



Arash Financial Academy

BLOCK CHAIN CONCEPTS

بلاک چین چیست؟

از دو واژه Block به معنی بلوک و Chain به معنی زنجیره تشکیل شده است و واژه بلاک چین به معنی زنجیره ای از بلوکهاست.



داده ها از جمله سوابق معاملات مالی که همواره در حال رشد هستند و به تعداد آنها اضافه به یکدیگر متصل (CRYPTOGRAPHY) میشود در بلاکها ثبت میشوند و از طریق رمزنگاری می شوند. رمزنگاری بر اساس الگوریتم های معمایی ریاضیات پیشرفته ایجاد شده است.

بلاک چین چیست؟



به عبارتی دیگر، بلاک چین به عنوان نوعی دفتر دیجیتالی کلی توزیع شده شناخته می شود که امکان مالکیت، کنترل و دستکاری شدن دیتاهای آن توسط فرد یا گروهی خاص امکان پذیر نیست زیرا اطلاعات ذخیره شده روی این نوع سیستم، میان همه اعضای شبکه به اشتراک گذاشته می شود و روی یک یا چند سرور مرکزی خاص ذخیره نمی شوند و این ویژگی غیر متمرکز بودن وجه تمایز اصلی بلاک چین با سایر سیستم های ذخیره اطلاعات می باشد در واقع تراکنشهای مالی انجام شده در بستر بلاک چین نیاز به تایید شخص ثالث ندارد.

گره یا Node چیست؟

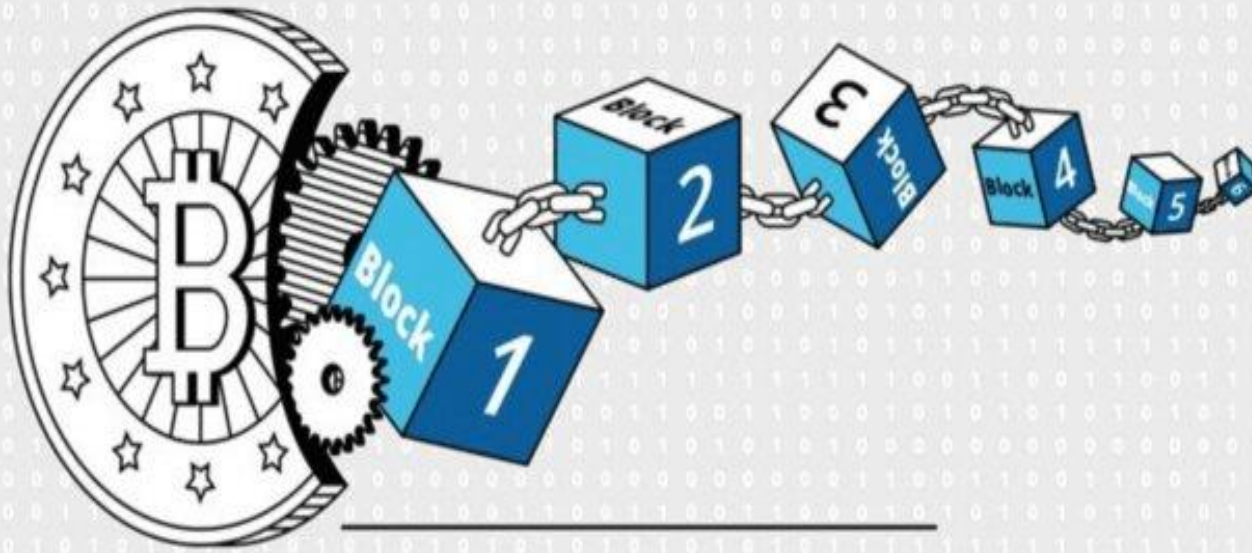
هر کامپیوتر یا سیستمی که به شبکه وصل شود، یک نسخه از اطلاعات را دریافت می کند. به هر کامپیوتری که به شبکه متصل می شود و یک کپی از بلاک چین را دریافت می کند، نود (Node) می گویند.

اگر اطلاعات در یکی از گره ها به هر دلیلی از بین برود تعداد بسیار زیادی سرور دیگر آن اطلاعات را در خود ذخیره کرده اند بنابراین یکی از مزایای بلاک چین امنیت بالای آن و اطمینان از عدم نابودی دیتاها می باشد.

بلاک چین در بیت کوین چگونه کار می کند؟

بیت کوین از بلاک چین به عنوان یک راهکار برای ذخیره اطلاعات مربوط به دارایی کاربران بهره برده است و در حال حاضر این رمز از معروف ترین کاربردهای بلاک چین است.

Bitcoin is based on a *distributed ledger* —
or rather a specific kind of distributed ledger: *a blockchain*.



Bitcoin's ledger was the first blockchain, but the technology has begun to spread across the global economy. The reason: blockchains let you keep thousands of strangers *honest and consistent*.

در واقع جهت استخراج بیت کوین و یا به روز رسانی اطلاعات در گره ها، بلاک چین بیت کوین از مکانیزم **PROOF OF WORK** به معنی اثبات کار (POW) استفاده می کند و هر کامپیوتری که به شبکه متصل باشد بر اساس قدرت پردازش خود، معادلات پیچیده شبکه را حل میکند و با حل این معماهای ریاضی، بلاکهایی از تراکنش های معتبر ایجاد و به بلاک چین متصل می کند. از آنجایی که این فرایند، رقابتی ست اولین نودی که معادله را حل کند، بیت کوین به عنوان پاداش دریافت می کند.

هش چیست؟

فرآیند رمزنگاری شبکه‌های بلاک چین با استفاده از سیستمی پیچیده صورت می‌گیرد که در نهایت امنیت شبکه را تامین می‌کند. هش در واقع یک تابع (عملگر) ریاضی است که از ورودی‌های متغیر، خروجی‌هایی با اندازه ثابت و رمزگذاری شده تولید می‌کند. این تابع، اعداد را یکی پس از دیگری در معادله امتحان می‌کند تا پاسخ معادله هر بلاک را به دست بیاورد. به این فرایند Hashing و به خروجی تابع هش، Hash گفته میشود. استخراج‌کنندگان باید به منظور دریافت پاداش، معادلات ریاضی بلاک چین را حل کنند که این کار نیاز به توان پردازشی بالایی دارد.



هش ریت چیست؟

مطابق سلاید قبل، متوجه شدیم که هش ، پاسخ یا خروجی تابع هش میباشد، پس هش ریت بیانگر میزان سرعتی ست که یک ماینر موفق به حل هش و دریافت جایزه میشود .

بنابراین هش ریت عددی ست که عملکرد دستگاه ماینر را برای استخراج ارز دیجیتال بر اساس واحد h/s (هش/ثانیه) اندازه گیری می کند و البته این واحد مانند تمامی واحد های اندازه گیری قابل تبدیل به واحد های بزرگتر و یا کوچکتر می باشد. مانند Th/s یا یک تریلیون هش بر ثانیه؛ معادل یک تراشه بر ثانیه

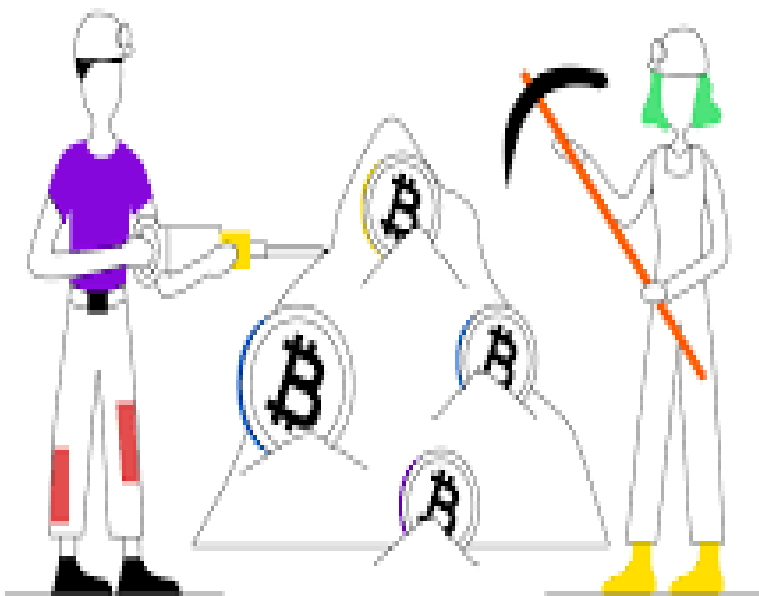
منظور از سختی شبکه یا Difficulty از چیست؟

Difficulty یا سختی در شبکه های بلاک چین پارامتریست که از افزایش تعداد کوین های استخراج شده در واحد زمان جلوگیری می کند و هدف آن ثابت نگه داشتن میانگین زمان ایجاد یک بلاک در شبکه به منظور جلوگیری از اثر تورمی در کوتاه مدت است.

به عنوان مثال :

زمان ایده آل ساخت هر بلاک طبق پروتکل بیت کوین ۱۰ دقیقه ست.

سختی شبکه بیت کوین هر دو هفته یک بار تغییر می کند تا زمان ایجاد هر بلاک به طور میانگین ۱۰ دقیقه باقی بماند. در صورتی که سختی شبکه وجود نداشته باشد، با وارد شدن ماینرهای بیشتر به شبکه، حدس هایی که درباره هش هر بلاک زده می شود نیز افزایش پیدا می کند. به دنبال افزایش تعداد حدس های زده شده، احتمال پیدا شدن هر بلاک در زمانی کمتر از ۱۰ دقیقه هم بیشتر می شود. بنابراین سختی شبکه یک عامل کنترل کننده ست که در صورت اضافه شدن تعداد زیادی ماینر به شبکه، مانع ماینرها از ایجاد بلاک در تایم کمتر از ۱۰ دقیقه بشود

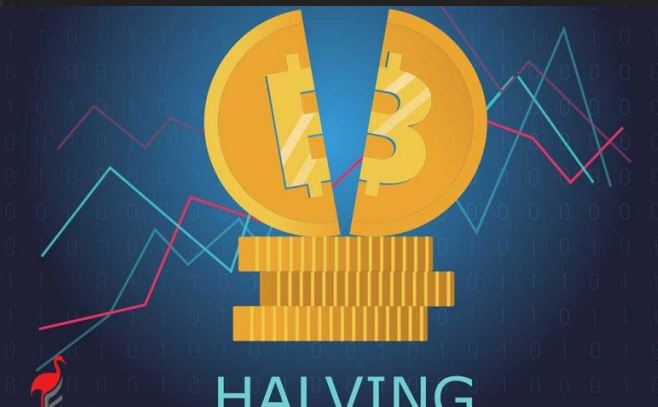


پاداش حل کردن بلاک :

مطابق سلاید قبل، استخراج کنندگان بیت کوین با استفاده از توان بالای پردازش دستگاههای استخراج (Minerها) به فرایند تایید تراکنش ها در شبکه بلاک چین کمک می کنند و در مقابل شبکه به ماینرها بیت کوین پاداش میدهد. این فرایند بر اساس الگوریتم اثبات کار (POW) و فرایند رمزنگاری (Hashing) انجام میشود و در عین حال چون از طریق فرایند Hashing انجام میشود، امنیت شبکه بیت کوین را حفظ می کند.



پاداش دریافتی ماینرها به منظور جلوگیری از تورم و ایجاد سریع بیت کوینها، هر ۴ سال یکبار یا هر ۲۱۰ هزار بلاک، نصف میشود و به این فرایند هاوینگ (HALVING) گفته میشود. به این ترتیب تعداد بیت کوین های در گردش، کنترل شده و از ارزش آنها به علت عرضه زیاد، کاسته نمی شود.



کارمزد ماینرها:

علاوه بر پاداشی که از ایجاد بلاکها و Hashing به ماینرها پرداخت می شود، اخذ کارمزد از کاربران، بابت تایید تراکنش ها، منبع درآمد دیگر ماینرها می باشد.

کارمزد تراکنش شبکه بلاک چین به منظور دو هدف اساسی به کار می رود. یکی اینکه این کارمزدها پاداشی برای ماینرها هستند و از طرفی شبکه را در برابر حملات اسپم محافظت می کند.

بر اساس فعالیت شبکه میزان کارمزد شبکه ممکن است کاهش یا افزایش یابد هم چنین عوامل موثر بر بازار ارز دیجیتال، بر میزان کارمزد تاثیرگذار است. این کارمزد در واقع مبلغی ست که به ماینرها جهت تایید تراکنش ها پرداخت میشود.

کارمزدی که در حین ارسال تراکنش توسط ارسال کننده بیت کوین تعیین می شود، مشخص کننده اولویت تراکنش هایی است که در بلاک ۱ مگابایتی قرار می گیرند و از آنجایی که ماینرها، تراکنش ها را برحسب میزان کارمزدشان اولویت بندی می کنند، تراکنش هایی که کارمزد کمتری دارند اولویت پایینی برای تایید پیدا می کنند.