مقالات آموزشی بنیاد سور

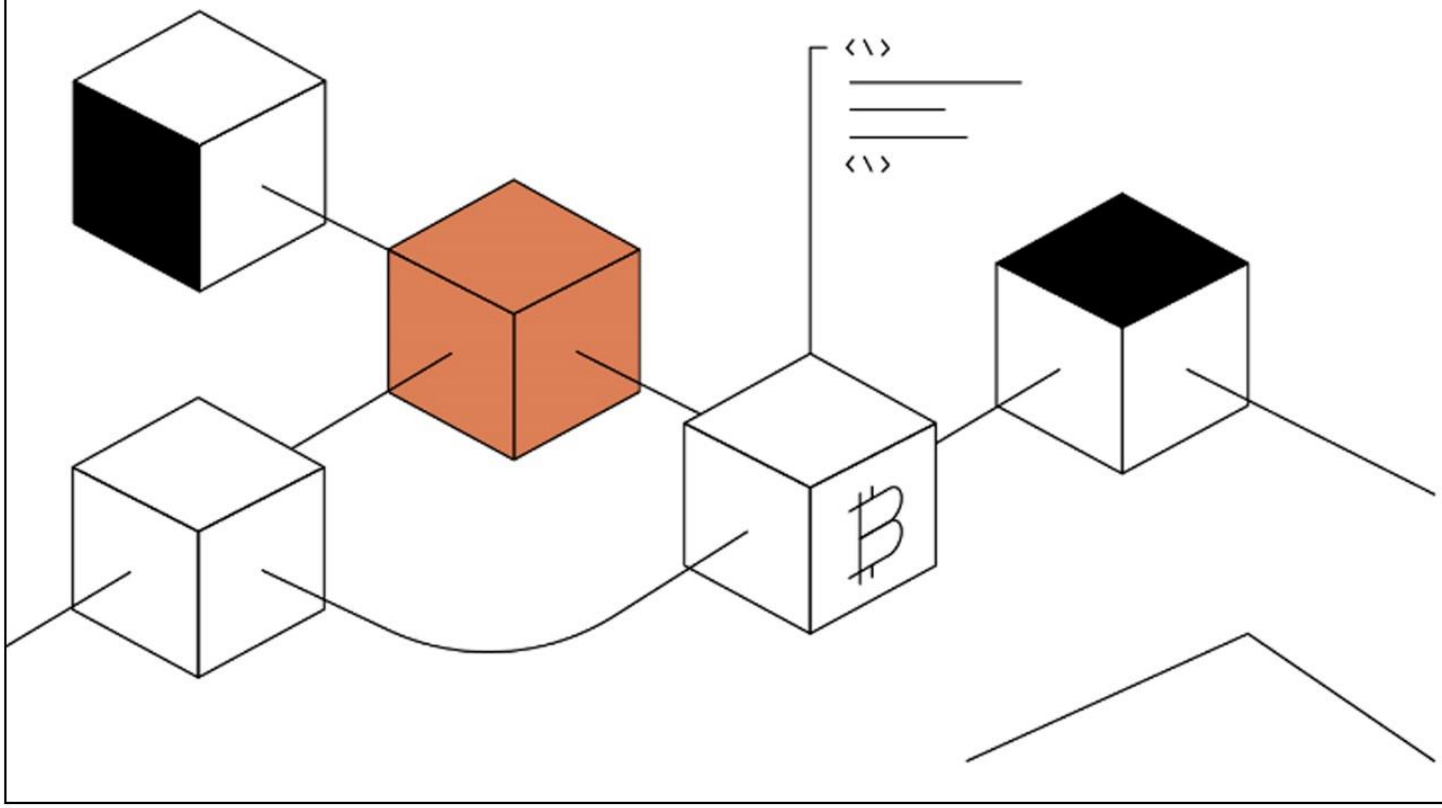
عنوان:

بررسی چیستی فناوری زنجیره بلوک

گردآورنده: بنیاد سور

نسخه: شماره سوم

شبکه بلاکچین سور
www.surnet.org



بررسی چیستی فناوری زنجیره‌بلوک

مقدمه

امروزه کمتر کسی هست که نام بیت‌کوین و زنجیره‌بلوک را نشنیده باشد. این دو پدیده که گاهی باهم اشتباه گرفته می‌شوند با ظهور خود نویدبخش انقلابی بزرگ در نظام اقتصادی و اجتماعی جهانی شدند. برای تفکیک این دو پدیده که رابطه تنگاتنگی باهم داشته و هم‌زمان ارائه شده‌اند باید گفت که بیت‌کوین یک رمزارز[1] است که بر بستر زنجیره‌بلوک ارائه شده است و زنجیره‌بلوک را می‌توان یک دفتر ثبت مرکزی که سوابق (تراکنش‌ها، اطلاعات فردی، حساب‌ها و به‌مانند آن) در آن به‌صورت کاملاً امن، شفاف، در دسترس و موردتوافق اعضا ثبت می‌شود در نظر گرفت که در بخش بعد به‌طور کامل چیستی آن تبیین خواهد شد. سامانه‌های مبتنی بر زنجیره‌بلوک به‌طورکلی به دودسته نیازمند تائید[2] و بدون نیاز به تائید[3] تقسیم می‌شوند. دسته اول که در آن هر عضو برای ورود نیاز به تائید یک‌نهاد ناظر (بانک و غیره) دارد بیشتر موردتوجه بانک‌ها و نهادهای دولتی و دسته دوم که برای ورود به آن نیازی به اخذ تأییدیه نیست و در پروتکل بیت‌کوین هم از آن استفاده می‌شود موردتوجه توسعه دهندگان رمزارزهای جدید قرار گرفته است. دسته اول به‌مانند سامانه‌های رایج امروزی، تائید اعتبار، صحت‌سنجی اسناد و تراکنش‌ها و غیره را به یک یا چند نهاد عالی‌رتبه مورداعتماد واگذار می‌کند؛ اما در دسته دوم، تصمیم‌گیری غیرمتمرکز بوده و همه اعضا در تائید هر تراکنش دخیل هستند. روش‌های مختلفی برای رسیدن به توافق در این دسته از زنجیره‌بلوک‌ها وجود دارد که در بخش‌های بعد به‌تفصیل بررسی خواهند شد. ماهیت شفاف، امن، قابل ردگیری و بر پایه دموکراسی (زنجیره‌بلوک بدون نیاز به تائید) زنجیره‌بلوک، این پدیده را برای هر صنعتی جذاب و قابل پیاده‌سازی کرده است. تقریباً تمامی فعالیت‌های اقتصادی، سیاسی و اجتماعی امروزی نیازمند مواردی که در بالا به آن اشاره شد هستند که در بخش آخر به بیان این نیازها و نحوه رفع آن‌ها توسط زنجیره‌بلوک در قالب کاربردهای زنجیره‌بلوک پرداخته خواهد شد.

چیستی زنجیره‌بلوک

برای درک بهتر چیستی زنجیره‌بلوک لازم است که با چهار ایده و مفهوم کلیدی مرتبط با آن آشنا شد تا بتوان تعریفی دقیق‌تر و جامع‌تر از آن ارائه داد. در واقع زنجیره‌بلوک چیزی فراتر از ادغام این مفاهیم نیست. این چهار مفهوم عبارت‌اند از: دفتر ثبت مشترک توزیع‌شده[4]، رمزنگاری[5]، اجماع[6] و قرارداد هوشمند که به ترتیب به تبیین چیستی آن‌ها پرداخته می‌شود.

دفتر ثبت مشترک توزیع‌شده

دفتر ثبت، به عنوان پایه و اساس حسابداری، قدمتی به عمق نوشتن و پول دارد. از همان ابتدا که بر روی سنگ و چوب و لوح نوشته می‌شد تا به امروز که بر روی کاغذ نوشته یا به‌صورت مجازی در کامپیوترها ذخیره می‌شود، هر شخص، نهاد یا شرکت برای خود یک دفتر ثبت جداگانه به‌منظور ثبت تمام تراکنش‌های خود در نظر داشته است. چنین روشی خالی از اشکال هم نیست. به‌طور مثال برای ثبت یک تراکنش بانکی چندین شرکت و نهاد درگیر، هرکدام، با دفتر ثبت شخصی خودشان، باید تراکنش را رصد، با سوابق مطابقت و تائید کنند که مسلماً

---

[1] Cryptocurrency

[2] Permissioned

[3] Permission-less

[4] Distributed Shared Ledger

[5] Cryptography

[6] Consensus

علاوه بر هزینه بالا زمان‌بر نیز هست. همچنین در صورت ازکارافتادن یکی از تائیدکنندگان کل سامانه از کار افتاده و ثبت تراکنش به تعویق می‌افتد. به تمامی این‌ها امکان هک شدن را هم باید افزود. این مشکلات به‌همراه افزایش قدرت رایانه‌ها، ظهور پدیده رمزنگاری و توسعه روش‌های اجماع باعث مطرح‌شدن پدیده‌ای به نام دفتر ثبت مشترک توزیع‌شده گردیده است.

دفتر ثبت مشترک توزیع‌شده یک پایگاه داده است که توسط گره‌ها[7] (اعضای شبکه) در یک شبکه بزرگ به‌صورت مستقل نگهداری و به‌روز می‌شود. کار اصلی این گره‌ها رسیدن به توافق بر سر درستی یک تراکنش و ثبت آن در دفتر ثبت مشترک است. زنجیره‌بلوک را می‌توان این دفتر ثبت مشترک دانست و هر بلوک را یک صفحه از آن. چند تراکنش که توسط گره‌ها صحت‌سنجی، تائید شده در هر بلوک ثبت می‌شود. همچنین هر بلوک به بلوک‌های قبلی متصل است و بدین ترتیب هرگونه ایجاد تغییر در یک بلوک به تغییر در بلوک‌های دیگر منجر می‌شود و بلافاصله توسط بقیه اعضا قابل‌تشخیص است. علاوه بر صرفه‌جویی در زمان و هزینه، این روش نسبت به خرابی یکی از گره‌ها و هک کاملاً انعطاف‌پذیر بوده و به کار خود ادامه می‌دهد.

رمزنگاری

روش رمزنگاری مورداستفاده در زنجیره‌بلوک همان روش رمزنگاری مورداستفاده در نظام بانکی روز دنیا است. ازاین‌رو نمی‌توان آن را موضوعی جدید و مبهم که همراه با فناوری زنجیره‌بلوک ظهور پیدا کرده است، دانست؛ اما چون یکی از کلیدی‌ترین مفاهیم مرتبط با زنجیره‌بلوک به شمار می‌آید در ذیل به بررسی آن پرداخته شده است.

برای دانستن ماهیت رمزنگاری ابتدا باید با مفاهیم تابع هش[8]، کلید عمومی و کلید خصوصی آشنا شده، سپس به نحوه رمزگذاری و امضای دیجیتال پرداخت.

تابع هش و الگوریتم رمزنگاری SHA-256

تابع هش، تابعی است که اطلاعات از هر نوع و در هراندازه‌ای را به اطلاعاتی در اندازه مشخص و از یک نوع خاص تبدیل می‌کند. هر ورودی مشخص یک خروجی منحصربه‌فرد داشته و اگر ورودی به این تابع یکسان باشد خروجی هم مشابه خواهد بود. از طرفی اندکی تغییر در ورودی منجر به تغییر اساسی در خروجی می‌شود. همچنین تابع هش یک تابع یک‌طرفه است؛ بدین معنی که رسیدن از خروجی به ورودی در آن کاری به‌شدت دشوار است و در عمل و با پردازنده‌های موجود تقریباً غیرممکن هست.

در فناوری زنجیره‌بلوک مورداستفاده در رمزارز بیت‌کوین، نام خروجی استاندارد تابع هش، SHA-256 است که یک کد دویست‌وپنجاه‌وشش رقمی متشکل از صفر و یک است. هر ورودی (چند تراکنش و غیره) تبدیل به این کد دویست‌وپنجاه‌وشش رقمی می‌شود. در ادامه این گزارش به‌جای عبارت "خروجی تابع هش" به‌اختصار از واژه "هش" استفاده شده است.

کلید عمومی، کلید خصوصی و رمزگذاری

برای فراهم کردن امنیت در زنجیره‌بلوک از روش کلید عمومی و کلید خصوصی استفاده می‌شود. هر شخص در شبکه (سامانه‌های بانکی امروزی، زنجیره‌بلوک و به‌مانند آن) یک کلید عمومی (در دسترس همه) و یک کلید خصوصی (تنها در اختیار خود شخص) در اختیار دارد که این دو به‌وسیله روابط ریاضی به هم مرتبط هستند. در بیشتر مواقع (به استثنای امضاهای دیجیتال و غیره) کلید عمومی وظیفه رمزگذاری را بر عهده دارد و کلید خصوصی وظیفه رمزگشایی. فقط کلید خصوصی می‌تواند اطلاعات رمزگذاری شده توسط کلید عمومی را رمزگشایی کند و بالعکس. این ارتباط باعث امنیت بالای اطلاعات در زنجیره‌بلوک می‌شود. به‌طور مثال، فرض شود قرار است

---

[7] Node

[8] Hash Function

بانکی به یکی از مشتریان خود نامه‌ای محرمانه بفرستد. بانک به‌وسیله کلید عمومی مشتری، نامه را رمزگذاری می‌کند و برای مشتری می‌فرستد و فقط خود مشتری با کلید خصوصی خودش که تنها در اختیار وی است قادر به رمزگشایی نامه و خواندن آن است. یکی از روش‌های رمزگذاری که در سامانه‌های زنجیره‌بلوکی نیز استفاده می‌شود، رمزگذاری به‌وسیله تابع هش است؛ بدین ترتیب که کلید عمومی اطلاعات را در هم می‌ریزد (هش اطلاعات را حساب می‌کند) و برای کلید خصوصی می‌فرستد و کلید خصوصی با دانستن الگوریتم تولید هش کلید عمومی، آن را رمزگشایی می‌کند. همان‌طور که قبلاً اشاره شد در تابع هش رسیدن از خروجی به ورودی بدون دانستن رابطه‌ای که ورودی را به خروجی تبدیل کرده عملاً غیرممکن است. بدین ترتیب سرقت اطلاعات امری بیهوده است زیرا سارق نمی‌تواند از این هش به سرقت رفته بدون دانستن رابطه‌ای که اطلاعات را تبدیل به کد کرده استفاده کند و فقط یک کد بی‌معنی را به سرقت برده است.

امضای دیجیتال

یکی دیگر از کاربردهای این روش رمزگذاری (کلید عمومی و خصوصی) امضای دیجیتال است. امضا توسط کلید خصوصی که فقط در اختیار خود صاحب امضا قرار دارد ایجاد شده، به اسناد الصاق شده و توسط کلید عمومی که در اختیار دیگر اعضای شبکه قرار دارد تائید می‌شود. بدین ترتیب تحویل‌گیرنده اسناد می‌تواند اطمینان حاصل کند که اسناد از طرف شخص موردنظر ارسال شده و مورد تائید وی هست و اگر امضای غیر معتبری به اسناد الصاق شود توسط کلید عمومی تائید نشده و مردود به‌حساب می‌آید. در این روش نیز، امضا می‌تواند یک هش باشد که توسط کلید خصوصی ایجاد شده و کلید عمومی به‌وسیله ارتباطی که با کلید خصوصی خود دارد آن را رمزگشایی و تائید کند. در مثال ارسال نامه از طرف بانک به مشتری، امضای دیجیتال بانک که توسط کلید خصوصی بانک تولید شده نیز به نامه الصاق می‌شود. بدین‌ترتیب مشتری اطمینان حاصل می‌کند که نامه از طرف بانک ارسال شده است (با کلید عمومی بانک امضا را تائید می‌کند). در سامانه زنجیره‌بلوکی بیت‌کوین نیز یکی از کارهایی که گره‌ها در راستای تائید تراکنش انجام می‌دهند بررسی امضای دیجیتال تراکنش است. با این کار گره‌ها مطمئن می‌شوند که تراکنش ایجادشده توسط صاحب حساب انجام شده است یا خیر.

اجماع

در سامانه‌های زنجیره‌بلوکی بدون نیاز به تائید، سامانه طوری طراحی شده است که نیازی به تائید طرف سوم در تراکنش‌ها وجود نداشته باشد که اصطلاحاً به این نوع سامانه‌ها، سامانه همتا-به-همتا[9] یا بی‌واسطه نیز می‌گویند. در سامانه‌های ثبت تراکنش بانکی امروزی وظیفه تائید تراکنش‌ها با بانک به‌عنوان طرف سوم است. به‌طور مثال وقتی می‌خواهیم پولی را از حساب خود به‌حساب شخص دیگر واریز کنیم، بانک پول را از حساب ما برداشته و به‌حساب دیگری انتقال می‌دهد و در حقیقت به‌واسطه اعتبار بانک، طرفین معامله به بانک اعتماد می‌کنند؛ حال‌آنکه در سامانه‌های زنجیره‌بلوکی بدون نیاز به تائید، نیاز به وجود چنین طرف سوم مورداعتمادی نیست و اعضای شبکه، همگی، بر سر درستی یک تراکنش، ثبت و اجرای آن به اجماع می‌رسند. اجماع به معنی توافق اعضای سامانه بر سر موضوعات زیر است:

- آیا تراکنش واردشده توسط خود صاحب حساب انجام شده است؟ یا توسط یک فرد دیگر (خرابکار)؟
- آیا بر اساس سوابق، انجام تراکنش مقدور است؟ به‌عنوان‌مثال: آیا موجودی ایجادکننده تراکنش برای انجام تراکنش کافی است؟
- چه کسی تراکنش را ثبت کند؟ به بیان بهتر چه کسی کارمزد ثبت تراکنش را دریافت کند؟ به‌عنوان‌مثال: در حال حاضر ثبت‌کننده هر بلوک (مجموعه‌ای از تراکنش‌ها) در سامانه بیت‌کوین دوازده‌ونیم بیت‌کوین کارمزد دریافت می‌کند که نشان از اهمیت توافق بر سر ثبت‌کننده تراکنش است.

[9] Peer-to-Peer (P2P)

- کدام تراکنش زودتر ثبت شود؟ در بخش انواع روش‌های اجماع اهمیت این موضوع روشن‌تر می‌شود.

قراردادهای هوشمند

یکی از مهم‌ترین مفاهیم مرتبط با زنجیره‌بلوک که به‌همراه آن عرضه و توسعه داده شده است، قراردادهای هوشمند است و به دلیل همین رابطه تنگاتنگ میان این دو، اکثراً قراردادهای هوشمند را از خواص فناوری زنجیره‌بلوک می‌دانند و نه از کاربردهای آن. در این قراردادها به‌محض سررسید موعد مقرر، قرارداد به‌صورت خودکار تعهدات طرفین و میزان تحقق آن را بررسی می‌کند و نیازی به پیگیری و یا انجام عملیات توسط طرفین قرارداد نیست. به‌طور مثال در قرارداد وام، مبلغ موردنظر به‌صورت خودکار از وام‌گیرنده به وام‌دهنده انتقال می‌یابد و یا پس از پرداخت نشدن چند قسط، فرد به‌طور خودکار تحت پیگرد قرارگرفته و به دادگاه احضار می‌شود. انجام خودکار این فرآیندها به میزان چشمگیری باعث صرفه‌جویی در زمان و هزینه می‌شود. لازمه اجرای چنین ایده‌ای یک دفترکل مرکزی و قابل نظارت از طرف همه نهادهاست که زنجیره‌بلوک، آن را فراهم می‌کند. همچنین اگر پرداخت‌ها در این قراردادها از طریق رمزارز انجام شود، فرآیند، شفاف‌تر و قابل‌پیگیری‌تر شده و صرفه‌جویی هرچه بیش‌تر حاصل می‌گردد.

حال که زنجیره‌بلوک و مفاهیم اصلی مرتبط با آن شرح داده شد، در بخش بعدی به بررسی انواع زنجیره‌بلوک و انواع روش‌های اجماع در آن پرداخته می‌شود.