بررسی اجمالی فناوری بلاکچین در حوزه اینترنت اشیاء (IoT)

سپیده شجاعی[1] سمیه خواجه حسینی[2]

۱. دانشجوی کارشناسی مهندسی نرم‌افزار ۲- استادیار دانشگاه سیرجان

چکیده

اگرچه بسیاری از محققان به اهمیت بلاکچین پی برده‌اند، با این حال تحقیقات در مورد بلاکچین هنوز در مراحل ابتدایی است. در نتیجه، این تحقیق، بروزترین تحقیقات آکادمیک را در مورد بلاکچین مورد مطالعه قرار می‌دهد. Blockchain یک دفتر توزیع شده، غیرمتمرکز و تغییرناپذیر دیجیتال است که معاملات را در یک شبکه جهانی رایانه‌ی ثبت می‌کند که در آن اطلاعات، از امنیت بالایی برخوردار هستند. اینترنت اشیا در حال هوشمند سازی شهرها، حمل‌ونقل، شبکه‌ها، خانه‌ها، صنعت کشاورزی و سیستم‌های بهداشتی است. بنابراین، استفاده از Blockchain در حوزه IoT دامنه جدیدی از Blockchain را در IoT (BIoT) بوجود می‌آورد. در چشم‌انداز اینترنت اشیا (IoT)، دستگاه‌های معمولی هوشمند و خودمختار می‌شوند. این چشم‌انداز به لطف پیشرفت فناوری در حال تبدیل شدن به واقعیت است، اما هنوز هم چالش‌هایی برای حل وجود دارد. این تحقیق می‌تواند یک نقطه یادگیری خوب برای محققان جوان جهت یافتن بینش تحقیقاتی جذاب در BIoT باشد.

کلیدواژه‌ها: اینترنت اشیا (IoT)، بسترهای نرم‌افزاری، بلاکچین(blockchain)، بیت کویین، رایانه، فناوری.

مقدمه

بلاکچین برای اولین بار توسط S. Nakamotoبه‌عنوان یک دفتر معاملاتی مطمئن برای ارز رمزنگاری‌شده جدید موسوم به بیت کوین معرفی شد. بلاک چین دنباله‌ای از بلوک‌هایی است که در مورد IoTها حاوی تراکنش یا پیام است. بلوک‌ها از طریق یک فرآیند استخراج به زنجیره بلوک اضافه می‌شوند که برای محاسبه یک بلوک معتبر که از نظر شبکه قابل‌قبول است، مقدار

قابل‌توجهی از قدرت پردازش لازم است. فناوری بلاکچین به‌گونه‌ای ایجاد شده است که توانایی تغییر یک بلاکچین و محتوای آن توسط قدرت پردازش محض را محدود می‌کند. تنها راه برای کنترل بلاکچین از طریق حمله نظری ۵۱٪ است، جایی که یک مهاجم باید حداقل ۵۱٪ از قدرت محاسباتی یک بلاکچین را داشته باشد تا بتواند محتوای بلوک را تغییر دهد و سریع‌تر از سایر کاربران ترکیبی شبکه اعتبارسنجی کند. بلاکچین برای اولین بار برای معاملات مالی در بیت کوین ارز رمزنگاری‌شده استفاده شد، اما در حال حاضر در چندین حوزه تحقیقاتی در حال ظهور است. در عین حال، فناوری بلاکچین در بسیاری از حوزه‌ها از جمله پزشکی، اقتصادی، اینترنت اشیا، مهندسی نرم‌افزار، مراقبت‌های بهداشتی، رأی‌گیری، اصلاحات در انتخابات، زنجیره تأمین، زنجیره ارزش، اعمال شده است (۱).

اینترنت اشیا زندگی ما را تغییر شکل داده و به بخشی جدایی‌ناپذیر از فعالیت‌های روزمره ما تبدیل‌شده است. خودروهایی که با دیگر وسایل نقلیه و مراکز راهنمایی و رانندگی ارتباط برقرار می‌کنند تا تجربه رانندگی ایمن و روان را فراهم کنند، ابزارها و ابزارهای پوشیدنی که داده‌های مربوط به بدن و فعالیت‌های ما را جمع‌آوری می‌کنند و به ما کمک می‌کنند سلامت و ابزار هوشمند خانگی خود را کنترل کنیم که قادر به بهبود کیفیت زندگی ما هستند. اینترنت اشیا (IOT) یک حوزه تحقیقاتی فعال است که نقشی اساسی در توسعه جامعه دارد. اصطلاح اینترنت اشیا توسط اشتون در سال ۱۹۹۸ معرفی شد. وی اهمیت اینترنت اشیا را برای تغییر جهان همانطور که اینترنت در اوایل دهه ۱۹۹۰ انجام داد، برجسته کرد. مرکز MIT Auto-ID در ارائه دیدگاه مربوط به اینترنت اشیا در سال ۲۰۰۱ پیشگام بود. بعداً در سال ۲۰۰۵، گزارش اینترنت ITU به‌طور رسمی مفهوم و فناوری IoT را معرفی کرد. اینترنت اشیا معمولاً به‌عنوان IoT تعریف می‌شود که به افراد و چیزها امکان اتصال در هر زمان و مکان، با هر چیز و هر کسی را به‌طور ایدئال با استفاده از هر شبکه و سرویس می‌دهد. دستگاه‌های اینترنت اشیا به هم مرتبط هستند و از طریق اینترنت به هم متصل می‌شوند. در این مقاله چالش‌های فعلی اینترنت اشیا و بلاکچین و مزایای بالقوه استفاده ترکیبی از آن‌ها مورد تجزیه و تحلیل قرار می‌گیرد.

مواد و روش‌ها

برای انتخاب مستندات مورد استفاده ابتدا عناوین یافت شده توسط موتور جستجو از نظر ارتباط موضوعی بررسی شدند. مطالب یافت شده در قالب بروزترین مقاله‌های علمی پژوهشی ترجمه شده و در این مقاله به کار برده شده است.

یافته‌ها

تاریخچه بلاکچین و انواع آن

دامنه تحقیق در بلاکچین از زمانی آغاز شد که ساتوشی ناکاموتو در سال ۲۰۰۸ مقاله‌ای سفید با معرفی نسخه کاملاً نظیر به نظیر پول نقد الکترونیکی موسوم به بیت کوین منتشر کرد. فناوری بلاکچین به‌عنوان ترکیبی از رمزنگاری، تئوری بازی و شبکه‌های نظیر به نظیر بدون هماهنگی مرکزی تعریف شده است. چندین الگوریتم اجماع وجود دارد که در تحقیقات مرتبط با بلاکچین اعمال می‌شود که به دو نوع اصلی تقسیم می‌شوند: الگوریتم اجماع مبتنی بر اثبات و الگوریتم اجماع مبتنی بر رأی. فناوری بلاکچین به دو نوع بلاکچین خصوصی و عمومی دسته‌بندی می‌شود. بلاکچین خصوصی توسط یک شرکت کنترل می‌شود و در نتیجه با اصل استقلال بلاکچین مطابقت ندارد. الگوریتم اجماع مبتنی بر اثبات در بلاکچین عمومی اعمال می‌شود، درحالی‌که الگوریتم اجماع مبتنی بر رأی در بلاکچین خصوصی اعمال می‌شود. بلاکچین ترکیبی از فناوری‌های متنوع است که برای مدت‌زمان طولانی به‌عنوان فناوری‌های استاندارد در نظر گرفته می‌شوند. این فناوری‌ها به سادگی با روشی جدید و خلاقانه ترکیب می‌شوند تا بستر جدیدی فراهم کنند که بتوان بر اساس آن راه‌حل‌های متنوعی ساخت. به‌طور کلی، بلاکچین مانند شبکه‌ای از رایانه‌های گره‌ای به نظر می‌رسد که در آن داده‌ها دیگر در مکان مرکزی ذخیره نمی‌شوند، بلکه با استفاده از بالاترین سطح رمزنگاری در یک دفتر جهانی توزیع می‌شوند. اجزای اصلی بلاکچین عبارت‌اند از: دفتر کل، شبکه همتا، خدمات عضویت، قرارداد هوشمند، کیف پول، رویدادها، مدیریت سیستم‌ها و ادغام سیستم‌ها. وقتی هر معامله‌ای در بلاکچین انجام می‌شود، درده‌ها هزار رایانه در سراسر جهان که بخشی از این شبکه بلاکچین هستند، ارسال می‌شود. این معاملات سپس به صورت بلوک ثبت می‌شوند. بعلاوه، این بلوک‌ها با استفاده از اطلاعات بلوک‌های مجاور در یک زنجیره به هم متصل می‌شوند.

سازوکار بلاکچین

بلاکچین از بلوک‌هایی تشکیل‌شده است که شامل زمینه‌های داده‌های لازم برای ایجاد زمینه‌ای برای بلاکچین شبکه شبیه‌سازی‌شده برای اینترنت اشیا است. در این پیاده‌سازی، بلوک‌ها اشیا هستند و بلاکچین یک لیست آرایه‌ای است.

بلاکچین با استفاده از یک حلقه تأیید می‌شود که از طریق تمام بلوک‌های بلاکچین تکرار می‌شود و سه شرط را در هر تکرار بررسی می‌کند. اگر تمام روش‌ها هر عنصر از یک بلوک را برای همه بلوک‌های زنجیره بلوک تأیید کنند، بلاکچین معتبر در نظر گرفته می‌شود.

۱) Check Current Hash: این روش با تولید هش داده‌های بلوک و مقایسه نتیجه با هش ذخیره شده در بلوک موجود، بررسی می‌کند که آیا CurrentHash به درستی محاسبه شده است.

۲) Check Previous Hash: این روش بررسی می‌کند که آیا هش قبلی همان هش فعلی بلوک قبلی است.

۳) Check Target: هدف رشته‌ای از نویسه‌ها است که اعتبار هش را تعیین می‌کند. در این روش، هدف با یک زیر رشته از CurrentHash یک بلوک مقایسه می‌شود. اگر هدف و هش زیر رشته با هم مطابقت داشته باشند، هش توسط پارامترهای بلاکچین معتبر در نظر گرفته می‌شود (۲).

کاربرد بلاک‌چین

- بلاکچین همچنین فناوری را ارائه داده است که می‌توان مفهوم قرارداد هوشمند را تحقق بخشید. به‌طور کلی، یک قرارداد هوشمند به پروتکل‌ها یا برنامه‌های رایانه‌ای اطلاق می‌شود که اجازه می‌دهد با در نظر گرفتن مجموعه‌ای از شرایط از پیش تعیین‌شده، قراردادی به‌طور خودکار اجرا یا اجرا شود. به‌عنوان مثال، قراردادهای هوشمند منطق کاربردی را تعریف می‌کنند که هر زمان معامله‌ای در مبادله ارز رمزنگاری‌شده انجام شود. در قراردادهای هوشمند، توابع و شرایط را می‌توان فراتر از مبادله ارزهای رمزپایه تعریف کرد، مانند اعتبار سنجی دارایی‌ها در طیف خاصی از معاملات با عناصر غیرپولی، که آن را به یک مولفه کامل برای گسترش فناوری بلاکچین در سایر مناطق تبدیل می‌کند.
- برخی از شبکه‌های بلاکچین از یک آدرس استفاده می‌کنند، این یک رشته کوتاه و حروف عددی است که از کلید عمومی کاربر شبکه بلاکچین با استفاده از یک تابع هش رمزنگاری‌شده همراه با برخی از داده‌های اضافی (به‌عنوان مثال، شماره نسخه، چک) استفاده می‌شود. بیشتر پیاده‌سازی‌های بلاکچین از آدرس‌ها به‌عنوان نقاط انتهایی "به to " و "از from " در معامله استفاده می‌کنند. آدرس‌ها کوتاه‌تر از کلیدهای عمومی هستند و مخفی نیستند. یک روش برای تولید آدرس ایجاد کلید عمومی، استفاده از یک تابع هش رمزنگاری‌شده و تبدیل هش به متن است:

public key →cryptographic hash function → address

هر پیاده‌سازی بلاکچین ممکن است روش دیگری را برای استخراج آدرس پیاده‌سازی کند.

- هویت: با استفاده از یک سیستم بلاکچین مشترک، شرکت‌کنندگان قادر به شناسایی هر دستگاه هستند. داده‌های ارائه‌شده و وارد شده به سیستم تغییرناپذیر است و داده‌های واقعی ارائه‌شده توسط دستگاه را به‌طور منحصر به فرد شناسایی می‌کند. علاوه بر این، بلاکچین می‌تواند تأیید اعتبار و مجوز توزیع شده قابل اعتماد دستگاه‌ها را برای برنامه‌های اینترنت اشیا فراهم کند. این می‌تواند پیشرفتی در زمینه اینترنت اشیا و شرکت‌کنندگان در آن باشد.
- خودمختاری: فناوری بلاکچین به ویژگی‌های کاربردهای بعدی قدرت می‌بخشد و توسعه دارایی‌ها و سخت‌افزارهای مستقل هوشمند را به‌عنوان یک سرویس امکان‌پذیر می‌کند . با استفاده از بلاکچین، دستگاه‌ها قادر به تعامل با یکدیگر بدون درگیر شدن هیچ سرور هستند. برنامه‌های اینترنت اشیا می‌توانند از این قابلیت برای ارائه برنامه‌های کاربردی و جداشده بهره‌مند شوند.
- قابلیت اطمینان: اطلاعات اینترنت اشیا می‌تواند بدون تغییر باقی بماند و به مرور در بلاکچین توزیع شود. مشارکت‌کنندگان در سیستم می‌توانند صحت داده‌ها را تأیید کنند و اطمینان دارند که در آن‌ها دست‌کاری نشده است. علاوه بر این، این فناوری قابلیت ردیابی و پاسخگویی داده‌های حسگر را فراهم می‌کند. قابلیت اطمینان جنبه اصلی بلاکچین برای وارد کردن اینترنت اشیا است.
- • امنیت: اگر اطلاعات و ارتباطات به‌عنوان معاملات بلاکچین ذخیره شوند، می‌توانند از امنیت برخوردار شوند. بلاکچین می‌تواند مبادله پیام دستگاه را به‌عنوان معامله‌ای که با قراردادهای هوشمند تأییدشده است، از این طریق با ایمن‌سازی ارتباطات بین دستگاه‌ها رفتار کند. پروتکل‌های استاندارد و ایمن فعلی که در اینترنت اشیا استفاده می‌شود می‌توانند با استفاده از بلاکچین بهینه شوند.
- بازار خدمات: بلاکچین می‌تواند ایجاد یک اکوسیستم اینترنت اشیا of از خدمات و بازارهای داده را تسریع کند، جایی که معاملات بین همتایان خارج از مقامات ممکن است. میکرو سرویس‌ها به‌راحتی قابل‌استفاده هستند و پرداخت خرد می‌تواند

در یک محیط بی‌اعتماد انجام شود این باعث بهبود اتصال اینترنت اشیا و دسترسی به داده‌های اینترنت اشیا در بلاکچین می‌شود.

استفاده از کد امن: با استفاده از فضای ذخیره‌سازی غیرقابل تغییر در زنجیره بلوک، کد می‌تواند ایمن باشد و به‌طور ایمن وارد دستگاه شود تولیدکنندگان می‌توانند وضعیت‌ها و به‌روزرسانی‌ها را با بالاترین اطمینان پیگیری کنند.

بلاکچین و ارتباط آن با اینترنت اشیا

بلاکچین به اینترنت اشیا کمک می‌کند. تصمیم‌گیری در مورد تعیین نیاز بلاکچین در اینترنت اشیا بر اساس عوامل مختلفی انجام شده است. بلاکچین در بسیاری از موارد و در بسیاری از مناطق که اینترنت اشیا درگیر است می‌تواند مورد استفاده قرار گیرد. چالش‌های اصلی در اینترنت اشیا و ویژگی‌های اصلی Blockchain به یکدیگر مرتبط هستند و زمینه را برای پژوهشگران در این حوزه باز می‌کنند. از این رو تعداد انتشارات در این حوزه در حال افزایش است. بلاکچین از اعتبار سنجی و اعتماد توزیع شده در بین گره‌های مشابه سیستم اینترنت اشیا اطمینان حاصل می‌کند و در نتیجه، به معنای یک لایه امنیتی اضافی برای سیستم اینترنت اشیا است.

Blockchain می‌تواند از بسیاری جهات به سیستم اینترنت اشیا کمک کند مانند:

• با استفاده از فناوری Blockchain، حسگرهای اینترنت اشیا می‌توانند داده‌ها را بدون درگیر کردن شخص ثالث برای ایجاد اعتماد مبادله کنند. بستر بلاکچین فضای توزیع شده برای اشتراک داده‌ها را فراهم می‌کند.

• هزینه عملکرد و استقرار سیستم‌های اینترنت اشیا می‌تواند به دلیل عدم نیاز به واسطه کاهش یابد زیرا از ارتباط بین همتا پشتیبانی می‌کند.

• در صورت عدم تطابق داده‌ها، دستگاه‌های معیوب اینترنت اشیا با کمک مکانیسم هش فناوری Blockchain به‌راحتی قابل تشخیص هستند.

• با استفاده از فناوری Blockchain در سیستم‌های اینترنت اشیا، می‌توان یک فرآیند تجاری ساده با هزینه عملیاتی کم و با کار آیی بالاتر را به وجود آورد.

اینترنت اشیا processes در حال تبدیل و بهینه‌سازی فرایندهای دستی است تا آن‌ها را بخشی از دوران دیجیتال قرار داده و حجم زیادی از داده‌ها را به دست آورد که دانش را در سطوح ناشناخته فراهم می‌کند. این دانش توسعه برنامه‌های هوشمند مانند بهبود مدیریت و کیفیت زندگی شهروندان را از طریق دیجیتالی سازی خدمات در شهرها تسهیل می‌کند. طی چند سال گذشته، فناوری‌های رایانش ابری به ارائه اینترنت اشیا با قابلیت‌های لازم برای تجزیه و تحلیل و پردازش اطلاعات و تبدیل آن‌ها به

اقدامات و دانش در زمان واقعی کمک کرده‌اند (۳). این رشد بی‌سابقه در اینترنت اشیا فرصت‌های جدید جامعه‌ای مانند مکانیسم‌های دسترسی و اشتراک اطلاعات را فراهم کرده است. الگوی داده‌های باز گل سرسبد در این ابتکارات است. با این حال، یکی از مهم‌ترین نقاط آسیب‌پذیر این اقدامات، همانطور که در بسیاری از سناریوها رخ داده است، عدم اعتماد به نفس است. معماری متمرکز مانند معماری مورد استفاده در محاسبات ابری به‌طور قابل‌توجهی در توسعه اینترنت اشیا کمک کرده است. با این حال، در مورد شفافیت داده‌ها، آن‌ها به‌عنوان جعبه‌های سیاه عمل می‌کنند و شرکت‌کنندگان در شبکه دید مشخصی از محل و نحوه استفاده از اطلاعات ارائه نمی‌دهند.

ادغام فن‌آوری‌های امیدوارکننده مانند اینترنت اشیا و رایانش ابری بسیار ارزشمند به اثبات رسیده است. به همین ترتیب، ما به توانایی عظیم بلاکچین در انقلابی در اینترنت اشیا اعتراف می‌کنیم. بلاکچین می‌تواند اینترنت اشیا را با ارائه یک سرویس اشتراک قابل اعتماد، جایی که اطلاعات قابل اعتماد و قابل‌ردیابی است، IoT غنی کند. منابع داده را می‌توان در هر زمان شناسایی کرد و داده‌ها با گذشت زمان تغییرناپذیر هستند، و امنیت آن‌ها را افزایش می‌دهد. در مواردی که اطلاعات اینترنت اشیا باید به‌طور ایمن بین بسیاری از شرکت‌کنندگان تقسیم شود، این یکپارچگی یک انقلاب اساسی است.

به‌عنوان مثال، یک ردیابی جامع در محصولات غذایی متعدد یک جنبه اصلی برای اطمینان از ایمنی مواد غذایی است. ردیابی مواد غذایی می‌تواند به مشارکت بسیاری از شرکت‌کنندگان نیاز داشته باشد: تولید، تغذیه، درمان، توزیع و غیره. نشت داده‌ها در هر قسمت از زنجیره می‌تواند منجر به تقلب شود و روند جستجوی عفونت را که می‌تواند زندگی شهروندان را تحت تأثیر جدی قرار دهد و هزینه‌های هنگفت اقتصادی را برای شرکت‌ها، بخش‌ها و کشورها در صورت شیوع مواد غذایی تحمیل کند، کاهش دهد. کنترل بهتر در این مناطق باعث افزایش ایمنی غذا، بهبود اشتراک داده‌ها بین شرکت‌کنندگان و کاهش زمان جستجو در مورد شیوع مواد غذایی می‌شود که می‌تواند جان انسان‌ها را نجات دهد. علاوه بر این، در مناطق دیگر مانند شهرهای هوشمند و اتومبیل‌های هوشمند، به اشتراک گذاشتن داده‌های قابل اعتماد می‌تواند شامل شرکت‌کنندگان جدید در اکوسیستم باشد و به بهبود خدمات و پذیرش آن‌ها کمک کند. بنابراین، استفاده از بلاکچین می‌تواند اینترنت اشیا را با اطلاعات مطمئن و مطمئن تکمیل کند. این موضوع همانطور که در ذکر هش، جایی که فناوری بلاک چین به‌عنوان کلید اصلی برای حل مقیاس‌پذیری، حریم خصوصی و قابلیت اطمینان مربوط به پارادایم اینترنت اشیا شناخته می‌شود، شروع به شناسایی می‌شود.

از دیدگاه ما اینترنت اشیا می‌تواند از قابلیت‌های ارائه‌شده توسط بلاکچین بسیار بهره‌مند شود و به توسعه بیشتر فناوری‌های فعلی اینترنت اشیا کمک خواهد کرد. شایان ذکر است که هنوز تعداد زیادی چالش تحقیقاتی و موضوعات باز وجود دارد که باید مورد استفاده قرار گیرد تا بتوان از این دو فناوری به‌طور یکپارچه استفاده کرد و این موضوع تحقیق هنوز در مرحله مقدماتی است.

به‌طور خاص، پیشرفت‌هایی که این ادغام می‌تواند به همراه داشته باشد (اما محدود نمی‌شوند)

جنبه دیگری که باید در نظر گرفته شود مربوط به تعاملات اینترنت اشیا است، به‌عنوان مثال ارتباط بین زیرساخت‌های اینترنت اشیا. هنگام ادغام بلاکچین، باید تصمیم‌گیری شود که این تعاملات در کجا اتفاق می‌افتد: در داخل اینترنت اشیا، یک طراحی ترکیبی شامل اینترنت اشیا و بلاکچین یا از طریق بلاکچین.

- اینترنت اشیا - اینترنت اشیا: این روش می‌تواند از نظر تأخیر و امنیت سریع‌ترین رویکرد باشد زیرا می‌تواند به صورت آفلاین کار کند. دستگاه‌های اینترنت اشیا باید بتوانند با یکدیگر ارتباط برقرار کنند، که معمولاً شامل مکانیسم‌های کشف و مسیریابی است. فقط بخشی از داده‌های اینترنت اشیا در زنجیره بلوک ذخیره می‌شود درحالی‌که تعاملات اینترنت اشیا بدون استفاده از زنجیره بلوک انجام می‌شود این روش در سناریوهایی با داده‌های قابل اعتماد اینترنت اشیا که تعاملات اینترنت اشیا با تأخیر کم در حال انجام هستند، مفید خواهد بود.
- IoT – Blockchain: در این رویکرد همه تعاملات از طریق بلاکچین انجام می‌شوند و امکان ایجاد یک ثبت تغییرناپذیر از تعاملات را فراهم می‌کنند. این روش تضمین می‌کند که کلیه اقدامات انتخابی قابل‌ردیابی هستند زیرا جزئیات آن‌ها در بلاکچین مورد پرسش قرار می‌گیرد و علاوه بر این استقلال دستگاه‌های اینترنت اشیا را افزایش می‌دهد. برنامه‌های اینترنت اشیا که قصد تجارت یا اجاره مانند Slock.it را دارند می‌توانند از این روش برای ارائه خدمات خود استفاده کنند. با این وجود، ثبت همه تعاملات در بلاکچین شامل افزایش پهنای باند و داده‌ها می‌شود که یکی از چالش‌های شناخته شده در بلاکچین است از طرف دیگر، تمام داده‌های اینترنت اشیا مرتبط با این معاملات نیز باید در بلاکچین ذخیره شوند (۴).

• رویکرد ترکیبی: سرانجام، یک طرح ترکیبی که فقط بخشی از تعاملات و داده‌ها در زنجیره بلوک انجام می‌شود و بقیه مستقیماً بین دستگاه‌های اینترنت اشیا به اشتراک گذاشته می‌شوند. یکی از چالش‌های موجود در این روش، انتخاب تعاملاتی

است که باید از طریق بلاکچین انجام شود و ارائه راهی برای تصمیم‌گیری در این زمینه. ارکستراسیون کامل این روش بهترین راه برای تلفیق فناوری‌ها خواهد بود زیرا از مزایای بلاکچین و مزایای تعاملات اینترنت اشیا در زمان واقعی بهره می‌برد. در این روش محاسبات مه می‌تواند به کار گرفته شود و حتی رایانش ابری نیز بتواند مکمل محدودیت‌های بلاکچین و اینترنت اشیا باشد.

زیرساخت و هویت کلید عمومی

برخی از افراد با شنیدن اینکه فناوری blockchain دارای یک زیرساخت کلید عمومی است و معتقدند که به‌طور ذاتی هویت را پشتیبانی می‌کند. این مورد نیست، زیرا ممکن است یک رابطه یک به یک جفت کلید خصوصی با کاربران وجود نداشته باشد (کاربر می‌تواند چندین کلید خصوصی داشته باشد) و همچنین یک رابطه یک به یک بین آدرس‌های بلاکچین و کلیدهای عمومی وجود ندارد (چندین آدرس را می‌توان از یک کلید عمومی به دست آورد).

از امضاهای دیجیتالی اغلب برای اثبات هویت در دنیای امنیت سایبری استفاده می‌شود و این می‌تواند منجر به سردرگمی در مورد کاربرد بالقوه زنجیره بلوک در مدیریت هویت شود. روند تأیید معامله blockchain معاملات را به دارندگان کلیدهای خصوصی پیوند می‌دهد اما هیچ تسهیلاتی برای ارتباط هویت‌های دنیای واقعی با این دارندگان فراهم نمی‌کند. در برخی موارد، امکان اتصال هویت‌های واقعی با کلیدهای خصوصی وجود دارد، اما این ارتباطات از طریق فرایندهایی خارج از بلاکچین انجام می‌شود و به صراحت توسط آن‌ها پشتیبانی نمی‌شود. به‌عنوان مثال، یک سازمان اجرای قانون می‌تواند پرونده‌هایی را از صرافی درخواست کند که معاملات را به افراد خاص متصل کند. مثال دیگر این است که فردی آدرس ارز رمزنگاری‌شده را در وب سایت شخصی یا صفحه رسانه‌های اجتماعی خود برای کمک‌های مالی ارسال می‌کند، این می‌تواند پیوندی از آدرس به هویت دنیای واقعی باشد.

درحالی‌که استفاده از فناوری بلاکچین در چارچوب‌های مدیریت هویت که به یک جز دفتر توزیع شده نیاز دارند، مهم است که درک کنیم پیاده‌سازی‌های معمولی بلاکچین برای استفاده به‌عنوان سیستم‌های مدیریت هویت مستقل طراحی نشده‌اند. داشتن هویت دیجیتالی ایمن بیشتر از اجرای ساده بلاکچین است (۵).

چالش‌های ادغام بلاکچین - اینترنت اشیا

این بخش چالش‌های اصلی را که باید هنگام استفاده از فناوری بلاکچین در حوزه اینترنت اشیا برطرف شود، بررسی می‌کند. ادغام فناوری بلاکچین با اینترنت اشیا امری پیش‌پاافتاده نیست. Blockchain برای یک سناریوی اینترنتی با رایانه‌های قدرتمند طراحی شده است و این از واقعیت اینترنت اشیا بسیار دور است. معاملات

بلاکچین به صورت دیجیتالی امضا می‌شوند و بنابراین دستگاه‌هایی که قادر به کار با ارز هستند باید به این قابلیت مجهز شوند. گنجاندن زنجیره بلوک در اینترنت اشیا چالش‌برانگیز است. برخی از چالش‌های شناسایی شده در این بخش ارائه‌شده است.

ظرفیت ذخیره‌سازی و مقیاس‌پذیری

همانطور که بیان شد، ظرفیت ذخیره‌سازی و مقیاس‌پذیری بلاکچین هنوز مورد بحث است، اما در زمینه برنامه‌های اینترنت اشیا، ظرفیت‌های ذاتی و مقیاس‌پذیری این چالش‌ها را بسیار بیشتر می‌کند. از این نظر، به نظر می‌رسد بلاکچین برای کاربردهای اینترنت اشیا نامناسب باشد، اما روش‌هایی وجود دارد که می‌توان این محدودیت‌ها را کاهش داد یا به‌طور کلی از آن‌ها جلوگیری کرد. در اینترنت اشیا، جایی که دستگاه‌ها می‌توانند گیگابایت (GB) داده در زمان واقعی تولید کنند، این محدودیت مانع بزرگی برای ادغام آن با بلاکچین است. شناخته شده است که برخی از پیاده‌سازی‌های فعلی بلاکچین فقط می‌توانند چند تراکنش در ثانیه را پردازش کنند، بنابراین این می‌تواند یک گلوگاه بالقوه برای اینترنت اشیا باشد. علاوه بر این، بلاکچین برای ذخیره مقادیر زیادی از داده‌ها مانند داده‌های تولیدشده در اینترنت اشیا طراحی نشده است. تلفیق این فناوری‌ها باید با این چالش‌ها مقابله کند. در حال حاضر، بسیاری از داده‌های اینترنت اشیا هستند. در ادبیات، تکنیک‌های مختلفی برای فیلتر کردن، عادی‌سازی و فشرده‌سازی داده‌های اینترنت اشیا با هدف کاهش آن‌ها ارائه‌شده است. اینترنت اشیا شامل دستگاه‌های جاسازی‌شده، ارتباطات و خدمات هدف (بلاکچین، ابر) است، بنابراین صرفه‌جویی در مقدار داده‌ای که اینترنت اشیا ارائه می‌دهد می‌تواند از چندین لایه بهره‌مند شود. فشرده‌سازی داده‌ها می‌تواند انتقال، پردازش وظایف و ذخیره حجم بالای داده‌های اینترنت اشیا را کاهش دهد. رفتارهای عادی، برخلاف داده‌های غیرعادی، معمولاً به اطلاعات اضافی و ضروری نیاز ندارند (۶).

آخرین اما نه کمترین، بلاکچین و به‌ویژه پروتوکول اجماعی آن که باعث ایجاد تنگنا می‌شود، همچنین می‌تواند برای افزایش پهنای باند و کاهش تأخیر معاملات خود، در نتیجه امکان انتقال بهتر به اینترنت اشیا نشان داده شده توسط Bitcoin-NG را تنظیم کند.

امنیت

برنامه‌های اینترنت اشیا باید با مشکلات امنیتی در سطوح مختلف کنار بیایند، اما به دلیل عدم عملکرد و ناهمگنی زیاد دستگاه‌ها، دارای پیچیدگی اضافی هستند. علاوه بر این، سناریوی اینترنت اشیا شامل مجموعه‌ای از خصوصیات است که بر امنیت تأثیر می‌گذارد، مانند تحرک، ارتباطات بی‌سیم یا مقیاس.

افزایش تعداد حملات به شبکه‌های اینترنت اشیا، و تأثیرات جدی آن‌ها، ایجاد اینترنت اشیا با امنیت

پیشرفته‌تر را بیش از پیش ضروری می‌کند. بسیاری از کارشناسان بلاکچین را به‌عنوان یک فناوری کلیدی در جهت ایجاد پیشرفته‌ای امنیتی مورد نیاز در اینترنت اشیا می‌دانند. با این حال، یکی از چالش‌های اصلی در ادغام اینترنت اشیا با بلاکچین، قابلیت اطمینان داده‌های تولیدشده توسط اینترنت اشیا است. بلاکچین می‌تواند اطمینان حاصل کند که داده‌های موجود در زنجیره غیرقابل تغییر هستند و می‌توانند تحولات آن‌ها را شناسایی کنند، با این وجود وقتی داده‌ها از قبل خراب شده در بلاکچین خراب می‌شوند، آن‌ها فاسد می‌مانند. داده‌های اینترنت اشیا خراب غیر از شرایط مخرب می‌تواند از موقعیت‌های بسیاری ناشی شود. رفاه معماری اینترنت اشیا تحت تأثیر بسیاری از عوامل مانند محیط، شرکت‌کنندگان، تخریب و خرابی دستگاه‌ها قرار دارد. بعضی اوقات خود دستگاه‌ها و سنسورها و محرک‌های آن‌ها از همان ابتدا به درستی کار نمی‌کنند. این وضعیت را نمی‌توان تشخیص داد تا زمانی که دستگاه موردنظر آزمایش شود، یا گاهی اوقات مدتی به درستی کار کند و به دلایلی رفتار خود را تغییر دهد (اتصال کوتاه، قطع اتصال، منسوخ شدن برنامه ریزی شده و غیره). علاوه بر این شرایط، تهدیدهای زیادی وجود دارد که می‌تواند IoT را تحت تأثیر قرار دهد مانند شنود، انکار سرویس یا کنترل . به همین دلیل، دستگاه‌های اینترنت اشیا باید قبل از ادغام با بلاکچین کاملاً آزمایش شوند و علاوه بر اینکه شامل تکنیک‌هایی برای تشخیص خرابی دستگاه به محض وقوع هستند، باید در مکان مناسب قرار بگیرند و در آن کپسول شوند (۷).

این دستگاه‌ها به احتمال زیاد هک می‌شوند، زیرا محدودیت‌های آن‌ها به‌روزرسانی سیستم عامل را محدود می‌کند و از این کار در مورد اشکالات احتمالی یا نقض امنیت جلوگیری می‌کند. علاوه بر این، گاهی اوقات دشوار است که دستگاه‌ها را به صورت یکپارچه به روز کنید، مانند استقرار جهانی اینترنت اشیا. بنابراین، مکانیزم های به‌روزرسانی و پیکربندی زمان اجرا باید در اینترنت اشیا قرار بگیرند تا با گذشت زمان اجرا شود. در حال حاضر، پروتکل‌های برنامه کاربردی اینترنت اشیا مانند CoAP و MQTT از پروتکل‌های امنیتی دیگری مانند TLS یا DTLS برای ارائه ارتباطات ایمن استفاده می‌کنند. این پروتکل‌های امن علاوه بر نیاز به مدیریت متمرکز و حاکمیت زیرساخت‌های کلیدی، معمولاً با PKI، پیچیده و سنگین هستند. در شبکه بلاکچین هر دستگاه اینترنت اشیا دارای GUID (شناسه جهانی منحصر به فرد) و جفت کلید نامتقارن خود است که پس از اتصال به شبکه نصب می‌شود. این پروتکل‌های امنیتی کنونی را که معمولاً باید گواهینامه‌های PKI را مبادله کنند ساده می‌کند و به آن‌ها امکان می‌دهد تا در دستگاه‌هایی با قابلیت‌های کمتری استفاده شوند.

یکی از پروژه‌های قابل‌توجه اینترنت اشیا از نظر امنیت با استفاده از بلاکچین، فیلامنت است.

Filament یک راه حل سخت‌افزاری و نرم‌افزاری است که عملکردی را برای پرداخت‌های مبتنی بر بیت کوین و قراردادهای هوشمند در اینترنت اشیا فراهم می‌کند. دستگاه‌های رشته‌ای پردازنده‌های رمزگذاری جاسازی‌شده‌ای دارند که از پنج پروتکل پشتیبانی می‌کنند: Blockname، Telehash و قراردادهای هوشمند برای کار، و علاوه بر این Pennyback و پروتکل‌های Bit-torrent. مدیریت هویت دستگاه با Blockname انجام می‌شود، درحالی‌که Telehash، پیاده‌سازی منبع باز Kademlia DHT، ارتباطات رمزگذاری شده ایمن را فراهم می‌کند و قراردادهای هوشمند روشی را برای استفاده از دستگاه تعریف می‌کنند(۹).

ناشناس بودن و حریم خصوصی داده‌ها

بسیاری از برنامه‌های اینترنت اشیا با داده‌های محرمانه کار می‌کنند، به‌عنوان مثال هنگامی که دستگاه به یک شخص متصل است، مانند سناریوی سلامت الکترونیکی، ضروری است که به مشکل حریم خصوصی داده‌ها و ناشناس ماندن بپردازید. Blockchain به‌عنوان راه حل ایدئال برای آدرس دهی به مدیریت هویت در اینترنت اشیا ارائه‌شده است، با این حال همانند بیت کوین، ممکن است برنامه‌هایی وجود داشته باشد که ناشناس بودن آن‌ها باید تضمین شود. این مورد مربوط به پوشیدنی است که توانایی پنهان کردن هویت شخص هنگام ارسال اطلاعات شخصی یا وسایل نقلیه هوشمندی را دارد که از حریم خصوصی برنامه‌های سفر کاربران محافظت می‌کنند (۸).

مشکل حریم خصوصی داده‌ها در بلاک چین‌های شفاف و عمومی قبلاً همراه با برخی از راه‌حل‌های موجود مورد بحث قرار گرفته است. با این حال، مشکل حریم خصوصی داده‌ها در دستگاه‌های اینترنت اشیا دشواری بیشتری را به همراه دارد، زیرا این مسئله از زمان جمع‌آوری اطلاعات شروع می‌شود و تا سطح ارتباطات و برنامه‌ها گسترش می‌یابد. ایمن‌سازی دستگاه به‌گونه‌ای که داده‌ها به‌صورت ایمن ذخیره شوند و افراد بدون اجازه به آن‌ها دسترسی نداشته باشند چالشی است زیرا نیاز به ادغام نرم‌افزار رمزنگاری امنیتی در دستگاه دارد. این پیشرفت‌ها باید محدودیت منابع دستگاه‌ها و محدودیت‌های مربوط به دوام اقتصادی را در نظر بگیرد. بسیاری از فناوری‌ها برای ایمن‌سازی ارتباطات با استفاده از رمزگذاری (IPsec، SSL / TLS، DTLS) استفاده‌شده‌اند. محدودیت‌های دستگاه اینترنت اشیا معمولاً استفاده از دستگاه‌های با محدودیت کمتر مانند درگاه‌ها برای ترکیب این پروتکل‌های امنیتی را ضروری می‌کند. استفاده از سخت‌افزار رمزنگاری می‌تواند عملیات رمزنگاری را تسریع کرده و از اضافه بار پروتکل‌های نرم‌افزاری امن پیچیده جلوگیری کند.

حفاظت از داده‌ها و حریم خصوصی چالش‌های اصلی اینترنت اشیا است، با استفاده از فناوری بلاکچین

می‌توان مشکل مدیریت هویت در اینترنت اشیا را کاهش داد. اعتماد یکی دیگر از ویژگی‌های اصلی اینترنت اشیا است که ادغام بلاکچین در آن می‌تواند نقش داشته باشد. در اهمیت اطمینان به سیستم‌های اینترنت اشیا به‌عنوان یکی از اهداف اصلی برای اطمینان از موفقیت آن مشخص‌شده است. تکنیک‌های یکپارچگی داده‌ها گزینه دیگری برای اطمینان از دسترسی به داده‌ها به‌طور هم‌زمان است زیرا از پر بار شدن بلاکچین با حجم عظیمی از داده‌های تولیدشده توسط اینترنت اشیا جلوگیری می‌کنند. این می‌تواند منجر به سیستم‌های عمومی‌شود، اما با یک کنترل دسترسی کارآمد و محدود. MuR-DPA [104]با وجود تأیید حسابرسی عمومی، به‌روزرسانی‌های داده‌های پویا و تأیید کارآمد را ارائه می‌دهد.

نتیجه‌گیری

فناوری Blockchain ابزاری جدید با کاربردهای بالقوه برای سازمان‌ها است که معاملات ایمن را بدون نیاز به مرجع مرکزی امکان‌پذیر می‌کند. از سال ۲۰۰۹، با استفاده از فناوری بلاکچین بیت کوین، تعداد بیشتری از راه‌حل‌های مبتنی بر فناوری بلاکچین وجود دارد.

اولین برنامه‌ها سیستم‌های نقدی الکترونیکی با توزیع یک دفتر جهانی بود که شامل همه معاملات بود. این تراکنش‌ها با هش‌های رمزنگاری ایمن می‌شوند و معاملات با استفاده از جفت کلیدهای نامتقارن امضا و تأیید می‌شوند. تاریخ معاملات به‌طور کارآمد و ایمن زنجیره‌ای از رویدادها را به‌گونه‌ای ثبت می‌کند که هرگونه تلاش برای ویرایش یا تغییر معامله گذشته نیز به محاسبه مجدد کلیه بلوک‌های بعدی معاملات نیاز دارد (۱۰).

استفاده از فناوری بلاکچین هنوز در مراحل اولیه است، اما بر اساس اصول رمزنگاری کاملاً شناخته شده و صوتی بنا شده است. در حال حاضر، هیجان زیادی در مورد این فناوری وجود دارد، و بسیاری از موارد استفاده شده برای آن استفاده شده است. با حرکت به جلو، احتمالاً اعتیاد به مواد مخدره از بین خواهد رفت و فناوری بلاکچین به ابزاری دیگر تبدیل خواهد شد که می‌تواند مورد استفاده قرار گیرد.

بلاکچین به‌عنوان یک فناوری نوظهور مهم، در بسیاری از زمینه‌ها نقش خواهد داشت. بنابراین، ما اعتقاد داریم که مسائل مربوط به کاربردهای تجاری زنجیره بلوک برای فعالیت‌های آکادمیک و اجتماعی بسیار حیاتی است. ما چندین پیشنهاد تحقیقاتی پیشنهادی را پیشنهاد می‌دهیم. اولین جهت مهم تحقیقاتی، درک سازوکارهایی است که بلاکچین از طریق آن‌ها روی کار آیی شرکت و بازار تأثیر می‌گذارد. دومین جهت تحقیق بالقوه، حفظ حریم خصوصی و مسائل امنیتی است. سومین مورد مربوط به نحوه مدیریت ارزهای دیجیتال و نحوه تنظیم بازار ارزهای رمزپایه است. چهارمین جهت تحقیق بالقوه نحوه ادغام عمیق فناوری بلاکچین و fintech است.

موضوع نهایی فناوری زنجیره‌ای متقابل است - اگر هر صنعت دارای سیستم بلاکچین خاص خود باشد، محققان و توسعه‌دهندگان باید روش‌های جدیدی را برای تبادل داده کشف کنند. این کلید دستیابی به اینترنت ارزش است. بنابراین، با گذشت زمان، فناوری بین زنجیره‌ای به موضوعی مهم تبدیل می‌شود.

مشاغل می‌توانند از فناوری بلاکچین به میزان قابل‌توجهی بهره‌مند شوند. بنابراین، ما پیشنهاد می‌کنیم که استفاده از بلاکچین در شرایطی موردتوجه قرار گیرد که مشاغل دارای شرایط زیر باشند: تسویه‌حساب، سرمایه‌گذاری گسترده، ذخیره و به اشتراک‌گذاری داده‌ها، مدیریت زنجیره تأمین و تجارت هوشمند. فناوری Blockchain ظرفیت فوق‌العاده‌ای دارد که می‌تواند روند تجاری موجود، خدمات دولت الکترونیکی، خدمات مالی، خدمات بهداشتی، خدمات کشاورزی و غیره را به ابعاد جدید تبدیل کند که مزایای اضافی از نظر کار آیی، هزینه، اعتماد، امنیت، یکپارچگی داده‌ها و غیره تضمین می‌شود. فناوری Blockchain نیاز شخص ثالث به اعتبار سنجی معاملات از طریق شبکه را از بین می‌برد.

در این مقاله ما در مورد فناوری Blockchain و کاربردهای آن برای سیستم‌های اینترنت اشیا بحث کردیم. ما همچنین در مورد نیاز مدیریت کلیدی برای Blockchain بحث کردیم که شامل مدیریت کلیدی برای کیف پول ارزی بیت کوین و زیرساخت کلید عمومی Blockchain است (۱۱).

منابع

1. Khan, M. A., and Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.
2. A systematic literature review of blockchain-based applications Current status, classifcation and open issues.
3. Blockchain for AI: Review and Open Research Challenges.
4. Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.
5. Drljevic, N., Aranda, D. A., and Stantchev, V. (2020). Perspectives on risks and standards that affect the requirements engineering of blockchain technology. Computer Standards and Interfaces, 69, 103409.
6. Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S., and Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry?. *Journal of Industrial Information Integration*, *17*, 100125.
7. Kamran, M., Khan, H. U., Nisar, W., Farooq, M., and Rehman, S. U. (2020). Blockchain and Internet of Things: A bibliometric study. *Computers and Electrical Engineering*, *81*, 106525.
8. Pal, O., Alam, B., Thakur, V., and Singh, S. (2019). Key management for blockchain technology. *ICT Express*.
9. Pereira, J., Tavalaei, M. M., and Ozalp, H. (2019). Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technological Forecasting and Social Change*, *146*, 94-102.
10. Reyna, A., Martín, C., Chen, J., Soler, E., and Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.
11. Gagneja, K., and Kiefer, R. (2020, February). Security Protocol for Internet of Things (IoT): Blockchain-based Implementation and Analysis. In *2020 Sixth International Conference on Mobile And Secure Services (MobiSecServ)* (pp. 1-6). IEEE.