بلاک چین و عملکرد آن در عصر دیجیتال

نویسندگان: محمود شاه‌چراغی- m.shahcheraghi1924@gmail.com
رضا ملاحسینی- m.mollahoseini@ardakan.ac.ir

چکیده: بلاک چین فناوری اصلی ارز دیجیتال است که حیات یک پلتفرم بدون وابستگی به نهاد مرکزی را تضمین می‌کند و می‌توان از آن در حوزه‌های مختلف استفاده کرد.
بلاک چین اختراعی برجسته و مبتکرانه است؛ زاییده فکر یک فرد یا گروهی از افراد که بانام مستعار ساتوشی ناکاموتو شناخته می‌شوند. اما از آن زمان که بلاک چین برای اولین بار معرفی شد، این فناوری به موجودیتی بزرگ تبدیل‌شده است و سؤال اصلی بسیاری از افراد این است که بلاک چین چیست؟
فناوری بلاک چین از طریق ایجاد امکان توزیع اطلاعات دیجیتال بدون کپی کردن آن، ستون فقرات نوع جدیدی از اینترنت را ایجاد کرد. در ابتدا برای پول دیجیتال بیت کوین طراحی شد، اما در حال حاضر جامعه فناوری در حال پیدا کردن دیگر کاربردهای بالقوه برای این فناوری است.
بیت کوین، «طلای دیجیتال» نام‌گذاری شده است و دلایل خوبی نیز برای این امر وجود دارد. بلاک چین می‌تواند انواع دیگری از ارزش دیجیتال را ایجاد کند. مانند اینترنت (یا خودرو)، شما برای استفاده از بلاک چین لازم نیست بدانید چگونه کار می‌کند. بااین‌حال، داشتن دانش اولیه در مورد این فناوری جدید به شما نشان خواهد داد که چرا انقلابی محسوب می‌شود.
بلاک چین یک دفترکل دیجیتالی غیرقابل‌تخریب از معاملات اقتصادی است که می‌تواند نه‌تنها برای ضبط معاملات مالی بلکه تقریباً برای ثبت هر دارایی ارزشمندی استفاده شود.در این مقاله به بررسی موضوع اصلی مقاله بلاک چین ،کاربردها،عملکرد و مقایسه آن با همنوعان خود می‌پردازیم.

کلیدواژه: بلاک چین- بیت کوین- ارزش دیجیتال- فناوری- اینترنت

۱ – مقدمه

زنجیره بلوک یکی از موضوعات موردتوجه دنیا امروز است که با هموار کردن مسیر معاملات دیجیتال، صنعت کسب‌وکار را متحول می‌نماید. دو عبارتی که این روزها زیاد می‌شنوید بلاک چین و بیت کوین است، باوجودی که به‌نوعی ازلحاظ معنایی مرتبط هستند به دو چیز متفاوت اشاره دارند که در ادامه به توضیح آن پرداختیم.

بیت کوین شکلی از ارز مجازی است که به‌عنوان رمزنگاری واحدهای پولی شناخته می‌شود و به‌صورت غیرمتمرکز امکان مبادله پول را بدون نیاز به شخص سوم فراهم می‌کند. کلیه تراکنش‌های بیتکوین ذخیره (لاگ) شده و در یک‌لایه عمومی در دسترس قرار می‌گیرند به‌نحوی‌که با اطمینان از صحت آن، از تقلب نیز جلوگیری می‌نماید؛ فناوری که موجب تسهیل این معاملات و حذف عنصر واسط گردید بلاک چین نامیده می‌شود.

یکی از مزایای اصلی بلاک چین وضوح و شفافیت آن است، همان‌طور که اشاره شد شما می‌توانید جز به‌جز تراکنش‌های فردی از طریق لاگ دریافتی مشاهده نمایید.

با هر تراکنش طرف اول ماجرا بیتکوین را مستقیماً به دیگری ارسال می‌کند و جزئیات معامله که شامل منبع، مقصد و تاریخ/زمان‌بندی است، به‌عنوان یک بلوک در نظر گرفته‌شده و زنجیروار به آن افزوده می‌شود. هر بلوک شامل تراکنش‌هایی است که بسته به بلاک چین و پیکربندی آن می‌تواند متفاوت باشد.

اعتبار تراکنش‌های درون بلوک رمزنگاری‌شده توسط سیستم‌های محاسباتی منتخب در شبکه بررسی و تأیید خواهد شد.

این سیستم‌های منتخب، کامپیوترهایی هستند که با به‌کارگیری GPU و یا CPU ها و برای حل مسائل ریاضی پیچیده پیکربندی‌شده‌اند. روش کار به این صورت است که داده‌های بلوک توسط الگوریتم‌های پیشرفته جداسازی می‌شوند تا زمانی که راه‌حل موردنظر یافت شود. پس از حل شدن، بلوک و تمام تراکنش‌های مربوطه به‌طور رسمی تائید خواهند شد. سپس پاداش (که می‌تواند بیتکوین یا لایتکوین باشد) میان کامپیوتر یا کامپیوترهای شرکت‌کننده تقسیم می‌گردد.

با کسب اعتبار، بلوک تراکنش به آخرین بلوک تائید شده در زنجیره ملحق و تابعی متوالی ایجاد می‌کند که توسط همه افراد قابل‌مشاهده است.

این فرآیند تا ابد ادامه می‌یابد، محتوای زنجیره بلوک‌ها گسترش داده می‌شوند و رکوردی عمومی و قابل‌اعتماد فراهم می‌کنند. علاوه بر به‌روزرسانی مدام، زنجیره و کلیه بلوک‌هایش در سراسر شبکه میان ماشین‌های بسیار پخش می‌گردند. این مسئله تضمین می‌کند که کلیه نسخه‌های این تابع غیرمتمرکز به‌صورت مجازی در همه‌جا وجود دارد و ساخت نسخه جعلی از آن را غیرممکن می‌سازد

۲- بلاک چین چگونه کار می‌کند

نحوه کار بلاک چین را می‌توان به‌عنوان سیستمی قلمداد کرد که به گروهی از رایانه‌ها اجازه می‌دهد تا یک نسخه واحد و امن از دفتر کل را نگهداری کنند. برای انجام تراکنش‌ها در بلاک چین، نیازمند کیف پول هستید. کیف پول برنامه‌ای است که اجازه می‌دهد بیت کوین‌ها را درون آن ذخیره و ارسال کنید. ازآنجایی‌که فقط شما باید بتوانید بیت کوین‌ها را خرج کنید هر کیف پول با استفاده از یک روش رمزنگاری محافظت می‌شود که از یک جفت کلید عمومی و خصوصی که به هم متصل هستند، استفاده می‌کند: کلید خصوصی و عمومی.

اگر پیامی به‌وسیله یک کلید عمومی رمزنگاری شود، تنها دارنده کلید خصوصی می‌تواند رمز آن را بگشاید. برعکس این اتفاق نیز صادق است: اگر شما پیامی را با کلید خصوصی خود رمزنگاری کنید تنها کلید جفت عمومی آن می‌تواند پیام را رمزگشایی کند.

وقتی علی می‌خواهد بیت کوین‌ها را ارسال کند، او باید این پیام را به‌صورت رمزنگاری و با کمک کلید خصوصی از کیف پولش ارسال کند. ازآنجایی‌که علی تنها دارنده کلید خصوصی برای بازگشایی کیف پولش است، او تنها کسی است که می‌تواند بیت کوین‌ها را خرج کند. هر نود در شبکه می‌تواند درخواست بازبینی تراکنش صورت گرفته را با کمک کلید عمومی خودش بدهد.

وقتی شما یک تراکنش صورت گرفته را با کمک کلید خصوصی بازگشایی می‌کنید شما یک امضای دیجیتال ایجاد می‌کنید که توسط رایانه‌های بلاک چین برای تأیید امنیت و اعتبار تراکنش مورداستفاده قرار می‌گیرد. این امضای دیجیتال، رشته‌ای از پیام‌های متنی از تراکنش درخواست شده توسط شما و کلید خصوصی‌تان است. بنابراین نمی‌توان از آن برای سایر تراکنش‌ها استفاده کرد. اگر یک کاراکتر تراکنش را تغییر دهید امضای دیجیتال هم‌تغییر می‌کند پس هیچ هکری نمی‌تواند تراکنش درخواست شده شمارا تغییر دهد یا میزان بیت کوین ارسالی شمارا دست‌کاری کند.

برای ارسال بیت کوین باید ثابت کنید که مالک کلید خصوصی یک کیف پول هستید و همین‌طور نیاز به کلید برای باز کردن تراکنش درخواست شده دارید. ازآنجایی‌که شما پیام را بعد از رمزگذاری ارسال کرده‌اید نیازی نیست که کلید خصوصی خود را افشا سازید.

مانده‌حساب بیت کوین در نحوه کار بلاک چین

هر نود بلاک چین یک کپی از دفتر کل را حفظ می‌کند. بنابراین یک نود چطور می‌داند که مانده‌حساب شما چقدر است؟

در نحوه کار بلاک چین سیستم بلاک چین میزان مانده‌حساب همه را حفظ نمی‌کند، فقط هر تراکنش ثبت و تأییدشده را نگه می‌دارد. بنابراین دفتر کل، مانده‌حساب‌ها را ردیابی نمی‌کند بلکه فقط تاریخچه تمام تراکنش‌های ارسال‌شده در شبکه بیت کوین را حفظ می‌کند. برای محاسبه میزان مانده‌حساب شما، باید تمام تراکنش‌های انجام‌شده و تأییدشده در کل شبکه به‌حساب شما موردبررسی قرار بگیرد.

تأیید مانده‌حساب بر اساس لینک‌های صورت گرفته به تراکنش‌های قبلی انجام می‌شود. برای اینکه علی ۱۰ بیت کوین برای محمد ارسال کند، علی باید تراکنشی را درخواست کند که شامل لینک‌های قبلی به تراکنش‌های گذشته به میزان حداقل ۱۰ بیت کوین باشد. این لینک‌ها را ورودی می‌خوانند. نودها در شبکه، میزان آن‌ها را تأیید می‌کنند و اطمینان می‌دهند که این لینک‌ها قبلاً خرج نشده‌اند. درواقع هر بار که شما به یک تراکنش رفرنس می‌دهید آن‌ها برای تراکنش‌های آینده غیرقابل مجاز در نظر گرفته می‌شوند. همه این‌ها به‌صورت خودکار در کیف علی انجام می‌شود و دوباره توسط نودهای شبکه بیت کوین هم مورد تأیید قرار

www.kahrobaonline.ir

می‌گیرد. علی ۱۰ بیت کوین تراکنش را به کیف محمد با استفاده از کلید عمومی ارسال می‌کند.

۳- کاربردها

از بلاک چین می‌توان در زمینه‌های صنعتی، پزشکی و زمینه‌های بسیار دیگری استفاده کرد. به‌عنوان‌مثال می‌توان آن را در بخش پزشکی -که سوابق بیماران دست‌کاری می‌شود- به کار گرفت. این فناوری به پزشکان اجازه می‌دهد تا پرونده‌ای از سوابق بیماران را با امنیت بالا ذخیره کرده و آن‌ها را در صورت لزوم در اختیار دیگر بیمارستان‌ها و مراکز درمانی قرار دهند. این کار علاوه برافزایش امنیت ذخیره‌سازی و انتقال داده‌ها، باعث کاهش خطرها و هزینه‌های مدیریت داده‌ها می‌شود.

بلاک چین برای دولت‌مردان کشورهای مختلف نیز جذابیت‌های خاص خود را دارد. در حال حاضر دولت‌مردان انگلیس در حال تحقیق برای بهبود روش‌های ذخیره‌سازی اطلاعات توسط بلاک چین هستند.

از این فناوری می‌توان برای مقابله با دریافت محصولات چندرسانه‌ای به‌صورت غیرقانونی نیز استفاده کرد.

همچنین ویج معتقد است از فناوری بلاک چین می‌توان برای اعتبارسنجی و جلوگیری از انجام تقلب در انتخابات الکترونیک نیز استفاده کرد

۴- چرا بلاک چین برای بانک‌ها جذاب است

مؤسسات مالی، شرکت‌هایی هستند که بلاک چین را وسیله‌ای برای افزایش موفقیت‌های خود می‌دانند. وینکلسپکت گفت: «آن‌ها می‌توانند درحالی‌که سامانه‌هایشان با پلتفرم‌های شرکت‌های دیگر سازگار است، داده‌های مربوط به موجودی و دارایی‌های خود را به‌صورت رمزنگاری‌شده و با امنیت بالا، تولید، مدیریت و ذخیره کنند. این شرکت‌ها می‌توانند خدماتی یا دیگر مؤسسات مالی باشند

البته مؤسسات مالی و بانک‌هایی که از بلاک چین استفاده می‌کنند، باید خطر کاهش قدرت در بازار تبادلات ارزی را بپذیرند.

استیفنز گفت: «بانک‌ها، به‌عنوان مجریان اصلی بازار تبادلات ارزی شناخته می‌شوند؛ اما این فناوری و بیت کوین، خلأ بزرگی در این بخش ایجاد می‌کنند؛ اما در هزینه‌ی ایجاد زیرساخت‌ها صرفه‌جویی خواهد شد.»

مقامات بانک انگلیسی سانتاندر (Santander) پیش‌بینی می‌کنند، بلاک چین می‌تواند در سال ۲۰۲۲ به‌صورت سالانه ۲۰ میلیارد دلار ذخیره‌ی مالی برای بانک‌ها فراهم کند

۵- طول عمر و ثبات بلاک چین

تکنولوژی بلاک چین درواقع مانند اینترنت است که ازنظر ثبات از پیش‌ساخته شده است. بلاک چین بلوک‌هایی از اطلاعات را ذخیره می‌کند. درواقع در مورد بلاک چین این موارد قابل انجام نیست:

۱- کنترل شدن توسط تنها یک موجودیت.

۲- هیچ نقطه در آن وجود ندارد که با ازکارافتادن، تمام سیستم از کار بیفتد.

بیت کوین در سال ۲۰۰۸ اختراع شد. از آن زمان تابه‌حال بلاک چین بدون هیچ مشکل عمده‌ای به فعالیت پرداخته است. تا به امروز مشکلات بلاک چین ناشی از هک و یا عدم مدیریت صحیح بوده است. این مشکلات ناشی از اشتباه انسانی می‌شود و نه اصل و اساس بلاک چین.

۶- آینده بلاک چین

فناوری بلاک چین نمی‌تواند به‌سرعت، اینترنت را تغییر دهد. وینکلسپکت گفت: «موارد زیادی است که این فناوری را به چالش می‌کشد. مردم ممکن است متوجه شوند این فناوری، یک تحول ایجاد خواهد کرد؛ اما نمی‌دانند این فناوری چگونه به بهبود کسب‌وکار آن‌ها کمک می‌کند.»

بلاک چین یک فناوری نوظهور است که نیاز دارد تا برنامه‌هایی سازگار با آن تولید شود. همچنین برای استفاده از این فناوری باید مجموعه‌ای مقررات تنظیم شود. همچنین این فناوری باید بتواند کارآمدی خود را اثبات کند تا بتواند به‌صورت گسترده به کار گرفته شود.

۷- ویژگی‌های بلاک چین

ویژگی فوق‌العاده تکنولوژی بلاک چین که درواقع قابلیت تمرکززدایی است، امکان ایجاد کسب‌وکارها و عملیات به‌صورت منعطف‌تر و امن‌تر می‌شود. درصورتی‌که شرکت‌های مختلف در ارائه خدمات و محصولات خود موفق به استفاده از این تکنولوژی شوند، اعتماد به بلاک چین افزایش پیدا می‌کند. درخواست‌ها برای استفاده از این تکنولوژی در حال افزایش است و همگام با آن این تکنولوژی رو به تکامل است. می‌توان گفت پتانسیل‌های بلاک چین درواقع بدون مرز است.

۸- سیستم اثبات کار در بلاک چین

از همین رو بلاک چین برای جلوگیری از این روند از سیستم proof-of-work یا اثبات کار استفاده می‌کند که توسط آن بلاک‌ها با سرعت کمتری شکل می‌گیرند. مثلاً برای بیت کوین محاسبه proof-of-work و افزودن یک بلاک به زنجیره حدود ۱۰ دقیقه طول می‌کشد که این مکانیسم امکان ایجاد تغییرات در هر بلاک را سخت و تقریباً غیرممکن می‌کند. یعنی اگر تغییری در یک بلاک انجام شود، لازم است که سیستم proof-of-work یا اثبات کار زمان‌بر برای تمام بلاک‌های بعدازآن نیز اعمال شود. پس امنیت بلاک چین بستگی به استفاده درست از hash و proof-of-work برای بلاک چین است.

و البته حفظ امنیت بلاک چین به پارامتر دیگری نیز وابسته است. بلاک چین یک شبکه توزیع‌شده است. به این معنی که به‌جای استفاده از یک‌نهاد متمرکز جهت کنترل زنجیره، بلاک چین از یک شبکه همتا به همتا استفاده می‌کند همه می‌توانند به آن شبکه ملحق شوند. هنگامی‌که یک نفر به شبکه اضافه می‌شوند، یک کپی از بلاک چین در اختیار او قرار داده می‌شود که این شخص می‌تواند توسط این کپی صحت اطلاعات را نیز تأیید کند.

وقتی یک بلاک جدید تولید می‌شود، آن بلاک به همه‌کسانی که به شبکه دسترسی دارند فرستاده می‌شود و هر شخص جهت اطمینان از عدم دست‌کاری، صحت بلاک را تأیید می‌کند و پس‌ازآن هر گره بلاک جدید را به بلاک چین خود اضافه می‌کند. تمامی گره‌های روی این شبکه یک توافق را شکل می‌دهند، که کدام بلاک‌ها معتبر و کدام‌یک مورد تغییرات و دست‌کاری قرارگرفته‌اند. بلاک‌های دست‌کاری شده با توافق همه رد می‌شوند.

بلاک چین هرروز درحال‌توسعه و تغییر و تحول است. توسعه قراردادهای هوشمند ازجمله تحولاتی است که به‌تازگی رخ‌داده است. این قراردادها برنامه‌های ساده‌ای هستند که روی بلاک چین ذخیره‌شده‌اند و می‌توانند طبق شرایط خاص برای تبادل کوین‌ها مورداستفاده قرار گیرند. فناوری بلاک چین به‌سرعت توجه همه را به خود جلب کرده است و خیلی زود همه متوجه شده‌اند که از بلاک چین می‌توانند در زمینه‌های مختلف مانند ذخیره سوابق پزشکی و یا ایجاد یک دفتر ثبت‌اسناد رسمی دیجیتال و جمع‌آوری مالیات مورداستفاده قرار بگیرد.

۱۰- مقایسه بلاک چین و پایگاه داده (Data Base)

در پایگاه داده‌ها کاربر با دسترسی مشخص توسط حساب کاربری خود می‌تواند نسبت به تغییر رکوردهای ذخیره‌شده در یک سرور مرکزی اقدام نماید. در این حالت مدیریت و کنترل پایگاه داده در اختیار مدیر آن قرار داده‌شده و کاربران در این بخش نقشی ندارد. برخلاف آن مدیریت blockchain به‌صورت مرکزی نبوده و مشارکت‌کننده‌ها در نگهداری، محاسبات و همچنین به‌روزرسانی آن نقش دارند. در این حالت همه اعضا در کنار یکدیگر فعال هستند تا با اطمینان به نتیجه یکسانی برسند. استفاده از این روش به همراه الگوریتم‌های ریاضی سبب می‌شود شبکه توزیع‌شده‌ای ایجاد شود که دارای امنیتی درون‌ساخته است.

در blockchain همانند پایگاه داده توزیع‌شده، امکان به اشتراک‌گذاری داده‌ها در میان کاربران گوناگون وجود دارد با این تفاوت که در آن هر رکورد دیجیتالی یا تراکنش (transaction) در یک بلاک ذخیره می‌شود.

مراجع

[1] Tomaso Aste and Paolo Tasca., Blockchain Technologies:The Foreseeable Impact on Society and Industry, PUB L ISHED B Y THE I EEE COMPUTER SOCI E T Y, 2 0 1 7.

[2] Yotaro Okazaki,Unveiling the Potential of Blockchain for Customs, Ph.D. Thesis, University of Washington, Seattle, WA, 2018.

[3] Zachman, John A., Block-secure: Blockchain based scheme for secure P2P cloud storage", Elsevier, 2018.