

در: بیت‌کوین و ارزها:

• بیت‌کوین:

یادتان باشد که هرگز بیت‌کوین را با بلاک‌چین، اشتباه نگیرید. بسیاری از افراد این دو مفهوم را به جای هم استفاده می‌کنند. پس همین حالا به خاطر بسپارید که بیت‌کوین چیزی نیست جز یک ارز دیجیتال که فناوری بلاک‌چین کار می‌کند.

(درباره بیت‌کوین بیشتر بخوانید)

• بلاک‌چین:

بلاک‌چین نوعی فناوری است که به انتقال دارایی‌های دیجیتالی نظیر بیت‌کوین از فردی به فرد دیگر کمک می‌کند.

پس مفهوم دقیق بلاک‌چین چیست؟

برای درک بیشتر بهتر است به مثالی توجه کنید که نمونه‌ای از راهکارهای بلاک‌چین را ارائه می‌کند. در این مثال به مقوله انتقال پول پرداخته خواهد شد.

فرض کنید که بهرام می‌خواهد به سپیده، مبلغی پرداخت کند. به طور معمول و سنتی، این تراکنش از طریق طرف ثالثی مانند بانک یا کارت اعتباری صورت می‌گیرد. حال اگر این افراد در ۲ شهر متفاوت نیز به سر تراکنش کمی به طول می‌انجامد. ضمن اینکه مبلغی نیز از طرف ثالث معامله که بانک است، برداشته می‌شود.

تمام تلاش سیستم بلاک‌چین، این است که طرف ثالث در تراکنش‌ها را حذف کند. بنابراین بسیاری از معاملات و تراکنش‌ها بسیار سریع‌تر از گذشته و بدون هیچ‌گونه واسطه‌ای انجام خواهند شد. علاوه بر زمان، برای استفاده از شخص و طرف ثالث پرداخت می‌شد نیز به کمک بلاک‌چین بسیار کمتر خواهد بود.

برای شرح چگونگی انجام عملیات انتقال از جانب سیستم بلاک‌چین، نیاز به شناخت مفاهیم پیچیده بسیاری وجود دارد که در ادامه به تعدادی از آنها پرداخته شده است:

لِجِر (Ledger)

لجر به مجموعه‌ای از حساب‌های شماره‌گذاری شده برای ثبت حساب‌های هر شرکت گفته می‌شود. لجر در طول حیات شرکت، تمام تراکنش‌های مالی را به ثبت می‌رساند و اطلاعات محاسباتی را فراهم می‌کند. اد برای ترازنامه‌های مالی نظیر: حساب دارایی‌ها، بدهی‌ها، سرمایه، درآمد و مخارج مورد نیاز است. به عبارت ساده‌تر، لجر زنجیره‌ای است که تراکنش‌های مالی مختلف را به هم مرتبط کرده و آنها را در کنار هم ثبت اصطلاح لجر باز (open ledger) نیز به معنای این است که هر کسی می‌تواند به این شبکه باز، بپیوندد و تمام تراکنش‌ها نیز در لجر به ثبت می‌رسند. شبکه، تمام داده‌های حاصل از تراکنش را در حافظه یا لجر می‌کند. لجر توزیع‌شده یا همان دفتر کل توزیع‌شده اساساً مانند لجر باز عمل می‌کند. تفاوت اصلی این است که لجر توزیع‌شده مانند لجر باز متمرکز نیست. تمرکززدایی در لجر توزیع‌شده به این معنا است که در ش دارای نسخه‌ای کپی از لجر روی گره است.

حال نیاز به شرح اصطلاح دیگری پیش می‌آید.

گره (Node) چیست؟

Node یا گره، به مفهوم همان دستگاهی هست که هر مشارکت‌کننده در شبکه داراست و یک کپی از لجر باز را در اختیار دارد.

ما از اصطلاح “گره”، به عنوان تعریفی از یک مشارکت‌کننده در زنجیره دفترکل توزیع شده استفاده می‌کنیم (یک مشارکت کننده در شبکه)

لجر باز (Open Ledger)

برای اینکه شرح دقیقی از این مفهوم در اختیارتان قرار بگیرد، بهتر است به مثالی دیگر توجه کنید. فرض کنید شبکه‌ای با ۴ عضو وجود دارد: بهرام، سپیده، شایان، داریوش. هر کس در این شبکه خواهان دریافت است. در آغاز شکل‌گیری این شبکه، بهرام دارای ۲۰ دلار است.

مفهوم و کاربرد لجر باز در اینجا به این صورت خواهد بود.

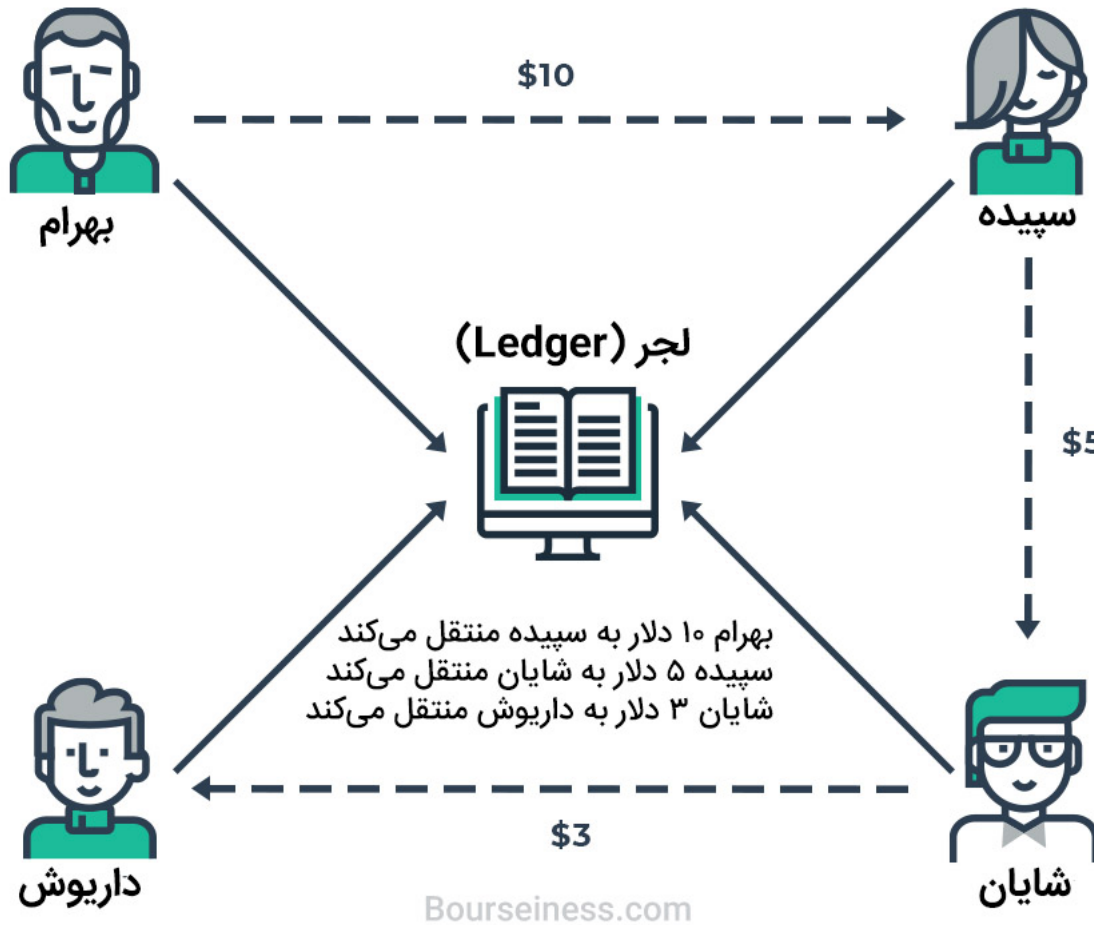
فرض کنید که تراکنش‌هایی میان اعضای شبکه رخ داده است:

- بهرام ۱۰ دلار به سپیده داده است.
- سپیده، ۵ دلار به شایان داده است.
- شایان نیز ۳ دلار به داریوش تحویل داده است.

تمام این تراکنش‌ها ثبت و به تراکنش‌های قبلی موجود در لجر، پیوند داده می‌شوند. یعنی در این مثال ۴ پیوند تراکنش در زنجیره لجر باز وجود دارد که اطلاعات نوع تراکنش و افرادی که در آن دخیل بوده‌اند، می‌گذارد.

Open "Centralized" Ledger

دفترکل (Ledger) باز و متمرکز



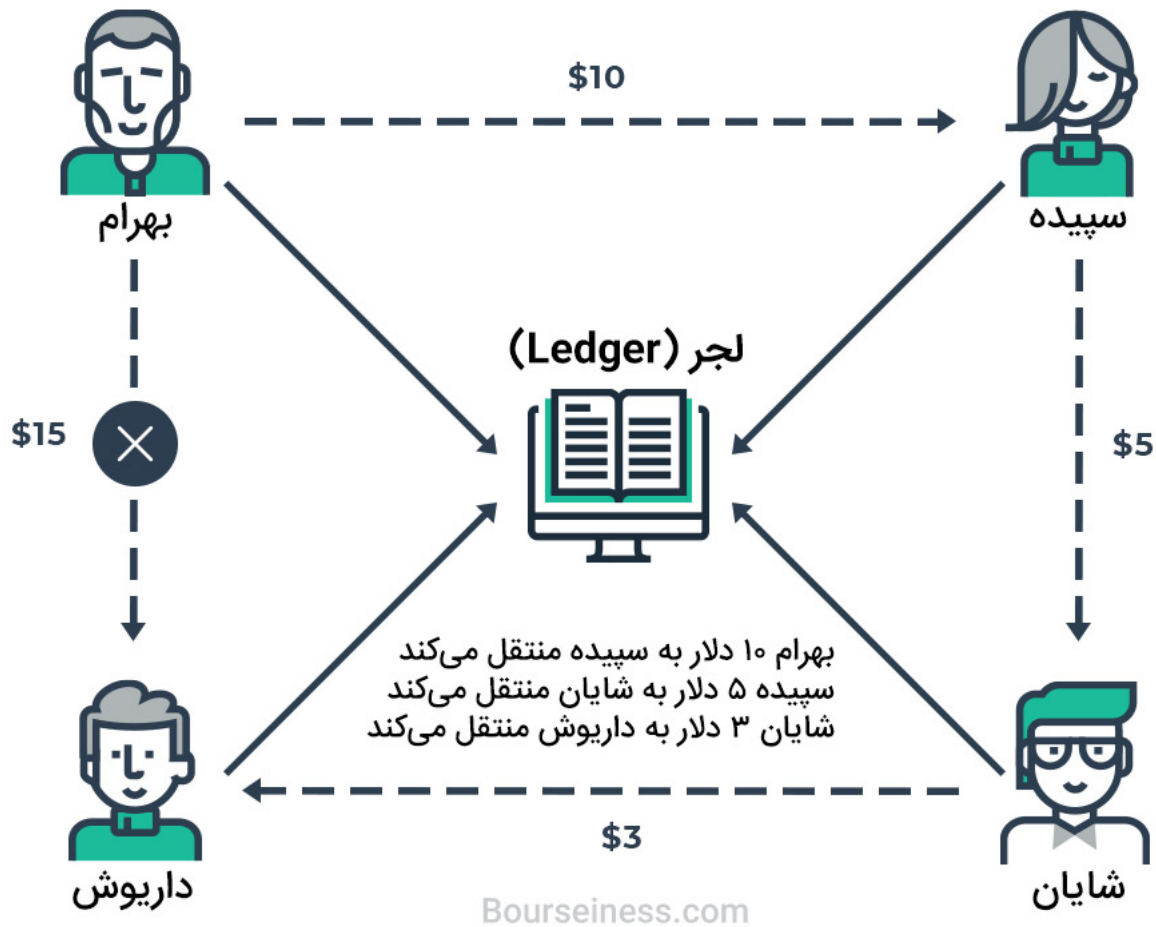
زنجیره تراکنش‌ها در لجر باز، مشخص و برای همه قابل دیدن و دسترسی است. یعنی همه اعضای شبکه می‌توانند از جای پول و مبلغی که هر شخص دارد، باخبر بشوند. علاوه بر این‌ها، هر عضو لجر باز، می‌تواند بودن یا نبودن تراکنش‌ها تصمیم بگیرد.

اجازه بدهید دوباره به مثال قبل اشاره کنیم.

در مثال عنوان‌شده، بهرام ۲۰ دلار در شروع کار داشت و ۱۰ دلار به سپیده منتقل کرد. بنابراین ۱۰ دلار برای بهرام باقی می‌ماند. حال، او تصمیم می‌گیرد که ۱۵ دلار دیگر به داریوش منتقل کند.

Open "Centralized" Ledger

دفترکل (Ledger) باز و متمرکز



در نتیجه، هر کس در شبکه می‌تواند متوجه نامعتبر بودن این تراکنش بشود زیرا پول باقی‌مانده برای بهرام، کفاف چنین تراکنشی را نمی‌دهد. بنابراین چنین تراکنشی به زنجیره تراکنش‌ها در لجر باز اضافه نخواهد شد.

لجر توزیع‌شده (Distributed Ledger)

یکی از مهم‌ترین اهداف فناوری بلاک‌چین ایجاد سیستمی غیرمتمرکز است. مفهوم تمرکززدایی زنجیره ارتباطات، لجر توزیع‌شده نام دارد. به زبانی دیگر، هر شخص یا گروه در شبکه، یک کپی از لجر دریافت می‌کند. سپیده، شایان و داریوش نیز مشارکت‌کنندگان در یک شبکه هستند، هرکدام یک نسخه کپی از لجر دریافت می‌کنند.

وقتی لجر در سطح شبکه توزیع می‌شود، هر عضو شبکه می‌تواند از زنجیره تراکنش‌های صورت گرفته اطلاع داشته باشد. پس در واقع، تمرکزگرایی موجود در لجر باز، در لجر توزیع‌شده، از بین می‌رود.



به عبارتی دیگر، همان شخص ثالثی که در معاملات و تراکنش‌های مختلف حضور داشت، اکنون در چنین سیستمی حضور نخواهد داشت.

البته مشکل جدیدی در اینجا شکل می‌گیرد. زیرا هر عضو شبکه دارای نسخه‌ای کپی از لجر است و در صورت هماهنگ نبودن لجر اعضا با هم، اشکالاتی پیش خواهد آمد. برای حل این مشکل، اجازه دهید مفهوم تکنولوژی بلاک‌چین با نام ماینینگ یا استخراج را شرح دهیم.

استخراج کردن (mining)

حال به خوبی می‌دانید که لجر توزیع شده، شبکه‌ای باز با قابلیت دسترسی عمومی است. نسخه کپی لجر در میان تمام گره‌های (اعضای) موجود در شبکه پخش می‌شود. اما اعتبار تراکنش‌های شبکه، چگونه تأیید باز بهتر است به مثال عنوان شده بازگردید.

فرض کنید که بهرام می‌خواهد ۱۰ دلار به سپیده منتقل کند. وقتی این تراکنش صورت می‌گیرد، به صورت خودکار، تراکنش صورت گرفته در سطح شبکه منتشر می‌شود. پس همه اعضا از وقوع چنین تراکنشی باخ ولی اعتبار آن هنوز به تأیید نرسیده است. تا تأیید تراکنش، این انتقال در لجر به ثبت نخواهد رسید. برای اینکه هر تراکنش در لجر تأیید و ثبت بشود، لازم است تا با اصطلاح دیگری به نام استخراج یا ماینینگ

ماینینگ برای حل محاسبات است. کسانی که وظیفه انجام این استخراج و اصطلاحاً ماینینگ را بر عهده دارند، گره‌ها یا اعضای ویژه هستند و می‌توانند به علت عمومی بودن لجر، وظیفه خود را در تمام شبکه ا،

مثلاً فرض کنید، شایان و داریوش هر دو از گره‌های خاص (مایرها) هستند. آنها وظیفه‌ای بسیار مهم بر عهده دارند. البته لازم به ذکر است که تمام استخراج‌کنندگان یا ماینرها با هم رقیب هستند.

در این مثال، شایان و داریوش هر دو با هم بر سر تأیید اعتبار تراکنش صورت گرفته از سوی بهرام و انتقال پول به سپیده رقابت می‌کنند. هر یک از آنها در تلاش است تا زودتر این تراکنش را تأیید کرده و به زنج کند. کسی که زودتر بتواند این کار را انجام دهد، امتیاز و پاداش دریافت خواهد کرد.

مثلاً اگر از این سیستم برای یک تراکنش بیت‌کوین استفاده بشود، پاداش و امتیازی که به ماینر داده می‌شود، بیت‌کوین خواهد بود.

مفهوم اینکه بیت‌کوین چگونه تولید می‌شود کمی پیچیده است. اما به طور مختصر باید گفت که بیت‌کوین از طریق فرایند محاسباتی تأیید تراکنش تولید می‌شود و نه از طریق پرداخت مستقیم بهرام و سپیده.

مطلب مرتبط: استخراج بیت کوین چیست؟

مایرها برای بردن رقیب باید ۲ گام را پشت سر بگذارند:

قدم اول – تأیید تراکنش جدید:

تأیید تراکنش تازه بسیار آسان است زیرا اطلاعات موجود در لجر در دسترس هستند. بنابراین، ماینر سریعاً می‌تواند با انجام محاسبات اعلام کند که فردی که تراکنش را آغاز کرده، بودجه کافی در دست داشته یا با این محاسبه، درمی‌یابد که تراکنش معتبر است یا غیرمعتبر.

قدم دوم – یافتن «کلید» مخصوص:

برای قفل کردن تراکنش جدید در زنجیره لجر، ماینر باید کلیدی مخصوص بیابد که این فرایند را فعال می‌سازد. کلیده‌ها به طور تصادفی امتحان می‌شوند. ماینرها باید از قدرت محاسباتی برای یافتن کلید مناسب کلیده‌ای تصادفی استفاده کنند که البته زمان زیادی می‌گیرد. پس لازم است از قدرت رایانه برای حدس کلیده‌ای تصادفی استفاده بشود. پس کسی که بتواند سریع‌تر این فرایند را به سرانجام برساند، برنده رقابت دیگر خواهد بود و امتیاز و جایزه را در قالب‌های مختلف (مثلاً بیت‌کوین) دریافت خواهد کرد.

لجرها چگونه در طول شبکه، همگام‌سازی می‌شوند؟

پرسش مهمی در اینجا پیش می‌آید. هر گره چگونه می‌تواند، تراکنش‌های صورت‌گرفته را به شکل همگام با آخرین تغییرات دریافت کند؟ این موضوع بسیار مهم است زیرا مشکل داشتن کپی یکسان از لجر را در شبکه برطرف می‌کند. مثلاً فرض کنید که داریوش توانست در رقابت با شایان، تراکنش را زودتر به تأیید برساند. بنابراین، تراکنش زودتر در لجر او به ثبت رسید. حال او باید نتیجه‌ای که حاصل کرده را در تمام شبکه سازد.

این موضوع به این معناست که او باید به شایان، سپیده و داریوش اطلاع دهد که معما را حل کرده و تراکنش را تأیید نموده است (تراکنشی که بهرام قصد داشت به سپیده ارسال کند)

وقتی این تراکنش از سوی داریوش (استخراج‌کننده موفق) به همه اطلاع‌رسانی شد، او باید کلیدی فراهم کند تا سایر اعضای گره را قادر سازد تا تراکنش را به لجرهای‌شان اضافه کنند.

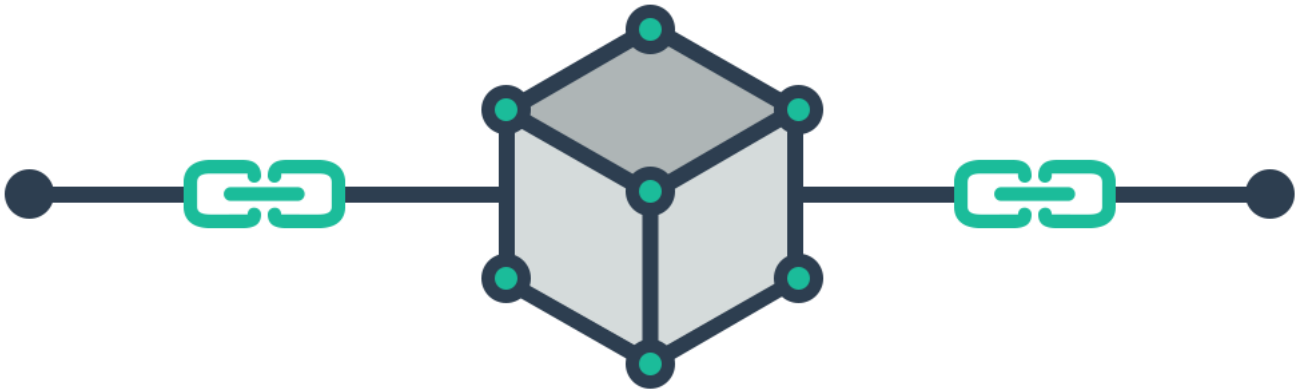
شایان (استخراج‌کننده دیگر) نیز این تراکنش را به لجر خود اضافه می‌کند، زیرا دیگر نیازی به نهایی کردن و تأیید آن تراکنش نیست، زیرا تأیید تراکنش توسط داریوش انجام گرفته و پاداش آن نیز به داریوش است. البته شایان می‌تواند در جستجوی تأیید تراکنش‌های دیگر باشد تا از این طریق پاداش استخراج مربوط به آنها را بدست آورد.

در نتیجه این فرایند، این تراکنش به لجر سایر افراد شبکه نیز اضافه می‌شود. سپیده نیز ۱۰ دلاری که بهرام برای وی ارسال کرده را دریافت می‌نماید، زیرا همه افراد موجود در شبکه به اتفاق پذیرفته‌اند که این تراکنش تأیید است.

در این هنگام، همه لجرهای توزیع شده در شبکه، بروزرسانی شده و زنجیره‌های تراکنش‌ها در همه آنها به شکلی مشابه و یکسان وجود دارد.

بلاک‌های موجود در زنجیره چیست؟

حال که کمی با مفاهیم اولیه در توضیح فناوری بلاک‌چین آشنا شده‌اید، بهتر است دقیق‌تر این موضوع را پیگیری کنید. تا اینجا کار درک کرده‌اید که با زنجیره‌ای از بلاک‌ها (بلوک‌ها) رو به رو هستید.



هر بلاک در زنجیره شامل داده‌های خاصی است:

۱ – داده

نوع داده ذخیره شده در بلاک وابسته به نوع بلاک‌چین است. برای مثال، هر بلاک در بلاک‌چین بیت‌کوین، اطلاعاتی مانند تعداد بیت‌کوین‌ها در بلاک را ذخیره می‌کند. یعنی مشخص می‌شود که چه کسی بیت و چه کسی آن را دریافت کرده است. اگر بلاک‌چین به کریپتوکارنسی دیگری مثل اتریوم تعلق داشته باشد، اطلاعات بلاک به جای بیت‌کوین درباره اتریوم خواهد بود.

۲ – هَش (hash)

هَش می‌تواند به این شکل باشد:

۸۲e۳۵a۶۱۳ceba۳۷e۹۶۵۲۳۶۶۲۳۴c۵dd۴۱۲ea۵۸۶۱۴۷۷۱e۴a۴۱ccde۱۶۱۴۹۲۳۸۱۸۷e۳dbf۹

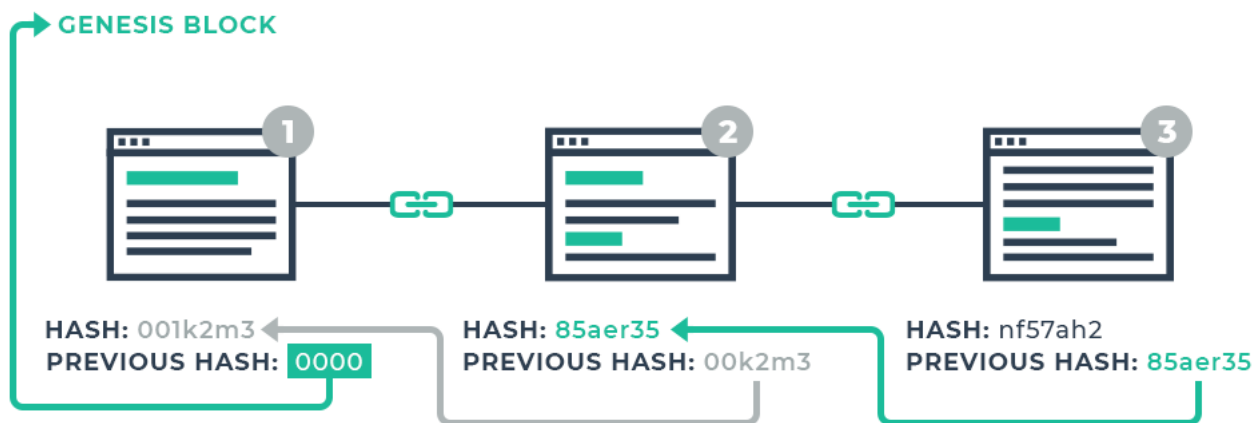
هر هَش کاملاً منحصر‌بفرد است و دربردارنده رشته‌ای از اعداد و حروف است. رشته منحصر‌بفرد اصولاً دربردارنده اطلاعات محتوایی است که در بلاک ذخیره می‌شود. وقتی یک بلاک ایجاد می‌گردد، هَش منحصر تولیدشده مورد محاسبه قرار می‌گیرد. با تغییر هر چیزی در بلاک (مثلاً کاهش تعداد بیت‌کوین‌ها)، هَش نیز تغییر می‌کند. به عبارت دیگر، وقتی هَش دچار تغییر می‌شود دیگر بخشی از بلاک پیشین نخواهد بود. بلاکی جدید تشکیل می‌شود.

۳ – هَش بلاک قبلی

هر بلاکی که تازه ایجاد می‌شود نیز حاوی رشته هَشی منحصر‌بفرد مربوط به بلاک قبلی است. به این صورت، تمام بلاک‌ها با هم مرتبط می‌شوند.



همانطور که در مثال زیر مشاهده می‌کنید، هر بلاک با عنوان کردن هاش بلاک قبلی، به آن بلاک متصل است.



اولین بلاک شامل هاش قبلی نمی‌شود زیرا بدیهی است که قبل از آن بلاکی وجود ندارد. اولین بلاک موجود در زنجیره، جنسیس بلاک (Genesis block) نام دارد.

امنیت بلاک‌چین چگونه است؟

اگر کسی درصدد ایجاد تغییری در بلاک باشد، هاش تغییر خواهد کرد. یعنی تمام بلاک‌های بعدی نیز نامعتبر می‌شوند. زیرا دربردارنده هاشی متفاوت نسبت به هاش تازه ایجاد شده است. برای رفع مشکل نامعتبری بلاک‌های دیگر تمام هاش‌های بلاک دیگر باید دوباره محاسبه بشوند. برای مواجهه با چنین مشکلی، داده‌ای به نام «اثبات کار» وجود دارد که تولید بلاک‌های جدید را آهسته می‌کند. دشواری ایجاد بلاک‌های جدید ماینرها کنترل می‌شود به همین خاطر، زمان لازم برای حل هر محاسبه و ایجاد بلاکی جدید تنها ۱۰ دقیقه طول می‌کشد.

لایه دیگری که در امنیت بلاک‌چین وجود دارد، شبکه همتا به همتا (P2P یا Peer to Peer Network) است. وجود شبکه P2P باعث ایجاد اطمینان نسبت به این موضوع می‌شود که بلاک‌چین در بین یک ش توزیع شده است. همان‌طور که قبلاً هم گفته شد، بلاک‌چین شبکه‌ای عمومی است که عضویت در آن برای همه آزاد است و با ورود به آن نسخه‌ای کپی از بلاک‌چین به هر عضو داده می‌شود.

با تشکیل هر بلاک جدید، (همانند تصویر زیر) یک نسخه از بلاک‌چین برای همه اعضا (Nodes) فرستاده خواهد شد.



بنابراین، هر گره از هر عضو در شبکه، بلاک‌های جدید را بررسی خواهد کرد و مشخص می‌کند که بلاک معتبر است یا نه. اگر بلاک تأیید بشود، هر گره (Node) آنرا به بلاک‌چین اضافه خواهد کرد. اگر تمام گره‌ها بلاک‌چینی مشابه باشند، به این معنی است که توافقی عمومی برای پذیرش آن بلاک‌چین به عنوان بلاک‌چین رسمی وجود دارد و بلاک‌چین‌های نامعتبر از اضافه شدن به بلاک‌چین منع خواهند شد.

در مورد امنیت، اگر بخواهید در یک بلاک‌چین مداخله کنید و آنرا تغییر دهید، باید تمام بلاک‌های بلاک‌چین عوض بشود، تمام هش‌ها دوباره محاسبه بشوند، برای «اثبات کار» جایگزینی بیابید و از همه مهم‌تر کنترل بیش از ۵۰ درصد شبکه P2P را بدست آورید. در غیر این صورت، اصلاحات و تغییراتی که روی بلاک‌چین انجام می‌دهید از سوی سایر اعضای شبکه مورد قبول واقع نخواهد شد.

طبیعی است که انجام چنین کاری تقریباً غیرممکن است و این موضوع را می‌رساند که امنیت بلاک‌چین به طور کلی بسیار بالا است.

خلاصه تکنولوژی بلاک‌چین

ابتدا فرا گرفتیم که بلاک‌چین و بیت‌کوین دو چیز کاملاً مجزا هستند. به علاوه، فهمیدیم که تکنولوژی بلاک‌چین براساس چندین اصول اولیه و پایه‌ای است.

۱ – دفترکل توزیع شده (distributed ledger) یک شبکه باز است که عموم به آن دسترسی دارند.

۲ – هر مشارکت‌کننده در شبکه می‌تواند تایید کننده تراکنش‌ها باشد.

۳ – دفترکل (لجر) در بین مشارکت‌کنندگان (Node) های زیادی توزیع شده است (این ویژگی باعث حذف شخص ثالث و واسط می‌شود).

۴ – مفهوم ماینینگ و نقش ماینرها، تایید تراکنش‌هایی است که در لجر انجام می‌شود و اینکار از طریق محاسبات ریاضی صورت می‌گیرد.

ماینرها، مشارکت‌کنندگانی در شبکه هستند که وظیفه‌شان تایید تراکنش‌های موردنظر، حل محاسبات و انتشار و به اشتراک‌گذاری آنها در شبکه است تا همه بتوانند این تراکنش را به دفترکل در زنجیره اضافه کنند.

ماینرها تلاش می‌کنند معماهای ریاضی را حل کنند. اینکار به مشارکت‌کنندگان در شبکه این اطمینان را می‌دهد که زنجیره جدید در دفتر کل رسمی ایجاد شده و همه افراد شبکه باید از آن استفاده کنند.

همچنین فرا گرفتیم که هر بلاک در بلاک‌چین دارای ۳ نوع داده است:

۱ – داده

۲ – هش

۳ – هش بلاک قبلی

البته چیزی که در هر بلاک نگهداری می‌شود بستگی به بلاک‌چین دارد. یک مثال این است که هر بلاک‌چین بیت‌کوین، هر بلاک شامل اطلاعاتی درباره بیت‌کوین است.

ما همچنین یاد گرفتیم که هر بلاک شامل یک سری از اعداد و حروف تصادفی است که "هش" نامیده می‌شود. هش، اطلاعات مرتبط با آن بلاک را در خود دارد، بنابراین هر زمان اطلاعاتی در بلاک تغییر کند، هش می‌کند.

برای اتصال بلاک‌ها به یکدیگر، هر بلاک، هش بلاک قبلی را در خود دارد. فقط اولین بلاک (جنسیس بلاک) است که شامل هش بلاک قبلی نیست (چون بلاک قبلی وجود ندارد).

آموزش بلاک‌چین

با گسترش روزافزون این تکنولوژی و علاقه شرکت‌ها و کسب و کارها به این زمینه، کسانی که مایلند در این حوزه بسیار تخصصی فعال باشند بهتر است منابع آموزشی زبان انگلیسی را دنبال کنند. به دلیل تغییرات حوزه، می‌توان با شرکت در دوره‌های آنلاین پایگاه‌های بروز که بطور تخصصی برای آموزش بلاک‌چین فعال هستند، از سایرین جلو افتاد.

سایت Blockgeeks یکی از سایت‌هایی است که دوره‌های آنلاین آموزش تخصصی بلاک‌چین را برگزار می‌کند: مشاهده دوره‌های blockgeeks

بطور کلی، پیاده‌سازی بلاک‌چین دارای جزئیات بسیار زیاد و دارای پیچیدگی زیادی است. ما در این مطلب تلاش کردیم بسیاری از سوالات اولیه شما در مورد بلاک‌چین را پاسخ دهیم.

