آشنایی با فناوری راهبردی زنجیره بلوکی و کاربردهای آن

کد موضوعی: ۲۸۰
شماره مسلسل: ۱۵۳۴۱
فروردین‌ماه ۱۳۹۶

معاونت پژوهش‌های زیربنایی و امور تولیدی
دفتر: مطالعات ارتباطات و فناوری‌های نوین

به‌نام خدا

فهرست مطالب

آشنایی با فناوری راهبردی زنجیره بلوکی و کاربردهای آن

چکیده

زنجیره بلوکی یک فناوری جدید در زمینه رایانش ایمن است. این فناوری می‌تواند دنیای دیجیتال را متحول کند و با استفاده از خصوصیت «تفاهم توزیع‌یافته» برای هر تراکنش آنلاین قدیمی یا فعلی، تراکنش‌ها را به نحوی اجرا نماید که دارایی‌های دیجیتالی درآینده نیز قابل شناسایی و اعتماد باشند. این امر بدون در خطر افتادن حریم خصوصی و امنیت دارایی‌های دیجیتال و طرف‌های درگیر انجام می‌گیرد. به بیان ساده، منطق فناوری زنجیره بلوکی این است که همانطور که سرقت کلوچه از مغازه‌ای خلوت بسیار ساده‌تر از دزدیدن آن از یک فروشگاه بزرگ در حضور هزاران شاهد است؛ فناوری زنجیره بلوکی با استفاده هنرمندانه از رمزنگاری و با توزیع اختیارات نظارت و مدیریت بر منابع اطلاعاتی و رایانشی و تاریخ‌مندسازی تراکنش‌ها، مجموعه‌ای از مزایای امنیتی و کارکردی به‌وجود آورده است. به‌طوری که درحال حاضر بسیار مورد توجه اتاق‌های فکر و مراکز قانون‌پژوهی دنیاست و توسط گروه مشاوره گارتنر در مجموعه فناوری‌های نوظهوری که بیشترین انتظارات از آنها می‌رود طبقه‌بندی شده است. کنگره و سنای آمریکا، بانک مرکزی چین، کارگروه دولتی زنجیره بلوکی روسیه، مجلس ملی فرانسه و پارلمان اتحادیه اروپا با برگزاری جلسات استماع، کارگاه‌ها و کنفرانس‌های مختلف و صدور قطعنامه مطالعه ابعاد مختلف فناوری، زنجیره بلوکی را در دستور کار خود قرار داده‌اند. ازجمله مزایای این فناوری این است که اطلاعات پایگاه‌های داده نسبت به تغییرات خلاف توافقات یا قانون مقاوم خواهند شد و با شفاف‌سازی تراکنش‌ها موجب جلب اعتماد شهروندان و دستگاه‌های امنیتی و قضایی به تراکنش‌های پایگاه داده، می‌شود. این فناوری با پراکندن پایگاه‌های داده در نقاط مختلف، از آنها در مقابل حملات فیزیکی نیز محافظ می‌کنند و در مواردی که دو نهاد دولتی به‌دلیل اختیارات متناسب با جایگاه قانونی خود نیازمند دسترسی‌های با شرایط مدیریتی متداخل به یک پایگاه داده یا منبع رایانشی واحد هستند (مانند برگزاری انتخابات)، استفاده از این فناوری می‌تواند تفاهم میان دستگاه‌ها را تسهیل کند. متخصصین فناوری اطلاعات که به‌دلیل تخصص فنی در جایگاه مدیریتی پایگاه‌های اطلاعاتی سنتی قرار می‌گرفتند با کمک این فناوری دیگر قدرت دخالت بدون بازخواست در پایگاه‌های اطلاعاتی را نخواهند داشت. زیرا سابقه اقدامات تمام اعضای سامانه نسبت به داده‌ها در زنجیره بلوکی ثبت شده و قابل مراجعه، بازبینی و بازخواست خواهد بود. در این گزارش علاوه‌بر معرفی فناوری زنجیره بلوکی، کاربردهای این فناوری در زمینه‌های بانکداری، بیمه، دفاتر اسناد

رسمی، ذخیره‌سازی داده‌ها و کنترل منابع اینترنتی و اینترنت اشیا و مقابله با جعل و تقلب بیان می‌شود. با توجه به طیف وسیع کاربردهای این فناوری، استفاده از آن در برگزاری انتخابات نیز قابل بررسی است.

مقدمه

فناوری زنجیره بلوکی، کاربردهای زیادی دارد. یکی از کاربردهای آن ایجاد زیرساخت‌های ارزهای رمز پایه است و فناوری زنجیره بلوکی یکی از زیرساخت‌های اساسی بیتکوین است.[۱] به بیان دیگر، فناوری زنجیره بلوکی در دامنه بسیار وسیعی از برنامه‌های کاربردی مالی و غیرمالی دیگر نیز به‌عنوان فناوری زیرساخت به‌خوبی به‌کار گرفته شده است و اختراعات متعددی در حوزه‌های اعتبارسنجی تراکنش‌های مراقبت‌های بهداشتی، مسائل بانکی، انتخابات و رایانشی به ثبت رسیده است و به همین دلیل دولت‌ها و مراکز قانونگذاری، مطالعه پیرامون بهره‌گیری از آن را در دستورکار خود قرار داده‌اند.

فناوری زنجیره بلوکی، سیستمی برای ایجاد «تفاهم توزیع‌یافته»[۲] در دنیای آنلاین دیجیتال پایه‌ریزی می‌کند. به این معنا که با توجه به ثبت انکارناپذیر اطلاعات در دفتر کل تمامی اجزای شبکه از تحقق یک رویداد دیجیتالی آگاه گشته و آن را به رسمیت می‌شناسند. این فناوری دریچه‌ای به‌سوی توسعه اقتصاد دیجیتالی باز و مقایسه‌پذیر در مقابل اقتصاد متمرکز فعلی، می‌گشاید. فرصت‌های بسیار بزرگی در پس این فناوری نهفته است و تحولات در این زمینه، تازه آغاز شده و کشورها و دولت‌ها مطالعه پیرامون این فناوری را آغاز کرده‌اند. برای مثال یکی از نمایندگان شرکت آی.بی.ام با شرکت در جلسات استماع کنگره آمریکا، مزیت‌های این فناوری و نحوه استفاده بخش دولتی از فناوری زنجیره بلوکی را به نمایندگان معرفی کرد (جری کوما، ۱۳۹۵). بانک مرکزی چین، کارگروه بررسی زنجیره بلوکی دولت روسیه، مجلس ملی فرانسه، پارلمان اتحادیه اروپا و بسیاری از دیگر دولت‌های جهان، مطالعه و بهره‌مندی از مزایای این فناوری را در دستورکار خود قرار داده‌اند.

فناوری زنجیره بلوکی اولین بار فقط برای تبادل ارزهای دیجیتالی به‌وجود آمده بود، ولی ویژگی‌هایی مانند متن‌باز بودن، رایگان بودن، امکان ثبت اسناد به‌صورت عمومی و غیرمتمرکز بودن آن باعث شد تا برای ارائه خدمات مختلفی مورد استفاده قرار گیرد. یکی از مسائل کلان و راهبردی کشور ایران بحث انتخابات و شمارش آرای انتخاباتی است. ازجمله اختراعات ثبت شده در زمینه فناوری زنجیره بلوکی، استفاده از این فناوری در زمینه ثبت و شمارش آرای انتخاباتی است. در این گزارش با معرفی زنجیره بلوکی و کاربردهای آن، امکان استفاده از این فناوری را برای موضوع انتخابات مورد بررسی قرار می‌گیرد. بنابراین ابتدا به معرفی ساده فناوری زنجیره بلوکی پرداخته می‌شود و سپس

۱. رجوع شود به: گزارش مرکز پژوهش‌هاي مجلس، بيتكوين ابزاري نوين در نظام پرداخت‌هاي الكترونيكي، شماره ۱۳۶۱۷.
2. Distributed Consensus

تاریخچه فناوری و روند توسعه آن مورد بررسی قرار می‌گیرد و نیز کاربردهای آن در زمینه امور مالی، بیمه، ثبت رسمی اسناد و مقابله با جعل معرفی می‌شود.

معرفی فناوری زنجیره بلوکی

فناوری زنجیره بلوکی[1] اساساً یک پایگاه داده توزیع شده از اسناد و یا دفترکل عمومی[2] از همه تراکنش‌ها یا رویدادهای دیجیتال[3] است که توسط اجزای تشکیل‌دهنده‌اش به شکل مشترک اجرا می‌شود. هر تراکنش در دفتر کل عمومی با توافق اکثریت اجزای سیستم محقق می‌گردد. اطلاعاتی که یکبار وارد سیستم شده باشد، هرگز پاک نمی‌شود. زنجیره بلوکی برای هر تراکنش منحصر به فردی که ایجاد شده باشد، اطلاعات قطعی و قابل بازبینی را ثبت می‌کند. برای مثال دزدیدن کلوچه از مغازه‌ای خلوت بسیار ساده‌تر از دزدیدن آن از یک فروشگاه بزرگ در حضور هزاران شاهد است.

بیتکوین[4] (پول دیجیتالی)[5] محبوب‌ترین نمونه‌ای است که براساس فناوری زنجیره بلوکی به‌وجود آمده و نامشان با هم عجین است. بیتکوین بحث‌برانگیزترین نمونه است، زیرا بازار جهانی چند میلیون دلاری را ایجاد کرده است که در آن می‌توان بدون نیاز به کنترل‌های دولتی تراکنش‌هایی را به‌طور ناشناس انجام داد. ازاین‌رو با مواردی برای هماهنگ‌سازی دولت‌های بین‌المللی و مؤسسات مالی مواجه است.

به هرحال فناوری زنجیره بلوکی به خودی خود جنجال‌برانگیز نیست و در طی سال‌ها به‌طور بی‌نقص و موفق در برنامه‌های کاربردی بین‌المللی مالی و غیرمالی به‌کار گرفته شده است. اظهارنظرهای متعددی در تأیید اهمیت فناوری زنجیره بلوکی وجود دارد. برای مثال یکی از کارشناسان معتبر فناوری اطلاعات مدل «زنجیره بلوکی توزیع‌یافته تطبیق‌پذیر» را مهمترین نوآوری بعد از اینترنت معرفی کرده است. «یوهان پالیچاتا» از بانک مشهور پاریباس بی.ان.پی در مجله «کوینتسنس» در مورد زنجیره بلوکی بیتکوین نوشته است: نقش نرم‌افزاری که امکان عملیاتی شدن واحد پول دیجیتال را به‌وجود آورده است، نظیر نقش اختراع موتور بخار یا موتور احتراقی در دنیای صنعت است و قابلیت این را دارد تا جهان مالی و آنچه در آن است را متحول کند.

این فناوری می‌تواند دنیای دیجیتال را متحول کند و با استفاده از خصوصیت «تفاهم توزیع‌یافته» برای هر تراکنش آنلاین قدیمی یا فعلی، تراکنش‌ها را به نحوی اجرا نماید که دارایی‌های دیجیتالی در آینده نیز قابل شناسایی باشند و این امر بدون در خطر افتادن حریم خصوصی و رعایت امنیت دارایی‌های دیجیتال و طرف‌های درگیر انجام می‌پذیرد.

1. Block chain
2. Ledger
3. Digital Events
4. Bitcoin
5. Digital Money

تفاهم توزیع‌یافته و حفظ حریم خصوصی، دو خصوصیت مهم و اصلی فناوری زنجیره بلوکی‌اند.

مزایای استفاده از فناوری زنجیره بلوکی بیش از مشکلات هماهنگ‌سازی و چالش‌های فنی آن است. یکی از موارد کلیدی نوظهور در استفاده از فناوری زنجیره بلوکی، «**قراردادهای هوشمند**»[1] است. قراردادهای هوشمند در اصل برنامه‌های رایانه‌ای هستند که می‌توانند به شکل خودکار، شرایط قرارداد را اجرا کنند. وقتی طرف‌های معامله با یک وضعیت از قبل تعیین شده در قرارداد هوشمند مواجه می‌شوند، می‌توانند به‌طور خودکار و براساس قرارداد مورد توافق، پرداخت‌ها را به‌صورت شفاف انجام دهند.

دارایی هوشمند،[2] مفهوم مرتبط دیگری است که درخصوص کنترل مالکیت دارایی‌ها از طریق زنجیره بلوکی و با استفاده از قراردادهای هوشمند به‌کار برده می‌شود. در اینجا دارایی می‌تواند اتومبیل، خانه، تلفن هوشمند و غیره از نوع فیزیکی و یا اینکه سهام شرکت‌ها از نوع غیرفیزیکی باشد.

مؤسسات مالی و بانک‌ها، دیگر فناوری زنجیره بلوکی را به‌عنوان تهدیدی برای مدل‌های کسب‌وکار سنتی خود به‌حساب نمی‌آورند. درواقع بزرگترین بانک‌های جهان با تحقیق و مطالعه درخصوص برنامه‌های کاربردی نوآورانه مبتنی‌بر زنجیره بلوکی، به‌دنبال فرصت‌های جدید هستند. مؤسس و مدیرعامل یکی از بانک‌های معتبر کشور استونی در یکی از مصاحبه‌های خود بیان داشت که آنها، زنجیره بلوکی را به‌عنوان امن‌ترین و آزموده‌شده‌ترین بستر برای برخی از برنامه‌های کاربردی بانکداری و امور مالی به‌شمار می‌آورند.[3]

برای برنامه‌های غیرمالی نیز فرصت‌های تجاری بی‌شماری وجود دارد. اطلاعات مربوط به تأییدیه تمامی اسناد حقوقی، مستندات پزشکی، پرداخت حق سهم تولیدکنندگان یک اثر هنری در صنعت موسیقی، دفتر اسناد رسمی، اوراق بهادار و مجوزهای ازدواج، به‌وسیله زنجیره بلوکی قابل نگهداری است.

تاریخچه مختصر بیتکوین به‌عنوان اولین کاربرد فناوری زنجیره بلوکی

در سال ۲۰۰۸ شخص یا گروهی به نام «ساتوشی ناکاماتو»[4] مقاله‌ای را با عنوان «بیت کوین: سیستم پول نقد الکترونیکی همتا به همتا»[5] منتشر کرد. این مقاله، نسخه‌ای از پول نقد الکترونیکی را معرفی می‌کرد که قادر به انجام پرداخت‌های آنلاین به‌صورت مستقیم از یک شخص به شخص دیگر (بدون نیاز به عبور از سیستم یک مؤسسه مالی) بود. بیتکوین اولین اشاره به این مفهوم بود. هم‌اکنون کلمه «ارز رمزپایه» برچسبی برای توصیف تمام شبکه‌ها و رسانه‌های ارزی است که با استفاده از رمزنگاری،

1. Smart Contract
2. Smart Asset
3. Corsbyete, 2015.
4. Satoshi Nakamoto
5. Peer to peer

تراکنش‌های ایمن را ایجاد می‌کند و در برابر سامانه‌هایی قرار می‌گیرد که در آن تراکنش‌ها از طریق یک نهاد مرکزی مورد اطمینان کانال‌دهی می‌شوند.

نویسنده مقاله اولیه قصد داشت ناشناس بماند و تا به امروز در مورد هویت «ساتوشی ناکاماتو» تفاهم صورت نگرفته است. چند ماه بعد، یک برنامه با منبع آزاد به‌منظور پیاده‌سازی این پروتکل جدید منتشر شد که برای شروع با استفاده از قالب مولد[1] ۵۰ سکه تعریف می‌کرد. همه می‌توانستند این برنامه منبع آزاد را نصب کنند و بخشی از شبکه همتا به همتای بیتکوین شوند و این سیر صعودی محبوبیت از همان زمان شروع شد.

- در سال ۲۰۰۸
  - ۱۸ آگوست: دامنه تبا نام «bitcoin.org» ثبت شد.
  - ۳۱ اکتبر: مقاله طرح بیتکوین منتشر شد.
  - ۹ نوامبر: پروژه بیتکوین در SourceForge.net ثبت شد.
- در سال ۲۰۰۹
  - ۳ ژانویه: قالب مولد در ساعت 18:15:05 GMT ایجاد شد.
  - ۹ ژانویه: بیتکوین نسخه ۰/۱ منتشر شد.
  - ۱۲ ژانویه: اولین تراکنش بیتکوین در قالب ۱۷۰ از «ساتوشی» به «هال فینی» روی داد.

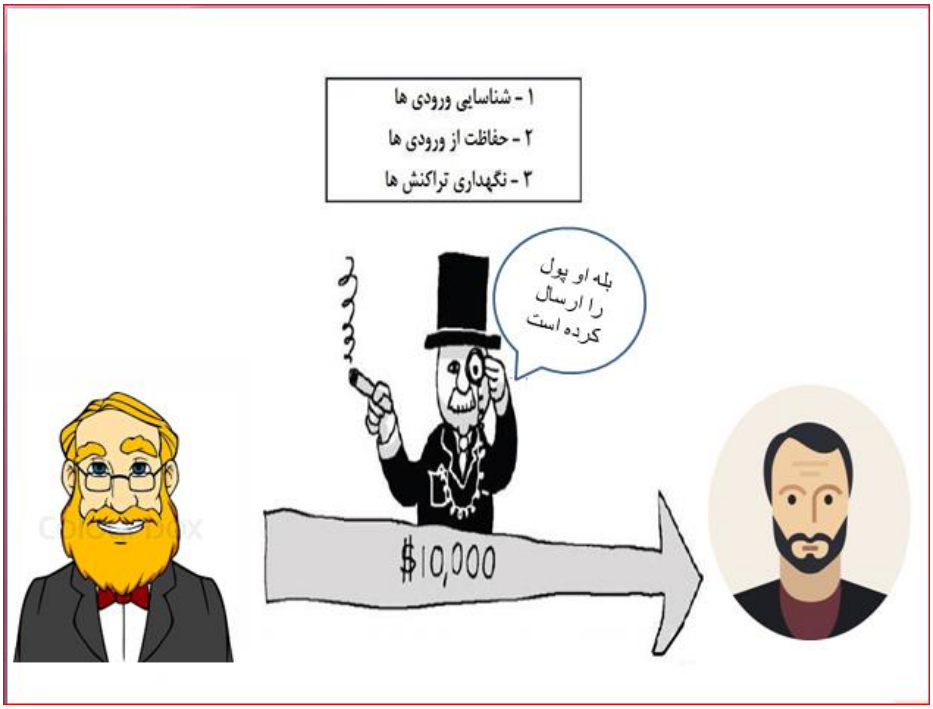
از آن تاریخ به بعد افزایش محبوبیت بیتکوین هیچگاه متوقف نشده است و فناوری زیرساختی زنجیره بلوکی اینک طیف جدیدی از برنامه‌های مالی را پوشش می‌دهد.

توضیح فنی فناوری زنجیره بلوکی

از آنجایی‌که مفهوم زنجیره بلوکی و بیتکوین اساساً به هم متصل‌اند، می‌توان مفهوم زنجیره بلوکی را با توضیح چگونگی کارکرد بیتکوین توضیح داد. هرچند که فناوری زنجیره بلوکی برای همه نوع تبادلات و تراکنش‌های مربوط به دارایی‌های دیجیتالی برخط قابل استفاده است.

1. Genesis Block

شکل ۱. تراکنش‌های آنلاین سنتی با استفاده از طرف سوم (بانک‌ها، طرف‌های پرداخت و غیره)



تجارت اینترنتی به‌طور انحصاری با مؤسسات مالی که به‌عنوان طرف سوم با ارائه خدمات مطمئن، واسطه تراکنش‌های الکترونیکی‌اند، عجین است. نقش طرف سوم مورد اعتماد، شناسایی، محافظت و نگهداری از تراکنش‌هاست. درصد معینی از تقلب در معاملات برخط یا آنلاین اجتناب‌ناپذیر است و همین امر باعث می‌شود تا نیازمند حضور طرف سوم برای واسطه‌گری در تراکنش‌های مالی باشیم و این موجب بالا رفتن هزینه تراکنش‌ها می‌شود. **بیتکوین به‌جای استفاده از طرف سوم مورد اعتماد در اجرای تراکنش برخط بین دو طرف، از نشانه‌های رمزگذاری استفاده می‌کند**. هر تراکنش از طریق یک امضای دیجیتالی[1] حفاظت می‌شود. هر تراکنش که با کلید خصوصی فرستنده امضای دیجیتالی شده باشد به کلید عمومی گیرنده ارسال می‌شود. به‌منظور خرج کردن پول، صاحب پول رمزگذاری شده، باید ثابت کند که مالکیت کلید خصوصی را داراست. نهادی که ارز دیجیتالی را دریافت می‌کند، امضای دیجیتالی (مالکیت کلید خصوصی) آن را با استفاده از کلید عمومی فرستنده شناسایی می‌کند.

هر تراکنش به تمامی گره‌های شبکه بیتکوین انتشار می‌یابد و بعد از شناسایی در دفتر کل عمومی ثبت می‌شود. هر تراکنش مجزا پیش از آنکه در دفتر کل عمومی ثبت شود، باید شناسایی شده و معتبر شناخته شود.

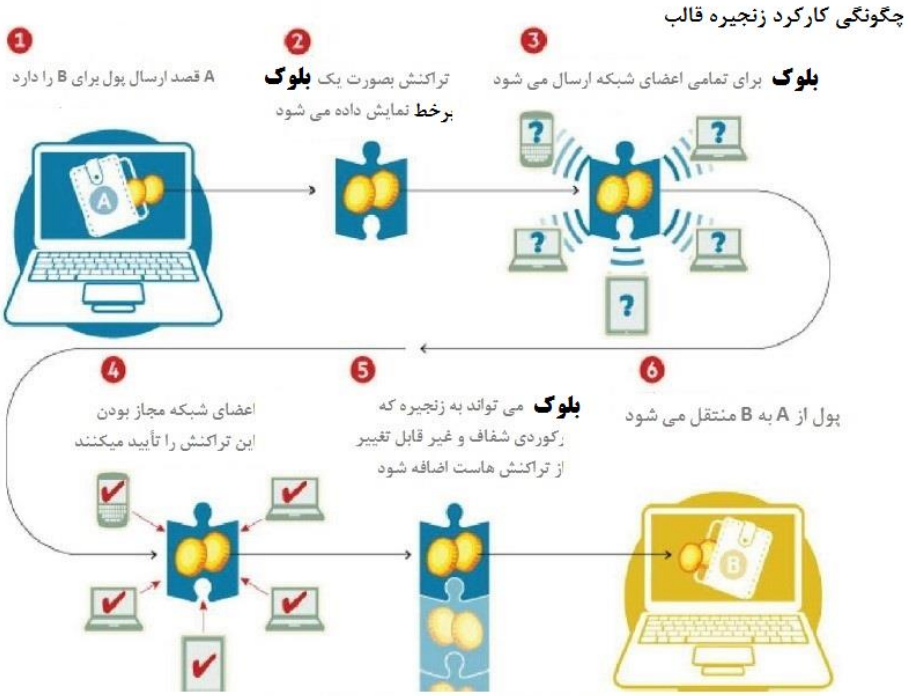
گره‌های شناسایی‌کننده باید پیش از ثبت هر تراکنش از دو موضوع اطمینان یابند:

1. Digital Signature

۱. پرداخت‌کننده، امضای دیجیتال معتبر رمزگذاری شده، برای انجام تراکنش را داراست.

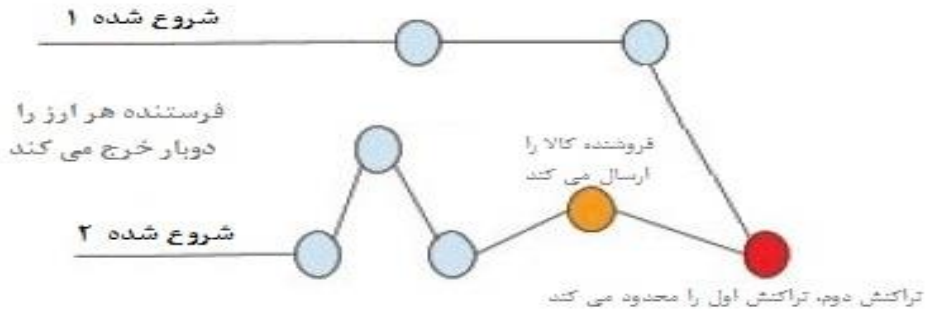
۲. پرداخت‌کننده، پول رمزگذاری شده کافی در حساب خود دارد: تمامی تراکنش‌های حساب (کلید عمومی) پرداخت‌کننده در دفتر کل باید کنترل شود تا از کفایت موجودی حساب خود مطمئن شود.

شکل ۲. تراکنش‌های مالی با استفاده از فناوری زنجیره بلوکی



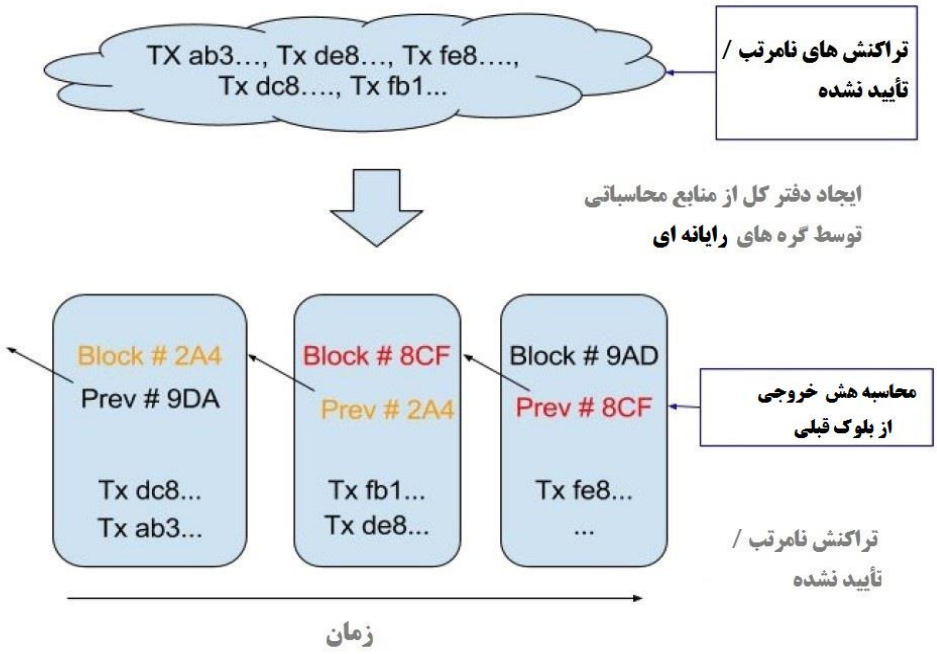
در اینجا مسئله حفظ ترتیب تراکنش‌های منتشر شده به سایر گره‌ها در شبکه همتا به همتای بیتکوین، مطرح می‌شود. تراکنش‌ها به ترتیبی که ایجاد شده‌اند انجام نمی‌شوند و به همین علت به سامانه‌ای نیاز داریم که به ما اطمینان دهد که پول رمزگذاری شده، دوبار پرداخت نشود (شکل۳). برای درنظر گرفتن این موضوع، تراکنش‌ها باید گره به گره در طول شبکه بیتکوین منتقل شوند و هیچ ضمانتی وجود ندارد که ترتیب دریافت تراکنش‌ها در گره‌ها با ترتیب ایجاد آنها مطابقت داشته باشد.

شکل ۳. پرداخت مجدد به‌علت تأخیر انتشار در شبکه همتا به همتا



این بدان معناست که مکانیسمی مورد نیاز است تا کل شبکه بیتکوین بتواند درمورد ترتیب تراکنش‌ها به توافق برسد و این مشکلی اساسی در سیستم‌های توزیع‌یافته است.

شکل ۴. تولید زنجیره بلوکی از تراکنش‌های نامرتب



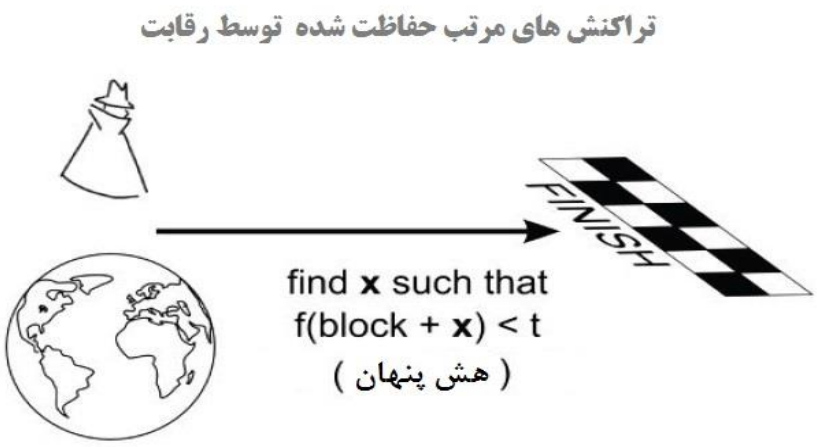
بیتکوین این مشکل را با مکانیسم فناوری زنجیره بلوکی حل کرده است. سیستم بیتکوین با قرار دادن تراکنش‌ها در گروهی از زنجیره‌های بلوکی و سپس اتصال این زنجیره‌های بلوکی به هم، آنها را مرتب می‌کند. تراکنش‌های هربلوک باید به‌طور همزمان روی دهند. این زنجیره‌های بلوکی مانند زنجیره‌ای در یک خط با توالی زمانی به هم متصل

هستند و هر بلوک خروجی تابع درهم‌سازی (هش)[1] از بلوک پیشین خود را ذخیره می‌کند.

هنوز یک مشکل باقی است. هر گره روی شبکه می‌تواند درخواست تراکنش‌های تأیید نشده را گرفته و از آن یک بلوک بسازد و روی شبکه به‌عنوان پیشنهادی برای تولید بلوک بعدی زنجیره بلوکی منتشر کند. شبکه چطور باید تصمیم بگیرد که کدام بلوک باید بلوک بعدی زنجیره بلوکی باشد؟ ممکن است زنجیره‌های بلوکی مختلفی توسط گره‌های مختلف به‌طور همزمان ایجاد شده باشند. تا زمانی‌که زنجیره‌های بلوکی بتوانند با ترتیب‌های مختلف در نقاط مختلف شبکه دریافت شوند، نمی‌توان به هیچ ترتیبی اعتماد کرد.

بیتکوین این مسئله را با تعریف یک معمای ریاضی حل کرده است. هر بلوکی که بخواهد به زنجیره بلوکی اضافه شود، باید در محتوای خود پاسخی برای یک مسئله ریاضی بسیار خاص داشته باشد که به آن «اثبات کارکرد» می‌گویند. گره‌ای که یک بلوک را تولید می‌کند، باید ثابت کند که منابع محاسباتی کافی برای حل معمای ریاضی را دارد. برای مثال، یک گره باید بتواند یک «مقدار موقت» را بیابد که با استفاده از آن خروجی تابع درهم‌ساز بلوک پیشین یا هشی را که با تعدادی مشخص از صفرها شروع می‌شود، ایجاد کند. متوسط تلاش‌های لازم، براساس تعداد بیت‌های صفر مورد نیاز تعریف می‌شود. اما فرآیند بازشناسی آن بسیار ساده است و با اجرای یک تابع درهم‌ساز انجام‌پذیر است.

شکل ۵. رقابت ریاضی برای حفاظت از تراکنش‌ها

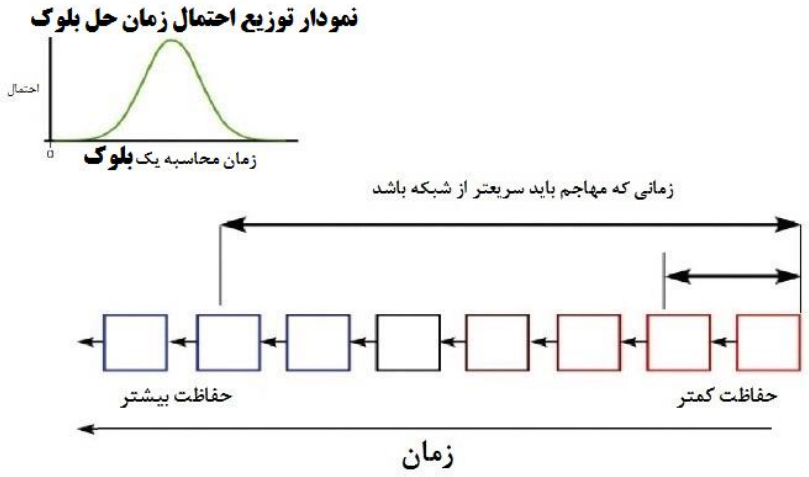


حل این معمای ریاضی ساده نیست و میزان پیچیدگی آن قابل تنظیم است. برای مثال می‌توان درجه دشواری مسئله را طوری تنظیم کرد که میانگین زمان حل آن برای یک گره در شبکه بیتکوین برای تولید بلوک ده دقیقه باشد و امکان اینکه بیش از یک بلوک در سیستم در زمان داده شده ساخته شود، بسیار ناچیز است. اولین گره‌ای که مسئله را حل کند بلوک خود را به سایر گره‌های زنجیره بلوکی انتشار می‌دهد. اگر درحالت خاص بیش از یک بلوک به‌صورت همزمان ساخته شود، به چند انشعاب مختلف منجر خواهد شد. هرچند مسئله‌ای که باید حل شود به قدری پیچیده است که زنجیره

1. Hash

بلوکی به‌سرعت تثبیت می‌شود و تمامی گره‌ها در مورد ترتیب زنجیره‌های بلوکی اخیر زنجیره توافق دارند. گره‌ها، منابع محاسباتی خود را برای حل مسئله به اشتراک می‌گذارند و بلوکی به‌عنوان «کمینه» را می‌سازند و درنهایت برای تلاش‌هایشان پاداش می‌گیرند.

شکل ۶. رقابت ریاضی برای حفاظت از تراکنش‌ها



شبکه فقط بلندترین زنجیره بلوکی را به‌عنوان زنجیره بلوکی معتبر شناسایی می‌کند. ازاین‌رو برای یک مهاجم تقریباً غیرممکن است که بتواند تراکنش تقلبی خود را تعریف کند، زیرا نه تنها باید بلوکی تولید کند که مسئله ریاضی را حل کرده باشد، بلکه باید به‌طور همزمان زنجیره‌های بلوکی پیشین را نیز بازسازی کند، به‌طوری‌که سایر گره‌های شبکه، آنها را مجاز بدانند. انجام این کار به‌علت اینکه زنجیره‌های بلوکی به‌صورت رمزگذاری شده به هم متصل شده‌اند، دشوارتر نیز می‌شود.

کاربردهای فناوری زنجیره بلوکی

فناوری زنجیره بلوکی، قابل راهیابی به برنامه‌های کاربردی در دو زمینه مالی و غیرمالی است، که به‌طور سنتی برای اعتباردهی و محافظت از تراکنش‌های آنلاین دارایی‌های دیجیتال بر طرف سوم مورد اعتماد، متکی هستند.

ایده برنامه کاربردی «قرارداد هوشمند» در سال ۱۹۹۴ به‌وسیله «نیک اسزابو» معرفی شد که ایده‌ای بزرگ برای اجرای خودکار قراردادها بین طرف‌های مربوط بود، اما تا زمان ایجاد پرداخت‌های برنامه‌پذیر و ارزهای رمزنگاری شده مورد استقبال قرار نگرفت. در این زمان بود که دو برنامه زنجیره بلوکی و قرارداد هوشمند با همکاری هم توانستند پرداخت‌ها را با شرایط از پیش برنامه‌ریزی شده یک توافق قراردادی راه‌اندازی کنند. قراردادهای هوشمند در حقیقت برنامه‌های کاربردی قدرتمندی در

دنیای ارز رمزگذاری شده هستند.

قراردادهای هوشمند، قراردادهایی هستند که به‌طور خودکار توسط پروتکل‌های رایانه‌ای اجرا می‌شوند. استفاده از فناوری زنجیره بلوکی موجب شد ثبت، شناسایی و اجرای قراردادهای هوشمند آسان‌تر شود. شرکت‌های متن باز مانند اتریوم و کودیوس امکان استفاده قراردادهای هوشمند از فناوری زنجیره بلوکی را فراهم کردند. بسیاری از شرکت‌هایی که روی موضوع بیتکوین و فناوری‌های زنجیره بلوکی کار می‌کردند قراردادهای هوشمند را نیز پشتیبانی می‌کنند و همچنین بسیاری از وضعیت‌هایی که در آن سرمایه تنها با وجود شرایط خاصی قابل انتقال بود (از قبیل ایجاد قراردادهای حضوری توسط وکلا و یا ارائه خدمات سپرده توسط بانک‌ها)، با کمک قراردادهای هوشمند جایگزین شد.

شرکت اتریوم بر این اساس یک پلتفرم برنامه‌پذیر ایجاد کرده است. اتریوم به افراد اجازه می‌دهد تا ارز رمزگذاری شده خود را بسازند و از آن برای اجرا و پرداخت قراردادهای هوشمند خود استفاده کنند. اتریوم برای خدمات پرداخت خود از ارز رمزگذاری شده اتر استفاده می‌کند. اتریوم طیف گسترده‌ای از برنامه‌های کاربردی اولیه در زمینه‌هایی نظیر حکمرانی، بانکداری مستقل، دسترسی بدون کلید، سرمایه‌گذاری و امور مالی تجاری با استفاده از قراردادهای هوشمند است.

همچنین تعدادی زنجیره بلوکی وجود دارند که از طیف گسترده‌ای از برنامه‌ها (نه فقط از برنامه‌های مربوط به ارز رمزگذاری شده). پشتیبانی می‌کنند درحال حاضر سه خط‌مشی در صنعت برای پشتیبانی از سایر برنامه‌ها و غلبه بر محدودیت‌های زنجیره بلوکی بیتکوین وجود دارد:

زنجیره بلوکی جایگزین‌شونده:[1] سیستمی است که با استفاده از الگوریتم زنجیره بلوکی آن به تفاهم توزیع شده درخصوص یک دارایی دیجیتالی خاص می‌پردازند. ممکن است منابع خود را از طریق شبکه‌ای مانند بیتکوین به اشتراک بگذارند که به آن منابع ادغامی می‌گویند. پیشنهاد شده است که با استفاده از زنجیره بلوکی برنامه‌هایی را از قبیل DNS،[2] SSL،[3] تأییدکننده گواهی، ذخیره‌سازی فایل‌ها و سیستم رأی‌گیری پیاده‌سازی کنند.

پروتکل مرجع آزاد «کالرد کوین»:[4] دسته‌ای از روش‌ها را برای سازندگان تعریف کرده است تا توسط آن دارایی‌های دیجیتالی در بالای زنجیره بلوکی بیتکوین و با استفاده از قابلیت‌های کاربردی ارز دیجیتالی تعریف شود.

«سایدچین‌ها»:[5] (زنجیره‌های جانبی) زنجیره‌های بلوکی تناوبی‌ای هستند که از طریق قرارداد بیتکوین پشتیبانی می‌شوند (مانند دلار و پوند که با طلا پشتیبانی می‌شوند). می‌توان هزاران زنجیره جانبی ایجاد کرد که هر کدام با مشخصه‌ها و اهداف متفاوت به سامانه بیتکوین متصل‌اند. تمام آنها

1. Alternative Blockchains
2. Domain Name System

۳. پروتکل حفظ امنیت مشاهده وبگاه‌ها.

4. Colored Coins
5. Side Chains

خاصیت منحصر به فرد بودن و انعطاف‌پذیری را به ضمانت زنجیره بلوکی بیتکوین دارند. زنجیره بلوکی بیتکوین در مقابل می‌تواند با تکرار خود از ویژگی‌های اضافه شده برای زنجیره‌های جانبی پشتیبانی کند.

شرکت‌هایی نظیر IBM، سامسونگ، اورستاک، آمازون، UBS، سی تی، EBAY و وریزون، تنها تعداد کمی از شرکت‌هایی هستند که به جستجوی کاربردهای جدید و متفاوت زنجیره بلوکی در برنامه‌های خود می‌پردازند. ۹ بانک بزرگ بین‌المللی، شامل بانک بارکلی و گلدمن، اخیراً (۱۵ سپتامبر ۲۰۱۵) با شرکت فناوری مالی نیویورکی R3 متحد شده‌اند تا چارچوبی در استفاده از فناوری زنجیره بلوکی در بازارهای مالی ایجاد کنند. ازجمله بانک‌های پیشرو در این زمینه می‌توان به بانک‌های جی.پی.مورگان، استریت استیت، UBS، بانک رویال اسکاتلند، کردیت سوئیس، BBVA و بانک کامانولت استرالیا نیز اشاره کرد که به این طرح ابتکاری پیوسته‌اند.

کاربردهای فناوری در زنجیره بلوکی به دو دسته کاربردهای مالی و غیرمالی قابل تقسیم است:

الف) استفاده از زنجیره بلوکی در فعالیت‌های مالی

عمومی کردن سهام یک شرکت بسیار پرهزینه است. یک اتحادیه از بانک‌ها باید برای تضمین معاملات و جذب سرمایه‌گذاران اقدام کنند. بورس باید فهرستی از سهام شرکت را در بازار فرعی به اشتراک گذارد تا معاملات به‌صورت مطمئن و در زمان منطقی انجام گرفته و تسویه شود. درحال حاضر به‌صورت نظری، شرکت‌ها می‌توانند به‌طور مستقیم سهامشان را از طریق زنجیره بلوکی صادر کنند. این سهام‌ها می‌تواند بعداً در بازار ثانویه که روی زنجیره بلوکی نصب شده است، خرید و فروش شود. در اینجا مثال‌هایی آورده شده است:

- **استفاده از زنجیره بلوکی در بازار سهام**

شرکت خصوصی نزدک:[1] این شرکت بورس مبادله دیون و سهام خصوصی خود را در سال ۲۰۱۴ ارائه کرد. این شرکت به‌منظور عرضه ویژگی‌های کلیدی مانند جدول علی‌الرأس اموال و مدیریت ارتباط سرمایه‌داران برای شرکت‌هایی که به عرضه اولیه سهام اقدام کرده‌اند و شرکت‌های خصوصی ایجاد شده است. درحال حاضر در بازار سهام اولیه، پروسه مبادلات سهام بسیار کُند است و این کُندی به‌علت وجود واسطه‌های چندگانه است. شرکت نزدک با شرکت نوپای چاین دات کام[2] برای پیاده‌سازی بورس سهام خصوصی از طریق زنجیره بلوکی همکاری می‌کند و به پیاده‌سازی قراردادهای هوشمند مبتنی‌بر زنجیره بلوکی می‌پردازد تا بتواند عملیات بورس را پیاده‌سازی کند. انتظار می‌رود این محصول سریع، قابل پیگیری و کارآ باشد.

پروژه‌ها و برنامه‌های کاربردی **مدیسی، بلاک استریم، کوین ستر، آگور و بیت شیرز** سایر

1. Nasdaq
2. chain.com

نمونه‌ها در این باره هستند.

- **استفاده از زنجیره بلوکی در امور بیمه**

دارایی‌هایی که می‌توانند به‌صورت منحصر به‌فرد به‌وسیله یک یا چند شناسه مشخص شوند و به سختی امکان تخریب یا جایگزینی دارند در زنجیره بلوکی ثبت می‌شوند. از این موضوع می‌توان برای شناسایی مالکیت دارایی و پیگیری تاریخچه تراکنش‌های آن استفاده کرد. هر دارایی (فیزیکی یا دیجیتالی نظیر املاک، اتومبیل‌ها، دارایی‌های فیزیکی، لپتاپ و سایر چیزهای ارزشمند) می‌تواند در زنجیره بلوکی ثبت شده و مالکیت و تاریخچه تراکنش‌های آن توسط هر شخص به‌خصوص بیمه‌گذار شناسایی شود.

اورلجر شرکتی است که با استفاده از فناوری زنجیره بلوکی، شناسنامه الماس‌ها و تاریخچه تراکنش‌های آنها را در یک دفتر کل ثبت می‌کند. خصوصیات منحصر به‌فرد مشخص‌کننده الماس‌ها از قبیل ارتفاع، عرض، وزن، قطر، رنگ و غیره به‌صورت رمزگذاری شده در این دفتر ثبت می‌شوند و شرکت‌های بیمه، آژانس‌های مجری قانون، مالکان و مدعیان می‌توانند برای شناسایی و تأیید الماس‌ها از آن استفاده کنند. این شرکت یک خدمت تحت وب (API) برای بررسی الماس‌ها دارد که شامل ایجاد، خواندن، به‌روزرسانی ادعاها (توسط شرکت‌های بیمه) و ایجاد، خواندن، به‌روزرسانی گزارش‌های پلیس در مورد الماس‌ها است.

ب) کاربردهای غیرمالی زنجیره بلوکی

در این بخش، دفاتر اسناد رسمی، ذخیره‌سازی غیرمتمرکز، اینترنت اشیا، روش‌های ضدجعل و برنامه‌های کاربردی اینترنتی، به‌مثابه کاربردهای غیرمالی زنجیره بلوکی معرفی می‌شوند.

- **دفتر اسناد رسمی**

شناسایی اعتبار اسناد می‌تواند از طریق زنجیره بلوکی انجام گرفته و نیاز به استعلام از مرجع مرکزی را از بین ببرد. این خدمت می‌تواند برای اسناد در سه زمینه گواهی سند صادر کند: در اثبات مالکیت (مالک آن سند کیست)، اثبات وجود (در یک زمان مشخص سند وجود داشته است) و اثبات اصالت سند (اینکه سند دستکاری نشده است). از آنجایی‌که این خدمات ضدجعل است و می‌تواند توسط طرف‌های ثالث اعتبارسنجی شود از لحاظ حقوقی الزام‌آور است. استفاده از زنجیره بلوکی برای گواهی محضری و رسمی، باعث حفظ حریم خصوصی صاحبان اسناد و افراد خواهان تأیید اسناد می‌شود. با انتشار مدارک با استفاده از رمزگذاری فایل‌ها در زنجیره بلوکی، مدت زمان انجام امور در دفاتر اسناد رسمی به‌شدت کاهش خواهد یافت. با توجه به قانون تجارت الکترونیکی ایران، این امکان فراهم است تا دیگر نیازی به پرداخت هزینه‌های سنگین برای گواهی محضری و رسمی و همچنین روش‌های بی

مورد و زمان بر استعلام‌های اسناد نباشد.

استمپری،[1] بلاک نوتاری،[2] ویاکوین،[3] کریپتوپابلیک نوتاری،[4] پروف آف اگزیستنس[5] و اسکرایب[6] نمونه‌هایی از شرکت‌های عرضه‌کننده خدمات دفاتر اسناد رسمی با کمک فناوری زنجیره بلوکی هستند.

- **ذخیره‌سازی غیرمتمرکز**

روش‌های ذخیره‌سازی ابری برای ذخیره‌سازی اسناد، عکس‌ها، فیلم‌ها و فایل‌های موسیقی نظیر دراپ‌باکس، گوگل درایو به‌شدت درحال محبوبیت یافتن است. با وجود محبوبیت، این روش‌های ذخیره‌سازی فایل معمولاً با چالش‌هایی در زمینه‌های امنیت حریم خصوصی و کنترل اطلاعات مواجه‌اند. مسئله اصلی این است که فرد باید درمورد فایل‌های محرمانه و شخصی خود به مرجع ثالثی اعتماد کند.

استوراج،[7] زنجیره‌ای بلوکی براساس پلتفرم ذخیره‌سازی ابر توزیع شده همتا به همتا دارد که امکان انتقال و به اشتراک‌گذاری اطلاعات را بدون نیاز به مرجع ثالث برای کاربران فراهم کرده است. این موضوع به افراد اجازه می‌دهد تا پهنای باند اینترنتی استفاده نشده یا فضای دیسک خالی رایانه‌های شخصی خود را در برابر پرداخت‌های مبتنی‌بر بیتکوین در اختیار کسانی که نیاز به ذخیره فایل‌های بزرگ دارند، قرار دهند.

نبود کنترل مرکزی اکثر خطاها و مشکلات سنتی اطلاعاتی را از بین می‌برد و همچنین باعث افزایش امنیت حریم خصوصی و کنترل داده می‌شود. پلتفرم استورج براساس الگوریتم رقابتی است تا کاربران را برای مشارکت در این شبکه تشویق کند. از این طریق پلتفرم استورج می‌تواند به‌صورت دوره‌ای و رمزگذاری شده صحت و در دسترس بودن فایل را نیز کنترل کند و پاداش‌های مستقیم به کسانی که در ذخیره‌سازی و حفاظت فایل شرکت داشته‌اند، ارائه دهد.

در اینجا از پرداخت‌های بیتکوینی هم به‌عنوان مشوق و هم نوعی پرداخت، استفاده شده و از یک زنجیره بلوکی جداگانه برای ذخیره‌سازی فایل فراداده استفاده می‌شود.

- **اینترنت اشیای غیرمتمرکز**

محبوبیت IOT یا اینترنت اشیای غیرمتمرکز چه در فضاهای تولیدی و چه در فضاهای سرمایه‌گذاری با رشدی روزافزون مواجه است. تعداد زیادی از پلتفرم‌های اینترنت اشیا براساس مدل متمرکزی ارائه

1. Stampery
2. Block Notary
3. Viacoin
4. Crypto Public Notary
5. Proof of Existence
6. Ascribe
7. STORJ

شده‌اند که در آن یک واسط یا هاب، تعامل بین دستگاه‌ها را کنترل می‌کند. هرچند که این روش برای بسیاری از سناریوها که در آن دستگاه‌ها نیاز به تبادل اطلاعات با هم و بدون واسطه دارند، غیرعملی است. این وضعیت خاص باید با کوشش بر ایجاد پلتفرم‌های غیرمتمرکز اینترنت اشیا، بهبود یابد.

فناوری زنجیره بلوکی پیاده‌سازی سکوهای اینترنت اشیای غیرمتمرکز را تسهیل می‌کند و امکان تبادل ایمن و مطمئن اطلاعات و ثبت داده‌ها را فراهم می‌آورد. در چنین ساختاری زنجیره بلوکی نقش دفتر کل عمومی را برعهده دارد و تمامی پیام‌های مبادله شده بین دستگاه‌های هوشمند در یک ریخت‌شناسی اینترنت اشیای غیرمتمرکز به‌صورت مطمئن ثبت می‌شود.

پلتفرم ادپت: شرکت آی.بی.ام با مشارکت شرکت سامسونگ، این پلتفرم را ارائه داده است (دورسنجی همتا به همتای غیرمتمرکز خودگردان) که از اجزای زیرساختی طرح بیتکوین برای ساخت یک شبکه توزیع شده از دستگاه‌های غیرمتمرکز از اینترنت اشیا استفاده کرده است. ادپت از سه پروتکل بیت تورنت (اشتراک‌گذاری فایل) اتریوم (قراردادهای هوشمند) و تله هش (پیام‌رسانی همتا به همتا) در پلتفرم خود استفاده می‌کند.

فیلامنت: شرکت نوپایی است که بسته نرم‌افزاری اینترنت اشیای غیرمتمرکز را با استفاده از زنجیره بلوکی بیتکوین تولید کرده است. این بسته نرم‌افزاری امکان فعال کردن دستگاه‌ها در اینترنت اشیا و ذخیره مشخصه‌های منحصر به‌فرد آنها را در یک دفتر کل عمومی دارد.

- **روش‌های ضدجعل مبتنی‌بر زنجیره بلوکی**

جعل یکی از بزرگترین مشکلاتی است که تجارت مدرن در دنیای دیجیتال امروزی با آن روبرو است. راه‌حل‌های ارائه شده فعلی، مبتنی‌بر اعتماد و اطمینان به مرجع قابل اطمینان ثالث است که تفاوت سطح منطقی بین تجار و مصرف‌کنندگان ایجاد می‌کند.

فناوری زنجیره بلوکی با پیاده‌سازی غیرمتمرکز و قابلیت‌های امنیتی، شیوه جدیدی برای مکانیسم‌های ضدجعل به‌شمار می‌آید. می‌توان سناریویی را تصور کرد که در آن برندها، تجار و بازارهای تجاری همگی به‌عنوان بخشی از یک شبکه زنجیره بلوکی باشند و گره‌های این شبکه اطلاعاتی را ذخیره کنند تا اصل بودن کالاها قابل شناسایی باشد. با استفاده از این فناوری، بخش تأمین کالا در فروشگاه‌ها برای تشخیص و تأیید اعتبار کالای خود، دیگر به تکیه بر تأیید یک مرجع مرکزی نیازی ندارند.

بلاک وریفای[1] (شناسایی بلاک) روشی ضدجعل مبتنی‌بر زنجیره بلوکی است که کار بخش کالا برای فروشندگان را شفاف می‌کند. برنامه‌های کاربردی آن در زمینه‌های دارویی، کالاهای قیمتی، الماس و صنایع الکترونیک تهیه شده است.

1. BLOCK VERIFY

- **استفاده برنامه‌های کاربردی اینترنتی از زنجیره بلوکی**

نیمکوین[1] یک فناوری زنجیره بلوکی دیگر است که با زنجیره بلوکی بیتکوین به دنبال پیاده‌سازی نسخه غیرمتمرکز خادم نام دامنه است. خادم‌های نام دامنه فعلی توسط دولت‌های خارجی و شرکت‌های بزرگ کنترل می‌شوند و می‌توانند از قدرتشان برای دزدیدن، یا جاسوسی نحوه استفاده افراد از اینترنت استفاده کنند. استفاده از فناوری زنجیره بلوکی به این معناست که خادم نام دامنه یا دفترچه تلفن اینترنت به طریقی غیرمتمرکز محافظت شود و هر کاربری بتواند داده دفترچه تلفن یکسانی روی رایانه خود داشته باشد. نیمکوین این مسئله را حل می‌کند.

زیرساخت کلید عمومی یا PKI به‌صورت گسترده‌ای برای مدیریت و توزیع متمرکز تأییدیه‌های دیجیتالی به‌کار می‌رود. هر وسیله باید یک تأییدیه اصلی از محل تأیید اعتبارات مرجع اعتبارسنجی CA برای شناسایی امضای دیجیتالی داشته باشد. با وجود اینکه زیرساخت کلید عمومی به‌صورت وسیعی گسترش یافته و موفق است، وابستگی آن به مرجع، مسئله گسترش‌پذیری را مطرح می‌کند.

خصوصیات زنجیره بلوکی می‌تواند کمک کند تا برخی محدودیت‌های زیرساخت کلید عمومی از طریق استفاده از زیرساخت امنیتی بدون کلید (KSI)[2] آدرس‌دهی شود. KSI از طریق یک تابع هش رمزگذاری، امکان اعتبارسنجی براساس توابع هش امنیتی و زنجیره بلوکی را فراهم می‌کند.

مخاطره‌های زنجیره بلوکی

زنجیره بلوکی یک فناوری پیشرفته با چشم‌انداز روشن است. همانطور که قبلاً توضیح داده شد تعداد زیادی آرایه برنامه کاربردی یا مشکلاتی که می‌تواند براساس فناوری زنجیره بلوکی حل شود وجود دارد. دامنه آن از برنامه‌های مالی (پرداخت‌های سرمایه‌گذاری بانکداری) تا برنامه‌های کاربردی غیرمالی نظیر خدمات اسناد رسمی گسترده می‌شود. **بیشتر تغییراتی که باید انجام گیرد، اصلاحات اساسی هستند**. همانطور که برای تطبیق همه نوآوری‌های اصلاحی اتفاق می‌افتد، مخاطره‌های مشخصی در رابطه با تطبیق با فناوری زنجیره بلوکی نیز وجود دارند.

تغییر رفتار: تغییرات الزامی هستند، اما همیشه در برابر تغییر مخالفت‌هایی وجود دارد. مدیران عالی و تصمیم‌گیرنده باید با این حقیقت روبرو شوند که در دنیای زنجیره بلوکی که نیازی به حضور مرجع سوم نیست، تراکنش‌های الکترونیک به‌صورت ایمن و کامل انجام می‌پذیرند. امروزه واسطه‌هایی نظیر ویزا و مسترکارد (به‌عنوان کارت‌های اعتباری) در زمینه مالی هم به‌دنبال تغییر نقش‌ها و مسئولیت‌ها هستند. تصور می‌شود که آنها نیز پلتفرم‌هایشان را به مدل مبتنی‌بر زنجیره بلوکی تبدیل

1. NAMECOIN
2. Keyless Security Infrastructure (KSI)

کرده. تا بتوانند در آینده خدماتی از نوع «ارتباط با مشتری» فراهم کنند.

مدت زمان: مدت زمان اجرای خدمات درحال پیدایش فعلی مبتنی‌بر زنجیره بلوکی مشکلی را به وجود آورده است. تصور کنید برای اولین بار درحال اجرای یک تراکنش زنجیره بلوکی هستید. باید یکسری دانلود از کل زنجیره بلوکی موجود را انجام دهید و پیش از آنکه بتوانید اولین تراکنش خود را انجام دهید باید کل زنجیره بلوکی شناسایی و معتبر شود. با توجه به اینکه تعداد زنجیره‌های بلوکی مداوم در حال افزایش است، این امر می‌تواند بیش از چند ساعت طول بکشد.

خودراه‌اندازی: برای تبدیل قالب یا چارچوب‌های کاری موجود به قالب قابل استفاده در زنجیره بلوکی جدید، نیازمند اجرای مجموعه‌ای از وظایف خاص به‌منظور این تبدیل قالب هستیم. برای مثال در مورد حق استفاده از تعرفه انتخاباتی، اسناد موجود که در یک سازمان یا شعبه استان و یا شهرستان نگهداری می‌شوند باید به قالب مورد پذیرش برای زنجیره بلوکی تبدیل شوند و این خود امری زمانبر و هزینه‌بر است.

قوانین دولتی: در دنیای جدید تراکنش‌های مبتنی‌بر زنجیره بلوکی، سازمان‌های دولتی با توجه به نگرانی‌های خود از مخاطرات استفاده از این فناوری‌ها، می‌توانند عمل تطبیق‌پذیری با این فناوری جدید را با صدور قوانین جدید برای کنترل آن، کُند نمایند. در برخی موارد اصلاح قوانین لازم است و در برخی موارد احتمالاً با استفسار از قوه مقننه، قوانین سابق برای کارکردهای جدید نیز مفید خواهند بود.

فعالیت‌های فریبکارانه: با توجه به خصوصیت استعاری تراکنش‌های زنجیره بلوکی و سهولت در انتقال مقادیر ارزشمند، افراد متقلب ممکن است از آن برای فعالیت‌های متقلبانه استفاده کنند. گفته می‌شود که با وجود مقررات کافی و با پشتیبانی فناوری، آژانس‌های مجری قانون می‌توانند بر فعالیت آنها نظارت نموده و آنها را تحت پیگیری قانونی قرار دهند.

رایانه‌های کوانتومی: بنیان فناوری زنجیره بلوکی بر این اصل متکی است که از نظر ریاضی، برای یک شخص منفرد، با توجه به کمبود قدرت محاسباتی رایانه‌ها، غیرممکن است که بتواند سیستم را به بازی بگیرد. ولی با ظهور رایانه‌های کوانتومی در آینده، کلیدهای رمزگذاری ممکن است به قدری ساده شوند که شکستن آنها برای افراد بدخواه در یک زمان منطقی قابل دسترسی باشد. این موضوع کل سیستم را به زانو در خواهد آورد. البته طراحی کلیدها می‌تواند قدرتمندتر شود تا شکست آنها ساده نباشد.

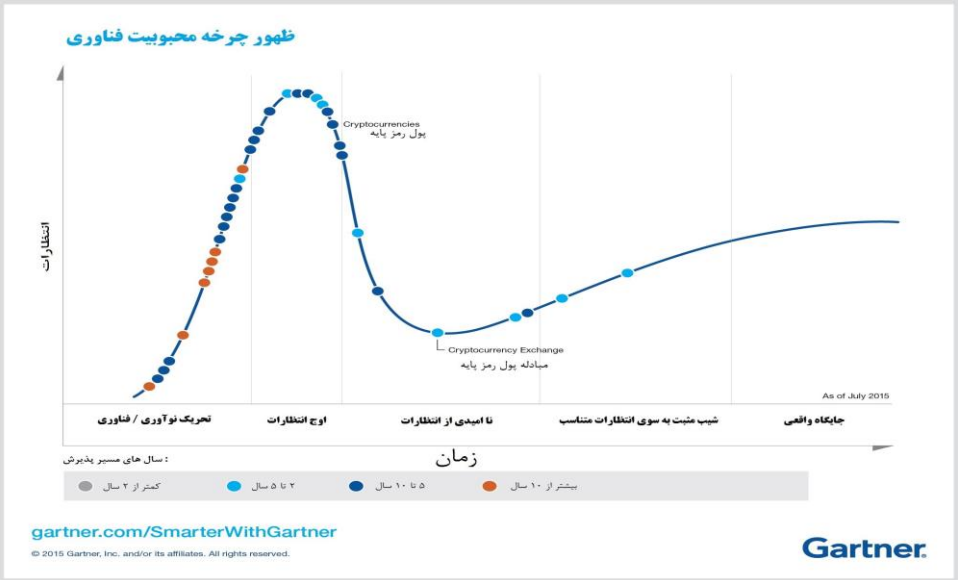
آینده زنجیره بلوکی در دوره محبوبیت گارتنر

فناوری زنجیره بلوکی در نمودار دوره محبوبیت گروه گارتنر[1] در دو سال متوالی مورد اشاره قرار گرفته است. ابتدا به‌صورت غیرمستقیم در سال ۲۰۱۵ در قالب ارزهای رمزپایه و مبادله ارز رمزپایه (نمودار ۱) و سپس در سال ۲۰۱۶ به‌صورت مستقل (نمودار ۲). همانطور که کاربردهای مختلف زنجیره بلوکی

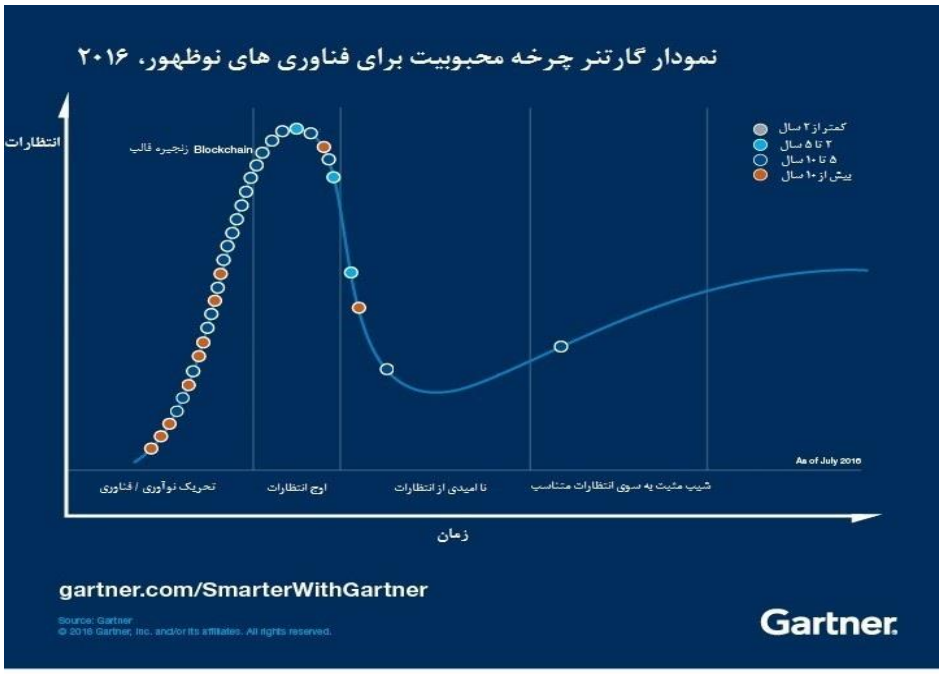
۱. براي آشنايي بيشتر با نمودار دوره محبوبيت گارتنر رجوع شود به پاورقي صفحه ۲۵ گزارش رايانش ابري به شماره مسلسل ۱۲۰۳۸ مرکز پژوهش‌هاي مجلس.

در زمینه‌های گوناگون مورد استقبال شرکت‌ها و دولت‌های بسیاری قرار گرفته است، استفاده از آن در امور حساس حکومتی مانند برگزاری انتخابات هم دور از انتظار نیست. البته مخاطرات مربوط به رایانه‌های کوانتومی در آینده و فعالیت‌های مخرب نیز وجود دارند که با توجه به قابلیت محدودسازی شبکه به اجزای شناسا و داخلی و اعمال کنترل شبکه‌ای و افزایش قدرت رمزنگاری باید با آنها مقابله شود. براساس پیش‌بینی گارتنر، این فناوری طی پنج تا ده سال آینده به‌طور کامل عملیاتی خواهد شد. البته پیش‌بینی و ملاحظات دیگر خبرگان بر این است که بسیار زودتر از یک تا دو سال آینده شاهد عملیاتی شدن بسیاری از پروژه‌های مبتنی‌بر فناوری زنجیره بلوکی خواهیم بود.

نمودار ۱. فرآیند منحنی اشتیاق فناوری گارتنر در سال ۲۰۱۵



نمودار ۲. فرآیند منحنی اشتیاق فناوری گارتنر در سال ۲۰۱۶



جمع‌بندی و نتیجه‌گیری

فناوری زنجیره بلوکی با توجه به طیف وسیع کاربردهای آن قابلیت این را دارد که به‌صورت بنیادین زندگی روزمره بشری را تغییر دهد. بسیاری از قوانین و مقررات وضع شده که تصور می‌شد نسبت به فناوری خنثی است، پس از عملیاتی شدن کامل فناوری زنجیره بلوکی قابل تجدید نظر خواهند بود. نظام مالی بین‌المللی و نظام‌های ملی از حالت متمرکز به سمت توزیع‌شدگی پیش می‌روند و نهادهای قدیمی بشری و اعتماد ناگزیر به بشر، جای خود را به اعتماد روزافزون به فناوری‌های رایانشی می‌دهند. نهادهای مالی و اقتصادی قدرتمندی همچون بانک‌ها، بیمه‌ها و بازارهای سرمایه طی سال‌های آینده دچار تغییرات شگرفی خواهند شد. نهادهای مدنی متمرکز مانند دفاتر اسناد رسمی به‌تدریج جای خود را به نهادهای توزیع شده چابک‌تر و کم‌هزینه‌تر رایانه‌ای می‌دهند. فضای نوظهور مجازی نیز خود دچار تغییرات مهمی خواهد شد. در این گزارش با توجه به کارکردهای جدید زنجیره بلوکی و استقبال بزرگترین بنگاه‌های حوزه فناوری اطلاعات از این فناوری و عملیاتی شدن بسیاری از پروژه‌های پیرامون آن، استفاده از فناوری زنجیره بلوکی در حل مسائل جاری کشور نیز قابل بررسی است. موارد بسیاری از خدمات الکترونیکی نیازمند پایگاه‌های اطلاعاتی متداخل که نیازمند همکاری میان دستگاه‌های اجرایی نیاز دارند هم‌اکنون به دلایل مختلف ازجمله عدم اعتماد دستگاه‌ها به یکدیگر (به‌دلایل حقوقی باید این چنین باشند) از پیشرفت لازم برخوردار نیستند یا حتی کنار گذاشته شده‌اند. فناوری زنجیره بلوکی این قابلیت را دارد که تفاهم و اعتماد را میان دستگاه‌ها جاری سازد و

جریان اطلاعات لازم میان دستگاه‌ها برای الکترونیکی شدن خدمات و تحقق دولت الکترونیکی در حوزه‌هایی که تاکنون قابل الکترونیکی کردن نبود را نیز فراهم بیاورد. بنابراین پیشنهاد می‌شود مطالعه فناوری زنجیره بلوکی و استفاده از آن برای حل مسائل جاری کشور مانند برگزاری انتخابات مورد توجه قرار بگیرد. همچنین مطالعات امکان‌سنجی بازنگری قوانین و مقررات پیشینی در صورت اثبات قابلیت‌های این فناوری در سال‌های پیش رو قابل اتخاذ است.

منابع و مآخذ

۱. جری کوما، زنجیره بلوکی پیشنهاد آی.بی.ام به دولت آمریکا؛ با جلسه استماع کنگره، بازیابی از کانال شخصی ابوالقاسم رجبی: http:aparat.com/viejf4d

2. Atzori, Marcella Ph. D .2015" .Blockchain Technology and Decentralized Governance: Is the State Still Necessary"?
3. bitcoinfoundation .2015 .Voting on the Blockchain – Version .۱،۰ https://bitcoinfoundation.org/voting-on-the-blockchain-version-./۰-۱
4. Crosby, Michael Google, Yahoo Nachiappan, Pradhan Yahoo Pattanayak, Sanjeev Samsung Research America Verma, Vignesh Fairchild Semiconductor Kalyanaraman, and Ikhlaq Prof. Sidhu. 2015. "BlockChain Technology Beyond Bitcoin." Sutardja Center for Entrepreneurship & Technology Technical Report.
5. Czepluch, Jacob Stenum, Nikolaj Zangenberg Lollike, and Simon Oliver Malone. 2015. The Use of Block ChainTechnology in DifferentApplication Domains. Copenhagen: The IT University of Copenhagen.
6. Gritzalis, Dimitris. 2002. "Principles and requirements for a secure e-voting system." Computers & Security 539-556.
7. Mitrou, Lilian, Gritzalis Dimitris, and K Sokratis. 2002. "Revisiting legal and regulatory requirements for secure e-voting." In Security in the Information Society 469-480.
8. Padget, Julian. 2005. "E-government and e-democracy in Latin America." IEEE Intelligent Systems 94-96.
9. Pilkington, Marc Associate Professor of economics at the University of Burgundy, France .2015" .Blockchain Technology: Principles and Applications".
10. Spanos, Nikolaos, Andrew R Martin, and Eric T Dixon. 2015. System and method for securely receiving and counting votes in an election. US Patent US20160027229 A1.
11. Swan, Melanie . 2015. Blockchain Blueprint for a New Economy. O'Reilly Media, Inc.
12. US UTAH Notarization and Authentication of Documents and Digital Signatures. 2003. Documents and Digital Signatures,. http://www.code-co.com/utah/code/04/codetab.htm.
13. Wattenhofer, Roger. 2016. The Science of the Blockchain. Inverted Forest.
14. Zissis, Dimitrios, and Lekkas Dimitrios. 2011. "Securing e-Government and e-Voting with an open cloud computing architecture." Government Information Quarterly 239-251.

شناسنامه گزارش	مرکز پژوهش‌های مجلس شورای اسلامی	شماره مسلسل: ۱۵۳۴۱

عنوان گزارش: آشنایی با فناوری راهبردی زنجیره بلوکی و کاربردهای آن

نام دفتر: مطالعات ارتباطات و فناوری‌های نوین (گروه ارتباطات و فناوری اطلاعات)

تهیه و تدوین‌کنندگان: ابوالقاسم رجبی، روح‌الله فریور

ناظر علمی: مهدی فقیهی

مدیر مطالعه: حسن پوراسماعیل

اظهارنظرکننده: شعبان الهی

متقاضی: معاونت پژوهش‌های زیربنایی و امور تولیدی

ویراستار تخصصی: ـــــــ

ویراستار ادبی: طاهره سیدمحمد

واژه‌های کلیدی:

۱. زنجیره بلوکی

۲. بیتکوین

۳. اقتصاد دیجیتالی

۴. امضای دیجیتالی

۵. قراردادهای هوشمند

۶. زنجیره قالب

۷. زنجیره بستک

۸. بلاک چین

۹. اقتصاد توزیع شده

۱۰. بانکداری نوین

۱۱. دفاتر اسناد رسمی توزیع شده

۱۲. ذخیره‌سازی غیرمتمرکز

۱۳. زیرساخت امنیتی بدون کلید

۱۴. اینترنت اشیای غیرمتمرکز

تاریخ انتشار: ۱۳۹۶/۱/۲۱