بلاکچین چیست؟

بلاک چین (Blockchain) از دو کلمه بلاک (Block) و چین (Chain) تشـکیل شـده است. معنای لغوی بلاک چین، زنجیره بلاک (زنجیره بلوک) است؛ زمانی که در مورد زنجیره و بلاک در بلاکچین صـحبت می‌کنیم، در واقع در مورد زنجیره‌ایی از اطلاعات دیجیتالی صـحبت می‌کنیم و هر بلاک این اطلاعات را در خود نگهداری می‌کند.

در یـک تعریف کلی، می‌توانیم بگوییم بلاک چین یـک دفتر کـل توزیع شـــده، غیرمتمرکز و اشـتراکی اسـت که به صـورت زنجیره‌ای از سـوابق بنام بلاک سـاخته شده است. هر بلاک در این زنجیره، مسئول ذخیره‌سازی نوعی از اطلاعات (مانند سوابق معاملات) است.

هر بلاک اطلاعات مربوط به معاملات مانند تاریخ، زمان، مبلغ خرید شـما از سـایت و اطلاعات فروشـندگان و خریداران در معاملات را ذخیره می‌کند. به جای اسـتفاده از نام واقعی شـما در معاملات، خرید شـما بدون هیچ گونه اطلاعات هویتی و با اسـتفاده از امضـای دیجیتال منحصر به فرد انجام می‌شود. برای مثال، در سایت دیجی کالا با استفاده نام کاربری، خرید شما ثبت می‌شود. هر بلاک کد منحصـر به فردی به نام هش را ذخیره می‌کند که برای تشـخیص هرگونه فعالیت در بلاک چین است.

به عنوان مثال، فرض کنید شـما قبلاً از دیجی کالا محصولی را خریداری کرده‌اید، بعد از مدتی، مجدد تصـمیم می‌گیرید که یک خرید دیگر انجام دهید. حتی اگر جزئیات خرید جدید شـما با خرید قبلی‌تان تقریباً یکسـان به نظر برسـد، سـایت دیجی کالا می‌تواند ۲ خرید شما را از هم جدا کند؛ بنابراین، به دلیل کدهای منحصـر به فردی که در بالا به نام هش عنوان شـد، ما می‌توانیم بلاک‌ها را از هم جدا کنیم.

مثـالی که در بالا برای ذخیره یک خرید واحد از دیجی کالا عنوان شـد، در واقعیت با بلاک در بلاک چین کمی متفاوت اسـت. یک بلاک روی بلاک چین حجم خاصـی از داده را می‌تواند ذخیره کند. این بدان معناسـت که بسته به اندازه معاملات، یک بلاک واحد می‌تواند چند هزار تراکنش را در خود جای دهد.

چرا به بلاکچین نیاز داریم؟

مفهوم بلاک چین برای اولین بار توسط استوارت هابر و دبلیو اسکات استورنتتا در سال ۱۹۹۱ به عنوان زنجیره‌ای از بلوک‌های امن از نظر رمزنگاری معرفی شد و با گذشت زمان جای خود را در میان پایگاه‌داده‌های سراسر دنیا باز کرد. مالکان کسب و کارهای دیجیتال به فکر استفاده از این فناوری در جهت پیشرفت امور خود افتادند و در نهایت نیاز به استفاده از این فناوری در همه دنیا احساس شد. اما سه دلیل اصلی برای نیاز به بلاک چین وجود دارد؛

افزایش قدرت پردازش دیجیتال

بلاک چین با توجه به ساختار طراحی شده‌اش به قدرت پردازش بالاتری نسبت به محاسبات داده‌های معمولی نیاز دارد. طراحی بلاکچین بر اساس رمزنگاری تعریف شده است و رمزگذاری و رمزگشایی داده‌ها طبیعتاً یک امر پرهزینه است. امروزه کامپیوترها به لطف پردازنده های مدرن توسعه یافته از قدرت پردازش بیشتری برخوردارند که این امر منجر به رشد تقاضا برای استفاده از این فناوری شده است.

رشد سریع جرایم سایبری

جرایم سایبری در چند سال گذشته چند برابر شده است. هک بیش از یک میلیارد حساب یاهو، لو رفتن اطلاعات کاربران در فیسبوک و افزایش آسیب های بدافزارها تنها چند مورد از این جرایم هستند. در واقع روزانه بیش از یک میلیون تهدید سایبری منتشر می‌شود که این به خودی

خود توجه بیشـتری به امنیت را ایجاد می‌کند. امروزه امنیت سایبری یکی از بزرگترین چالش‌های مالکان کسـب و کارهای اینترنتی است Blockchain .با استفاده از سیستم رمزنگاری قدرتمند خود تا حدودی این نیاز را پاسخ می‌دهد.

ظهور بیت کوین و ارز دیجیتال

بیت کوین و سایر ارزهای دیجیتال یکی از بزرگترین دلایل افزایش محبوبیت Blockchain هستند. بیت کوین یک ارز دیجیتال است که توسط شخصی ناشناس به نام ساتوشی ناکاموتو ایجاد شده است که از فناوری بلاکچین برای ایجاد و توزیع ارز دیجیتال امن استفاده کرده است.

بلاکچین چگونه کار می‌کند؟

همانطور که اکنون می‌دانید، بلاک چین شامل چندین بلاک است که به هم وصل شده‌اند. برای اینکه یک بلاک به بلاک چین اضافه شود باید ۴ اتفاق رخ دهد:

۱ .شروع یک معامله یا تراکنش

هر گونه معامله یا تراکنشـی که در شـبکه انجام می‌شود، منجر به افزوده شدن یک بلاک جدید در بلاک چین می‌شود. به عنوان مثال، در صورتی که قصد دارید مقداری اتریوم کیف پول دوستتان واریز کنید، این تراکنش با ایجاد بلاکی جدید در اکوسیستم اتریوم انجام می‌شود.

۲ .تایید تراکنش

پس از ثبت درخواسـت انتقال شـما، ماینرهای شـبکه مسـئول تایید تراکنش شما خواهند بود. ابتدا نیاز اسـت که اطلاعات جدید وارد سـیستم شود. این کار به عهده کامپیوترها است. این شبکه غالباً از هزاران کامپیوتر تشکیل شده است که در سراسر جهان پخش شده‌اند.

۳ .ذخیره معامله

معامله شـما باید در یک بلاک ذخیره شـود. پس از تأیید صـحت معامله، مبلغ درخواسـتی شما برای واریز و امضای دیجیتالی شما در یک بلاک ذخیره می‌شوند .

۴ .اضافه شدن بلاک به بلاکچین با استفاده از هش

پس از تأیید کلیه معاملات یک بلاک، باید یک کد شـناسایی کننده منحصر به فرد به نام هش (Hash)به بلاک اختصـاص یابد. پس از هش شدن می‌توان بلاک را به Blockchain اضافه کرد.

پس از ایجاد یک بلاک جدید در شبکه، این بلاک برای همه در دسترس خواهد بود. به عنوان مثال اگر نگاهی به بلاکچین بیت کوین بیندازید، خواهید دید که به داده‌های معامله دسترسی دارید و می‌توانید اطلاعات زیر را مشاهده کنید:

- **ارتفاع بلاک** (Height) که بر اساس تعداد کل بلاک‌ها محاسبه می‌شود و نشان می‌دهد که این چندمین بلاکی است که روی زنجیره بلاک چین قرار می‌گیرد.
- **هش بلاک** (Hash) که یک رشته کد ۶۴ رقمی که شامل اعداد و حروف است و با صفر شروع می‌شود.
- چه زمانی طول کشیده است تا بلاک استخراج شود.(Mined)
- توسط چه کسی استخراج شده است.(Miner)
- اندازه بلاک چقدر است.(Size)
-

انواع شبکه های بلاک چین

بلاکچین دسته بندی‌های مختلفی دارد که عبارتند از: بلاک چین عمومی، خصوصی، کنسرسیومی و هیبرید. در ادامه به بررسی انواع بلاک چین و ویژگی‌های آن‌ها می‌پردازیم.

بلاکچین عمومی

در بلاکچین عمومی مانند بیت کوین، همه افراد می‌توانند عضو سیستم شوند و محدودیت دسترسی وجود ندارد. هر کسی می‌تواند محتویات بلاک چین‌های عمومی مانند بلاک چین بیت کوین را مشاهده کند. همچنین، کاربران می‌توانند کامپیوترهای خود را به شبکه بلاک چین متصل کنند. با انجام این کار، هر زمان که یک بلاک جدید اضافه شود، کامپیوترها یک نسخه از بلاک چین را که به طور خودکار بروزرسانی می‌شود، دریافت می‌کنند.

بلاکچین خصوصی

در بلاکچین خصوصی مانند بلاک چین‌های شرکتی، محدودیت دسترسی به اطلاعات (مانند دستمزد کارمندان) وجود دارد و برای ثبت نام و استفاده از این سیستم، به تایید نیاز دارید.

بلاکچین کنسرسیومی

بلاکچین کنسرسیوم (Consortium Blockchain) نیمه غیرمتمرکز است. این بلاک چین‌ها زمانی بسیار کاربردی هستند که چند سازمان یا شرکت، قصد شراکت و همکاری با یکدیگر را دارند. آن‌ها می‌توانند در این بستر یک فضای مشترک ایجاد کنند و به راحتی اطلاعات را در امنیت کامل با یکدیگر به اشتراک بگذارند.

بلاکچین هیبرید

بلاکچین هیبرید ترکیبی از بلاک چین‌های عمومی و خصوصی است. از مزایای هر دو نوع این بلاکچین‌ها بهره برده و معایب را به حداقل رسانده است. در این نسخه، اجازه‌ی عضویت با دستور مسئول کنترل کننده‌ی آن صادر می‌شود و میزان اجازه‌ی فعالیت در شبکه نیز با همین روش مشخص می‌شود. ورود به این شبکه برای عموم آزاد نیست.

هر کامپیوتر در شبکه Blockchain یک کپی از بلاک چین دارد. در مورد بیت کوین، میلیون‌ها نسخه از بلاک چین وجود دارد که بین هزاران نفر پخش شده است. گسترش اطلاعات در یک شبکه از کامپیوترها باعث می‌شود که دستکاری اطلاعات دشوارتر شود.

با این حال، با نگاهی به Blockchain بیت کوین متوجه می‌شوید که به اطلاعات کاربرانی که در حال انجام معاملات هستند، دسترسی ندارید. اطلاعات شخصی در مورد کاربران فقط به امضای دیجیتال یا نام کاربری آنها محدود می شود .

آیا بلاکچین امن است؟

فناوری بلاک چین موضـــوعات مختلفی از جمله امنیت و اعتماد را پوشـــش می‌دهد. بلاک‌های جدید همیشه بصورت خطی ذخیره و به انتهای زنجیره Blockchain اضافه می‌شوند. این بدان معنی اســـت که جدیدترین بلاک همیشـــه در انتهای زنجیره قرار دارد. بعد از اینکه یک بلاک به انتهای بلاکچین اضـافه شـد، برگرداندن و تغییر محتوای بلاک بسـیار دشوار است. به این دلیل که هر بلاک حاوی هش مخصـــوص به خود و هش بلاک قبل از آن اســـت. کدهای هش توســـط یک عملکرد ریاضـــی (تابع هش) ایجاد می‌شـوند که اطلاعات دیجیتال را به رشـــته‌ای از اعداد و حروف تبدیل می‌کند. اگر آن اطلاعات به هر طریقی ویرایش و دستکاری شود، کد هش نیز تغییر می‌کند؛ این مسئله برای امنیت شبکه مهم است.

برای مثال، فرض کنید یک هکر سـعی دارد معاملات شما را از سایت دیجی کالا ویرایش کند تا مجبور شـوید دوبار هزینه خرید خود را بپردازید. به محض اینکه مقدار تومان معامله شـما توسـط هکر تغییر کند، هش بلاک تغییر خواهد کرد. بلاک بعدی در زنجیره هنوز حاوی هش قدیمی است و هکر برای پوشش تغییرات خود باید بلاک قدیمی را به روز رسانی کند. با انجام این کار، هش این بلاک تغییر خواهد کرد.

بنـابراین، بـه منظور تغییر یـک بلاک واحـد، یـک هکر بـایـد هر بلاکی کـه پس از آن روی Blockchainایجاد شـده است را تغییر دهد. محاسبه مجدد همه این هش‌ها، انرژی محاسباتی بسـیار زیاد و غیرقابل تصوری را به همراه دارد و برای هکرها صرفه اقتصادی ندارد. بنابراین، پس از افزودن یک بلاک به بلاکچین، ویرایش آن بسیار مشکل خواهد بود و حذف آن غیرممکن است.

الگوریتم اجماع در بلاکچین

برای حل مسـئله اعتماد، انواع شـبکه‌های بلاک چین تسـت‌هایی را برای کامپیوترهایی که می‌خواهند به آنها بپیوندند و بلاک‌های جدیدی به زنجیره اضـافه کنند، در نظر گرفته اسـت. این آزمایشـات که الگوریتم اجماع (consensus models) نامیده می‌شـود، کاربران را مجبور می‌کند قبل از شـرکت در یک شـبکه Blockchain و اضـافه کردن بلاک، خود را ثابت کنند. یکی از متداول‌ترین این نمونه‌ها که در شبکه بیت کوین به کار می‌رود، گواه اثبات کار (proof of work)نامیده می شود.

در سـیسـتم اثبات کار، کامپیوترها باید ثابت کنند که روی حل یک مسئله پیچیده ریاضی، کار کرده‌اند. اگر کامپیوتری یکی از این مسـائل را حل کند، واجد شـرایط اضـافه شـدن یک بلاک به بلاک چین می‌شود. اما روند افزودن بلاک، آنچه جهان کریپتوکارنسی آن را ماینینگ (Minig) می‌نامد آسان نیست.

در حقیقـت، با توجه به سـایت خبریBlockExplorer.com ، شـانس حل یکی از این مسـائل ریاضـی در شـبکه بیت کوین در فوریه ۲۰۱۹، حدود ۱ در ۵,۸ تریلیون بود. برای حل این مسـائل پیچیده، باید از دستگاه‌هایی استفاده شود که قدرت محاسباتی بالایی دارند. این دستگاه‌ها انرژی زیادی مصرف می‌کنند و ماینرها باید هزینه‌های زیادی را پرداخت کنند.

اثبـات کار، حملات هکرها را غیرممکن نمی‌کند، اما باعث می‌شـود این حملات تا حدودی بی فـایده باشـند. اگر یک هکر بخواهد حمله به Blockchain را هماهنگ کند، او باید مسـائل پیچیده ریاضـی را با شـانس ۱ در ۵,۸ تریلیون درسـت مثل هر فرد دیگری در شـبکه، حل کند. هزینه سازماندهی چنین حمله‌ای تقریباً و مطمئناً از مزایای آن فراتر خواهد رفت.

تفاوت بلاکچین و بیت کوین

هدف از بلاکچین، فراهم آوردن بستری است که اطلاعات دیجیتالی ضبط و توزیع شوند، اما ویرایش و دستکاری نشوند. دقت کنید که Blockchain همان بیت کوین نیست. بیت کوین تنها یکی از برنامه‌های بی شماری است که بر روی بلاک چین ساخته شده است. بیت کوین در حال حاضر بدون شک محبوب‌ترین پروژه Blockchain است، اما **فناوری بلاک چین** می‌تواند فراتر از بیت کوین عمل کند. در کلامی دیگر می‌توان گفت که این فناوری برای بیت کوین مثل اینترنت برای گوگل است.

در ادامه، بررسی می‌کنیم که بیت کوین به عنوان یکی از نخستین کاربردهای بلاک چین، چگونه کار می‌کند.

در سراسر جهان افرادی وجود دارند که صاحب بیت کوین هستند و بر اساس مطالعات مرکز کمبریج در سال ۲۰۱۷، این تعداد بیش از ۶ میلیون نفر عنوان شده است. وقتی صحبت از پول چاپی می‌شود، استفاده از ارز چاپی توسط یک مقام مرکزی (معمولاً یک بانک یا دولت) تنظیم و تأیید می‌شود، اما بیت کوین توسط کسی کنترل نمی‌شود. در عوض، معاملات انجام شده در بیت کوین توسط شبکه‌ای از کامپیوترها در سراسر جهان تأیید می‌شود که به نود (NODE) معروف هستند.

فرض کنیـد یک نفر از این ۶ میلیون نفر بخواهد بیت کوین خود را در یک میوه فروشـــی خرج کند. اینجاسـت که Blockchain وارد عمل می‌شـود. هنگامی که یک نفر برای خرید کالا قصد پرداخت بیت کوین به فروشـــنده را دارد، برخی از کامپیوترهای موجود در شـــبکه بیت کوین برای تـاییـد معامله با هم رقابت می‌کنند که به آنها ماینر می‌گویند. ماینرها برای انجام این کار برنامه‌ای را روی کامپیوترهای خود اجرا می‌کنند و سعی می‌کنند که مسئله ریاضی پیچیده‌ای را حل کنند.

هنگامی که کامپیوتر با هش کردن بلاک مسئله را حل کند، در واقع معامله را تایید کرده است. معاملهٔ تکمیل شـــده به صـــورت عمومی در زنجیره بلاک ثبت و ذخیره می‌شـــود و در این مرحله، تغییرنـاپذیر می‌شـــود. در مورد بیت کوین، کامپیوترهایی که با موفقیت بلاک‌ها را تأیید می‌کنند، مبلغی بیت کوین به عنوان پاداش دریافت می‌کنند که پاداش استخراج نام دارد.

کلید عمومی و کلید خصوصی در بلاکچین

برای انجام معاملات در شـبکه بلاکچین، شـرکت کنندگان باید برنامه‌ای با نام کیف پول را اجرا کنند .**اکوسـیستم بلاکچین** مجهز به کیف پول اختصاصی خود به نام کیف پول بلاکچین است. هر کیف پول از دو کلید رمزنگاری منحصـر به فرد و مجزا تشکیل شده است: یک **کلید عمومی** و یک **کلید خصـوصی** .کلید عمومی مکانی است که معاملات به آن سپرده شده و از آن خارج می شـوند (مانند شماره حساب). این کلید همچنین به عنوان امضای دیجیتالی کاربر در صفحه اصلی Blockchainظاهر می‌شود.

کلید عمومی کاربر نسـخه کوتاه شـده از کلید خصـوصـی آنها اسـت که از طریق یک الگوریتم پیچیده ریاضـی ایجاد شده است. با این حال، به دلیل پیچیدگی این معادله، معکوس کردن روند و تولید کلید خصـوصـی از یک کلید عمومی غیرممکن اسـت. به همین دلیل، این فناوری محرمانه تلقی می‌شود.

اجازه دهید با یک مثال کلید عمومی و کلید خصـوصـی را توضـیح دهیم: صـندوق انتقادات و پیشنهادات را در مدرسه به خاطر دارید؟ معلمان و دانش آموزان می‌توانستند نامه‌ها و یاداشت‌های خود را در این صـندوق قرار دهند و تنها کسی که کلید صندوق را داشت، می‌توانست به محتویات صندوق دسترسی داشته باشد. کلید صندوق در دفتر اصلی مدرسه نگه‌داری می‌شد. در بلاک چین، کلید عمومی مانند همان صـندوق عمومی مدرسـه و کلید خصـوصـی مانند کلید صـندوق عمل می‌کند اما تفاوت‌هایی بین آنها وجود دارد.

بر خلاف مدرسه که اطلاعات و کلیدهای خصوصی در دفتر اصلی نگه‌داری و مدیریت می‌شود، هیچ مرکزی وجود ندارد که کلیدهای خصوصی Blockchain را ردیابی کنند و به آنها دسترسی داشته باشد. اگر یک کاربر کلید خصوصی خود را فراموش کند و آن را از دست بدهد، دسترسی به کیف پول بیت کوین خود را برای همیشه از دست خواهد داد.

تاثیر الگوریتم اجماع در امنیت بلاک چین

در شبکه بیت کوین، بلاک چین نه تنها توسط یک شبکه عمومی از کاربران به اشتراک گذاشته شده و نگه‌داری می‌شود، بلکه در مورد آن توافق صورت می‌گیرد. کاربرانی که از طریق کامپیوترهای خود به شبکه متصل می‌شوند، یک نسخه از بلاکچین را دریافت می‌کنند که به محض اضافه شدن بلاک جدید به زنجیره، بروزرسانی می‌شود .

بلاک چین با استفاده از فرآیندی به نام الگوریتم اجماع (consensus) مانع از ایجاد چندین بلاک چین می‌شود. وجود کاربران بیشتر در شبکه بلاک چین به این معنی است که بلاک‌ها می‌توانند به سرعت به انتهای زنجیره اضافه شوند. با این منطق، بلاک چین همیشه همان چیزی خواهد بود که بیشتر کاربران به آن اعتماد دارند.

الگوریتم اجماع در شبکه‌ی بلاکچین و ارزهای رمزنگاری‌شده اهمیت بسیار زیادی دارد و به عنوان یکی از نقاط قوت بلاک چین به شمار می‌رود و به همراه رمزنگاری، امنیت بلاک چین را تضمین می‌کند. الگوریتم اجماع انواع مختلفی دارد که در حالت کلی به دو دسته الگوریتم گواه اثبات کار (PoW) و الگوریتم گواه اثبات سهام (PoS) تقسیم می‌شود.

آیا ممکن است اثبات کار در بلاک چین توسط هکرها انجام شود؟

در تئوری، ممکن است هکر بتواند از حق اکثریت که به آن حمله ۵۱ درصدی% ۵۱ (attack)گفته می‌شود، برای دستکاری بلاک‌ها استفاده کند. این حمله چگونه اتفاق می افتد؟

فرض کنید که که ۵ میلیون کامپیوتر در شبکه بیت کوین وجود دارد. برای دستیابی به اکثریت در شبکه، یک هکر باید حداقل ۲,۵ میلیون از آن کامپیوترها را کنترل کند. با انجام این کار، یک هکر یا گروهی از هکرها می توانند در روند ثبت معاملات جدید دخالت کنند. آنها می‌توانند معامله‌ای را انجام دهند و سپس همان معامله را دستکاری کنند؛ به گونه‌ای که به نظر می‌رسد ارز دیجیتالی که قبلاً برای شخص دیگری ارسال کردند، هنوز وجود دارد. این آسیب‌پذیری که به دو

بار خرج کردن یا خرج کردن مضاعف معروف است، معادل جعل دیجیتالی است و باعث می‌شود کاربران بتوانند بیت کوین‌های خود را بیش از یکبار خرج کنند.

اجرای چنین حمله‌ای برای یک Blockchain در مقیاس بیت کوین بسیار دشوار است، زیرا یک هکر نیاز دارد تا کنترل میلیون‌ها کامپیوتر را بدست بگیرد. از زمان معرفی بیت کوین و استخراج اولین بلاک آن، بیش از ۱۰ سال می‌گذرد و تاکنون حلمه ۵۱ درصدی و دستکاری در بلاک‌های بلاک چین رخ نداده است.

فناوری بلاک چین و تاثیر آن در آینده

اگرچه فناوری Blockchain کمی از بیت کوین قدیمی‌تر است، اما این فناوری اصلیترین عامل در شبکه‌های کریپتوکارنسی به شمار می‌رود. همه روزه کوین‌ها و توکن‌های جدیدی در بازار ایجاد می‌شود که استفاده دقیق‌تر و کامل‌تری از بلاک چین دارند. در آینده با افزایش محبوبیت متاورس و البته NFT ها، فناوری بلاکچین تغییرات گسترده‌تری خواهد داشت که البته این تغییرات در جهت بهبود بلاک چین ایجاد خواهد شد. در نهایت باید گفت که آینده بلاکچین از نظر متخصصان روشن است و افراد زیادی از آن در حوزه‌های مختلف کمک خواهند گرفت.