DOR: 20.1001.1.2538161.1404.10.1.8.4

DOI: 10.22034/csj.2025.222121

بهار ۱۴۰۴، دوره ۱۰، شماره ۱، پیاپی ۳۶

دریافت مقاله: ۱۴۰۳/۰۸/۰۳

پذیرش مقاله: ۱۴۰۳/۱۱/۰۶

نوع مقاله: مروری

مروری بر ادغام زنجیرهٔ بلوکی و محاسبات لبه در اینترنت اشیاء

کیانوش بابادی*

گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی، واحد دزفول، ایران

پست الکترونیکی: kianoush.babadi@yahoo.com

حمید براتی

گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه آزاد اسلامی، واحد دزفول، ایران

پست الکترونیکی: hbarati@iaud.ac.ir

چکیده

سیستم‌های اینترنت اشیاء به طور گسترده در برنامه‌های کاربردی مختلف از جمله مراقبت‌های بهداشتی، کشاورزی، تولید و شهرهای هوشمند استفاده می‌شوند. با این حال، این سیستم‌ها همچنان دارای محدودیت‌هایی مانند عدم امنیت، تأخیر بالا، ناکارآمدی انرژی، ناکارآمدی استفاده از پهنای باند و با کمبود خودکارسازی مواجه هستند. ادغام محاسبات لبه و زنجیرهٔ بلوکی در اینترنت اشیاء برای رفع این محدودیت‌ها پیشنهاد شده است. با این حال، این ادغام با چالش‌هایی مواجه است که نیاز به بررسی‌های دقیق‌تر دارند. هدف این مقاله بررسی ادغام محاسبات لبه و زنجیرهٔ بلوکی در سیستم‌های اینترنت اشیاء است. به طور خاص، ابتدا یک نمای کلی از زنجیرهٔ بلوکی، محاسبات لبه و اینترنت اشیاء ارائه می‌دهیم. سپس یک معماری کلی از یک سیستم ادغام زنجیرهٔ بلوکی و محاسبات لبه در اینترنت اشیاء ارائه می‌کنیم و در ادامه به جنبه‌های ادغام و کاربردهای آن پرداخته می‌شود. علاوه بر این، این بررسی، بحث‌های جامعی در مورد چالش‌ها و بینش‌هایی در مورد جهت‌گیری آینده سیستم‌های اینترنت اشیاء لبه مبتنی بر زنجیرهٔ بلوکی ارائه می‌کند. هدف این بررسی این است که به عنوان یک نقطه ورود برای خوانندگان و محققان به جنبه‌های مختلف سیستم‌های اینترنت اشیاء لبه مبتنی بر زنجیرهٔ بلوکی عمل کند.

واژه‌های کلیدی: زنجیرهٔ بلوکی، امنیت، اینترنت اشیاء، محاسبات لبه، مدیریت داده

۱. مقدمه

در سال‌های اخیر، شاهد پیشرفت‌های سریع در اینترنت اشیاء[1] (IoT) بوده‌ایم که به دلیل گسترش دستگاه‌های تلفن همراه مانند گوشی‌های هوشمند، رایانه‌های قابل‌حمل، حسگرها، پوشیدنی‌ها و غیره صورت گرفته است. پیش‌بینی می‌شود که تا سال ۲۰۳۰، تعداد دستگاه‌های متصل اینترنت اشیاء از ۵۰۰ میلیون دستگاه فراتر رود. انتظار می‌رود این گسترش عظیم اینترنت اشیاء، برنامه‌ها و خدمات متعددی

1-Internet of Things

* نویسندهٔ مسئول

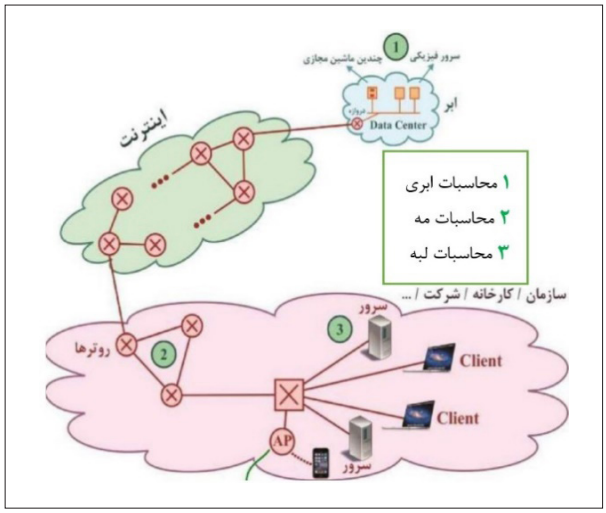
را در حوزه‌هـــای کاربردی مختلف، از صنعت ســـرگرمی گرفتـــه تا بازی‌های موبایل و نظـــارت [۱] ایجاد کند. چنین برنامه‌های IoT اغلب به منابع محاسباتی بالایی نیاز دارند تا داده‌های انبوه تولید شده از دستگاه‌های حسگر با الزامات تأخیر را برای ارائه خدمات مشتری حساس به زمان، مانند حمل‌ونقل و مراقبت‌های بهداشـــتی هوشمند، مدیریت کنند. رایانش ابری[۲] می‌تواند به دســـتگاه‌های اینترنت اشیاء در انجام وظایف محاســـباتی کمک کند، امـــا تأخیر انتقال بالا به دلیل فاصله زیاد از کاربران همچنان یک چالش اســـت. محاســـبات لبه[۳] اخیراً برای پشـــتیبانی از اینترنت اشیاء با ایجاد شـــبکه‌های لبه اشیاء[۴] (EoT)، با انتقال محاســـبات و ذخیره‌ســـازی به لبه شبکه، به عنوان مثال، نقاط دسترسی یا ایستگاه‌های پایه شبکه‌های دسترسی رادیویی پیشنهاد شـــده است. در این راســـتا، بار محاسباتی تحمیل شده بر حســـگرهای IoT با محدودیت منابع را می‌توان حذف کرد و ســـربار ارتباط به طور قابل توجهی کاهش می‌یابد و در عین حال تجربه محاســـباتی بهتری بـــرای کاربران فراهم می‌کنـــد. بنابرایـــن، EoT توانایی پشـــتیبانی از برنامه‌های کاربردی IoT توزیع‌شده آگاه از مکان را برای تسهیل ارائه خدمات حساس به زمان با کاهش پیچیدگی‌های محاسباتی دارد. ماهیـــت توزیع شـــده EoT چالش‌های امنیتی و حریم خصوصی جدیدی را معرفی می‌کند. مهاجرت سرویس‌های محاســـباتی و ذخیره‌سازی در مقیاس بزرگ به لبه، امکان تهدیـــدات امنیـــتی را ایجـــاد می‌کند و به کنترل شـــبکه یا جلوگیری از حملات به منابع در گره‌های لبه کمک می‌کند. علاوه بر این، بارگذاری داده‌ها در لبه شبکه نیز نگرانی‌های حیاتی در خصوص حریم خصـــوصی داده‌ها مانند نقض داده‌ها، حملات داده‌هـــا و تغییرات داده را افزایش می‌دهد. فناوری زنجیرهٔ بلوکی[۵] که در ســـال‌های اخیر ظهور کرده اســـت، به عنوان یک راه‌حل امیدوارکننده برای حل مسائل امنیتی و حریم خصوصی در شـــبکه‌های محاسباتی لبه و همچنین توانمندسازی نسل‌های بعدی فناوری EoT در نظر گرفته شده اســـت. به‌طور خاص، همگرایی زنجیرهٔ بلوکی و EoT یـــک چارچوب جدید به نام زنجیـــرهٔ بلوکی در لبه اینترنت اشیاء[۶] (BEoT) ایجاد می‌کند که شبکه‌های معمولی لبه اینترنت اشیـــاء را برای فعال کردن برنامه‌ها و خدمات صنعتی و مشتری جدید شـــکل و تغییر می‌دهد. به عنوان مثال، BEoT برای ارائه خدمات شـــهر هوشمند ایمن مانند مدیریت قابل اعتماد خـــودرو و کنترل ترافیک با تأخیر کم اســـتفاده شده است [۲]. علاوه بر این، BEoT تجزیه‌وتحلیل هوشمند مراقبت‌های بهداشـــتی و پردازش پزشکی IoT را به دلیل ویژگی‌های محاسباتی و ارتباطی در مقیاس بزرگ EoT و ویژگی‌های امنیتی زنجیرهٔ بلوکی ارتقا داده اســـت. همگرایی این فناوری‌های نوظهور به طور بالقوه یک عامل کلیدی برای خدمات و برنامه‌های کاربردی آینده است.

۲. مقدمات: محاســـبات لبه، محاســـبات مه و محاسبات ابری

از نظـــر برنامه‌های کاربردی اینترنت اشیاء حســـاس زمانی، کارسازهای ابری متمرکز که برای پردازش داده‌ها استفاده می‌شـــوند، ممکن اســـت به دلیل پاسخ دیرهنگام ناشی از انتقال حجم زیاد داده مناســـب نباشند. در عوض، برخی از بخش‌های داده را می‌توان به صورت توزیع‌شده در دســـتگاه‌های لبـــه و مه ذخیـــره و پـــردازش کرد، که می‌تواند به عنوان محاســـبات لبه و محاسبات مه[۷] در نظر گرفته شـــود. به ویژه، محاســـبات لبه [۳] و محاسبات مه [٤] با هدف تغییر محاســـبات از کارسازهای ابری متمرکز به منابع توزیع‌شـــده نزدیک‌تر به جایی کـــه داده‌ها گرفته می‌شـــود، می‌باشد. محاسبات لبه و مه شباهت‌های زیادی دارنـــد. به عنوان مثال، آن‌ها یـــک لایه میانی بین منبع داده و کارســـازهای ابری را فعال می‌کنند. این لایه قابلیت‌های آگاهی از موقعیت جغرافیایی و ذخیره‌ســـازی و محاسبات توزیع‌شـــده را ارائه می‌دهد. با این حـــال، این‌ها روش‌های

2-Cloud computing
3-Edge computing
4-Edge of Things
5-Blockchain
6-Blockchain Edge of Things
7-Fog computing

محاسباتی یکسان نیستند. جزئیات انواع محاسبات به شرح زیر ارائه شده است:



شکل ۱: لبه، ابر، مه: نگاهی کلی و دقیق‌تر

۱-۱- محاسبات لبه

همان‌طور که در شکل ۱ نشان داده شده است، محاسبات لبه نزدیک‌ترین لایه به منبعی است که داده‌ها در آن تولید می‌شوند. محاسبات لبه می‌تواند از دستگاه‌های لبه‌ای مختلف مانند دستگاه‌های پوشیدنی، دستگاه‌های محدود به منابع یا دروازه‌های لبه تشکیل شده باشد. محاسبات لبه خدمات مختلف لبه را فعال می‌کند، از جمله تجزیه‌وتحلیل بیدرنگ، ذخیره‌سازی توزیع‌شده، آگاهی از موقعیت مکانی، پشتیبانی از قابلیت همکاری، پشتیبانی جابه‌جایی، و هوش مصنوعی در لبه (edge-AI)[8]، که به افزایش قابل‌توجه کیفیت خدمات، کمک می‌کند [۵]. محاسبات لبه همچنین سطوح امنیتی و کارایی انرژی را با رمزگذاری داده‌های ارسال شده از طریق شبکه و بارگیری وظایف محاسباتی سنگین به دستگاه‌های قدرتمندتر افزایش می‌دهد.

محاسبات لبه را می‌توان بر اساس الگوهای معماری، مدل‌های استقرار یا استفاده خاص دسته‌بندی کرد. محاسبات لبه با دسترسی چندگانه (MEC)[9]، که یک نوع محاسبات لبه است که به طور خاص برای کار با شبکه‌های سلولی طراحی شده است [٦]. MEC ایستگاه‌های پایه توزیع‌شده را برای محاسبات لبه مستقر می‌کند و از آنها استفاده می‌کند. یکی دیگر از انواع محاسبات لبه، ابرهای کوچک هستند که از مراکز داده کوچک تشکیل شده‌اند که در لبه یک شبکه قرار گرفته‌اند. نوع دیگر، محاسبات لبه‌های صنعتی است که شامل دستگاه‌های لبه‌ای است که برای برآوردن استانداردها و الزامات صنعتی مانند استحکام، قابلیت اطمینان، مقیاس‌پذیری، تحمل دما، امنیت و پشتیبانی از پروتکل‌های ارتباطی صنعتی مشخص شده‌اند.

۱-۲- محاسبات مه

محاسبات مه، همان‌طور که در شکل ۱ نشان داده شده است، برای اولین بار توسط سیسکو در سال ۲۰۱۲ به عنوان یک الگوی محاسباتی لایه میانی معرفی شد که قابلیت‌های محاسبات ابری را به لبه شبکه نزدیک می‌کند. این نه تنها قابلیت‌های محاسباتی بلکه شبکه، ذخیره‌سازی و سایر خدمات را نیز در بر می‌گیرد. اجزای شبکه در محاسبات مه با مدیریت منابع شبکه و پشتیبانی از تحرک و همچنین آگاهی از موقعیت چندین گره مه توزیع‌شده در مناطق، به پوشش جغرافیایی و مسائل تأخیر بالا می‌پردازند. برای ارائه این خدمات، محاسبات مه مکان‌های فیزیکی دستگاه‌های متصل و امکان جابه‌جایی این دستگاه‌ها از محدوده پوشش یا از یک منطقه تحت پوشش به منطقه دیگر را تخمین زده یا ردیابی می‌کند. اجزایی مانند مسیریاب‌ها، نقاط دسترسی، سوئیچ‌ها یا ایستگاه‌های پایه می‌توانند لایه مه را تشکیل دهند [۷]. بسته به کاربرد، تعداد دستگاه‌های مه می‌تواند متفاوت باشد و هم‌بندی شبکه این دستگاه‌ها ممکن است متفاوت باشد. علاوه بر این، لایه مه شامل کارسازهایی است که داده‌های موقتی را ذخیره می‌کنند که می‌توانند پس از مدتی پاک شوند. در مقایسه با محاسبات لبه، مه اغلب از دستگاه‌ها و کارسازهای مرتبط با شبکه قوی‌تر از دستگاه‌هایی که در لبه استفاده می‌شوند تشکیل شده است. بنابراین، لایه مه می‌تواند تخصیص منابع تحلیلی و پویای

8-Artificial Intelligence at the Edge
9-Multi- access Edge Computing

پیشـــرفته‌تری را انجام دهد. محاسبات مه غالباً شبکه‌های بزرگ‌تر را پوشش می‌دهد، مانند شبکه‌های چند ساختمان که ده‌ها یا صدها دستگاه دارند، در حالی که محاسبات لبه اغلب به شبکه‌های کوچک‌تر، مانند چندین دستگاه پوشیدنی یا دســـتگاه‌های اینترنت اشیاء در یک خانه هوشمند اشاره دارد. بر این اســـاس، مقدار داده در مه اغلب بسیار بیشتر از داده‌های جمع‌آوری شـــده در دســـتگاه‌های لبه اســـت. محاسبات مه مخصوصاً در شـــرایطی که حجم زیادی از داده‌ها از طریق شـــبکه منتقل می‌شود و منابع زیادی برای حفظ کیفیت ارتباط مورد نیاز است اهمیت دارد [۷]. اگرچه دستگاه‌های مه قوی هستند، اما همه وظایف را نمی‌توان در مه پردازش کرد، مانند کارهای محاسباتی سنگین. بنابراین، تعیین این که کدام وظایف باید در مه انجام شود و کدامیک بایـــد در لایه‌های بعدی مانند کارســـازهای ابری پردازش شـــوند، برای دســـتیابی به راندمان انرژی بالا و تأخیر کم بسیار مهم است.

۱-۳- محاسبات ابری

در شکل ۱، ابر به عنوان دورترین لایه ارائه شده است کـــه بسیاری از خدمات پیشـــرفته از جمله زیرســـاخت به عنوان خدمت (IaaS)[10]، بُن‌سازه به عنوان خدمت (PaaS)[11]، بدون کارساز و نرم‌افزار به عنوان خدمت (SaaS)[12] را ارائه می‌دهد. محاسبات ابری ظرفیت قوی، فضای ذخیره‌سازی جهانی و مقیاس‌پذیری را فراهم می‌کند و آن را به یک الگوی ایده‌آل برای بســـیاری از برنامه‌ها تبدیـــل می‌کند. یکی از مزایای اصلی محاسبات ابری، توانایی آن در پشتیبان‌گیری از داده‌ها در مکان‌های مختلف ذخیره‌سازی خارج از پایگاه، تضمیـــن بازیابی اطلاعـــات پس از خرابی ســـخت‌افزار یا نرم‌افزار است. محاسبات ابری همچنین دسترسی آسان به داده‌ها را از هر مکان یا دســـتگاهی فراهم می‌کند. علاوه بر این، خدمات ابری را می‌توان برای برآورده کردن نیازهای متغیر محاسباتی، ذخیره‌سازی یا پهنای باند شبکه، به‌طور منعطف کوچک یا بزرگ کرد. با این حال، این لایه همچنان دارای معایب بسیاری اســـت، مانند خطرات امنیتی، تأخیر بالا و یک نقطه شکســـت. کارسازهای ابری معمولاً در یک مکان متمرکز هستند، از نظر جغرافیایی دور از دستگاه‌های اینترنت اشیاء. در نتیجه، ارسال یا درخواست داده می‌تواند تأخیر زیادی داشـــته باشـــد. هنگامی که هـــزاران یا حتی میلیون‌ها دســـتگاه جغرافیایی توزیع شده در شبکه وجود دارد، این مشـــکل تأخیر بدتر می‌شود. علاوه بر این، انتقال از راه دور نیـــز بر محرمانه بودن داده‌ها تأثیر می‌گذارد و خطر از دست دادن یا نشت داده‌ها را افزایش می‌دهد [۸].

جـــدول ۱ انـــواع مختلف محاســـبات مانند لبـــه، مه و محاســـبات ابری را خلاصه می‌کند. در حالی که محاسبات ابری جدا از بقیه اســـت، انواع دیگر محاسبات شباهت‌های زیادی دارند، مانند ذخیره‌ســـازی داده‌های توزیع شـــده و محاســـبات، پشـــتیبانی از تحرک و آگاهی از موقعیت. این روش‌های محاســـباتی با حفظ پهنای باند شـــبکه، کاهش تأخیـــر و ارائه تحمل خطا بـــه افزایش کیفیت خدمات کمک می‌کنند.

۲. اینترنت اشیاء

اینترنت اشیاء شـــبکه‌ای از اشیاء و حسگرهای فیزیکی است که داده‌ها را از طریق اینترنت جمع‌آوری، به اشتراک گذاشـــته و انتقال می‌دهد. به عنوان مثـــال، می‌توان از یک دســـتگاه هوشـــمند برای اندازه‌گیری و تنظیـــم گرمایش داخل یک اتاق یا ســـاختمان استفاده کرد. این دستگاه‌های هوشـــمند را می‌توان از راه دور با اســـتفاده از یک برنامه گوشی هوشـــمند کنترل کرد. اینترنـــت اشیاء یک محیط به هم پیوسته را از طریق تولید و به اشتراک‌گذاری اطلاعات بیدرنگ بدون دخالت انسان امکان‌پذیر می‌کند. این می‌تواند برای افراد و کســـب و کارها بـــرای تصمیم‌گیری آگاهانه بهتر مفید باشد. دستگاه‌های اینترنت اشیاء مانند حسگرها، میکروکنترلرها، محرک‌ها و دستگاه‌های ارتباطی داده‌ها را از محیـــط عملیاتی محلی خود جمع‌آوری می‌کنند. ســـپس

10-Infrastructure-as-a-Service
11-Platform-as-a-Service
12-Software-as-a-Service

جدول ۱: مقایسه ویژگی‌های مختلف محاسبات لبه، مه و ابر

الگوها	محاسبات لبه با دسترسی چندگانه[۶]	لبه [۳]	مه [۴]	ابر [۸]
توزیع	توزیع‌شده	توزیع‌شده	توزیع‌شده	متمرکز
فاصله تا داده	نزدیک	نزدیک	نسبتاً نزدیک	دور
ظرفیت ذخیره سازی	کم	کم	کم	بالا
نگهداری داده‌ها	گذرا	گذرا	گذرا	دائمی
خدمت	محلی	محلی	محلی	جهانی
تأخیر در ارتباط	کم	کم	کم	زیاد
تحرک	پشتیبانی می‌شود	پشتیبانی می‌شود	پشتیبانی می‌شود	محدود
کاربرد بیدرنگ	پشتیبانی می‌شود	پشتیبانی می‌شود	پشتیبانی می‌شود	پشتیبانی نمی‌شود
آگاهی از موقعیت مکانی	پشتیبانی می‌شود	پشتیبانی می‌شود	پشتیبانی می‌شود	پشتیبانی نمی‌شود
امنیت	بیشتر	بیشتر	بهتر به دلیل پردازش محلی	آسیب‌پذیر به دلیل انتقال داده
مقیاس‌پذیری	کم	کم	محدود به دستگاه‌های محلی	بسیار بالا

داده‌ها برای پردازش، تجزیه‌وتحلیل، تصمیم‌گیری و تجزیه‌وتحلیل بیشتر به حافظه خارجی مانند ابر فرستاده می‌شود.

دستگاه‌ها و حسگرهای IoT با فناوری پیشرفته مزایای مختلفی را در حوزه‌های مختلف از جمله بهبود تصمیم‌گیری، تجربه کاربر، کارایی و کاهش هزینه ارائه می‌کنند. ما می‌توانیم وظایف و فرآیندها را برای افزایش کارایی و به حداقل رساندن دخالت انسان در حوزه‌های مختلف به صورت خودکار انجام دهیم. علاوه بر این مزایا، اینترنت اشیاء با چالش‌های زیادی از جمله امنیت، قابلیت همکاری، حریم خصوصی، مدیریت داده‌ها و مقیاس‌پذیری مواجه است [۹]. فقدان استانداردسازی و تنوع پروتکل‌های ارتباطی در محیط اینترنت اشیاء منجر به مشکلات قابلیت همکاری می‌شود. ذخیره‌سازی، انتقال و پردازش ایمن حجم عظیمی از داده‌های تولید شده توسط دستگاه‌های IoT نیز به یک چالش واقعی تبدیل شده است.

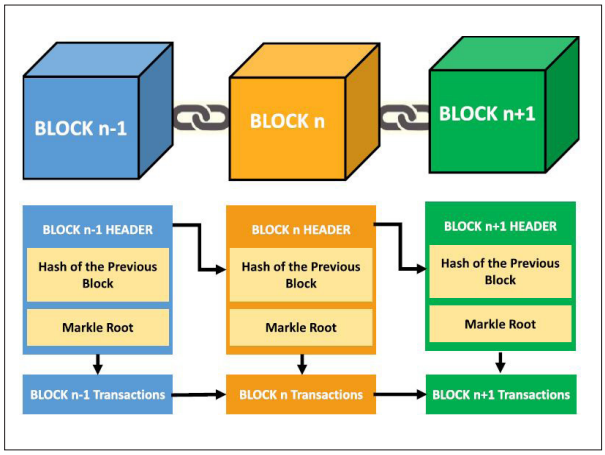
۳. زنجیرۀ بلوکی

زنجیرۀ بلوکی یک فناوری برای ثبت و ضبط داده‌ها به صورت غیرمتمرکز به حساب می‌آید. در این بخش ابتدا مروری بر زنجیرۀ بلوکی و ویژگی‌های آن پرداخته و سپس دو نمونه از بُن‌سازه‌های معروف آن شرح داده شده است.

۳-۱- مروری بر فناوری زنجیرۀ بلوکی

زنجیرۀ بلوکی یک روش غیرمتمرکز برای ثبت اطلاعات به‌صورت دائمی و سازمان‌دهی شده است، به طوری که هر کسی در اینترنت می‌تواند کل تاریخچه اطلاعات را در یک مجموعه داده مشخص ببیند، بنابراین امکان دسترسی به اطلاعات در هر نقطه از جهان را فراهم می‌کند. در اصل، زنجیرۀ بلوکی یک دفتر کل دیجیتال از تمام تراکنش‌ها است. زنجیرۀ بلوکی به طور مداوم در حال رشد است، زیرا بلوک‌های جدید تکمیل شده با دنباله جدیدی از تراکنش‌ها اضافه می‌شوند. هر بلوک جدید حداقل حاوی چکیدۀ رمزنگاری بلوک قبلی و همچنین داده‌های مربوط به تراکنش است، همان‌طور که در شکل ۲ نشان داده شده است. بلوک اولیه یک زنجیرۀ بلوکی اغلب به عنوان یک بلوک پیدایش تعیین می‌شود. یک بلوک جدید ایجاد شده به

زنجیرهٔ بلوکی اضافه می‌شود و هرگز قابل تغییر یا حذف نیست. این به این دلیل است که هر بلوک در یک زنجیرهٔ بلوکی شامل یک چکیدهٔ رمزنگاری از بلوک قبلی و همچنین یک مهر زمانی است. تغییر هرگونه اطلاعات در یک بلوک باعث تغییر چکیده می‌شود که همه بلوک‌های بعدی را باطل می‌کند. ما خوانندگان را به خواندن [۱۰] در مورد جزئیات فنی در بلوک چین توصیه می‌کنیم. سه ویژگی مهم زنجیرهٔ بلوکی عبارتند از:



شکل ۲: ساختار زنجیرهٔ بلوکی [۱۱]

- غیرمتمرکز: برخلاف سیستم‌های سنتی، زنجیرهٔ بلوکی غیرمتمرکز است. هیچ مرجع مرکزی وجود ندارد و کنترل در سراسر گره‌های شبکه توزیع می‌شود.
- امنیت: زنجیرهٔ بلوکی یک مفهوم بسیار امن است که مبتنی بر رمزنگاری و سازوکارهای اجماع است. این بدان معناست که وقتی داده‌ها در زنجیرهٔ بلوکی ذخیره می‌شوند، نمی‌توان آن‌ها را به طور مخرب تغییر داد.
- شفافیت: زنجیرهٔ بلوکی نیز یک فناوری شفاف است، زیرا داده‌های تراکنش در دسترس عموم است و به راحتی قابل تأیید است.
- زنجیرهٔ بلوکی را می‌توان به سه دسته کلی تقسیم کرد: عمومی، خصوصی و ترکیبی. زنجیرهٔ بلوکی عمومی، به هر کسی اجازه می‌دهد به شبکه زنجیرهٔ بلوکی بپیوندد و به آن دسترسی پیدا کند. یک زنجیرهٔ بلوکی خصوصی، تنها به نهادها و سازمان‌های شرکت‌کننده اجازه دسترسی و انجام تراکنش‌ها در شبکه زنجیرهٔ بلوکی را می‌دهد. زنجیرهٔ بلوکی خصوصی برای سازمان‌هایی در نظر گرفته شده است که حفظ حریم خصوصی یک نیاز اصلی است. در یک زنجیرهٔ بلوکی ترکیبی، یک زنجیره مجزا برای زنجیره‌های بلوکی عمومی و خصوصی حفظ می‌شود. زنجیرهٔ بلوکی از اجزای کلیدی زیر تشکیل شده است:
- تراکنش‌ها: تراکنش‌ها عملیاتی هستند که بر روی وضعیت فعلی زنجیرهٔ بلوکی انجام می‌شوند.
- بلوک‌ها: تراکنش‌ها در بلوک‌ها گروه‌بندی می‌شوند و سپس به زنجیرهٔ بلوکی اضافه می‌شوند. هر بلوک از نظر رمزنگاری به بلوک قبلی متصل می‌شود، بنابراین یک زنجیره ناگسستنی از بلوک‌ها ایجاد می‌شود.
- گره‌ها: کاربران و سازمان‌ها از طریق گره‌ها در یک شبکه زنجیرهٔ بلوکی شرکت می‌کنند. تراکنش‌ها نیز از طریق گره‌ها آغاز و پردازش می‌شوند. یک نسخه از زنجیرهٔ بلوکی توسط گره‌های سازمان نگهداری می‌شود.
- رمزنگاری: امنیت و تغییرناپذیری شبکه‌های زنجیرهٔ بلوکی از طریق روش‌های اولیه رمزنگاری مختلف، به‌عنوان مثال، امضای دیجیتال، رمزگذاری و چکیده به‌دست می‌آید.
- سازوکار اجماع: به مجموعه‌ای از الگوریتم‌ها و فرآیندهایی اطلاق می‌شود که برای تأمین توافق و هم‌راستایی در شبکه‌های توزیع‌شده مانند زنجیرهٔ بلوکی استفاده می‌شوند. هدف اصلی این سازوکارها این است که تمام گره‌های شبکه بتوانند بدون نیاز به مرجع مرکزی به یک توافق مشترک در مورد وضعیت فعلی شبکه برسند. در شبکه‌های زنجیرهٔ بلوکی، معمولاً تعداد زیادی گره وجود دارد که باید در مورد صحت تراکنش‌ها یا بلوک‌های جدید اجماع کنند. این سازوکارها نقش مهمی در جلوگیری از تقلب، حملات و خطاهای سیستم دارند و از آن‌ها برای تأمین امنیت شبکه استفاده می‌شود. انواع مختلفی از

سازوکارهای اجماع وجود دارد که در اینجا به چند مورد از آن‌ها اشاره می‌شود:

۱. اثبات کار (PoW): در این سازوکار، گره‌ها باید مسائل پیچیده ریاضی را حل کنند تا یک بلوک جدید به زنجیره اضافه شود. اولین گرهی که این مسئله را حل کند، حق اضافه کردن بلوک را به دست می‌آورد و پاداش دریافت می‌کند. این سازوکار در زنجیرهٔ بلوکی بیت‌کوین استفاده می‌شود.

مزایای اثبات کار

- امنیت بالا: PoW یکی از امن‌ترین سازوکارهای اجماع است، زیرا حمله به شبکه نیاز به قدرت محاسباتی زیادی دارد. برای تغییر اطلاعات یک بلوک، حمله‌کننده باید بیش از ۵۰ درصد از توان محاسباتی شبکه را در اختیار داشته باشد که بسیار هزینه‌بر و دشوار است.
- تمرکززدایی: PoW باعث می‌شود که شبکه به طور غیرمتمرکز و بدون نیاز به اعتماد به یک نهاد مرکزی عمل کند. همه گره‌ها به طور مستقل در اجماع شرکت می‌کنند.
- ساده‌فهم و معتبر: مفهوم و عملکرد PoW نسبتاً ساده و به‌طور گسترده‌ای در پروژه‌های مختلف (مانند بیت‌کوین) ثابت شده است.
- پشتیبانی از زنجیره‌های بلوکی عمومی: به ویژه برای زنجیره‌های بلوکی عمومی مناسب است که نیاز به امنیت و اعتبارسنجی از سوی تعداد زیادی از شرکت‌کنندگان دارند.

معایب سازوکار اثبات کار

- مصرف بالای انرژی: یکی از بزرگ‌ترین مشکلات PoW، مصرف انرژی بسیار زیاد است. حل مسائل پیچیده ریاضی برای استخراج بلوک‌ها به منابع انرژی قابل‌توجهی نیاز دارد که موجب نگرانی‌های زیست‌محیطی می‌شود.
- تمرکز در استخراج: با گذشت زمان، استخراج‌کنندگان به دستگاه‌های قدرتمندتر و هزینه‌بر نیاز دارند. این امر می‌تواند منجر به تمرکز استخراج در دست تعداد کمی از استخراج‌کنندگان و شرکت‌ها شود که از نظر اصولی با هدف تمرکززدایی در تضاد است.
- مقیاس‌پذیری محدود: فرآیند اجماع در PoW زمان‌بر است و تعداد تراکنش‌هایی که می‌توانند در هر ثانیه پردازش شوند، محدود است. این می‌تواند در شبکه‌های بزرگ باعث افزایش زمان تایید و کارمزدهای بالاتر شود.
- هزینه‌های بالای راه‌اندازی: برای شرکت در فرآیند PoW، ماینرها به تجهیزات گران‌قیمت (مانند دستگاه‌های ASIC) و برق زیاد نیاز دارند که هزینه‌های اولیه و عملیاتی بالایی ایجاد می‌کند.

۲. اثبات سهام (PoS): در این سازوکار، گره‌ها با گذاشتن سرمایه (استیکینگ) در شبکه می‌توانند شانس انتخاب برای اضافه کردن بلوک جدید را به‌دست آورند. هرچه مقدار بیشتری از ارز در اختیار گره باشد، احتمال انتخاب آن گره برای تایید بلوک بیشتر می‌شود. این سازوکار نسبت به PoW از نظر مصرف انرژی بهینه‌تر است و در زنجیره‌های بلوکی مانند اتریوم ۲/۰ استفاده می‌شود.

مزایای اثبات سهام

- مصرف انرژی کمتر: در مقایسه با اثبات کار، اثبات سهام انرژی بسیار کمتری مصرف می‌کند. چون در این سیستم نیازی به حل مسائل پیچیده ریاضی توسط استخراج‌کنندگان نیست و به‌جای آن از فرآیند انتخابی برای تایید تراکنش‌ها استفاده می‌شود.
- مقیاس‌پذیری بهتر: PoS می‌تواند تعداد بیشتری از تراکنش‌ها را در واحد زمان پردازش کند زیرا نیازی به عملیات پیچیده محاسباتی ندارد و در نتیجه زمان تایید بلوک‌ها کاهش می‌یابد.
- هزینه پایین‌تر: در PoS، نیازی به سخت‌افزارهای گران‌قیمت و مصرف بالای انرژی نیست. تنها کافی است که کاربران ارزهای دیجیتال خود را در شبکه به

اشتراک بگذارند (استیک کنند) تا بتوانند در فرآیند اجماع مشارکت کنند.

- تمرکززدایی بیشتر: PoS باعث می‌شود که فرآیند اجماع در دست افرادی با دارایی‌های زیاد نباشد. در این سازوکار، هر کسی که مقدار مناسبی از ارز را به اشتراک گذاشته باشد، می‌تواند شانس تایید تراکنش‌ها را داشته باشد.
- معایب اثبات سهام:
- مشکل «نیاز به خوابیدن»: برای مشارکت در PoS، باید مقدار معینی از ارز دیجیتال خود را به‌عنوان «ذخیره» در شبکه قفل کنید. این موضوع ممکن است برای برخی کاربران مشکل ایجاد کند زیرا نمی‌توانند به سرعت به دارایی‌های خود دسترسی داشته باشند یا آن‌ها را جابجا کنند.
- پیچیدگی در طراحی و پیاده‌سازی: برخلاف PoW که سازوکار ساده‌ای دارد، طراحی و پیاده‌سازی PoS پیچیده‌تر است. نیاز به الگوریتم‌هایی برای انتخاب بلوک‌ساز و جلوگیری از حملات مختلف می‌تواند طراحی را پیچیده‌تر کند.
- گرایش به تمرکز قدرت: با گذشت زمان، ذخیره کردن ممکن است به‌طور تدریجی به افرادی که قدرت مالی بیشتری دارند منتقل شود، که باعث می‌شود غول‌های اقتصادی و نهادهای مالی قادر به کنترل شبکه شوند و از تمرکززدایی که هدف اصلی زنجیرۀ بلوکی است، کاسته شود.

۳. اثبات تاریخچه: در این سازوکار، زمان وقوع هر رویداد یا تراکنش ثبت و غیرقابل تغییر می‌شود. این روش به‌ویژه در شبکه‌های مبتنی بر زنجیره‌های بلوکی سریع مانند Solana به کار می‌رود.

٤. اثبات ظرفیت: در این سازوکار، گره‌ها از فضای دیسک سخت خود برای ذخیره‌سازی داده‌ها و حل مسائل استفاده می‌کنند. به هر میزان که فضای بیشتری اختصاص دهند، شانس آن‌ها برای تایید بلوک بیشتر می‌شود.

۵. اثبات اعتبار: در این سازوکار، گره‌هایی که شناخته شده و مورد اعتماد هستند، مسئول تایید تراکنش‌ها و بلوک‌ها هستند. این سازوکار به‌ویژه در شبکه‌های خصوصی و کنسرسیوم‌ها مورد استفاده قرار می‌گیرد.

۴- بُن‌سازه‌های زنجیرۀ بلوکی

اولین بُن‌سازه زنجیرۀ بلوکی، بیت‌کوین برای اهداف مالی با چالش‌های مختلفی مانند سرعت و مصرف انرژی معرفی شد. با توجه به ماهیت مالی بیت‌کوین و چالش‌های مختلف، بسیاری از بُن‌سازه‌های جدید برای پاسخگویی به نیازهای متنوع صنعت در حال رشد زنجیرۀ بلوکی معرفی شده‌اند. در زیر دو تا از بُن‌سازه‌های زنجیرۀ بلوکی معرفی شده است.

- بیت‌کوین: بیت‌کوین پیشگام و یکی از پیشروترین بُن‌سازه‌های زنجیرۀ بلوکی عمومی ارزهای دیجیتال است. بیت‌کوین بر اساس سازوکار اجماع اثبات کار [۱۲] است، که در آن استخراج‌کنندگان برای حل یک معمای رمزنگاری برای تولید بلوک‌های جدید و تأیید تراکنش‌ها با هم رقابت می‌کنند. با توجه به ظهور سازوکارهای اجماع کارآمد جدید، PoW اکنون یک سازوکار محاسباتی و انرژی‌بر در نظر گرفته می‌شود.

کاربردهای خاص بیت‌کوین

حفظ ارزش در کشورهای با تورم بالا، پول دیجیتال در مناطق فاقد دسترسی به بانک، پرداخت‌های بین‌المللی سریع و ارزان و گسترش نوآوری‌های مالی.

چالش‌های بیت‌کوین

نوسانات شدید قیمت، محدودیت مقیاس‌پذیری، مصرف انرژی بالا، محدودیت‌های قانونی و نظارتی و مسائل مربوط به کارمزد تراکنش.

- اتریوم: اتریوم دومین بُن‌سازه عمومی زنجیرۀ بلوکی مبتنی بر ارزهای دیجیتال شناخته شده است. اتریوم یک زنجیرۀ بلوکی عمومی غیرمتمرکز است که از برنامه‌های

کاربـــردی توزیع‌شـــده برای بـــه اشـــتراک‌گذاری امن و دسترســـی به اطلاعات در سراسر جهان پشتیبانی می‌کند. اتریوم در ابتدا بر اساس الگوریتم اجماع PoW بود. اخیراً، اتریوم برای محاســـبات و انرژی کارآمدتر به ســـازوکار اجماع اثبات ســـهام تغییر کرده اســـت. در اجماع PoS، به جای حل معماهـــای رمزنگاری، بلوک‌های جدید توســـط اعتبارسنجی‌هایی با سهام بالا در شبکه تولید می‌شوند.

کاربردهای خاص اتریوم

قراردادهـــای هوشـــمند، بن‌ســـازه بـــرای برنامه‌های غیرمتمرکز، محیط ایجاد و تست پروژه‌های زنجیرۀ بلوکی و حاکمیت غیرمتمرکز.

چالش‌های اتریوم

هزینه‌هـــای بالای گاز، مشـــکلات امنیـــتی و حفره‌های قراردادهـــا، مقیاس‌پذیری محدود، محدودیت‌های قانونی و نظارتی.

۵. ادغام زنجیرۀ بلوکی و محاسبات لبه (IBEC)[۱۳]

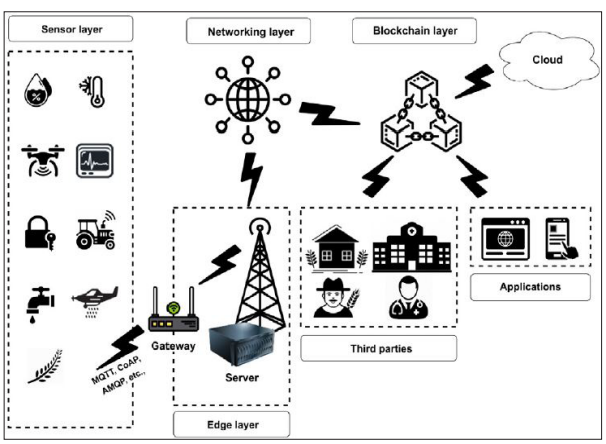
چارچوب‌هایی کـــه زنجیرۀ بلوکی و محاســـبات لبه را ادغام می‌کنند در بسیاری از سناریوهای اینترنت اشیاء مانند اینترنت وســـایل نقلیه (IoV)[۱۴]، شـــبکه هوشمند[۱۵] و اینترنت اشیاء صنعتی (IIoT)[۱۶] اعمال شـــده اســـت [۱۳]. هنگامی که زنجیرۀ بلوکی با محاســـبات لبه ملاقات می‌کند، حفظ حریم خصوصی، تغییرناپذیری و قابلیـــت ردیابی زنجیرۀ بلوکی می‌تواند برای بهبود امنیت محاســـبات لبه در اینترنت اشیاء مورد اســـتفاده قرار گیرد. از ســـوی دیگر، محاسبات لبه را می‌توان بـــرای ارائه مقادیر زیـــادی از منابع برای عملکرد بـــا کارایی بالای زنجیرۀ بلـــوکی مورد اســـتفاده قرار داد. انگیزه‌های ترکیب این دو فناوری به شرح زیر است:

- غنی‌سازی منابع: کاربردهای زنجیرۀ بلوکی در بسیاری از سناریوهای اینترنت اشیاء (مانند اشتراک‌گذاری داده‌ها و مدیریت منابع) به دســـتگاه‌های مستقر در اینترنت اشیاء برای اجرای الگوریتم‌های اجماع، پخش یا تأیید تراکنش‌ها و ثبت تراکنش‌های تاریخی روی زنجیرۀ بلوکی نیاز دارد. این یک چالش برای دســـتگاه‌های اینترنت اشـــیاء با منابع محدود است. محاســـبات لبه می‌تواند منابع ذخیره‌سازی، محاسباتی و ارتباطی غنی را برای دستگاه‌های لبه در این سناریوها فراهم کند.
- تضمیـــن امنیت و حریم خصوصی: در محاســـبات لبه، هم‌بندی پویا شـــبکه‌ها و تحرک و ناهمگنی دســـتگاه‌های لبه منجر بـــه چالش‌های امنیتی می‌شـــود. زنجیرۀ بلوکی می‌تواند نه تنها برای اطمینان از سازگاری، ردیابی و ضد دستکاری داده‌ها، بلکه برای محافظت از حریم خصوصی داده‌ها اســـتفاده شـــود. به عنوان مثال، با تأثیر سازوکار اجماع در زنجیرۀ بلوکی، شرکت‌کنندگان می‌توانند به طور مشترک امنیت داده‌ها را حفظ کنند. علاوه بر این، معماری غیرمتمرکـــز آن مبتنی بر شـــبکه همتا به همتـــا (P2P) با معماری محاسبات لبه در اینترنت اشیاء مطابقت دارد.
- افزایش مقیاس‌پذیری: IBEC، دســـتگاه‌های لبه محدود با منابع را قادر می‌ســـازد تا برای پردازش وظایف کارآمد و حفظ زنجیرۀ بلوکی با سازوکارهای طراحی خاص در آن شرکت کنند. در واقع، حتی دســـتگاه‌های لبه با محدودیت منابع نیز می‌توانند در وظایف اســـتخراج شـــرکت کنند. به عنوان مثال، دستگاه‌های لبه محدود شده با منابع می‌توانند داده‌های جمع‌آوری شده را برای به دست آوردن بازده با یک سازوکار انگیزشی مؤثر در زنجیرۀ بلوکی به اشتراک بگذارند. بر این اساس، IBEC مقیاس‌پذیری و انعطاف‌پذیری کل سیستم را بهبود می‌بخشد.
- معماری IBEC در شـــکل ۳ نشان داده شده است. در این معماری، انواع دســـتگاه‌های لبه بـــا منابع محدود از طریق راه‌های دسترســـی مختلف، مانند 5G، Wi-Fi و بلوتوث به شبکه لبه متصل می‌شوند. با توجه به مناطق مختلف، انواع مختلفی از دســـتگاه‌های لبه وجود دارد. به عنوان مثال، در حوزه اینترنت وسایل نقلیه، دستگاه‌های لبه شامل وسایل

13-Integration of Blockchain and Edge Computing
14-Internet of Vehicles
15-Smart Grid
16-Industrial Internet of Things

نقلیه هوشمند، دوربین‌های نظارتی، چراغ‌های راهنمایی و غیره است. زنجیرهٔ بلوکی محلی، که معمولاً زنجیرهٔ بلوکی مجاز یا زنجیرهٔ بلوکی خصوصی است، همیشه در لایه لبه مستقر می‌شود تا به مدیریت داده‌ها از دستگاه‌های لبه کمک کند. کارسازهای لبه به طورکلی به عنوان گره‌های زنجیرهٔ بلوکی و ماینرهای دستگاه‌های لبه‌ای عمل می‌کنند، زیرا نگهداری زنجیره‌های بلوکی به منابع ذخیره‌سازی، محاسبات و شبکه کافی نیاز دارد. به عنوان مثال، در سناریوی تجارت انرژی شبکه هوشمند، کارسازهای لبه مسئول اجرای قراردادهای هوشمند برای متقاضیان تجارت انرژی هستند. در بالای معماری، ابر قرار دارد که برای مقابله با برخی از وظایف بسیار پیچیده که کارسازهای لبه نمی‌توانند انجام دهند، استفاده می‌شود. زنجیرهٔ بلوکی جهانی که معمولاً زنجیرهٔ بلوکی عمومی است، همیشه در لایه ابری مستقر می‌شود تا در صورت لزوم نشانی‌های ذخیره‌سازی داده‌ها را مدیریت کند. به عنوان مثال، برخی از داده‌های خام با سربار ذخیره‌سازی بالا (به عنوان مثال، تصویر اشعه ایکس در مراقبت‌های بهداشتی) را می‌توان در برخی از مراکز داده توزیع‌شده ذخیره کرد، در حالی که اَبَر داده‌های آنها در زنجیرهٔ بلوکی جهانی ذخیره می‌شود.

ویژگی‌ها و مزایای بالا چارچوب IBEC را قادر می‌سازد تا برنامه‌های کاربردی بیشتری را در اینترنت اشیاء، از جمله مدیریت داده/ دانش، امنیت و حریم خصوصی، ارتباطات قابل‌اعتماد و سایر برنامه‌ها گسترش دهد.



شکل ۳: یک معماری کلی ادغام زنجیرهٔ بلوکی و سیستم‌های محاسباتی [۱۳]

۶- IBEC برای مدیریت داده/ دانش

مدیریت داده‌ها بر ذخیره‌سازی، دسترسی، اشتراک‌گذاری و ردیابی ایمن و کارآمد داده‌های تولید شده از محیط اینترنت اشیاء دارای محاسبات لبه فعال تمرکز دارد. زنجیرهٔ بلوکی می‌تواند یک محیط غیرمتمرکز و بدون شخص‌ثالث در محاسبات لبه بر اساس ویژگی‌های شبکه P2P زیربنایی فراهم کند. بر این اساس، غیرمتمرکز و خودسازماندهی یک سیستم مدیریت داده را می‌توان با استفاده از زنجیرهٔ بلوکی تضمین کرد.

ذخیره‌سازی امن داده‌های اینترنت اشیاء یکی از محتویات تحقیقاتی مدیریت داده است. هدف کارهای موجود به ترتیب یکپارچگی، ناشناس بودن و وفق‌پذیری [۱۴]، قابلیت اطمینان و یکپارچگی داده [۱۵]، و ناشناس بودن داده‌ها [۱۶] است.

در [۱۴]، مسائل ذخیره‌سازی امن یکپارچگی، وفق‌پذیری و ناشناس بودن به طور جداگانه توسط سرویس یکپارچگی داده، کانال‌های حالت خارج از زنجیره (ارائه شده توسط شبکه‌های لایتنینگ یا شبکه‌های Raiden) و یک سازوکار رمزنگاری ترکیبی با امضای حلقه قابل پیوند و تکنیک‌های zerocash مورد بررسی قرار می‌گیرد. در [۱۵]، یک مدل ذخیره‌سازی امن سه لایه پیشنهاد شده است که در آن لایه خدمات ابری زنجیرهٔ بلوکی جهانی را حفظ می‌کند و لایه لبه، زنجیرهٔ بلوکی محلی را حفظ می‌کند. فناوری کد بازسازی برای ارائه افزونگی داده‌ها به منظور بهبود قابلیت اطمینان داده‌ها در لایه خدمات ابری استفاده می‌شود. علاوه بر این، سازوکار تأیید برای کارسازهای ابری طراحی شده است تا مقادیر چکیدهٔ داده‌های بارگذاری شده از کارسازهای لبه را محاسبه کند. سپس، کارسازهای لبه نتایج را با مقادیر چکیدهٔ ذخیره شده در زنجیرهٔ بلوکی محلی مقایسه می‌کنند تا تصمیم بگیرند که آیا داده‌ها را در زنجیرهٔ بلوکی جهانی بنویسند یا خیر، بنابراین از یکپارچگی داده‌ها اطمینان حاصل می‌کنند. در [۱۶]، یک پروتکل ذخیره‌سازی ناشناس داده و یک پروتکل تراکنش ناشناس داده با استفاده از IBEC برای

جدول ۲: کاربردهای IBEC: مدیریت داده/ دانش

مراجع	کاربردها	اهداف	مشارکت‌ها	سایر فناوری‌های پشتیبانی
[۱۴]	مدیریت داده	یکپارچگی، وفق‌پذیری و ناشناس بودن در ذخیره‌سازی امن داده‌ها	پیشنهاد یک چارچوب مفهومی IBEC برای اینترنت اشیاء با استفاده از فناوری‌های متنوع DIS، کانال‌های حالت خارج از زنجیره، ترکیبی از سازوکارهای رمزنگاری و غیره، و پیاده‌سازی نمونه اولیه سیستم با استفاده از اتریوم	خیر
[۱۵]	مدیریت داده	یکپارچگی و قابلیت اطمینان در ذخیره‌سازی امن داده‌ها	پیشنهاد یک معماری ذخیره‌سازی امن سه لایه. طراحی یک سازوکار مبتنی بر کد احیاکننده برای ذخیره‌سازی داده‌های افزونگی زنجیرهٔ بلوکی جهانی و پیشنهاد یک پروتکل تأیید برای همگام‌سازی داده‌ها بین زنجیرهٔ بلوکی جهانی و زنجیرهٔ بلوکی محلی	خیر
[۱۶]	مدیریت داده	ناشناس بودن در ذخیره‌سازی امن داده‌ها و تجارت داده‌ها	پیشنهاد یک پروتکل ذخیره‌سازی ناشناس داده و یک پروتکل تراکنش داده، که به طور جداگانه از هویت‌های شبه مبتنی بر سیستم رمزنگاری الگامال و بررسی‌های الکترونیکی مبتنی بر امضای کورکننده استفاده می‌کند.	خیر
[۱۷]	مدیریت دانش	به اشتراک‌گذاری دانش قابل اعتماد و کارآمد.	پیشنهاد یک چارچوب اشتراک‌گذاری دانش مبتنی بر کاربرمحور (UCB) سه لایه و سازوکار اجماع PoP. طراحی رتبه‌بندی ارزش پیشنهادی و انتخاب الگوریتم و الگوریتم تولید بلوک آگاه از امنیت	هوش مصنوعی

دستیابی به ناشناس بودن در طول فرآیندهای ذخیره‌سازی و داد و ستد داده‌ها پیشنهاد شده است. در پروتکل ذخیره‌سازی ناشناس داده‌ها، بر اساس سیستم رمزگذاری الگامال، دستگاه‌های لبه‌ای که نقش کارسازها را ایفا می‌کنند، مسئول تولید هویت‌های شبه برای داده‌های جمع‌آوری شده از دستگاه‌های اینترنت اشیاء هستند، داده‌ها را با استفاده از کلید متقارن رمزگذاری می‌کنند، سپس داده‌ها را در جدول چکیدهٔ توزیع شده[17] (DHT) ذخیره می‌کنند. و در نهایت نشانی‌ها را به‌دست آورید. در پروتکل تراکنش ناشناس داده، فناوری امضای کور برای پیاده‌سازی ناشناس و قابل تأیید مصرف‌کنندگان داده معرفی شده است.

امنیت، حریم خصوصی و کارایی نیز از نقاط تمرکز در مدیریت داده/ دانش هستند. در [۱۷]، یک چارچوب زنجیرهٔ بلوکی کاربرمحور (UCB)[18] برای مقابله با مشکلات امنیتی ناشی از ضعف حفاظت از حق چاپ، حسابداری نامعتبر در لبه و اجماع ناکارآمد در اشتراک دانش ارائه شده است. در UCB، یک سازوکار اجماع اثبات محبوبیت (PoP)[19] با در نظر گرفتن رتبه‌بندی ارزش پیشنهادی کاربرمحور و الگوریتم انتخابی و الگوریتم تولید بلوک آگاه از امنیت طراحی شده است.

مطالعات فوق در مورد مدیریت داده/ دانش در جدول ۲ خلاصه شده است.

۷- IBEC برای ارتباطات قابل‌اعتماد

در [۱۸]، یک رویکرد انتقال مبتنی بر زنجیرهٔ بلوکی برای اطمینان از اتصال، در دسترس بودن و بق۴٦٨+l طراحی شده است، که در دستیابی به ارتباطات فوق‌العاده قابل‌اعتماد و تأخیر کم در MEC با ترکیب زنجیرهٔ بلوکی و شبکه عصبی برای یافتن حداکثر مقدار و گره مسیر خروجی در این مقدار به عنوان یک مسیر قابل‌اعتماد، اساسی هستند. در [۱۹]، یک طرح انتقال داده مبتنی بر زنجیرهٔ بلوکی برای ارتباطات دستگاه به دستگاه (D2D) در محاسبات لبه، توسعه یافته است که در آن سازوکار اجماع اثبات قابلیت اطمینان (PoR) به گونه‌ای طراحی شده است که کاربرانی که اعتبار و حامیان کافی دارند اجازه انتقال داده‌ها را داشته باشند. زنجیرهٔ بلوکی برای اطمینان

17-Distributed Hash Table
18-User-Centric Blockchain
19-Proof-of-Popularity

جدول ۳: ارتباطات قابل اعتماد

مراجع	کاربردها	اهداف	مشارکت‌ها	سایر فناوری‌های پشتیبانی
[۱۸]	پروتکل انتقال داده	دستیابی به ارتباطات فوق‌العاده قابل اطمینان در MEC از نظر در دسترس بودن، اتصال و بقا	استفاده از یک شبکه عصبی برای سازوکار انتقال محتوای هوشمند مبتنی بر زنجیرهٔ بلوکی و قراردادهای هوشمند برای قابلیت‌های ذخیره‌سازی وسایل نقلیه هوایی بدون سرنشین (UAV)	شبکه عصبی، UAV
[۱۹]	پروتکل انتقال داده	تضمین قابلیت اطمینان انتقال داده در اینترنت اشیاء	پیشنهاد یک سازوکار انتقال داده در محیط محاسبات لبه بر اساس یک زنجیرهٔ بلوکی بهینه شده که در آن کارسازهای لبه زنجیرهٔ بلوکی کامل را حفظ و به روز می‌کنند و گره‌های سبک‌وزن عمومی از داده‌های موجود در زنجیره استفاده می‌کنند و سازوکار اجماع به عنوان PoR دوباره طراحی شده است	خیر
[۲۰]	پروتکل پیام‌رسان	بهینه‌سازی امنیت و کارایی ارتباطات ماشین به ماشین (M2M) در محیط اینترنت اشیاء	ایجاد یک مدل پیام‌رسان ترکیبی که در آن لایه دستگاه‌های اینترنت اشیاء، زنجیره‌های بلوکی خصوصی چندگروهی را حفظ می‌کند و لایه کارسازهای لبه، یک زنجیرهٔ بلوکی عمومی را حفظ می‌کند	خیر
[۲۱]	پروتکل پیام‌رسان	طراحی یک پروتکل پیام‌رسانی متناسب با IBEC	مقایسه و تحلیل پروتکل‌های پیام‌رسانی MQTT و CoAP در شبکه اینترنت اشیاء و پیشنهاد یک پروتکل جدید با ترکیب این دو پروتکل	خیر

از دستکاری و قابلیت ردیابی داده‌ها (به عنوان مثال، پیام‌ها و داده‌های رفتاری) در اینترنت اشیا معرفی شده است. به منظور دستیابی به پیام‌رسانی ایمن و کارآمد، یک مدل پیام‌رسانی در [۲۰] توسعه یافته است. زنجیرهٔ بلوکی خصوصی و زنجیرهٔ بلوکی عمومی با هم در مدل پیام‌رسانی برای پشتیبانی از ارتباطات در یک گروه لبه و در کل شبکه مورد استفاده قرار می‌گیرند. به طور متوالی، یک روش پیام‌رسانی ترکیبی در [۲۱] با ادغام انتقال تله متری صف‌بندی پیام (MQTT) و پروتکل برنامه محدود شده (CoAP) پیشنهاد شده است، که در آن پروتکل کم‌مصرف CoAP برای پایانه‌های محدود منابع برای برقراری ارتباط با کارسازهای لبه‌شان استفاده می‌شود. در حالی که پروتکل MQTT برای ارتباط بین گره‌های لبه/مه استفاده می‌شود. مطالعات فوق در مورد ارتباطات قابل اعتماد در جدول ۳ خلاصه شده است.

۸. IBEC برای امنیت و حریم خصوصی

در دنیای دیجیتالی امروزی، امنیت سایبری یک نگرانی اصلی برای تجارت، دولت و افراد است. با اتصال میلیون‌ها دستگاه، رخنه‌گران آسیب‌پذیری‌های جدیدی را برای انجام حملات پیچیده‌تر پیدا می‌کنند که شناسایی، محافظت و پاسخ به این تهدیدات را برای سیستم‌ها بسیار دشوارتر می‌کند. علاوه بر سرقت اطلاعات یا مختل‌کردن فعالیت‌های تجاری، رخنه‌گران اکنون نقاط ورودی بیشتری دارند که به آنها اجازه می‌دهد به دنیای فیزیکی ما آسیب برسانند و خطرات امنیتی جدی برای شرکت‌ها، کارخانه‌ها، حمل‌ونقل و سایر زیرساخت‌های حیاتی ایجاد کنند. فناوری زنجیرهٔ بلوکی یکی از راه‌حل‌های برآورده کردن این الزامات امنیتی در EoT از طریق تراکنش‌های شفاف است. دفتر کل زنجیرهٔ بلوکی هر سری تراکنش را از سر به انتها فهرست می‌کند و قابلیت اطمینان، همگام‌سازی و ردیابی همه تراکنش‌ها را امکان‌پذیر می‌کند. سازوکارهای مختلف امنیتی و حریم خصوصی مانند کنترل دسترسی، احراز هویت، مدیریت اعتماد و شناسایی حمله را می‌توان در IBEC اعمال کرد.

- **دسترسی به احراز هویت**: شبکه‌های سلولی مختلف اتصال یکپارچه را برای میلیاردها اشیاء یا دستگاه ارائه می‌دهند. برای محافظت از تبادل داده‌ها، سازندگان دستگاه‌ها باید هویت‌های دیجیتال منحصر به فرد و قابل

اعتمـــادی را ارائه دهنـــد و از تبادل امـــن داده‌ها اطمینان حاصل کنند. زنجیـــرهٔ بلوکی امنیت را در برابر رخنه‌گران فراهم می‌کند، رمزگذاری انتها به انتها داده‌هایی را که آنها به اشـــتراک می‌گذارند را فعال می‌کند. در [۲۲] روشـــی را برای بهبود خدمات احراز هویت توزیع شده و قابل‌اعتماد در زنجیرهٔ بلوکی و EoT معرفـــی می‌کند. الگوریتم اجماع تحمل خطای بیزانسی برای توسعه یک زنجیرهٔ بلوکی برای ذخیره‌سازی داده‌ها و احراز هویت پیشنهاد شد. محاسبات لبه با ارائه دو گره لبه، یک گره لبه وضوح و یک گره نهان به یک زنجیرهٔ بلوکی اعمال شد. گره‌های لبه تفکیک‌پذیری وضـــوح نام را ارائه می‌کنند و گره ذخیره‌ســـازی با هدف احراز هویت لبه با اســـتفاده از قراردادهای هوشـــمند و به بهبود نسبت اصابت کمک می‌کند. مدل رمزنگاری نامتقارن برای رســـیدگی به چالش‌های امنیتی بین پایانه‌ها و گره‌ها پیشـــنهاد شـــد. نتایج تجربی کارایی الگوریتـــم را از نظر هزینه‌های ارتباطی و محاســـباتی مؤثر نشان می‌دهد، در حالی که مدل پیشنهادی با کاهش نرخ تأخیر ٦ تا ۱۲ درصد و افزایـــش نرخ اصابت ۸ تا ١٤ درصد، از مدل‌های موجود بهتر عمل می‌کند. با این حال، مدل پیشـــنهادی را می‌توان با کاهـــش تأخیر در حین انتقال بســـته‌های داده بزرگ به مقصد تقویت کرد. در کار مشابهی در [۲۳]، نویسندگان یک پروتکل توافق کلید ایمن با استفاده از زنجیرهٔ بلوکی برای سیستم‌های محاسباتی لبه شبکه هوشمند پیشنهاد کردند. نیاز اصلی این مدل پیشنهادی این است که کنتور هوشمند گاهی اوقـــات صحت کنترل تـــوان الکتریکی را بررســـی نمی‌کنـــد و بنابراین فرآیند احراز هویت با ســـرعت بهتری انجام نمی‌شود. انتقال ایمن کالا از مبدا به مقصد با استفاده از زنجیـــره تامین نیاز به پهنای‌باند بالایی دارد که می‌توان با EoT دارای 5G به آن دست یافت. رشد سریع محاسبات لبه وسیله نقلیه (VEC) در حمل‌ونقل هوشمند، پیاده‌سازی‌ها را در سیستم‌های ترافیکی تشـــدید کرده است. دسترسی به کانال‌هـــای ارتباطی، احراز هویـــت حریم خصوصی و مدیریت اعتمـــاد در خودروها، VEC را بســـیار رایج کرده است. در [٢٤]، نویسندگان یک مدل زنجیرهٔ بلوکی VEC را بر اساس جهت‌های نقشه قابل ردیابی با استفاده از زنجیره چکیدهٔ مسیر پویا پیشنهاد کردند. چشم‌انداز این مدل ایجاد یک سیســـتم غیرمتمرکز و ایمن با هزینه ارتباط کم است. علاوه بر این، مدل پیشـــنهادی به تأخیر و سربار ارتباطی بهتری برای پیام داده‌ای ٢٥٦ بیتی دست نمی‌یابد، بنابراین از سودمندی آن در VEC جلوگیری می‌کند.

- **حفظ حریم خصوصی داده‌ها:** حفظ حریم خصوصی داده‌هـــا یکـــی از الزامات کلیدی اســـت کـــه از داده‌ها در برابر دسترســـی‌های مخرب محافظـــت می‌کند. تعدادی از سازوکارهای موجود برای حفظ حریم خصوصی داده‌ها شـــامل رمزگذاری، رمزگشایی، مبتنی بر اختلال و زنجیره بلوکی اســـت. داده‌ها بـــه طور ایمن در زنجیـــرهٔ بلوکی با حفظ مهرهای زمانی و توابع چکیده‌ســـاز منتقل می‌شوند. اطلاعات مشـــترک در چندین پایگاه با استفاده از یک دفتر کل توزیع‌شده توزیع می‌شود.

در [۲۵]، نویســـندگان حفظ حریـــم خصوصی را برای برنامه‌های شـــبکه هوشمند پیشنهاد کردند. در این فرآیند، مصرف برق را می‌توان به راحتی بدون افشـــای اطلاعات کاربر نهایی ردیابی کرد تا با بالا بردن هشـــدار با استفاده از زنجیرهٔ بلوکی، رفتارهای مصرف انرژی نامناســـب را شناسایی کرد. تعداد کمی ابرگره در زنجیرهٔ بلوکی مستقر شده‌اند که مســـئول تخصیص منابع هســـتند که گره‌های لبه را تایید می‌کنند. در اینجا گره‌های لبه کنتور هوشـــمند و حســـگر قدرت در نظر گرفته می‌شـــوند. این گره‌های لبه انرژی را بـــه کاربر نهایی توزیع می‌کنند که بار سیســـتم مرکزی را کاهش می‌دهد و به بهبود فرآیند محاسبات کمک می‌کند. گره لبه با اســـتفاده از طـــرح مجوز کانال مخفی و طرح کنترل دســـترسی تأیید می‌شود. اعتبارسنجی طوری طراحی شده است که اطمینان حاصل شود که یک حمله ۵۱ درصد تضمین می‌کند که اکثر شرکت‌کنندگان خوب هستند. تخصیص بهینه منابع انرژی از طریق یک قرارداد هوشمند انجام می‌شود که سه عنصر شامل مصرف انرژی، تأخیر

و امنیت ارتباطات را پوشش می‌دهد. کار در [۲۶]، یک مدل توزیع‌شده IIoT را برای کارخانه هوشمند با استفاده از زنجیرۀ بلوکی معرفی می‌کند. به منظور اطمینان از حریم خصوصی مناسب، نویسندگان رویکرد کنترل دسترسی محتاطانه (BLP)[20] را معرفی کردند که با مدل biba [۲۷] ادغام شده است. یافته‌های تجربی نشان می‌دهد که مدل پیشنهادی ویژگی‌های امنیتی و حریم خصوصی را افزایش می‌دهد. با این حال، مدل پیشنهادی نتوانست به راهبردهای تخصیص منابع مناسب دست یابد و در نتیجه سودمندی آن را کاهش داد. در [۲۸]، نویسندگان یک مدل زنجیرۀ بلوکی نوآورانه برای معماری‌های اینترنت اشیاء مبتنی بر لبه به نام LiTichain با بلوک‌های متعدد، هر کدام با طول عمر محدود، پیشنهاد کردند. در صورت پایان یافتن عمر تراکنش، بلوک از زنجیره حذف خواهد شد. LiTichain از ادغام دو نمودار مختلف ایجاد می‌شود. یک نمودار نشان‌دهنده عمر تراکنش است و نمودار دوم نشان‌دهنده تشکیل یک بلوک در زنجیره است. از آنجایی که تعداد تراکنش‌ها ارتفاع زنجیره را افزایش می‌دهد، نویسندگان یک روش بلوک K- ارتفاع را برای محدود کردن ارتفاع زنجیره معرفی کرده‌اند.

● **تشخیص حمله**: مهاجمان سایبری در حال بررسی آسیب‌پذیری‌های مختلف برای سوءاستفاده از حملات بسیار پیچیده هستند، که شناسایی، محافظت و پاسخ به چنین حملاتی را برای سیستم‌ها بسیار دشوار می‌کند. سیستم تشخیص حمله یکی از الزامات نظارت بر سیستم ارتباطی و محافظت در برابر حملات مخرب است. یکی دیگر از چارچوب‌های زنجیرۀ بلوکی را می‌توان در [۲۹] مشاهده کرد که در آن از انکار اقتصادی پایداری (EDoS)[21] از مهاجمان مخرب جلوگیری می‌شود. طرح به اشتراک‌گذاری مخفی (SSS)[22] برای تامین امنیت هر زمان که کارسازهای لبه (ES) از کار بیفتند، معرفی شده است. گاهی اوقات، هر زمان که کارسازهای لبه به دلیل حمله مخرب مهاجم از کار بیفتد، مدل پیشنهادی از سازوکار جستجوی دودویی برای شناسایی و مکان‌یابی کارسازهای لبه آسیب دیده استفاده می‌کند. نتایج نشان می‌دهد که مدل پیشنهادی از داده‌های متن رمزی ۱۲۸ بیتی، کلید Diffie-Hellman ۲۵۶ بیتی، به ۰/۰۰٤ میلی‌ثانیه برای رمزگذاری و ۰/۰۰۳۹ میلی‌ثانیه برای رمزگشایی نیاز دارد. کل زمان محاسباتی مدل پیشنهادی برای بارگذاری و دسترسی به داده‌ها ۱٤/۱۱۹۹ میلی‌ثانیه است. علاوه بر عملکرد محاسباتی، مدل پیشنهادی به نرخ پیشگیری از حمله بهتری دست می‌یابد. پیام‌های رویدادمحور در شبکه‌های وسایل نقلیه در هنگام وقوع تصادفات، لغزش جاده تولید می‌شوند. EDMها از عکس‌ها، فیلم‌ها و غیره تشکیل شده‌اند و در حین ارسال این پیام‌ها با چالش‌های متعددی مانند امنیت و تأخیر مواجه هستند. کار در [۳۰] یک بُن‌سازۀ زنجیرۀ بلوکی قابل‌اعتماد با محاسبات لبه وسیله نقلیه مجهز به 5G را برای انتقال EDM به کاربران نهایی با بهینه‌سازی هزینه‌های ارتباطی معرفی می‌کند. در طی این فرآیند، EDMها به ES مجاور منتقل می‌شوند تا زمان پاسخ را کاهش دهند. فناوری زنجیرۀ بلوکی در گره‌های لبه برای ردیابی پیام‌ها و محافظت از پیام‌ها در برابر انواع حملات استفاده می‌شود. نتایج نشان می‌دهد که مدل پیشنهادی EDMها را از انواع مختلف حملات محافظت می‌کند، مانند حملات جعل هویت، حملات DDoS، حملات دگرنمایی (بالماسکه)، و هزینه‌های ارتباطی را کاهش می‌دهد.

● **مدیریت اعتماد**: با توجه به رشد سریع پیشرفت‌های فنی، مقادیر زیادی داده از گره‌های لبه یا دستگاه‌های اینترنت اشیاء جمع‌آوری می‌شوند، اما حفاظت از داده، مدیریت اعتماد و حفظ حریم خصوصی الزامات بسیار مهمی در ES هستند، به‌ویژه زمانی که داده‌های جمع‌آوری شده مخرب هستند و می‌توانند مشکلات جدی ایجاد کنند. کار در [۳۱] یک سیستم مدیریت داده قابل‌اعتماد مبتنی بر زنجیرۀ بلوکی (BlockTDM) را در محاسبات لبه معرفی می‌کند. در این فرآیند، مدل زنجیرۀ بلوکی برای اطمینان از

20-Bell-La Padula
21-Economic Denial of Sustainability
22-Secret Sharing Scheme

جدول ۴: بررسی امنیت و حفظ حریم خصوصی

سرویس‌های امنیتی	مراجع	دامنه برنامه	مشارکت‌ها
دسترسی به احراز هویت	[۲۲]	سیستم IoT	گره‌های لبه تفکیک نام را ارائه می‌دهند و گره نهان با استفاده از قراردادهای هوشمند احراز هویت لبه را ارائه می‌دهد
	[۲۳]	شبکه هوشمند	پروتکل توافق کلید، کنتورهای هوشمند را قادر می‌سازد تا از طریق یک کلید خصوصی، خدمات توان قابل‌اعتماد را از کنترل توزیع به دست آورند
	[۲۴]	شبکه وسایل نقلیه	مسیرهای نقشه قابل ردیابی با استفاده از زنجیره چکیدهٔ مسیر پویا و برای ساختن یک سیستم غیرمتمرکز و ایمن با سربار ارتباط کم
حریم خصوصی داده‌ها	[۲۵]	شبکه هوشمند	تعداد کمی ابرگره در زنجیرهٔ بلوکی مستقر شده‌اند که مسئول تخصیص منابع هستند که گره‌های لبه را تایید می‌کنند.
	[۲۶]	IIoT	رویکرد BLP با مدل biba [۲۷] یکپارچه شده است تا از حریم خصوصی داده‌ها اطمینان حاصل شود
	[۲۸]	شبکه IoT	مدل زنجیرهٔ بلوکی LiTichain از ادغام دو نمودار مختلف ایجاد می‌شود. یک نمودار نشان‌دهنده عمر تراکنش است و نمودار دوم نشان‌دهنده تشکیل یک بلوک در زنجیره است.
تشخیص حمله	[۲۹]	سیستم خدمات	EDoS از مهاجمان مخرب جلوگیری می‌شود، SSS برای ایجاد امنیت در هر زمان که کارسازهای لبه شکست می‌خورد
	[۳۰]	شبکه وسایل نقلیه	بُن‌سازه زنجیرهٔ بلوکی قابل‌اعتماد با محاسبات لبه وسیله نقلیه مجهز به G۵ برای انتقال EDM به کاربران نهایی با بهینه‌سازی هزینه‌های ارتباطی
مدیریت اعتماد	[۳۱]	شبکه IoT	۱. BlockTDM حریم خصوصی داده‌ها را از طریق ارائه یک بخش داده چندکاناله تضمین می‌کند. ۲. رمزگذاری داده‌ها با استفاده از تکنیک‌های رمزگذاری تعریف شده توسط کاربر انجام می‌شود و رمزگشایی توسط hyperledger به عنوان یک قرارداد هوشمند انجام می‌شود.
	[۳۲]	محاسبات سیار	۱. الگوریتم RL برای کاهش زمان تأخیر محاسباتی، بهینه‌سازی مصرف انرژی و کاهش زمان تخصیص منابع دستگاه‌های لبه ۲. پروتکل PoW برای ساخت سریع سوابق خدمات در زنجیرهٔ بلوکی استفاده می‌شود
	[۳۳]	شبکه ذخیره‌سازی	۱. سرور نام دامنه درخواست کاربر را برای کاهش تأخیر انتشار به کارسازهای لبه ارسال می‌کند ۲. برای دستیابی به قابلیت اطمینان و امنیت، همه شرکت‌کنندگان اطلاعات بلوک و جزئیات تراکنش خود را به اشتراک می‌گذارند

احراز هویت متقابل، قرارداد هوشمند و اجماع انعطاف‌پذیر طراحی شده است. Block-TDM پیشنهادی حریم خصوصی داده‌هـــا را از طریق ارائه یک بخش داده چند کاناله تضمین می‌کند. داده‌ها با استفاده از تکنیک‌های رمزگذاری تعریف شده توسط کاربر درست قبل از ذخیره تراکنش در زنجیرهٔ بلوکی رمزگذاری می‌شـــوند. رمزگشایی و تراکنش داده‌ها در یـــک زنجیرهٔ بلوکـــی امن با اســـتفاده از hyperledger به عنوان یک قرارداد هوشـــمند انجام می‌شـــود. یکی دیگر از برنامه‌هـــای هیجان‌انگیز زنجیـــرهٔ بلوکی را می‌توان در [۳۲] یافـــت، که MEC را از تهدیدات ســـوابق خدمات جعلی و تهدیدات لبه‌های مخرب محافظت می‌کند. نویسندگان یک الگوریتم RL را برای کاهش تأخیر محاسباتی، بهینه‌سازی مصرف انرژی و کاهش زمان تخصیص منابع دستگاه‌های لبه پیشنهاد کردند. نتایج تجربی نشان می‌دهد که نویسندگان از مدل زنجیرهٔ بلوکی در اتریوم استفاده کرده‌اند، پروتکل PoW برای ساخت سریع سوابق خدمات در زنجیرهٔ بلوکی استفاده می‌شود. مدل پیشنهادی نرخ حمله مخرب را تا ٦٦/٤ درصد کاهش می‌دهد، مصرف انـــرژی را تا ۱۰/۵ درصد بهینه می‌کنـــد و تأخیر را تـــا ٦٧/٤ درصد کاهش می‌دهد. در [۳۳]، نویســـندگان یک مدل زنجیرهٔ بلوکی غیرمتمرکز و قابل‌اعتماد را در محاســـبات لبه معرفی کردند. کارساز نام دامنه درخواســـت کاربر را به ES مناسب می‌فرستد که

تأخیر انتشـــار را کاهش می‌دهد. برای دستیابی به قابلیت اطمینان و امنیت، همه شرکت‌کنندگان درگیر در تراکنش‌ها باید اطلاعات بلوک و جزئیات تراکنش خود را به اشـــتراک بگذارند. شرکت‌کنندگانی که در این شبکه مشارکت می‌کنند، شناسه‌های زنجیرۀ بلوکی کسب خواهند کرد. نتایج تجربی نشان می‌دهد که مدل پیشنهادی ۱۲/۵٤ درصد نرخ تأخیر بهینه را در مقایسه با سایر مدل‌های موجود فراهم می‌کند.

مطالعات فوق در مورد ســـازوکارهای امنیتی و حریم خصوصی در جدول ٤ خلاصه شده است.

۹- کاربرد زنجیرۀ بلوکی در حوزه‌های مرتبط با اینترنت اشیاء

ویژگی‌هـــای زنجیرۀ بلوکی مانند تغییر ناپذیری، امنیت و عدم تمرکز آن را برای غلبه بر مســـائل امنیتی، اعتماد و قابلیت ردیابی در اینترنت اشیاء ایـــده‌آل می‌کند. بنابراین، فنـــاوری زنجیـــرۀ بلوکی پتانسیـــل زیادی بـــرای کاربرد موفقیت‌آمیز در موارد مختلف اســـتفاده در حوزه اینترنت اشیاء دارد. این بخش بـــرخی از کاربردهای مفید زنجیرۀ بلوکی را در حوزه‌هـــای مرتبط با اینترنت اشیاء همانطور که در شکل ٤ نشان داده شده است، ارائه می‌کند.

۱۰- خانه‌های هوشمند

فنـــاوری زنجیرۀ بلوکی این پتانسیـــل را دارد که دامنه خانه‌هـــای هوشـــمند را متحول کنـــد و از ارتباطات امن و مطمئن و به اشـــتراک‌گذاری داده‌ها بین دستگاه‌های خانه هوشـــمند اطمینان حاصل کنـــد [۳٤]. در زیـــر چند مورد اســـتفاده مفید برای خانه‌های هوشـــمند مبتنی بر زنجیرۀ بلوکی آورده شده است.

- **تجارت غیرمتمرکز انرژی**: امروزه بسیاری از خانه‌های هوشـــمند با اســـتفاده از پنل‌های خورشـــیدی برق تولید می‌کنند. زنجیرۀ بلوکی و اینترنت اشـــیاء را می‌توان برای خودکارســـازی تجارت انرژی مازاد بدون دخالت انســـان استفاده کرد.
- **قفل‌های هوشمند**: سازوکارهای احراز هویت غیرمتمرکز مبتنی بر زنجیرۀ بلوکی می‌توانند برای کنترل دسترسی به خانه‌های هوشمند استفاده شوند. به عنوان مثال، صاحبان خانه می‌توانند از راه دور دسترسی به خانه‌های خود را با اســـتفاده از قفل‌های هوشمند پیکربندی شده با هویت‌های دیجیتال مبتنی بر زنجیرۀ بلوکی کنترل کنند.
- **لوازم خانگی هوشمند**: با ساختن لوازم خانگی هوشمند مانند ماشـــین لباسشـــویی و یخچال کـــه توانایی تعمیر و نگهداری، خـــود ســـفارش دادن و حتی پرداخـــت هزینه، زنجیرۀ بلوکی مداخله انسان را کاهش می‌دهد.
- **بیمه خانه**: زنجیرۀ بلوکی می‌تواند در خودکارســـازی سیاست‌های تضمین خانه و ارزیابی ریسک با استفاده از داده‌های دستگاه‌های خانه هوشمند استفاده شود.
- **صورت‌حساب و پرداخت‌های خودکار**: زنجیرۀ بلوکی می‌تواند مصرف انرژی خانه هوشـــمند و پرداخت قبوض تعمیر و نگهـــداری را از طریق اجرای خودکار قراردادهای هوشمند خودکار کند.

۱۱- مدیریت زنجیره تأمین

مدیریـــت زنجیره تامیـــن (SCM)[۲۳] [۳۵] مفهوم تحویل، ردیابی و مدیریت کالاها و خدمات از ســـازنده تا مشـــتری نهایی اســـت. تعدادی از نهادها یا سودبران در طول چرخه عمر SCM درگیر هستند، مانند تولیدکنندگان، تأمین‌کنندگان، توزیع‌کنندگان، خرده‌فروشـــان و مشتریان. زنجیرۀ بلوکی در چند ســـال اخیر در عرضه SCM مبتنی بر اینترنت اشیاء به دلیل شـــفافیت، ویژگی‌های تغییر ناپذیـــری و امنیت آن محبوبیت زیادی به‌دســـت آورده است. این می‌تواند اساساً فرآیند SCM را با ایجاد زنجیرۀ بلوکی با اعتماد بیشـــتر بین طرفین، ردیابی و تأیید مالکیت کالا تغییر دهد تا فرآیند SCM آسان‌تر شـــود. زنجیرۀ بلوکی می‌تواند با ارائه یک دفتر کل غیرقابل تغییر و ضد دســـتکاری که جریان کالاها را در هر مرحله از SCM با کمک حســـگرهای اینترنت اشیاء پیگیری می‌کند، اعتماد بیشتری را برای طرفین درگیر فراهم کند.

23-Supply Chain Management

فناوری بلوک چین می‌تواند شفافیت و دید را با ردیابی کالاهـــا و خدمات در بیدرنگ با اســـتفاده از حســـگرهای اینترنت اشیاء افزایش دهد. زنجیرهٔ بلوکی می‌تواند زمان و هزینه‌های مرتبط با اسناد و تایید SCM را با هموارسازی فرآینـــد مرتبـــط بـــا SCM کاهش دهـــد. به طور مشـــابه، قراردادهای هوشـــمند زنجیرهٔ بلوکی می‌تواند بسیاری از فعالیت‌های SCM را خودکار کند، به عنوان مثال، پرداخت، ترخیص سفارشی و کنترل‌های کیفیت.

۱۲- مراقبت‌های بهداشتی

زنجیـــرهٔ بلـــوکی می‌توانـــد بـــا موفقیـــت بـــرای بـــه اشـــتراک‌گذاری، امنیـــت، قابلیت همـــکاری و حفظ حریم خصـــوصی داده‌های مراقبت‌های بهداشـــتی بین بیماران، ارائه دهندگان مراقبت‌های بهداشـــتی، داروخانه‌ها و سایر ذی‌نفعان مورد استفاده قرار گیرد. سیستم‌های مراقبت‌های بهداشتی مبتنی بر زنجیرهٔ بلوکی محبوب شامل MedRec و شبکه بهداشت Gem است. در زیر برخی از کاربردهای مفید فناوری زنجیرهٔ بلوکی در مراقبت‌های بهداشتی مبتنی بر اینترنت اشیاء آورده شده است:

- داده‌های مراقبت‌های بهداشـــتی بیمار: این روزها بیمار از پوشـــیدنی‌ها و حســـگرهای مبتنـــی بر اینترنت اشـــیاء بـــرای مراقبت‌های بهداشـــتی اســـتفاده می‌کنـــد. امنیت و حریم خصوصـــی داده‌های مراقبت‌های بهداشـــتی بیمار یک نگرانی مهم اســـت. بنابراین، زنجیـــرهٔ بلوکی می‌تواند مدیریت داده‌های بیمار را تنظیم کند که در آن بیماران باید اطلاعات خود را برای به اشتراک گذاشتن اطلاعات خود با همه ارائه‌دهندگان مراقبت‌های بهداشتی، محققین، یا سایر عوامل به روشی ایمن و کنترل‌شده فراهم کنند.
- به اشـــتراک‌گذاری ایمن ســـوابق پزشـــکی: در پرونده الکترونیکی سلامت (EHR) سیستم زنجیرهٔ بلوکی می‌تواند بـــرای اطمینان از حریم خصوصی و امنیت داده‌های بیمار استفاده شود. به عنوان مثال، زنجیرهٔ بلوکی می‌تواند نقش حیاتی در به اشتراک‌گذاری داده‌های بیمار بین ارائه‌دهندگان مختلف مراقبت‌های بهداشتی و همچنین بین ارائه‌دهندگان مراقبت‌های بهداشتی و آزمایشگاه‌ها داشته باشد.
- تحقیقات بالینـــی: دو عامل برجســـته مرتبط با عرصه تحقیقات بالینی، شـــفافیت و پاســـخگویی است. شفافیت و پاسخگویی داده‌های تحقیقات بالینی را می‌توان با استفاده از سوابق تغییرناپذیر و قابل حسابرسی مبتنی بر زنجیرهٔ بلوکی از تمـــام داده‌های مرتبط با تحقیقات بالینی تضمین کرد.
- مدیریـــت زنجیره تامین دارو: زنجیـــرهٔ بلوکی می‌تواند زنجیره تأمین محصولات دارویی را از ســـازنده تا کاربر نهایی از طریق حسگرهای اینترنت اشیاء پیگیری و ردیابی کند. این رویکرد می‌تواند ایمنی، شـــفافیت، پاســـخگویی و اثبات تقلبی داروها را تضمین کند.
- پرداخت و بیمه: زنجیرهٔ بلوکی می‌تواند تقلب و اشتباهات در پرداخت و بیمه مراقبت‌های بهداشتی را با خودکارسازی و ساده‌سازی فرآیندهای اداری به حداقل برساند.

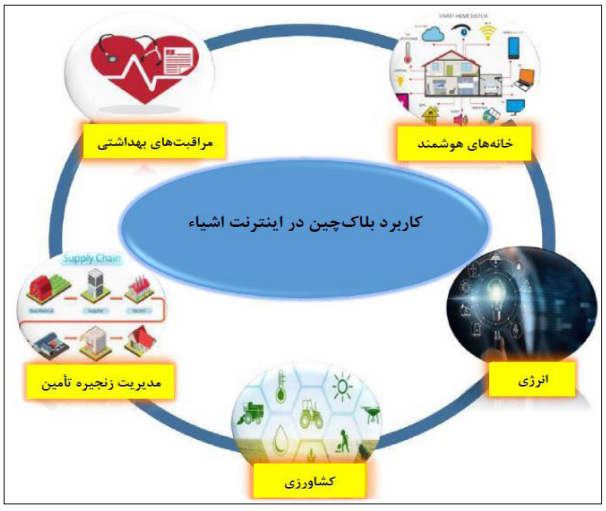
۱۳- مدیریت انرژی

زنجیـــرهٔ بلوکی دارای پتانسیل عظیمی در تحول بخش انرژی با تضمین سیســـتم‌های غیرمتمرکز، شفاف و ایمن برای مدیریت انرژی اســـت [۳۶]. شـــبکه هوشـــمند که با داده‌های بیدرنگ مبتنی بر زنجیرهٔ بلوکی و اینترنت اشیاء تکمیل می‌شـــود، می‌تواند تولید، ذخیره و توزیع انرژی را بهبود بخشـــد. یکی از کاربردهای بالقوه زنجیرهٔ بلوکی در بخش انرژی، بُن‌ســـازه‌های تجارت انرژی P2P است [۳۷]. چنین بُن‌ســـازه‌ای می‌تواند تجارت مازاد انرژی تجدیدپذیر (خورشیـــدی) را بین خانه‌ها و شـــرکت‌ها امکان‌پذیر کند. امنیت و شفافیت تجارت انرژی و پرداخت مربوط به آن را می‌توان با استفاده از فناوری زنجیرهٔ بلوکی تضمین کرد. بهبود در مدیریت انرژی از طریق زنجیرهٔ بلوکی می تواند با شـــکل دادن به سیســـتم‌های ذخیره انرژی غیرمتمرکز تحقق یابد. کنتورهای هوشمند و سیستم‌های ذخیره انرژی کـــه از طریق ادغام زنجیرهٔ بلـــوکی و اینترنت اشیاء ایجاد

شده‌اند، می‌توانند شبکه‌های ذخیره انرژی توزیع شده را پیش ببرند. به طور مشابه، زنجیرهٔ بلوکی همچنین می‌تواند نیروگاه‌های مجازی را ارتقا دهد. پروژه‌های ریزشبکه بروکلین و بنیاد وب انرژی نتیجه کاربرد موفقیت‌آمیز برنامه‌های زنجیرهٔ بلوکی در بخش انرژی هستند.

۱۴- کشاورزی

فناوری زنجیرهٔ بلوکی همچنین می‌تواند تغییراتی در مورد قابلیت ردیابی، شفافیت و کارایی در زنجیره تأمین مواد غذایی کشاورزی ایجاد کند. حسگرهای اینترنت اشیاء می‌توانند داده‌ها را در زنجیره تأمین مواد غذایی کشاورزی جمع‌آوری کرده و برای اهداف ذخیره‌سازی و گزارش‌دهی به زنجیرهٔ بلوکی منتقل کنند. در نتیجه، این به عنوان شواهد مفیدی برای همه سودبران در مورد منبع، پردازش و حمل و نقل محصولات عمل می‌کند. متعاقباً، این امر باعث افزایش اطمینان مشتریان، قابلیت اطمینان و اعتماد نسبت به کالاهایی که می‌خرند، می‌شود. سایر فرآیندهای کشاورزی که این فناوری می‌تواند به طور بالقوه بهبود بخشد، علاوه بر ایمنی مواد غذایی، ثبت زمین [۳۸]، بیمه محصول [۳۹] و تأمین مالی زنجیره تأمین است.



شکل ۴: کاربرد زنجیرهٔ بلوکی در اینترنت اشیاء

۱۵- خلاصه و بینش

با توجه به ویژگی‌های مختلف زنجیرهٔ بلوکی، می‌توان آن را با موفقیت در انواع برنامه‌های مبتنی بر اینترنت اشیاء، به عنوان مثال، خانه‌های هوشمند، SCM، مراقبت‌های بهداشتی، مدیریت انرژی، و کشاورزی استفاده کرد. زنجیرهٔ بلوکی برای ارتباطات ایمن و به اشتراک‌گذاری داده‌ها در سناریوهای خانه هوشمند مانند قفل هوشمند، لوازم خانگی هوشمند، بیمه خانه و تجارت انرژی مازاد خانه ایده‌آل است. یکی دیگر از کاربردهای ارزشمند زنجیرهٔ بلوکی، اطمینان از اشتراک‌گذاری داده، امنیت، حریم خصوصی و قابلیت همکاری در حوزه مراقبت‌های بهداشتی مبتنی بر اینترنت اشیاء است.

۱۶- چالش‌ها و جهت‌گیری آینده

این بخش چالش‌ها و راه‌حل‌های بالقوه ادغام زنجیرهٔ بلوکی و اینترنت اشیاء را ارائه می‌دهد.

۱۷- چالش‌های استفاده از زنجیرهٔ بلوکی در اینترنت اشیاء

زنجیرهٔ بلوکی فرصت‌ها و مزایای زیادی مربوط به حوزه اینترنت اشیاء را فراهم می‌کند. در اینجا، چندین مورد استفاده و دامنه‌های مرتبط با اینترنت اشیاء را ارائه می‌کنیم که در آن زنجیرهٔ بلوکی در حال حاضر نویدبخش است. با وجود این فرصت‌ها، چالش‌های زیادی از طریق ادغام زنجیرهٔ بلوکی و اینترنت اشیاء در حال ظهور هستند

۱- **مقیاس‌پذیری**: در حال حاضر، فناوری زنجیرهٔ بلوکی از مشکلات مقیاس‌پذیری رنج می‌برد زیرا باید حجم عظیمی از داده‌ها و تراکنش‌ها را پردازش کند. محیط اینترنت اشیاء شامل دستگاه‌ها و حسگرهای زیادی است که می‌توانند حجم زیادی از تراکنش‌ها را ایجاد کنند. این بر چگونگی مقیاس‌پذیری برای پردازش و انجام تعداد زیادی تراکنش به دفتر کل در یک زمان معین تأثیر می‌گذارد.

سازوکار اجماع، یک تراکنش و یک بلوک را به زنجیره بلوکی تأیید و تثبیت می‌کند. عوامل اصلی که به مسئله مقیاس‌پذیری زنجیرهٔ بلوکی کمک می‌کنند، سازوکارهای اجماع زنجیرهٔ بلوکی و پروتکل‌های زیربنایی هستند. برای اجماع بین شرکت‌کنندگان در شبکه زنجیرهٔ بلوکی، محاسبات، ارتباطات و توافق گسترده لازم است. این در نتیجه مقیاس‌پذیری شبکه زنجیرهٔ بلوکی را در کل کاهش داده است. عنصر دیگری که بر مقیاس‌پذیری زنجیرهٔ بلوکی تأثیر می‌گذارد، اندازه زنجیرهٔ بلوکی است. هنگامی که تراکنش‌های جدید اضافه می‌شوند، اندازه زنجیرهٔ بلوکی افزایش می‌یابد. پردازش چنین حجم زیادی از تراکنش‌ها از نظر محاسباتی چالش برانگیز می‌شود.

۲- **مصرف انرژی**: چالش مهم دیگر استفاده از زنجیرهٔ بلوکی در اینترنت اشیاء مربوط به مصرف انرژی است. از آنجایی که زنجیرهٔ بلوکی از الگوریتم‌های محاسباتی پیچیده برای اعتبارسنجی، امنیت و تثبیت در تراکنش‌ها استفاده می‌کند، فناوری زنجیرهٔ بلوکی به عنوان محاسباتی و انرژی‌بر رتبه‌بندی شده است. این چالش در زمینه اینترنت اشیاء اهمیت بیشتری پیدا می‌کند، جایی که دستگاه‌های اینترنت اشیاء دارای انرژی، قدرت و قابلیت‌های پردازش محدودی هستند. دلایل متعددی به جنبه‌های انرژی مرتبط با فناوری زنجیرهٔ بلوکی کمک می‌کند. این عمدتاً به دلیل الگوریتم‌های اجماع ناکارآمد مانند اثبات کار است. در الگوریتم‌های اجماع مبتنی بر اثبات کار، استخراج‌کنندگان برای حل یک معمای ریاضی بسیار سخت برای اعتبارسنجی تراکنش‌ها با انتظار دریافت پاداش رقابت دارند. این فرآیند به انرژی و قدرت پردازش زیادی نیاز دارد. یکی دیگر از عوامل موثر در انرژی زنجیرهٔ بلوکی، الگوریتم‌های رمزنگاری است که در ایمن‌سازی و تأیید تراکنش‌ها استفاده می‌شود.

۳- **حریم خصوصی و امنیت داده‌ها**: زنجیرهٔ بلوکی به دلیل ویژگی‌های مرتبط با امنیت به دلیل الگوریتم‌های رمزنگاری قوی‌اش شناخته شده است. با این حال، زنجیرهٔ بلوکی هنوز در برابر حملات یا نقض‌های مختلف مبتنی بر امنیت آسیب‌پذیر است. دستگاه‌های اینترنت اشیاء معمولاً در یک محیط باز کار می‌کنند و داده‌های حساس تولید می‌کنند. هنگامی که داده‌ها از یک محیط اینترنت اشیاء به یک زنجیرهٔ بلوکی برای اهداف ذخیره‌سازی و اشتراک‌گذاری منتقل می‌شوند، حفاظت مبتنی بر امنیت بسیار مطلوب است. ماهیت توزیع شده زنجیرهٔ بلوکی چندین چالش جدید مبتنی بر امنیت را ایجاد می‌کند. اول، به دلیل ماهیت توزیع‌شده داده‌های زنجیرهٔ بلوکی، تکثیر در چندین گره در شبکه اتفاق می‌افتد. این امر احتمال تهدیدات امنیتی و حملات مرتبط با آنها را افزایش می‌دهد. دوم، گره‌های زنجیرهٔ بلوکی را می‌توان در تعداد زیادی از مکان‌های جغرافیایی با قوانین حفظ حریم خصوصی مرتبط قرار داد، بنابراین، اعمال حریم خصوصی داده‌های کافی دشوار است. علاوه بر این، دستگاه‌های اینترنت اشیاء با قابلیت‌های امنیتی محدود می‌توانند به راحتی قربانی تهدیدات و حملات مبتنی بر امنیت شوند.

۴- **پیچیدگی یکپارچه‌سازی**: عوامل متعددی در ایجاد این چالش‌ها و پیچیدگی‌های یکپارچه‌سازی نقش دارند. اول این که، ماهیت و دامنه متنوع حسگرها و دستگاه‌های IoT این یکپارچگی را پیچیده و چالش برانگیز می‌کند. فقدان استانداردها در صنعت IoT دلیل دیگری است. دامنه وسیعی از پروتکل‌های ارتباطی و قالب‌های مختلف داده در اینترنت اشیاء استفاده می‌شود. بنابراین، استانداردسازی رابط‌ها برای ادغام زنجیرهٔ بلوکی با اینترنت اشیاء را بسیار سخت می‌کند.

۵- **انطباق با مقررات**: چالش دیگر در ادغام زنجیرهٔ بلوکی و اینترنت اشیاء، الزامات و انطباق مقررات است. به عنوان مثال، قانون قابل حمل و پاسخگویی بیمه سلامت و استاندارد امنیت داده صنعت کارت پرداخت به ترتیب دو مقررات بهداشتی و مالی هستند که باید در حین ادغام زنجیرهٔ بلوکی با اینترنت اشیاء مورد توجه قرار گیرند. یکی دیگر از قوانین حفاظتی کلیدی و مرتبط در این زمینه،

مقررات عمومی حفاظت از داده‌های اتحادیه اروپا است.

۶- **هزینه**: الزامات سخت‌افزاری، نرم‌افزاری و نگهداری در فناوری زنجیرهٔ بلوکی می‌تواند پرهزینه باشد. بنابراین، استفاده از فناوری زنجیرهٔ بلوکی در یک محیط اینترنت اشیاء به یک چالش محدودیت منابع تبدیل می‌شود، به‌ویژه جایی که هزینه موضوع اصلی است. علاوه بر این، راه‌حل‌های اینترنت اشیاء مبتنی بر زنجیرهٔ بلوکی در مقایسه با سیستم‌های متمرکز اینترنت اشیاء موجود، گران هستند. یکی از هزینه‌های کلیدی در محیط‌های زنجیرهٔ بلوکی، قدرت پردازش مربوط به اعتبارسنجی تراکنش و تعهد است. در یک فرآیند منظم اعتبارسنجی تراکنش، هر گره باید یک تراکنش معین را پردازش و تایید کند. چنین نوع اعتبارسنجی می‌تواند هزینه محاسباتی را تا حد زیادی افزایش دهد.

۷- **تمرکز**: فناوری زنجیرهٔ بلوکی یک فناوری توزیع‌شده و غیرمتمرکز است که سازمان‌ها را از الزام یک مرجع مرکزی یا واسطه معاف می‌کند. پیاده‌سازی زنجیرهٔ بلوکی در اینترنت اشیاء همچنان می‌تواند به یک مرجع مرکزی نیاز داشته باشد، به عنوان مثال، اپراتورهای گره زنجیرهٔ بلوکی یا ارائه‌دهندگان خدمات ابری. این با تمرکززدایی که زنجیرهٔ بلوکی‌ها واقعاً برای آن هستند در تضاد است و ممکن است نگرانی‌های امنیتی و حریم خصوصی را افزایش دهد. این تمرکز برای شناسایی یک یا چند گره برای اعتبار سنجی تراکنش می‌تواند منجر به یک نقطه شکست شود. تمرکز همچنین می‌تواند بر شفافیت و پاسخگویی کلی سیستم اساسی تأثیر بگذارد. در بدترین حالت، تمرکز ممکن است منجر به به خطر افتادن سیستم و منجر به دستکاری یا از دست رفتن داده شود.

۱۸- روندهای آینده و جهت‌گیری‌های تحقیقاتی

در این بخش، جهت‌گیری‌های تحقیقاتی آینده را ارائه می‌دهیم که برای کمک به غلبه بر چالش‌هایی که به دلیل ادغام زنجیرهٔ بلوکی و اینترنت اشیاء به سرعت پیش می‌آیند، به تحقیقات بیشتری نیاز دارند. اگرچه هیچ راه‌حل یکسانی ممکن نیست، اما برای ادغام موفقیت‌آمیز زنجیرهٔ بلوکی و اینترنت اشیاء، ترکیبی از راه‌حل‌های هیجان‌انگیز و نوآورانه در این جهت‌های نوظهور مورد نیاز است.

۱- **مقیاس‌پذیری**: مقیاس‌پذیری می‌تواند به یکی از مشکلات اصلی در محیط‌های اینترنت اشیاء مبتنی بر زنجیرهٔ بلوکی تبدیل شود. با توجه به پذیرش شبکه‌های پرسرعت نسل ۵ توسط دستگاه‌های IoT، مسئله مقیاس‌پذیری چالش برانگیزتر می‌شود. در ادامه روندهای تحقیقاتی مورد انتظار آینده آمده است که برای مواجهه با چالش‌های مقیاس‌پذیری به تحقیقات بیشتری نیاز دارند.

تجزیه: در این راه‌حل مقیاس‌پذیری، شبکه اصلی به شبکه‌های فرعی کوچکتر تقسیم می‌شود و آن را قابل مدیریت و مقیاس‌پذیر می‌کند. شاردینگ با پردازش سریع و کارآمد تراکنش‌های بیشتر، تراکم کمتری را در شبکه اصلی زنجیرهٔ بلوکی فراهم می‌کند.

- الگوریتم‌های اجماع بهینه شده: راهبرد دیگر، استفاده از تکنیک‌های اجماع بهینه شده، مانند اثبات سهام و اثبات سهام توسعه‌یافته (DPoS)[۲۴] است. چنین الگوریتم‌های اجماع بهینه‌شده‌ای از منابع محاسباتی کمتری استفاده می‌کنند و برای حل چالش مقیاس‌پذیری مناسب هستند.
- معماری زنجیرهٔ بلوکی ترکیبی: راه دیگر برای بهبود مقیاس‌پذیری، استفاده از راه‌حل‌های زنجیرهٔ بلوکی ترکیبی است. زنجیرهٔ بلوکی ترکیبی ویژگی‌های زنجیرهٔ بلوکی عمومی و خصوصی را به ارث می‌برد. زنجیرهٔ بلوکی ترکیبی می‌تواند پردازش تراکنش سریع‌تر و کارآمدتر را فراهم کند و امنیت و حریم خصوصی داده‌ها را تضمین کند.

۲- **بهره‌وری انرژی**: به دلیل تقاضای انرژی و بحران‌ها، تقاضای بهره‌وری برای راه‌حل‌ها و فناوری‌های کارآمد انرژی همچنان در حال افزایش است. موارد زیر برخی از روندها و پیشرفت‌های جدیدی است که احتمالاً جنبه بهره‌وری انرژی اینترنت اشیاء مبتنی بر زنجیرهٔ بلوکی را شکل می‌دهند.

24-Delegated Proof-of Stake

● دستگاه‌های اینترنت اشیاء کم مصرف: دستگاه‌های کم مصرف برای مصرف حداقل انرژی در نظر گرفته شده‌اند، به ویژه دستگاه‌هایی که بر اساس پروتکل‌هایی مانند پروتکل LoRaWAN ساخته شده‌اند. این دستگاه‌ها انرژی کمتری مصرف می‌کنند و می‌توانند برای مدت طولانی‌تری قبل از نیاز به تعویض باتری کار کنند.

● سیستم‌های تجارت و مدیریت انرژی مبتنی بر زنجیرهٔ بلوکی می‌توانند برای بهره‌وری در مصرف انرژی و کاهش هدر رفت انرژی به کار گرفته شوند. با ایجاد چنین سیستم تجارت انرژی همتا به همتا، اتلاف انرژی می‌تواند کاهش یابد و بهره‌وری انرژی با ارائه این امکان به مصرف‌کنندگان برای فروش انرژی اضافی خود به مصرف‌کنندگان دیگر افزایش یابد.

● ابتکارات زنجیرهٔ بلوکی سبز: ابتکارات زنجیرهٔ بلوکی سبز آتی، مانند شبکه چیا، می‌تواند در ساخت شبکه‌های زنجیرهٔ بلوکی سبز و کارآمد از انرژی استفاده شود. هدف آن ایجاد پروتکل‌های زنجیرهٔ بلوکی کارآمدتر و سازگار با محیط‌زیست است.

۳- امنیت و حریم خصوصی: ادغام اینترنت اشیاء با استفاده از زنجیرهٔ بلوکی امنیت و حریم خصوصی را با ارائه حفاظت مناسب در برابر دسترسی غیرمجاز، افشا و دستکاری داده‌های حساس تولید شده توسط این دستگاه‌ها تضمین می‌کند. روندهای تحقیقات آتی که در زمینه امنیت و حریم خصوصی برای سیستم‌های اینترنت اشیاء مبتنی بر زنجیرهٔ بلوکی در حال ظهور بوده است در اینجا ارائه شده است.

● فناوری‌های حفظ حریم خصوصی: تکنیک‌های آینده حفظ حریم خصوصی مانند اثبات دانش صفر (ZKP)[۲۵] و رمزگذاری هومومورفیک، می‌توانند امنیت و حریم خصوصی داده‌های تولید شده توسط دستگاه‌ها و حسگرها در محیط‌های IoT را تکمیل کنند. در هر دوی این تکنیک‌ها، داده‌ها را می‌توان دستکاری و پردازش کرد بدون این که محتویات آن در یک محیط غیرقابل اعتماد قرار گیرد.

راه‌حل‌های هویت غیرمتمرکز: تکنیک‌های مدیریت هویت متمرکز یک مکان واحد را برای مهاجم فراهم می‌کند و بنابراین مستعد سرقت هویت و سایر حملات نقض اطلاعات هستند. در مقابل، راه‌حل‌های هویت غیرمتمرکز، به عنوان مثال، هویت خودمختار (SSI)[۲۶]، می‌تواند راه بهتری برای کنترل هویت کاربران باشد.

۴- قابلیت همکاری: چندین پروتکل و استاندارد متنوع برای دستگاه‌های IoT و زنجیرهٔ بلوکی وجود دارد. این امر باعث می‌شود که موضوع قابلیت همکاری در محیط‌های اینترنت اشیاء مبتنی بر زنجیرهٔ بلوکی بسیار مهم باشد. روندهای آینده برای کمک به قابلیت همکاری در اینترنت اشیاء مبتنی بر زنجیرهٔ بلوکی عبارتند از:

● استانداردسازی: استانداردها و پروتکل‌های مشترک نیازهای ضروری برای ادغام موفقیت‌آمیز زنجیرهٔ بلوکی و اینترنت اشیاء هستند. ابتکار اخیر برای توسعه استانداردهای مشترک توسط چندین نهاد استانداردسازی مانند IEEE و IETF قطعاً به سمت جنبه قابلیت همکاری زنجیرهٔ بلوکی و اینترنت اشیاء حرکت خواهد کرد.

● میان‌افزار: یک چارچوب میان‌افزار مشترک بین دستگاه‌های IoT و زنجیرهٔ بلوکی باید توسعه یابد. تحقیقات بیشتر در این حوزه برای پشتیبانی از ارتباطات و ترجمه یکپارچه بین دستگاه‌های IoT و شبکه‌های زنجیرهٔ بلوکی ضروری است.

۵- محاسبات لبه: محاسبات لبه یک ابتکار محاسباتی نوظهور برای پردازش داده‌های نزدیک‌تر به دستگاه‌های اینترنت اشیاء است. در زیر چند مزیت قابل توجه استفاده از محاسبات لبه در زمینه ادغام زنجیرهٔ بلوکی و اینترنت اشیاء آورده شده است.

● تأخیر کم: ارسال حجم عظیمی از داده‌های تولید شده توسط دستگاه‌های اینترنت اشیاء به یک محیط متمرکز مبتنی بر ابر، تأخیر قابل توجهی را ایجاد می‌کند. تأخیر را می‌توان با استفاده از محاسبات لبه، به طور قابل‌توجهی کاهش داد.

25-Zero Knowledge Proof

26-Self Sovereign Identity

● امنیت و حریم خصوصی داده‌ها: محاسبات لبه اجازه می‌دهد تا داده‌های حساس به صورت محلی پردازش شوند و در نتیجه، قرار گرفتن در معرض تهدیدات داده‌ها در طول انتقال کاهش می‌یابد.

● انطباق و نگرانی‌های نظارتی: در بسیاری از شرایط، داده‌های دستگاه اینترنت اشیاء باید با مقررات صریح منطقه‌ای یا استانداردهای انطباق مطابقت داشته باشد. محاسبات لبه می‌تواند در این زمینه به پشتیبانی از پردازش داده‌ها بر اساس مقررات یا استانداردهای منطقه‌ای در سطح محلی کمک کند.

۱۹- نتیجه‌گیری

در حالی که سیستم‌های IoT کاربردهای متعددی پیدا کرده‌اند، هنوز با چالش‌هایی مانند آسیب‌پذیری‌های امنیتی، غیرقابل اعتماد بودن و تأخیر بالا مواجه هستند. برای رفع این محدودیت‌ها، ادغام محاسبات لبه و زنجیرۀ بلوکی پیشنهاد شده است. با این حال، بررسی جامع استفاده ترکیبی این فناوری‌ها در سیستم‌های IoT وجود ندارد. هدف این مقاله پر کردن این شکاف با ارائه یک تجزیه‌وتحلیل کامل از سیستم‌های لبه مبتنی بر زنجیرۀ بلوکی است، جایی که محاسبات لبه و زنجیرۀ بلوکی برای بهبود عملکرد و امنیت سیستم‌های اینترنت اشیاء با هم کار می‌کنند. در ابتدا مروری بر محاسبات لبه، اینترنت اشیاء و زنجیرۀ بلوکی شده است و در ادامه معماری لبه اینترت اشیاء مبتنی بر زنجیرۀ بلوکی را معرفی کرده‌ایم و سپس موضوعات مربوط به ادغام زنجیرۀ بلوکی و اینترنت اشیاء مانند مدیریت، ارتباطات و امنیت مانند احراز هویت، حریم خصوصی، تشخیص حمله و اعتماد/ اطمینان را مورد بحث قرار داده‌ایم. علاوه بر این، این مقاله به بحث و تجزیه‌وتحلیل مناسب بودن سیستم‌های لبه مبتنی بر زنجیرۀ بلوکی برای کاربردهای مختلف، مانند مراقبت‌های بهداشتی هوشمند، شبکه هوشمند، مدیریت زنجیره تأمین، کشاورزی و انرژی می‌پردازد و سپس با برجسته کردن چالش‌های فعلی مانند مقیاس‌پذیری، مصرف انرژی، حریم خصوصی و امنیت، یکپارچه‌سازی، هزینه و تمرکز و همچنین مسیر آینده برای ادغام موفقیت‌آمیز زنجیرۀ بلوکی و اینترنت اشیاء به پایان می‌رسد.

۲۰- مراجع

1. Gupta, T., & Patel, H. B. 2024. “Integrating Blockchain Technology with Internet of Things and Edge Computing to Achieve Security, Journal of Ecohumanism, Volume: 3, No: 7, pp. 5127–5136.
2. Khan, I., Majib, Y., Ullah, R. & Rana, O. 2024. Blockchain Applications for Internet of Things: A Survey, Journal of IoT, https://doi.org/10.1016/j.iot.101254.
3. Satyanarayanan, M. 2017. The emergence of edge computing. Computer 50 (1), 30–39. http://dx.doi.org/10.1109/ MC. 9.
4. Bonomi, F., Milito, R., Zhu, J. & Addepalli, S. 2012. Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. MCC ’12, Association for Computing Machinery, New York, NY, USA, pp. 13–16.
5. Nawaz, A., Queralta, J. P., Guan, J., Awais, M., Gia, T. N., Bashir, A. K., Kan, H. & Westerlund, T. 2020. Edge computing to secure iot data ownership and trade with the ethereum blockchain. Sensors 20 (14), 3965.
6. Hu, Y. C., Patel, M., Sabella, D., Sprecher, N. & Young, V. 2015. Mobile edge computing a key technology towards 5G. ETSI White Paper 11 (11), 1–16, 2015.
7. Yi, S., Li, C. & Li, Q. 2015. A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data. pp. 37–42.
8. Khan, H. & Masood, T. 2022. Impact of blockchain technology on smart grids. Energies 15 (19), 7189.
9. Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F. & Chaudhry, S. R. 2016. IoT architecture challenges and issues: Lack of standardization, in: Future Technologies Conference, IEEE, pp. 731–738.
10. Yi, X., Yang, X., Kelarev, A., Lam, K.Y. & Tari, Z. 2022. Blockchain Foundations and Applications, Springer Nature.
11. Lastovetska, A. 2016. Blockchain Architecture Basics: Components, Structure, Benefits & Creation, URL https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/.
12. Zhang, C., Wu, C., Wang, X. 2020. Overview of blockchain consensus mechanism, in: International Conference on Big Data Engineering, pp. 7–12.
13. Xue, H., Chen, D., Zhang, N., Dai, H. & Yu, K. July 2023. Integration of blockchain and edge computing in internet of things: A survey, in: Future Generation Computer Systems, Volume 144, P. 307-326.
14. Nyamtiga, B. W., Sicato, J. C., Rathore, S., Sung, Y. & Park, J. H. 2019. Blockchainbased secure storage management with edge computing for IoT, Electronics, 828,

(8).
15. Ren, Y., Leng, Y., Cheng, Y. & Wang, J. 2019. Secure data storage based on blockchain and coding in edge computing, Math. Biosci. Eng. 16, 1874–1892, (4).
16. Qiao, Z., Zhu, C., Wang, Z. & Yang, N. 2019. Anonymous IoT data storage and transaction protocol based on blockchain and edge computing, in: International Conference on Science of Cyber Security, Springer, pp. 181–189.
17. Li, G., Dong, M., Yang, L.T., Ota, K., Wu, J. & Li, J. 2020. Preserving edge knowledge sharing among IoT services: A blockchain-based approach, IEEE Trans. Emerg. Top. Comput. Intell. 4, 653–665, (5).
18. Sharma, V., You, I., Jayakody, D. N., Reina, D. G., Choo, K. K. R. 2019. Neural blockchain- based ultrareliable caching for edge-enabled UAV networks, IEEE Trans. Ind. Inform. 15, 5723–5736, (10).
19. Zhang, P., Pang, X., Kumar, N., Aujla, G.S. & Cao, H. 2020. A reliable datatransmission mechanism using blockchain in edge computing scenarios, IEEE Internet Things J.
20. Jiang, Y., Bai, H. & Yang, H. 2019.The messaging model design based blockchain and edge computing for the internet of things, in: 2019 IEEE 10th International Conference on Software Engineering and Service Science, ICSESS, IEEE, pp. 604–608.
21. Bai, H., Jiang, Y., Yang, H. & Xia, G. 2019.The messaging protocols analysis of integrating blockchain and edge computing for IoT, in: 2019 IEEE 10th International Conference on Software Engineering and Service Science, ICSESS, IEEE, pp. 99–102.
22. Guo, S., Hu, X., Guo, S., Qiu, X. & Qi, F. 2020. "Blockchain meets edge computing: A distributed and trusted authentication system," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1972–1983.
23. Mahmood, K., Li, X., Chaudhry, S. A., Naqvi, H., Kumari, S., A. Sangaiah, K. & Rodrigues, J. J. 2018. "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," Future Generation Computer Systems, vol. 88, pp. 491–500.
24. Liu, H., Zhang, P., Pu, G., Yang, T., Maharjan, S. & Zhang, Y. 2020. "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing", IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4221–4232.
25. Gai, K., Wu, Y., Zhu, L., Xu, L. & Zhang, Y. 2019. "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7992–8004.
26. Wan, J., Li, J., Imran, M. & Li, D. 2019. "A blockchain-based solution for enhancing security and privacy in smart factory," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3652–3660.
27. Lin, G.-Y., He, S., Huang, H., Wu, J.-Y. & Chen, W. 2012. "Access control security model based on behavior in cloud computing environment," Journal of China Institute of Communications, vol. 33, no. 3, pp. 59– 66.
28. Pyoung C. K. & Baek, S. J. 2019. "Blockchain of finite-lifetime blocks with applications to edge-based IoT," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2102–2116.
29. Pu, Y., Hu, C., Deng, S. & Alrawais, A. 2020. "Rpeds: A recoverable and revocable privacy-preserving edge data sharing scheme," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8077–8089.
30. Nkenyereye, L., Adhi Tama, B., Shahzad, M. K. & Choi, Y.-H. 2020. "Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing," Sensors, vol. 20, no. 1, p. 154.
31. Zhaofeng, M., Xiaochang, W., Jain, D. K., Khan, H., Hongmin, G. & Zhen, W. 2019. "A blockchain-based trusted data management scheme in edge computing," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2013–2021.
32. Xiao, L., Ding, Y., Jiang, D., Huang, J., Wang, D., Li, J. & Poor, H. V. 2020. "A reinforcement learning and blockchain-based trust mechanism for edge networks," IEEE Transactions on Communications, vol. 68, no. 9, pp. 5460–5470.
33. Cui, L., Yang, S., Chen, Z. 2019. 2019. "A decentralized and trusted edge computing platform for Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3910- 3922.
34. Robles, R. J. & Kim, T. h. 2010. Applications, systems and methods in smart home technology: Int. J. Adv. Sci. Technol. 15, 37–48.
35. Tan, K.C. 2002. Supply chain management: practices, concerns, and performance issues, J. Supply Chain Manag. 38 (4) 42–53.
36. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D. & McCallum, P. 2019. Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renew. Sustain. Energy Rev. 100, 143–174.
37. Wongthongtham, P., Marrable, D., Abu-Salih, B., Liu, X. & Morrison, G. 2021. Blockchain-enabled Peer-to-Peer energy trading, Comput. Electr. Eng. 94, 107299.
38. Barbieri, M. & Gassen, D. 2017. Blockchain-can this new technology really revolutionize the land registry system, in: Responsible Land Governance: Towards an Evidence Based Approach: Proceedings of the Annual World Bank Conference, pp. 113.
39. Kshetri, N. 2021. Blockchain-based smart contracts to provide crop insurance for smallholder farmers in developing countries, IT Prof. 23, 58–61, (6).

۴۰. رضایی، م. ر. و دشتی، س. ا. ۱۴۰۳. «چارچوب بلوک چین فازی هوشمند ایمن برای محاسبات لبه و مه تقویت شده با هوش مصنوعی»، نهمین همایش ملی مطالعات و تحقیقات نوین در حوزه علوم کامپیوتر، برق و مکانیک ایران.. ۱۴۰۳

۴۱. موحدی، ز. و فولادی قلعه ک. ۱۴۰۰. «تخصیص منابع در محاسبات لبه ای با استفاده از زنجیره ی بلوکی»، هفتمین کنفرانس بین المللی وب پژوهی.

۴۲. قهرمانی، ح. و ولائی، م. ۱۴۰۲. «مروری بر ترکیب اینترنت اشیاء صنعتی و بلوکچین»، نهمین کنفرانس بین المللی مهندسی برق، کامپیوتر و مکانیک.