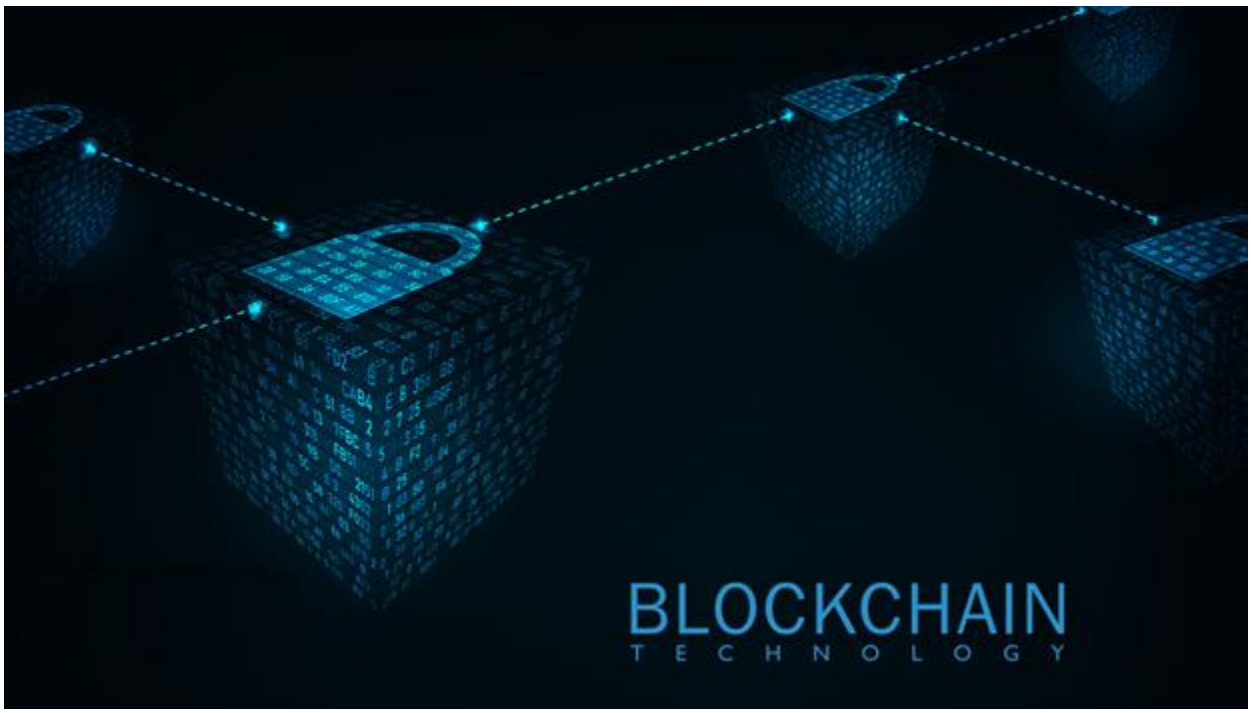
فناوری بلاک چین چیست؟



اصطلاح بلاک چین (Blockchain) در حالت لغوی به‌معنای زنجیره‌ای از بلاک‌هاست .

فناوری بلاک چین مفهومی نسبتاً جدید است که امکان ثبت داده‌ها در فضایی به‌نام بلاک و سپس اتصال این بلاک‌ها به هم مانند یک زنجیره را فراهم می‌کند. همین اتصال زنجیروار بلاک‌ها به هم امنیت داده‌ها را تضمین می‌کند و امکان تغییر آن‌ها را به حداقل می‌رساند.

فناوری بلاک چین بی‌تردید یکی از بزرگ‌ترین نوآوری‌های قرن بیست‌ویکم است. باتوجه‌به تأثیر موجی بلاک چین روی بخش‌ها و صنایع مختلف، از امور مالی گرفته تا زنجیره تأمین و حتی آموزش و پرورش، آشنایی با این فناوری و نحوه به‌کارگیری مؤثر آن، از اهمیت بسیار زیادی

برخوردار است .کاربردهای فناوری بلاک چین در دنیای واقعی، آن‌قدر زیاد و جذاب است که نمی‌توان آن را نادیده گرفت.

بلاک چین چیست؟

بلاک چین (blockchain) یک دفتر کل توزیع شده دیجیتال غیرمتمرکز و عمومی است که انواع داده‌ها و اطلاعات را در خود ذخیره می‌کند. شاید فکر کنید هر پایگاه داده دیگری هم قادر است چنین کاری را انجام دهد؛ پس بلاک چین چه تفاوتی با سایر پایگاه‌های داده دارد؟

تفاوت اصلی بلاک چین با هر پایگاه داده دیگری این است که کاملاً غیرمتمرکز عمل می‌کند؛ یعنی داده‌ها را مانند بانک در یک صفحه اکسل یا سرورهای مرکزی ذخیره نمی‌کند؛ بلکه نسخه‌های بسیار زیادی از آن‌ها را بین شبکه‌ای از رایانه‌ها توزیع می‌کند. به همین دلیل، نیازی به یک قدرت متمرکز برای مدیریت پایگاه داده خود ندارد.

به‌کمک بلاک چین می‌توان به‌صورت دائمی، تغییرناپذیر و شفاف، همه داده‌ها و تراکنش‌ها را ثبت کرد. هرچیزی که دارای ارزش است، خواه کالای فیزیکی باشد یا غیرفیزیکی، در این شبکه مبادله‌شدنی است. بعد از ثبت اطلاعات در بلاک چین، هرگز نمی‌توان چیزی را در آن تغییر داد.

ویژگی‌های اصلی بلاک چین

فناوری بلاک چین دارای شش ویژگی اصلی است:

۱ .تغییرناپذیری و شفافیت

مکانیسم بلاک چین طوری است که وقتی بلاک‌های جدید به دفتر کل اضافه می‌شوند، دیگر کسی نمی‌تواند به عقب برگردد و آن را دستکاری، حذف یا ویرایش کند.

۲ .غیرمتمرکز بودن

بلاک چین هیچ مرجع یا نهاد واحدی ندارد که آن را کنترل کند. گروهی متشکل از رایانه‌ها که به آن‌ها نود (Node) می‌گویند شبکه را مدیریت می‌کنند. می‌توانیم هرچیزی از ارز دیجیتال گرفته

تا اسناد مهم و قراردادها را در آن ذخیره کنیم و با استفاده از کلید خصوصی مستقیماً به آن‌ها دسترسی داشته باشیم.

۳ .امنیت پیشرفته

همین که بلاک چین نیازی به مرجع مرکزی ندارد، امنیت آن را تضمین می‌کند. زیرا هیچ قدرتی نمی‌تواند به‌میل خود ویژگی‌های شبکه را تغییر دهد. بااین‌حال، استفاده از رمزنگاری در این سیستم هم لایه امنیتی دیگری به آن اضافه می‌کند.

سیستم امنیتی بلاک چین از نوع «دو کلید» است. تمام اطلاعات موجود در بلاک چین رمزنگاری شده‌اند و ماهیت واقعی داده‌ها پنهان است. با کلید عمومی که فقط یک آدرس شامل رشته‌ای از حروف و اعداد است تراکنش‌ها را انجام می‌دهید و برای دسترسی به داده‌ها از کلید خصوصی استفاده می‌کنید.

۴ .دفتر کل توزیع‌شده

بلاک چین دفتر کل عمومی است که اطلاعاتی درباره تراکنش‌ها ارائه می‌دهد .همه‌چیز در فضای باز قرار دارد و چیزی از کسی پنهان نمی‌ماند. همه مشارکت‌کنندگان در شبکه، این دفتر کل را ذخیره می‌کنند و می‌دانند در آن چه می‌گذرد.

۵ .مکانیسم اجماع

هر بلاک چین شامل الگوریتم اجماع است. به‌زبان ساده، اجماع نوعی فرایند تصمیم‌گیری برای گروهی از نودهای فعال در شبکه است که درست مانند سیستم رأی‌گیری، اکثریت پیروز می‌شود و اقلیت باید از آن حمایت کند.

الگوریتم‌های اجماع متفاوتی وجود دارد که مهم‌ترین آن‌ها، اثبات کار (PoW) و اثبات سهام (PoS)هستند. به‌خاطر اجماع است که در شبکه بلاک چین، نیازی نیست نودها به هم اعتماد داشته باشند. اجماع تضمین می‌کند که اکثریت با تصمیمِ گرفته‌شده موافق‌اند و این خودش اعتماد ایجاد می‌کند.

۶ .سرعت در تسویه واریزها

در سیستم سنتی، برخی نقل و انتقالات بانکی ممکن است حتی چند روز طول بکشد یا سیستم خراب شود. بلاک چین در مقایسه با سیستم‌های بانک‌داری سنتی برای تسویه واریزها، سریع‌تر است. مخصوصاً واریزهای برون‌مرزی برای کارگران خارج از کشور که باید برای خانواده‌شان پول ارسال کنند، با بلاک چین بسیار سریع‌تر انجام می‌شود.

کارمزد آن‌ها هم بسیار کمتر از بانک‌های سنتی است.

تاریخچه بلاک چین

یک باور رایج نادرست درباره بلاک چین این است که این فناوری در سال ۲۰۰۸ ابداع شده است. درحالی‌که تاریخچه بلاک چین به سال ۱۹۹۱ برمی‌گردد. در آن زمان، استوارت هابر (Stuart Haber) و دبلیو اسکات استورنتا (W. Scott Stornetta) چیزی را که امروز به‌عنوان فناوری بلاک چین می‌شناسیم، در رویای خود می‌دیدند.

اولین کاری که آن‌ها انجام دادند، تلاش برای ایجاد زنجیره‌ای از بلاک‌های امن رمزنگاری‌شده بود؛ به‌طوری‌که هیچ‌کس نتواند برچسب زمانی اسناد موجود در آن را دستکاری کند. یک‌سال بعد، آن‌ها سیستم خود را ارتقا دادند و درخت مرکل را در آن گنجاندند. این کار باعث شد کارایی شبکه افزایش یابد و در نتیجه، امکان جمع‌آوری اسناد بیشتر در یک بلاک فراهم شود.

با همه این اوصاف، تاریخچه بلاک چین از سال ۲۰۰۸ به بعد اهمیت واقعی خود را پیدا می‌کند. زمانی‌که فرد یا گروهی ناشناس به‌نام ساتوشی ناکاموتو وارد عمل شدند.

ساتوشی ناکاموتو مغز متفکر پشت فناوری بلاک چین است. هنوز هیچ‌کس چیز زیادی درباره ساتوشی نمی‌داند. او کسی بود که بیت کوین را به جهان معرفی کرد؛ پادشاه ارزهای دیجیتال که اولین کاربرد فناوری بلاک چین است.

ساتوشی در سال ۲۰۰۹، وایت پیپری درباره بلاکچین منتشر کرد و در آن، جزئیاتی درباره این‌که چطور این فناوری به‌خوبی برای افزایش اعتماد دیجیتال تجهیز شده است ارائه داد.

ساتوشی توضیح داد که غیرمتمرکز بودن بلاک چین بدان معناست که هیچ‌کس هرگز بر چیزی کنترل نخواهد داشت.

اززمانی‌که ساتوشی ناکاموتو از صحنه خارج شد و توسعه بیت کوین را به دیگر توسعه‌دهندگان اصلی سپرد، بلاک چین همچنان تکامل یافته است.

سیر تکاملی بلاک چین به این صورت است:

فاز یک، تراکنش‌ها

فاز اول blockchain و ظهور بیت کوین؛ از ۲۰۰۸ تا ۲۰۱۳

بیشتر افراد تصور می‌کنند بیت کوین و بلاک چین یکی هستند. این در حالی است که بلاک چین در اصل یک فناوری زیربنایی است و ارزهای دیجیتال مانند بیت کوین روی آن ایجاد می‌شوند.

بیت کوین در سال ۲۰۰۸ متولد شد و اولین کاربرد فناوری بلاک چین بود. ساتوشی ناکاموتو در وایت پیپر خود از آن به‌عنوان «سیستم الکترونیکی همتا به همتا» یاد کرد. او ابتدا بلاک جنسیس را تشکیل داد و سپس سایر بلاک‌ها را از آن استخراج و به یکدیگر متصل کرد .به این ترتیب، یکی از بزرگترین زنجیره‌های بلوکی تشکیل شد که حاوی اطلاعات و تراکنش‌ها است.

فاز دو، قراردادها

فاز دوم blockchain و توسعه اتریوم؛ از سال ۲۰۱۳ تا ۲۰۱۵

در آن زمان، یکی از توسعه‌دهندگانی که احساس می‌کردند بیت کوین هنوز به پتانسیل کامل خود نرسیده است، ویتالیک بوترین، نابغه کانادایی‌روسی علوم رایانه بود. بوترین به‌خاطر محدودیت‌های بیت کوین، روی چیزی که آن را نوعی بلاک چین انعطاف‌پذیر می‌دانست، کار کرد .بلاک چینی که می‌توانست علاوه بر اینکه یک شبکه همتا به همتا باشد، کارهای مختلفی هم انجام دهد.

اتریوم در سال ۲۰۱۳، به‌عنوان یک بلاک چین عمومی جدید با عملکردهای بیشتر درمقایسه‌با بیت کوین متولد شد؛ نوآوری بزرگی که آن را نقطه‌عطف تاریخ بلاک چین می‌دانند.

بوترین با فعال‌کردن عملکردی که به افراد اجازه می‌دهد سایر دارایی‌ها نظیر قراردادها را هم در بلاک چین ثبت کنند، اتریوم را از بلاک چین بیت کوین متمایز کرد. این ویژگی جدید، قابلیت‌های اتریوم را از یک ارز دیجیتالِ صرف، به پلتفرمی برای توسعه برنامه‌های غیرمتمرکز گسترش داد.

فاز ۳، برنامه‌های کاربردی غیرمتمرکز

فاز سوم blockchain و آینده؛ سال ۲۰۱۸

تاریخچه تکامل بلاک چین با اتریوم و بیت کوین متوقف نمی‌شود. در سال‌های اخیر، تعدادی از پروژه‌ها همه قابلیت‌های فناوری بلاک چین را به کار گرفته‌اند .پروژه‌های جدید علاوه بر ارائه ویژگی‌های نو با استفاده از قابلیت‌های بلاک چین، به‌دنبال رفع برخی از کمبودهای بیت کوین و اتریوم هستند.

نئو (NEO)، یکی از این برنامه‌های کاربردی است که به‌عنوان اولین پلتفرم بلاک چینی منبع باز و غیرمتمرکز راه‌اندازی شد. بعد از آن آیوتا (IOTA) بود که در آن، برخی از توسعه‌دهندگان در رقابت برای سرعت‌بخشیدن به توسعه اینترنت اشیا، به گونه‌ای مناسب از فناوری بلاک چین استفاده کردند.

علاوه بر این دو، پلتفرم‌های بلاک چینی دیگری نظیر زی‌کش، مونرو و دش هم به‌عنوان راهی برای رسیدگی به پاره‌ای از مشکلات امنیتی و مقیاس‌پذیری مرتبط به برنامه‌های بلاک چین ۱.۰ به وجود آمدند. این سه پلتفرم که آلت‌کوین‌های حریم خصوصی نامیده می‌شوند، قصد دارند سطوح بالایی از حریم خصوصی و امنیت در هنگام اجرای تراکنش را ارائه دهند.

بلاک چین چگونه کار می‌کند؟

برای درک عملکرد بلاک چین، باید ابتدا با سه مفهوم اصلی یعنی بلاک، نود و ماینر و نیز مفاهیم وابسته به آن‌ها، یعنی تابع هش، نانس و الگوریتم اجماع آشنا شویم. بیایید با مثال پیش برویم که درک سازوکار آن‌ها ساده‌تر شود.

فرض کنیم ۱۰ نفر با هم تصمیم گرفته‌اند یک ارز دیجیتال جدید بسازند. آن‌ها باید جریان وجوه را پیگیری کنند تا از اعتبار کوین‌ها در اکوسیستم پولی خود اطمینان داشته باشند. یکی از آن‌ها که او را باب می‌نامیم، تصمیم می‌گیرد فهرستی از همه اقدامات را در یک دفتر به‌صورت صفحه اکسل درج کند. شخص دیگری که او را جک می‌نامیم، تصمیم دارد پول‌ها را بدزدد. او توانست مقداری پول سرقت کند و برای پنهان‌کردن آن، ورودی‌های دفتر را تغییر داد.

تابع هش یا تابع درهم‌سازی

مدتی بعد، باب متوجه می‌شود شخصی دفتر او را تغییر داده است. برای جلوگیری از این دستکاری در آینده، او فرمت دفتر را تغییر می‌دهد. برای این کار از تابع هش استفاده می‌کند که متن دفتر را به مجموعه‌ای از حروف و اعداد تبدیل می‌کند. چگونه؟

این فرایند از یک الگوریتم هش ایمن (SHA) استفاده می‌کند که ورودی‌های با مقادیر متغیر را دریافت کرده و به خروجی رمزگذاری‌شده با طول ثابت تبدیل می‌کند. این خروجی هش (hash) نامیده می‌شود. یک تغییر کوچک در یک رشته، هش کاملاً جدیدی تولید می‌کند. باب بعد از ثبت

هر تراکنش در دفتر، یک هش درج می‌کرد. اما جک توانست سابقه را تغییر دهد و هش جدیدی تولید کند بدون این‌که آب از آب تکان بخورد.

باب دوباره متوجه می‌شود. برای پیچیده‌تر کردن فرایند، بعد از هر ثبت، یک هش جدید از آخرین هش ثبت‌شده به آن اضافه می‌کند. حالا هر ورودی به ورودی قبل از خودش بستگی دارد. بنابراین اگر جک بخواهد در دفتر تغییر ایجاد کند، باید هش همه ورودی‌های قبلی را تغییر دهد. جک دزد مصممی بود، بنابراین وقت گذاشت و همه هش‌ها را یکی‌یکی تغییر داد!

نانس یا عدد تصادفی

باب تسلیم نشد. این بار بعد از هر ثبت، یک عدد تصادفی با عنوان نانس (nonce) به داده‌ها اضافه کرد. این عدد باید به‌گونه‌ای انتخاب می‌شد که هش تولیدشده حتماً به دو صفر ختم شود. برای جعل سوابق دفتر، حالا جک باید ساعت‌ها صرف پیداکردن نانس برای هر خط می‌کرد. یافتن نانس‌ها حتی برای سریع‌ترین رایانه‌ها هم دشوار است.

نود یا گره

باب برای مدت کوتاهی می‌توانست تراکنش‌ها را به این شکل ثبت کند. بعد از مدتی، با انجام تراکنش‌های جدید، او تحت‌فشار قرار گرفت و سیستم فعلی را ناپایدار دید. بنابراین دفتر خود را در اختیار ۳۰۰۰ رایانه در سراسر جهان قرار داد. این رایانه‌ها همان نودها هستند.

هربار که تراکنشی ثبت می‌شود، آن نودها آن را اعتبارسنجی می‌کنند و نیازی نیست باب به‌تنهایی این کار را انجام دهد. وقتی اکثر نودها تراکنش را معتبر اعلام می‌کنند، آن را به یک مجموعه به نام بلاک می‌افزایند. حال اگر جک بخواهد یک ورودی را در دفتر تغییر دهد، همه نودهای دیگر هش اصلی را دارند و اجازه این کار را نخواهند داد.

بلاک

واژه بلاک چین از دو جزء بلاک (block) و زنجیره (chain) ساخته شده است. بنابراین هر زنجیره بلاک چینی از چندین بلاک متصل به هم تشکیل می‌شود. هر بلاک دارای سه مؤلفه اصلی است:

- داده‌های درون بلاک شامل برچسب زمانی و اطلاعات مربوط به تراکنش‌ها
- نانس (Nonce) یا عدد تصادفی
- هش.

نودها بعد از تأیید هر تراکنش آن را به یک بلاک اضافه می‌کنند. هر بلاک تا جایی که ظرفیت دارد (۱ مگابایت) با تراکنش‌های جدید پر می‌شود. وقتی یک بلاک پر شد، به بلاک چین اضافه می‌شود و نودها کار روی بلاک بعدی را آغاز خواهند کرد.

این بلاک چین هر ۱۰ دقیقه یک‌بار با یک بلاک جدید به‌روز می‌شود و این به‌روزرسانی کاملاً خودکار است و همزمان در همه رایانه‌های موجود در شبکه انجام می‌شود. به‌محض به‌روزشدن بلاک چین، دیگر نمی‌توان آن را تغییر داد. هر تغییر در بلاک چین، مستلزم اجماع اکثریت شرکت‌کنندگان در شبکه است.

ماینر یا استخراج‌کننده

به فرایندی که در آن بلاک‌ها به زنجیره اضافه می‌شوند، ماینینگ و به نودهایی که این کار را انجام می‌دهند، ماینر می‌گوییم.

در شبکه‌های بلاک چینی که از اجماع اثبات کار استفاده می‌کنند، یک ماینر باید ثابت کند در حال انجام محاسبات و مصرف انرژی لازم برای استخراج بلاک است .ازآنجاکه هر بلاک حاوی نانس و هش منحصربه‌فرد خود است ولی به هش بلاک قبلی هم اشاره دارد، استخراج یک بلاک مخصوصاً در زنجیره‌های بزرگ دشوار خواهد بود. بنابراین، ماینرها باید از نرم‌افزارهای تخصصی برای حل مسئله ریاضی دشوارِ تولید هش قابل‌قبول با استفاده از نانس استفاده کنند.

ازآنجاکه نانس ۳۲ بیت است و هش ۲۵۶ بیت، حدود چهار میلیارد ترکیب نانس‌هش وجود دارد که باید بررسی شود تا ترکیب طلایی پیدا شود. این کار با دستگاه‌های ماینینگ بسیار سریع و قدرتمند محاسباتی نظیر ماینرهای ای‌سیک(ASIC) ، امکان‌پذیر است.

ماینرها برای یافتن این ترکیب با هم رقابت می‌کنند و وقتی پیدا کردند، بلاک خود را به زنجیره اضافه می‌کنند. هر ماینری که زودتر از دیگران موفق به انجام کار شود، ماینرهای دیگر آن را تأیید می‌کنند و پاداش بلاک به ماینر تعلق می‌گیرد.

در الگوریتم اثبات سهام، دیگر اثبات کار و استخراج وجود ندارد و ماینرها فقط تراکنش‌ها را اعتبارسنجی می‌کنند. برای اثبات درستکاری خود، آن‌ها باید مبلغ مشخصی را در شبکه به‌عنوان وثیقه قفل کرده و به‌اصطلاح استیک کنند.

نمونه هایی از پروتکل های پیاده شده در بلاک چین

مثال اول

مثال دوم

مثال سوم

فناوری بلاک چین شامل مجموعه بزرگی از قوانین است که پروتکل‌های آن نامیده می‌شوند. برای مثال:

- اطلاعات ورودی برای هر هش باید شامل هش بلاک قبلی باشد.
- در بلاک چین بیت کوین، پس از استخراج هر ۲۱۰،۰۰۰ بلاک که چهار سال طول می‌کشد، پاداش استخراج بلاک باید به نصف کاهش یابد. این رویداد هاوینگ نامیده می‌شود.
- برای حفظ زمان استخراج درحدود ۱۰ دقیقه، سختی استخراج هر ۲۰۱۶ بلاک مجدداً محاسبه می‌شود. با کاهش و افزایش میزان سختی، شبکه تعادل را حفظ می‌کند. هرچه تعداد ماینرها بیشتر باشد، فضا رقابتی‌تر است و استخراج بلاک‌ها دشوارتر. وقتی ماینرها کمتر هستند، یعنی استخراج بلاک‌ها نسبتاً آسان‌تر است و ماینرها را به مشارکت ترغیب می‌کند.

مزایای فناوری بلاک چین

پتانسیل بلاک چین با تمام پیچیدگی‌هایی که دارد، به‌عنوان شکلی غیرمتمرکز از ثبت سوابق تقریباً بدون محدودیت است. برخی از مزایای این فناوری عبارت‌اند از:

افزایش دقت با حذف دخالت انسان در فرایند راستی‌آزمایی

برای تأیید تراکنش‌های شبکه بلاک چین، هزاران رایانه و دستگاه در شبکه مشارکت می‌کنند. بنابراین چیزی به‌صورت دستی انجام نمی‌شود و این به‌نوبه‌خود، خطای انسانی را کاهش می‌دهد. درنتیجه، اطلاعات دقیق‌تر ثبت می‌شوند. حتی اگر رایانه‌ای در شبکه یک اشتباه محاسباتی انجام دهد، این خطا فقط در یک نسخه از بلاک چین وجود خواهد داشت و شبکه آن را رد خواهد کرد.

کاهش هزینه با حذف واسطه‌های شخص ثالث

حتماً می‌دانید که برای انجام تراکنش‌های بانکی یا امضای یک سند در دفتر اسناد رسمی، باید هزینه‌های مختلفی پرداخت کنید. صاحبان مشاغل وقتی در دستگاه کارت‌خوان کارت می‌کشند، برای هر تراکنش باید کارمزد بپردازند؛ زیرا این تراکنش‌ها را بانک‌ها و شرکت‌های پرداخت به‌عنوان شخص ثالث پردازش می‌کنند .این در حالی است که با بلاک چین، هیچ واسطه و شخص ثالثی وجود ندارد و فقط یک کارمزد پرداخت می‌شود.

تمرکز زدایی و دشواری دستکاری

بلاک چین هیچ یک از اطلاعات خود را در یک مکان مرکزی ذخیره نمی‌کند. در عوض، نسخه‌هایی از آن بین همه رایانه‌های موجود در شبکه توزیع می‌شود. هرزمان که یک بلاک جدید به بلاک چین اضافه می‌شود، این نسخه به‌روز شده، به‌شکل همزمان در اختیار همه رایانه‌های موجود در شبکه قرار می‌گیرد. با انتشار اطلاعات در شبکه به‌جای یک پایگاه داده مرکزی، دستکاری بلاک چین دشوارتر می‌شود.

تراکنش‌های کارآمد، خصوصی و امن

اگر قبلاً تراکنش‌های بین بانکی یا برون‌مرزی انجام داده باشید، می‌دانید که گاهی بسته به نوع واریز، ممکن است چند روزی طول بکشد تا پول در حساب گیرنده بنشیند. گاهی تسویه چکی که چهارشنبه واریز شده است، به بعد از تعطیلات و روز شنبه موکول می‌شود. این در حالی است که بلاک چین ۳۶۵ روز سال و در تمام روزهای هفته به‌صورت ۲۴ساعته فعال است.

تراکنش‌ها در برخی از بلاک چین‌ها در عرض چند دقیقه تکمیل می‌شوند؛ مخصوصاً برای معاملات برون مرزی، بلاک چین بسیار کارآمدتر از بانک‌هاست.

بسیاری از شبکه‌های بلاک چین به‌عنوان پایگاه‌های داده عمومی عمل می‌کنند، بدین معنا که هرکسی با اتصال به اینترنت می‌تواند فهرستی از تاریخچه تراکنش‌های شبکه را مشاهده کند . بااین‌حال این جزئیات شامل اطلاعات مربوط به شناسایی کاربرانی که آن تراکنش را انجام داده‌اند

نمی‌شود. فقط یک آدرس قابل‌مشاهده وجود دارد و بنابراین هویت افراد و تراکنش‌های آن‌ها خصوصی باقی می‌ماند.

پس از ثبت تراکنش، شبکه بلاک چین صحت آن را تأیید می‌کند. پس از تأیید، تراکنش به بلاک در بلاک چین اضافه می‌شود. همان‌طور که گفتیم تغییر این بلاک‌ها غیرممکن است و این امنیت تراکنش‌ها را تضمین می‌کند.

شفافیت فناوری

بیشتر بلاک چین‌ها کاملاً منبع باز هستند؛ یعنی همه می‌توانند کد آن را مشاهده کنند. بااین‌حال، هیچ مرجعی وجود ندارد که بتواند کدهای آن را کنترل یا ویرایش کند. به همین دلیل هرکسی می‌تواند تغییرات یا ارتقای سیستم را پیشنهاد دهد. اگر بیشتر کاربران شبکه موافق باشند که نسخه جدید کد یا ارتقای آن درست و ارزشمند است، می‌توان تغییرات را در بلاک چین اعمال کرد.

بانکداری بدون بانک

بلاک چین جایگزینی مناسب برای بانک و راهی برای ایمن‌سازی اطلاعات محرمانه شهروندانی است که در کشورهایی با دولت‌های خودکامه یا توسعه‌نیافته زندگی می‌کنند. شاید بهترین جنبه بلاک چین و البته ارزهای دیجیتال، این باشد که هرکسی صرف‌نظر از قومیت، نژاد، جنسیت و محدوده جغرافیایی که در آن ساکن است، می‌تواند از آن استفاده کند.

براساس گزارش بانک جهانی، میلیاردها بزرگ‌سال در جهان در مناطقی زندگی می‌کنند که خدمات بانکی وجود ندارد و بنابراین آن‌ها برای ذخیره پول و ثروتشان جایی را سراغ ندارند .آن‌ها تراکنش‌هایشان را با پول نقد فیزیکی می‌پردازند یا سرمایه‌شان را در خانه ذخیره می‌کنند؛ بنابراین از شر دزدان و تبه‌کاران در امان نیستند. این افراد به‌راحتی می‌توانند از بلاک چین و ارزهای دیجیتال بهره‌مند شوند.

معایب فناوری بلاک چین

با همه مزایایی که فناوری بلاک چین دارد، چندان هم بی‌عیب نیست. برخی از معایب بلاک چین عبارت‌اند از:

هزینه گزاف فناوری‌های مرتبط با بلاک چین

بلاک چین می‌تواند در هزینه‌های تراکنش‌ها صرفه‌جویی کند؛ اما خود این فناوری که رایگان نیست. برای نمونه، سیستم اثبات کار شبکه بیت کوین برای اعتبارسنجی تراکنش‌ها، توان محاسباتی زیادی مصرف می‌کند.

در دنیای واقعی، میزان انرژی که میلیون‌ها دستگاه در شبکه بیت کوین مصرف می‌کنند، از مصرف سالانه انرژی در کشور پاکستان بیشتر است. البته راه‌حل‌هایی مانند مزارع استخراج بیت کوین برای استفاده از انرژی خورشیدی، بادی یا گاز طبیعی اضافی راه‌اندازی شده‌اند که ممکن است مشکل را حل کند.

نرخ TPS (تراکنش در ثانیه) پایین

سرعت تسویه تراکنش‌ها در بلاک چین بسیار سریع‌تر از بانک‌داری سنتی است .بااین‌حال، تعداد تراکنش‌هایی که این شبکه در ثانیه می‌تواند پردازش کند، بسیار کمتر از شبکه‌هایی مانند ویزا است.

یک مطالعه موردی عالی برای ناکارآمدی احتمالی بلاک چین از نظر سرعت انجام تراکنش، بیت کوین است. برای سیستم اثبات کار بیت کوین، حداقل ۱۰ دقیقه زمان نیاز است تا یک بلاک جدید به بلاک چین اضافه شود.

با این نرخ، تعداد تراکنش در ثانیه (TPS) شبکه بلاک چین بیت کوین فقط ۷ تاست. اتریوم هم اوضاع بهتری ندارد؛ زیرا آن‌هم به ۱۴ تراکنش در ثانیه محدود است. این مقدار را با ویزا مقایسه کنید که ۶۵،۰۰۰ تراکنش را در ثانیه پردازش می‌کند.

البته در سال‌های اخیر، راه‌حل‌هایی با عنوان راه‌کارهای لایه دوم توسعه یافته‌اند که سعی می‌کنند ازدحام شبکه را کاهش دهند و فرایند پردازش تراکنش‌ها را سریع‌تر کنند .روش‌های نوآورانه نظیر شاردینگ در اتریوم یا معرفی شبکه‌های فرعی و نمونه‌گیری تصادفی در اولنچ دو نمونه از این راه‌کارها هستند.

بحث تغییر اندازه بلاک هم از مسائل مهمی است که برای مقیاس‌پذیری بلاک چین و افزایش TPSمدت‌هاست موردبررسی قرار گرفته است.

فعالیت‌های غیرقانونی

بااین‌که محرمانه‌بودن فعالیت‌ها در شبکه بلاک چین، از کاربران دربرابر هک محافظت می‌کند، نباید از بستری که برای فعالیت غیرقانونی در شبکه برای مجرمان فراهم می‌آورد غافل شد.

در سال‌هایی که بلاک چین رشد و توسعه یافته است، موارد متعددی از کاربرد آن در دارک وب و فعالیت‌های مجرمانه گزارش شده است. مشهورترین آن‌ها بازاری آنلاین با استفاده از بلاک چین برای فروش موادمخدر و پول‌شویی بود که سیلک رود یا جاده ابریشم نامیده می‌شد. این بازار از فوریه ۲۰۱۱ آغاز به کار کرد تا اینکه FBI در اکتبر ۲۰۱۳ موفق شد آن را تعطیل کند.

دارک وب به کاربران امکان می‌داد با استفاده از مرورگر Tor کالاهای غیرقانونی خریدوفروش کنند و مبالغ آن را با بیت کوین و ارزهای دیجیتال پرداخت کنند که قابل‌ردیابی نبود. البته جالب اینجاست که بیت کوین خیلی هم ناشناس نیست و نمی‌توان آن را غیرقابل‌ردیابی دانست.

برخی هم استدلال می‌کنند که بسیاری از فعالیت‌های مجرمانه در جهان با پول نقد مخصوصاً دلار آمریکا انجام می‌شود که قابل‌ردیابی نیستند و اتفاقاً موارد آن‌ها بسیار بیشتر از بلاک چین است.

انواع بلاک چین

بلاک چین‌ها به‌طور کلی به چهار دسته تقسیم می‌شوند:

اول؛ بلاک چین عمومی

دوم؛ بلاک چین خصوصی

سوم؛ بلاک چین هیبریدی

چهارم؛ بلاک چین کنسرسیومی

بلاک چین عمومی

بلاکچین‌های عمومی بدون نیاز به مجوز هستند و هرکسی می‌تواند در آن‌ها مشارکت کند. هیچ مرجع واحدی نودهای این بلاک چین را کنترل نمی‌کند؛ بنابراین کاملاً غیرمتمرکز است و تغییر تراکنش‌های ثبت‌شده در آن بسیار دشوار است. این بلاک چین‌ها برای معامله و استخراج ارزهای دیجیتالی مانند بیت کوین مناسب‌اند.

بلاک چین خصوصی

بلاک چین خصوصی را یک سازمان یا گروه کنترل می‌کنند. آن‌ها می‌توانند تصمیم بگیرند که چه کسی وارد این سیستم می‌شود و می‌تواند به داده‌ها دسترسی داشته باشد. به‌دلیل این محدودیت، این بلاک چین‌ها فقط تاحدودی غیرمتمرکز هستند.

این فرایند بیشتر شبیه یک سیستم ذخیره‌سازی داده داخلی است و فقط برای افزایش امنیت بین تعدادی نود توزیع شده است. گروهِ کنترل درصورت لزوم می‌توانند به عقب برگردند و بلاک‌ها را تغییر دهند. ریپل یکی از نمونه‌های بلاک چین خصوصی است.

بلاک چین هیبریدی

بلاک چین‌های هیبریدی ترکیبی از عناصر شبکه‌های بلاک چینی خصوصی و عمومی هستند . مثلاً یک شرکت تمایل دارد یک بلاک چین خصوصی و مبتنی‌برمجوز راه‌اندازی کند؛ ولی یک سیستم عمومی هم درکنار آن داشته باشد. در چنین شبکه‌ای، سازمان می‌تواند دسترسی به داده‌های خاص ذخیره‌شده در بلاک چین را کنترل کند و بقیه داده‌ها را عمومی نگه دارد.

اعضای عمومی می‌توانند با استفاده از قراردادهای هوشمند تعبیه‌شده در این بلاک چین، بررسی کنند که آیا تراکنش‌های خصوصی انجام شده‌اند یا خیر.

بلاک چین کنسرسیومی

این بلاک چین‌ها بین گروهی از سازمان‌ها مشترک هستند. بیشتر برای صنایعی کاربرد دارند که در آن‌ها تعداد زیادی سازمان با اهداف و مسئولیت مشترک، باید به داده‌های صنعت خود دسترسی داشته باشند.

حفظ و مدیریت این شبکه‌ها برعهده تمام سازمان‌های مشمول در آن است. برای نمونه، کنسرسیوم شبکه تجارت جهانی کشتی‌رانی، یک کنسرسیوم غیرانتفاعی بلاک چین است که هدف آن دیجیتالی‌کردن صنعت حمل‌ونقل و افزایش همکاری بین اپراتورهای صنعت دریایی است.

کاربردهای بلاک چین

بلاک چین در سیر تکاملی خود، دائماً رشد کرده و پتانسیل خود را برای ادغام با صنایع متنوع نشان داده است. هرچند هنوز کاربرد بلاک چین در این صنایع به جایی نرسیده است که همه در سراسر جهان از آن استفاده کنند؛ اما به‌زودی این اتفاق رخ خواهد داد.

برخی از کاربردهای بلاک چین در صنایع عبارت‌اند از:

قراردادهای هوشمند

شاید بدانید قرارداد سنتی، کاغذی است که در آن شما و یک فرد (نهاد) دیگر، درباره زمینه خاصی توافق می‌کنید. در این توافق یک‌سری بایدها و نبایدها تعریف می‌شود که هر دو طرف قرارداد با آن هم‌نظر هستید و به‌موجب آن، باید تعهدات درج‌شده در قرارداد را اجرا کنید.

قراردادهای هوشمند درست مشابه قراردادهای سنتی هستند؛ با این تفاوت که این تعهدات را در فضای دیجیتال تعریف می‌کنند و البته اجرای آن تعهدات کاملاً خودکار اجرا می‌شود.

برای مثال، فرض کنید قرار است آپارتمانی را با کمک قرارداد هوشمند اجاره کنید .صاحب‌خانه موافقت می‌کند که به‌محض دریافت پیش‌پرداخت شما، کدِ در آپارتمان را تحویل دهد. این کد در قرارداد هوشمند تعبیه می‌شود.

وقتی شما پیش‌پرداخت را واریز می‌کنید، قرارداد هوشمند خودبه‌خود کد را در اختیار شما قرار خواهد داد. اما پرداخت اجاره ماهیانه چطور؟ قرارداد هوشمند را طوری تنظیم می‌کنید که درصورت پرداخت‌نکردن اجاره تا مهلت مشخص‌شده، کد در را تغییر دهد.

امور مالی غیرمتمرکز

یکی از کاربردهای فناوری بلاک چین، امور مالی غیرمتمرکز یا دیفای است که به کاربران اجازه می‌دهد مانند چیزی که در دنیای مالی سنتی رایج است، به خدمات مالی دسترسی داشته باشند با این تفاوت که این خدمات کاملاً غیرمتمرکز هستند.

با استفاده از راه‌حل‌های مختلف دیفای، کاربران می‌توانند وام بگیرند، وجوه مدنظرشان را برای انجام معامله قرض بگیرند و همه این‌ها بدون وجود یک مرجع متمرکز روی بلاک چین اداره می‌شوند.

توکن‌های غیرمثلی

توکن‌های غیرمثلی یاNFT ها، کاربرد ارزشمندی از فناوری بلاک چین با پتانسیل‌های گسترده هستند. این توکن‌های منحصربه‌فرد را نمی‌توان به‌صورت نظیر به نظیر و با ارزش یکسان مبادله کرد. یکی از موارد کاربرد آن‌ها قانون کپی‌رایت و احراز هویت آثار هنری است؛ چیزی که می‌تواند اصالت و مالکیت آن‌ها را تأیید و از کپی‌کردن غیرمجاز آن‌ها جلوگیری کند.

زنجیره تأمین

استفاده از فناوری بلاک چین در زنجیره تأمین می‌تواند به رهگیری و اثبات منشأ حقیقی مواد اولیه، غذاها و کالاهای مصرفی کسب‌وکارها کمک کند. هرگونه اطلاعات درباره زنجیره تأمین، بدون هیچ تغییری در بلاک چین ثبت می‌شود. فرایندی کاملاً شفاف که از هرگونه تقلب جلوگیری به عمل می‌آورد.

مطالبات بیمه

یکی از بهترین کاربردهای بلاک چین را می‌توان صنعت بیمه دانست. فرایند کنونی مطالبه بیمه، بسیار دشوار و وقت‌گیر است. با قرارداد هوشمند می‌توان مجموعه خاصی از معیارها را برای شرایط خاص مرتبط با بیمه ایجاد کرد. کاربر می‌تواند مطالبات بیمه‌ای را به‌صورت آنلاین به بلاک چین ارسال کند تا پس از بررسی، درصورتی‌که شرایط استفاده از بیمه را دارد، به‌شکل خودکار و کاملاً آنی پرداختش انجام شود.

تأیید هویت

به‌لطف جنبه غیرمتمرکز بلاک چین، می‌توان فرایند تأیید هویت آنلاین را بسیار سریع‌تر و احتمالاً ایمن‌تر انجام داد. نگهداری داده‌های هویت آنلاین در یک مکان مرکزی خطرات بالقوه‌ای دارد؛ این در حالی است که با کمک بلاک چین، هکرهای رایانه دیگر نقاط آسیب‌پذیری متمرکز در برابر حمله را در اختیار نخواهند داشت.

اینترنت اشیا

اینترنت اشیا (IoT) اکوسیستمی از دستگاه‌ها و تجهیزات محیط پیرامون ماست که مشخصات فنی خاصی دارند و با اتصال به اینترنت، می‌توانند با نرم‌افزارهای موجود در تلفن‌های هوشمند، رایانه و نظایر آن‌ها تعامل برقرار کنند. این فناوری امکان کنترل و مدیریت ازراه‌دور این دستگاه‌ها را برای ما فراهم می‌کند.

فناوری بلاک چین می‌تواند با ارائه روش‌هایی برای محافظت دربرابر هکرها، در آینده اینترنت اشیا نقش داشته باشد. ازآنجاکه بلاک چین امکان کنترل غیرمتمرکز را فراهم می‌کند، طرح امنیتی مبتنی بر آن باید به‌اندازه کافی مقیاس‌پذیر باشد تا بتواند شبکه عظیم اینترنت اشیا را پوشش دهد.

آرشیو و ذخیره فایل

گوگل درایو، دراپ باکس و برنامه‌های نظیر آن، آرشیو الکترونیکی اسناد را با استفاده از روش‌های متمرکز امکان‌پذیر کرده‌اند و چه سفره وسوسه‌انگیزی هم برای هکرها هستند! بلاک چین و قراردادهای هوشمند می‌توانند روش‌هایی برای کاهش قابل‌توجه این تهدید در ذخیره‌سازی اطلاعات ارائه دهند. سلام بر حریم خصوصی واقعی!

سیستم رأی‌گیری

با کمک بلاک چین و قرارداد هوشمند می‌توان یک سیستم رأی‌گیری مدرن طراحی کرد که کسی نتواند آرای مردم را دستکاری کند. انتخابات میان‌دوره‌ای نوامبر ۲۰۱۸ که در ویرجینیای غربی در آمریکا به‌شکل آزمایشی با کمک بلاک چین انجام شد، نشان داد که این سیستم می‌تواند تقلب را در انتخابات حذف کند و شهروندان واجدشرایط بیشتری را به مشارکت وادارد.

در این روش، دستکاری آرا تقریباً غیرممکن است و شفافیت حاصل از آن، نیاز به بازشماری مجدد و نگرانی از تقلب را از بین می‌برد. حتی نیازی به کارکنان انسانی برای شمارش آرا نیست و نتایج فوراً در اختیار مقامات قرار خواهد گرفت.

مراقبت‌های بهداشتی

ارائه‌دهندگان مراقبت‌های بهداشتی می‌توانند از بلاک چین برای ذخیره ایمن سوابق پزشکی بیماران خود استفاده کنند. پرونده‌های پزشکی بلاک چینی به بیماران اطمینان می‌دهد که سابقه آن‌ها قابل‌تغییر نیست. همچنین با کمک کلید خصوصی در بلاک چین می‌توان کاری کرد این پرونده فقط در دسترس افراد خاصی قرار گیرد.

سوابق مالکیت اموال

ثبت حقوق مالکیت در صنعت املاک و مستغلات کاری بسیار دشوار و ناکارآمد است .اسناد فیزیکی، کاغذبازی و ثبت به‌صورت دستی در پایگاه داده متمرکز، همگی مستعد بروز خطای انسانی هستند.

هر اشتباه در این اسناد می‌تواند ردیابی مالکیت دارایی را با مشکل مواجه کند .کاربرد بلاک چین در صنعت املاک و مستغلات می‌تواند این مشکلات را تا حد زیادی حل کند و سوابق مالکیت را به‌شکل دقیق و دائمی در خود نگه دارد.

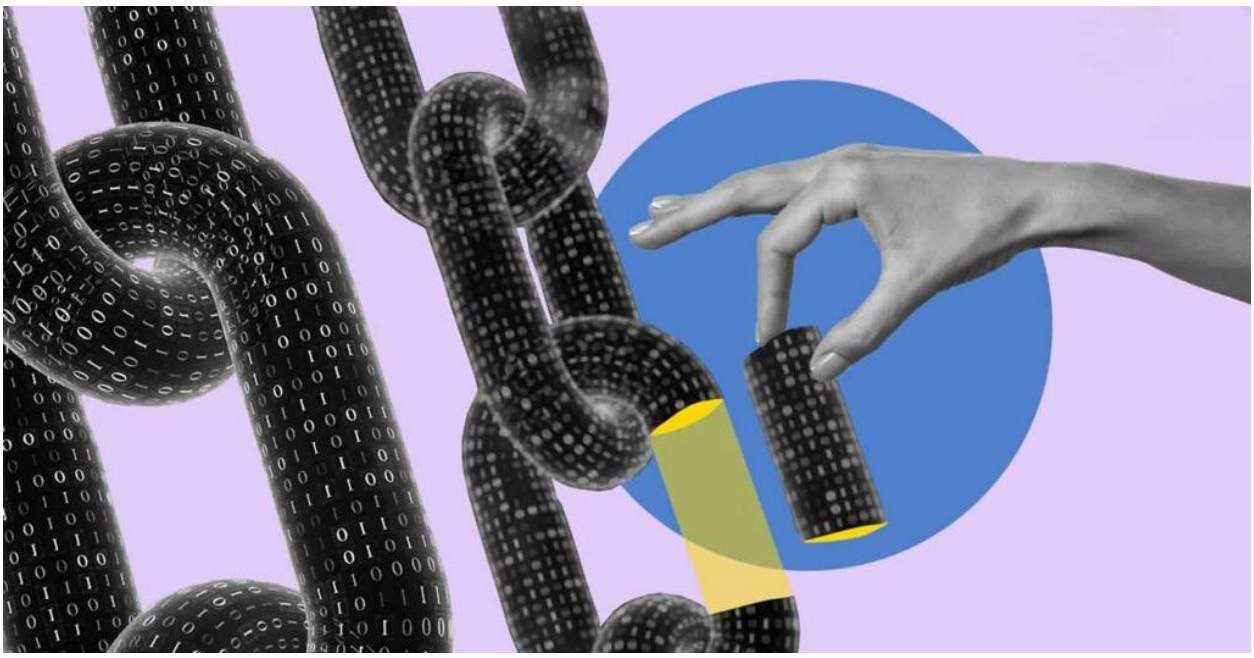
تفاوت بلاک چین با بیت کوین

بسیاری بلاک چین و بیت کوین را با هم یکی می‌دانند؛ اما این دو کاملاً با هم متفاوت‌اند. بیت کوین اولین کاربرد بلاک چین بود؛ به همین دلیل افراد به‌شکل ناخواسته تصور کردند این دو یکی هستند. فناوری بلاک چین کاربردهای زیادی به جز بیت کوین دارد.

بیت کوین یک ارز دیجیتال است که از فناوری بلاک چین استفاده می‌کند. بلاک چین زنجیره‌ای از بلاک‌های متصل به هم است که امکان ساخت ارزهای دیجیتالی نظیر بیت کوین را فراهم می‌کند.

شبکه بیت کوین یک دفتر کل است که همه تراکنش‌های بیت کوین را ثبت می‌کند و سرورهای سراسر جهان، نسخه‌هایی از این دفتر کل را نگهداری می‌کنند.

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 Blockchainبه 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.

بلاک چین در صنعت مالی، زنجیره‌ی تأمین، رایانش ابری و سایر زمینه‌هایی که نیاز به ذخیره‌سازی و انتقال اطلاعات دارند، اهمیت بسیار بالایی پیدا کرده و در کنار افزایش سرعت و

کاهش هزینه‌ها، خدماتی مانند فراهم کردن مالکیت برای دارایی‌های دیجیتال، امنیت برای داده‌ها، امکان ردگیری و شفاف‌سازی زنجیره تامین کالا و خدمات را در اختیار دنیای امروز قرار می‌دهد.

در سال‌های اخیر، افراد بسیاری به‌دنبال خرید و فروش بیت کوین و استفاده از قابلیت‌های دیگر این ارز دیجیتال بوده‌اند. از افراد مبتدی و تازه‌کار تا تریدرهای حرفه‌ای دنیای جذاب ارزهای دیجیتال، همه به این پدیده‌ی نوظهور و خاص قرن ۲۱، علاقه‌ی بسیاری پیدا کرده‌اند.

با وجود افزایش روزافزون تعداد تریدرهای بازار ارزهای دیجیتال، افراد کمی درباره‌ی فناوری زیرساختی بیت کوین، یعنی بلاک چین مطالعه کرده و از آن آگاهی دارند؛ حتی ممکن است از ساخت ارزهای دیجیتال دیگر بر پایه بلاک چین هم بی‌اطلاع باشند.

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.

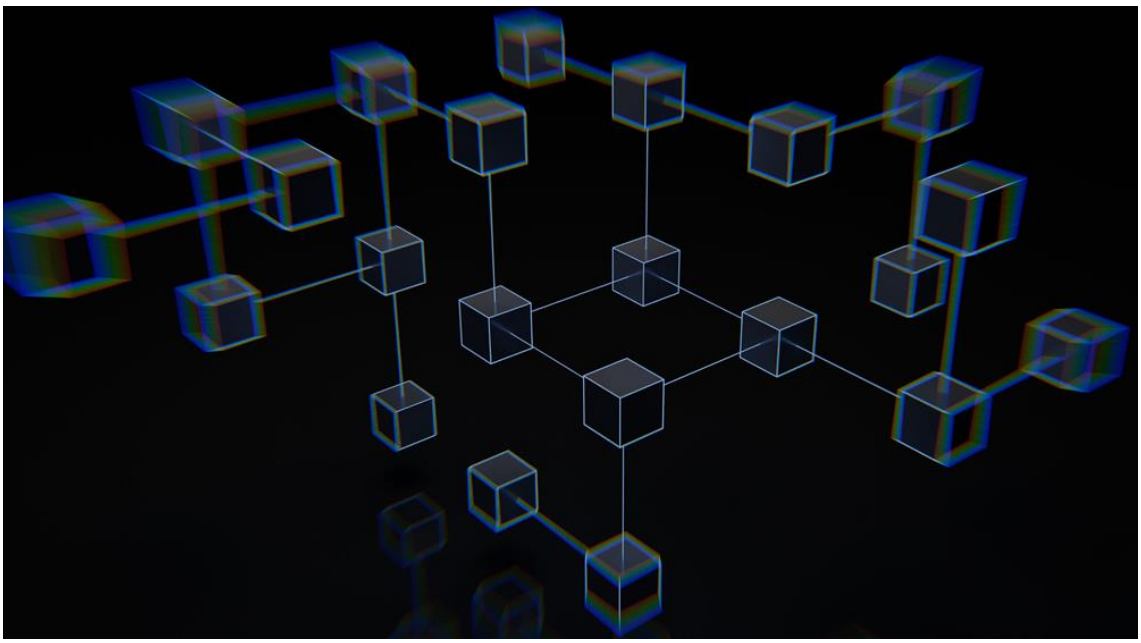
فرض کنید که دو ستون روی برگه‌ای دارید و هر اطلاعاتی که می‌خواهید نگهداری کنید را در سطر اول ستون اول بگذارید. داده داخل این سلول، طی فرآیندی محاسباتی تبدیل به یک کلمه جدید با دو حرف می‌شود. این کلمه در ورودی بعدی مورد استفاده قرار می‌گیرد. در این حالت، هر تغییری در سلول اول، منجر به تغییراتی در سلول 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.
٤. به هر بلاک، باید هَش (کد) داده شود: پس از تأیید تمام معامله‌های یک بلاک، باید به آن بلاک یک کد شناسایی منحصر به فرد به 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 چینR3 ، بلاک چین Quorum و اسمارت چین بایننس 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 چینDragonchain ، 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

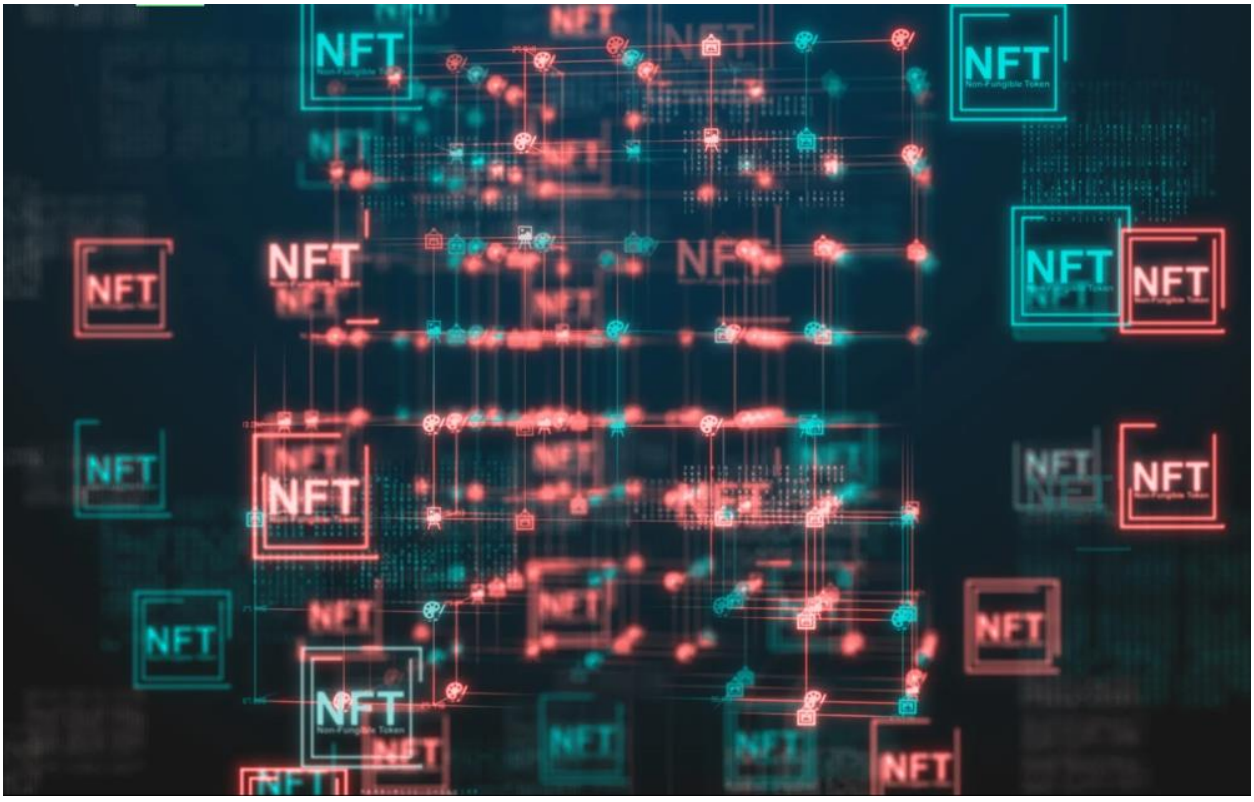
انتقال پول در سطح بین‌المللی با سیستم بانک‌داری سنتی، دردسرساز است .به دلیل وجود شبکه پیچیده‌ای از واسطه‌ها، استفاده از سیستم بانکی سنتی، انتقال پول، پرهزینه و به کندی انجام می‌شود، اما ارزهای دیجیتال و بلاک چین، این واسطه‌ها را از بین می‌برند و امکان انتقال پول را به شکلی سریع و آسان به سرتاسر جهان 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.



برخی دیگر از کاربردهای فناوری بلاک چین در دنیای مدرن امروز عبارت‌اند از:

- **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.

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.

بلاک چین چه مشکلات و محدودیت‌هایی دارد؟

به طور کلی، بلاک چین با وجود مزایایی که به همراه دارد، هنوز در مراحل اولیه توسعه و بهبود به سر می‌برد و مانند هر فناوری دیگری، مشکلات و محدودیت‌هایی دارد. البته انتظار می‌رود که با پیشرفت فناوری و بهبود در مشکلات آن، این فناوری انقلابی بتواند در بسیاری از حوزه‌ها استفاده شود .برخی از مشکلات و محدودیت‌هایی که با بلاک چین مرتبط هستند، عبارت‌اند از:

- **اصطلاحات تخصصی**: این فناوری به دلیل نوظهوری دارای مجموعه واژگانی کاملا جدید است. خوشبختانه در طول این چند سال تلاش‌های متعددی در زمینه ارائه واژه‌نامه‌ها، تعاریف و فهرست‌های کامل و آسان انجام شده است. شما در آکادمی ارز دیجیتال بیت‌پین، می‌توانید با خواندن دو مقاله‌ی ۱۰ مورد از بهترین فیلم‌ها در مورد بیت کوین و بلاک چین یا ۱۰ مورد از بهترین کتاب‌های ارز دیجیتال و بلاک چین، با منابعی برای آشنایی با این واژه‌ها آشنا شوید یا با مطالعه‌ی مطالب خودِ آکادمی به دنیای از دانش در مورد بلاک چین و ارزهای دیجیتال، دسترسی داشته باشید.
- **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، Blockchainفناوری 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 نوعBlockchain ، 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

درBlockchain 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.