بلاک‌چین و کاربرد آن در ذخیره اطلاعات به عنوان پایگاه داده توزیع شده امن

زهرا شریف‌خطیبی[۱]، سید کامیار ایزدی[۲]
۱- کارشناسی ارشد دانشکده علوم و فن‌آوری‌های نوین - دانشگاه الزهرا - تهران- ایران
z.sharifkhatibi@student.alzahra.ac.ir
۲- استادیارگروه علوم کامپیوتر - دانشکده علوم ریاضی - دانشگاه الزهرا - تهران- ایران
k.izadi@alzahra.ac.ir

چکیده: فن‌آوری نوین بلاک‌چین، فرمت جدیدی را برای ذخیره‌سازی در یک پایگاه‌داده فراهم می‌کند و الگوی پردازش تراکنش‌ها در این فن‌آوری، سطح بالایی از غیرمتمرکزبودن را امکان‌پذیر می‌نماید. بنابراین، کاربرد این فن‌آوری در زمینه‌های مختلف، به‌دلیل کنترل توزیع‌شده و غیرمتمرکز داده‌ها، مدیریت ایمن، مقیاس‌پذیر و کارآمد منابع را امکان‌پذیر می‌سازد. بلاک‌چین را می‌توان دنباله‌ای از بلاک‌های‌داده متصل در نظر گرفت که هریک به بلاک قبلی وابسته است و یک ساختارداده‌ی زنجیره‌وار پیوسته را تشکیل می‌دهد. در این مقاله، پس از معرفی اجمالی بلاک‌چین، چارچوب و اجزای سازنده‌ی این فن‌آوری، ویژگی‌های منحصربه‌فرد آن و همچنین الگوریتم‌های توافق مورد استفاده در آن توصیف می‌گردد. باتوجه به ویژگی‌های بلاک‌چین، این فن‌آوری در زمینه‌های مختلفی نظیر اینترنت اشیا، کلان داده، رایانش ابری، مدیریت هویت، قراردادهای هوشمند، زنجیره‌های تأمین، انفورماتیک پزشکی، ارتباطات و ... کاربرد دارد. در این مقاله، سعی بر آن است که ضمن معرفی این کاربردها، مروری بر تحقیقات مرتبط در این زمینه انجام شود. علاوه براین، با در نظر گرفتن آسیب‌پذیری‌های امنیتی بلاک‌چین و همچنین محدودیت‌های عملکردی آن، چالش‌های مختلف برای پیاده‌سازی این فن‌آوری بررسی می‌شود. از آنجاکه میزان پردازش تراکنش‌ها یا توان عملیاتی سیستم‌های بلاک‌چین نسبت به پایگاه‌داده‌های دیگر نسبتا پایین است و از طرف دیگر تأخیر تراکنش یا زمان پاسخ در این فن‌آوری نسبتا بالاست، بهبود عملکرد بلاک‌چین در این زمینه‌ها، مسئله‌ی با اهمیتی است. راهکارهای مختلفی در این زمینه مطرح شده‌است که یکی از آن‌ها استفاده از پایگاه‌داده‌های بلاک‌چینی نظیر **BigchainDB** می‌باشد.

واژه های کلیدی: بلاک‌چین، پایگاه‌داده‌های بلاک‌چینی، اینترنت اشیا، رایانش ابری، کلان‌داده

تاریخ ارسال مقاله: ۹۹/۰۴/۲۴
تاریخ پذیرش مقاله: ۹۹/۰۶/۲۸
نام نویسنده مسئول: سید کامیار ایزدی

۱-مقدمه

توسعه مستمر فناوری اطلاعات و رشد بی‌وقفه فن‌آوری‌هایی نظیر اینترنت اشیا[1]، رایانش ابری[2] و کلان داده[3] نیاز به راه‌حل‌های جدیدی را برای مدیریت غیرمتمرکز و توزیع‌شده ایجاد می‌نماید. درواقع، مدیریت ایمن، مقیاس‌پذیر و کارآمد منابع در این فن‌آوری‌ها، نیازمند ذخیره‌سازی داده‌ها به‌صورت غیرمتمرکز و توزیع‌شده است. علاوه‌براین، باتوجه به حجم بالای داده‌های کاربران و همچنین آسیب‌پذیری آن‌ها، اجرای خدمات ایمن، قابل اعتماد و قابل تأیید در این فن‌آوری‌ها اهمیت بسیاری دارد. در سال‌های اخیر، بایگانی الکترونیکی اطلاعات با مشکلاتی از قبیل نشت اطلاعات، دستکاری و ازبین‌رفتن آن‌ها روبرو بوده‌است و این امر ضرورت بهبود مدیریت داده‌ها را مطرح می‌کند. در سیستم‌های نرم‌افزاری، غیرمتمرکز بودن، رابطه نامتقارنی را بین کاربران و ارائه‌دهندگان خدمات ایجاد می‌کند و سبب دشواری مدیریت فردی اطلاعات می‌شود. به‌همین دلیل، غیرمتمرکز بودن یکی از دلایل اصلی آسیب‌پذیری در این سیستم‌ها می‌باشد.

در فن‌آوری نوین بلاک‌چین، الگوی پردازش تراکنش‌ها به‌گونه‌ای است که علاوه بر امکان‌پذیرکردن سطح بالایی از غیرمتمرکزبودن، مواردی نظیر حفظ حریم‌خصوصی و امنیت کاربر را فراهم می‌نماید، بنابراین از قابلیت بالایی برای مدیریت داده‌های مختلف برخوردار است. از طرف دیگر، بلاک‌چین با داشتن ویژگی‌هایی نظیر تغییرناپذیری و قابلیت ردیابی، کاربرد بسیاری را در مدیریت غیرمتمرکز و توزیع‌شده حجم بالایی از داده‌ها داراست. دلیل دیگر گرایش به این فن‌آوری در زمینه مدیریت اطلاعات، مدیریت برنامه‌ها به‌صورت توزیع‌شده و بدون نیاز به شخص سوم قابل اعتماد است. سیستم‌های مدیریت متمرکز کنونی که براساس شخص سوم قابل اعتماد ساخته شده‌اند، نگرانی‌های مربوط به حریم خصوصی را افزایش داده‌اند و یک نقطه آسیب‌پذیر مرکزی را نشان می‌دهند. با این حال، با وجود ویژگی‌های منحصربه‌فرد و خاص بلاک‌چین، کاربرد این فن‌آوری در زمینه‌های مختلف با محدودیت‌ها و چالش‌های متعددی روبروست. با توجه به وجود الگوریتم‌های توافق در سیستم‌های بلاک‌چین، توان عملیاتی در این فن‌آوری به طورقابل‌توجهی کم‌تر از سیستم‌های پایگاه‌داده‌ی دیگر است. از طرف دیگر، زمان پاسخ یا تأخیر تراکنش‌ها در این سیستم‌ها نسبتا بالاست. بنابراین، بهبود عملکرد بلاک‌چین مسئله‌ی بسیار بااهمیتی است.

در این زمینه، راهکارهای مختلفی ارائه شده‌است، که یکی از مطرح‌ترین آن‌ها، استفاده از پایگاه‌داده‌های بلاک‌چینی است. پایگاه‌داده‌های بلاک‌چینی، ویژگی‌های خاص بلاک‌چین نظیر غیرمتمرکز بودن و تغییرناپذیری و همچنین، خواص مطلوب و منحصربه‌فرد پایگاه‌داده‌ها نظیر زمان تأخیر کم و توان عملیاتی بالا را دارا هستند. پایگاه‌داده‌های بلاک‌چینی با ویژگی‌های منحصربه‌فردشان، می‌توانند در طیف گسترده‌ای از زمینه‌ها، از جمله اینترنت اشیا مورد استفاده قرار گیرند.

این مقاله در بخش دوم، به معرفی اجمالی فن‌آوری بلاک‌چین می‌پردازد. این بخش شامل بررسی چارچوب بلاک‌چین و اجزای سازنده آن، انواع آن، الگوریتم‌های توافق و همچنین مروری بر ویژگی‌های اساسی این فن‌آوری است. کاربردهای نوین این فن‌آوری در بخش سوم مطرح شده، در این بخش همچنین مروری بر تحقیقات انجام‌شده در این زمینه ارائه شده‌است. در بخش چهارم، چالش‌های مرتبط با این فن‌آوری مورد بحث و بررسی قرار گرفته‌است. راهکارهای مختلف جهت بهبود عملکرد این فن‌آوری و همچنین معرفی نرم‌افزار BigchainDB در بخش پنجم مطرح شده‌است. نتیجه‌گیری و جمع‌بندی نهایی نیز در بخش پایانی قرار دارد.

۲-معرفی بلاک‌چین

بلاک‌چین، پایه و اساس بیت‌کوین و سایر ارزهای رمزنگاری شده را تشکیل می‌دهد. در واقع، بیت‌کوین، اولین ارز رمزنگاری‌شده بود که با انتشار مقاله‌ای توسط Satoshi Nakamoto در سال ۲۰۰۸ پیشنهاد شد و در سال ۲۰۰۹ نیز پیاده‌سازی گردید. بخش عظیمی از فن‌آوری اصلی بلاک‌چین در دهه ۱۹۹۰ توسعه یافت، اما این فن‌آوری در دهه‌های بعدی به دلیل رونق بیت‌کوین و سایر ارزهای رمزنگاری شده، مورد توجه گسترده مردم قرار گرفت [۱]. بلاک‌چین را می‌توان به‌عنوان یک دفتر عمومی در نظر گرفت که در آن کلیه تراکنش‌های به‌اتمام‌رسیده در یک زنجیره از بلاک‌ها ذخیره می‌شوند. در این ساختار، هر بلاک به بلاک قبلی وابسته است و یک ساختار داده زنجیره‌وار پیوسته را تشکیل می‌دهد [۲.۳].

بلاک یک ظرف ساختارداده با اندازه ثابت است. در برخی موارد، بلاک‌ها معمولا شامل هزاران تراکنش هستند و اندازه معمول یک بلاک می‌تواند به چندین مگابایت هم برسد، که به طور مستقیم بر تعداد تراکنش‌هایی که در ثانیه پردازش می‌شود، تأثیر می‌گذارد. همانطور که در شکل (۱) نشان داده شده‌است،

[1] Internet of Things
[2] Cloud Computing
[3] Big Data

یک بلاک به طور معمول شامل یک سرآیند[1] و بدنه اصلی است. سرآیند بلاک شامل اجزای مختلفی می‌باشد که در ادامه به اختصار توصیف شده‌اند. به‌طورکلی می‌توان سرآیند بلاک را شامل سه مجموعه متادیتا درنظر گرفت. متادیتا، داده‌ای است که اطلاعاتی را در مورد داده‌های دیگر ارائه می‌دهد. در بلاک‌چین، متادیتا، اطلاعاتی را در مورد داده‌های اصلی (تراکنش‌ها) ارائه می‌دهد. مجموعه اول متادیتا یا هش بلاک قبلی، مرجعی برای اشاره به بلاک قبلی است و هر بلاک را به بلاک قبلی پیوند می‌دهد. مجموعه دوم، مربوط به رقابت در فرآیند ماینینگ یا استخراج است که شامل اجزای timestamp، nonce و nBits است. در نهایت، مجموعه سوم متادیتا، ریشه درخت مرکل است.

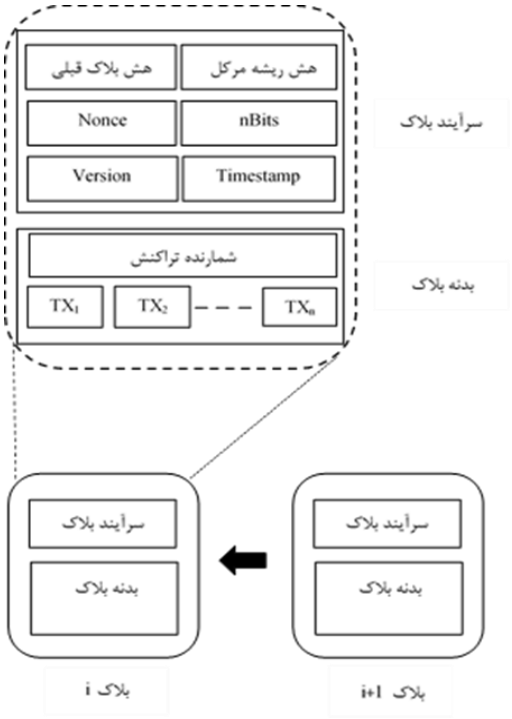
در بلاک‌چین، از توابع هش رمزنگاری شده[2]، استفاده می‌شود. باتوجه به ویژگی مقاومت در برابر برخورد[3] توابع هش، می‌توان از آن‌ها برای تأیید صحت بلاک‌ها استفاده کرد. با توجه به اینکه در بلاک‌چین، هر بلاک شامل مجموعه‌ای از تراکنش‌های جدید و همچنین مقدار هش بلاک قبلی است، درصورتی‌که شخصی قصد تغییر یا اصلاح بلاک خاصی را داشته باشد، با تغییر آن بلاک، هش آن بلاک در بلاک بعدی نیز تغییر می‌کند. بنابراین، هرگونه تلاش برای دستکاری یک بلاک، مستلزم تغییر همه بلاک‌های جدیدتر در زنجیره است و این مسئله به راحتی قابل تشخیص است. بدین ترتیب وجود توابع هش و ویژگی مقاومت آن‌ها، سبب غیرقابل دستکاری شدن بلاک‌چین می‌گردد [۲].

مجموعه دوم متادیتا، مربوط به رقابت در فرایند ماینینگ است. در واقع، ماینینگ یا استخراج، فرآیند کامپیوتری ثبت و تأیید اطلاعات (داده‌های مربوط به تراکنش‌ها) بر روی بلاک‌چین است. در بلاک‌چین، تراکنش‌ها پس از ایجاد در سراسر شبکه پخش می‌شوند تا در بلاک‌های معتبر جمع‌آوری شوند. در این فرآیند، Timestamp، زمان تقریبی ایجاد یک بلاک را نشان می‌دهد و برای ردیابی نیز مورد استفاده قرار می‌گیرد. در فرآیند ماینینگ، Nonce یک عدد یکبار مصرف[4] است، یعنی یک عدد کاملا تصادفی است که فقط یک بار در محاسبات مربوط به فرآیند توافق (که در واقع نوعی فرآیند ماینینگ است) مورد استفاده قرار می‌گیرد.

در فرآیند توافق، هر عضو از شبکه مقدار هش سرآیند بلاک را محاسبه می‌کند. در شبکه‌های غیرمتمرکز، همه شرکت‌کنندگان باید مقدار هش را بطور مداوم با استفاده از nonceهای مختلف تا رسیدن به یک مقدار هدف خاص، محاسبه کنند. وقتی یک شرکت‌کننده مقدار مربوطه را به دست آورد، دیگران باید صحت مقدار را تأیید کنند. پس از آن، تراکنش‌ها در بلاک جدید اعتبار می‌یابند و توسط یک بلاک جدید در بلاک‌چین ثبت می‌شوند. برای تأیید اعتبار یک بلاک، مقدار هش محاسبه‌شده در فرآیند ماینینگ باید کمتر از آستانه هدف باشد. nBits، شکل کد گذاری شده‌ی آستانه هدف است. در فرآیند رقابت ماینینگ، شرکت‌کنندگان میلیون‌ها Nonce را در ثانیه آزمایش کرده و کنار می‌گذارند تا زمانی که مقدار مناسب را به‌دست آورند. به منظور انجام سریعتر این فرآیند، شرکت‌کنندگان با استفاده از توان محاسباتی رایانه خود با یکدیگر به رقابت می‌پردازند. پس از یافتن مقدار مناسب، شخص موردنظر می‌تواند بلاک را تکمیل کرده و آن را به بلاک‌چین اضافه کند. ریشه درخت مرکل (یا درخت هش) تراکنش‌های بلاک را به روشی کارآمد و ایمن رمزنگاری کرده و امکان بررسی سریع تراکنش‌های بلاک را فراهم می‌کند. هش ریشه درخت مرکل را می‌توان هش همه‌ی هش‌های تمام تراکنش‌ها در یک بلاک درنظر گرفت.

در مقابل، بدنه بلاک معمولاً شامل شمارنده تراکنش[5] و تمام تراکنش‌ها یا رکورد داده‌ها است. در بلاک‌چین، تراکنش‌ها به صورت رکورد داده ذخیره می‌شوند، درواقع یک تراکنش، سندی از تعاملاتی خاص مانند انتقال وجه یا ذخیره داده در یک پایگاه‌داده است که در زمان خاصی انجام گرفته‌اند. تعداد تراکنش‌های یک بلاک به اندازه بلاک و اندازه هر تراکنش بستگی دارد [۲،۳].

[1] Header
[2] Cryptographic Hash Functions
[3] Collision-resistance property
[4] Number used once
[5] Transaction counter



شکل (۱) : ساختار بلاک‌های بلاک‌چین [۲]

بلاک‌چین در ابتدایی‌ترین سطح خود یک زنجیره پیوسته از بلاک‌های داده است و هر بلاک در این زنجیره به بلاک قبلی خود وابسته است. در سطح بالاتر، بلاک‌چین را می‌توان به عنوان چارچوبی اساسی در نظر گرفت که شامل تعدادی از اجزای لازم و فعال، مانند محیط تعامل و برنامه‌های کاربردی است. چارچوب بلاک‌چین شامل لایه داده، لایه شبکه و لایه کاربرد می‌باشد [۲]. جزء اصلی لایه داده، بلاک‌های داده متصل به‌هم یا درواقع همان محیط تعامل بلاک‌چین است. محیط تعامل، فضایی است که تعاملاتی خاص مانند انتقال وجه یا ذخیره داده در آن انجام می‌شود. در لایه داده، واحدهای اصلی بلاک‌چین قرار دارد که شامل انواع ساختارداده‌ها و الگوریتم‌ها از جمله هش و اشاره‌گر هش، درخت مرکل و امضای دیجیتال است. لایه شبکه برای فعال‌کردن محیط‌های تعامل بلاک‌چین استفاده می‌شود. این لایه شامل شبکه غیرمتمرکز مبتنی بر پروتکل‌های IP و شبکه همتا به همتا[1]، اسکریپت‌های قفل‌کردن و بازکردن قفل و از همه مهم‌تر مکانیزم‌های توافق است. علاوه‌براین، لایه شبکه به‌روزرسانی و توزیع بلاک‌چین را بین کاربران امکان‌پذیر می‌کند. سرانجام، لایه کاربرد، کاربردهای مختلفی نظیر توافق بین گره‌ها، قراردادهای هوشمند و اجزای رمزنگاری را ارائه می‌دهد [۲].

از الگوریتم‌های مهم لایه داده، می‌توان به رمزنگاری نامتقارن و امضاهای دیجیتال اشاره نمود. بلاک‌چین از یک مکانیزم رمزنگاری نامتقارن برای تأیید صحت تراکنش‌ها استفاده می‌کند. رمزنگاری نامتقارن از طرح کلید عمومی-محرمانه، استفاده می‌کند. در این سیستم رمزنگاری، کلیدهای عمومی به طور گسترده‌ای در دسترس تمام کاربران قرار دارد و آن‌ها قادرند پیامی را رمزگشایی کنند که فقط مالک اصلیش، قادر به رمزنگاری آن است [۲].

امضاهای دیجیتال نیز از طرح کلید عمومی-محرمانه بهره می‌گیرند. به بیان دیگر، امضای دیجیتال هر کاربر دارای یک جفت کلید خصوصی و کلید عمومی است. از کلید خصوصی برای امضای تراکنش‌ها استفاده می‌شود. تراکنش‌های امضاشده دیجیتال در کل شبکه پخش‌شده و سپس توسط کلیدهای عمومی قابل مشاهده و بررسی هستند. یک کاربر خارجی می‌تواند یک پیام رمزنگاری شده با کلید خصوصی، را با رمزگشایی آن با کلید عمومی، بررسی کند.

یک امضای دیجیتال معمول شامل دو فاز، فاز امضا و فاز بررسی می‌باشد. زمانی که یک کاربر می‌خواهد تراکنشی را امضا کند، ابتدا یک مقدار هش برگرفته از تراکنش ایجاد می‌کند. سپس این مقدار هش را با استفاده از کلید خصوصی خود رمزنگاری کرده و آن را همراه با داده‌های اصلی برای کاربر دیگر می‌فرستد. کاربر دوم، تراکنش‌های دریافت‌شده را از طریق مقایسه بین هش رمزگشایی شده (با استفاده از کلید عمومی کاربر اول) و مقدار هش به‌دست‌آمده از داده‌های دریافتی توسط همان تابع درهم ساز کاربر اول، بررسی می‌کند. بنابراین، در مورد بلاک‌چین، استفاده از امضاهای دیجیتالی، منشا تراکنش از یک کاربر به کاربر بعدی را تضمین می‌کند، چرا که هر تراکنش به تراکنش‌های قبلی خود مرتبط است. الگوریتم امضای دیجیتال معمول مورد استفاده در بلاک‌چین، الگوریتم امضای دیجیتال منحنی بیضوی[2] است [۳].

یکی از ساختارداده‌های مهم لایه داده، درخت مرکل است. در بلاک‌چین، تراکنش‌ها به‌عنوان بخشی از یک درخت به نام درخت مرکل ذخیره می‌شوند. درخت مرکل با ایجاد یک اثر انگشت دیجیتالی از کل مجموعه تراکنش‌ها، کلیه تراکنش‌ها را در یک بلاک خلاصه می‌کند. در ساختار درخت مرکل، گره‌های برگ مقدار هش مربوط به هر تراکنش را نشان می‌دهند. هر مجموعه از هش‌های گره‌های فرزند با هم ترکیب می‌شوند و این فرایند درهم‌سازی تا رسیدن به ریشه درخت ادامه دارد. درختان مرکل باینری هستند و به همین دلیل به تعداد زوج گره‌های برگ نیاز دارند. اگر تعداد تراکنش‌ها فرد باشد، آخرین هش یک

[1] Peer to Peer (P2P) network

[2] Elliptic curve digital signature algorithm (ECDSA)

بار تکرار می‌شود تا تعداد زوج گره‌های برگ ایجاد شود. از آنجا که در درخت مرکل، مقدار هش در هر گره والد، به مقدار هش در گره‌های فرزندش بستگی دارد، دستکاری یک تراکنش بدون تغییر سایرین تقریباً غیرممکن است. بنابراین، هرگونه تغییر در تراکنش، تا ریشه درخت مرکل بر مقدار هش تأثیر می‌گذارد. در نتیجه می‌توان از ریشه به عنوان یک شناسه استفاده کرد [۲].

یکی از مهم‌ترین اجزای لایه شبکه بلاک‌چین، شبکه همتابه‌همتا است. در این شبکه، کاربر، پایه و اساس شبکه را همان زمان هم استفاده می‌کند و هم ارائه می‌دهد، اگرچه ارائه منابع کاملاً داوطلبانه است. در این شبکه، هر یک از همتاها یکسان و برابر در نظر گرفته شده و معمولاً هر یک به‌عنوان یک گره معرفی می‌شوند. با توجه به برابر بودن همه گره‌ها، آن‌ها می‌توانند نقش‌های مختلفی را در بلاک‌چین ایفا کنند. جز مهم دیگر در این لایه، الگوریتم‌های توافق است [۲].

یکی از مهم‌ترین ویژگی‌های بلاک‌چین، غیرمتمرکز بودن آن است، به این معنی که یک سرور مرکزی برای ذخیره‌سازی اطلاعات وجود ندارد و اطلاعات در همه گره‌های شرکت‌کننده (سرور) تکثیر می‌شود. این ویژگی سبب می‌شود که اگر اطلاعات روی یکی از سرورها (گره‌ها) به نوعی از بین برود یا دستخوش تغییر بشود، بتوان از اطلاعات مشابهی که روی گره‌های (سرورهای) دیگر ذخیره شده است استفاده کرد. بنابراین، باتوجه به اینکه بلاک‌چین در همه گره‌های شرکت‌کننده تکثیر می‌شود، جهت اضافه‌شدن هر بلاک جدید به زنجیره، همه‌ی گره‌ها باید در مورد ماهیت گره‌ی اضافه‌کننده و همچنین خود بلاک به توافق برسند [۱]. از طرف دیگر، جهت فراهم‌کردن امکان غیرمتمرکزبودن در بلاک‌چین، گره‌های درگیر در انجام تراکنش‌ها و همچنین ایجاد بلاک‌ها، باید قادر باشند اعتبار بلاک‌هایی را که به زنجیره اضافه می‌کنند، تایید کنند. مکانیسم‌های متفاوتی جهت تأیید اعتبار یک بلاک وجود دارد که به الگوریتم‌های توافق معروف هستند. هدف نهایی این توافقات، تعیین دقیق صحت بلاک‌های اضافه شده در یک زنجیره بلاک‌چین، با چک کردن اعتبار هر بلاک است. تفاوت‌ها در این است که چه کسی و با حل چه معمایی می‌تواند اعتبار بلاک موردنظر را تأیید کرده و بلاک‌ها را به زنجیره اضافه نماید.

درواقع الگوریتم توافق، روشی گام به گام برای رسیدن به جواب مساله یا همان معمای مطرح شده‌است. در بلاک‌چین الگوریتم‌های متنوع توافق، از جمله اثبات کار، اثبات سهام، اثبات سهام محول‌شده و توافق بیزانس مورد استفاده قرار می‌گیرد، که در ادامه توصیف شده‌اند [۲].

در تمام الگوریتم‌های توافق، کار اصلی کاربران آن‌ها این است که یک بلاک جدید را تایید کرده و سپس این بلاک جدید را به بلاک‌چین اضافه نمایند. توافق اثبات کار برای بلاک‌چین‌های عمومی طراحی شده است که در آن تعداد گره‌های شرکت‌کننده در شبکه به طور مداوم درحال‌تغییر است، هر رایانه‌ای می‌تواند بلاک‌چین را دانلود نماید و برای اضافه‌کردن بلاک‌ها تلاش کند. مسئله مهم در این زمینه این است که توافق اثبات‌کار، به حل یک معمای پیچیده با یک فرآیند محاسباتی پیچیده برای تایید اعتبار بلاک‌ها نیازمند است. پاسخ مسئله‌ی اثبات کار یا معمای پیچیده ریاضی آن، هش نام دارد. هش، یک فرمول ریاضی تصادفی و پیچیده است که در فرآیند تأیید بلاک استفاده می‌شود. در اثبات کار، هر گره‌ای از شبکه که اصطلاحا ماینر نیز نامیده می‌شود، مقدار هش سرآیند بلاک را محاسبه می‌کند. توافق مستلزم آن است که مقدار هش محاسبه‌شده، برابر یا کوچکتر از یک حد مشخص یا مقدار آستانه تعیین‌شده باشد. این حد مشخص را سختی می‌نامند که مشخص‌کننده ماهیت رقابتی عمل ماینینگ است. به‌عبارت دیگر این مقدار آستانه مشخص، یکی از اجزای اصلی سرآیند بلاک است که به شکل کدگذاری‌شده، تحت‌عنوان nBits در بخش سرآیند هر بلاک قرار دارد. درواقع، یک بلاک تنها در صورتی معتبر شناخته می‌شود که مقدار هش کل بلاک از یک مقدار آستانه مشخص کمتر باشد.

در شبکه‌های غیرمتمرکز، همه شرکت‌کنندگان یا ماینرها باید مقدار هش را بطور مداوم با استفاده از nonceهای مختلف تا رسیدن به مقدار تعیین‌شده، محاسبه کنند. وقتی یک گره مقدار مربوطه را به دست آورد، تمام گره‌های دیگر باید به طور متقابل صحت مقدار را تأیید کنند، پس از آن، تراکنش‌ها در بلاک جدید اعتبار می‌یابند [۳]. در واقع، ماینر یا استخراج‌گر یک کاربر است که از کامپیوتر خودش برای ثبت تراکنش‌ها و اعتباربخشی به آن‌ها استفاده می‌کند [۲].

درواقع، توافق اثبات کار یک نوع فرآیند استخراج یا ماینینگ‌کردن است که نیازمند هزینه و انرژی و قدرت محاسبه بالای کامپیوتری جهت تاییدکردن بلاک‌ها می‌باشد [۲].

در شبکه غیرمتمرکز بلاک‌چین، این امکان وجود دارد که چندین گره (ماینر) به‌طور همزمان مقدار nonce مناسب را محاسبه کنند. این مسئله ممکن است منجر به ایجاد انشعابات فرعی در زنجیره اصلی بلاک‌چین شود. با این وجود امکان افزودن بلاک جدید به هر دو انتهای انشعابات فرعی ایجادشده، آن هم به‌صورت همزمان تقریبا بعید است. بنابراین یکی از

انشعابات طولانی‌تر شده و زنجیره اصلی درنظر گرفته می‌شود، درحالیکه انشعاب دیگر متروک می‌ماند. ایجاد انشعابات فرعی در زنجیره اصلی بلاک‌چین، مشکلاتی را به‌دنبال دارد که جهت غلبه بر این مسئله، معمولا مقدار آستانه هدف را به‌گونه‌ای انتخاب می‌نمایند که یافتن nonce فرآیند ساده‌ای نباشد و به‌راحتی محاسبه نشود [۲].

توافق اثبات سهام، یک نوع الگوریتم توافق است که برخلاف توافق اثبات کار نیازمند هزینه و انرژی بسیار بالایی نمی‌باشد. در این سیستم اعتبارسنج‌ها جای ماینرها را می‌گیرند. در این نوع توافق، دیگر نیازی به محاسبه‌های پیشرفته و تجهیزات سنگین کامپیوتری نیست و افراد می‌توانند با ایجاد سهام (سرمایه‌گذاری در شبکه) اقدام به اعتبارسنجی بلاک‌های جدید در شبکه نمایند. درواقع، در این نوع الگوریتم، در ابتدا، گره‌ی خاصی براساس میزان سهامش برای ایجاد بلاک جدید، مشخص می‌شود و برای ایجاد بلاک جدید رقابتی وجود ندارد. باتوجه به اینکه این نوع انتخاب (انتخاب صرفا براساس میزان سهام) سبب برتری افراد ثروتمند (دارای بیشترین سهام) در شبکه می‌شود، راه‌کار خاصی برای مقابله با این مسئله مطرح شده‌است. در این ارتباط از یک فرایند شبه تصادفی برای انتخاب گره موردنظر استفاده می‌شود. در این انتخاب عواملی از قبیل میزان سهام یا دارایی گره، مدت زمان حضور سهام (سن سهام) و انتخاب تصادفی تاثیرگذار است. در روش انتخاب تصادفی، گره موردنظر با جست‌وجو در میان گره‌ها بر اساس ترکیبی از پایین‌ترین مقدار محاسبه‌شده هش و بالاترین مقدار سهام، انتخاب می‌شود. در روش سن سهام، گره‌ها بر اساس مدت زمانی که سهام را سرمایه‌گذاری کرده‌اند، انتخاب می‌شوند. این مدت با ضرب تعداد روزهایی که سهام بلاک شده در میزان سهام، محاسبه می‌شود. هنگامی که یک گره موفق به ایجاد یک بلاک جدید می‌شود، سن سهام آن صفر می‌شود و مدت معینی را برای اینکه بتواند یک بلاک دیگر بسازد، باید صبر کند. این امر مانع از تسلط گره‌هایی می‌شود که سهام بزرگی در بلاک‌چین دارند. مزیت مهم دیگر این الگوریتم، امنیت بالای آن است.

توافق اثبات سهام، از کاربران، درخواست می‌کند که مالکیت مقدار ارز یا سهام خود در شبکه را اثبات کنند. زیرا اعتقاد بر این است که افرادی که ارز یا سهام بیشتری دارند، کمترین احتمال حمله به شبکه را نیز دارند. در واقع، آسیب رساندن به شبکه‌ای که بخش قابل توجهی از سهام آن متعلق به خود شخص است، آسیب به مال و اموال خود شخص محسوب می‌شود [۳].

در توافق اثبات سهام محول‌شده، مشابه توافق اثبات سهام، اولویت ماینرها برای تولید بلاک با توجه به سهام آن‌ها تعیین می‌شود. با این تفاوت که در این توافق، سهام‌داران، نماینده خود را برای تولید و اعتبارسنجی یک بلاک انتخاب می‌کنند. بنابراین، باتوجه‌به‌اینکه گره‌های کمتری برای اعتبارسنجی بلاک‌ها استفاده می‌گردد، یک بلاک به سرعت تأیید می‌شود، و این امر باعث می‌شود تراکنش‌ها به سرعت تأیید شوند [۳].

توافق بیزانس نوعی توافق مبتنی بر پیام است که به طور گسترده در سیستم‌های پایگاه‌داده توزیع‌شده استفاده می‌شود. تحمل خطای بیزانس، یعنی توانایی یک شبکه کامپیوتری توزیع‌شده برای عملکرد مطلوب و صحیح که در نهایت این عملکرد منجر به نوعی توافق شود. این توافق در حالتی ایجاد می‌شود که گره‌های مخرب سیستم در انتقال اطلاعات به همتاهای دیگر خود شکست می‌خورند و یا اطلاعات نادرست را به آن‌ها انتقال می‌دهند. هدف از این عملکرد صحیح، دفاع در برابر شکست‌های سیستم است که این کار با کاهش تاثیرگذاری گره‌های مخرب بر روی عملکرد صحیح شبکه انجام می‌شود و سبب توافق صحیحی می‌شود که توسط گره‌های صادق در سیستم انجام می‌شود. در الگوریتم توافق بیزانس، گره‌های شبکه به شیوه‌ای مرتب شده‌اند که یک گره رئیس وجود دارد و بقیه گره‌ها به‌عنوان گره پشتیبان شناخته می‌شوند. تمام گره‌های شبکه با هم ارتباط دارند و هدف همه گره‌های صادق رسیدن به توافق از طریق رای اکثریت است. در این الگوریتم گره‌ها شدیدا با همدیگر ارتباط دارند. مکانیزم توافق بیزانس، یک نوع توافق قطعی است، به این معنی که اگر اکثریت گره‌ها بر روی یک بلاک خاص توافق کنند، آن بلاک نهایی خواهد شد. این امر به‌دلیل توافق گره‌های صادق بر روی یک بلاک خاص در یک زمان، در نتیجه ارتباط آن‌ها با یکدیگر است. این مکانیزم در سه مرحله انجام می‌شود و به ارتباط شبکه برای پیاده‌سازی نیازمند است. در مرحله اول یا مرحله قبل از آماده‌سازی، رئیس ارزش موردنظر برای تعهد به بلاک‌چین را به گره‌ها ارسال می‌کند. سپس، در مرحله آماده‌سازی، گره‌ها، ارزشی را که قصد متعهد شدن به آن را دارند، پخش می‌کنند. در نهایت، در مرحله تکمیلی، بیش از دو سوم از گره‌ها باید بر روی مقدار مرحله آماده‌سازی، توافق کنند [۲].

دو نمونه پرکاربرد از این نوع توافق شامل تحمل خطای بیزانس عملی[1] (PBFT) و Tendermint است. در توافق PBFT، یک بلاک جدید، در یک دور تعیین می‌شود. در هر دور، یک

[1] Practical byzantine fault tolerance (PBFT)

مسئول اولیه مطابق با برخی از قواعد انتخاب می‌شود که مسئولیت تنظیم تراکنش‌ها را بر عهده دارد. کل فرایند، در سه مرحله قبل از آماده‌سازی، آماده‌سازی و مرحله تکمیلی انجام می‌شود. اگر گره‌ای در هر مرحله، بیش از دوسوم از رأی همه گره‌ها را دریافت کند، می‌تواند وارد مرحله بعدی شود. بنابراین PBFT نیازمند این است که هر گره برای شبکه شناخته شده باشد. در توافق Tendermint، نیز شبیه PBFT، یک بلاک جدید در یک دور مشخص می‌شود و یک پیشنهاددهنده برای پخش یک بلاک تأییدنشده، در این دور انتخاب می‌شود. بنابراین، همه گره‌ها باید برای انتخاب پیشنهاددهنده، شناخته شوند. تفاوت این دو نوع توافق در این است که در توافق PBFT، برای انتخاب عضو اصلی در هر دور، هویت هر ماینر باید شناخته شود، درحالی‌که، در توافق Tendermint برای انتخاب پیشنهاددهنده، اعتبارسنج‌ها باید شناسایی شوند [۳].

به‌طورکلی می‌توان گفت که، یک الگوریتم توافق خوب به معنای کارایی، ایمنی و سادگی است. توافقات اثبات کار و اثبات سهام اغلب برای بلاک‌چین‌های عمومی مناسب هستند. درحالی‌که، بلاک‌چین‌های کنسرسیوم یا خصوصی، توافقات بیزانس (PBFT و Tendermint) و توافق اثبات سهام محول‌شده را ترجیح می‌دهند. نتایج مطالعات انجام شده نشان داده‌اند که الگوریتم‌های توافق ذکرشده، هنوز هم کمبودهای زیادی دارند. به‌عنوان‌مثال، یک مسئله مهم در این زمینه، جداکردن فرایندهای ایجاد بلاک‌ها و تأیید تراکنش‌ها است، تا بتوان سرعت توافق را بطور قابل توجهی افزایش داد [۳].

در انتها قابل ذکر است که مفهوم الگوریتم‌های توافق در مراجع [۴.۵.۶.۷] نیز ذکر گردیده است.

به طور کلی بلاک‌چین می‌تواند به عنوان شبکه permissioned یا (خصوصی) که می‌تواند برای گروه خاصی از شرکت‌کنندگان محدود شود، یا شبکه permission-less یا (عمومی) که برای هر شخصی برای پیوستن به آن آزاد است، ساخته شود. بلاک‌چین‌های Permissioned حریم خصوصی بیشتر و کنترل دسترسی بهتری را ارائه می‌دهند [۸].

سیستم‌های بلاک‌چین فعلی به سه نوع بلاک‌چین عمومی، بلاک‌چین خصوصی و بلاک‌چین کنسرسیوم تقسیم می‌شوند [۳.۴.۹].

یک بلاک‌چین عمومی، یک سیستم غیرمتمرکز است که در آن هر گره آزادانه می‌تواند به سیستم بپیوندد و یا از آن خارج شود. در یک بلاک‌چین عمومی (نظیر بیت‌کوین یا اتریوم)، تمام تراکنش‌ها برای عموم قابل مشاهده هستند و هر یک از شرکت‌کنندگان قادر به دریافت و ارسال تراکنش‌ها در شبکه می‌باشند. علاوه‌براین، هر شرکت‌کننده می‌تواند در فرآیند توافق شرکت کند. باتوجه به اینکه تراکنش‌های بلاک‌چین در گره‌های مختلف شبکه، ذخیره می‌شوند، دستکاری بلاک‌چین‌های عمومی تقریباً غیرممکن است. در بلاک‌چین‌های عمومی، به‌دلیل تعداد بسیارزیاد گره‌ها و همچنین با در نظر گرفتن ایمنی شبکه، محدودیت‌های مربوطه بسیار دقیق‌تر خواهد بود. بنابراین، در این نوع بلاک‌چین، توان عملیاتی سیستم محدود بوده و زمان تأخیر نسبتا بالا است [۳.۴.۹].

یک بلاک‌چین کنسرسیوم (نظیر Hyperledger) تا حدودی غیرمتمرکز است و در آن یک مکانیسم کنترل دسترسی دقیق جهت بررسی هویت تمام گره‌هایی که خواستار پیوستن به سیستم هستند، وجود دارد. در این نوع بلاک‌چین، یک سازمان یا کنسرسیوم تصمیم می‌گیرد که قابلیت مشاهده‌ی اطلاعات ذخیره‌شده، عمومی بوده یا محدود به شرکت‌کنندگان خاص باشد. فرآیند توافق در این نوع بلاک‌چین، توسط یک مجموعه گره از پیش انتخاب‌شده کنترل می‌شود، بنابراین، امکان هرگونه تغییر یا دستکاری در صورت موافقت اکثریت، وجود دارد [۳.۴.۹].

بلاک‌چین خصوصی کاملاً متمرکز است، زیرا توسط یک گروه واحد کنترل می‌شود و هر گره برای پیوستن به فرآیند توافق به گواهی نیازمند است. در این نوع بلاک‌چین، یک گروه تصمیم می‌گیرد که قابلیت مشاهده‌ی اطلاعات ذخیره‌شده، عمومی بوده یا محدود به شرکت‌کنندگان خاص باشد. در بلاک‌چین خصوصی، فرآیند توافق توسط یک گروه خاص کنترل می‌شود، بنابراین، امکان هرگونه تغییر یا دستکاری در صورت موافقت اکثریت، در این بلاک‌چین وجود دارد [۳.۴.۹].

بلاک‌چین عمومی با توجه به ویژگی‌های خاصش، کاربران زیادی را به سوی خود جلب می‌کند. امروزه بیشتر پروژه‌ها به بلاک‌چین عمومی متکی هستند، که دسترسی به تعداد زیادی از کاربران، گره‌های شبکه و بازار را امکان‌پذیر می‌کند. بلاک‌چین کنسرسیوم در بسیاری از کاربردهای تجاری استفاده می‌شود. بلاک‌چین خصوصی، نیز در بسیاری از شرکت‌ها برای بهره‌وری و حسابرسی مورد استفاده قرار می‌گیرد [۳.۴.۹].

به‌طورکلی می‌توان گفت که انواع مختلف بلاک‌چین، شامل ویژگی‌هایی نظیر شفافیت، پایداری، غیرمتمرکزبودن، انکارناپذیری، ناشناس‌بودن، قابلیت ردیابی، تحمل خطا و مقاومت در برابر حمله می‌باشند که در ادامه توصیف شده‌اند.

شفافیت: در شبکه بلاک‌چین، طبق فرآیند توافق، هر ورودی جدیدی از تراکنش‌ها جهت اضافه‌شدن به زنجیره بلاک‌چین باید توسط اکثریت گره‌ها بررسی و تأیید شود. علاوه‌براین، در این شبکه، دستکاری یا حذف تراکنش‌های قدیمی نیز به توافق اکثریت گره‌های شبکه نیازمند است. درنتیجه، در شبکه بلاک‌چین هر تراکنشی بسیار دقیق بررسی می‌شود و تمام تراکنش‌های تأییدشده در دفتر ثبت می‌شوند. تراکنش‌های ثبت‌شده، معمولا قابل ویرایش یا تغییر نیستند. بنابراین، بلاک‌چین به‌عنوان یک دفتر عمومی، سطح بالایی از شفافیت را فراهم می‌کند [۲].

پایداری: باتوجه به اینکه بلاک‌چین در همه گره‌های شرکت‌کننده تکثیر می‌شود، جهت اضافه‌شدن هر بلاک جدید به زنجیره، همه‌ی گره‌ها باید در مورد ماهیت گره‌ی اضافه کننده و همچنین ماهیت تراکنش‌های موجود در آن بلاک، به توافق برسند. از طرف دیگر، هرگونه تلاش برای دستکاری یا حذف تراکنش‌های قدیمی نیز نیازمند توافق اکثریت گره‌ها است، که تقریبا غیرممکن است. بنابراین، میزان پایداری در بلاک‌چین بسیار بالاست [۲].

غیرمتمرکز بودن: در سیستم‌های تراکنش متمرکز، هر تراکنش باید از طریق یک سازمان مرکزی قابل‌اعتماد تأیید شود و این مسئله موجب افزایش هزینه‌ها و تنگناهای عملکردی در سرور مرکزی می‌شود. درحالی‌که در شبکه‌های بلاک‌چینی غیرمتمرکز، تراکنش‌های بین دو گره‌ی همتا می‌تواند بدون تأیید اعتبار توسط سازمان مرکزی انجام شود و این مسئله سبب کاهش هزینه‌های سرور مرکزی (از جمله هزینه توسعه و هزینه بهره‌برداری) و همچنین تنگناهای عملکردی آن می‌گردد [۳.۴.۱۰.۱۱]. البته میزان غیرمتمرکزبودن در انواع مختلف بلاک‌چین متفاوت است. به‌عنوان مثال، در یک بلاک‌چین عمومی، کنترل بلاک‌چین با توافق اکثریت گره‌ها بدون هیچ سرور کنترل‌کننده مرکزی انجام می‌شود. در انواع دیگر بلاک‌چین‌ها نیز میزان کنترل مرکزی محدود است و فقط شامل اجازه دسترسی و مدیریت هویت می‌باشد و سایر اقدامات به‌صورت غیرمتمرکز انجام می‌شود [۱].

انکار ناپذیری: هر فعالیتی که توسط یک کاربر در بلاک‌چین انجام شود، به‌صورت رمزنگاری شده توسط کاربر امضا می‌شود. بنابراین این امضا ثابت می‌کند که کاربر مسئول تراکنش موردنظر می‌باشد و هیچ‌گونه امکان انکاری در این زمینه وجود ندارد [۱.۱۱].

ناشناس بودن: هر کاربری در بلاک‌چین دارای یک شناسه کاربری است که به طور مستقیم به اطلاعات شناسایی شخصی او مرتبط نیست. بنابراین، هر کاربر می‌تواند با یک آدرس ساختگی در عوض هویت واقعی خود با شبکه ارتباط برقرار کند. علاوه‌براین، یک کاربر می‌تواند آدرس‌های بسیاری را برای جلوگیری از در معرض قرارگرفتن هویتش، ایجاد نماید. از طرف دیگر، در بلاک‌چین هیچ بخش مرکزی اطلاعات خصوصی کاربران را حفظ نمی‌کند، بنابراین کاربران تقریبا ناشناس مانده و حریم خصوصی افراد تا حدودی محافظت می‌شود. اگرچه در بلاک‌چین، آدرس کاربران نام‌های مستعار هستند، اما پیوند دادن آدرس‌ها به هویت واقعی کاربران امکان‌پذیر است، زیرا بسیاری از کاربران مرتباً با همان آدرس تراکنش انجام می‌دهند [۳.۹.۱۰].

قابلیت ردیابی: هر تراکنش ذخیره شده در بلاک‌چین با یک timestamp ضمیمه می‌شود. بنابراین، کاربران می‌توانند به راحتی پس از تجزیه و تحلیل داده‌های بلاک‌چین با timestampهای مربوطه، ریشه موارد داده‌های تاریخی را بررسی و ردیابی کنند [۱۱].

تحمل خطا: شبکه‌ی بلاک‌چین، یک سیستم غیرمتمرکز با تعداد بسیاری از شرکت‌کنندگان مختلف است. در یک شبکه‌ی بلاک‌چین، هر گره (یک شرکت‌کننده) هنگام دریافت یک تراکنش تازه‌توزیع‌شده در شبکه، این انتخاب را دارد که یا آن تراکنش را بپذیرد (یعنی آن را به نسخه محلی دفترش اضافه کند) یا آن را نادیده بگیرد. توافق زمانی حاصل می‌شود که اکثریت گره‌ها در مورد یک وضعیت واحد تصمیم‌گیری نمایند. در نتیجه، خطاهایی که ممکن است در تعداد کمی از گره‌ها اتفاق بیفتد، احتمالاً وضعیت دفتر عمومی را تغییر نمی‌دهند و با به‌روزشدن بلاک‌چین اصلاح می‌گردد. بنابراین، تا زمانی که تعداد گره‌هایی که در آن‌ها خطایی رخ داده در اقلیت باقی بماند، بلاک‌چین دچار تغییر نشده یا اصطلاحا خطای رخ داده را تحمل می‌نماید [۲.۴].

مقاومت در برابر حمله: سیستم‌های متمرکز، با آسیب‌پذیری بسیاری در برابر حملات مختلف (از جمله نفوذ یا هک‌کردن) مواجه هستند. درحالیکه سیستم غیرمتمرکز بلاک‌چین، یک شبکه همتا به همتا از شرکت‌کنندگان مختلف است. گره‌های شرکت‌کننده در این شبکه، همتا و یکسان بوده و هریک نقش یکسان و برابری را در شبکه دارا هستند. داده‌های بلاک‌چین در تمام گره‌های مستقل این شبکه تکثیر و توزیع می‌شود و هر گره یک کپی کامل از بلاک‌چین را دارا می‌باشد. تا زمانی که هر گره در شبکه یک کپی از بلاک‌چین را حفظ کند، گره‌های به خطر

افتاده، قادر به معرفی تراکنش‌ها یا بلاک‌های جعلی به زنجیره نیستند. در نتیجه، یکپارچگی رکوردها در بلاک‌چین حفظ می‌گردد. دقیقاً مانند ویژگی تحمل خطا، این امر تا زمانی که تعداد گره‌های به خطر افتاده در اقلیت باقی بماند، صادق است. نسخه‌های صحیح بلاک‌چین در گره‌های به‌خطرنیفتاده، یک نسخه پشتیبان مطمئن برای سیستم و همچنین برای رونویسی نسخه‌های هک‌شده فراهم می‌کند [۲].

۳-کاربردهای فن‌آوری بلاک‌چین

باتوجه به ویژگی‌های بلاک‌چین و همچنین مزایای آن، این فن‌آوری در زمینه‌های مختلفی شامل اینترنت اشیا، کلان داده، رایانش ابری، مدیریت هویت، قراردادهای هوشمند، زنجیره‌های تأمین، انفورماتیک پزشکی و ارتباطات کاربرد دارد. در ادامه به‌بررسی اجمالی این موارد پرداخته شده‌است.

توسعه فن‌آوری‌های بلاک‌چین، توجه بسیاری را به کاربرد این فن‌آوری در زمینه اینترنت اشیا سوق داده است. کاربرد گسترده دستگاه‌های دارای قابلیت محاسبات محدود برای جمع‌آوری و انتقال داده‌ها، نگرانی‌های امنیتی و حفظ حریم خصوصی قابل‌توجهی را ایجاد می‌کند. در این زمینه، Dorri و همکاران [۱۲]، چارچوبی مبتنی بر بلاک‌چین را برای خانه‌های هوشمند جهت افزایش میزان امنیت داده‌های جمع‌آوری‌شده، پیشنهاد کرده‌اند. در این بررسی، هر خانه هوشمند شامل یک ذخیره‌ساز محلی، یک ماینر خانه هوشمند، دستگاه‌های اینترنت اشیا و یک بلاک‌چین خصوصی محلی است که این اجزای محلی را کنترل می‌کند. باتوجه به اینکه، در هر طرح امنیتی، سه نیازمندی امنیتی اصلی شامل محرمانگی، صحت یا تمامیت و دردسترس‌بودن باید مورد توجه قرار گیرند، در این طرح نیز چگونگی فراهم‌نمودن این نیازمندی‌ها مطرح است. منظور از محرمانگی، اطمینان از این مسئله است که تنها کاربر مجاز، قادر به خواندن پیام فرستاده‌شده است. صحت یا تمامیت نیز به‌معنای اطمینان از بدون تغییر ماندن پیام ارسال‌شده در فرآیند انتقال می‌باشد. دردسترس‌بودن نیز به این معنا است که هر سرویس یا داده‌ای در زمان مورد نیاز برای کاربر در دسترس است.

در چارچوب مبتنی بر بلاک‌چین طراحی‌شده، هر یک از موارد امنیتی فوق با استفاده از مکانیسم خاصی فراهم می‌شود. به‌اختصار می‌توان گفت، محرمانگی در این سیستم از طریق مکانیسم رمزنگاری متقارن حاصل می‌شود. صحت و تمامیت داده‌های ارسال‌شده نیز از طریق فرآیند هش‌کردن یا درهم‌آمیختن فراهم می‌شود. درنهایت، دردسترس‌بودن نیز به‌واسطه محدودکردن تراکنش‌های قابل‌قبول به‌وسیله دستگاه‌ها و ماینرها فراهم می‌شود. بدین منظور، تراکنش‌های دریافت‌شده به‌وسیله ماینرها قبل از فرستادن به دستگاه‌ها مورد تأیید و تصدیق قرار می‌گیرند و دستگاه‌ها از درخواست‌های بدخواهانه محافظت می‌شوند.

به همین ترتیب، Polyzos و Fotiou [۱۳]، یک سیستم توزیع اطلاعات وابسته به بلاک‌چین را برای IoT معرفی کرده‌اند و چالش‌های امنیتی و حفظ حریم خصوصی و پایداری این سیستم را مورد ارزیابی قرار داده‌اند. این گروه مدلی را در نظر گرفته‌اند که در آن وظایف مربوط به بلاک‌چین به یک gateway شبکه منتقل می‌شود تا بر محدودیت‌های محاسباتی دستگاه‌های IoT غلبه کند. همانطور که قبلا هم اشاره شد، تراکنش‌های بلاک‌چین نیازمند عملیات رمزنگاری مانند امضاهای دیجیتالی هستند. با این حال، در برخی موارد بلاک‌چین نمی‌تواند از یک کار فشرده محاسباتی حمایت کند. به همین دلیل، در این مطالعه، یک رویکرد مبتنی بر gateway اتخاذ شده‌است که در آن تمام عملیات مربوط به بلاک‌چین به سمت gateway تخلیه می‌شوند و یک رابط برنامه کاربردی یا API مناسب برای هر چیزی که باید استفاده شود ارائه می‌گردد. در این طراحی، فرض شده‌است که هر ارائه‌دهنده یا مصرف‌کننده اطلاعات در شبکه، توسط یک شناسه منحصربه‌فرد شناسایی می‌شوند و این شناسه و آدرس شبکه مربوط به آن در بلاک‌چین ذخیره می‌شود. این طراحی، روشی ایمن برای شناسایی و تعیین موقعیت ارائه‌دهندگان خدمات و همچنین مصرف‌کنندگان خدمات است.

همچنین، Jung و Jang [۱۴]، یک سیستم مدیریت و جستجوی داده برای اینترنت اشیا ایجاد کرده‌اند که از بلاک‌چین برای ذخیره آدرس IP صاحب داده و نام داده، در یک تراکنش استفاده می‌کند. سیستم مدیریت داده مطرح‌شده در این مقاله بر اساس بلاک‌چین است و امنیت را با استفاده از امضای دیجیتال ECDSA و عملکرد هش SHA-256 تضمین می‌کند. این سیستم با استفاده از ویژگی‌های امنیتی بلاک‌چین مانند تأیید هویت، انکارناپذیری و صحت داده، امنیت بیشتری را در مقایسه با سیستم‌های مدیریت و جستجوی داده‌ی دیگر که از پایگاه‌داده‌ی متمرکز یا شبکه‌های P2P استفاده می‌کنند، فراهم می‌کند.

به‌طورکلی، کلان‌داده، داده‌هایی با حجم زیاد، تنوع، سرعت، صحت و ارزش بالا هستند که نمی‌توان از خدمات ذخیره‌سازی، نگهداری و تجزیه‌وتحلیل سنتی، برای رسیدگی به آن‌ها استفاده کرد. حجم بالای اطلاعات جمع‌آوری‌شده در سیستم‌های

مدیریت اطلاعات مختلف، سنگ بنایی را برای توسعه‌ی کلان‌داده فراهم می‌کند. در سال‌های اخیر، بایگانی الکترونیکی این اطلاعات با مشکلاتی از قبیل نشت اطلاعات، دستکاری و ازبین‌رفتن آن‌ها روبرو شده‌است و این امر ضرورت بهبود مدیریت اطلاعات شخصی را ایجاب می‌نماید. بنابراین، بلاک‌چین، با داشتن ویژگی‌های منحصربه فردی نظیر عدم دستکاری، قابلیت ردیابی و همچنین فرآیند پردازش غیرمتمرکز، قابلیت بالایی را برای پیشرفت فن‌آوری کلان‌داده ارائه می‌دهد [۱۵]. اگرچه بلاک‌چین از قابلیت بالایی برای مدیریت کلان‌داده‌ها برخوردار است، ولی با محدودیت‌هایی نظیر فضای ذخیره‌سازی محدود و زمان هماهنگ‌سازی کند مواجه است. در این زمینه، Chen و همکاران [۱۵]، با تجزیه‌وتحلیل محدودیت‌های معمول بلاک‌چین، یک مدل جدید ذخیره‌سازی داده on-chain و out-of-chain را مطرح کرده‌اند که قادر است مسئله‌ی افزونگی داده‌ها و فضای کافی برای ذخیره‌سازی آن‌ها را به‌طورمؤثری مرتفع نماید.

در این زمینه، Karafiloski و Mishev [۱۶]، کاربرد بلاک‌چین را برای حل چالش‌های کلان‌داده، در حوزه‌های مدیریت غیرمتمرکز داده‌های شخصی، شفافیت ویژگی‌های دیجیتال و ارتباطات IoT، بررسی کرده‌اند. در این مطالعه، راه‌حل‌های جدیدی جهت توانمندسازی زمینه‌های مختلف کلان‌داده با استفاده از فن‌آوری بلاک‌چین مطرح شده‌است.

در ارتباط با کاربرد بلاک‌چین در مدیریت کلان‌داده، Kiyomoto و همکاران [۱۷]، یک پلت‌فرم توزیع‌شده را برای مجموعه‌داده‌ی ناشناس بدون هیچ شخص ثالث قابل‌اعتماد متمرکز طراحی کرده‌اند که از بلاک‌چین منبع‌باز Hyperledger Fabric استفاده می‌کند. این پلت‌فرم متشکل از همتاها و مکانیزم‌های بلاک‌چین مبتنی بر توافق است که هر همتا به‌عنوان کارگزار، گیرنده یا تأییدکننده‌ی داده، در تراکنش انتقال داده عمل می‌کند. کارگزار داده، داده‌های شخصی را با رضایت مالک داده جمع‌آوری می‌کند، یک مجموعه داده ناشناس تولید می‌کند و آن را بین گیرندگان داده توزیع می‌کند.

رایانش ابری، به عنوان یک الگوی محاسباتی نوین، دارای مزایای زیادی از جمله انعطاف‌پذیری، کارایی بالا و دردسترس‌بودن است. با ظهور پلت‌فرم رایانش ابری، تعداد بسیاری از شرکت‌ها و اشخاص حقیقی از این فن‌آوری نوین استفاده نموده‌اند و حجم زیادی از داده‌های خود را برای صرفه‌جویی در هزینه‌های ذخیره‌سازی محلی به یک پلت‌فرم ابری انتقال داده‌اند. پلت‌فرم ابری، خدمات فوری را برای ذخیره‌سازی و محاسبات از راه دور ارائه می‌دهد، که در هر زمان و هر مکان دسترسی به داده‌ها و استفاده از آن‌ها را تسهیل می‌کند. مسئله مهم در این زمینه این است که، محیط‌های رایانش ابری باتوجه به تنوع بالای ارائه‌دهندگان خدمات آن، بسیار توزیع شده و ناهمگن هستند و این مسئله، سبب آسیب‌پذیری امنیتی این محیط‌ها می‌شود. بنابراین، تضمین امنیتی مدیریت و انتقال داده درون ابر و بین ابر و همچنین حفظ حریم خصوصی کاربران به‌عنوان یک مسئله مهم و کلیدی در محیط‌های رایانش ابری مطرح است.

باتوجه به ویژگی‌های منحصربه‌فرد فن‌آوری بلاک‌چین، یک چارچوب مبتنی بر بلاک‌چین می‌تواند، یک سیستم ایمن و کارآمد را برای برون‌سپاری داده‌ها در محیط‌های ابری فراهم کند. یکی از مهم‌ترین راه‌کارهای اطمینان از امنیت داده‌ها و همچنین حفظ حریم خصوصی کاربران در محیط‌های رایانش ابری، ذخیره‌سازی داده‌ها در قالب متون رمزنگاری‌شده بر روی سرورهای ابر است. اما چگونگی کنترل دسترسی و جستجو در داده‌های رمزنگاری‌شده یک چالش بزرگ است.

در زمینه کنترل دسترسی داده‌های رمزنگاری‌شده، Wang و همکاران [۱۸]، با استفاده از فن‌آوری بلاک‌چین، چارچوب جدیدی را جهت ذخیره‌سازی ایمن در محیط‌های ابری پیشنهاد کرده‌اند. در این طرح، مالک داده قادر است، دسترسی به داده‌ها را با استفاده از روش رمزنگاری مبتنی بر ویژگی سیاست متن رمزی[1] (CP-ABE)، کنترل نماید. در این مقاله، از فن‌آوری قرارداد هوشمند اتریوم برای ذخیره داده‌ها در شبکه بلاک‌چین، استفاده شده‌است. کاربران داده و مالکان داده از قراردادهای هوشمند اتریوم برای ذخیره و بازیابی داده‌های رمزنگاری‌شده و همچنین برای اجرای الگوریتم‌های رمزنگاری و رمزگشایی استفاده کرده‌اند. در این طرح، باتوجه به اینکه تمام رکوردهای دسترسی در بلاک‌چین ذخیره می‌شود، امکان نظارت و ردیابی بر دسترسی داده‌ها وجود دارد. بنابراین، اطلاعات منتقل شده بین کاربران داده و مالکان داده غیر قابل دستکاری و غیر قابل انکار است. در زمینه جستجو در داده‌های رمزنگاری‌شده در محیط‌های ابری نیز، فن‌آوری رمزنگاری قابل جستجو، امکان محرمانه‌بودن داده‌ها و همچنین قابلیت جستجو بر روی داده‌های رمزنگاری‌شده را فراهم می‌کند. در طرح‌های رمزنگاری قابل جستجو، برای انجام درست عملیات جستجو و بازگشت نتایج جستجو صحیح و کامل، یک سرویس ابری قابل اعتماد مورد نیاز است. با این حال، اگر سرویس ابری درستکار نباشد، حتی در

[1] Ciphertext-policy attribute-based encryption (CP-ABE)

صورت پرداخت هزینه توسط کاربر داده، ممکن است نتایج ناقص یا حتی اشتباه را به کاربر بازگرداند. از طرف دیگر، اگر نتایج جستجو قبل از پرداخت هزینه، به کاربر داده ارسال شود، کاربر غیردرستکار ممکن است عمداً از پرداخت هزینه خدمات خودداری کند، حتی اگر نتیجه جستجو صحیح باشد.

در این زمینه، Yang و همکاران [۱۹]، یک سیستم جستجوی رتبه‌بندی‌شده چندکلیدواژه مبتنی بر بلاک‌چین با قابلیت پرداخت عادلانه[1] (BMFP) را پیشنهاد داده‌اند. در این طرح، بررسی صحت و کامل‌بودن نتایج جستجو با استفاده از قراردادهای هوشمند انجام می‌شود. علاوه‌براین، قرارداد هوشمند پرداخت عادلانه هزینه‌ها را نیز تضمین می‌کند. طرح پیشنهادی BMFP، تبادل عادلانه بین پلت‌فرم ابری، مالک داده و کاربر داده را تضمین می‌کند. بدین ترتیب که، اگر سرور غیردرستکار باشد و نتایج جستجو ناقص و اشتباه بازگرداند، هزینه سپرده‌گذاری‌شده کاربر به حساب کاربر باز می‌گردد. درمقابل اگر، صحت نتایج جستجو تأیید شود، کاربر داده نمی‌تواند عمداً از پرداخت هزینه سرور و مالک داده امتناع ورزد، زیرا هزینه‌ی سپرده‌گذاری‌شده قبلاً توسط قرارداد پرداخت عادلانه قفل شده‌است. بنابراین، پرداخت عادلانه در BMFP تضمین شده است.

در همین ارتباط، Zhang و همکاران [۲۰]، یک طرح جستجوی کلید واژه قابل اعتماد بر روی داده‌های رمزنگاری‌شده[2] (TKSE) پشنهاد داده‌اند. در این طرح، شاخص داده‌ی رمزنگاری‌شده بر اساس الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA) به کاربر اجازه می‌دهد تا بر روی داده‌های رمزنگاری‌شده جستجو کند و نتایج جستجو را بر اساس صحت و درستی بررسی نماید. علاوه‌براین، این طرح، با استفاده از الگوریتم امضای دیجیتال جهت بررسی اعتبار داده‌های رمزنگاری شده در فاز ذخیره‌سازی داده‌ها، سرورهای ابر درستکار را از تهدید مالکان داده مخرب محافظت می‌کند. بدین ترتیب که، مالک داده ممکن است به طور مخربانه اطلاعات نامعتبر را در فاز ذخیره‌سازی داده‌ها برون‌سپاری کند و به طور متقلبانه از سرور ادعای جبران خسارت کند. ویژگی‌های خاص و کاربردی بلاک‌چین در این طرح نظیر توابع هش و الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA)، یک مکانیزم پرداخت عادلانه و بدون معرفی هیچ شخص سوم قابل‌اعتمادی را فراهم می‌کند.

از طرف دیگر، Liang و همکاران [۲۱]، با استفاده از فن‌آوری بلاک‌چین، یک معماری منشأ داده‌ی ابر غیرمتمرکز و مورداعتماد تحت‌عنوان ProvChain را پیشنهاد داده‌اند. منشا داده ابر، متادیتایی است که تاریخچه ایجاد و عملیات انجام شده بر روی یک شی داده ابر را ثبت می‌کند. منشأ داده‌ی مبتنی بر بلاک‌چین می‌تواند رکوردهای ضد دستکاری را ارائه دهد، شفافیت پاسخگویی به داده‌ها در ابر را فعال کند و به بهبود حریم خصوصی و دردسترس‌بودن داده‌ی منشا کمک کند. بدین‌ترتیب که، در معماری ProvChain، ابتدا رکوردهای منشا داده جمع‌آوری می‌شود، سپس تمام داده‌های هش‌شده (درهم‌آمیخته‌شده) به صورت بلاک در بلاک‌چین ذخیره می‌شود. در مرحله بعد، تمام داده‌های منشا به شکل بلاک ثبت‌شده و توسط گره‌های بلاک‌چین اعتبارسنجی می‌شوند. هر گره بلاک‌چین طی فرآیند ماینینگ داده‌های یک بلاک را تایید می‌نماید، پس از آن محتویات یک بلاک که در این معماری، رکوردهای منشا داده است، اعتبار یافته و غیرقابل تغییر می‌گردند. با سرویس منشا داده‌ی ابر مبتنی بر بلاک چین، کلیه عملیات داده‌ها به صورت شفاف و دائمی ثبت می‌شوند. بنابراین، اعتماد بین کاربران و ارائه‌دهندگان خدمات ابری به راحتی برقرار می‌شود. در این معماری، رکوردهای منشا داده با شناسه کاربر هش‌یافته مرتبط است، بدین ترتیب هر گره‌ای در شبکه بلاک‌چین نمی‌تواند رکوردهای داده‌ی مرتبط را با یک کاربر خاص پیوند دهد و تنها ارائه‌دهنده خدمات می‌تواند هر رکورد را با مالک اصلی آن پیوند دهد، بنابراین حریم خصوصی اشخاص در این معماری محفوظ می‌ماند.

Sharma و همکاران [۲۲] نیز، با توجه به نیازهای زیرساخت‌های ابری نظیر مقیاس‌پذیری، امنیت، انعطاف‌پذیری و زمان تأخیر کم، یک معماری ابری توزیع‌شده مبتنی بر بلاک‌چین را با یک شبکه تعریف‌شده نرم‌افزار[3] پیشنهاد داده‌اند. این معماری دسترسی اقتصادی، ایمن و براساس تقاضا را در زیرساخت‌های محاسباتی یک شبکه IoT فراهم می‌کند.

همچنین Xu و همکاران [۲۳]، یک چارچوب مدیریت منبع آگاه از انرژی مبتنی بر بلاک‌چین را برای مرکزداده‌های ابری بررسی کرده‌اند. با استفاده از این چارچوب می‌توان انرژی را ذخیره نمود و هزینه‌ی مرکزداده را به‌طور قابل‌توجهی کاهش داد.

علاوه بر این، Do و Ng [۲۴]، سیستمی را معرفی کرده‌اند که از فن‌آوری بلاک‌چین برای ذخیره‌سازی توزیع‌شده و ایمن

[1] Blockchain based multi-keyword ranked search with fair payment system (BMFP)
[2] Trustworthy Keyword Search scheme over Encrypted data (TKSE)
[3] Software defined networking (SDN)

داده‌ها با سرویس جستجوی کلیدواژه، استفاده می‌کند. این سیستم مشتری‌ها را جهت بارگذاری داده‌های رمزنگاری‌شده و توزیع آن‌ها در گره‌های ابری قادر ساخته و دردسترس‌بودن داده‌ها را با استفاده از تکنیک‌های رمزنگاری تضمین می‌کند.

در جامعه آنلاین امروزی، اشخاص در انواع مختلفی از فعالیت‌ها شرکت می‌کنند، حضور دیجیتالی متفاوتی را به نمایش می‌گذارند، اعتبار دیجیتالی شخصی ایجاد می‌کنند و بازخوردهایی را از جوامع آنلاینی که درگیر آن هستند، دریافت می‌کنند. این منابع اطلاعاتی متنوع پس از جمع‌آوری، می‌توانند مرجع ارزشمندی را برای بررسی هویت دیجیتال آنلاین شخصی ارائه دهند. از آنجاکه معیارهای هویت ذخیره‌شده برای استفاده از خدمات و محصولات متنوع (نظیر ایمیل، رسانه‌های اجتماعی، نرم‌افزار و غیره) ضروری است، امنیت یک هویت به سیستم‌های نرم‌افزاری زیربنایی که اطلاعات هویتی را در خود جای داده‌اند، و همچنین به ارتباطاتی که باید هویت آن‌ها تأیید شود، بستگی دارد. در این زمینه، امضای دیجیتال ابزاری مطمئن برای تأیید هویت کاربران است. کاربرد بلاک‌چین در این رابطه، با غیرمتمرکزکردن فرآیندهای دسترسی و تأیید صحت تراکنش‌ها، قادر به بهبود هویت رمزنگاری‌شده امن است [۲].

در این زمینه، Yasin و Liu [۲۵]، یک سیستم مدیریت هویت مبتنی بر بلاک‌چین و یک سیستم مدیریت قرارداد هوشمند ایجاد کرده‌اند که به طور جداگانه اعتبار آنلاین، رتبه‌بندی شخصی و رتبه‌بندی حرفه‌ای را ارزیابی می‌کنند. این سیستم‌ها به منظور تأمین امنیت هویت کاربران با استفاده از بلاک‌چین طراحی شده‌اند.

همچنین، Yan و همکاران [۲۶]، یک مخزن داده‌ی شخصی مبتنی بر بلاک‌چین[1] را پیشنهاد داده‌اند که از چارچوب OpenPDS/SafeAnswers برای ذخیره‌سازی ایمن متادیتاهای شخصی استفاده می‌کند. در این مطالعه، یک سیستم کنترل دسترسی خودکار[2] پیشنهاد شده، که دسترسی را بر اساس ارتباط بین کلیه کاربران مجاز و صاحب متادیتاها فراهم می‌کند.

در مورد هویت مربوط به دستگاه‌های محاسباتی، Zhu و همکاران [۲۷]، یک چارچوب هویت مبتنی بر بلاک‌چین را برای دستگاه‌های IoT[3] پیشنهاد داده‌اند. چارچوب طراحی شده که یک سیستم مدیریت هویت خودمختار برای دستگاه‌های IoT است، از یک بلاک‌چین برای ایجاد هویت کاربر یا مالک دستگاه و همچنین ایجاد هویت لوازم‌خانگی موردنظر استفاده می‌کند.

مفهوم قرارداد هوشمند در سال ۱۹۹۴ توسط Nick Szabo، به‌عنوان یک پروتکل تراکنش رایانه‌ای که شرایط یک قرارداد را اجرا می‌کند، معرفی شده‌است. یک قرارداد هوشمند، در حقیقت، یک شکل دیجیتالی از قرارداد حقوقی است که توسط یک برنامه رایانه‌ای اجرا می‌شود. در ارتباط با بلاک‌چین، قراردادهای هوشمند اسکریپت‌هایی هستند که روی بلاک‌چین ذخیره می‌شوند [۲۸]. اسکریپت یا زبان برنامه‌نویسی برای قراردادهای هوشمند "Solidity" نامیده می‌شود که زبانی شبیه JavaScript است [۸]. باتوجه به اینکه، هر قرارداد هوشمند در بلاک‌چین یک آدرس منحصربه‌فرد دارد، توسط پیام‌ها یا تراکنش‌های ارسال‌شده به آدرسش راه‌اندازی می‌شود. سپس با توجه به داده‌هایی که در تراکنش راه‌اندازی شده، گنجانده شده است، قرارداد به طور مستقل و خودکار روی هر گره شبکه اجرا می‌شود. به این صورت که هر گره در بلاک‌چین با یک قرارداد هوشمند فعال، یک ماشین مجازی را اجرا می‌کند، و شبکه بلاک‌چین به عنوان یک ماشین مجازی توزیع‌شده عمل می‌کند [۲۸]. هر کاربری در بلاک‌چین، می‌تواند با ارسال یک تراکنش، یک قرارداد هوشمند بسازد. توجه به این نکته مهم است که کد برنامه یک قرارداد هوشمند، پس از ایجاد آن ثابت است و نمی‌تواند تغییر یابد. با توجه به اینکه، یک قرارداد هوشمند روی بلاک‌چین مستقر است، کد آن توسط هر یک از شرکت‌کنندگان شبکه (گره‌ها) قابل بررسی است. از آنجا که تمام تعامل‌ها با یک قرارداد هوشمند از طریق پیام‌های امضاشده روی بلاک‌چین اتفاق می‌افتد، همه شرکت‌کنندگان شبکه یک اثر قابل اطمینان رمزنگاری شده از عملکرد قرارداد دریافت می‌کنند [۲۹].

اپلیکیشن‌های قرارداد هوشمند بلاک‌چین بی‌کران است، از رمزارز و تجارت تراکنش‌های ماشین به ماشین مستقل، از زنجیره تأمین و پیگیری دارایی گرفته تا کنترل دسترسی و به اشتراک‌گذاری خودکار، و از هویت دیجیتال و رای‌گیری گرفته تا صدور گواهینامه، مدیریت و اداره رکوردها، داده‌ها یا موارد گسترش می‌یابد [۸].

زنجیره تأمین، مجموعه‌ای از اشخاص است که با همکاری یکدیگر، محصول یا خدماتی را ارائه می‌دهند. جهت ایمن‌بودن محصول ارائه‌شده، صداقت بین افراد و پایبندی به مقررات اهمیت بسیاری دارد. با رشد سریع تکنولوژی‌های اینترنتی، سیستم‌های قابل ردیابی جدیدی در حوزه زنجیره تأمین مورد استفاده قرار گرفته‌است. با این حال، اغلب این سیستم‌ها متمرکز و انحصاری هستند که می‌تواند منجر به مشکلاتی نظیر تقلب، فساد، دستکاری و جعل اطلاعات شود. علاوه‌براین، سیستم‌های

[1] Blockchain-based Personal Data Store (BC-PDS)
[2] AutoNomybased Access Control (ANAC)
[3] Blockchain-based Identity Framework for IoT (BIFIT)

متمرکز در برابر فروپاشی آسیب‌پذیر هستند، چون یک نقطه‌ی شکست منجر به سقوط کل سیستم خواهد شد. جهت مقابله با این مشکلات، به‌ویژه باتوجه به رسوائی‌های مختلف ایمنی و کیفیت در صنایع غذایی، کاربرد بلاک‌چین به‌عنوان یک سیستم غیرمتمرکز برای اطمینان از قابلیت ردیابی در زنجیره تأمین مطرح شده است.

در این زمینه، Tian [۲۹]، یک سیستم ردیابی غیرمتمرکز جدید را براساس فن‌آوری بلاک‌چین و اینترنت اشیا پیشنهاد داده است. این سیستم با ارسال اطلاعات بی‌وقفه برای تمامی اعضای زنجیره تأمین در زمینه ایمنی محصولات غذایی، خطر سیستم‌های متمرکز را کاهش داده و امنیت، شفافیت، قابلیت اطمینان و همکاری بین اعضا را افزایش می‌دهد. بدیهی است که چنین سیستمی ایمنی صنایع غذایی را افزایش داده و سبب افزایش اعتماد مصرف‌کنندگان به صنایع غذایی می‌گردد.

همچنین، Lu و Xu [۳۰]، از یک پلت‌فرم بلاک‌چین کنسرسیوم تحت عنوان Origin Chain برای ارائه خدمات ردیابی در زنجیره‌های تأمین پیچیده استفاده کرده‌اند. Origin Chain، یک بلاک‌چین کنسرسیوم توزیع شده جغرافیایی است که در سه کشور در زمینه ارائه خدمات ردیابی فعال است. این برنامه، یک پلت‌فرم قابل اطمینان را بین آزمایشگاه‌ها، تأمین‌کنندگان بزرگ، خرده‌فروشان و شرکت‌ها ایجاد می‌نماید. در مقایسه با یک بلاک‌چین عمومی، این بلاک‌چین کنسرسیوم، از عملکرد بهتر و هزینه کمتری برخوردار بوده‌است.

داده‌های پزشکی، اطلاعاتی بسیار حساس و خصوصی هستند، بنابراین مطالعات قابل توجهی جهت ایجاد چارچوب‌های امنیتی مناسب در زمینه ذخیره‌سازی و حفظ این داده‌ها انجام شده است. بلاک‌چین به‌عنوان یک فن‌آوری جدید، این پتانسیل را دارد که مدیریت و انتقال داده‌های پزشکی را مستقیماً در اختیار بیماران قرار دهد، به‌صورتی‌که تاریخچه پزشکی بیمار حفظ‌شده و قابل جستجو باشد و فقط ارائه‌دهندگان درمان مجاز به مشاهده و ذخیره آن باشند.

در این زمینه، Magyar [۳۱]، یک مدل برنامه مبتنی بر بلاک‌چین را برای ذخیره‌سازی امن داده‌های پزشکی و همچنین اطمینان از دسترسی به این داده‌ها در مواقع اضطراری و حیاتی پیشنهاد داده‌است. در واقع، ویژگی‌های غیرمتمرکزبودن، عملکرد بدون واسطه و رمزنگاری شده بلاک‌چین، روش جدیدی را برای ذخیره اطلاعات بیمار به صورت ایمن و در عین حال دردسترس ارائه می‌دهد.

علاوه‌براین، Shae و Tsai [۳۲]، معماری پلت‌فرم بلاک‌چین جدید را برای آزمایشات بالینی و پزشکی دقیق پیشنهاد داده‌اند، که به‌اشتراک‌گذاری و ذخیره‌سازی اطلاعات حساس پزشکی را امکان‌پذیر می‌نماید. در این معماری چهار مؤلفه جدید شامل محاسبات موازی توزیع‌شده[1]، مدیریت ذخیره‌سازی داده‌ها[2]، مدیریت هویت ناشناس[3] و مدیریت اشتراک‌داده‌ها[4] به سیستم بلاک‌چین سنتی اضافه شده‌است. این مؤلفه‌ها در تجزیه و تجلیل و ذخیره‌سازی ایمن این حجم بالا از داده‌ها و همچنین حفظ حریم خصوصی بیماران و همزمان با آن به‌اشتراک‌گذاری داده‌ها جهت تحقیقات پزشکی مشترک نقش دارند.

علاوه‌براین، Azaria و همکاران [۳۳]، سیستم مدیریت داده‌ی غیرمتمرکز جدید تحت عنوان MedRec را با استفاده از فن‌آوری بلاک‌چین، برای ذخیره‌سازی و به‌اشتراک‌گذاری داده‌های پزشکی ارائه داده‌اند. این سیستم یک گزارش جامع، غیرقابل تغییر و در دسترس از اطلاعات پزشکی را از طریق ارائه‌دهندگان و سایت‌های درمانی به بیماران می‌دهد. با استفاده از ویژگی‌های منحصربه‌فرد بلاک‌چین، MedRec هنگام تأیید اطلاعات حساس، احراز هویت، محرمانه‌بودن، پاسخگویی و به‌اشتراک‌گذاری داده‌ها را مدیریت می‌کند.

کاربرد بلاک‌چین برای مدیریت ارتباطات و شبکه، امکان ارتباطات شبکه‌ای ایمن و تأییدشده را فراهم می‌کند. علاوه‌بر ارتباطات ایمن، ذخیره‌سازی داده‌های رمزنگاری‌شده و پیاده‌سازی قراردادهای هوشمند مزایای دیگری هستند که می‌توانند با کمک زیرساخت‌های شبکه مبتنی بر بلاک‌چین محقق شوند.

در این زمینه، Cha و همکاران [۳۴]، یک طرحی از دروازه متصل به بلاک‌چین[5] را ارائه داده‌اند که حریم خصوصی کاربر را برای دستگاه‌های IoT در شبکه بلاک‌چین حفظ می‌کند. این سیستم با محافظت از اطلاعات حساس کاربران از نشت حریم خصوصی جلوگیری می‌نماید. در این طراحی، یک مکانیزم امضای دیجیتال قوی به منظور احراز هویت و مدیریت ایمن حریم خصوصی ارائه شده است.

همچنین، Yin و همکاران [۳۵]، یک پارادایم شبکه‌ای و محاسباتی قابل‌اعتماد، غیرمتمرکز و جدید تحت‌عنوان HyperNet، را برای مقابله با چالش ازدست‌دادن کنترل داده‌ها،

[1] Distributed parallel computing
[2] Data storage management
[3] Anonymous identity management
[4] Data sharing management
[5] Blockchain connected gateway

ارائه داده‌اند. HyperNet از سیستم سلولی دیجیتال شخصی[1] (PDC) هوشمند تشکیل شده است که به عنوان کلون دیجیتال یک فرد انسانی در نظر گرفته می‌شود. ارتباط قابل اعتماد و غیرمتمرکز در این الگوی شبکه‌ای، مدیریت ایمن شی دیجیتال و مکانیسم مسیریابی شناسه‌محور[2] را امکان‌پذیر می‌سازد.

۴-چالش‌های مرتبط با فن‌آوری بلاک‌چین

بلاک‌چین به عنوان یک فن‌آوری نوظهور، با چالش‌ها و مشکلات متعددی روبرو است. در این مقاله، دو چالش اصلی شامل الزامات عملکردی و اجرایی و همچنین امنیت سیستم‌های بلاک‌چین مورد بررسی قرار گرفته‌است.

بلاک‌چین، شامل مجموعه‌ای از تراکنش‌ها در طول زمان است که تغییر آن‌ها دشوار است. مشکل اصلی این است که با رشد مداوم تعداد تراکنش‌ها، اندازه بلاک‌چین نیز افزایش می‌یابد. نتیجه این رشد مداوم نه تنها افزایش میزان هزینه‌های ذخیره‌سازی است، بلکه در کاهش سرعت توزیع بلاک‌چین روی شبکه نیز تأثیرگذار است. علاوه‌براین، بلاک‌چین‌های عمومی، به‌منظور بهره‌گیری از امنیت مکانیزم توافق، یک محدودیت‌هایی را بر روی اندازه بلاک و بازه زمانی تراکنش‌ها ایجاد می‌کنند، که این مسئله در نهایت منجر به کاهش بازده تراکنش‌ها می‌شود. مقیاس‌پذیری مسئله مهمی است و باید در طراحی برنامه‌های بلاک‌چین در نظر گرفته شود [۲]. برای حل مسئله مقیاس‌پذیری، طرح‌های متعددی مورد بررسی و مطالعه قرار گرفته است که به دو گروه اصلی، بهینه‌سازی ذخیره‌سازی و طراحی مجدد بلاک‌چین، طبقه‌بندی شده‌است [۳].

در روش اول، سوابق تراکنش‌های قدیمی توسط شبکه حذف می‌شود و از پایگاه‌داده‌ای به نام درخت حساب[3] استفاده می‌شود تا تعادل همه‌ی آدرس‌های غیرخالی را حفظ کند. به این ترتیب، گره‌ها برای بررسی اینکه آیا یک تراکنش معتبر است یا خیر، نیازی به ذخیره کلیه تراکنش‌ها ندارند. در روش دوم، هر بلاک معمولی به دو بخش تقسیم می‌شود، بلاک اصلی برای انتخاب رئیس و میکروبلاک برای ذخیره تراکنش‌ها در نظر گرفته می‌شود. در این روش، بلاک‌چین مجدداً طراحی شده و رابطه‌ی بین اندازه بلاک و امنیت شبکه مورد بررسی قرار می‌گیرد [۳]. مسئله مهم در این زمینه، تهیه یک راه‌حل مقیاس‌پذیر است که با برنامه‌های موجود مطابقت داشته باشد.

Xie و همکاران [۳۶] ، یک مقاله‌ی مروری بر روی مفهوم مقیاس‌پذیری در سیستم‌های بلاک‌چین و همچنین راه‌حل‌های موجود در این زمینه را ارائه نموده‌اند. نویسندگان در این مقاله، مسئله‌ی مقیاس‌پذیری بلاک‌چین را از سه دیدگاه توان عملیاتی، ذخیره‌سازی و شبکه مورد تجزیه و تحلیل قرار داده‌اند. سپس در ادامه‌ی مقاله، تعدادی از تکنولوژی‌های فعال برای مقیاس‌پذیری سیستم‌های بلاک‌چین از جمله تکنولوژی‌های فعال مرتبط با تعداد تراکنش‌ها در هر بلاک، شامل (افزایش سایز بلاک، کاهش سایز تراکنش و کاهش تعداد تراکنش‌های پردازش‌شده توسط گره‌ها از طریق (تراکنش‌های Off-chain، تقسیم‌بندی، مدیریت/کنترل جدا از اجرا)، تکنولوژی‌های فعال مرتبط با بازه‌ی زمانی بلاک، شامل (A single leader،Fixed leaders و Collective leaders)، تکنولوژی‌های فعال مرتبط با ذخیره‌سازی داده و تکنولوژی‌های فعال مرتبط با انتقال داده، شامل (اتخاذ روش‌های انتقال داده‌ی مؤثر و کاهش مقدار داده‌ی منتشر شده از طریق شبکه‌ی بلاک‌چین) را مطرح نموده‌اند.

Zhou و همکاران [۳۷] نیز، در مقاله‌ای تعدادی از راه‌حل‌های موجود برای حل مسئله‌ی مقیاس‌پذیری بلاک‌چین را در سه لایه، لایه‌ی ۰، لایه‌ی ۱ (راه‌حل‌های ON-CHAIN) و لایه‌ی ۲ (راه‌حل‌های NON ON-CHAIN) طبقه‌بندی نموده‌اند. راه‌حل‌های لایه‌ی ۰، در یک دسته‌ی انتشار داده، شامل (erlay، kadcast، velocity و bloXroute) ، راه‌حل‌های لایه‌ی ۱، در چهار دسته‌ی راه‌حل‌های مرتبط با بلاک داده، شامل (گواهی مجزا، Bitcion-cash، فشرده‌سازی بلاک، بهینه‌سازی طرح ذخیره‌سازی) ، استراتژی‌های توافق مختلف، شامل (اثبات کار، اثبات سهام، اثبات سهام محول‌شده، تحمل خطای بیزانس عملی، توافق هیبرید، اثبات اختیار، اثبات ظرفیت و اثبات مشارکت) ، تقسیم‌بندی، شامل (Elastico، OMNILEDGER، RapidChain و MONOXIDE) و گراف غیر مدور مستقیم و راه‌حل‌های لایه‌ی ۲، در پنج دسته‌ی کانال پرداخت، شامل (شبکه‌ی LIGHTNING و شبکه‌ی RAIDEN) ، زنجیره‌ی جانبی، شامل (PLASMA و شبکه‌ی LIQUIDITY) ، محاسبات OFF-CHAIN، شامل (TRUEBIT و ARBITRUM) و تکنیک‌های CROSS-CHAIN، شامل (COSMOS و POLKADOT) طبقه‌بندی شده‌اند.

علاوه‌براین، Hafid و همکاران [۳۸]، در مقاله‌ی خود راه‌حل‌های مقیاس‌پذیری بلاک‌چین را تشریح نموده‌اند. آن‌ها راه‌حل‌های بلاک‌چین را در دو لایه طبقه‌بندی نموده‌اند که در لایه‌ی اول اصلاحاتی (به‌عنوان‌مثال، تغییر ساختار بلاک‌چین،

[1] Personal digital cellular (PDC)
[2] Identifier-driven routing
[3] Account tree

مانند اندازه بلاک) را پیشنهاد می‌دهند و در لایه‌ی دوم مکانیسم‌هایی را پیشنهاد می‌دهند که خارج از بلاک‌چین اجرا می‌شوند.

علاوه بر مقیاس‌پذیری، دردسترس‌بودن سیستم بلاک‌چین یکی از مشکلات بالقوه در زمینه عملکرد این سیستم‌ها است. به‌طورکلی می‌توان گفت که توان عملیاتی پایین و تأخیر تراکنش یک چالش مداوم در بلاک‌چین است. در واقع با افزایش حجم تراکنش‌ها، سیستم‌های بلاک‌چین معمولی نمی‌توانند فعالیت خود را به‌درستی انجام دهند. به‌منظور بررسی عملکرد سیستم‌های بلاک‌چین، Dinh و همکاران [۳۹]، ارزیابی جامعی را از سه سیستم بلاک‌چین شامل سیستم‌های Ethereum، Parity و Hyperledger Fabric براساس چارچوب طراحی‌شده‌ی BLOCKBENCH، انجام داده‌اند. BLOCKBENCH، یک چارچوب معیار برای درک عملکرد بلاک‌چین‌ها در برابر بارکاری پردازش داده است. در این بررسی معیارهایی نظیر توان عملیاتی، زمان تأخیر، زمان اجرا و میزان مصرف حافظه مورد سنجش قرار گرفته‌است. نتایج این بررسی نشان داده‌است که بلاک‌چین Hyperledger Fabric دارای بهترین عملکرد در بین سیستم‌های ذکرشده می‌باشد. بنابراین، با درنظرگرفتن تعداد تراکنش‌های مورد نیاز در یک بازه‌زمانی خاص، می‌توان قابلیت اجرای سیستم‌های بلاک‌چین را بر اساس نوع استفاده، مورد تجزیه‌وتحلیل قرار داد. در مورد دستگاه‌های منفرد IoT، بلاک‌چین‌های خصوصی مناسب هستند، ولی در ارتباط با سیستم‌های هوشمند مبتنی بر IoT یا سیستم‌های کلان‌داده امکان استفاده از بلاک‌چین‌ها دشوارتر می‌شود.

امنیت بلاک‌چین، دقیقاً شبیه هر سیستم دیگری، به امنیت اجرای اصلی آن در نرم‌افزار و سخت‌افزار و همچنین پروتکل‌های لازم برای عملکرد آن بستگی دارد. درحالی‌که، مکانیسم توافق، راهی برای اطمینان از عدالت و اعتماد در یک سیستم غیرقابل‌اعتماد در نظر گرفته می‌شود، از طرف دیگر هدفی را برای مهاجمان احتمالی فراهم می‌کند.

Li و همکاران [۴۰] ، یک مقاله‌ی مروری بر روی مفهوم امنیت در سیستم‌های بلاک‌چین را ارائه نموده‌اند. آن‌ها در این مقاله، ریسک‌های امنیتی رایج در سیستم‌های بلاک‌چین را به نه دسته، شامل آسیب‌پذیری ۵۱ درصد، امنیت کلید خصوصی، فعالیت خاطی، هزینه مضاعف و نشت حریم خصوصی تراکنش در بلاک‌چین‌های ۱.۰ و ۲.۰ و قراردادهای هوشمند خاطی، آسیب‌پذیری در قراردادهای هوشمند، قراردادهای هوشمند Under-optimized و عملیات Under-priced در بلاک‌چین‌های ۲.۰ تقسیم‌بندی نموده‌اند. همچنین در بخشی از مقاله، حملات واقعی بر روی سیستم‌های بلاک‌چین از جمله حمله‌ی ماینینگ خودخواه، حمله‌ی سازمان خودگردان غیرمتمرکز، حمله‌ی سرقت پروتکل gateway مرزی، حمله‌ی گرفتگی، حمله‌ی Livenes و حمله‌ی Balance را توصیف نموده‌اند. در بخش دیگری نیز، پیشرفت‌های امنیتی برای سیستم‌های بلاک‌چین از جمله SmartPool، Framework Quantitative، Oyente، Hawk و Town Crier را که می‌توانند برای توسعه‌ی سیستم‌های بلاک‌چین مورد استفاده قرار گیرند، توصیف نموده‌اند.

علاوه‌براین، در تمام تراکنش‌های عمومی، نشت حریم خصوصی یک مسئله بالقوه است [۲]. اعتقاد کلی بر این است که بلاک‌چین بسیار ایمن است، زیرا کاربران فقط با آدرس‌های ایجادشده به جای هویت واقعی، تراکنش انجام می‌دهند. علاوه‌براین، کاربران می‌توانند در صورت نشت اطلاعات خود، آدرس‌های جدید بسیاری ایجاد کنند. اگرچه در بلاک‌چین، آدرس کاربران نام‌های مستعار هستند، اما پیوند دادن آدرس‌ها به هویت واقعی کاربران امکان‌پذیر است، زیرا بسیاری از کاربران مرتباً با همان آدرس تراکنش انجام می‌دهند.

Biryukov و همکاران [۴۱] ، روشی را برای پیوند نام مستعار کاربر به آدرس‌های IP آن‌ها، حتی وقتی کاربران پشت NAT یا فایروال‌ها هستند، ارائه داده‌اند. با توجه به تحقیقات Biryukov و همکاران، هر مشتری می‌تواند با مجموعه‌ای از گره‌هایی که به آن متصل می‌شود، بطور منحصربه‌فرد شناسایی شود. درواقع، این مجموعه می‌تواند برای یافتن منشأ تراکنش مورد استفاده قرار گیرد.

یکی از ویژگی‌های دیگر بلاک‌چین این است که به کاربران خود اجازه می‌دهد تراکنش‌های ناشناس انجام دهند. با این وجود، از آنجا که تراکنش‌ها عمومی است، ممکن است سرنخ‌هایی قابل ردیابی وجود داشته باشد که بتوانند هویت و اطلاعات خصوصی کاربران را آشکار سازند. در ارتباط با مسائل مربوط به حفظ ناشناس‌بودن در بلاک‌چین‌ها، چندین طرح پیشنهاد شده است که شامل مخلوط کردن آدرس‌های ورودی متعدد به چندین آدرس خروجی، پنهان کردن مقادیر و ارزش‌های سکه‌های پنهان شده توسط کاربران در تراکنش و غیره می‌باشد [۳]. در این ارتباط سرویس خاصی تحت‌عنوان Mixing service وجود دارد که نوعی سرویس است که با انتقال وجه از آدرس‌های ورودی چندگانه به آدرس‌های خروجی چندگانه، ناشناس بودن را فراهم می‌کند.

در زمینه‌ی حفظ حریم خصوصی در سیستم‌های بلاک‌چین، Bernabe و همکاران [۴۲]، در مقاله‌ای مروری بر راه‌حل‌های موجود برای حفظ حریم خصوصی را مطرح نموده‌اند. در این مقاله، تعدادی از چالش‌های حریم خصوصی از جمله پیوندپذیری تراکنش‌ها، مدیریت و بازیابی کلیدهای خصوصی، قراردادهای هوشمند بدخواه، حریم خصوصی داده‌های غیرقابل پاک‌شدن و داده‌های on-chain، مقاومت در برابر محاسبات POST-QUANTUM، عملکرد CRYPTO-PRIVACY، PRIVACY-USABILITY، شخص سوم قابل اعتماد مخرب یا کنجکاو، اجرای حریم خصوصی در سیستم‌های محدود شده و قابلیت همکاری حریم خصوصی در سراسر سناریوهای بلاک‌چین مختلف توصیف شده است. همچنین در بخشی از این مقاله، تکنیک‌ها و راه‌حل‌های رمزنگاری اصلی، از جمله محاسبات چند جانبه ایمن، اثبات دانش صفر، طرح‌های تعهد، zkSNARK، امضای حلقه و پنهان‌سازی همگن که می‌توانند به عنوان پایه‌ای برای حفظ حریم خصوصی در بلاک‌چین استفاده شوند، معرفی شده‌اند.

همچنین، WANG و همکاران [۴۳]، یک مقاله‌ی مروری بر روی مفهوم حفظ حریم خصوصی در بلاک‌چین را ارائه نموده‌اند. نویسندگان در این مقاله، چالش‌های حفظ حریم خصوصی بلاک‌چین را به دو جنبه‌ی هویت کاربر و تراکنش‌های کاربر تقسیم نموده و سپس چندین تکنیک کلیدی از جمله مکانیزم COIN MIXING، اثبات دانش صفر، امضای حلقه، رمزنگاری همگن، آدرس پنهان، طرح تعهد PEDERSEN، محاسبات چند جانبه ایمن و محیط اجرای قابل اعتماد را برای حفظ حریم خصوصی بلاک‌چین با توجه به آن دو جنبه چالش مطرح شده، پیشنهاد نموده‌اند.

در همین ارتباط، Feng و همکاران [۹] نیز، مروری بر مفهوم حفظ حریم خصوصی در سیستم‌های بلاک‌چین را بررسی نموده‌اند. نویسندگان در این مقاله، نیازمندی‌های حریم خصوصی که باید در نظر گرفته شود را به دو عامل حریم خصوصی هویت و حریم خصوصی تراکنش تقسیم نموده‌اند. در این مقاله، تهدیدات حریم خصوصی برای بلاک‌چین در دو دسته‌ی آشکارسازی هویت، شامل (تجزیه و تحلیل شبکه، خوشه‌بندی آدرس، انگشت نگاری تراکنش، حملات انکار سرویس و حمله‌ی Sybil) و در معرض قرار گرفتن الگوی تراکنش، شامل (تجزیه و تحلیل گراف تراکنش و تجزیه و تحلیل استقرار در سطح AS) تقسیم‌بندی شده است. سپس نویسندگان در این مقاله برای حفظ حریم خصوصی هویت، روش‌های Mixing Services، امضای حلقه و اثبات دانش صفر غیر تعاملی و برای حفظ حریم خصوصی تراکنش، روش‌های اثبات دانش صفر غیر تعاملی و سیستم رمزنگاری همگن را معرفی نموده‌اند.

علاوه‌براین، دو نوع تهدید اساسی علیه فن‌آوری بلاک‌چین از جمله حمله اکثریت[1] و ماینینگ خودخواه[2] وجود دارد که در ادامه به اختصار توضیح داده شده‌است.

به‌طورکلی، در بلاک‌چین، کلیه تراکنش‌ها پس از اعمال مکانیسم توافق و تأیید یک بلاک در زنجیره، تغییرناپذیر تلقی می‌شوند. با توجه به اینکه بلاک‌چین در گره‌های مستقل بسیاری تکثیر و توزیع می‌شود، هیچ گره منفرد یا مجموعه کوچکی از گره‌ها نمی‌توانند بلاک‌چین را دستکاری کنند. از آنجاکه بلاک‌چین در گره‌های متعدد تکرار می‌شود، برای حفظ توافق در مورد وضعیت فعلی صحیح بلاک‌چین از الگوریتم توافق توزیع‌شده استفاده می‌شود. به‌این‌ترتیب، حتی اگر برخی از گره‌ها (ماینرها) سعی کنند محتوای بلاک‌چین را دستکاری کنند، تا زمانی که اکثریت درستکار باشند، تصمیم‌گیری بر اساس اکثریت آرا می‌تواند صحت بلاک‌چین را تضمین کند [۱]. با این وجود، حمله اکثریت، زمانی اتفاق می‌افتد که بیش از نیمی از قدرت پردازشی کل شبکه در اختیار یک گروه یا یک فرد قرار بگیرد. در این شرایط، آن‌ها می‌توانند هر فرآیندی را متوقف و تراکنش‌ها را دستکاری کنند [۲]. در برخی موارد، یک مهاجم می‌تواند تعداد زیادی سیستم ایجاد کند که هرکدام به عنوان یک شرکت کننده به بلاک‌چین بپیوندند. در نتیجه مهاجم می‌تواند اکثریت سیستم‌های شرکت کننده را کنترل کند [۱]. در این حالت، کل فرآیند نوشتن بلاک در زنجیره قابل هک نمودن است و بلاک‌های بالقوه نادرست قابلیت ورود به زنجیره را می‌یابند. علاوه‌براین، با کنترل بخشی از قابلیت محاسباتی گره‌ها، یک مهاجم قادر است تاریخچه تقریباً تمام تراکنش‌ها را با جعل بازیابی کند و یک تاریخچه اصلاح‌شده یا جعلی ارائه دهد [۲].

برخلاف حمله اکثریت، می‌توان مهاجمی را در نظر گرفت که کمتر از پنجاه درصد از کل توان محاسباتی را در اختیار داشته باشد که هنوز بسیار خطرناک است. در ماینینگ خودخواه، مهاجم (ماینر) ، بلاک‌ها را به جای پخش‌کردن آن‌ها در شبکه، در یک شعبه خصوصی قرار می‌دهد. با افزایش تعداد بلاک‌ها و طولانی‌تر شدن این زنجیره خصوصی، احتمال گرایش ماینرهای دیگر به این زنجیره بیشتر می‌گردد. تمایل ماینرها به عضویت در این شعبه خصوصی با انگیزه‌های مختلف، سبب افزایش قدرت

[1] Majority Attack
[2] Selfish Mining

محاسباتی ماینرهای خودخواه و توانایی استخراج زنجیره‌ای طولانی‌تری می‌گردد. در نهایت ماینر خودخواه کنترل اکثریت شبکه را به‌دست گرفته و امکان هرگونه دستکاری و جعل در تراکنش‌ها وجود دارد [۲].

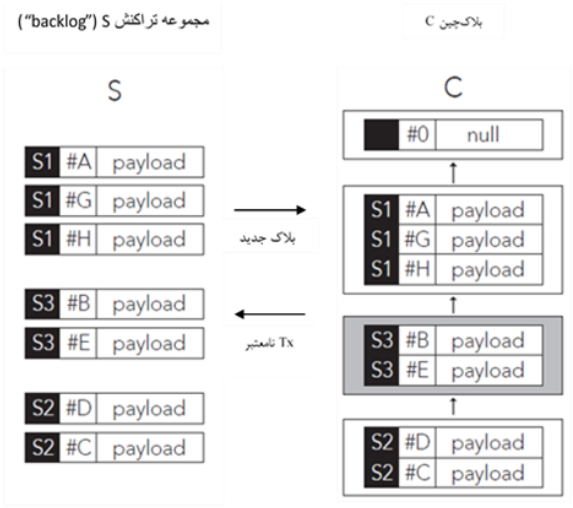
۵-تقویت عملکرد بلاک‌چین

عملکرد یک سیستم بلاک‌چین دارای سه مؤلفه اصلی شامل مدیریت توافق، مدیریت دسترسی حالت[1] و اجرای قرارداد هوشمند است. درواقع، عملکرد پردازش تراکنش‌ها، تحت تسلط عملکرد مدیریت توافق قرار دارد. مدیریت دسترسی حالت، روش‌های دسترسی جهت بازیابی حالت فعلی بلاک‌چین است که یک فهرست ساده برای یافتن تراکنش‌ها از یک شناسه حساب یا شناسه کاربری خاص تا سیستم‌های ذخیره ارزش کلیدی، و حتی یک رابط SQL کامل را شامل می‌گردد. در سیستم‌های بلاک‌چین، اجرای قراردادهای هوشمند، معمولاً در یک محیط مجازی برای امنیت و ایمنی بیشتر انجام می‌شود [۱].

میزان پردازش تراکنش‌ها، که به توان عملیاتی سیستم اشاره دارد، در سیستم بلاک‌چین به طورقابل‌توجهی کم‌تر از سیستم‌های پایگاه‌داده‌ی سنتی است. دلیل این امر هم وجود الگوریتم‌های توافق است، که سبب محدودیت تعداد بلاک‌هایی می‌شوند که باید در واحد زمان به زنجیره اضافه شوند. در اغلب کاربردها، توان عملیاتی تراکنش‌ها، تنها معیار عملکرد نیست. معیار دوم و اغلب مهم‌تر، تأخیر تراکنش یا زمان پاسخ است. در اینجا نیز الگوریتم‌های توافق موردنیاز سیستم‌های بلاک‌چین یک مسئله جدی است. درحالی‌که در سیستم‌های پایگاه‌داده‌ی سنتی، تراکنش‌های منفرد انجام می‌شود و این سیستم‌ها می‌توانند به راحتی به زمان پاسخ میلی‌ثانیه برسند [۱].

دو رویکرد اصلی برای بهبود عملکرد توافق در سیستم‌های بلاک‌چین وجود دارد که شامل تقسیم‌بندی‌کردن و پردازش تراکنش‌های Off-chain است. در روش اول، نوعی توزیع‌کار بین گره‌ها جهت استخراج بلاک‌های جدید انجام می‌شود که سبب ایجاد حالت توازی و برابری بین گره‌ها می‌گردد. در روش دوم، سیستم‌های قابل‌اعتماد تراکنش‌ها را به‌صورت داخلی و بدون قراردادن آن‌ها در بلاک‌چین انجام می‌دهند. سپس این تراکنش‌ها در یک تراکنش واحد گروه‌بندی شده و در بلاک‌چین قرار می‌گیرند. این گروه‌بندی ممکن است متناوباً انجام شود یا فقط در خاتمه توافق رخ دهد [۱]. یکی از مشکلات اصلی روش اول این است که تقسیم‌بندی گره‌های ماینینگ (استخراج‌کننده)، باعث ایجاد مجموعه‌های کوچکتر از ماینرها می‌شود که بیشتر در معرض حمله قرار می‌گیرند، زیرا هزینه حمله به مجموعه‌های کوچکتر کمتر است. با این وجود روش‌هایی برای کاهش این ریسک وجود دارد. در روش دوم نیز، مدیریت تراکنش‌های Off-chain، به استقرار یک سیستم جداگانه نیازمند است. شناخته‌شده‌ترین شبکه در این زمینه، شبکه‌ی Lightning است، که تراکنش‌های بلاک‌چین را از طریق پردازش off-chain سرعت می‌بخشد و توان عملیاتی و تاخیر تراکنش‌ها را در حد یک سیستم پایگاه‌داده‌ی سنتی تضمین می‌کند [۱].

مسئله مهم دیگر این است که برخی از سیستم‌های بلاک‌چین، یک شاخصی را در شناسه کاربر یا شناسه حساب، جهت تسهیل در جستجوی تراکنش‌های ساده، ارائه می‌دهند. با این وجود، قراردادهای هوشمند پیچیده به اجرای پرس‌وجوهای همه‌منظوره در برابر وضعیت فعلی ذخیره‌شده بلاک‌چین نیازمند هستند.



شکل (۲) : معماری BigchainDB [۴۵]

سیستم‌های بلاک‌چین ساخته‌شده بر روی یک پایگاه‌داده سنتی یا NoSQL اطلاعات وضعیت را در آن پایگاه‌داده نگهداری می‌نمایند و اجرای پرس‌وجوهای سبک پایگاه‌داده سطح بالاتری را برای قراردادهای هوشمند امکان‌پذیر می‌نمایند. این مزیت به قیمت استفاده از یک قالب ذخیره‌سازی پایگاه‌داده است که ممکن است فاقد محافظت دقیق رمزنگاری‌شده یک بلاک‌چین واقعی باشد. یک راهکار مناسب در این زمینه، این است که پایگاه‌داده توسط یک ارائه‌دهنده معتبر میزبانی شود و

[1] State-access management

به‌روزرسانی نه تنها برای پایگاه‌داده بلکه برای بلاک‌چین نیز انجام شود[۱] .

BigchainDB نمونه‌ای از بلاک‌چین است که از یک پایگاه‌داده برای ذخیره حالت استفاده می‌کند و امکان جستجوی آن حالت را دارد. یک پایگاه‌داده توزیع‌شده مدرن دارای توان بیش از ۱ میلیون تراکنش در هر ثانیه، ظرفیت در حد پتابایت، تأخیر زمانی درحد کسری از ثانیه و توان و ظرفیتی است که با افزودن گره ها افزایش می یابد. پایگاه‌داده‌های مدرن همچنین توانایی لازم برای افزودن، پرس‌وجو و کنترل دسترسی در SQL یا NoSQL را دارند.

نرم‌افزار BigchainDB، اولین بار در فوریه ۲۰۱۶ انتشار یافت. این نرم‌افزار به دلیل داشتن برخی از خصوصیات بلاک‌چین و برخی از خصوصیات پایگاه‌داده، یک پایگاه‌داده بلاک‌چینی نامیده می‌شود. طراحی اصلی این نرم‌افزار با یک پایگاه‌داده آغاز شد و سپس برخی از ویژگی‌های بلاک‌چین نظیر غیرمتمرکز بودن و تغییرناپذیری به آن اضافه شد. ایده این بود که سیستم حاصل از آن خواص مطلوب پایگاه داده مانند تأخیر کم، نرخ تراکنش بالا، ظرفیت بالا، نمایه‌سازی و پرس‌وجو از داده‌های ساختار یافته را به ارث ببرد [۴۴.۴۵].

نرم‌افزارBigchainDB، رابط برنامه‌نویسی کاربردی[1] خود را که یک پایگاه‌داده بلاک‌چین واحد است، به مشتری‌ها ارائه می‌دهد. همانطور که در شکل (۲) قابل مشاهده می‌باشد، در معماری این نرم‌افزار، دو پایگاه‌داده توزیع شده، شامل پایگاه‌داده S (مجموعه تراکنش‌ها یا backlog) و پایگاه‌داده C (بلاک‌چین) وجود دارد که توسط الگوریتم توافق BigchainDB[2] متصل شده‌اند. هر یک از پایگاه‌داده‌های توزیع شده‌ی S و C، یک پایگاه‌داده کلان‌داده قابل‌دسترس[3] هستند. اولین پایگاه‌داده (پایگاه‌داده S)، مجموعه‌ای از تراکنش‌های نامرتب را نگهداری می‌نماید. هنگامی که یک تراکنش وارد می‌شود، ابتدا توسط گره گیرنده اعتبارسنجی می‌گردد و در صورت اعتبار، در S ذخیره می‌شود. علاوه‌براین، گره گیرنده، تراکنش‌ها را به طور تصادفی به گره‌های دیگر اختصاص می‌دهد. گره k که الگوریتم BCA را اجرا می‌کند تراکنش‌ها را از مجموعه نامرتب Sk (مجموعه تراکنش‌های اختصاص یافته به گره k) به یک لیست مرتب منتقل می‌کند، و یک بلاک برای تراکنش‌ها ایجاد می‌کند و سپس بلاک را در پایگاه‌داده C قرار می‌دهد. C لیست بلاک‌های مرتب است که هر بلاک به یک بلاک والد و داده‌های آن، یعنی یک بلاک‌چین ارجاع داده می‌شود.

BigchainDB، داده‌های خود را در پایگاه‌داده‌ای به نام bigchain ذخیره می‌کند. پایگاه‌داده bigchain شامل چندین مجموعه از جمله تراکنش‌ها، دارایی‌ها، متادیتا و بلاک‌ها است. این مجموعه‌ها را می‌توان با استفاده از پرس‌وجوهای MongoDB جستجو کرد. هر اپراتور گره می‌تواند تصمیم بگیرد که چگونه به کاربران خارجی اجازه بدهد که از پایگاه‌داده MongoDB محلی خود اطلاعاتی را کسب کنند. در نسخه‌های قدیمی BigchainDB، تنها یک پایگاه‌داده MongoDB وجود داشت، بنابراین در معرض قرار گرفتن این پایگاه‌داده برای کاربران خارجی بسیار ریسک‌پذیر بود. در BigchainDB نسخه ۲.۰.۰ و بعد از آن، هر گره BigchainDB، همانطور که در شکل (۳) مشخص است، دارای پایگاه‌داده‌ی محلی MongoDB خاص خود است. در این معماری، ارتباطات بین گره‌ها با استفاده از پروتکل‌های توافق Tendermint، انجام می‌شود. در این حالت اگر پایگاه‌داده محلی MongoDB یک گره به خطر بیفتد، هیچ یک از پایگاه‌داده‌های MongoDB دیگر (در گره‌های دیگر) تحت تأثیر قرار نمی‌گیرند. علاوه‌براین، پردازش پرس‌وجو می‌تواند کاملاً منبع محور باشد، در این حالت قراردادن MongoDB در یک دستگاه جداگانه از دستگاه‌هایی که BigchainDB Server و Tendermint Core را اجرا می‌کنند، راه‌حل مناسبی است. از طرف دیگر، برخی از پرس‌وجوها ممکن است خیلی طولانی باشد یا از منابع متعددی استفاده کند. یک اپراتور گره قادر است، کران‌های بالایی را برای منابع پرس‌وجو قرار دهد و هر پرس‌وجویی را که از این مرزها فراتر رفت متوقف کند. برای کارآمدترشدن پرس‌وجوهای MongoDB، می‌توان شاخص‌هایی ایجاد کرد. این شاخص‌ها ممکن است توسط اپراتور گره یا توسط برخی کاربران خارجی ایجاد شود.

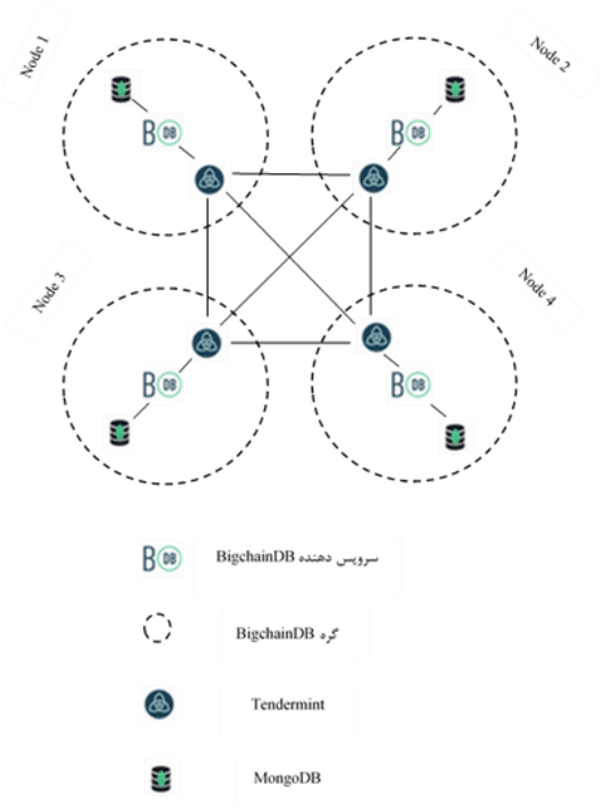
پایگاه‌داده BigchainDB قابلیت ذخیره‌سازی انواع داده‌ها را داراست، اما به‌گونه‌ای طراحی شده است که برای ذخیره‌سازی، ثبت و انتقال دارایی‌ها مناسب است. تراکنش ایجاد، برای ثبت هر نوع دارایی به همراه متادیتاهای مربوطه مورد استفاده قرار می‌گیرد. مالکان دارایی می‌توانند شرایط (رمزنگاری) را مشخص کنند که باید توسط هر کسی که بخواهد دارایی را به مالکان جدید منتقل کند، اجرا شود. BigchainDB، اجرای شرایط ذکرشده را به‌عنوان بخشی از مسیر بررسی اعتبار تراکنش انتقال، تأیید می‌کند. به‌این‌ترتیب، BigchainDB مانع از دو بار خرج‌کردن دارایی می‌شود.

[1] Application programming interface (API)
[2] BigchainDB Consensus Algorithm (BCA)
[3] Off-the-shelf big data

BigchainDB قابلیت ذخیره‌سازی کد منبع هر قرارداد هوشمند (یعنی یک برنامه رایانه‌ای) را داراست، اما قراردادهای هوشمند دلخواه را اجرا نمی‌کند. یک شبکه BigchainDB می‌تواند از طریق oracleها یا پروتکل‌های ارتباطی بین زنجیره‌ای به شبکه‌های دیگر بلاک‌چین متصل شود و به‌نوعی برای اجرای قراردادهای هوشمند مورد استفاده قرار گیرد [۴۴.۴۵].

BigchainDB، دارای ویژگی‌هایی نظیر تغییر ناپذیری، غیرمتمرکز بودن، دارایی‌های تحت کنترل مالک، نرخ بالای تراکنش، تاخیر کم، نمایه‌سازی و پرس‌وجوی داده‌های ساختاریافته، تحمل خطای بیزانس و تحمل خطای Sybil می‌باشد که در ادامه توصیف شده‌اند.

تغییر ناپذیری: با ذخیره‌سازی داده‌ها در یک شبکه BigchainDB، تغییر یا حذف آن‌ها تقریبا غیرممکن بوده و یا درصورت امکان بسیار دشوار است. این پایگاه‌داده، برای دستیابی به تغییرناپذیری از چندین استراتژی متفاوت استفاده می‌کند. ساده‌ترین استراتژی این است که BigchainDB برای تغییر یا حذف داده‌های ذخیره‌شده، هیچ نوع API ارائه نمی‌دهد. استراتژی دیگر این است که هر گره دارای یک کپی کامل از تمام داده‌ها در یک پایگاه داده مستقل MongoDB است. درمواردی که یک گره خراب یا نابود شود، داده‌های گره‌های



شکل (3) : معماری گره‌های BigchainDB [۴۴]

دیگر تحت‌تأثیر قرار نمی‌گیرند و همچنان یک کپی از همه داده‌ها در اختیار خواهد بود. علاوه‌براین، تمام تراکنش‌ها در BigchainDB بصورت رمزنگاری شده، امضا شده‌اند و پس از ذخیره یک تراکنش، تغییر محتویات آن تراکنش، سبب تغییر امضا می‌شود، که قابل تشخیص است (مگر اینکه کلید عمومی نیز تغییر کند، اما این مورد نیز قابل تشخیص است، زیرا هر بلاک توسط یک گره امضا می‌شود و کلیدهای عمومی همه گره‌ها شناخته شده‌اند).

غیرمتمرکز بودن: درBigchainDB، هیچ شخص خاصی همه چیز را در اختیار یا کنترل ندارد. در حالت ایده‌آل، هر گره توسط شخص یا سازمان متفاوتی کنترل می‌شود.

دارایی‌های تحت کنترل مالک: فقط مالک (یا مالکان) یک دارایی در BigchainDB قادر به انتقال آن دارایی هستند. (مالکان، دارندگان یک مجموعه خاص از کلیدهای خصوصی هستند).

نرخ بالای تراکنش: یکی از اهداف طراحی BigchainDB توانایی پردازش تعداد زیادی تراکنش در هر ثانیه است.

تاخیر کم: در پایگاه‌داده BigchainDB، زمانی در حد چند ثانیه (یا کمتر) برای قراردادن یک تراکنش در یک بلاک به اتمام‌رسیده جدید مورد نیاز است.

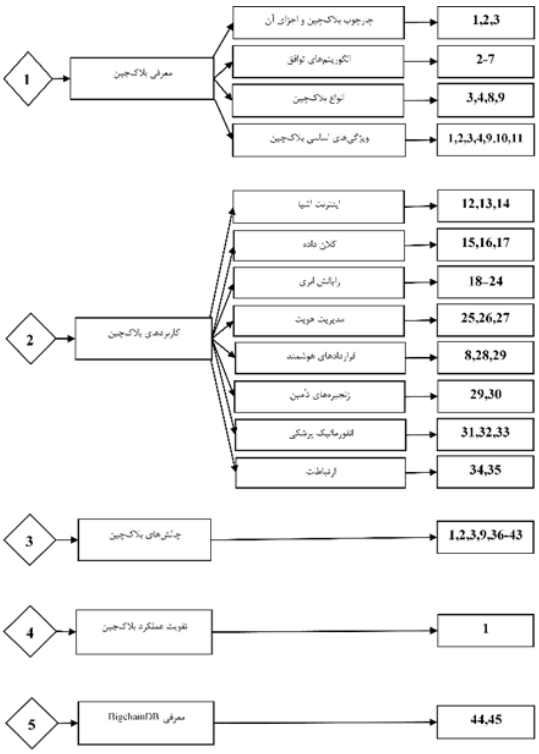
نمایه‌سازی و پرس‌وجوی داده‌های ساختاریافته: هر گره در یک شبکه BigchainDB پایگاه‌داده MongoDB محلی خاص خود را دارد. به این صورت که هر اپراتور گره برای نمایه‌سازی و پرس‌وجوی داده‌های ذخیره‌شده (تراکنش‌ها، دارایی‌ها، بلاک‌ها و متادیتا که همه رشته‌های JSON هستند) به قدرت کامل MongoDB دسترسی دارد. هر اپراتور گره این قابلیت تصمیم‌گیری را دارد که چه میزان از این قدرت را در معرض استفاده کاربران خارجی قرار دهد. علاوه‌براین، هر اپراتور گره می‌تواند شاخص‌های اضافی و APIهای پرس‌وجو را اضافه کند.

تحمل خطای بیزانس: BigchainDB، از یک نوع توافق بیزانس تحت‌عنوان Tendermint، برای همه شبکه‌ها و توافق‌ها استفاده می‌کند. همانطور که قبلا نیز اشاره شده، در BigchainDB هر گره دارای پایگاه‌داده MongoDB محلی خاص خودش است و کلیه ارتباطات بین گره‌ها با استفاده از پروتکل‌های Tendermint انجام می‌شود. بنابراین سیستم BigchainDB، دارای ویژگی تحمل خطای بیزانس است. در نتیجه اگر یک هکر مخرب، مدیریت یکی از پایگاه‌داده‌های MongoDB محلی را در اختیار گیرد، درنهایت موفق به تغییر یا

حذف داده‌ها در آن پایگاه‌داده محلی می‌شود و پایگاه‌داده‌های MongoDB در گره‌های دیگر تحت‌تأثیر قرار نمی‌گیرند.

تحمل خطای Sybil: برخی از شبکه‌های بلاک‌چین (مانند Bitcoin)، امکان اضافه کردن گره به شبکه را برای هر شخصی فراهم می‌کنند. این مسئله ممکن است سبب حمله اکثریت (حمله Sybil) شود، به‌این‌صورت که شخصی با اضافه‌کردن گره‌های بسیار، کنترل شبکه را دراختیار بگیرد. در BigchainDB، با وجود سازمانی که لیست اعضا مؤثر در شبکه را کنترل می‌کند، حملات Sybil مسئله‌ای نیست. در نهایت می‌توان گفت که، از آنجایی که نرم‌افزار BigchainDB، دارای خواص متعدد پایگاه‌داده و همچنین بلاک‌چین است، در طیف گسترده ای از زمینه‌ها، از جمله زنجیره تأمین، مدیریت حقوق IP، جفت های دیجیتالی و IoT، هویت، حاکمیت داده‌ها و مسیرهای حسابرسی تغییرناپذیر، کاربرد دارد [۴۴.۴۵].

در انتها قابل ذکر است که یک دسته‌بندی موضوعی از بلاک‌چین به صورتی که در شکل (۴) نمایش داده شده است، می‌باشد. در این شکل همچنین منابع مرتبط با موضوعات نیز ذکر گردیده است.



شکل(۴): دسته‌بندی موضوعی از بلاک‌چین و منابع مرتبط

۶-نتیجه

توسعه فن‌آوری بلاک‌چین، توجه بسیاری را به کاربرد این فن‌آوری در زمینه‌های مختلف سوق داده است. به‌عنوان‌مثال، در زمینه اینترنت اشیا، کاربرد گسترده دستگاه‌های IoT برای جمع‌آوری و انتقال داده‌ها، نگرانی‌های امنیتی و حفظ حریم خصوصی قابل‌توجهی را ایجاد می‌کند. کاربرد بلاک‌چین در این زمینه، امنیت بیشتری را در مقایسه با سیستم‌های مدیریت داده سنتی فراهم می‌نماید. از طرف دیگر، باتوجه به حجم بالای داده‌های جمع‌آوری شده، کلان‌داده کاربرد قابل توجهی را به عنوان چارچوبی برای تجزیه‌وتحلیل این حجم بالا از داده‌ها به‌دست آورده‌است. در این زمینه، بلاک‌چین، با داشتن ویژگی‌هایی از جمله عدم دستکاری، قابلیت ردیابی و همچنین فرآیند پردازش غیرمتمرکز، قابلیت بالایی را برای پیشرفت فن‌آوری کلان‌داده ارائه می‌دهد. بنابراین، می‌توان از فن‌آوری بلاک‌چین جهت توانمندسازی زمینه‌های مختلف کلان‌داده استفاده کرد. علاوه‌براین، با توجه به نیازهای زیرساخت‌های ابری کنونی نظیر مقیاس‌پذیری، امنیت، انعطاف‌پذیری و تأخیر کم، یک معماری مبتنی بر بلاک‌چین می‌تواند دسترسی اقتصادی، ایمن و براساس تقاضا را در این زیرساخت‌ها فراهم نماید. علاوه‌براین، بلاک‌چین در مواردی نظیر مدیریت هویت، قراردادهای هوشمند، زنجیره‌های تأمین، انفورماتیک پزشکی و ارتباطات کاربرد دارد. ولی همانطور که قبلاً نیز اشاره شد، پیاده‌سازی یک سیستم بلاک‌چین با چالش‌های متعدد امنیتی و عملکردی روبروست. این چالش‌ها و تهدیدات مسائل مهمی هستند و باید در طراحی برنامه‌های بلاک‌چین در نظر گرفته شوند.

ازطرف دیگر، باتوجه به کاربرد روزافزون این فن‌آوری در زمینه‌های مختلف، تقویت عملکرد آن موضوع مهمی است. در این زمینه، سیستم‌های بلاک‌چین ساخته‌شده برروی پایگاه‌داده‌های سنتی، موضوع مهمی است که می‌توان بیشتر به آن پرداخت.

مراجع

[1] Silberschatz, A., Korth, H. F., Sudarshan, S. *Database System Concepts*, McGraw-Hill Education, 2020.

[2] Gao, W., Hatcher, W. G., Yu, W., *"A Survey of Blockchain: Techniques, Applications, and Challenges"*, 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–11, 2018.

[3] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., *"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends"*, IEEE 6th International. Congress on Big Data, pp. 557–564, 2017.

[4] Salek Ali, M., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M. H., *'"Applications of Blockchains in the Internet of Things: A Comprehensive Survey"* IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 21, pp. 1676-1717, 2019.

[5] Sharma, K., Jain, D., *"Consensus Algorithms in Blockchain Technology: A Survey"*, 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019.

[6] ALI SYED, T., ALZAHRANI, A., JAN, S., SIDDIQUI, M. Sh., NADEEM, A., ALGHAMDI, T., *"A Comparative Analysis of Blockchain Architecture and Its Applications: Problems and Recommendations"*, IEEE Access, vol. 7, pp. 176838-176869, 2019.

[7] ROUHANI, S., DETERS, R., *"Security, Performance, and Applications of Smart Contracts: A Systematic Survey"*, IEEE Access, vol. 7, pp. 50759-50779, 2019.

[8] Minhaj Ahmad Khan and Khaled Salah, *"IoT security Review, blockchain solutions, and open challenges"*, Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.

[9] Feng, Qi., He, D., Zeadally, Sh., Khurram Khan, M., Kumar, N., *"A survey on privacy protection in blockchain system"*, Journal of Network and Computer Applications, vol. 126, pp. 45-58, 2019.

[10] Monrat, A. A., Schelen, O., Andersson, K., *"A Survey of Blockchain from the Perspectives of Applications Challenges and Opportunities"*, IEEE Access, vol. 7, pp. 117134-117151, 2019.

[11] Dai, H. N., Zheng, Z., Zhang, Y., *" Blockchain for Internet of Things: A Survey"*, IEEE Internet of Things Journal, vol. 6, pp. 8076-8094, 2019.

[12] Dorri, A., Kanhere, S. S., Jurdak, R., Gauravaram, P., *"Blockchain for IoT security and privacy: The case study of a smart home"*, IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623, 2017.

[13] Polyzos, G. C., Fotiou, N., *"Blockchain-Assisted Information Distribution for the Internet of Things"*, IEEE International Conference on Information Reuse and Integration (IRI), pp. 75–78, 2017.

[14] Jung, M. Y., Jang, J. W., *"Data management and searching system and method to provide increased security for IoT platform"*, International Conference on Information and Communication Technology Convergence (ICTC), pp. 873–878, 2017.

[15] Chen, J., Lv, Z., Song, H., *"Design of personnel big data management system based on blockchain"*, Future Generation Computer Systems, vol. 101, pp. 1122–1129, 2019.

[16] Karafiloski, E., Mishev, A., *"Blockchain solutions for big data challenges: A literature review"*, in IEEE EUROCON 2017 -17th International Conference on Smart Technologies, pp. 763–768, 2017.

[17] Kiyomoto, S., Rahman, M. S., Basu, A., *"On blockchain-based anonymized dataset distribution platform"*, IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), pp. 85–92, 2017.

[18] Wang, S., Wang, X., Zhang, Y., *"A Secure Cloud Storage Framework with Access Control Based on Blockchain"*, IEEE Access, vol. 7, pp. 112713–112725, 2019.

[19] Yang, Y., Lin , H., Liu , X., Guo, W., Zheng , X., Liu, Z., *"Blockchain-Based Verifiable Multi-Keyword Ranked Search on Encrypted Cloud With Fair Payment"*, IEEE Access, vol. 7, pp. 140818–140832, 2019.

[20] Zhang, Y., Deng, R. H., Shu, J., Yang, K., Zheng, D., *"TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain"*, IEEE Access, vol. 6, pp. 31077–31087, 2018.

[21] Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L., *"ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability"*, in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468–477, 2017.

[22] Sharma, P. K. Chen, M.-Y. Y., Park, J. H., *"A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT"*, IEEE Access, vol. 6, pp. 115–124, 2018.

[23] Xu, C., Wang, K., Guo, M., *"Intelligent Resource Management in Blockchain-Based Cloud Datacenters"*, IEEE Cloud Computing, vol. 4, pp. 50–59, 2017.

[24] Do, H. G., Ng, W. K., *"Blockchain-Based System for Secure Data Storage with Private Keyword Search"*, IEEE World Congress on Services (SERVICES), pp. 90–93, 2017.

[25] Yasin, A., Liu, L., *"An Online Identity and Smart Contract Management System"*, in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), pp. 192–198, 2016.

[26] Yan, Z., Gan, G., Riad, K., *"BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains*

[40] Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., *"A survey on the security of blockchain systems"*, Future Generation Computer Systems, vol. 107, pp. 841-853, 2020.

[41] Biryukov, A., Khovratovich, D., Pustogarov, I., *"Deanonymisation of Clients in Bitcoin P2P Network"*, in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14, pp. 15–29, 2014.

[42] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., Skarmeta, A., *"Privacy-preserving solutions for Blockchain: review and challenges"*, IEEE Access, vol. 7, pp. 164908-164940, 2019.

[43] Wang, D., Zhao, J., Wang, Y., "A Survey on Privacy Protection of Blockchain: the Technology and Application", IEEE Access, 2020.

[44] BigchainDB, *"BigchainDB"*, pp. 1–14, 2018.

[45] Mcconaghy, T., Marques, R., M¨uller, A., Jonghe, D. D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., Granzotto, A., *"BigchainDB: A Scalable Blockchain Database (DRAFT)"*, pp. 1–65, 2016.

for OpenPDS", in 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 138–144, 2017.

[27] Zhu, X., Badr, Y., Pacheco, J., Hariri, S., *"Autonomic Identity Framework for the Internet of Things"*, in 2017 International Conference on Cloud and Autonomic Computing (ICCAC), pp. 69–79, 2017.

[28] Christidis, K., Devetsikiotis, M., *"Blockchains and Smart Contracts for the Internet of Things"*, IEEE Access, vol. 4, pp. 2292–2303, 2016.

[29] Feng Tian, *"A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things"*, in 2017 International Conference on Service Systems and Service Management, pp. 1–6, 2017.

[30] Lu, Q., Xu, X., *"Adaptable Blockchain-Based Systems: A Case Study for Product Traceability"*, IEEE Softw., vol. 34, pp. 21–27, 2017.

[31] Magyar, G., *"Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management"*, in 2017 IEEE 30th Neumann Colloquium (NC), vol. 2018-Janua, pp. 000135–000140, 2017.

[32] Shae, Z., Tsai, J. J. P., *"On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine"*, in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 1972–1980, 2017.

[33] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., *"MedRec: Using Blockchain for Medical Data Access and Permission Management"*, in 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, 2016.

[34] Cha, S.-C., Chen, J.-F., Su, C., Yeh, K.-H., *"A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things"*, IEEE Access, vol. 6, pp. 24639–24649, 2018.

[35] Yin, H., Guo, D., Wang, K., Jiang, Z., Lyu, Y., Xing, J., *"Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm"*, IEEE Netw., vol. 32, pp. 112–117, 2018.

[36] Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., Liu, Y., *"A survey on the scalability of blockchain systems"*, IEEE Network, vol. 33.5, pp. 166-173, 2019.

[37] Zhou, Q., Huang, H., Zheng, Z., Bian, J., *"Solutions to scalability of blockchain: A survey"*, IEEE Access, vol. 8, pp. 16440-16455, 2020.

[38] Hafid, A., Hafid, A. S., Samih, M., *"Scaling Blockchains: A Comprehensive Survey"*, IEEE Access, vol. 8, pp. 125244-125262, 2020.

[39] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., Wang, J., *"Untangling Blockchain: A Data Processing View of Blockchain Systems"*, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, vol. 30, pp. 1366–1385, 2018.