پارسا رهبران

قرارداد بی‌برگ و امضا

بیـــش از یک دهه اســـت که از معرفـــی بیت‌کوین و صنعت بلاک‌چیـــن می‌گذرد؛ فناوری‌ای انقلابی که تا به امروز همچنان در حال رشد و تکامل بوده است، تا جایی که امروز از نسل‌های متعدد این صنعت صحبت می‌شود.

نسل اول بلاک‌چین با بیت‌کوین آغاز شد. در مراحل اولیه، بلاک‌چین یـــک دفتر کل عمومی مشـــترک را ایجاد کرد که از یک شـــبکهٔ ارز دیجیتال پشتیبانی می‌کرد. نسل اول بلاک‌چین به دنبال بهبود نظام پولی سنتی بود. بیت‌کوین و ســـایر ارزهای رمزنگاری‌شده در این مرحله معرفی شدند که عمدتاً به زبان سی‌پلاس‌پلاس[1] نوشته شده بودند و برای به‌کارگیری مدل اجماع اثبات کار استفاده می‌شدند. در واقع هدف اصلی این نسل انتقال ارزش بود.

اگرچه ارزهای رمز پایه، مبتنی بر بلاک‌چین، تراکنش را راحت‌تر کردند، با این حال توســـعه‌دهندگان متوجه شدند این فناوری ظرفیت بســـیار بیشتری فراتر از رمزارزها دارد. با گذشت زمان، توسعه‌دهندگان به این باور رسیدند که هر بلاک‌چین می‌تواند چیزی بیش از ثبت تراکنش‌ها را انجام دهد. برای مثال، بنیان‌گذاران اتریوم این ایده را داشتند که دارایی‌ها و قراردادهای بر پایهٔ اعتماد نیز می‌توانند از مدیریت بلاک‌چین بهره ببرند. به این ترتیب، اتریوم نشان‌دهندهٔ نسل دوم فناوری بلاک‌چین است.

نـــوآوری اصلی اتریوم ظهور قراردادهای هوشـــمند[2] بود. به‌طور معمول، قراردادها در دنیای کسب‌وکار اصلی بین دو نهاد مجزا مدیریت می‌شوند. مانند قرارداد همکاری که افراد با یکدیگر می‌بندند و طرفین با شـــرایطی ملزم به انجام آن هستند.

نسل دوم بلاک‌چین که با معرفی اتریوم آغاز شد، نه‌تنها بـــه کاربران اجازهٔ انتقال ارزش را می‌داد، بلکه با معرفی قراردادهای هوشمند، اجازهٔ انتقال پول، تحت شرایطی خاص، را می‌داد.

در این شـــماره به‌طور ویـــژه به قراردادهای هوشـــمند می‌پردازیم.

قراردادهای هوشمند برنامه‌های خودکاری هستند که در صورت برآورده‌شـــدن شرایط از پیش تعریف‌شده اجرا و در بلاک‌چین ذخیره می‌شوند. این قراردادها نسخه‌های دیجیتال قرارداد کاغذی استاندارد هستند که شرایط توافقنامهٔ آن‌ها در خطوط کد نوشته شده است. این قراردادها به‌طور خودکار معاملات را در صورت رعایت شـــرایط خاص، بدون نیاز به کمک شـــخص ثالث، برای مدیریت یا تأیید تراکنش انجام می‌دهند. این شخص ثالث می‌تواند سازمانی دولتی، وکیل یا هر نهاد دیگری باشد. برای مثال، در قراردادهای کاغذی ســـنتی، یک سند شرایط بین دو طرف را مشخص می‌کند که با قانون قابل‌اجراست. اگر یکی از طرفین، برای مثال الف، شرایط را نقض کند، طرف ب می‌تواند طرف الف را به دلیل رعایت‌نکردن قرارداد به دادگاه بکشد. از آنجا که در قرارداد هوشمند، این‌گونه قراردادها به‌صورت کد نوشته می‌شوند، بنابراین، شـــرایط قرارداد به‌طور خـــودکار و بدون دخالت و بدون وجود شخص ثالث اجرا می‌شود.

قراردادهای هوشمند چگونه کار می‌کنند؟

چرخهٔ عمر قراردادهای هوشمند چهار مرحلهٔ متوالی دارد: ایجاد، استقرار، اجرا و تکمیل.

۱. ایجاد: قبل از هر معامله، طرفین قرارداد شرایط قرارداد را تعیین می‌کنند مانند قراردادهای سنتی که طرفین تعهدات خود را پای برگه می‌نویســـند. پس از نهایی شدن شرایط و ضوابط قرارداد، این قرارداد جهت اجرا به کد برنامه‌نویسی

قرارداد هوشـــمند ترجمه می‌شوند. اساساً، کد تعدادی از عبارات شرطی مختلف را نشـــان می‌دهد که سناریوهای احتمالی یک تراکنش آینده را توصیف می‌کند. «اگر «شرط» درســـت است، «پس» دستور» اجرا می‌شود، در حالی که اگر شرط نادرست باشد، دستور else اجرا می‌شود.

۲. اســـتقرار: هنگامی که قرارداد هوشـــمند ایجاد می‌شود، طرفین می‌توانند با اعمـــال امضای دیجیتال خود در قرارداد، با شـــرایط و ضوابط موافقت کنند. امضای دیجیتال یک فن رمزنگاری اســـت که شـــخص را به داده‌های دیجیتال وصل می‌کند. سپس قرارداد هوشمند در شبکهٔ بلاک‌چین ذخیره می‌شود و نمی‌توان آن را تغییر داد یا اصلاح کرد. هرگونه اصلاح یا تجدیدنظر در قرارداد، مستلزم ایجاد قرارداد جدید است. به همین دلیل، باید به نوشتن و آزمون کد توجه ویژه‌ای شود تا از ایجاد اشکال‌هایی در قرارداد جلوگیری شود که هرگز برطرف نمی‌شوند.

به دلیل ذخیرهٔ قراردادهای هوشـــمند در بلاک‌چین، آن‌ها غیرمتمرکز می‌شوند. یعنی قراردادهای هوشمند با ماشین یا انسان کنترل نمی‌شوند.

علاوه بر این، در این مرحله، هرگونه انتقال به نشـــانی کیف پول دریافتی قرارداد هوشمند مسدود می‌شود. برای مثال، هر قرارداد هوشمند بین خریدار و تأمین‌کننده امضا می‌شود. طبق قرارداد، انتقال وجه از کیف پول خریدار به تأمین‌کننده، تنها زمانی انجام می‌شود که خریدار کالا را از تأمین‌کننده دریافت کند. در نتیجه، هر نوع انتقال وجه در کیف پول تأمین‌کننده مســـدود خواهد شد. گره‌های شبکه (که در قسمت‌های قبل به‌عنوان اعضای شبکهٔ بلاک‌چین شناخته‌ایم) به‌عنوان بدنهٔ حاکم عمل می‌کنند که تأیید می‌کنند آیا شـــرایط ازپیش تعریف‌شده برای اجرای قرارداد برآورده شده است یا خیر؟

۳. اجرا: پس از استقرار قراردادهای هوشمند، تمام گره‌های بلاک‌چین در شـــبکه، شـــرایط قرارداد را نظـــارت و ارزیابی می‌کنند. پس از برآورده‌شـــدن شـــرایط ازپیش تعریف‌شده، قرارداد خودبه‌خود اجرا می‌شود. وجه به‌صورت سکه، از کیف پول خریدار خارج و به تأمین‌کننده منتقل می‌شود (به‌عنوان تعهد مبادلهٔ کالا). در نتیجه، گره‌های موجود در بلاک‌چین، تراکنش اجراشده را اعتبارسنجی می‌کنند تا از تحقق شرایط قرارداد اطمینان حاصل شود. فرایند تأیید را سازوکارهای اجماع اثبات کار یا اثبات سهام انجام می‌دهند. در انتها، تراکنش‌های تأییدشـــده و وضعیت به‌روزشـــدهٔ قراردادهای هوشمند در بلاک‌چین ذخیره می‌شوند.

۴. تکمیل: با توجه به شرایط ازپیش‌تعریف‌شده در قرارداد هوشمند، پس از دریافت کالا توسط خریدار از فروشنده، کیف پول فروشنده باز می‌شود. بنابراین، وجه از خریدار به کیف پول تأمین‌کننده منتقل می‌شود. این مرحله نشان‌دهندهٔ تکمیل قرارداد هوشـــمند است که سپس بسته و در بلاک‌چین ثبت می‌شود.

توجـــه به این نکته حائز اهمیت اســـت که یـــک توالی از تراکنش‌ها در مراحل استقرار، اجرا و تکمیل قرارداد هوشمند انجام شده است. بنابراین، هر سه مرحله به نوشتن داده‌ها در بلاک‌چین نیاز دارند.

مزایای قراردادهای هوشمند

۱. اعتماد: یکی از مهم‌ترین مزایایی که قراردادهای هوشمند نســـبت به قراردادهای ســـنتی دارند، این است که زمانی که شرایط توافق برآورده می‌شوند، به‌طور خودکار اجرا می‌شوند. نیازی نیســـت منتظر بمانید شخص ثالثی آن‌ها را اجرا کند. به عبارت دیگر، قراردادهای هوشمند نیاز به اعتماد را برطرف می‌کند.

۲. شفافیت: یکی دیگر از ویژگی‌های قراردادهای هوشمند که آن‌ها را بســـیار حیاتی می‌کند، شفافیتی است که با خود به همـــراه دارند. همان‌طور که قبلاً بحث شـــد، قراردادهای هوشمند حاوی فهرست دقیقی از شرایط و ضوابط مورد توافق طرفین درگیر هستند. این تنظیم ازپیش توافق‌شده، با پیشنهاد و تصویب شرایط و ضوابط توسط خود طرفین، احتمال بروز مسائل و اختلافات در مراحل بعدی را از بین می‌برد.

این شـــرایط و ضوابط بـــرای هر طرف درگیـــر در معامله قابل‌مشاهده است. بنابراین، شفافیت در سامانه ایجاد می‌شود. مسائل مربوط به شکاف‌های ارتباطی نیز با اجرای قراردادهای هوشمند کاهش می‌یابند، زیرا تنها یک نسخه از واقعیت وجود دارد که در شبکه قابل‌مشاهده برای همه است.

۳. تغییرناپذیری: قراردادهای هوشمند تغییرناپذیرند، به این معنی که کد و شـــرایط آن‌ها پس از اســـتقرار در بلاک‌چین قابل‌تغییر یا به‌روزرسانی نیستند. علاوه بر این، آن‌ها در سراسر سامانهٔ بلاک‌چین توزیع‌شده ذخیره و تکرار می‌شوند. بنابراین قابل‌ردیابی و ممیزی هستند. در نتیجه می‌توان از رفتارهای مخرب مانند کلاه‌بـــرداری مالی، تا حد زیادی کاســـت. اگر می‌خواهید قرارداد هوشمند موجود را تغییر دهید، باید نسخهٔ جدیدی از آن را ایجاد کنید.

بـــازده زمانی بهتر: یکی دیگر از مزایـــای قابل‌توجه اجرای قراردادهای هوشمند، بهره‌وری بهتر است. در نظام سنتی، با انجام کارهای اداری، معمولاً چند روز طول می‌کشـــد تا یک درخواســـت پردازش شود و در مراحل فرایند، اسناد و مدارک تکراری غیرضروری زیادند. علاوه بر این، دخالت تعداد زیادی واســـطه، فرایند را پیچیده‌تر، دســـت و پاگیرتر و وقت‌گیرتر می‌کند. اما با اجرای قراردادهای هوشمند، تمامی این مراحل زائد و غیرضروری حذف می‌شـــوند و از زمان صرف‌شده برای تکمیل تراکنش‌ها به میزان قابل‌توجهی کاهش می‌دهد.

۴. ایمنی و امنیت: قراردادهای هوشمندِ همراه با بلاک‌چین، ضد دست‌کاری، قابل‌اعتماد و ایمن هستند. ویژگی امنیت و ایمنی، ارزش و اعتماد بیشتری را در معاملات مرتبط به ارمغان می‌آورد.

پی‌نوشت‌ها

1. C++
2. Smart Contarct