"مقاله مروری ادغام بلاک چین و شبکه های تعریف شده در نرم افزار برای اینترنت اشیا"

دکتر محمدرضا ملاخلیلی میبدی، ناهید نادری زاد[۲]

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

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

چکیده

اینترنت اشیا (IoT) با فراهم‌سازی بستری برای ارتباط و تعامل گسترده میان دستگاه‌ها، تحولی چشمگیر در حوزه‌های مختلفی مانند مراقبت‌های بهداشتی، کشاورزی، شهرهای هوشمند و اتوماسیون صنعتی ایجاد کرده است. با این حال، افزایش تعداد دستگاه‌های متصل، چالش‌های امنیتی متعددی از جمله تهدیدات سایبری، عدم احراز هویت ایمن و نقض یکپارچگی داده‌ها را به همراه داشته است. در این راستا، فناوری بلاک چین به عنوان یک راهکار نویدبخش، با بهره‌گیری از ویژگی‌های غیرمتمرکز، تغییرناپذیر و شفاف خود، امکان بهبود امنیت و اعتماد در اکوسیستم IoT را فراهم می‌آورد. این مقاله مروری به بررسی ادغام بلاک چین و شبکه‌های نرم‌افزارمحور (SDN) در چارچوب اینترنت اشیا می‌پردازد و یک سیستم مدیریت هویت غیرمتمرکز را برای دستگاه‌های IoT پیشنهاد می‌کند. همچنین، چالش‌های ناشی از افزایش تعداد دستگاه‌های متصل، اهمیت احراز هویت ایمن و حفظ یکپارچگی داده‌ها را مورد تحلیل قرار می‌دهد. در نهایت، با مرور پژوهش‌های اخیر، چالش‌های موجود، فرصت‌های تحقیقاتی و مسیرهای آینده برای توسعه سیستم‌های نوین امنیتی در اینترنت اشیا مبتنی بر بلاک چین و SDN تبیین می‌گردد.

واژه‌های کلیدی: اینترنت اشیا(IoT) ، بلاک چین(BC) ، شبکه‌های نرم‌افزارمحور(SDN) .

۱- مقدمه

با پیشرفت فناوری و گسترش اینترنت اشیا(IoT) ، تعداد دستگاه‌های متصل به شبکه‌های ارتباطی به‌طور چشمگیری افزایش یافته است. این دستگاه‌ها، که در حوزه‌هایی مانند مراقبت‌های بهداشتی، حمل‌ونقل هوشمند، کشاورزی، و صنعت مورد استفاده قرار می‌گیرند، نیازمند یک زیرساخت ارتباطی کارآمد، امن و مقیاس‌پذیر هستند .(S. W. Turner et al, ۲۰۲۳) با این حال، IoT چالش‌های متعددی از جمله مدیریت متمرکز، ضعف در احراز هویت، کنترل دسترسی، و تهدیدات امنیتی را به همراه دارد. به دلیل معماری توزیع‌شده و منابع محدود بسیاری از دستگاه‌هایIoT ، رویکردهای امنیتی سنتی مانند فایروال‌ها و سامانه‌های شناسایی نفوذ (IDS) دیگر کارایی لازم را ندارند.(M. Karakus et al, ۲۰۲۳)

برای غلبه بر این چالش‌ها، ترکیب شبکه‌های نرم‌افزارمحور (SDN) و بلاک چین (BC) به عنوان یک راهکار نوین پیشنهاد شده است. SDN با جداسازی لایه کنترل از لایه داده، امکان مدیریت پویا، متمرکز و انعطاف‌پذیر شبکه را فراهم می‌کند و بهبود عملکرد و مقیاس‌پذیری را به همراه دارد .(E. Guler et al, ۲۰۲۳) از سوی دیگر، بلاک چین با ویژگی‌های غیرمتمرکز، تغییرناپذیر و شفاف خود، سطح بالایی از امنیت، احراز هویت و یکپارچگی داده را برای شبکه‌های IoT تضمین می‌کند (S. Uludag et al, ۲۰۲۳) .

ادغام این دو فناوری، که از آن به‌عنوان IoT مبتنی بر بلاک چین و SDN (BC-SDIoT) یاد می‌شود، راهکاری مؤثر برای بهبود امنیت، کاهش هزینه‌های مدیریت شبکه، و افزایش قابلیت اطمینان سیستم‌های IoT ارائه می‌دهد.

تحقیقات اخیر نشان داده‌اند که استفاده از بلاک چین در معماری SDN می‌تواند به بهبود امنیت سایبری IoT کمک کند. به عنوان مثال، برخی مطالعات پیشنهاد داده‌اند که از قراردادهای هوشمند برای کنترل خودکار دسترسی و احراز هویت دستگاه‌های IoT استفاده شود. (S.W.Turner et al, ۲۰۲۳) همچنین، ترکیب SDN و بلاک چین در شبکه‌های IoT منجر به بهینه‌سازی مصرف منابع و کاهش تأخیر در پردازش داده‌ها می‌شود، زیرا SDN امکان مدیریت کارآمد جریان داده‌ها را فراهم کرده و بلاک چین از طریق ثبت تغییرناپذیر تراکنش‌ها، از جعل و حملات سایبری جلوگیری می‌کند.(M. Karakus et al, ۲۰۲۳)

با وجود مزایای قابل‌توجهBC-SDIoT ، چالش‌های متعددی همچنان باقی مانده است که باید مورد بررسی قرار گیرند. از جمله این چالش‌ها می‌توان به سربار پردازشی ناشی از اجرای الگوریتم‌های اجماع بلاک چین، مقیاس‌پذیری محدود، و مسائل مربوط به حریم خصوصی اشاره کرد.(E. Guler et al, ۲۰۲۳) بنابراین، این مقاله مروری به بررسی جامع پژوهش‌های اخیر در زمینه ترکیب بلاک چین و SDN در اینترنت اشیا پرداخته و مزایا، چالش‌ها و مسیرهای آینده تحقیقاتی را تحلیل می‌کند.

ساختار مقاله به شرح زیر است :در بخش دوم، مفاهیم پایه SDN و بلاک چین مورد بررسی قرار می‌گیرند. بخش سوم، انگیزه‌ها و دلایل استفاده از BC-SDIoT را تحلیل می‌کند. در بخش چهارم، مطالعات مرتبط در زمینه ترکیب SDN و بلاک چین در شبکه‌های IoT مرور می‌شود. در بخش پنجم، دسته‌بندی پژوهش‌های انجام‌شده بر اساس اهداف پیاده‌سازی ارائه خواهد شد. در بخش ششم، چالش‌های موجود و مسیرهای تحقیقاتی آینده بررسی شده و در نهایت، بخش هفتم نتیجه‌گیری مقاله را ارائه می‌دهد.

۲- بررسی مفاهیم پایه SDN و بلاک چین

۲-۱- شبکه‌های نرم‌افزارمحور (SDN)

شبکه‌های نرم‌افزارمحور (Software-Defined Networking - SDN) یکی از مهم‌ترین پیشرفت‌ها در معماری شبکه‌های مدرن محسوب می‌شوند که هدف اصلی آن‌ها، جداسازی لایه کنترل از لایه داده است. در معماری سنتی شبکه‌ها، کنترل و مدیریت ترافیک به‌صورت توزیع‌شده توسط تجهیزات مختلف مانند روترها و سوئیچ‌ها انجام می‌شود، اما درSDN ، این وظایف به یک کنترل‌کننده مرکزی سپرده می‌شود که امکان مدیریت و پیکربندی پویای شبکه را فراهم می‌کند. (S. W. Turner et al, ۲۰۲۳)

۲-۱-۱. معماری SDN

معماری SDN از سه لایه اصلی تشکیل شده است :

۱. **لایه داده : (Data Plane)** شامل تجهیزات فیزیکی و مجازی شبکه مانند سوئیچ‌ها و روترها است که وظیفه پردازش و ارسال بسته‌های داده را بر عهده دارند .

۲. **لایه کنترل : (Control Plane)** شامل کنترل‌کننده SDN است که تصمیمات مربوط به مسیریابی و مدیریت جریان داده‌ها را اتخاذ می‌کند. این کنترل‌کننده از پروتکل‌هایی مانند OpenFlow برای برقراری ارتباط با تجهیزات لایه داده استفاده می‌کند (S. W. Turner et al, ۲۰۲۳)

۳. **لایه کاربرد : (Application Plane)** شامل برنامه‌ها و سرویس‌های شبکه‌ای است که از قابلیت‌های SDN برای مدیریت بهتر شبکه بهره می‌برند .

۲-۱-۱. مزایا و چالش‌های SDN

از جمله مزایای SDN می‌توان به انعطاف‌پذیری بالا، مدیریت متمرکز، پویایی در تغییر پیکربندی و بهینه‌سازی کارایی شبکه اشاره کرد. همچنین، SDNامکان بهبود امنیت شبکه را از طریق اعمال سیاست‌های متمرکز فراهم می‌کند. (S. W. Turner et al,۲۰۲۳) با این حال، چالش‌هایی مانند متمرکز بودن کنترل‌کننده که می‌تواند نقطه‌ای حساس برای حملات باشد، مقیاس‌پذیری محدود و نیاز به استانداردسازی در پیاده‌سازی‌های مختلف، از موانع اصلی گسترش SDN به شمار می‌آیند.

۲-۲- بلاک چین (Blockchain)

بلاک چین یک فناوری دفترکل توزیع‌شده است که امکان ثبت و ذخیره‌سازی داده‌ها را به‌صورت غیرقابل‌تغییر و بدون نیاز به یک مرجع مرکزی فراهم می‌کند. این فناوری برای اولین بار در سال ۲۰۰۸ توسط بیت‌کوین معرفی شد و از آن زمان تاکنون در حوزه‌های مختلفی مانند امور مالی، زنجیره تأمین و اینترنت اشیا مورد استفاده قرار گرفته است.(S. W. Turner et al, ۲۰۲۳)

۲-۲-۱. ساختار بلاک چین

بلاک چین شامل مجموعه‌ای از بلوک‌ها است که به‌صورت زنجیره‌ای به یکدیگر متصل شده‌اند. هر بلوک شامل اطلاعات تراکنش‌ها، یک زمان‌سنج، هش بلوک قبلی و یک هش منحصربه‌فرد است که امنیت و یکپارچگی داده‌ها را تضمین می‌کند. مکانیزم اجماع،

مانند اثبات کار (Proof of Work - PoW) و اثبات سهام(Proof of Stake - PoS) ، در بلاک چین به‌کار گرفته می‌شود تا از صحت داده‌ها اطمینان حاصل شود. (S. W. Turner et al, ۲۰۲۳)

۲-۲-۲. مزایا و چالش‌های بلاک چین

از جمله مزایای بلاک چین می‌توان به شفافیت، غیرمتمرکز بودن، تغییرناپذیری و امنیت بالا اشاره کرد. این ویژگی‌ها بلاک چین را به گزینه‌ای مناسب برای تضمین امنیت و حریم خصوصی در شبکه‌های IoT تبدیل می‌کند. با این حال، چالش‌هایی نظیر مقیاس‌پذیری، مصرف بالای انرژی و تأخیر در پردازش تراکنش‌ها، از موانع گسترش این فناوری محسوب می‌شوند. (S. W. Turner et al, ۲۰۲۳)

۲-۳- ترکیب SDN و بلاک چین در اینترنت اشیا

ادغام SDN و بلاک چین در اینترنت اشیا می‌تواند نقاط ضعف هر یک از این فناوری‌ها را کاهش دهد .SDN با ارائه مدیریت متمرکز و انعطاف‌پذیر، عملکرد شبکه را بهبود می‌بخشد، در حالی که بلاک چین امنیت و اعتماد را در این محیط غیرمتمرکز افزایش می‌دهد. با ترکیب این دو فناوری، می‌توان راهکارهای نوینی برای مقابله با چالش‌های امنیتی، احراز هویت غیرمتمرکز و مدیریت داده‌های IoT ارائه کرد (S.W.Turner et al, ۲۰۲۳) .

۳- تحلیل انگیزه‌ها و دلایل استفاده از BC-SDIoT

ادغام فناوری بلاک چین (BC) و شبکه‌های نرم‌افزارمحور (SDN) در اینترنت اشیا (IoT) به عنوان یک رویکرد نویدبخش برای حل چالش‌های امنیتی، مدیریت شبکه و مقیاس‌پذیری در محیط‌های پیچیده مطرح شده است. در این بخش، دلایل اصلی استفاده از BC-SDIoT را بررسی کرده و به تحلیل مزایا و انگیزه‌های کلیدی این ترکیب می‌پردازیم.

۳-۱- افزایش امنیت و کاهش تهدیدات سایبری

امنیت یکی از مهم‌ترین چالش‌های اینترنت اشیا است، زیرا دستگاه‌های IoT به دلیل منابع محاسباتی محدود، اغلب فاقد مکانیزم‌های امنیتی قوی هستند .(S. W. Turner et al, ۲۰۲۳) بلاک چین با ساختار غیرمتمرکز و تغییرناپذیر خود، امکان ثبت و ذخیره‌سازی امن داده‌ها را فراهم کرده و از حملاتی مانند جعل هویت، حملات مرد میانی (MITM) و دستکاری داده‌ها جلوگیری می‌کند .(M. H. H. Sedjelmaci et al, ۲۰۲۱) از سوی دیگر، SDNبا جدا کردن لایه کنترل از لایه داده، امکان نظارت و مدیریت هوشمند بر ترافیک شبکه را ایجاد کرده و در ترکیب با بلاک چین، قابلیت شناسایی و واکنش سریع به تهدیدات را افزایش می‌دهد.(A. S. Alharbi et al, ۲۰۲۲)

۳-۲- بهبود مدیریت هویت و کنترل دسترسی

یکی از چالش‌های اساسی در اینترنت اشیا، احراز هویت و کنترل دسترسی ایمن برای تعداد زیادی از دستگاه‌های متصل است. رویکردهای سنتی مدیریت هویت معمولاً متمرکز بوده و دارای نقاط شکست و آسیب‌پذیری هستند .(L. Xu et al, ۲۰۲۱) بلاک چین امکان ایجاد یک سیستم مدیریت هویت غیرمتمرکز (DID) را فراهم می‌کند که در آن دستگاه‌های IoT می‌توانند از

طریق قراردادهای هوشمند و کلیدهای رمزنگاری، هویت خود را تأیید کرده و به شبکه دسترسی پیدا کنند (S. W. Turner et al, ۲۰۲۳). علاوه بر این، SDNبا توانایی تعریف قوانین کنترلی پویا، می‌تواند در کنترل بهتر دسترسی و جلوگیری از نفوذ غیرمجاز نقش موثری ایفا کند.(Y. Zhang et al, ۲۰۲۰)

۳-۳- بهینه‌سازی عملکرد و مقیاس‌پذیری

با افزایش تعداد دستگاه‌هایIoT ، نیاز به مدیریت کارآمد منابع شبکه بیش از پیش احساس می‌شود SDN .امکان مدیریت متمرکز و پویا را فراهم کرده و از این طریق به بهینه‌سازی جریان داده و کاهش تأخیر کمک می‌کند (X. Wang et al, ۲۰۲۱) .در همین راستا، بلاک چین می‌تواند به عنوان یک دفتر کل توزیع‌شده برای ذخیره‌سازی و تأیید داده‌های شبکه مورد استفاده قرار گیرد، بدون اینکه نیاز به سرورهای متمرکز باشد .(S. W. Turner et al, ۲۰۲۳) به‌کارگیری این دو فناوری در کنار یکدیگر، علاوه بر افزایش قابلیت اعتماد در انتقال داده‌ها، می‌تواند مشکلات ناشی از بار اضافی پردازشی و تأخیر در شبکه‌های IoT را کاهش دهد.(H. Kim et al, ۲۰۲۲)

۳-٤- افزایش قابلیت اعتماد و تحمل‌پذیری خطا

بلاک چین با ماهیت غیرمتمرکز خود، از یک نقطه شکست واحد جلوگیری کرده و داده‌ها را در تمامی گره‌های شبکه همگام‌سازی می‌کند، که این امر موجب افزایش قابلیت اعتماد سیستم‌های IoT می‌شود .(B. Li et al, ۲۰۲۱) همچنین، SDNبا داشتن کنترلرهای هوشمند، امکان تغییر مسیر ترافیک در صورت خرابی یک مسیر را فراهم کرده و از این طریق تحمل‌پذیری خطا را بهبود می‌بخشد .(S. W. Turner et al, ۲۰۲۳) ترکیب این دو فناوری، نه‌تنها به کاهش قطعی‌های شبکه کمک می‌کند، بلکه موجب افزایش تاب‌آوری در برابر حملات سایبری نیز می‌شود.(R. K. Gupta et al, ۲۰۲۲)

۳-۵- افزایش شفافیت و قابلیت حسابرسی

یکی دیگر از انگیزه‌های کلیدی برای استفاده ازBC-SDIoT ، افزایش شفافیت و امکان حسابرسی برای داده‌های IoT است. بلاک چین یک دفتر کل تغییرناپذیر ایجاد می‌کند که تمامی تراکنش‌های شبکه را ثبت کرده و از این طریق امکان ردیابی و حسابرسی داده‌ها را فراهم می‌آورد .(J. Park et al, ۲۰۲۱) این ویژگی برای کاربردهایی مانند زنجیره تأمین هوشمند، مدیریت داده‌های بهداشتی و امنیت سایبری بسیار مفید است .(S. W. Turner et al, ۲۰۲۳) در کنار آن، SDNقابلیت تنظیم سیاست‌های امنیتی و مدیریت پویا را فراهم کرده و از این طریق کنترل بهتری بر ترافیک و پردازش داده‌ها ارائه می‌دهد. (Y. Shen et al, ۲۰۲۰)

۳-٦- چالش‌های موجود و مسیرهای آینده

با وجود مزایای ذکر شده، پیاده‌سازی BC-SDIoT همچنان با چالش‌هایی از جمله مصرف بالای منابع محاسباتی در بلاک چین، نیاز به طراحی الگوریتم‌های اجماع سبک، و مسائل مرتبط با هماهنگ‌سازی میان کنترلرهای SDN مواجه است (S. W. Turner et al, ۲۰۲۳). از این رو، تحقیقات آینده باید بر روی توسعه مدل‌های بهینه برای کاهش سربار پردازشی، بهبود روش‌های رمزنگاری سبک‌وزن و ایجاد پروتکل‌های ارتباطی کارآمدتر تمرکز کنند.(X. Zhao et al, ۲۰۲۲)

ادغام بلاک چین و SDN در اینترنت اشیا به عنوان یک راهکار مؤثر برای بهبود امنیت، مدیریت هویت، مقیاس‌پذیری و اعتمادپذیری سیستم‌های IoT شناخته شده است. ترکیب این دو فناوری، علاوه بر افزایش کارایی شبکه، امکان مقابله با تهدیدات سایبری و بهینه‌سازی کنترل دسترسی را فراهم می‌آورد. با این حال، بهینه‌سازی مصرف منابع و هماهنگ‌سازی بهتر این فناوری‌ها از جمله چالش‌هایی است که نیازمند تحقیقات بیشتر است. مسیرهای تحقیقاتی آینده می‌توانند بر توسعه الگوریتم‌های اجماع سبک، کاهش سربار پردازشی و بهبود روش‌های مدیریت هویت غیرمتمرکز متمرکز شوند تا BC-SDIoT بتواند به عنوان یک استاندارد جامع در اینترنت اشیا مورد استفاده قرار گیرد.

٤- مرور مطالعات مرتبط در زمینه ترکیب SDN و بلاک چین در شبکه‌های IoT

این بخش مطالعات مرتبط در زمینه ترکیب SDN و بلاک چین در شبکه‌های IoT را بررسی کرده و به مزایا و چالش‌های هر یک پرداخته است. در بخش‌های بعدی، روش‌های ادغام این دو فناوری در اینترنت اشیا و تأثیرات آن‌ها بر امنیت و عملکرد شبکه مورد بررسی قرار خواهند گرفت .

٤-١- شبکه‌های نرم‌افزارمحور(SDN)

شبکه‌های نرم‌افزارمحور (SDN) یک معماری نوین در مدیریت و کنترل شبکه‌های کامپیوتری هستند که با جداسازی لایه کنترل از لایه داده، مدیریت شبکه را تسهیل می‌کنند. در معماری SDN ، کنترل‌کننده مرکزی، تصمیم‌گیری‌های مربوط به جریان داده‌ها را انجام داده و تجهیزات شبکه مانند سوییچ‌ها و روترها صرفاً وظیفه ارسال بسته‌های داده را بر عهده دارند. (S. W. Turner et al., ۲۰۲۳) این معماری به دلیل ویژگی‌هایی همچون مدیریت متمرکز، پیکربندی پویا، بهبود امنیت و افزایش انعطاف‌پذیری، به‌عنوان یک رویکرد مؤثر در شبکه‌های مدرن مطرح شده است.

یکی از مهم‌ترین استانداردهای مورد استفاده در SDN ، **پروتکل OpenFlow** است که به کنترل‌کننده اجازه می‌دهد تا مستقیماً مسیرهای داده را در سوئیچ‌های شبکه مدیریت کند .(M. Al-Fares et al., ۲۰۱۰) این ویژگی باعث می‌شود که شبکه‌های SDN در مقایسه با معماری‌های سنتی، مدیریت بهتری بر ترافیک شبکه و تخصیص منابع داشته باشند. (N. McKeown et al., ۲۰۰۸)

مزایای SDN :

- **مدیریت متمرکز :** تسهیل کنترل شبکه از طریق یک کنترل‌کننده مرکزی.
- **افزایش امنیت :**توانایی پیاده‌سازی سیاست‌های امنیتی در سطح کنترل شبکه.
- **انعطاف‌پذیری بالا :**قابلیت تغییر مسیرهای شبکه بدون نیاز به تغییر سخت‌افزاری.
- **بهینه‌سازی عملکرد :**امکان بهبود توزیع ترافیک و جلوگیری از ازدحام شبکه.(S. W. Turner et al., ۲۰۲۳)

با این حال،SDN نیز با چالش‌هایی همراه است که از جمله آن‌ها می‌توان به مقیاس‌پذیری محدود، وابستگی به کنترل‌کننده مرکزی، و تهدیدات امنیتی مرتبط با حملات به کنترل‌کننده SDN اشاره کرد. (J. Fu et al., ۲۰۱۷) یکی از راهکارهای نوین برای بهبود امنیتSDN ، ادغام آن با فناوری بلاک چین است که در ادامه بررسی می‌شود.

٤-۲- فناوری بلاک چین(Blockchain)

بلاک چین یک دفتر کل توزیع‌شده و غیرقابل تغییر است که اطلاعات را به صورت بلوک‌های زنجیره‌ای ذخیره می‌کند. این فناوری در ابتدا برای رمزارز بیت‌کوین معرفی شد (S. Nakamoto, ۲۰۰۸) اما به سرعت در حوزه‌های مختلف از جمله امنیت شبکه، اینترنت اشیا و مدیریت داده‌ها گسترش یافت. بلاک چین با استفاده از مکانیزم‌های رمزنگاری و الگوریتم‌های اجماع، امنیت و شفافیت را در پردازش تراکنش‌ها تضمین می‌کند.(X. Liang et al., ۲۰۱۸)

٤-۲-۱. ویژگی‌های کلیدی بلاک چین:

- **غیرمتمرکز بودن :** حذف نیاز به نهادهای واسطه در پردازش و ذخیره اطلاعات.
- **تغییرناپذیری :** عدم امکان تغییر یا حذف داده‌های ذخیره‌شده در زنجیره بلوک‌ها.
- **شفافیت و امنیت :** تمامی تراکنش‌ها به صورت عمومی قابل مشاهده و تأیید هستند.
- **مقاومت در برابر حملات :** استفاده از رمزنگاری و مکانیزم‌های اجماع برای تأمین امنیت (S. W. Turner et al., ۲۰۲۳).

٤-۲-۲. مکانیزم‌های اجماع در بلاک چین:

برای حفظ امنیت و توافق بین نودهای شبکه، بلاک چین از الگوریتم‌های اجماع مانند **اثبات کار(PoW) ، اثبات سهام (PoS)، و اثبات اعتبار (PoA)** استفاده می‌کند. (G. Wood, ۲۰۱۵) این الگوریتم‌ها تضمین می‌کنند که تنها تراکنش‌های معتبر در زنجیره بلاک قرار می‌گیرند.

٤-۳- ادغام SDN و بلاک چین

با توجه به چالش‌های امنیتیSDN ، ترکیب این فناوری با بلاک چین به عنوان یک راهکار نوین برای افزایش امنیت و اعتماد در شبکه‌های نرم‌افزارمحور مطرح شده است .(S. W. Turner et al., ۲۰۲۳) بلاک چین می‌تواند به عنوان یک **مکانیزم توزیع‌شده برای ذخیره قوانین کنترل شبکه، ثبت رویدادهای امنیتی، و جلوگیری از تغییرات غیرمجاز در زیرساخت SDN**مورد استفاده قرار گیرد . (A.Reyna et al., ۲۰۱۸)

مزایای ادغام SDN و بلاک چین:

- **افزایش امنیت :** جلوگیری از حملات به کنترل‌کننده مرکزی SDN .

- **یکپارچگی داده‌ها :** ثبت تمامی تغییرات و سیاست‌های شبکه در یک دفتر کل تغییرناپذیر.
- **مدیریت غیرمتمرکز :** توزیع کنترل و کاهش وابستگی به یک نقطه مرکزی.
- **بهبود اعتماد :** استفاده از قراردادهای هوشمند برای اجرای سیاست‌های شبکه.(Z. Li et al., ۲۰۲۰)

SDN و بلاک چین هر دو فناوری‌های کلیدی در تحول شبکه‌های مدرن محسوب می‌شوند. SDN با ارائه مدیریت پویا و متمرکز، انعطاف‌پذیری شبکه را افزایش می‌دهد، در حالی که بلاک چین با ساختار غیرمتمرکز و مقاوم در برابر تغییر، می‌تواند امنیت و یکپارچگی داده‌ها را تضمین کند. ترکیب این دو فناوری، راهکاری قدرتمند برای مقابله با چالش‌های امنیتی شبکه‌های IoT ارائه می‌دهد و بستری مناسب برای توسعه زیرساخت‌های ارتباطی آینده فراهم می‌کند.

۵- دسته‌بندی پژوهش‌های انجام‌شده بر اساس اهداف پیاده‌سازی

ادغام فناوری بلاک چین (BC) و شبکه‌های نرم‌افزارمحور (SDN) در اینترنت اشیا (IoT) رویکردی نوین برای بهبود امنیت، مدیریت داده‌ها و کارایی شبکه محسوب می‌شود. در سال‌های اخیر، پژوهش‌های متعددی در این زمینه انجام شده که می‌توان آن‌ها را بر اساس اهداف پیاده‌سازی به چند دسته کلی تقسیم کرد. در ادامه، یک دسته‌بندی جامع از این پژوهش‌ها ارائه شده است که بر مبنای بررسی مطالعات اخیر، شکل گرفته است.

۵-۱- امنیت

یکی از مهم‌ترین اهداف ادغام بلاک چین و SDN درIoT ، افزایش امنیت شبکه و مقابله با تهدیدات سایبری است. بسیاری از پژوهش‌ها به بررسی روش‌های تشخیص و مقابله با حملات توزیع‌شده منع سرویس(DDoS) ، جعل هویت، و حملات تزریق داده پرداخته‌اند. به عنوان مثال، برخی مطالعات از قراردادهای هوشمند برای اجرای سیاست‌های امنیتی در کنترلرهای SDN استفاده کرده‌اند . (S. W. Turner et al, ۲۰۲۳) همچنین، برخی پژوهش‌ها از روش‌های یادگیری ماشین برای تشخیص رفتارهای غیرعادی در ترافیک شبکه بهره گرفته‌اند.

۵-۲- مدیریت اعتماد

اعتماد میان دستگاه‌های IoT یکی از چالش‌های اساسی در شبکه‌های توزیع‌شده است. پژوهش‌های مختلفی به استفاده از بلاک چین برای مدیریت اعتماد در محیط‌های IoT پرداخته‌اند. در این راستا، برخی مطالعات از مدل‌های مبتنی بر امتیازدهی و رأی‌گیری در بلاک چین برای ارزیابی اعتبار دستگاه‌ها و کاربران استفاده کرده‌اند .(S. W. Turner et al, ۲۰۲۳) همچنین، برخی روش‌ها ترکیبی از BC و SDN را برای بهبود امنیت داده‌ها و جلوگیری از فعالیت‌های مخرب پیشنهاد داده‌اند.

۵-۳- احراز هویت و کنترل دسترسی

احراز هویت غیرمتمرکز و کنترل دسترسی از دیگر اهداف پیاده‌سازی BC-SDN در IoT است. در این زمینه، بسیاری از مطالعات به استفاده از بلاک چین برای ذخیره و مدیریت کلیدهای رمزنگاری‌شده دستگاه‌ها و کاربران پرداخته‌اند. برخی پژوهش‌ها

معماری‌هایی را پیشنهاد داده‌اند که از SDN برای مدیریت دسترسی به منابع شبکه و از بلاک چین برای ثبت و تأیید هویت کاربران استفاده می‌کنند.(S. W. Turner et al, ۲۰۲۳)

۵-٤- حریم خصوصی و یکپارچگی داده

حفظ حریم خصوصی کاربران و یکپارچگی داده‌های IoT یکی دیگر از اهداف کلیدی پژوهش‌های اخیر بوده است. بلاک چین با ارائه یک دفتر کل توزیع‌شده، امکان ذخیره‌سازی تغییرناپذیر داده‌ها را فراهم می‌کند و SDN می‌تواند با تنظیم قوانین ترافیکی مناسب، از افشای اطلاعات حساس جلوگیری کند. برخی پژوهش‌ها از روش‌های رمزنگاری پیشرفته همراه با BC-SDN برای افزایش امنیت داده‌ها استفاده کرده‌اند.(S. W. Turner et al, ۲۰۲۳)

۵-۵- بهبود کارایی شبکه

یکی از چالش‌هایIoT ، مدیریت منابع شبکه و بهینه‌سازی عملکرد آن است SDN .با ارائه کنترل مرکزی و امکان تغییر پویای مسیرهای ترافیکی، می‌تواند کارایی شبکه را بهبود دهد. برخی مطالعات پیشنهاد داده‌اند که ترکیب SDN با بلاک چین می‌تواند مدیریت بهتری بر توزیع داده‌ها و تخصیص منابع ارائه دهد.(S. W. Turner et al, ۲۰۲۳)

۵-٦- رایانش مه و لبه

رایانش مه و لبه به عنوان راهکاری برای پردازش محلی داده‌های IoT و کاهش تأخیر شبکه مورد توجه قرار گرفته است. برخی پژوهش‌ها از SDN برای مدیریت ارتباط میان گره‌های لبه و از بلاک چین برای ثبت سوابق پردازشی و حفظ امنیت داده‌ها استفاده کرده‌اند.(S. W. Turner et al, ۲۰۲۳)

۵-۷- ادغام بلاک چین با اینترنت اشیا

حریم خصوصی داده‌ها، امنیت، یکپارچگی و مقیاس‌پذیری از 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 [R.S. Velamakanni,۲۰۲٤] , [M. Kumaresan,۲۰۲۲] ,[T. Wang,۲۰۲٤] 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] نیز 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 این جدول، از چندین مقاله بررسی شده که طی سال‌های ۲۰۱۷-۲۰۲۴ منتشر شده‌اند، استفاده شده است.

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

مرجع	نویسنده	سال	موضوع تمرکز	فواید	محدودیت‌ها
[۱۳]	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
[۱۴]	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.
[۱۵]	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
[۱۶]	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
[۱۷]	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
[۱۸]	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.

[۱۹]	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.
[۲۰]	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.
[۲۱]	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
[۲۲]	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.
[۲۳]	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.
[۲۴]	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
[۲۵]	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.
[۲۶]	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

[۲۷]	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. 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.

با توجه به بررسی‌های انجام‌شده، ترکیب بلاک چین و SDN در IoT می‌تواند در حل چالش‌های امنیتی، مدیریتی و عملکردی این حوزه نقش بسزایی داشته باشد. با این حال، همچنان چالش‌هایی مانند مقیاس‌پذیری، مصرف انرژی و پیچیدگی‌های پیاده‌سازی این رویکرد نیازمند تحقیقات بیشتر است. پژوهش‌های آینده می‌توانند بر توسعه مدل‌های سبک‌تر بلاک چین، بهینه‌سازی الگوریتم‌های اجماع، و ترکیب روش‌های یادگیری ماشین با BC-SDN تمرکز کنند.

٦- بررسی چالش‌های موجود و مسیرهای تحقیقاتی آینده در حوزه BC-SDIoT

با توجه به رشد سریع فناوری‌های اینترنت اشیاء(IoT) ، شبکه‌های نرم‌افزار محور (SDN) و بلاک‌چین(BC) ، ترکیب این فناوری‌ها به عنوان یک پارادایم نوظهور به نام (Blockchain-enabled Software-Defined IoT) **BC-SDIoT** مطرح شده است. این ترکیب می‌تواند به بهبود امنیت، مدیریت شبکه و عملکرد سیستم‌های IoT کمک کند. با این حال، این حوزه با چالش‌های متعددی روبرو است که نیاز به تحقیقات بیشتر و ارائه راه‌حل‌های نوآورانه دارد. در این بخش، چالش‌های موجود و مسیرهای تحقیقاتی آینده در حوزه BC-SDIoT بررسی می‌شود.

۶-۱- چالش‌های امنیتی در BC-SDIoT

یکی از مهم‌ترین چالش‌ها در حوزه BC-SDIoT ، امنیت دستگاه‌های IoT است. دستگاه‌های IoT به دلیل سادگی سخت‌افزاری و محدودیت‌های منابع، اغلب فاقد قابلیت‌های امنیتی پیشرفته هستند. این موضوع آن‌ها را در برابر حملات سایبری مانند حمله مرد میانی (MITM) و حملات انکار سرویس توزیع‌شده (DDoS) آسیب‌پذیر می‌کند .(S. W. Turner et al., ۲۰۲۳)

- ❖ احراز هویت دستگاه‌های IoT : یکی از چالش‌های اصلی، احراز هویت اولیه و حفظ آن در طول زمان است. با توجه به تعداد زیاد دستگاه‌های IoT ، مدیریت کلیدهای امنیتی و احراز هویت به‌صورت متمرکز دشوار است. استفاده از بلاک‌چین برای مدیریت غیرمتمرکز کلیدها و احراز هویت می‌تواند راه‌حلی مؤثر باشد.(Al-Sakran et al., ۲۰۱۹)

- ❖ حریم خصوصی داده‌ها : حفظ حریم خصوصی داده‌های تولید شده توسط دستگاه‌های IoT نیز یک چالش بزرگ است. با توجه به اینکه دستگاه‌های IoT اغلب داده‌های حساسی مانند اطلاعات سلامت یا داده‌های شخصی را جمع‌آوری می‌کنند، استفاده از الگوریتم‌های رمزنگاری سبک‌وزن (Lightweight Cryptography) که اخیراً توسط NIST معرفی شده‌اند، می‌تواند به بهبود امنیت و حریم خصوصی کمک کند.(S. W. Turner et al., ۲۰۲۳)

۶-۲- چالش‌های مقیاس‌پذیری

با افزایش تعداد دستگاه‌های IoT (پیش‌بینی می‌شود تا سال ۲۰۲۵ به ۷۶ میلیارد دستگاه برسد)، مقیاس‌پذیری سیستم‌های BC-SDIoT به یک چالش بزرگ تبدیل شده است .

مقیاس‌پذیری بلاک‌چین : الگوریتم‌های اجماع (Consensus Algorithms) مانند Proof of Work (**PoW**) و Proof of Stake (**PoS**) به دلیل مصرف بالای منابع و تأخیر در پردازش، برای شبکه‌های IoT با تعداد زیاد دستگاه‌ها مناسب نیستند. تحقیقات اخیر نشان می‌دهد که استفاده از الگوریتم‌های اجماع سبک‌وزن مانند **Proof of Authority (PoA)** یا **Sharding** می‌تواند به بهبود مقیاس‌پذیری کمک کند.(Qiu et al., ۲۰۱۹)

مدیریت دینامیک خوشه‌های IoT : با توجه به پویایی بالای شبکه‌های IoT ، مدیریت خوشه‌ها و انتخاب سرخوشه‌ها (Cluster Heads) به‌صورت کارآمد یک چالش است. استفاده از الگوریتم‌های یادگیری ماشین (ML) برای انتخاب بهینه سرخوشه‌ها و کاهش مصرف انرژی می‌تواند راه‌حلی مؤثر باشد.(Rahman et al., ۲۰۲۱)

۶-۳- یکپارچه‌سازی هوش مصنوعی و یادگیری ماشین

هوش مصنوعی (AI) و یادگیری ماشین (ML) می‌توانند نقش مهمی در بهبود امنیت و عملکرد سیستم‌های BC-SDIoT ایفا کنند. با این حال، تحقیقات در این حوزه هنوز در مراحل اولیه است.

تشخیص حملات با استفاده از ML : استفاده از تکنیک‌های یادگیری عمیق (Deep Learning) برای تشخیص حملات سایبری در شبکه‌های IoT یک زمینه تحقیقاتی امیدوارکننده است. به عنوان مثال، استفاده از شبکه‌های عصبی برای تشخیص حملات DDoS در شبکه‌های SDN مبتنی بر بلاک‌چین می‌تواند به بهبود امنیت کمک کند.(Rathore et al., ۲۰۱۹)

بهینه‌سازی شبکه با استفاده ازAI : الگوریتم‌های یادگیری تقویتی (Reinforcement Learning) می‌توانند برای بهینه‌سازی مسیریابی و مدیریت منابع در شبکه‌های SDN استفاده شوند. این روش‌ها می‌توانند به کاهش تأخیر و بهبود کیفیت خدمات (QoS) کمک کنند.(Qiu et al., ۲۰۱۹)

۶-۴- BC-SDIoTدر شبکه‌های G۶

با ظهور شبکه‌های نسل ششم(٦G) ، فرصت‌های جدیدی برای تحقیقات در حوزه BC-SDIoT ایجاد شده است. شبکه‌های ۶ G با پشتیبانی از نرخ‌های داده بسیار بالا (تا چند ترابایت بر ثانیه) و پشتیبانی از دستگاه‌های متنوع) مانندIoT ، ربات‌ها و سیستم‌های واقعیت مجازی(، نیازمند راه‌حل‌های نوآورانه برای مدیریت امنیت و مقیاس‌پذیری هستند.

امنیت در شبکه‌های G۶ : استفاده از بلاک‌چین برای مدیریت امنیت و احراز هویت در شبکه‌های ۶ Gمی‌تواند به کاهش حملات سایبری کمک کند. به عنوان مثال، استفاده از بلاک‌چین برای مدیریت کلیدهای امنیتی و احراز هویت دستگاه‌های IoT در شبکه‌های ۶ Gیک زمینه تحقیقاتی امیدوارکننده است.(Saad et al., ۲۰۲۰)

مدیریت داده‌های بزرگ (Big Data) : با افزایش حجم داده‌های تولید شده توسط دستگاه‌های IoT در شبکه‌های G۶، مدیریت و تحلیل این داده‌ها به یک چالش بزرگ تبدیل شده است. استفاده از فناوری‌های Edge Computing و Fog Computing در ترکیب با بلاک‌چین می‌تواند به بهبود مدیریت داده‌ها و کاهش تأخیر کمک کند. (Yousefpour et al., ۲۰۱۹)

۶-۵- BC-SDIoTدر متاورس

متاورس به عنوان یک محیط مجازی تعاملی، نیازمند امنیت و قابلیت اطمینان بالا است IoT . و بلاک‌چین دو فناوری کلیدی در متاورس هستند که می‌توانند به بهبود امنیت و مدیریت داده‌ها کمک کنند.

احراز هویت و کنترل دسترسی : استفاده از بلاک‌چین برای احراز هویت دستگاه‌ها و کاربران در متاورس می‌تواند به کاهش خطرات امنیتی مانند حملات انکار سرویس (DoS) کمک کند.(Tuan et al., ۲۰۲۲)

مدیریت شبکه‌های متاورس SDN : با قابلیت‌های مدیریت متمرکز و انعطاف‌پذیر، می‌تواند به بهبود مدیریت شبکه‌های متاورس کمک کند. ترکیب SDN با بلاک‌چین می‌تواند امنیت و قابلیت اطمینان شبکه‌های متاورس را افزایش دهد. (Wang et al., ۲۰۲۳)

۶-۶- یادگیری فدرال (Federated Learning) در BC-SDIoT

یادگیری فدرال (FL) یک روش یادگیری ماشین توزیع‌شده است که به دستگاه‌ها اجازه می‌دهد بدون به اشتراک گذاشتن داده‌های خام، مدل‌های محلی خود را آموزش دهند. این روش می‌تواند به بهبود حریم خصوصی و امنیت داده‌ها در شبکه‌های IoT کمک کند.

یادگیری فدرال مبتنی بر بلاک‌چین : استفاده از بلاک‌چین برای مدیریت مدل‌های محلی و توزیع پاداش‌ها به دستگاه‌های مشارکت‌کننده در یادگیری فدرال می‌تواند به بهبود امنیت و قابلیت اطمینان سیستم کمک کند.(Li et al., ۲۰۲۰)

ترکیب فناوری‌های بلاک‌چین، SDNو IoT به عنوان یک پارادایم نوظهور به نامBC-SDIoT ، فرصت‌های زیادی برای بهبود امنیت، مدیریت شبکه و عملکرد سیستم‌های IoT فراهم کرده است. با این حال، چالش‌های متعددی مانند امنیت، مقیاس‌پذیری، حریم خصوصی و مدیریت داده‌ها وجود دارد که نیاز به تحقیقات بیشتر دارد. استفاده از فناوری‌های نوین مانند هوش مصنوعی، یادگیری ماشین و شبکه‌های ۶ Gمی‌تواند به حل این چالش‌ها کمک کند و زمینه‌های تحقیقاتی جدیدی را در این حوزه ایجاد کند.

۷- نتیجه گیری

در این مقاله، ادغام فناوری‌های بلاکچین، اینترنت اشیا (IoT) و شبکه‌های تعریف‌شده توسط نرم‌افزار (SDN) به عنوان یک رویکرد نوآورانه و آینده‌نگرانه برای مواجهه با چالش‌های امنیتی، حریم خصوصی و مدیریت منابع در سیستم‌های پیشرفته امروزی مطرح شده است. پژوهش‌های مورد بررسی نشان می‌دهند که بلاکچین با ارائه ساختاری غیرمتمرکز و قابل اعتماد، می‌تواند امنیت داده‌ها و تراکنش‌ها را در اکوسیستم IoT تقویت کند، در حالی که SDN با قابلیت مدیریت پویا و انعطاف‌پذیر شبکه، امکان بهینه‌سازی زیرساخت‌ها و افزایش مقیاس‌پذیری را فراهم می‌سازد. این هم‌افزایی نه تنها به بهبود کارایی عملیاتی منجر می‌شود، بلکه راه‌حل‌های نوینی برای کاربردهایی نظیر شهرهای هوشمند، سیستم‌های بهداشتی هوشمند و مدیریت زنجیره تأمین ارائه می‌دهد. با این حال، چالش‌هایی نظیر پیچیدگی پیاده‌سازی، مصرف انرژی بالا در برخی معماری‌های بلاکچین، و نیاز به استانداردسازی پروتکل‌ها همچنان باقی است. پژوهش‌های آتی باید بر توسعه راهکارهای بهینه‌تر، کاهش تأخیر در پردازش، و ایجاد چارچوب‌های یکپارچه برای این فناوری‌ها تمرکز کنند. در نهایت، این تلفیق می‌تواند به عنوان پایه‌ای برای نسل بعدی سیستم‌های هوشمند و امن عمل کند و پتانسیل بالایی برای تحول در صنایع مختلف داشته باشد.

۸- مراجع

[۱] 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_۲۰۱۸,۲۰۱۸,۰۰۱۸

[۲] Z. Li et al., ۲۰۲۰. "Blockchain and SDN for Cybersecurity Applications: A Comprehensive Survey." IEEE Communications Surveys & Tutorials.

[۳] A. Reyna et al., ۲۰۱۸. "On blockchain and its integration with IoT: Challenges and opportunities." Future Generation Computer Systems.

[٤] N. McKeown et al., ۲۰۰۸. "OpenFlow: Enabling Innovation in Campus Networks." ACM SIGCOMM.

[٥] M. Al-Fares et al., ٢٠١٠. "A Scalable, Commodity Data Center Network Architecture." ACM SIGCOMM.

[[٦] S. Nakamoto, ٢٠٠٨. "Bitcoin: A Peer-to-Peer Electronic Cash System."

[٧] Al-Sakran, H., Alharbi, Y., & Serguievskaia, I. (٢٠١٩). Framework architecture for securing IoT using blockchain, smart contract and software defined network technologies. In **Proc. ٢nd Int. Conf. New Trends Comput. Sci**. (pp. ١-٦).

[٨] Qiu, C., Yu, F. R., Xu, F., Yao, H., & Zhao, C. (٢٠١٩). Blockchain-based distributed software-defined vehicular networks via deep Q-learning. In *Proc. ٨th ACM Symp. Design Anal. Intell. Veh. Netw. Appl.* (pp. ٨-١٤).
[٩] Rahman, A., Islam, M. J., Nasir, M. K., et al. (٢٠٢١). SmartBlock-SDN: An optimized blockchain-SDN framework for resource management in IoT. *IEEE Access*, vol. ٩, pp. ٢٨٣٦١-٢٨٣٧٦.
[١٠] Saad, W., Bennis, M., & Chen, M. (٢٠٢٠). A vision of ٦G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network*, vol. ٣٤, no. ٣, pp. ١٣٤-١٤٢.

[١١] Tuan, D. T., Duy, P. T., Hau, L. C., & Pham, V. H. (٢٠٢٢). A blockchain-based authentication and access control for smart devices in SDN-enabled networks for metaverse. In **Proc. ٩th NAFOSTED Conf. Inf. Comput. Sci.** (pp. ١٢٣-١٢٨).

[١٢] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (٢٠٢٠). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, vol. ٣٧, no. ٣, pp. ٥٠-٦٠
[١٣] 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

[١٤] 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_٢٠١٨,٢٠١٨,٠٠١٨٩

[١٥] A.F. Zorzo, H.C. Nunes, R.C. Lunardi, R.A. Michelin, S.S. Kanhere
Dependable IoT using blockchain-based technology
٢٠١٨ Eighth Latin-American Symposium on Dependable Computing (LADC), IEEE (Oct. ٢٠١٨), pp. ١-٩, ١٠.١١٠٩/LADC.٢٠١٨.٠٠٠١٠

[١٦] 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

[۱۷] T. Alam
Blockchain and its role in the internet of things (IoT)
۵ (۱) (۲۰۱۹), pp. ۱۵۱-۱۵۷, ۱۰.۳۲۶۲۸/CSEIT۱۹۵۱۳۷

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

[۱۹] 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

[۲۰] 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. ۲٥٥۴-۲٥۶۱

[۲۱] 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

[۲۲] 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

[۲۳] 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

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

[۲٥] M. Sallal, R. de Fréin, A. Malik
PVPBC: privacy and verifiability preserving E-voting based on permissioned blockchain
Future Internet, ۱٥ (٤) (Mar. ۲۰۲۳), p. ۱۲۱, ۱۰,۳۳۹۰/fi۱٥۰٤۰۱۲۱

[۲٦] T. Magara, Y. Zhou
Internet of things (IoT) of smart homes: privacy and security
Journal of Electrical and Computer Engineering, ۲۰۲٤ (Apr. ۲۰۲٤), pp. ۱-۱۷, ۱۰,۱۱٥٥/۲۰۲٤/۷۷۱٦۹٥٦

[۲۷] 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., ۱٥۳ (Apr. ۲۰۲٤), pp. ۲٥۱-۲٦۱, ۱۰,۱۰۱٦/j.future.۲۰۲۳,۱۱,۰۳۲

[۲۸] S. W. Turner et al., "A Promising Integration of SDN and Blockchain for IoT Networks: A Survey," IEEE Access, vol. ۱۱, pp. ۲۹۸۰۰-۲۹۸۲۳, ۲۰۲۳.

۹- Conclusion

In this article, the integration of blockchain, Internet of Things (IoT), and Software-Defined Networking (SDN) technologies is presented as an innovative and forward-looking approach to address the challenges of security, privacy, and resource management in contemporary advanced systems. The reviewed research indicates that blockchain, by offering a decentralized and trustworthy structure, can enhance the security of data and transactions within the IoT ecosystem, while SDN, with its dynamic and flexible network management capabilities, enables the optimization of infrastructure and improves scalability. This synergy not only leads to enhanced operational efficiency but also provides novel solutions for applications such as smart cities, intelligent healthcare systems, and supply chain management. However, challenges such as implementation complexity, high energy consumption in certain blockchain architectures, and the need for standardized protocols persist. Future research should focus on developing more efficient solutions, reducing processing latency, and establishing integrated frameworks for these technologies. Ultimately, this convergence has the potential to serve as a foundation for the next generation of intelligent and secure systems, offering significant transformative potential for various industries.