"مقاله مروری افزایش امنیت اینترنت اشیا با استفاده از بلاک چین برای مدیریت هویت غیرمتمرکز"

دکنر رضا عزیزی[۱]، عزیزه آقایی میبدی[۲]

گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران[۱]

گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران[۲]

چکیده

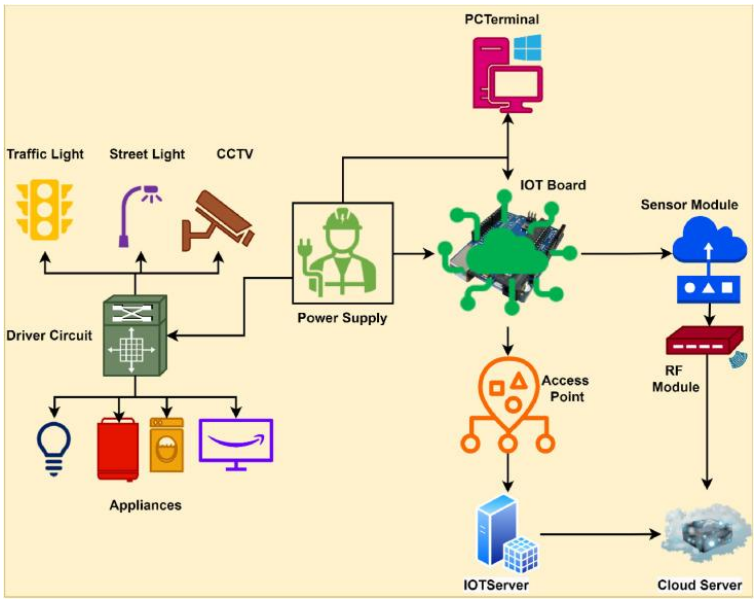
اینترنت اشیا انقلابی در نحوه ارتباط و تعامل دستگاه‌ها با یکدیگر ایجاد کرده است, که منجر به افزایش کارایی در بخش‌های مختلف مانند مراقبت‌های بهداشتی, کشاورزی, شهرهای هوشمند, و اتوماسیون صنعتی شده است. با این حال، این گسترش سریع دستگاه‌های به هم پیوسته، خطرات امنیتی را نیز افزایش داده است و حفاظت از داده‌ها و سیستم‌های حساس را در اولویت قرار داده است. یکی از راه حل‌های امیدوارکننده برای افزایش امنیت اینترنت اشیا، فناوری بلاک چین است. با استفاده از ماهیت غیرمتمرکز و تغییرناپذیر بلاک چین, می‌توانیم وضعیت امنیتی برنامه‌های اینترنت اشیا را به میزان قابل توجهی بهبود بخشیم. این مقاله بررسی می‌کند که چگونه می‌توانیم از فناوری بلاک چین برای ایجاد یک سیستم مدیریت هویت غیرمتمرکز برای دستگاه‌های اینترنت اشیا استفاده کرد. چالش‌های ناشی از افزایش تعداد دستگاه های متصل و اهمیت احراز هویت ایمن و یکپارچگی داده ها را بررسی می‌کند.

واژه‌های کلیدی: اینترنت اشیا، امنیت اینترنت اشیا، بلاک چین

۱- مقدمه

اینترنت اشیاء (Internet of Things) اختصاری (IOT)به مجموعه ای از ارتباطات و تعاملات رایانه ای و فناوری بنیاد مانند حسگر، واحدهای پردازش، نرم‌افزار و سخت افزار با دیگر دستگاه‌ها و سامانه‌ها (که در اصطلاح فنی اشیاء یا چیزها نامیده می‌شوند) از طریق اینترنت یا دیگر شبکه‌های ارتباطی است.(شکل ۱) اینترنت اشیا ادغام اشیاء فیزیکی با سیستم‌های اطلاعات دیجیتال را نشان می‌دهد و به میلیاردها دستگاه - از حسگرها گرفته تا وسایل هوشمند - امکان اتصال، جمع آوری و تبادل داده‌ها را به صورت یکپارچه می‌دهد. این تکامل قابلیت‌های اینترنت را فراتر از دستگاه‌های سنتی گسترش می‌دهد و فرصت‌های جدیدی را برای زیرساخت‌های هوشمند و اتوماسیون ایجاد می‌کند. در نهایت، اینترنت اشیا در حال تغییر نحوه تعامل انسان ها با فناوری در صنایع مختلف و برنامه های روزمره است.

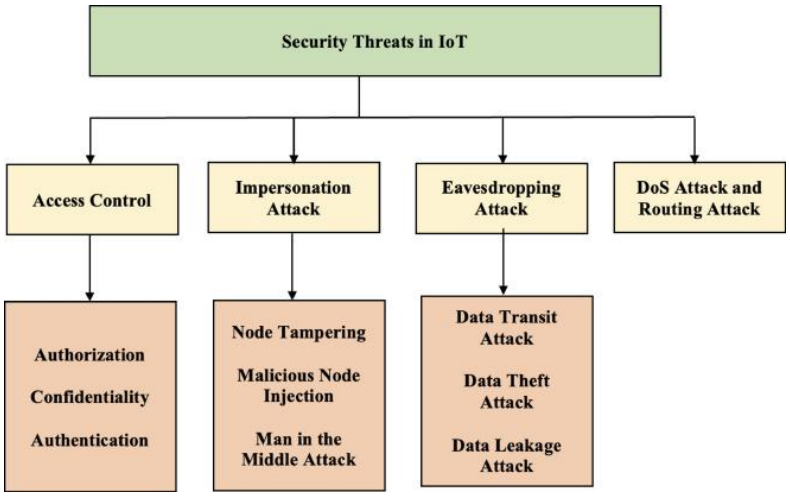
اما همان‌طور که می‌دانید اغلب همزمان با هر میزان رشدی، یکسری مشکلات و چالش‌های امنیتی برای وسایل و تجهیزاتی که قابلیت‌های بالایی در استفاده دارند، به وجود می‌آیند. آسیب پذیری‌های اینترنت اشیا باعث شده تا کمپانی‌های بزرگ و مصرف‌کنندگان این تجهیزات نگران مشکلاتی که ممکن است در حین راه‌اندازی و استفاده به وجود بیاید، باشند. لذا باید با بکارگیری دانش و پشتکار خود برای برطرف کردن این مشکلات راه حلی اساسی بیابیم. از جمله کاربردهای فراوان تجهیزات اینترنت اشیا، در خانه‌های هوشمند می‌باشد. اما متأسفانه در حال حاضر شاهد هک شدن و ایجاد آسیب‌پذیری‌هایی در دستگاه‌های کاربردی در خانه‌های هوشمند از قبیل تجهیزات مربوط به مراقبت از کودکان و بزرگسالان گرفته تا از کار انداختن کامل اینترنت می‌باشیم. (G. Sagirlar etal ۲۰۱۸)



شکل (۱): اینترنت اشیا

۲- چالش ها در امنیت اینترنت اشیا و راهکارهای آن با بلاک چین

فناوری بلاک چین به عنوان یک راهکار نوآورانه برای بهبود امنیت و کارایی در اینترنت اشیا (IoT) شناخته می‌شود. در زیر به برخی از جنبه‌های کلیدی پیاده‌سازی بلاک چین در IoT اشاره می‌شود.شکل(۲)



شکل(۲): چالش ها در امنیت اینترنت اشیا

۲-۱- تمرکززدایی و اعتماد

معماری‌های سنتی اینترنت اشیا معمولا برای جمع آوری، ذخیره و پردازش داده‌ها به سرورهای متمرکز متکی هستند. این تمرکز یک نقطه شکست ایجاد می‌کند و این سیستم‌ها را در برابر حملاتی مانند نقض داده‌ها و حملات انکار سرویس (DoS) آسیب پذیر می‌کند. در مقابل، بلاک چین داده‌ها را در شبکه ای از گره‌ها توزیع می‌کند و تنها نقطه شکست را از بین می‌برد و سیستم انعطاف پذیرتری را ارائه می‌دهد. هر دستگاه در شبکه اینترنت اشیا می‌تواند مستقیما از طریق قراردادهای هوشمند در بلاک چین با یکدیگر تعامل داشته باشد و باعث افزایش اعتماد بدون نیاز به مرجع مرکزی شود.

۲-۲- سوابق داده تغییرناپذیر

بلاک چین با استفاده از رمزنگاری و ساختار غیرمتمرکز خود، امنیت داده‌های جمع‌آوری‌شده از دستگاه‌های IoT را افزایش می‌دهد. این امر به جلوگیری از دسترسی غیرمجاز و تغییر داده‌ها کمک می‌کند. فناوری بلاک چین امکان ایجاد سوابق ضد

دستکاری تمام تراکنش‌ها و تبادل داده‌ها را فراهم می‌کند. هر بلوک در زنجیره دارای مهر زمانی است و به بلوک قبلی متصل می‌شود و تاریخچه‌ای دائمی و غیرقابل تغییر از تعاملات ایجاد می‌کند. این ویژگی برای برنامه‌های اینترنت اشیا بسیار ارزشمند است, به ویژه در بخش‌هایی مانند مدیریت زنجیره تامین و مراقبت‌های بهداشتی, جایی که یکپارچگی داده‌ها بسیار مهم است. به عنوان مثال، یک دستگاه سلامت هوشمند می‌تواند داده‌های بیمار را در یک بلاک چین ثبت کند و اطمینان حاصل کند که اطلاعات دقیق، قابل ردیابی و قابل اعتماد هستند.

۲-۳- احراز هویت و کنترل دسترسی پیشرفته

یکی از چالش‌های مهم در امنیت اینترنت اشیا این است که اطمینان حاصل شود که فقط دستگاه‌ها و کاربران مجاز می‌توانند به داده‌ها و منابع حساس دسترسی داشته باشند. بلاک چین می‌تواند فرآیندهای احراز هویت را از طریق تکنیک های رمزنگاری افزایش دهد. با صدور کلیدهای رمزنگاری منحصر به فرد به دستگاه ها، بلاک چین تأیید هویت ایمن را امکان پذیر می‌کند و تضمین می‌کند که فقط دستگاه‌های قانونی می‌توانند در شبکه شرکت کنند. علاوه بر این، قراردادهای هوشمند می‌توانند کنترل دسترسی را خودکار کنند و قوانینی را برای افرادی که می‌توانند بر اساس شرایط از پیش تعیین شده به داده‌ها یا عملکردهای خاص دسترسی داشته باشند، تعریف کنند.

۲-٤- اشتراک گذاری ایمن داده‌ها و قابلیت همکاری

دستگاه‌های اینترنت اشیا اغلب متعلق به سازندگان مختلف هستند و از پروتکل‌های ارتباطی مختلفی استفاده می‌کنند, ایجاد مشکلاتی در اشتراک گذاری داده‌ها و قابلیت همکاری، بلاک چین با ارائه یک چارچوب مشترک برای تراکنش ها، اشتراک گذاری امن داده ها را بین دستگاه‌های مختلف تسهیل می‌کند. این نه تنها تضمین می‌کند که داده‌ها می‌توانند به طور ایمن مبادله شوند، بلکه همکاری بین اکوسیستم‌های مختلف اینترنت اشیا را نیز تقویت می‌کند. به عنوان مثال، در یک شهر هوشمند، سیستم‌های مدیریت ترافیک می‌توانند داده های بلادرنگ را از منابع مختلف از طریق یک بلاک چین به اشتراک بگذارند و جریان کلی ترافیک را بهبود بخشند و در عین حال امنیت را حفظ کنند.

۲-۵- انعطاف پذیری در برابر حملات سایبری

تهدیدات امنیت سایبری مانند هک، فیشینگ و حملات بدافزار در شبکه‌های اینترنت اشیا فراگیر است. ساختار غیرمتمرکز بلاک چین، به خطر انداختن شبکه را برای مهاجمان به طور قابل توجهی چالش برانگیزتر می‌کند. از آنجایی که هیچ مخزن مرکزی داده برای هدف قرار دادن وجود ندارد، یک مهاجم باید کنترل چندین گره را به دست آورد تا تأثیری داشته باشد و پیچیدگی و هزینه یک حمله را به میزان قابل توجهی افزایش دهد. علاوه بر این، استفاده از دفتر کل توزیع شده می‌تواند نظارت و تشخیص رفتار غیرعادی را در زمان واقعی تسهیل کند و امکان پاسخ سریع تر به تهدیدات بالقوه را فراهم کند.

۲-٦- قابلیت حسابرسی و انطباق

با ثبت تمام تراکنش‌ها و داده‌ها در یک دفتر کل توزیع‌شده، بلاک چین امکان ردیابی و شفافیت را فراهم می‌کند. این ویژگی به ویژه در زنجیره تأمین و مدیریت دارایی‌ها مفید است . مشاغلی که در صنایع تنظیم شده فعالیت می‌کنند باید استانداردهای انطباق

سختگیرانه در مورد مدیریت داده‌ها را رعایت کنند. دفتر کل تغییرناپذیر بلاک چین ابزاری موثر برای حسابرسی تراکنش ها و تبادل داده‌ها فراهم می کند و نشان دادن انطباق را برای سازمان ها آسان تر می کند. هر تراکنش را می‌توان به منشأ خود ردیابی کرد و ذینفعان می‌توانند به داده‌های تاریخی دسترسی داشته باشند تا انطباق با مقرراتی مانند GDPR یا قوانین مراقبت های بهداشتی را تأیید کنند..

۲-۷- مدیریت هویت

بلاک چین می‌تواند به مدیریت هویت دستگاه‌های IoT کمک کند. هر دستگاه می‌تواند یک هویت دیجیتال منحصر به فرد داشته باشد که به آن اجازه می‌دهد به طور ایمن با سایر دستگاه‌ها ارتباط برقرار کند.

۲-۸- قراردادهای هوشمند

استفاده از قراردادهای هوشمند در بلاک چین به دستگاه‌های IoT این امکان را می‌دهد که به صورت خودکار و بدون نیاز به واسطه، تراکنش‌ها را انجام دهند. این امر می‌تواند به بهینه‌سازی فرآیندها و کاهش هزینه‌ها کمک کند.

۲-۹- کاهش هزینه‌ها

با حذف واسطه‌ها و بهبود کارایی، بلاک چین می‌تواند هزینه‌های مربوط به مدیریت و پردازش داده‌ها را کاهش دهد.

۳- بررسی متون

ادغام فناوری بلاک چین با اینترنت اشیا در سال‌های اخیر توجه قابل توجهی را به خود جلب کرده است و محققان رویکردهای مختلفی را برای رسیدگی به چالش‌ها و بهره‌برداری از مزایای در حوزه‌های مختلف بررسی می‌کنند. دلیل این ادغام پرداختن به چالش‌های زیادی مانند حریم خصوصی داده‌ها، امنیت، یکپارچگی و مقیاس‌پذیری است، این موارد حیاتی در محیط‌های IoT هستند که توسط شبکه‌های قابل‌توجهی از دستگاه‌های متصل به هم توصیف شده‌اند. مطالعات مختلف توسط بسیاری از محققان، کاربردهای بلاک چین را در بسیاری از حوزه‌ها مانند مراقبت‌های بهداشتی، زنجیره تامین، صنعت، شهر هوشمند، مخابرات، رای‌گیری الکترونیکی و غیره با تمرکز بر افزایش مسائل امنیتی و قابلیت اطمینان سیستم‌های اینترنت اشیا مورد بررسی قرار دادند. در مدیریت زنجیره تامین [A. Kaur,۲۰۲۲][Y. Madhwal etal ۲۰۲۳][S. Aich etal ۲۰۱۹],[A. Rejeb etal ۲۰۱۹] بلاک چین برای اطمینان از یکپارچگی و قابلیت ردیابی کنترل می شود و امکان نظارت بر زمان واقعی کالاها را هنگام عبور از شبکه جهانی پیچیده فراهم می کند. بلاک چین در مراقبت های بهداشتی],[T. Wang,۲۰۲٤ [P. Hemalatha,۲۰۲۱] [[R.S. Velamakanni,۲۰۲٤],[M. Kumaresan,۲۰۲۲ برای ایمن سازی داده‌های بیمار، تضمین حریم خصوصی و یکپارچگی داده‌های ثبت اختراع، همچنین به اشتراک گذاری امن داده‌ها در بین سازمان‌ها استفاده می‌شود.

علاوه بر این، شهرهای هوشمند [H.M. Rai,۲۰۲۳, L.T. Khrais,۲۰۲۰] همچنین با تضمین یکپارچگی داده ها و امکان تصمیم گیری غیرمتمرکز، بلاک چین را برای اداره و بهبود زیرساخت‌های کلان شهرها، از شبکه‌های انرژی گرفته تا سیستم‌های حمل و نقل عمومی، پیاده سازی می‌کنند.

جدول ۱ رویکردهای متنوع و تمرکز آنها بر ادغام IoT و Blockchain در برنامه‌های مختلف، همراه با یافته‌ها و محدودیت‌ها را در بر می‌گیرد. در طول بررسی خود، از چندین مقاله بررسی شده که طی سال‌های ۲۰۱۷-۲۰۲٤ منتشر شده‌اند، استفاده کردیم. بر اساس بینش جمع آوری شده از جدول، مشاهدات خود را ارائه می‌کنیم.

جدول ۱. مروری بر ادغام اینترنت اشیا و بلاک چین در سراسر دامنه ها

مرجع	نویسنده	سال	موضوع تمرکز	فواید	محدودیت‌ها
[۱۲]	A.Dorri	۲۰۱۷	بهینه سازی بلاک چین برای اینترنت اشیا	بهینه سازی فناوری بلاک چین برای استفاده کارآمد و مقرون به صرفه در برنامه های IoT.	مبادله بین مقیاس پذیری و امنیت، پتانسیل آسیب پذیری در مکانیسم های اجماع اساسی
[۱۳]	G. Sagirlar et al.	۲۰۱۸	معماری بلاک چین هیبریدی برای اینترنت اشیا	زیرساخت مقیاس پذیر و غیرمتمرکز برای تبادل امن داده در شبکه های IoT	افزایش پیچیدگی در مقایسه با معماری های سنتی، پتانسیل ایجاد گلوگاه مقیاس پذیری در حجم تراکنش های بالا.
[۱٤]	A. F. Zorzo et al.	۲۰۱۸	اینترنت اشیا قابل اعتماد با استفاده از بلاک چین	استفاده از بلاک چین برای اطمینان از یکپارچگی داده ها و تحمل خطا در سیستم های اینترنت اشیا.	چالش های مقیاس پذیری و پتانسیل تراکم شبکه با افزایش تعداد دستگاه ها
[۱۵]	A. Rejeb et al.	۲۰۱۹	استفاده از اینترنت اشیا و بلاک چین در SCM	ترکیب اینترنت اشیا و بلاک چین برای بهبود دید زنجیره تامین و کاهش هزینه ها	افزایش پیچیدگی در اجرا و مسائل بالقوه قابلیت همکاری‌های مختلف
[۱٦]	T. Alam	۲۰۱۹	نقش بلاک چین در اینترنت اشیا	استفاده از بلاک چین برای یکپارچگی داده ها، شفافیت و کنترل غیرمتمرکز در سیستم های اینترنت اشیا	محدودیت‌های مقیاس‌پذیری بالقوه و افزایش مصرف انرژی در مقایسه با رویکردهای متمرکز

[۱۷]	L. T. Khrais	۲۰۲۰	نقش اینترنت اشیا و بلاک چین در شهر هوشمند	استفاده از اینترنت اشیا و بلاک چین برای افزایش امنیت داده ها و بهبود کارایی در برنامه های شهر هوشمند	چالش های یکپارچه سازی بین سیستم های مختلف و نگرانی های بالقوه حفظ حریم خصوصی در مورد داده های جمع آوری شده.
[۱۸]	D. Pavithran	۲۰۲۰	چارچوب بلاک چین برای اینترنت اشیا	توسعه یک چارچوب بلاک‌چین برای مدیریت امن و قابل اعتماد داده‌ها در شبکه‌های اینترنت اشیاء.	محدودیت‌های مقیاس‌پذیری و گلوگاه‌های بالقوه عملکردی با رشد شبکه.
[۱۹]	P. Hemalatha et al.	۲۰۲۱	نظارت و تأمین امنیت داده‌های بهداشتی	فعال‌سازی سوابق داده‌های بهداشتی غیرقابل تغییر و امنیت بهبود یافته از طریق فناوری بلاک‌چین.	نگرانی‌های مربوط به حریم خصوصی در مورد داده‌های حساس سلامت و موانع احتمالی قانونی در مدیریت داده‌های بهداشتی.
[۲۰]	E. A. Shammar and A. T. Zahary	۲۰۲۱	نگرش امنیتی به ادغام اینترنت اشیاء	تقویت امنیت داده‌ها و کاهش ریسک تقلب از طریق ادغام بلاک‌چین با سیستم‌های اینترنت اشیا.	افزایش پیچیدگی و احتمال بار اضافی عملکرد به دلیل ماهیت توزیع‌شده بلاک‌چین
[۲۱]	Kumaresan et al., ۲۰۲۲	۲۰۲۲	بلاک‌چین، اینترنت اشیاء و G۵ در بهداشت و درمان هوشمند	استفاده از مزایای ترکیبی فناوری بلاک‌چین، اینترنت اشیاء و G۵ برای بهبود امنیت و حریم خصوصی در سیستم‌های بهداشت و درمان هوشمند.	چالش‌های ادغام بین این فناوری‌های مختلف و مشکلات بالقوه مقیاس‌پذیری.
[۲۲]	Alzuabi et al.	۲۰۲۲	مسائل حریم خصوصی و امنیت در سیستم‌های اینترنت اشیاء مبتنی بر بلاک‌چین	شناسایی و رسیدگی به آسیب‌پذیری‌های حریم خصوصی و امنیتی در سیستم‌های اینترنت اشیاء مبتنی بر بلاک‌چین.	توازن بین نگرانی‌های حریم خصوصی و نیاز به شفافیت داده‌ها و احتمال سوءاستفاده‌های

					امنیتی در فناوری بلاک‌چین زیرین.
[۲۳]	Santos et al.	۲۰۲۳	مدیریت وفاداری مبتنی بر بلاک چین	استفاده از بلاک چین برای ایجاد انگیزه برای وفاداری مشتری و کاهش هزینه ها در برنامه های وفاداری.	نیاز به یک پلت فرم عمومی برای تسهیل پذیرش گسترده و چالش های بالقوه یکپارچه سازی با سیستم های موجود
[۲٤]	Sallal et al.	۲۰۲۳	حفظ حریم خصوصی و قابلیت تایید در رای گیری الکترونیکی	دستیابی به حریم خصوصی و قابلیت تایید در سیستم های رای گیری الکترونیکی با استفاده از رمزنگاری های اولیه فعال شده توسط بلاک چین.	افزایش پیچیدگی به دلیل تکنیک های رمزنگاری و چالش های بالقوه قابلیت استفاده برای رأی دهندگان.
[۲۵]	Magara & Zhou	۲۰۲۴	بررسی برنامه های کاربردی اینترنت اشیا و نگرانی های حفظ حریم خصوصی/امنیتی	تجزیه و تحلیل خطرات حریم خصوصی و امنیتی مرتبط با برنامه های مختلف اینترنت اشیا و پیشنهاد مقیاس پذیر.	مشکل در اجرای راه‌حل‌های مؤثر و تطبیق چارچوب‌های خط‌مشی موجود برای رسیدگی به ماهیت در حال تحول تهدیدات اینترنت اشیا
[۲٦]	T. Wang et al.	۲۰۲۴	ایجاد انقلابی در اشتراک گذاری داده های مراقبت های بهداشتی با استفاده از رویکرد بلاک چین هیبریدی ایمن	باز کردن قدرت تبادل داده های سلامت ایمن و خصوصی.	پیمایش در پیچیدگی ها: پیچیدگی پیاده سازی و موانع مقیاس پذیری بالقوه.

Dorri (۲۰۱۷) به موضوع حیاتی بهینه‌سازی بلاک چین برای محیط‌های IoT با محدودیت منابع می‌پردازد. هدف این رویکرد غلبه بر محدودیت‌ها در مقیاس‌پذیری و کارایی با طراحی معماری بلاک چین به‌طور خاص برای موارد استفاده از اینترنت اشیا است. G. Sagirlar (۲۰۱۸) یک استراتژی ترکیبی را ترویج کرد که از مزایای بلاک چین های خصوصی و عمومی استفاده می کند. برای کاربردهای اینترنت اشیا، این رویکرد امنیت، تمرکززدایی و مقیاس‌پذیری را ارتقا می‌دهد. از سوی دیگر، رسیدگی به پیچیدگی‌های زیر بلاک‌چین اثبات کار نیازمند بررسی دقیق است. A.F. Zorzo etal (۲۰۱۸) امکان بلاک چین برای ایجاد IoTsolution های قابل اعتماد را بررسی کرد. تمرکز اصلی آنها بر یکپارچگی و قابلیت اطمینان داده ها است، که اجزای ضروری

برای سیستم های حیاتی هستند که به اطلاعات قابل اعتماد وابسته هستند. با این حال، مسائل مربوط به سازگاری و تراکم ترافیک در شبکه‌ها ممکن است این استراتژی را برای کاربردهای مقیاس بزرگ غیرعملی کند.

(A. Rejeb etal ۲۰۱۹) بینشی در مورد احتمالات انقلابی برای فناوری بلاک چین در خدمات زنجیره تامین ارائه کرد. زنجیره‌های تامین ممکن است به لطف این فناوری دستخوش تحولی اساسی شوند که می‌تواند تقلب را کاهش دهد و شفافیت و قابلیت ردیابی را افزایش دهد. پذیرش گسترده هنوز به دلیل مسائل مربوط به غلبه بر نگرانی های یکپارچه سازی با سیستم های فعلی و تضمین سازگاری محدود است.(Alam ۲۰۱۹) بر نقش حیاتی بلاک چین در اینترنت اشیا تاکید کرد. فناوری بلاک چین با ارتقای یکپارچگی داده ها، شفافیت و کنترل غیرمتمرکز، این پتانسیل را دارد که ارتباطات و تعامل داده بین دستگاه های IoT را تغییر دهد. مشکلات مقیاس پذیری و مصرف انرژی همچنان موانع اصلی اجرای گسترده تر هستند.(Pavithran ۲۰۲۰) یک چارچوب بلاک چین طراحی شده برای راه اندازی اینترنت اشیا ارائه کرد. این استراتژی به دنبال حل مسائل متمایز دستکاری داده ها و دسترسی غیرقانونی در شبکه های IoT با بهبود یکپارچگی داده ها و کنترل غیرمتمرکز است. با این حال، مشکلات مقیاس پذیری و محدودیت های احتمالی عملکرد باید در طول فرآیند نصب به دقت مورد توجه قرار گیرند. کریس (L.T. Khrais ۲۰۲۰) مزایای بالقوه ترکیب اینترنت اشیا و بلاک چین را در توسعه شهر هوشمند برجسته کرد. این استراتژی پتانسیل بهبود امنیت داده‌ها، کارایی و فعال‌سازی خدمات جدید را دارد که در نتیجه ایجاد زیرساخت شهری پایدار و انعطاف‌پذیر است. با این حال، مسائل یکپارچه سازی و مشکلات بالقوه حریم خصوصی باید به دقت مورد بررسی قرار گیرد تا به طور کامل وعده این فناوری در برنامه های کاربردی شهر هوشمند محقق شود.

(Shammar and Zahary ۲۰۲۱) مفاهیم امنیتی ترکیب بلاک چین با اینترنت اشیا را بررسی کردند. تکنیک آنها از دفتر کل غیرقابل تغییر بلاک چین و رمزگذاری قوی برای بهبود امنیت داده ها و کاهش خطرات کلاهبرداری در شبکه های IoT استفاده می کند. با این حال، پیچیدگی های پیاده سازی و سربار عملکرد قابل توجه نیاز به بررسی دقیق دارد. (P. Hemalatha ۲۰۲۱) استفاده از اینترنت اشیا و بلاک چین را برای نظارت و ایمن سازی داده های مراقبت های بهداشتی بررسی کرد. این استراتژی سوابق داده های تغییرناپذیر و افزایش امنیت را تضمین می کند که برای محافظت از حریم خصوصی بیمار و جلوگیری از دسترسی غیرقانونی به اطلاعات حساس پزشکی ضروری است.

(W. Alzuabi etal ۲۰۲۲) بر اهمیت شناسایی و رفع هرگونه نقص امنیتی در این سیستم ها تأکید کرد. سیاست گذاران، رهبران صنعت، و محققان باید با یکدیگر همکاری کنند تا چارچوب های موفقی را ایجاد کنند که ضمن محدود کردن خطرات، نوآوری را تشویق کند. (M. Kumaresan ۲۰۲۲ etal) و .T. (T. Wang etal ۲۰۲۴) تکنیک هایی را برای رسیدگی به مسائل مقیاس پذیری مرتبط با ادغام بلاک چین با اینترنت اشیا ارائه کرد. این پیشرفت‌ها برای اجازه دادن به استقرار در مقیاس بزرگ فناوری حیاتی هستند. (M. Sallal etal ۲۰۲۳) و (Magara & Zhou ۲۰۲٤) روش هایی را برای گنجاندن مکانیسم های حفظ حریم خصوصی در سیستم های اینترنت اشیاء مبتنی بر بلاک چین مورد بررسی قرار دادند. این امر در ایجاد تعادل بین نیازهای باز بودن و امنیت اطلاعات، به ویژه در بخش های بسیار حساس مانند مراقبت های بهداشتی، بسیار مهم است.

افزایش امنیت، یکپارچگی داده ها، باز بودن، و کاهش تقلب از مزایای تکرارشونده در میان تکنیک های مختلف است. با این وجود، موانع مهمی با مشکلات مقیاس پذیری، پیچیدگی پیاده سازی، حریم خصوصی و هزینه عملکرد احتمالی ایجاد می شوند. بسیاری از

استراتژی‌ها و حوزه‌های تمرکز برای ترکیب بلاک چین با اینترنت اشیا در این مرور کلی نشان داده شده‌اند. همه استراتژی ها مزایای متفاوتی دارند و با موانع مختلفی روبرو می شوند. فناوری بلاک چین پتانسیل زیادی برای بهبود امنیت، کارایی و شفافیت در IoTsystems دارد، اما تحقق پتانسیل کامل آن در کاربردهای عملی نیازمند حل چالش‌ها با مقیاس‌پذیری، قابلیت همکاری و قانون است. برای اینکه راه‌حل‌های مبتنی بر بلاک چین در سراسر اکوسیستم‌های اینترنت اشیا به کار گرفته شوند، رهبران صنعت، محققان و قانون‌گذاران باید برای غلبه بر این موانع با یکدیگر همکاری کنند.

٤- نتیجه

این مقاله یک تحلیل جامع در مورد کاربرد بلاک چین برای سیستم‌های اینترنت اشیا و تهدیدات مختلفی که بر امنیت و حریم خصوصی داده‌های اینترنت اشیا تأثیر می‌گذارد ارائه می‌کند. این بررسی طبقه‌بندی تهدیدات امنیتی مختلف در اینترنت اشیا را مورد بحث قرار می‌دهد و به طور مختصر کارهای موجود را که از بلاک چین برای امنیت اینترنت اشیا استفاده می‌کنند، مورد بحث قرار می‌دهد. علاوه بر این، بررسی بر بحث ادغام بلاک چین با اینترنت اشیا تمرکز دارد و مزایا، چالش‌ها، تکنیک‌های امنیتی و پارامترهای ارزیابی عملکرد را تشریح می‌کند. از این بررسی می توان استنباط کرد که فناوری بلاک چین یکی از فناوری های امیدوارکننده است که می تواند مزایای بی شماری را از نظر افزایش امنیت و حفظ حریم خصوصی داده های اینترنت اشیا ارائه دهد و به گسترش اینترنت اشیا برای کاربردهای مختلف کمک کند. مسائل شناسایی شده نشان می دهد که استقرار بلاک چین برای اینترنت اشیا هنوز در مرحله اولیه خود است و تقاضای فزاینده ای برای کارهای تحقیقاتی برای رسیدگی به چالش ها و پیچیدگی های مرتبط با ادغام بلاک چین با اینترنت اشیا وجود دارد. در این زمینه، این بررسی برخی از موضوعات باز برجسته و جهت‌گیری‌های احتمالی تحقیقاتی آینده را شناسایی می‌کند که می‌تواند به محققانی که قصد ادغام بلاک چین و اینترنت اشیاء را دارند کمک کند.

٥- مراجع

[١] G. Sagirlar, B. Carminati, E. Ferrari, J.D. Sheehan, E. Ragnoli
Hybrid-IoT: hybrid blockchain architecture for internet of things - PoW sub-blockchains
٢٠١٨ IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE (Jul. ٢٠١٨), pp. ١٠٠٧-١٠١٦, ١٠,١١٠٩/Cybermatics_٢٠١٨,٢٠١٨,٠٠١٨

[٢] A. Rejeb, J.G. Keogh, H. Treiblmaier
Leveraging the internet of things and blockchain technology in supply chain management
Future Internet, ١١ (٧) (Jul. ٢٠١٩), p. ١٦١, ١٠,٣٣٩٠/fi١١٠٧٠١٦١

[٣] S. Aich, S. Chakraborty, M. Sain, H. Lee, H. Kim

A review on benefits of IoT integrated blockchain based supply chain management implementations across different sectors with case study
٢٠١٩ ٢١st International Conference on Advanced Communication Technology (ICACT) (٢٠١٩), pp. ١٣٨-١٤١, ١٠,٢٣٩١٩/ICACT.٢٠١٩,٨٧٠١٩١٠
February

[٤] Y. Madhwal, Y. Yanovich, S. Balachander, K.H. Poojaa, R. Saranya, B. Subashini
Enhancing supply chain efficiency and security: a proof of concept for IoT device integration with blockchain
IEEE Access, ١١ (٢٠٢٣), pp. ١٢١١٧٣-١٢١١٨٩, ١٠,١١٠٩/ACCESS.٢٠٢٣,٣٣٢٨٥٦٩

[٥] A. Kaur, G. Singh, V. Kukreja, S. Sharma, S. Singh, B. Yoon
Adaptation of IoT with blockchain in food supply chain management: an analysis-based review in development, benefits and potential applications
Sensors, ٢٢ (٢١) (Oct. ٢٠٢٢), p. ٨١٧٤, ١٠,٣٣٩٠/s٢٢٢١٨١٧٤

[٦] P. Hemalatha, S. Balaji, E. Chandru, P. Pradeep, D. Saravanan
Monitoring and securing the healthcare data harnessing IOT and blockchain technology
١٢ (٢) (٢٠٢١), pp. ٢٥٥٤-٢٥٦١

[٧] T. Wang, Q. Wu, J. Chen, F. Chen, D. Xie, H. Shen
Health data security sharing method based on hybrid blockchain
Future Generat. Comput. Syst., ١٥٣ (Apr. ٢٠٢٤), pp. ٢٥١-٢٦١, ١٠,١٠١٦/j.future.٢٠٢٣,١١,٠٣٢

[٨] M. Kumaresan, R. Gopal, M. Mathivanan, T. Poongodi
Amalgamation of blockchain, IoT, and ٥G to improve security and privacy of smart healthcare systems
Blockchain Applications for Healthcare Informatics, Elsevier (٢٠٢٢), pp. ٢٨٣-٣١٢, ١٠,١٠١٦/B٩٧٨-٠-٣٢٣-٩٠٦١٥-٩,٠٠٠١٥-٣

[٩] R.S. Velamakanni, D.P.S. Patwal
Enhancing IoT Security through Experimental Methods and Blockchain Integration
Educational Administration Theory and Practices (May ٢٠٢٤), ١٠,٥٣٥٥٥/kuey.v٣٠i٥,٤٤٦٨

[١٠] H.M. Rai, Atik Ur-Rehman, A. Pal, S. Mishra, K.K. Shukla
Use of Internet of Things in the context of execution of smart city applications: a review
Discover Internet of Things, ٣ (١) (Aug. ٢٠٢٣), ١٠,١٠٠٧/s٤٣٩٢٦-٠٢٣-٠٠٠٣٧-٢

[١١] L.T. Khrais
IoT and Blockchain in the Development of Smart Cities
(January, ٢٠٢٠), ١٠,١٤٥٦٩/IJACSA.٢٠٢٠,٠١١٠٢٢٠

[١٢] A. Dorri, S.S. Kanhere, R. Jurdak
Towards an optimized BlockChain for IoT
Proceedings of the Second International Conference on Internet-Of-Things Design and Implementation, ACM, New York, NY, USA (Apr. ٢٠١٧), pp. ١٧٣-١٧٨, ١٠,١١٤٥/٣٠٥٤٩٧٧,٣٠٥٥٠٠٣

[١٣] G. Sagirlar, B. Carminati, E. Ferrari, J.D. Sheehan, E. Ragnoli
Hybrid-IoT: hybrid blockchain architecture for internet of things - PoW sub-blockchains

۲۰۱۸ IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE (Jul. ۲۰۱۸), pp. ۱۰۰۷-۱۰۱٦, ۱۰,۱۱۰۹/Cybermatics_۲۰۱۸,۲۰۱۸,۰۰۱۸۹

[۱٤] A.F. Zorzo, H.C. Nunes, R.C. Lunardi, R.A. Michelin, S.S. Kanhere
Dependable IoT using blockchain-based technology
۲۰۱۸ Eighth Latin-American Symposium on Dependable Computing (LADC), IEEE (Oct. ۲۰۱۸), pp. ۱-۹, ۱۰,۱۱۰۹/LADC.۲۰۱۸,۰۰۰۱۰

[۱٥] A. Rejeb, J.G. Keogh, H. Treiblmaier
Leveraging the internet of things and blockchain technology in supply chain management
Future Internet, ۱۱ (۷) (Jul. ۲۰۱۹), p. ۱٦۱, ۱۰,۳۳۹۰/fi۱۱۰۷۰۱٦۱

[۱٦] T. Alam
Blockchain and its role in the internet of things (IoT)
٥ (۱) (۲۰۱۹), pp. ۱٥۱-۱٥۷, ۱۰,۳۲٦۲۸/CSEIT۱۹٥۱۳۷

[۱۷] L.T. Khrais
IoT and Blockchain in the Development of Smart Cities
(January, ۲۰۲۰), ۱۰,۱٤٥٦۹/IJACSA.۲۰۲۰,۰۱۱۰۲۲۰

[۱۸] D. Pavithran, K. Shaalan, J.N. Al-Karaki, A. Gawanmeh
Towards building a blockchain framework for IoT
Cluster Comput., ۲۳ (۳) (Sep. ۲۰۲۰), pp. ۲۰۸۹-۲۱۰۳, ۱۰,۱۰۰۷/s۱۰٥۸٦-۰۲۰-۰۳۰٥۹-٥

[۱۹] P. Hemalatha, S. Balaji, E. Chandru, P. Pradeep, D. Saravanan
Monitoring and securing the healthcare data harnessing IOT and blockchain technology
۱۲ (۲) (۲۰۲۱), pp. ۲٥٥٤-۲٥٦۱

[۲۰] E.A. Shammar, A.T. Zahary
A survey of IoT and blockchain integration : security perspective
IEEE Access, ۹ (۲۰۲۱), pp. ۱٥٦۱۱٤-۱٥٦۱٥۰, ۱۰,۱۱۰۹/ACCESS.۲۰۲۱,۳۱۲۹٦۹۷

[۲۱] M. Kumaresan, R. Gopal, M. Mathivanan, T. Poongodi
Amalgamation of blockchain, IoT, and ٥G to improve security and privacy of smart healthcare systems
Blockchain Applications for Healthcare Informatics, Elsevier (۲۰۲۲), pp. ۲۸۳-۳۱۲, ۱۰,۱۰۱٦/B۹۷۸-۰-۳۲۳-۹۰٦۱٥-۹,۰۰۰۱٥-۳

[۲۲] W. Alzuabi, Y. Ismail, W. Elmedany
Privacy and security issues in blockchain based IoT systems: challenges and opportunities
۲۰۲۲ International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (۳ICT), IEEE (Nov. ۲۰۲۲), pp. ۲٥۸-۲٦٥, ۱۰,۱۱۰۹/۳ICT٥٦٥۰۸,۲۰۲۲,۹۹۹۰٦۷۹

[۲۳] A.F. Santos, J. Marinho, J. Bernardino
Blockchain-based loyalty management system
Future Internet, ۱٥ (٥) (Apr. ۲۰۲۳), p. ۱٦۱, ۱۰,۳۳۹۰/fi۱٥۰٥۰۱٦۱

[۲٤] M. Sallal, R. de Fréin, A. Malik
PVPBC: privacy and verifiability preserving E-voting based on permissioned blockchain

Future Internet, ١٥ (٤) (Mar. ٢٠٢٣), p. ١٢١, ١٠,٣٣٩٠/fi١٥٠٤٠١٢١

[٢٥] T. Magara, Y. Zhou
Internet of things (IoT) of smart homes: privacy and security
Journal of Electrical and Computer Engineering, ٢٠٢٤ (Apr. ٢٠٢٤), pp. ١-١٧, ١٠,١١٥٥/٢٠٢٤/٧٧١٦٩٥٦

[٢٦] T. Wang, Q. Wu, J. Chen, F. Chen, D. Xie, H. Shen
Health data security sharing method based on hybrid blockchain
Future Generat. Comput. Syst., ١٥٣ (Apr. ٢٠٢٤), pp. ٢٥١-٢٦١, ١٠,١٠١٦/j.future.٢٠٢٣,١١,٠٣٢

٤- Conclusion

This article provides a comprehensive analysis of the application of blockchain for Internet of Things (IoT) systems and the various threats that impact the security and privacy of IoT data. It discusses the classification of different security threats in IoT and briefly reviews existing works that utilize blockchain for IoT security. Furthermore, the review focuses on the integration of blockchain with IoT, outlining the benefits, challenges, security techniques, and performance evaluation parameters. From this review, it can be inferred that blockchain technology is one of the promising technologies that can offer numerous advantages in terms of enhancing security and preserving the privacy of IoT data, thereby aiding the expansion of IoT for various applications. The identified issues indicate that the deployment of blockchain for IoT is still in its early stages, and there is an increasing demand for research efforts to address the challenges and complexities associated with the integration of blockchain with IoT. In this context, the review highlights some open issues and potential future research directions that could assist researchers intending to integrate blockchain and IoT.