارز دیجیتال، بلاکچین جایگزین بانک شده است. در واقع بلاک چین به فرستندگان و ارسال کنندگان پول این امکان را می‌دهد که به صورت مستقیم با یکدیگر در ارتباط باشند و نیاز به شخص سوم نداشته باشند. برخلاف سیستم‌های بانکی که در یک موقعیت جغرافیایی مشخص و متمرکز واقع شده اند.



بلاک چین چگونه کار می‌کند؟

اطلاعات در بلوک‌هایی که در بالا با آن آشنا شدیم ذخیره می‌شود. هر بلوک ظرفیت مشخص و محدودی را دارد. زمانی که ظرفیت یکی از بلاک‌ها پر شود، این بلوک به بلوک پر قبلی و بلوک خالی بعدی وصل می‌شود. از این رو ما شاهد زنجیره‌ای از بلوک‌ها و اطلاعات هستیم.

بنابراین پایگاه داده بلاک چین، یک پایگاه داده زنجیروار است که مرکزیت خاصی نداشته و توسط گروه یا ارگان خاصی کنترل نمی‌شود. نکته مهم و قابل توجه آن که تمامی اطلاعات قرار داده شده در بلاک چین با تمامی اعضای شبکه به اشتراک گذاشته می‌شود. این اطلاعات ذخیره شده نه تنها مربوط به اطلاعات تراکنش‌های مالی نیست بلکه می‌تواند مربوط به هر اطلاعات دیگر نیز باشد. هر بلاک دارای یک خروجی رمزنگاری شده تحت عنوان هش بوده که ترکیبی از حروف و اعداد است.

بلاکچین چیست؟ و چه کاربردی دارد؟

این اطلاعات و هش از یک الگوریتم بسیار پیشرفته استفاده می‌کند و در صورت هر گونه تغییر یا حذف اطلاعات در هر بلوک، هش مربوطه نیز تغییر پیدا می‌کند. از این رو امکان هک کردن بلاک چین تقریباً غیر ممکن است.

یکی از مثال‌های کاربردی بلاک چین، گوگل داکس است. در گوگل داکس زمانی که شما به عنوان یک کاربر یک سند تولید کرده و در شبکه بارگزاری می‌کنید، بقیه اعضای گوگل داکس نیز می‌توانند به آن دسترسی داشته باشند. تمام تغییرات بلافاصله در سند ایجاد شده و هیچ کاربری برای کار کردن با آن فایل، معطل کاربر دیگر نمی‌ماند.



تاریخچه بلاک چین

قبل از آن که بیشتر با این مفهوم پرکاربرد آشنا شویم، می‌خواهیم بدانیم که تاریخچه آن به چه زمانی برمی‌گردد؟

این تکنولوژی برای اولین بار در سال ۲۰۰۹ و توسط بیت کوین در کدهای برنامه نویسی آن مورد استفاده قرار گرفت.

بعد از بیت کوین ارزهای دیگر نیز توانستند از بلاک چین استفاده کرده و کوین مخصوص به خود را راه اندازی کنند.

تنها مدتی کوتاه بعد از این مساله، متخصصان حوزه تکنولوژی دریافتند که بلاک چین تنها محدود به ارزهای دیجیتال نیست و می‌تواند کاربردهای فراوان دیگری داشته باشد. در واقع دومین فناوری بلاک چین مرحله‌ای بود که کارشناسان این حوزه متوجه شدند که این فناوری را می‌توان از بیت کوین جدا کرده و آن را برای اهداف دیگر مورد استفاده قرار داد.

سومین نوآوری در حوزه بلاک چین، تولد فناوری قرارداد هوشمند بود. در این نسل بلاک چین با عنوان اتریوم خود را به جهان معرفی کرد که تا کنون پیشرفت‌های بسیاری نیز داشته است.

چهارمین نوآوری مهم در حوزه بلاک چین، تغییر شیوه برقراری امنیت شبکه از روش اثبات کار Proof of Work به روش اثبات سهام Proof of Stake بود. در روش اثبات کار، تصمیمات امنیت شبکه توسط گروهی گرفته می‌شود که بیشترین قدرت پردازشی را برای تولید یا استخراج بلاک دارند.

در روش اثبات سهام با توجه به مقدار و تعداد کوین‌های بومی که تحت مالکیت دارند، به افراد اجازه مشارکت در تصمیم‌های امنیتی و تولید و اعتبار سنجی بلوک داده می‌شود.

به عبارت دیگر افراد با سرمایه گذاری در شبکه بلاک چین، مجوز دریافت و استخراج پاداش و اعتبار سنجی بیشتری از شبکه را دریافت می‌کنند. پنجمین فناوری انجام شده در حوزه بلاک چین، فناوری بلاک چین مقیاس بندی شده و یا Scaled Blockchain است. در فناوری‌های گذشته بلاک چین، تمامی کامپیوترهای موجود در شبکه وارد فرآیند پردازش می‌شدند. این مساله باعث کند شدن شبکه می‌شد. در بلاک چین مقیاس بندی شده تعداد مشخصی از کامپیوترها، برای تقسیم کار پردازش و اعتبار سنجی مورد استفاده قرار می‌گیرند. این مساله باعث می‌شود بدون کاهش امنیت شبکه، سرعت پردازش چند برابر شود.

آیا تغییر اطلاعات در بلاک ها ممکن است؟

بسیاری از افراد تصور می‌کنند که تغییر اطلاعات در بلاک چین غیر ممکن است. این تصور اشتباه است، در واقع این افراد متوجه مفهوم چگونگی تغییر اطلاعات در بلاک چین نشده‌اند. تغییر اطلاعات در بلاک چین ممکن است اما این تغییر از چشم دیگر کاربران نیز مخفی نمانده و تقریباً فاقد اعتبار خواهد بود. اجازه دهید با یک مثال ساده متوجه این مساله شویم. تصور کنید که شما اطلاعات یک سند رسمی مهم را در بلاک چین ذخیره کرده‌اید، تمامی کاربران آن را مشاهده کرده و در واقع یک نسخه کپی از آن را خواهند داشت اگر شما هر تغییر در این اطلاعات ایجاد کنید، کاربران دیگر نسخه اصلی فایل را دارند و این تغییرات دیگر ارزش و اعتباری نخواهد داشت.



انواع بلاک چین

بعد از آن که با مفهوم و کارکرد بلاک چین آشنا شدیم، بهتر است بدانیم این فناوری چه انواع مختلفی دارد. بلاک چین‌ها به طور کلی به دو دسته عمومی و خصوصی تقسیم بندی می‌شوند.

بلاک چین عمومی

همان طور که از نام این بلاک چین پیدا است، این بلاک چین محدودیتی برای اعضا و استفاده نداشته و توسط خودمردم کنترل می‌شود. لایت کوین، بیت کوین و اتریوم از جمله شناخته شده‌ترین انواع بلاک چین عمومی هستند. این نوع بلاک چین‌ها متن باز و شفاف هستند و تصمیم‌گیری‌های نهایی از طریق الگوریتم‌های اجماع مانند اثبات سهام یا اثبات کار انجام می‌شود. در واقع هر کس که به اینترنت دسترسی دارد، می‌تواند به یک عضو شبکه یا اصطلاحاً نود تبدیل شده و به عنوان بخشی از شبکه بلاکچین در نظر گرفته شود.

در این حالت کاربر می‌تواند به اطلاعات قبلی دسترسی پیدا کرده، آن‌ها را اصلاح یا تایید کند. هرکس می‌تواند تراکنش داشته باشد و یا عملیات ماینینگ را انجام دهد.

بلاک چین خصوصی

همانطور که از نام این بلاک چین پیدا است، استفاده از آن عمومی نبوده و محدودیت در میزبان دارد. این نوع معمولا دارایی خصوصی یک شخص و یا یک سازمان به شمار می‌رود. برخلاف انواع عمومی، در نوع خصوصی یک نفر مسئول موارد مهمی مانند نوشتن و خواندن است. در این نوع، تصمیم‌گیری‌ها و اجازه ماینینگ به کاربر توسط مسئول مرکزی است و به اجماع گذاشته نمی‌شود. در واقع بلاک چین خصوصی یک شبکه کوچک است که اختیارات در آن بر عهده یک شخص یا اشخاص مشخص و محدود است.



آشنایی با مفاهیم کاربردی در بلاک چین

در بخش های بالا از کلمات مانند بلوک، گره و ماینینگ یا استخراج استفاده کردیم.

در واقع زمانی که صحبت از بلاک چین است، ما با این سه مفهوم بالا سروکار داریم که باید با آنها آشنا شویم.

بلوک

با مفهوم بلوک آشنا شدیم و متوجه شدیم تمامی اطلاعات ما در واحدهایی به نام بلوک ذخیره می شود. بلوک در زمان ساخت بلوک برای هر اطلاعات، یک عدد ۳۲ بیتی به طور تصادفی ساخته می شود که به آن nonce گفته می شود. در همین زمان هش نیز به صورت تصادفی به صورت یک عدد ۲۵۶ بیتی ترکیبی از اعداد و کاراکترها ساخته می شود.

ماینر و ماینینگ

بلوک های جدیدی که اطلاعات در آن ذخیره می شود، باید توسط کامپیوترهایی در سراسر جهان تولید شود. به فرآیند تولید بلوک ماینینگ یا استخراج و به سیستم های کامپیوتر ماینر گفته می شود. در ماینینگ هر بلوک دارای هش و nonce مخصوص به خود است اما باید به بلوک قبلی نیز مرتبط باشد. از آن جایی که هش ۲۵۶ و nonce ۳۲ بیتی است، تقریباً ۴ میلیارد ترکیب ممکن برای استخراج بلوک وجود دارد. از این رو ماینرها باید با استفاده از نرم افزارهای پیشرفته ریاضی این معادلات پیچیده را حل کنند.

بلاکچین چیست؟ و چه کاربردی دارد؟

نکته قابل توجه آن که هر تغییر در اطلاعات بلوک‌ها نیازمند تولید nonce و هش جدید است. از این رو امکان کلاه برداری در این حوزه تا حد بسیار زیادی پایین است.

گره

مفهوم مهم دیگر در بلاک چین، گره است. به تمامی کامپیوترها و دستگاه‌های دیجیتالی که نسخه‌های کپی شده را حفظ کند، گره نامیده می‌شود. این گره‌ها به صورت زنجیروار به یکدیگر وصل هستند از این رو یک کامپیوتر و یا سازمان خاص نمی‌تواند مالک این زنجیره باشد. هر گره باید به صورت الگوریتمی بلوک‌های جدید ایجاد شده را برای تایید زنجیره، اعتماد سازی و به روز رسانی تایید کند.



مراحل کاری بلاک چین

در این بخش از مقاله می‌خواهیم بدانیم که بلاک چین چگونه کار کرده و چه روال کاری دارد.

بلاک چین تک به تک اطلاعات و تراکنش‌های انجام شده را در خود ذخیره کرده تا اگر یک شخص به منظور کلاه برداری خواست یک ارز دیجیتال را دو بار معامله کند، مانع آن شود. در هر تراکنش و هر ذخیره اطلاعات ۴ مرحله زیر به ترتیب انجام می‌شود:

۱. در مرحله اول معامله انجام می‌شود.

۲. بعد از خرید و انجام معامله، صحت آن باید تایید شود. این کار توسط هزاران یارانه‌ی موجود در سراسر جهان بررسی شده و سپس در زمان بسیار کوتاهی تایید می‌شود.

۳. بعد از تایید باید اطلاعات مربوط به تراکنش شما در یک بلوکی که در بالا با آن آشنا شدیم، ذخیره می‌شود. این اطلاعات در کنار میلیاردها اطلاعات دیگر ذخیره می‌شود.

۴. بعد از ذخیره شدن اطلاعات در هر بلوک، به آن یک هش اختصاص داده می‌شود که در بالا با آن آشنا شدیم. با اختصاص دادن یک هش به یک بلوک، آن بلوک به زنجیره بلاک چین اضافه می‌شود.

کاربردهای بلاک چین

همان طور که در بالا نیز به این مساله اشاره کردیم، مهم‌ترین کاربرد این فناوری در حوزه ارزهای دیجیتال است، اما آیا این کاربرد تنها محدود به همین حوزه خواهد شد؟ بدون شک خیر!

• استفاده از این فناوری در ارزهای دیجیتال باعث می‌شود، امکان کلاه بردای، فروش یک رمز ارز به چند نفر و دیگر موارد ممکن به صفر برسد.

• از دیگر کاربردهای این فناوری می‌توان به استفاده از آن در سیستم‌های رای گیری و انتخابات آنلاین اشاره کرد. با استفاده از بلاک چین در این حوزه می‌توان، امکان تقلب و یا خطای انسانی را تا حد زیادی کاهش داد.

• یکی دیگر از کاربردهای بلاک چین آن است که شما می‌توانید تمام دارایی‌های خود را به توکن‌های دیجیتال تبدیل کرده و به راحتی بتوانید آن را معامله کنید. برای مثال اگر ملک شما چند میلیارد تومان قیمت دارد، می‌توانید آن را هزاران توکن دیجیتال تبدیل کرده و آن‌ها را به افراد مختلف بفروشید. در واقع ممکن است شما ماه‌ها منتظر یک مشتری دست به نقد برای خانه میلیاردی خود بمانید اما در زمان کوتاهی می‌توانید میلیون‌ها توکن خود را بفروشید.

• کاربرد دیگر بلاکچین در سیستم حمل و نقل است. شرکت‌های تولید کننده می‌توانند اطلاعات سیستم حمل و نقل و کالاهای خود را از ابتدای تولید و حرکت از کارخانه در یک پایگاه داده ثبت کرده و آن در اختیار خریداران و کارکنان کارخانه بگذارند.

• از دیگر کاربردهای این فناوری می‌توان به استفاده از آن در حوزه پزشکی و دارویی اشاره کرد. برای مثال پلتفرم Clin Tex از این فناوری استفاده می‌کند تا مطمئن شود محصولات کاربردی و البته کم یاب واقعا به دست افرادی که بیشترین نیاز را به آن دارند، می‌رسد.

• کاربرد دیگر بلاک چین در حوزه تولید دستگاه‌های هوشمند و دیجیتال به خصوص تلفن‌های هوشمند است. برای مثال شرکت سامسونگ در گوشی‌های سری جدید گلکسی خود از این فناوری استفاده کرد است.

در واقع کاربرد بلاک چین در هر حوزه‌ای برای حفظ امنیت اطلاعات کاربران و حقوق آنها است تا عدالت اجتماعی و امنیت در حوزه‌های مختلف در بهترین حالت ممکن انجام شود.



ویژگی‌های بلاک چین

تکنولوژی بلاک چین دارای ویژگی‌های منحصر به فردی است که تا اینجای مقاله کم و بیش با آن آشنا شدیم. به طور کلی ویژگی‌های این تکنولوژی شامل موارد زیر است:

امنیت

همان طور که در بالا نیز اشاره شد، رمزنگاری ارزها در بلاک چین با ۴ میلیارد حالت ممکن انجام می‌شود. از این رو امنیت در آن بسیار بالا بوده و امکان تقلب و کلاه برداری در آن تقریباً صفر است.



نهایت شفافیت

همان طور که در بالا نیز اشاره شد اطلاعات در بلاک چین به صورت شفاف به همه کاربران ارائه می‌شود. نکته قابل توجه آن که این شفافیت اطلاعات مربوط به اطلاعات تراکنش است اما اطلاعات شخصی شما و مبلغ موجود در کیف پول اطلاعاتی شخصی است. برای مثال زمانی که شما یک بیت کوین را از یک کاربر دیگر می‌خرید، این تراکنش به صورت شفاف به کاربران نمایش داده می‌شود تا امکان تقلب در آن وجود نداشته باشد.

غیر قابل تغییر بودن

همان طور که در بالا نیز اشاره شد، تغییر اطلاعات در بلاک چین نیازمند تولید هش و نونس جدید است. از طرف دیگر این تغییرات از دید کاربران دیگر قابل مشاهده بوده و ارزش خود را از دست می‌دهد.

از این رو گفته می‌شود که تغییر اطلاعات در بلاک چین غیر ممکن است چرا که تغییر اطلاعات کاری بی ارزش و بیهوده است.

محدودیت‌ها و مشکلات مربوط به بلاک چین

در این بخش می‌خواهیم بدانیم که تکنولوژی پرترفدار دارای چه محدودیت‌ها و مشکلاتی است.

اصطلاحات تخصصی:

این فناوری یک فناوری جدید با اصطلاحات تخصصی است. متأسفانه بسیاری از افراد بدون اطلاعات و دانش خاصی وارد این حوزه می‌شوند.

هزینه تراکنش‌ها

در چند سال اول تراکنش و مبادله ارزهای دیجیتال به خصوص بیت کوین رایگان انجام می‌شد، اما این هزینه به مرور افزایش پیدا کرد به طوری که در حال حاضر این مبلغ، مبلغ قابل توجهی به شمار می‌رود.

امکان نقض سیستم ایمنی

در صورتی که بیش از ۵۰ درصد از گره‌های شبکه، صحت یک معامله اشتباه را درست تشخیص دهند، آن معامله با وجود اشتباه بودن تایید می‌شود. البته امکان بروز این مساله بسیار کم است.



بلاک چین در آینده

همان طور که می‌دانید این فناوری چند سالی است که به دنیا معرفی شده است اما در همین زمان کوتاه توانسته است جایگاه قابل توجهی را به دست آورد. بدیهی است با توجه به ویژگی‌های منحصر به فرد این تکنولوژی، استفاده از آن در آینده بسیار پررنگ‌تر از حال حاضر خواهد بود. مردم ترجیح می‌دهند به جای آن که اموال خود را در بانک نگه داری کنند، آن در کیف پول‌های دیجیتال خود نگه داشته و بتوانند به راحتی و بدون نیاز به واسطه آن را مبادله کنند. همچنین با استفاده از این تکنولوژی شما می‌توانید فارغ از بسیاری از تحریم‌های مالی به سیستم جهانی وصل شده و مبادلات مالی خود را انجام دهید.

جمع بندی

بلاک چین یکی از جدیدترین تکنولوژی‌های موجود است که ساختاری غیر متمرکز و با امنیت بسیار بالا دارد. در این تکنولوژی در کنار امنیت، اطلاعات به طور شفاف در اختیار کاربران قرار گرفته و تصمیم‌گیری‌های مالی توسط خود کاربران با الگوریتم‌های جمعی انجام می‌شود. بلاک چین دارای کاربردها و مفاهیم زیادی است که در این مقاله به زبان ساده با آن‌ها آشنا شده‌ایم.