بلاک چین چیست؟

همه آنچه باید درباره
فناوری Blockchain بدانید

بلاک چین، سیستم ثبت دیجیتالی است که تراکنش‌های مالی و برخی داده‌های دیگر را به صورت زنجیره‌ای از بلاک‌های رمزگذاری‌شده، به صورت امن ذخیره می‌کند.

بلاک چین، فناوری نوآورانه‌ای است که برای ذخیره و انتقال داده‌ها استفاده می‌شود؛ این فناوری اولین بار در سال ۲۰۰۸ توسط شخص یا گروهی با نام مستعار ساتوشی ناکاموتو به عنوان نویسنده اصلی وایت پیپر بیت کوین (Bitcoin Whitepaper) معرفی شد و به مجموعه‌ای از بلاک‌های متصل به یکدیگر اشاره دارد که در هر بلاک، تعدادی تراکنش (Transaction) در قالب یک فهرست وجود دارند.

هر بلاک، حاوی کُدِ هَش (Hash Code) برای تأیید اعتبار داده‌های موجود در آن است و به صورت خودکار رمزنگاری می‌شود. در هش کد هر بلاک، هش کد بلاک قبلی نیز موجود است و Blockchain به همین ترتیب به شکل زنجیره‌ای از بلاک‌هایی که به یکدیگر متصل هستند، شکل می‌گیرد. با توجه به اینکه هر بلاک به بلاک قبلی متصل است، امکان تغییر داده‌ها در بلاک‌های گذشته وجود ندارد و این موضوع، امنیت و اعتماد بیشتر به داده‌های ذخیره شده در بلاک چین را به همراه خواهد داشت.

بـلاک چیـن در صنعـت مالـی، زنجیـره‌ی تأمیـن، رایانـش ابـری و سـایر زمینه‌هایـی کـه نیـاز بـه ذخیره‌سـازی و انتقـال اطلاعـات دارنـد، اهمیت بسیار بالایـی پیـدا کرده و در کنار افزایش سـرعت و کاهـش هزینه‌هـا، خدماتـی ماننـد فراهـم کـردن مالکیـت بـرای دارایی‌هـای دیجیتـال، امنیـت بـرای داده‌هـا، امـکان ردگیـری و شفاف‌سـازی زنجیـره تامیـن کالا و خدمـات را در اختیـار دنیـای امـروز قـرار می‌دهـد.

در سـال‌های اخیـر، افـراد بسـیاری به‌دنبـال خریـد و فـروش بیـت کویـن و اسـتفاده از قابلیت‌هـای دیگـر ایـن ارز دیجیتـال بوده‌انـد. از افـراد مبتـدی و تـازه‌کار تـا تریدرهـای حرفـه‌ای دنیـای جـذاب ارزهـای دیجیتـال، همـه بـه ایـن پدیـده‌ی نوظهـور و خـاص قـرن ۲۱، علاقـه‌ی بسـیاری پیـدا کرده‌انـد.

بـا وجـود افزایـش روزافـزون تعـداد تریدرهـای بـازار ارزهـای دیجیتـال، افـراد کمـی دربـاره‌ی فنـاوری زیرسـاختی بیـت کویـن، یعنـی بـلاک چیـن مطالعـه کـرده و از آن آگاهـی دارنـد؛ حتـی ممکـن اسـت از سـاخت ارزهـای دیجیتـال دیگـر بـر پایـه بـلاک چیـن هـم بی‌اطـلاع باشـند. در ایـن مقالـه از بیت پین، قصـد داریـم دربـاره فنـاوری Blockchain و کاربردهـای آن در دنیـای مـدرن توضیـح دهیـم.

بلاک چین چیست؟

در جامعه سنتی، ما برای انجام تراکنش‌های مالی باید از واسطه‌هایی مانند بانک‌های دولتی و خصوصی استفاده کنیم؛ اما، بلاک چین با از بین بردن این نیاز، به خریداران و فروشندگان (ارسال‌کنندگان و دریافت کنندگان پول دیجیتال) اجازه می‌دهد تا به‌صورت مستقیم و بدون واسطه یا حضور شخصی ثالث، با هم در ارتباط باشند و ارزهای دیجیتال را معامله کنند. به این شکل از انجام تراکنش، مکانیسم «همتا به همتا» گفته می‌شود.

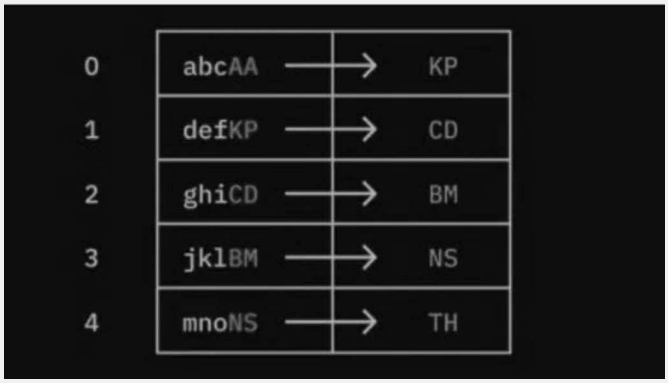
فناوری بلاک چین از رمزنگاری برای افزایش امنیت در خرید و فروش ارز دیجیتال و حتی تبادلات استفاده می‌کنند . سیستم‌های بانکی دارای موقعیت مکانی مشخصی هستند و به اصطلاح، متمرکز فعالیت می‌کنند، اما مرکز داده‌ای که شبکه‌های بلاک چین در آن قرار دارند، کاملا غیرمتمرکز بوده و در سراسر جهان توزیع شده‌اند.

به محل نگه‌داری و حفظ اطلاعات بلاک چین‌ها، «دفتر کل توزیع شده» گفته می‌شود؛ دفتر کل توزیع شده برای تمام اعضای حاضر در شبکه و با جزئیات کامل، قابل دسترسی است و حتی جزئی‌ترین تغییرات در تبادلات، برای همه به صورت شفاف قابل مشاهده و بررسی است. در واقع، دفتر کل توزیع شده، زنجیره‌ای از رایانه‌هایی است که درستی تراکنش‌های صورت گرفته بین کاربر اول و کاربر دوم را بررسی و تایید کرده و پس از آن، اطلاعات تراکنش را به بلاک چین ارسال می‌کنند.

تمامی داده‌ها در شبکه Blockchain در ساختار بلاکی (Block) وارد پایگاه داده می‌شوند و هر بلاک در ادامه بلاک قبلی و با اطلاعات آن بلاک، ایجاد می‌شود. با توجه به این‌که این بلاک‌ها با کمک اطلاعاتی به یک‌دیگر متصل هستند، بنابراین می‌توان گفت که زنجیر یا چِین (Chain) را تشکیل می‌دهند که در آن، بلاک‌ها به ترتیب ساخت در کنار هم قرار می‌گیرند. اولین بلاک شبکه که قبل از آن، بلاک دیگری وجود ندارد، «جنسیس بلاک» نام دارد.

ساده‌ترین تعریف برای بلاک چین، فهرست دیجیتالی توزیع شده است که اطلاعات را به صورت زنجیره‌ای از بلاک‌های رمزگذاری شده ذخیره کرده و امنیت، شفافیت و پایداری را برای تراکنش‌ها به ارمغان می‌آورد.

فرض کنید که دو ستون روی برگه‌ای دارید و هر اطلاعاتی که می‌خواهید نگهداری کنید را در سطر اول ستون اول بگذارید. داده داخل این سلول، طی فرآیندی محاسباتی تبدیل به یک کلمه جدید با دو حرف می‌شود. این کلمه در ورودی بعدی مورد استفاده قرار می‌گیرد. در این حالت، هر تغییری در سلول اول، منجر به تغییراتی در سلول بلاک دوم و تا انتهای زنجیره می‌شود. تصویر زیر مثالی گویا از پایگاه داده‌ای است که اطلاعات در آن به صورت زنجیره‌ای به‌هم متصل شده‌اند.



با توجه به تصویر بالا می‌توان گفت که آخرین شناسنامه‌ی بلاکی که در اینجا TH است، نتیجه‌ی تمام داده‌های وارد شده در ردیف‌های قبلی است و هر تغییری در یکی از این داده‌ها منجر به تغییر تمام داده‌ها خواهد شد. اکنون که این مثال را مرور کردید، می‌توان گفت که به زبان ساده با فرآیند هشینگ (Hashing) در بلاک چین آشنا شدید. مارک اندرسون (Marc Andreess)، مؤسس شرکت خدمات رایانه‌ای نت‌اسکیپ (Netscape) درباره‌ی بلاک چین می‌گوید:

بلاک چین روشی برای کاربران اینترنتی است تا قطعه‌ای از دارایی‌های دیجیتالی یکتای خود را به دیگر کاربران انتقال دهند؛ این انتقال تضمین شده و امن است و هیچ فردی نمی‌تواند مشروعیت آن را به چالش بکشد؛ دستاوردهای این پیشرفت بسیار اغراق‌آمیز خواهد بود.

نگاهی کوتاه به
تاریخچه بیت کوین
اولین ارز دیجیتال جهان

در ۳۱ اکتبر ۲۰۰۸، فردی (یا گروهی) با عنوان مستعار و ناشناس ساتوشی ناکاموتو، مقاله‌ای منتشر کرد و در آن مفهوم بیت کوین را به عنوان پول نقدی الکترونیکی و عملکرد آن برای ارسال و دریافت پول بین دو نفر، بدون واسطه و ناشناس، معرفی کرد. با توجه به اینکه بیت کوین برای عملکرد خود از رمزنگاری بهره می‌برد، اصطلاح ارز دیجیتال را برای این ابزار به کار می‌برند.

هدف از اختراع بیت‌کوین، در درجه‌ی اول، تمرکززدایی تراکنش‌های مالی بود؛ اما با گذشت زمان، محققان با بررسی فناوری زیرساختی آن، متوجه ظرفیت‌های بالاتری برای استفاده از آن در صنایع دیگر شدند. ظرفیتی که می‌توانست برنامه‌های حرفه‌ای با رویکرد فناوری مدرن و به‌روز برای صنایع مختلف خلق کند. این‌گونه بود که بلاک چین، به عنوان فناوری جذاب و انقلابی برای پیاده‌سازی زیرساخت‌های تاثیرگذار معرفی شد.

بلاک چین
چگونه کار می‌کند؟

بلاک چین، همه داده‌ها و جزئیات یک‌به‌یک تراکنش‌های انجام شده با این رمزارز را در خود ذخیره می‌کند و اگر کاربری بخواهد یک بیت کوین را بیش از دوبار معامله کند (به نوعی، قصد کلاهبرداری داشته باشد) مانع از انجام آن کار می‌شود. در هر بلاک، به محض وارد شدن اطلاعات جدید، این اطلاعات ذخیره شده و به بلاک چین اضافه می‌شود. این گونه، بلاک چین با زنجیره‌ای از چندین بلاک به‌هم پیوسته، شکل می‌گیرد.

برای اضافه شدن یک بلاک، باید چهار مرحله زیر، طی شوند:

۱. در مرحله‌ی اول، یک معامله باید انجام شود.

۲. پس از خرید، معامله‌ی باید بررسی و تایید شود. این کار را شبکه‌ای از هزاران رایانه که در سراسر جهان توزیع شده‌اند، انجام می‌دهند و سپس شبکه آن‌ها را بررسی می‌کند.

۳. محل ذخیره هر معامله باید در دل یک بلاک باشد. پس از بررسی و تایید صحت معامله شما، اطلاعات در یک بلاک اختصاصی ثبت و نگهداری می‌شود و در آن‌جا، داده‌های مرتبط با معامله در کنار بی‌شمار تراکنش مشابه، جا می‌گیرد.

۴. به هر بلاک، باید هَش (کد) داده شود: پس از تأیید تمام معامله‌های یک بلاک، باید به آن بلاک یک کد شناسایی منحصر به فردبه نام هَش داده شود. پس از اخذ هش اختصاصی، آن بلاک به شبکه‌ی بلاک چین اضافه می‌شود.

انواع شبکه های بلاک چین

شبکه‌های بلاک چین، بر اساس میزان دسترسی و مشارکت کاربران در شبکه، به چهار دسته تقسیم می‌شوند: شبکه‌های عمومی، خصوصی، تجاری (Consortium) و هیبرید (Hybrid)

شبکه‌های بلاک چین عمومی (Public Blockchain)

این نوع شبکه‌ها برای همگان قابل دسترس هستند و هر فردی می‌تواند به عنوان نود (Node) در شبکه شرکت کند. این نودها مسئول تأیید تراکنش‌ها و تولید بلاک‌های جدید هستند و به عنوان پاداش، رمزارز مربوط به شبکه را دریافت می‌کنند. این شبکه‌ها دارای حداکثر شفافیت و غیرمتمرکزی هستند، اما معایبی مانند کندی، پیچیدگی و مصرف زیاد انرژی را نیز دارند. بیت کوین، اتریوم و لایت کوین مثال‌هایی از این نوع شبکه‌ها هستند.

شبکه‌های بلاک چین خصوصی (Private Blockchain)

این نوع شبکه‌ها توسط سازمان یا گروه خاصی کنترل می‌شوند و فقط اعضای مجاز می‌توانند به آن دسترسی داشته باشند. این شبکه‌ها دارای حداقل شفافیت و حداکثر کارایی هستند، اما معایبی مانند کمبود حفاظت از حقوق کاربران و خطر سانسور را نیز دارند. هایپرلجر فابریک، کوردا و IBM، مثال‌هایی از این نوع شبکه‌ها هستند.

شبکه‌های بلاک چین تجاری (Consortium Blockchain)

این نوع شبکه‌ها توسط چند سازمان یا گروه با هدف همکاری در پروژه یا زمینه‌ای خاص اداره می‌شوند و فقط نودهای منتخب مجاز به تأیید تراکنش‌ها هستند. این شبکه‌ها دارای تعادل مناسب بین شفافیت و کارایی هستند، اما معایبی مانند قطعی نبودن قوانین و استانداردهای شبکه را نیز دارند. بلاک چین R۳، بلاک چین Quorum و اسمارت چین باینانس مثال‌هایی از این شبکه‌ها هستند.

شبکه‌های بلاک چین هیبرید (Hybrid Blockchain)

این نوع شبکه‌ها ترکیبی از شبکه‌های عمومی و خصوصی هستند و امکان انتخاب سطح دسترسی و مشارکت را برای کاربران فراهم می‌کنند. این شبکه‌ها مزایای هر دو نوع شبکه را دارند، اما معایبی مانند پیچیدگی فنی و تطابق نداشتن با قوانین و مقررات نیز آن‌ها را تهدید می‌کند. بلاک چین Dragonchain، بلاک چین XinFin و بلاک چین Kadena مثال‌هایی از این شبکه‌ها هستند.

چرا بلاک چین مهم است؟

فناوری بلاک چین و کاربردهای آن در دنیای مدرن، می‌تواند در صنایع مالی، زنجیرهای تأمین، رایانش ابری و سایر زمینه‌هایی که نیاز به ذخیره‌سازی و انتقال اطلاعات، انقلابی بی‌نظیر ایجاد کند. بلاک چین یک فناوری امنیتی است که برای حل مشکلات اعتماد و شفافیت در بسیاری از زمینه‌ها کاربرد دارد؛ این فناوری به غیر از کاربردی که در تمرکززدایی معاملات مرتبط با ارزهای دیجیتال دارد، در صنایع دیگری نیز کاربرد دارد که در ادامه برخی از آن‌ها را معرفی می‌کنیم.

الگوریتم‌های اجماع در بلاک چین

روش‌های مختلفی برای تأیید صحت تراکنش‌ها و تولید بلاک‌های جدید در شبکه بلاک چین وجود دارند؛ الگوریتم‌های اجماع نقش محوری در حفظ اعتبار و غیرقابل تغییر بودن داده‌های ذخیره شده در بلاک چین ایفا می‌کنند و و جلوی تقلب و تغییر داده‌ها را می‌گیرند؛ برخی از معروف‌ترین این الگوریتم‌های اجماع عبارت‌اند از: اثبات کار (Proof of Work)، اثبات سهام (Proof of Stake)، اثبات مالکیت (Proof of Authority)، اثبات وزن (Proof of Weight)، و اثبات تاریخچه (Proof of History).

اثبات کار (Proof of Work): الگوریتم اثبات کار برای شبکه‌های بلاک چین عمومی مانند بیت کوین و اتریوم استفاده می‌شود. در این الگوریتم، نودهای شبکه که به نام ماینر (Miner) شناخته می‌شوند، باید معمای ریاضی سختی را حل کنند تا بلاک جدید را تولید و به زنجیره اضافه کنند. این معما ریاضی به نام مسئلهٔ سخت (Hard Problem) شناخته می‌شود و نیاز به توان پردازشی زیاد دارد. ماینری که اولین بلاک جدید را تولید کند، پاداشی در قالب رمزارز دریافت می‌کند. این الگوریتم شفاف و غیرقابل تغییر است، اما انرژی زیادی مصرف می‌کند و کند است.

اثبات سهام (Proof of Stake): الگوریتم اثبات سهام برای شبکه‌های بلاک چین عمومی و خصوصی استفاده می‌شود. در این الگوریتم، نودهای شبکه که به نام ولیدیتور (Validator) شناخته می‌شوند، باید چند قسمت از رمزارز خود را به عنوان سپرده، استیک (Stake) کنند تا به عنوان نامزدی برای تولید و تأیید بلاک جدید، شناخته شوند. نامزدهای بلاک جدید با استفاده از الگوریتم‌های تصادفی یا قرعه‌کشی مشخص می‌شوند. نامزدهای بلاک جدید پاداش رمزارز را در قالب هزینه کارمزد (Transaction Fee) دریافت می‌کنند. این الگوریتم کارآیی و امنیت بالایی داشته، اما با مشکلاتی مانند تمرکز سهام و حمله‌های ۵۱ درصد نیز دست و پنجه نرم می‌کند.

تحمل خطای بیزانس (Byzantine Fault Tolerance): این الگوریتم برای شبکه‌های بلاک چین تجاری و خصوصی استفاده می‌شود. در این الگوریتم، نودهای شبکه که به نام تولیدکننده (Producer) شناخته می‌شوند، باید با استفاده از روش‌های رأی‌گیری یا توافق، بلاک جدید را تولید و تأیید کنند. این الگوریتم قادر است خطاها و خیانت‌های احتمالی در شبکه را تحمل کند و به سرعت به توافق برسد؛ سرعت و کارایی بالای داشته، اما معایبی مانند کمبود شفافیت و غیرقابل تغییر بودن را نیز دارد.

بلاک چین چه کاربردهایی دارد؟

فناوری بلاک چین، کاربردهای بی‌شماری دارد. همان طور که گفتیم، در هر بستری که نیاز به ثبت و انتقال اطلاعات یا پیام وجود دارد، می‌توان از بلاک چین استفاده کرد. به طور خلاصه، بلاک چین به عنوان فناوری پایه‌ای، قابلیت اعتماد و شفافیت را در بسیاری از زمینه‌های کاربردی فراهم می‌کند. در ادامه به معرفی دو کاربرد اصلی و مهم بلاک چین می‌پردازیم.

پرداخت‌های بین‌المللی

انتقال پول در سطح بین‌المللی با سیستم بانک‌داری سنتی، دردسرساز است. به دلیل وجود شبکه پیچیده‌ای از واسطه‌ها، استفاده از سیستم بانکی سنتی، انتقال پول، پرهزینه و به کندی انجام می‌شود، اما ارزهای دیجیتال و بلاک چین، این واسطه‌ها را از بین می‌برند و امکان انتقال پول را به شکلی سریع و آسان به سرتاسر جهان فراهم می‌کنند. بسیاری از پروژه‌های بلاک چینی از این فناوری برای انجام تراکنش‌های ارزان و تقریبا سریع و فوری، استفاده می‌کنند؛ البته گاهی اوقات برخی از ویژگی‌های اصلی بلاک چین مثل غیرمتمرکز بودن در آن‌ها نادیده گرفته می‌شود.

بازی‌های کامپیوتری

صنعت بازی‌های کامپیوتری، یکی از صنایع بزرگ در حوزه تفریح و سرگرمی دنیا است که می‌تواند از Blockchain، استفاده کند. در بیشتر بازی‌های کامپیوتری، کاربران مجبورند که قوانین توسعه‌دهندگان بازی را پذیرفته و اجرا کنند و از بستر مشخص شده توسط آن‌ها استفاده کنند. امکان اعمال تغییر و توسعه نیز در بسیاری از آن‌ها برای کاربران وجود ندارد. بلاک چین می‌تواند در زمینه تمرکززدایی از مالکیت، مدیریت و نگهداری بازی‌ها مفید باشد.

با استفاده از قابلیت‌های بلاک چین، بازی‌ها در بلندمدت می‌توانند پایدار بمانند؛ اقلام درون بازی‌ها به عنوان مجموعه‌های رمزنگاری صادر شده، ارزشی واقعی پیدا می‌کنند و در دنیای واقعی خرید و فروش شوند. امروزه بازی‌های پیاده‌سازی‌شده بر پایه‌این فناوری از NFT استفاده می‌کنند و کاربران می‌توانند آیتم‌های داخل بازی را درست کرده و به دیگران بفروشند.

ردیابی لجستیک: بلاک چین قابلیت ردیابی دقیق و مستقل برای محصولاتی مانند مواد غذایی، دارو و کالاهای لوکس را فراهم کرده و به شرکت‌ها کمک می‌کند تا محصولات خود را از مبدا تا مقصد به طور کامل ردیابی کنند.

قراردادهای هوشمند: این فناوری به شرکت‌ها کمک می‌کند تا برای قراردادهای هوشمند، فرایند امضای دیجیتالی، تایید و اجرای خودکار آن‌ها را فراهم کنند. این اقدام باعث افزایش اعتماد بین طرفین قرارداد می‌شود.

امنیت اینترنت اشیاء: بلاک چین امکان استفاده از اینترنت اشیاء برای تبادل اطلاعات و انجام تراکنش‌ها را برای شرکت‌ها فراهم می‌کند. با استفاده از بلاک چین، اطلاعات بین دستگاه‌های مختلف به طور ایمن و بدون واسطه منتقل می‌شود.

احراز هویت: این فناوری به شرکت‌ها کمک می‌کند تا به طور امن هویت کاربران را تایید کرده و از سرقت هویت جلوگیری کنند. برای مثال، اطلاعات شخصی، مانند شماره تلفن، آدرس و اعتبارات مالی در شناسنامه‌های دیجیتالی به صورت ایمن و کاملا خصوصی در بلاک چین ذخیره می‌شوند.

انتخابات الکترونیکی: بلاک چین به عنوان یک فناوری امنیتی می‌تواند به صورت امن و شفاف برای انجام انتخابات الکترونیکی استفاده شود؛ بلاک چین می‌تواند از طریق تضمین شفافیت و امنیت، برای کاهش احتمال تقلب در انتخابات کمک کند.

امنیت اطلاعات بانکی: بلاک چین می‌تواند به شرکت‌های بانکی کمک کند تا از امنیت بیشتری برای اطلاعات و داده‌ها برخوردار شوند. این فناوری می‌تواند از طریق رمزگذاری قوی از سرقت داده‌های حساس، پولشویی و دیگر خطرات امنیتی جلوگیری کند.

شبکه‌های اجتماعی: بلاک چین می‌تواند به امنیت و شفافیت بیشتری را برای شبکه‌های اجتماعی فراهم کند. این فناوری به صورت امن از پروفایل کاربری و پیام‌های ارسالی حفاظت می‌کند.

سیستم ذخیره فایل توزیع شده
در بلاک چین

ذخیره فایل توزیع‌شده در بستر اینترنت، در مقایسه با روش‌های سنتی متمرکز، از مزایای زیادی برخوردار است. بیشتر داده‌های ذخیره شده در فضاهای ابری بر بستر سرویس‌های متمرکز قرار داشته و در معرض حمله و حذف اطلاعات هستند. علاوه‌براین، در برخی مواقع کاربران با خواست مدیران سرورها ممکن است از دسترسی به سرور و اطلاعات خود محروم شوند.

از دیدگاه کاربران، راه‌حل‌های ذخیره‌سازی داده‌ها مبتنی بر بلاک چین، مانند دیگر روش‌های ذخیره‌سازی فایل عمل می‌کند. شما در هر دو این روش‌ها می‌توانید داده‌های خود را آپلود و نگهداری کنید و هر زمان خواستید به آن‌ها دسترسی داشته باشید. اما آنچه در پشت پرده‌ی این دو روش رخ می‌دهد، متفاوت است.

زمانی که فایلی را در بلاک چین ذخیره می‌کنید، فایل شما بین چندین نود، توزیع می‌شود. در برخی مواقع ممکن است هر نود بخشی از فایل شما را ذخیره کند. این نودها نمی‌توانند با داده‌های شما خرابکاری کنند؛ اما شما می‌توانید از نودها برای ارائه قسمت‌های مختلف فایل، درخواست کرده و با ترکیب آن‌ها فایل اصلی خود را بسازید.

این فضا با گرد هم آمدن اشخاصی به وجود می‌آید که فضای ذخیره‌سازی و پهنای باند خود را در اختیار شبکه قرار می‌دهند. به طور معمول، این شرکت‌کنندگان انگیزه اقتصادی برای تامین منابع دارند و اگر از قوانین پیروی نکنند یا در ذخیره و ارائه پرونده‌ها کوتاهی کنند، مجازات می‌شوند.

بلاک چین و کاربردش
در اینترنت اشیاء

در حال حاضر تعداد زیادی از اشیاء فیزیکی به اینترنت متصل هستند و این میزان، هر روز در حال افزایش است؛ ارتباط و همکاری بین این اشیاء به‌طور محسوسی توسط بلاک چین قابل انجام است. برای مثال، پرداخت‌های خودکار ربات به ربات می‌تواند شاخه‌ی جدیدی از اقتصاد را ایجاد کند که برای اجرای آن، راه‌حلی ایمن و با توان بالا نیاز است. بلاک چین به سادگی توانایی توسعه فضای کار اینترنت اشیا را در خود دارد.

پیش‌تر در مقاله‌ی آشنایی با پروژه Fetch.ai و توکن FET درباره‌ی پروژه‌ای که به کمک فناوری هوش مصنوعی، اینترنت اشیا و یادگیری ماشینی را با شبکه بلاک چین ادغام کرده صحبت کردیم؛ این پروژه با توکن FET می‌خواهد سیستمی با مقیاس جهانی را برای اهداف بسیار بلندپروازانه و شگفت‌انگیز خود، ایجاد کند.

سیستم بهداشت و درمان

ذخیره‌سازی امن داده‌های پزشکی برای هر سیستم بهداشت و درمانی، مهم و ضروری است. اتکای سیستم درمان به سرورهای متمرکز، آن را در موقعیت حساس و خطرناکی قرار می‌دهد و امنیت و شفافیتِ فناوری بلاک چین می‌توان پلتفرمی مناسب و کاربردی برای ذخیره داده‌های پزشکی ایجاد کند.

بیماران با داشتن اطلاعات درمانی خود به صورت رمزنگاری‌شده در بلاک چین، می‌توانند همزمان با حفظ حریم خصوصی، اطلاعات پزشکی خود را با هر موسسه درمانی به اشتراک بگذارند. اگر تمامی اعضای سیستم بهداشت و درمان فعلی دنیا در سیستمی جهانی و امن حضور داشته باشند، در این‌صورت، جریان اطلاعات بین آن‌ها سریع‌تر گسترش پیدا می‌کند. این‌کار با استفاده از فناوری بلاک چین قابل انجام است و منجر به بهبود سیستم درمان در دنیا می‌شود.

کاربرد بلاک چین
در چرخه زنجیره تامین

زنجیره تامین کالا، هسته اصلی بسیاری از شرکت‌های موفق است که هدف آن، مدیریت توزیع کالا و خدمات از تولیدکننده به مصرف‌کننده است. هماهنگی ذی‌نفعان متعدد صنعتی خاص، با استفاده از روش‌های سنتی بسیار سخت است.

تکنولوژی بلاک چین می‌تواند سطوح پیشرفته‌تری از شفافیت را در بسیاری از صنایع ایجاد کند. اکوسیستم زنجیره تامین که قابلیت تعامل داشته باشد و حول پایگاه داده‌ای تغییرناپذیر بچرخد، فناوری است که بسیاری از صنایع برای قوی‌تر و قابل اعتمادتر شدن به آن نیاز دارند. بلاک چین دقیقا این نیاز را برطرف می‌کند.

ایجاد شناسنامه دیجیتال

مدیریت امن هویت افراد و موجودیت‌ها در اینترنت، نیازمند راه‌حلی سریع است. مقادیر بسیار زیادی از داده‌های شخصی ما روی سرورهای متمرکز ذخیره می‌شوند؛ این اطلاعات بدون توجه به رضایت ما توسط الگوریتم‌های هوش مصنوعی بررسی می‌شود.

فناوری بلاک چین به کاربران اجازه می‌دهد تا خودشان مالکیت داده‌های خود را در اختیار داشته باشند. در این شبکه‌ها افراد می‌توانند هر اطلاعاتی که خودشان می‌خواهند با بقیه به اشتراک بگذارند و بقیه داده‌ها همچنان خصوصی باقی بماند. این اتفاق را معجزه رمزنگاری می‌نامند که می‌تواند بدون هیچ آسیبی به حریم خصوصی افراد، تجربه‌ای کاربرپسند را برای آن‌ها در فضای آنلاین ایجاد کند؛ با گسترش روزافزون استفاده از شبکه‌های اجتماعی، اهمیت این موضوع بیشتر از همیشه احساس می‌شود.

استفاده از بلاک چین
در امور خیریه

سازمان‌های خیریه اغلب با محدودیت‌هایی در نحوه پذیرش وجوه خیریه روبه‌رو هستند. مهم‌تر از آن، ردیابی دقیق مقصد نهایی وجوه اهدا شده از این سازمان ها دشوار است. همین موضوع باعث می‌شود بسیاری از افراد از این سازمان‌ها حمایت نکنند. رمزنگاری بشردوستانه (Cryptophilanthropy) مفهومی است که از بلاک چین برای دور زدن این محدودیت‌ها استفاده می‌کند. این حوزه با تکیه بر فناوری بلاک چین به دنبال شفافیت بیشتر، مشارکت جهانی و کاهش هزینه‌ها است؛ رمزنگاری بشر دوستانه در حال توسعه و گسترش در سطح جهانی است.

ساختار غیرمتمرکز
بلاک چین چیست؟

تا به اینجا ساختار بلاک چین را به عنوان پایگاه داده بررسی کردیم و دیدیم که داده‌ها در این ساختار، زنجیروار به یکدیگر متصل هستند. اگر بلاک چین را تنها پایگاه داده‌ای مستقل در نظر بگیریم، آنگاه فقط در برخی از اپلیکیشن‌های کاربردی استفاده خواهد شد، اما بلاک چین‌ها ابزاری برای هماهنگی افراد مختلف هم هستند.

در این حالت بلاک چین می‌تواند با استفاده از نظریه بازی (Game Theory) و سایر فناوری‌ها، به عنوان دفتر کل توزیع شده (Distributed Ledger) عمل کند که توسط هیچ نهادی کنترل نمی‌شود. بنابراین می‌توان اینطور در نظر گرفت که دفتر کل به طور هم‌زمان متعلق به تمام افراد است و برای هر تغییری در آن باید اکثریت به توافق برسند.

گستردگی شبکه: Blockchain نیز مانند تمام سامانه‌های توزیع شده با حملات مقابله کرده و به مرور زمان رشد می‌کند و برای این کار به شبکه‌ی بزرگی از کاربران نیاز دارد. البته بحث‌هایی هم پیرامون این موضوع وجود دارد و برخی معتقدند که چنین وسعتی برای بلاک چین‌ها می‌تواند بسیار مهلک باشد، در نتیجه تعیین اندازه‌ی مناسب و نگهداری از آن از بسیار مهم و چالش‌آفرین است.

هزینه تراکنش‌ها: تبادلات بیت کوین که در چند سال اول حضورش به‌طور تقریبی رایگان اعلام شد، اکنون هزینه‌های قابل توجهی دارد.

نقص امنیتی غیرقابل اجتناب: در بیت کوین و سایر بلاک چین‌ها یک نقص امنیتی قابل توجه وجود دارد؛ اگر بیش از نیمی از رایانه‌هایی که به عنوان نود در شبکه فعالیت می‌کنند دروغ بگویند (دقت داشته باشید بیش از نیمی از رایانه‌ها)، دروغ به حقیقت تبدیل می‌شود. این نقص حمله ۵۱ درصد نامیده می‌شود و به همین دلیل استخرهای استخراج بیت کوین توسط جمع به دقت مورد نظارت قرار می‌گیرد تا اطمینان حاصل شود که ناآگاهانه چنین نفوذی در شبکه اتفاق نیافتد.

خطای انسانی: اگر بلاک چین به عنوان پایگاه داده استفاده شود، داده‌هایی که در آن ذخیره می‌شوند باید از کیفیت بالایی برخوردار باشند. داده‌های ذخیره شده در بلاک چین به صورت ذاتی قابل‌اعتماد نیستند؛ بنابراین داده‌ها باید به شکلی دقیق در آن وارد شوند. سامانه‌های Blockchain از اصل ورودی زباله، خروجی زباله (GIGO) پشتیبانی کرده و اگر داده‌های ورودی اشتباه یا نامعتبر باشند، خروجی نیز نامعتبر معرفی خواهد شد.

قطع ارتباط شبکه بلاک چین و اصل غیرمتمرکز بودن

حال سوالی که ممکن است برای خیلی از ما پیش بیاید این است که تناقض بین قطع ارتباط شبکه بلاک چینی با کاربر، با اصل غیرمتمرکز بودن بلاک چین و متکی نبودن آن به چند سرور، چگونه قابل توجیه است؟

اصل غیرمتمرکز بودن بلاک چین، به این معنا است که هیچ نهاد یا سازمانی کنترل شبکه را در دست ندارد. در شبکه، هر شخصی می‌تواند گره یا همان نود را راه‌اندازی کند و به شبکه متصل شود. این امر باعث می‌شود که شبکه بلاک چین در برابر سانسور و دستکاری مقاوم باشد.

غیرمتمرکز بودن شبکه به این معنا نیست که شبکه در برابر قطع ارتباط ایمن است؛ این قطع ارتباط شبکه بلاک چین با کاربر ممکن است به دلایل مختلفی رخ دهد:

- **خطای نرم‌افزاری:** خطای نرم‌افزاری در یکی از اجزای شبکه بلاک چین می‌تواند باعث قطع شدن شبکه شود.
- **حملات سایبری:** حملات سایبری به شبکه Blockchain می‌تواند باعث از کار افتادن شبکه شود.
- **نقص سخت‌افزاری:** نقص سخت‌افزاری در یکی از اجزای شبکه بلاک چین قطع شدن ارتباط شبکه با کاربر را منجر شود.

در هر شبکه بلاک چینی، هر گره یک کپی از کل Blockchain را در اختیار دارد. بنابراین، اگر گره‌ای از شبکه جدا شود، همچنان می‌تواند به تراکنش‌های خود ادامه دهد. با این حال، اگر تعداد زیادی از گره‌ها از شبکه جدا شوند، شبکه ممکن است به طور کامل از کار بیفتد.

برای جلوگیری از قطع شدن شبکه بلاک چینی، توسعه‌دهندگان این شبکه‌ها باید اقدامات لازم را برای شناسایی و رفع خطاهای نرم‌افزاری و سخت‌افزاری انجام دهند. همچنین، شبکه‌های بلاک چینی باید از حملات سایبری محافظت شوند.

پس غیرمتمرکز بودن شبکه بلاک چینی و متکی نبودن آن به چند سرور، قطع نشدن شبکه را تضمین نمی‌کند و لزوما این دو موضوع ربطی به هم ندارند.

انواع بلاک چین چیست؟

همان‌طور که تا اینجا اشاره کردیم، Blockchain فناوری امنیتی است که اطلاعات را در قالب بلاک‌هایی ذخیره و به صورت پایدار و بدون نیاز به واسطه‌ای در شبکه انتقال می‌دهد. انواع مختلفی از بلاک چین وجود دارند که در زیر به برخی از آن‌ها اشاره می‌کنیم.

بلاک چین
عمومی ضد انحصاری

اغلب شما بدون اینکه بلاک چین عمومی ضد انحصاری را بشناسید، با مفهوم آن آشنا هستید؛ در این نوع Blockchain، ما انحصار تراکنش‌ها را در اختیار نداریم: بیت کوین، اتریوم، لایت کوین و انواع سیستم‌های عمومی و آزاد مبتنی بر بلاک چین، نمونه‌هایی از این نوع هستند.

برای مثال فرض کنید، می‌خواهیم ۵ بیت کوین ارسال کنیم و این موضوع را به افراد فعال در شبکه یا همان ماینرها اعلام می‌کنیم. اما آیا من واقعاً ۵ بیت کوین دارم؟ ادعای دروغ نیست؟ نمی‌خواهم تقلب کنم؟ افراد فعال در شبکه بیت کوین پیغام من را می‌شنوند و روند تأیید معامله را شروع می‌کنند. فردی که تراکنش را تأیید می‌کند، انتخابی نیست و ما نمی‌توانیم تأییدکننده را تعیین کنیم. به این نوع بلاک چین، عمومی ضد انحصاری می‌گویند و زمانی از آن استفاده می‌شود که نظر تمام جامعه مهم باشد، نه فقط چند فرد خاص!

در این بلاک چین هر فرد می‌تواند قراردادهای هوشمند ایجاد کرده یا پول و داده‌ها را منتقل کند؛ اطلاعات مهم در این بلاک چین‌ها به صورت رمزنگاری شده قابل ذخیره‌سازی هستند.

بلاک چین
عمومی انحصاری

در Blockchain عمومی انحصاری افرادی خاص برای تأیید فعالیت‌ها انتخاب می‌شود. این افراد می‌توانند کارمندی ارشد، کارکنان دولت، موسسه یا اشخاص دیگری باشند. در این نوع از بلاک چین داده‌ها قابل مشاهده برای عموم هستند اما می‌توان از یک سری اطلاعات خاص محافظت کرد.

برای مثال فرض کنید فردی پرورشگاه ماهی دارد و می‌خواهد زنجیره تأمین پرورشگاهش را برای عموم شفاف‌سازی کند. او می‌خواهد مردم بدانند که ماهی خریداری شده، صیدِ کجا بوده یا چه زمانی بسته‌بندی شده است و هم‌زمان از باقی اطلاعات خود نیز محافظت کند. برای این کار، کافی است تا روی ماهی‌هایش کد QR قرار دهد و مشتریان نیز می‌توانند با اسکن این کد، از اطلاعات آن آگاه شوند. مشتریان تنها می‌توانند اطلاعات به اشتراک گذاشته شده را مشاهده کنند و نه بیشتر!

بلاک چین
خصوصی انحصاری

بلاک چین خصوصی انحصاری می‌تواند برای نهادهای مختلف خصوصی و دولتی استفاده شود. در آن، افرادی خاص برای تایید فعالیت‌ها انتخاب می‌شوند و تنها افرادی خاص امکان مشاهده اطلاعات ثبت شده را دارند.

سیستم‌های پرداخت حقوق با بلاک چین یکی از مثال‌های کاربردی Blockchain خصوصی انحصاری است؛ فرض کنید کسب‌وکار رضا به دو شرکت کوچک و یک شرکت حسابداری دیگر مرتبط است. آن‌ها به طور منظم با یکدیگر همکاری می‌کنند و رضا می‌خواهد اعتمادی کامل بین طرفین برقرار شود، اما نمی‌خواهد به جز سران شرکت، فرد دیگری اطلاعات را دستکاری کند یا بخواند. بهترین گزینه برای پیشبرد این هدف استفاده از نوع سوم بلاک چین است.

بلاک چین در آینده

بلاک چین طی پروژه‌ای تحقیقاتی در سال ۱۹۹۱ معرفی شد و حالا کم‌کم به اواخر دههٔ دوم زندگی‌اش نزدیک می‌شود. مانند بسیاری از تکنولوژی‌های جدید دیگر، در طی این دو دهه، بررسی‌های موشکافانه‌ی روی این فناوری انجام شده و افراد زیادی درباره‌ی ظرفیت‌های این تکنولوژی و مسیر آینده‌ی آن تحقیق می‌کنند. بلاک چین به کلمه‌ای تبدیل شده که همه در دنیا در مورد آن صحبت می‌کنند و می‌تواند کسب‌وکارها و عملیات‌های دولتی را دقیق‌تر، بهینه‌تر و امن‌تر بهینه‌سازی کند.

در حالی که آماده‌ی ورود به دهه‌ی سوم زندگی بلاک چین می‌شویم، دیگر این سؤال مطرح نیست که «آیا کمپانی‌های افسانه‌ای از این تکنولوژی استفاده خواهند کرد یا خیر؟» بلکه این سؤال مطرح است که «آن‌ها چه زمانی از این فناوری بهره خواهند برد؟»

گفتار پایانی

بلاک چین، فناوری نوینی به شمار می‌رود که هدف از ایجاد آن ذخیره‌سازی و انتقال هر نوع داده به صورت غیرمتمرکز است. در این سیستم نودها وظیفه تایید و ثبت تراکنش‌ها را دارند، هرکدام از این نودها در سراسر دنیا توزیع شده و برای انجام درست وظایف خود، از الگوریتم‌های اجماع استفاده می‌کنند.

امنیت شبکه بلاک چین حاصل استفاده از ایده‌های مبتکرانه در حوزه رمزنگاری و اقتصاد است و ما هم در این مقاله سعی کردیم تا علاوه بر بررسی تمام جنبه‌های فنی و عملی آن، کاربردهای بلاک چین در حوزه‌های مختلف را توضیح دهیم.