بلاک چین بیت کوین چگونه عمل می کند؟

آشنایی با بلاک چین

طبیعتا اولین قدم در شناسایی «بلاک چین بیت کوین» آشنایی با ماهیت خود بلاک چین است. به طور کلی اگر بخواهیم تعریفی جامع از بلاک چین ارائه دهیم باید بگوییم که بلاک چین در واقع نوعی پایگاه داده به شمار می‌آید که نوع جدیدی از پایگاه داده توزیع شده است و بر مبنای مجموعه‌ای از قوانین محاسباتی عمل می‌کند.

در بلاک چین‌های مختلف همچون بلاک چین بیت کوین، تراکنش‌ها با رمزنگاری تغییرناپذیر به نام هش، ثبت می‌شوند و دقیقا همین مسئله امنیت تراکنش‌ها را بیش از پیش تامین می‌نماید؛ چراکه اگر بلاک یک زنجیره تغییر کند این بدان معنا خواهد بود که آن دستکاری شده است.

به بیان ساده، اگر هکرها قصد داشته باشند که یک سیستم بلاک چین را خراب کنند، حتما باید کلیه بلوک موجود در زنجیره را در تمام نسخه‌های توزیع شده تغییر دهند که کاری بسیار دشوار و حتی غیرممکن است.

اصولا امنیت بلاک چین بیت کوین و همچنین اتریوم ETH (به دلیل محبوبیت بالای این دو ارز دیجیتالی) همواره در حال رشد است؛ چراکه این محبوبیت سبب می‌شود تا میزان تراکنش‌های انجام یافته در بستر چنین بلاک چینی افزایش یابد و ظرفیت بلاک‌ها سریعا تکمیل گردد و همین مسئله بر امنیت دفتر کل غیرمتمرکز می‌افزاید.

اصولا یکی از موانع اصلی موجود بر سر راه جهانی شدن استفاده از ارزهای دیجیتالی این بود که کاربران نمی‌توانستند سرمایه خود را به فرد دیگری بسپارند یا به بیان دیگر به او اعتماد کنند و همواره این سوال را می‌پرسیدند که چه تضمینی وجود دارد که این فرد سرمایه آن‌ها را ندزدد؟!

همین اشکال و عدم اعتماد سبب شد تا خالقان اولیه ارزهای دیجیتالی همچون بیت کوین به سمت طراحی نوع خاصی از پایگاه داده به نام بلاک چین، روی آورند؛ اما چرا نوع خاصی از پایگاه داده؟! پاسخ به این سوال ساده است و علت آن را می‌توان در ویژگی پایگاه داده‌های معمولی همچون پایگاه داده SQL جستجو کرد.

مطلب پیشنهادی : لایتنینگ بیت کوین

این پایگاه‌های داده معمولی دارای فردی مسئول است که می‌تواند ورودی‌ها را تغییر دهد ولی مسئله‌ای مشابه مورد گفته شده در بلاک چین بیت کوین وجود ندارد و این بلاک چین دارای فضایی متفاوت است؛ چراکه در بلاک چین بیت کوین، هیچ فردی مسئول انجام چنین کاری نیست و این پایگاه منحصرا به وسیله افرادی که از آن استفاده می‌کنند، اداره می‌شود.

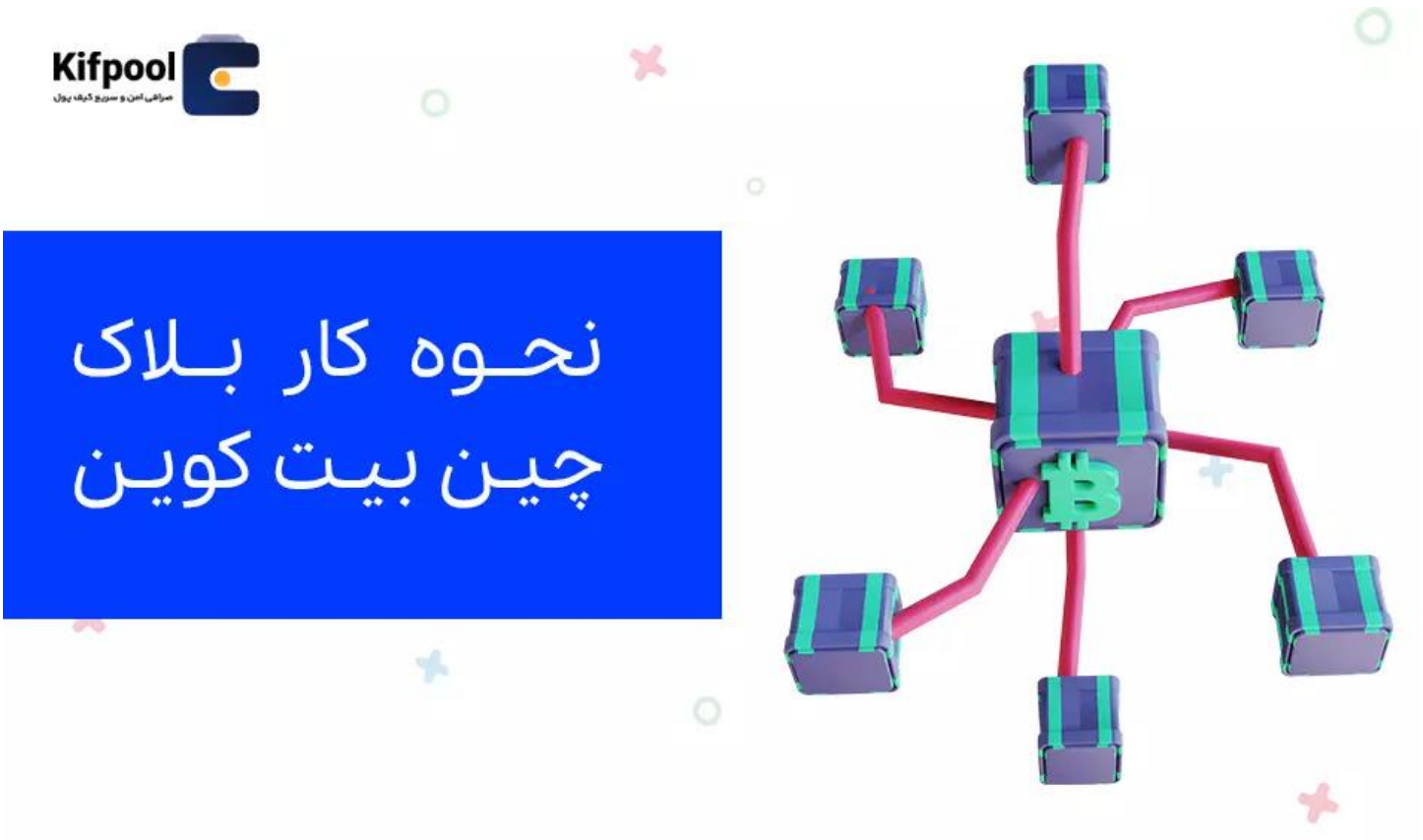
مروری بر ماهیت بیت کوین

حال که با خود اصطلاح بیت کوین آشنا شدید، ضرورت دارد که مروری بر خود بیت کوین، پادشاه رمزارزها، داشته باشیم تا تفاوت این دو مفهوم روشن‌تر گردد. بیت کوین در واقع یک رمزارز غیرمتمرکز بوده که در ژانویه سال 2009 ایجاد شده است.

هویت فرد یا افرادی که این ارز دیجیتال را خلق کرده‌اند همچنان به عنوان یک راز باقی مانده است. منظور از غیرمتمرکز بودن این ارز دیجیتالی این است که برخلاف ارزهای سنتی و فیات صادر شده از سوی دولت همچون دلار، از سوی یک پایگاه غیرمتمرکز اداره می‌شود و به بیان ساده‌تر هیچ دولت و بانکی بر آن نظارت نمی‌کند.

همان طور که گفته شد، بیت کوین یک ارز دیجیتال است و همان طور که از نام آن هم پیداست، یک ارز مجازی بوده و به صورت فیزیکی و ملموس چاپ نمی‌شود. این رمزارز در یک دفتر کل نگهداری می‌شود که به صورت عمومی در دسترس همه قرار دارد (هرچند که هر رکورد به صورت رمزگذاری شده است). تمامی تراکنش‌های بلاک چین بیت کوین به وسیله انجام حجم عظیمی از محاسبات موسوم به ماینینگ و استخراج، تائید می‌شوند.

نحوه کار بلاک چین بیت کوین



همان طور که به طور اجمالی در مطالب فوق مشاهده کردید، ارزهای رمزنگاری شده همچون بیت کوین به وسیله فناوری تحت عنوان بلاک چین اداره می‌شوند. در یک تصور ساده شاید بتوان چنین گفت که بلاک چین بیت کوین، لیستی از مجموع تراکنش‌هایی بوده که هر فردی قادر به مشاهده و تائید آن است و این فناوری به ارزهای دیجیتالی مثل بیت کوین قدرت می‌دهد تا امکان انتقال ارزش آنلاین را بدون نیاز به واسطه‌هایی نظیر بانک و شرکت کارت اعتباری، فراهم سازد.

جالب است بدانید که بلاک چین بیت کوین قادر است حدودا 7 تراکنش جدید را در ثانیه پرازش نماید که این مسئله این بلاک چین را با مشکل مقیاس‌پذیری مواجه کرده است.

مسئله مقیاس‌پذیری یکی از مشکلات اساسی موجود بر سر راه پذیرش عمومی ارزهای دیجیتالی بوده است؛ چراکه اگر روزی بیت کوین بخواهد به طور کامل جایگزین ارزهای فیات گردد، حتما بایستی در ثانیه، صدها هزار تراکنش را پردازش کند.

راه‌حلی که برای این مشکل ارائه شده، شبکه لایتنینگ (انجام تراکنش‌ها و تسویه حساب‌های خارج از زنجیره) است. این شبکه با تسریع زمان پردازش و همچنین کاستن از هزینه کارمزدها، این مشکل مقیاس‌پذیری بلاک چین بیت کوین را برطرف نموده است.

امنیت بلاک چین بیت کوین

به طور کلی، بلاک چین بیت کوین از هش رمزگذاری به منظور ایمن‌سازی داده‌ها کمک می‌گیرد و غالبا بر الگوریتم SHA256 برای چنین کاری تکیه می‌زند. به بیان دیگر، کلیه اطلاعات نظیر آدرس فرستنده یا همان کلید عمومی، آدرس گیرنده، تراکنش و در نهایت جزئیات کلید خصوصی از طریق الگوریتم SHA256 منتقل می‌گردد.

این اطلاعات رمزگذاری شده که در میان کاربران بلاک چین بیت کوین به رمزگذاری هش معروف است به نودهای موجود در سرتاسر جهان منتقل شده و پس از تائید، زنجیره بلوکی جدید اضافه می‌شود.

بلاک‌ها در بلاک چین بیت کوین نقش اساسی را ایفا می‌کنند و در واقع هر زنجیره در فضای بلاک چین بیت کوین از همین بلاک‌ها شکل گرفته است و آن‌ها حاوی کلیه اطلاعات مرتبط با یک تراکنش هستند.

ناگفته نماند که هر بلاک دارای یک nonce و هش منحصربه‌فرد است که نه تنها به صورت خطی ذخیره می‌شود، بلکه از نظر زمانی نیز همواره در انتهای بلاک چین قرار دارد که چنین امری، این مزیت اصلی و اساسی را با خود به همراه دارد که با افزایش تعداد زنجیره‌ها، بازگشت به عقب، دستکاری یا مختل کردن این زنجیره‌ها به عملی غیرممکن تبدیل می‌شود.

اصلی‌ترین تفاوت بلاک چین و بیت کوین

همان طور که در مطالب فوق مطالعه کردید، بلاک چین در واقع یک پایگاه داده بوده که وظیفه اداره و پردازش تراکنش‌های ارزهای دیجیتالی را برعهده دارد و این در حالی است که خود بیت کوین یک ارز دیجیتالی است.

انتقال بیت کوین به معنای انتقال یک رمزارز است و این انتقال بایستی حتما در بستر یک بلاک چین صورت گیرد؛ چراکه این بلاک چین است که وظیفه انتقال اطلاعات اختصاصی، دارایی‌های دیجیتال، حق مالکیت و مواردی نظیر موارد گفته شده را برعهده دارد.

مطلب پیشنهادی : ترید بیت کوین

یکی از اصلی‌ترین دلایل روی آوردن مردم به سمت ارزهای دیجیتالی، کسب اعتماد آن‌ها از سوی شبکه‌های بلاک چینی نظیر بلاک چین بیت کوین است و این امر برای تمامی کاربران دنیای کریپتوکارنسی به یک اصل مسلم درآمده است که با توجه به پیچیدگی‌های بلاک چین بیت کوین، عملا امکان هک آن وجود ندارد.

ناگفته نماند که اگر در ارتباط با بلاک چین بیت کوین سوالی دارید که در این مقاله از وبلاگ کیف پول من به آن اشاره نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.