فناوری بلاکچین در سیستم‌های مراقبت بهداشتی: الگوریتم‌های اجماع به‌همراه فصل‌مشترک آن‌ها با حوزه داده‌کاوی، چالش‌های امنیتی و رویکردهای آتی

یاسمن علی‌اکبرپور [*۱]، سمیرا اسدزاده [۲]

۱- گروه مهندسی کامپیوتر، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران

y.aliakbarpoor@iaushiraz.ac.ir

۲- گروه مهندسی کامپیوتر، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران

s.asadzadeh@iaushiraz.ac.ir

چکیده

فناوری بلاکچین در سالیان اخیر، به عنوان ابزاری موثر در فراهم آوردن مزایایی از قبیل یکپارچگی و غیرمتمرکزسازی داده‌ها، سبب جذب پژوهشگران به این حوزه شده‌است. اگرچه امنیت، حفظ حریم خصوصی و مقیاس‌پذیری همچنان به‌عنوان چالش‌های این فناوری محسوب می‌گردد، اما ویژگی کلیدی بلاکچین در غیرمتمرکزسازی داده‌ها باعث ایجاد بستری برای پیاده‌سازی انوع پلتفرم‌ها به‌ویژه سیستم‌های مراقبت بهداشتی شده است. این مقاله یک مرور کلی بر پژوهش‌های اخیر بر روی کاربرد فناوری بلاکچین در سیستم‌های مراقبت بهداشتی است. در این مطالعه یک طرح جامع از معماری و طبقه‌بندی بلاکچین، الگوریتم‌های اجماع قابل استفاده در برنامه‌های بهداشتی و همچنین موارد استفاده از این فناوری مورد بررسی قرار داده است. بعلاوه، چالش‌های امنیتی و فرصت‌های تحقیقاتی آتی در بکارگیری این فناوری در حوزه مراقبت‌های بهداشتی ارائه شده‌اند تا نقشه راهی برای تحقیقات آتی، به‌ویژه در سیستم های مراقبت بهداشتی ایران باشد. در عین حال، تکنیک‌های داده‌کاوی برای استخراج بینش از مجموعه داده‌های بزرگ اهمیت فزاینده‌ای پیدا کرده‌اند. در این مقاله، ما تقاطع الگوریتم‌های اجماع بلاکچین و داده‌کاوی را بررسی می‌کنیم و چارچوبی را برای استفاده از الگوریتم‌های اجماع در برنامه‌های داده‌کاوی پیشنهاد می‌کنیم. در دنیای امروز، حفظ امنیت و حریم خصوصی نه بطور کامل بلکه به قدر کافی از دیدگاه متخصصان امر، قابل پیاده‌سازی است. از این‌رو مطالعه حاضر در پایان با بررسی حملات امنیتی شناخته و انجام شده در بلاکچین، روش‌هایی را با هدف افزایش امنیت و بهبود حریم خصوصی کاربران مورد ملاحظه قرار داده است.

کلمات کلیدی: بلاکچین، الگوریتم‌های اجماع، سیستم‌های مراقبت بهداشتی، امنیت، بلاکچین در سیستم‌های مراقبت بهداشتی، تقاطع داده‌کاوی و بلاکچین

* **Corresponding author: گروه مهندسی کامپیوتر، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران**
Email: y.aliakbarpoor@iaushiraz.ac.ir

۱. مقدمه

اخیراً فناوری‌های بلاکچین توانسته‌اند در بسیاری از بخش‌ها، محبوبیت قابل توجهی را به دست آورند [۱]. پتانسیل فزاینده فناوری بلاکچین باعث شده تا این فناوری نه تنها در برنامه‌های کاربردی حوزه مراقبت های بهداشتی، بلکه در بسیاری دیگر از حوزه‌ها مورد استقبال و استفاده قرار گیرد [۲]. سیستم‌های مبتنی بر بلاکچین به عنوان پلتفرم‌های امن در نظر گرفته می‌شوند [۳] که در آن تمام فعالیت‌های گره‌ها ثبت شده و افزایش بی وقفه زنجیره سبب می‌گردد تا هرگونه تغییر در بلوک از نظر محاسباتی چالش برانگیز باشد [۴].

بلاکچین ما را قادر می‌سازد تا کنترل دسترسی را به عنوان یک قرارداد هوشمند بین صاحب داده و کاربران پیاده‌سازی کنیم. هر صاحب داده قرارداد هوشمند خود را ایجاد می‌کند که در آن کاربر داده می‌تواند با ثبت تراکنش، درخواست دسترسی به یک فایل خاص را داشته باشد. در پاسخ، صاحب داده، اعتبار مورد نیاز را برای کاربر ارسال می‌کند و از این طریق او را قادر می‌سازد تا فایل مورد نظر را در فضای ذخیره‌سازی ابری، رمزگشایی کند. ساختار توزیع شده بلاکچین نقش مهمی در کاهش حملات DoS دارد [۵].

به طور واضح، افزایش سن جمعیت و افزایش نرخ ابتلای افراد به بیماری‌های مزمن، نیازمند دانش بیشتری از مسائل بهداشتی و همچنین ارائه مراقبت‌های بهتر است [۶]. اینترنت اشیا پزشکی (IoMT[1]) یکی از گامهای فناورانه موثر در زمینه خدمات بهداشتی می‌باشد که به تازگی معرفی شده است. با این حال، این فناوری با چالش‌هایی از قبیل محاسبات و ذخیره‌سازی متمرکز روبه‌رو است که منجر به مشکلاتی مانند دستکاری داده‌ها و بی‌اعتمادی و در نهایت شکست می‌گردد. چالش مهم دیگر در مراقبت‌های بهداشتی الکترونیکی و فراگیر، حفاظت از امنیت تمام تجهیزات اینترنتی است [۷]. ادغام بلاکچین با مراقبت‌های بهداشتی باعث غیرمتمرکزسازی محاسبات، ذخیره سازی و در نتیجه بهبود امنیت می‌شود. پتانسیل امیدوارکننده فناوری بلاکچین به بهبود پشتیبانی مراقبت‌های بهداشتی برای پرسنل پزشکی و سایر ذینفعان از نظر پرونده-های تأیید و احراز شده [۸] ، قابلیت همکاری [۹]، ذخیره کارامد پرونده‌های سلامت [۱۰] و سیستم‌های امنیتی [۱۱] کمک کرده است.

داده‌کاوی شامل کشف الگوها، همبستگی‌ها و سایر اطلاعات مفید از مجموعه داده‌های متنوع است. با این حال، رویکردهای سنتی برای داده کاوی اغلب شامل سیستم‌های متمرکزی است که در برابر هک و نقض داده‌ها آسیب‌پذیر هستند. فناوری بلاکچین با ارائه یک پلتفرم غیرمتمرکز و امن برای ذخیره و به اشتراک گذاری داده ها، راه حلی به نسبت ایمن‌تر ارائه می‌دهد. در قلب فناوری بلاکچین، الگوریتم اجماع وجود دارد که تضمین می‌کند همه گره‌های شبکه در مورد وضعیت دفتر کل توافق دارند. در این مقاله، چگونگی استفاده از الگوریتم‌های اجماع بلاکچین را در برنامه‌های داده‌کاوی بررسی می‌کنیم. تاکنون پژوهش‌های متعددی در زمینه بکارگیری فناوری بلاکچین در حوزه‌های مختلف انجام شده است. با این حال، همچنان نیاز به بررسی و پژوهش بیشتر در خصوص سیستم‌های مراقبت بهداشتی مبتنی بر بلاکچین و مسائل مختلف امنیتی و حریم خصوصی محسوس می‌باشد.

بخشهای آتی این مقاله به شرح زیر سازماندهی شده است: بخش ۲، بلاکچین و ویژگی‌های آن را در راستای برنامه‌های مراقبت بهداشتی معرفی می‌کند. در بخش۳، مدل کارکرد بلاکچین و لایه‌های معماری بلاکچین شرح داده شده است. در بخش۴ موارد استفاده از بلاکچین در سیستم های مراقبت بهداشتی را شرح داده است. بخش۵ طبقه‌بندی بلاکچین را مورد بحث قرار می‌دهد. در بخش۶، الگوریتم‌های اجماع مختلف و همچنین نکات کلیدی در خصوص بکارگیری فناوری بلاکچین در داده‌کاوی معرفی شده است. در ادامه، مبحث داده‌کاوی با تمرکز بر بستر بلاکچین در بخش ۷ مقاله حاضر مورد بررسی قرارگرفته‌است. در بخش۸ چالش‌ها و فرصت‌های پژوهشی این حوزه شناسایی شده است. در پایان با بخش ۹ با عنوان نتیجه، مقاله را به پایان رسانده‌ایم.

۲. بررسی اجمالی بلاکچین

بلاکچین یک پلتفرم فناوری توزیع شده نظیر به نظیر[۲] است که در سال ۲۰۰۸ برای صنعت مالی با ایجاد بیت کوین معرفی شد [۱۲] ، اما اکنون تا حدی پیشرفت کرده است که به عنوان یک فناوری پایه برای انواع مختلف اپلیکیشن‌های غیرمتمرکز در نظر گرفته شده است. بلاکچین از چندین بلوک متصل بهم بوسیله توابع رمزنگاری تشکیل شده است. برای شروع یک فرایند، یک بلوک توسط یکی از مشارکت کنندگان در یک تراکنش به وجود می آید. هزاران کامپیوتر از طریق اینترنت، این بلاک جدید را تایید می‌کنند. بلاک تایید شده به زنجیره اضافه می شود. در بلاکچین، تراکنش‌ها زمانی معتبر تلقی می‌شوند که اجماع بلوک‌ها از طریق قراردادها توافق کنند. ماهیت غیرمتمرکز فناوری بلاکچین، اعتماد را غیرمتمرکز می‌کند. بنابراین اعتماد در میان کاربران سیستم برای اشتراک‌گذاری کلیدها ضروری است. در حقیقت بلاکچین یک فناوری توزیع شده است که امکان تراکنش بین دو طرف را بدون نیاز به واسطه فراهم می‌کند. ماهیت غیرمتمرکز بلاکچین آن را بسیار ایمن و شفاف می‌کند و در عین حال خطر تقلب یا دستکاری را از بین می‌برد.

بیت کوین اولین پیاده سازی موفق فناوری بلاکچین است. بیت کوین یک ارز دیجیتال غیرمتمرکز است که در شبکه P2P عمل می‌کند. تراکنش‌های شبکه بیت‌کوین توسط گره‌های شبکه تأیید می‌شوند و اطلاعات در یک دفتر کل عمومی ذخیره می‌شوند. بیت‌کوین از مکانیزم اجماع اثبات کار[۳](PoW) برای اعتبارسنجی تراکنش‌ها استفاده می‌کند. ماینرها، الگوریتم‌های پیچیده ریاضی را حل می‌کنند تا بلاک‌های جدیدی به بلاکچین اضافه کنند. اتریوم، دومین نسخه بلاکچین است و یک پلتفرم متن باز است که توسعه‌دهندگان را قادر می‌سازد تا برنامه‌های غیرمتمرکز را با استفاده از قراردادهای هوشمند بسازند. قراردادهای هوشمند قراردادهایی هستند که خوداجرایی می‌شوند و شرایط توافق‌نامه در کد نوشته شده است. اتریوم از مکانیزم توافقی به نام اثبات‌سهام[4](PoS) استفاده می‌کند که در آن اعتبارسنج‌ها توکن‌های خود را برای شرکت در اعتبارسنجی بلوک قرار می‌دهند. مکانیسم PoS مصرف انرژی را کاهش می‌دهد و مقیاس پذیری را در مقایسه با مکانیسم PoW بهبود می‌بخشد [۱۳].

۲-۱. بلاکچین در مراقبت‌های بهداشتی

در سال‌های اخیر، علاقه فزاینده‌ای به استفاده از بلاکچین در مراقبت‌های بهداشتی برای مقابله با چالش‌های مختلف در این صنعت، مانند قابلیت همکاری، حریم خصوصی داده‌ها و امنیت وجود داشته است. این بخش مروری کلی از پیشرفت‌های اخیر استفاده از بلاکچین در مراقبت‌های بهداشتی با تمرکز بر تحقیقات منتشر شده بین سال‌های ۲۰۲۱ و ۲۰۲۳ ارائه می‌کند.

صنعت مراقبت‌های بهداشتی حجم وسیعی از داده‌ها را از منابع مختلف، از جمله پرونده‌های الکترونیک سلامت [۵]، آزمایش‌های بالینی، دستگاه‌های پزشکی و پوشیدنی‌ها تولید می‌کند. با این حال، این داده‌ها اغلب به صورت ایزوله، تکه تکه و چالش برانگیز برای دسترسی و به اشتراک‌گذاری در میان سیستم‌ها و ذینفعان مختلف هستند. علاوه بر این، مدل‌های اشتراک‌گذاری فعلی داده، نگرانی‌هایی را در مورد حفظ حریم خصوصی، امنیت و رضایت بیمار ایجاد می‌کند. بلاکچین با ارائه یک زیرساخت غیرمتمرکز، شفاف و ضد دستکاری برای تبادل داده و همکاری، راه حل امیدوارکننده‌ای را برای این مسائل ارائه می‌دهد. فناوری بلاکچین پتانسیل قابل توجهی در متحول ساختن مراقبت های بهداشتی با فعال کردن تبادل اطلاعات ایمن و شفاف، بهبود حریم خصوصی و کنترل بیمار، و بهبود مدیریت زنجیره تامین، آزمایشات بالینی و ردیابی دستگاه های پزشکی دارد. بررسی‌ها نشان می‌دهند که اخیرا پیشرفت‌هایی در برنامه‌های مراقبت بهداشتی مبتنی بر بلاکچین رخ داده است [۱۴ - ۱۸]:

- **قابلیت همکاری**: بلاکچین می‌تواند با ایجاد یک دفتر مشترک از اطلاعات بیمار که برای اشخاص مجاز در دسترس است، قابلیت همکاری بین سیستم های EHR مختلف را تسهیل کند.
- **حریم خصوصی داده‌ها**: بلاکچین می‌تواند بیماران را قادر سازد تا داده‌های سلامت خود را در یک شبکه غیرمتمرکز ذخیره و صدور رضایت برای استفاده از آن را مدیریت کنند. این رویکرد با ارائه مالکیت و شفافیت اطلاعات بیماران به موضوع نقض داده‌ها و دسترسی غیرمجاز می‌پردازد.
- **مدیریت زنجیره تامین**: بلاکچین می‌تواند شفافیت و قابلیت ردیابی زنجیره‌های تامین دارویی را افزایش دهد و ذینفعان را قادر می‌سازد تا منشأ دارو را ردیابی کنند و از خرید و استفاده از محصولات تقلبی جلوگیری کنند.
- **آزمایشات بالینی**: بلاکچین می‌تواند کارایی و شفافیت آزمایشات بالینی را با ایجاد یک رکورد امن و قابل بازرسی از داده‌های بالینی بهبود بخشد. این رویکرد همچنین می‌تواند جذب بیمار و مدیریت رضایت را تسهیل بخشد.

ردیابی دستگاه های پزشکی: بلاکچین می‌تواند ردیابی و نظارت بر دستگاه‌های پزشکی را در طول چرخه عمر آنها میسر سازد و ایمنی و انطباق با مقررات را افزایش دهد.

۲-۲. مطالبات کاربران از فناوری بلاکچین

نگرانی‌های مربوط به حریم خصوصی، مشکلات فنی و فقدان سیستمی برای دستیابی به توافق در مورد نحوه استفاده یا اشتراک‌گذاری داده‌ها، باعث شده تا موسسات پزشکی تمایلی به همکاری با یکدیگر نداشته باشند. داده‌های بهداشتی همیشه در زمان واقعی در دسترس بیماران و موسسات پزشکی نیست. متداول‌ترین و برجسته‌ترین نیازهای کاربران سیستم‌های مراقبت بهداشتی مبتنی بر بلاکچین که گفته شده می‌توانند مشکلات بالقوه را حل کنند، شامل مواردی از قبیل وجود پرونده‌های سلامت شخصی [۶]، محرمانگی اطلاعات، قابلیت اطمینان، کارایی، قابلیت همکاری و کنترل دسترسی است. پرونده‌های سلامت شخصی، بیماران را قادر می سازند تا مراقبت‌های خود را با ارائه دسترسی دقیق، فردی و ایمن به داده های پزشکی خود مدیریت نمایند [۱۹]. هدف این سیستم فراهم آوردن بستری برای بیماران است تا از داده‌هایشان برای حمایت و پیشبرد اهداف مراقبت‌های پزشکی خود استفاده کنند . البته این پلتفرم می‌بایست دارای مکانیسم‌های رضایت قوی برای به اشتراک‌گذاری داده ها بین مؤسسات و برنامه‌های مختلف باشد.

بسیاری از فرآیندها توسط سیستم‌های مراقبت بهداشتی مبتنی بر بلاکچین، ساده و یکپارچه می‌شوند و سرعت، چابکی و کارایی سیستم تا حد زیادی افزایش می‌یابد. همچنین به دلیل قابلیت درون عملیاتی و انعطاف پذیری آن، عملکرد یک مرکز مراقبت بهداشتی و ظرفیت درمان بیماران بهبود می‌یابد. سیستم‌های مراقبت بهداشتی مبتنی بر بلاکچین در برابر هرگونه اختلال تکنولوژیکی یا خرابی‌هایی که توسط سایر سیستم های تکنولوژیکی ایجاد می‌شود، تا حدود زیادی مقاوم هستند. این سیستم‌ها از منظر امنیت داده‌ها، نه به طورکامل، ولی بطور قابل توجهی امن هستند. بعلاوه دارای رابط کاربری بصری مناسبی هستند که در نهایت موجب افزایش رضایت تجربه کاربران در حین کار با سیستم‌ها می‌شوند. پرونده‌های پزشکی، از راه دور به روز شده و بدون ایجاد اختلال در فعالیت‌های روزمره بهبود می‌یابند. در دسترس بودن سیستم و منابع در هر زمان، عاملی برای موفقیت این سیستم‌ها بشمار می‌رود. به طور خلاصه، بلاکچین چارچوبی در سطح بالا ارائه می دهد که چگونه یک بیمار می‌تواند به طور ایمن با چندین ذینفع ارتباط برقرار کند، خود را در هر مؤسسه شناسایی کند و داده های سلامت خود را به شیوه ای بادوام جمع کند یک پزشک باید قبل از دسترسی به سوابق پزشکی بیمار، از بیمار رضایت بگیرد در غیر این صورت، سیستم دسترسی وی را ممنوع خواهد کرد. همچنین بیمار بتواند به طور مستقل به سایرین دسترسی موقت داده و هر گونه امتیاز دسترسی را برای سایر کاربران سیستم حذف کند.

۳. مدل کارکرد بلاکچین

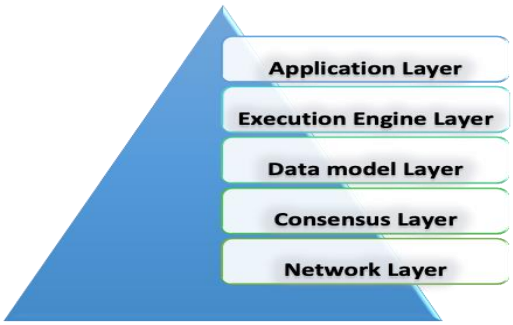
سیستم‌های مبتنی بر بلاکچین توانایی کاهش یا حذف هزینه‌ها و اصطکاک مرتبط با واسطه‌های فعلی را دارند. برای کسانی که در صنعت مراقبت‌های بهداشتی هستند، ظهور بلاکچین پیامدهای گسترده‌ای داشته است. استفاده از این فناوری امکان ادغام سیستم‌های منفصل و بهبود ارزیابی مراقبت را فراهم می‌کند. یک شبکه بلاکچین برای اطلاعات الکترونیکی پزشکی در سراسر کشور، می‌تواند در نهایت موجب افزایش بهره‌وری شده و در نتیجه سلامت بیمار را بهبود بخشد که هدف غائی در سیستم‌های مراقبت بهداشتی است. در این بخش، مدل عملکردی اصلی یک بلاکچین مورد بحث قرار می گیرد.
بلاکچین از بلوک‌های اطلاعات دیجیتالی تشکیل شده است. بلوک‌ها برای تشکیل یک زنجیره، به یکدیگر متصل می‌شوند. هر بلوک از سه قسمت تشکیل شده است: «اطلاعات مربوط به تراکنش‌ها»، «افراد درگیر در تراکنش‌ها» و «کدهای رمزنگاری». نحوه عملکرد بلاکچین را می‌توان در چهار گام زیر خلاصه کرد:

۱) تراکنش (رد و بدل اطلاعات) انجام می شود.
۲) تراکنش تأیید و سپس اعتبارسنجی می شود.
۳) تراکنش در بلوک ذخیره می شود.
۴) بلوک هش (کدگذاری) شده و به بلاکچین اضافه می شود.

بلاکچین در محیطی کار می‌کند که در آن طرفین تجاری با یک رکورد امن و همزمان از تراکنش‌ها در شبکه مشخص می‌شوند. دفتر کل بلاکچین هر جریان تراکنش را از ابتدا تا انتها ثبت می‌کند..

۳-۱. معماری پنج لایه بلاکچین

این بخش، به جزئیات معماری لایه‌ای بلاکچین می‌پردازد. این لایه‌ها عبارتند از: لایه کاربردی (Application)، لایه موتور اجرا (Execution Engine)، لایه مدل داده (Data Model)، لایه توافق یا اجماع (Consensus) و لایه شبکه (Network). شکل (۱) ساختار هرمی لایه‌های بلاکچین را نمایش می‌دهد.



شکل ۱- معماری پنج لایه بلاکچین [۳۲]

لایه کاربردی، بالاترین لایه در معماری بلاکچین است. این لایه یک رابط کاربری گرافیکی برای تعامل کاربران با سیستم را فراهم می‌کند. لایه موتور اجرا، لایه‌ای است که از قراردادهای هوشمند، قوانین اساسی و کد زنجیره‌ای تشکیل شده است. یک تراکنش از لایه کاربردی به لایه اجرا انتقال می‌یابد. چالش‌های لایه موتور اجرا مربوط به تهدیدات و خطرات قراردادهای هوشمند است. قبل از انتشار باید یک مجموعه کامل از بررسی‌ها و تست‌های امنیتی انجام گیرد. همچنین، متخصصان بایستی بهینه سازی و کنترل‌های مکرر کد را انجام دهند و رفتار غیرعادی قراردادهای اجرا شده را نظارت کنند. لایه مدل داده، سادگی را برای ارزهای دیجیتال تضمین می‌کند. مدل داده هر برنامه مجزا متفاوت است. داده‌ها شامل داده‌های تراکنش، داده‌های اصلی و داده‌های مرجع است. ساختارهای داده بلاکچین دارای دو جزء اصلی اشاره‌گر و لیست پیوندی هستند.

بلوک‌های زنجیره‌ای، لیست‌های مرتبطی هستند که هر بلوک به بلوک قبلی اشاره می‌کند. امنیت بلاکچین به قدرت هش مشارکت‌کنندگان بستگی دارد. لایه اجماع یکی از مهمترین لایه‌ها در بلاکچین است. الگوریتم اجماع، الگوریتم نتیجه‌گیری نیز نامیده می‌شود. بدون الگوریتم اجماع، بلاکچین وجود ندارد. اعتبارسنجی بلوک‌ها توسط یک الگوریتم اجماع انجام می‌شود. مسئولیت لایه اجماع این است که همه کاربران را بر روی یک قانون تراکنش مشترک به توافق برسانند. در بخش ۶، به معرفی برخی از الگوریتم‌های اجماع پرداخته‌ایم. لایه شبکه یا P2P یا انتشار، لایه‌ای است که مسئول ارتباطات بین گره‌ای است. این لایه تضمین می‌کند که گره‌ها می‌توانند یکدیگر را پیدا کرده و برای حفظ وضعیت فعلی معتبر شبکه بلاکچین، ارتباط برقرار کنند، منتشر و هماهنگ شوند.

۴. موارد استفاده از بلاکچین در سیستم مراقبت‌های بهداشتی

بلاکچین در آستانه تغییر سیستم‌های مراقبت بهداشتی است. برپایه اصل غیرمتمرکز بودن، بلاکچین می‌تواند امنیت اطلاعات بیمار را افزایش دهد، سلسله مراتب مراقبت‌های بهداشتی را تغییر داده و سیستم جدیدی ایجاد کند که در آن مردم درمان خود را مدیریت می کنند [۲۰]. این امکان، در راستای ارتقا فرهنگ مدیریت خود-مراقبتی [۷]ایجاد شده است. در یک سیستم مراقبت بهداشتی سنتی، سوابق پزشکی حساس، فاقد چارچوب ایمن هستند. مراقبت‌های بهداشتی از زمان پیشرفت فناوری‌ها رشد فوق‌العاده‌ای داشته است. مانند پزشکی از راه دور و IoMT در در عصر حاضر .

۴-۱. مدیریت داده‌های بیمار

فناوری بلاکچین در مقیاس وسیعی برای مدیریت موثر داده‌های بیمار با هدف افزایش امنیت و کاهش هزینه‌ها استفاده می‌شود. فناوری بلاکچین جزئیات متنوعی را برای اهداف مدیریتی ارائه می‌کند که پاسخگوی ذینفعان مختلف مانند بیماران، پزشکان، سازمان‌های دولتی، بیمارستان‌ها، بیمه‌گران و موارد مشابه باشد. با استفاده از فناوری بلاکچین، تاریخچه پزشکی جامع یک فرد را می‌توان مدیریت، به طور ایمن ثبت و برای مراجعات بعدی ذخیره کرد.

۴-۲. قابلیت ردیابی دارو

شرکت‌های داروسازی، در نتیجه جعل دارو، متحمل ضررهای مالی و احتمالاً از دست دادن وجهه حرفه‌ای خود می‌شوند. بهره‌گیری از یک سیستم با توانایی ردیابی دارو مبتنی بر بلاکچین، به جای استفاده از یک سیستم مدیریت زنجیره تامین استاندارد، کارایی زنجیره تامین را بهبود می بخشد. در [۲۱] ، یک سیستم ردیابی طراحی شده است که تعاملات بین ذینفعان و همچنین سیستم ردیابی دارو را بوسیله قرارداد هوشمند اجرایی می‌نماید.

۴-۳. آزمایش‌های بالینی و امنیت داده‌ها

در مطالعات بالینی، جمع‌آوری داده‌های معتبر و صحیح بسیار مهم است. در حقیقت این ویژگی‌ها برای ایجاد همبستگی8 بین داده ها، اندازه‌گیری و تجزیه و تحلیل مهم هستند. تا به امروز، چندین مطالعه اهمیت بلاکچین را برای آزمایش‌های بالینی مورد بررسی قرار داده‌اند [۲۲ ، ۲۳].

۴-۴. ردیابی دستگاه

یکی دیگر از راه حل‌های ایجاد تغییرات اساسی در مراقبت‌های بهداشتی، ردیابی دستگاه‌های پزشکی از زمان ساخت تا از کار افتادن آنها و همچنین مکان‌یابی آسان تجهیزات در مواقع اضطراری است. تمام بیمارستان‌ها با مدیریت مجموعه‌ای از تجهیزات پزشکی که توسط بخش‌ها و بیماران متعدد استفاده می شود، دست و پنجه نرم می‌کنند. قابل‌توجه‌ترین ویژگی بلاکچین تغییرناپذیری آن است. فناوری بلاکچین می‌تواند برای ایجاد یک گزارش تغییرناپذیر در راستای کمک به رعایت مقررات، با نگهداری اطلاعات مکان فعلی، مکان‌های قبلی، فروشنده، شماره سریال و غیره استفاده شود. از دیگر مزایای این فناوری، می‌توان به مکان‌یابی آسان تجهیزات در مواقع اضطراری اشاره کرد.

۴-۵. اینترنت اشیا در پزشکی

گسترش اینترنت اشیا، حجم عظیمی از داده‌ها را تولید می‌کند. یکی از راه‌های ارائه اعتبار در داده‌های ارسالی و دریافتی اینترنت اشیا از طریق فناوری بلاکچین، توسط هر شرکت‌کننده است که تضمین می‌کند داده‌ها تغییرناپذیر باقی بمانند. فناوری بلاکچین در صنعت مراقبت‌های بهداشتی، پتانسیل بهبود امنیت و شفافیت داده‌های اینترنت اشیا را دارد و در عین حال کارایی، مقیاس پذیری و استانداردسازی اینترنت اشیاء را در آینده ممکن می‌سازد. در پژوهش [۲۴]، مدلی پیشنهاد شده است که داده‌ها در بستر اینترنت اشیا مبتنی بر بلاکچین به طور ایمن منتقل شوند. این مدل انتقال، امنیت و یکپارچگی داده‌ها را ضمانت می‌کند. پژوهش [۲۵] به جهت رسیدگی به چالش‌های مربوطه همانند مدیریت داده‌ها و حفاظت از داده‌هاُ، ثبت تشخیص‌های پزشکی، سرعت و ایمنی تراکنش‌ها ،یک سیستم پردازش داده‌های چندرسانه‌ای را برای اینترنت اشیا در مراقبت‌های بهداشتی پیشنهاد کرده است.

.

۴-۶. بیمه سلامت، رسیدگی به دعاوی

یکی از ضروریات زندگی در جامعه امروز، بهره مندی از بیمه سلامت است. در چند سال گذشته، کلاهبرداری، موضوعی حساس در صنعت بیمه سلامت بوده است. بنابراین، توسعه فناوری‌هایی برای شناسایی موارد و پرداخت‌های متقلبانه نه تنها برای مقامات ملی بلکه برای شرکت‌های تجاری بیمه گذار قابل توجیه است. برای مرتفع ساختن نیازهای بهره‌وری و امنیت، بسیاری از سیستم‌های موجود از یک دفترکل غیرقابل تغییر برای یافتن هزینه‌های مضاعف ارزهای دیجیتال استفاده می‌کنند که توسط فناوری بلاکچین ایجاد شده است [۲۶].

۴-۷. فناوری بلاکچین در همه‌گیری کووید-۱۹

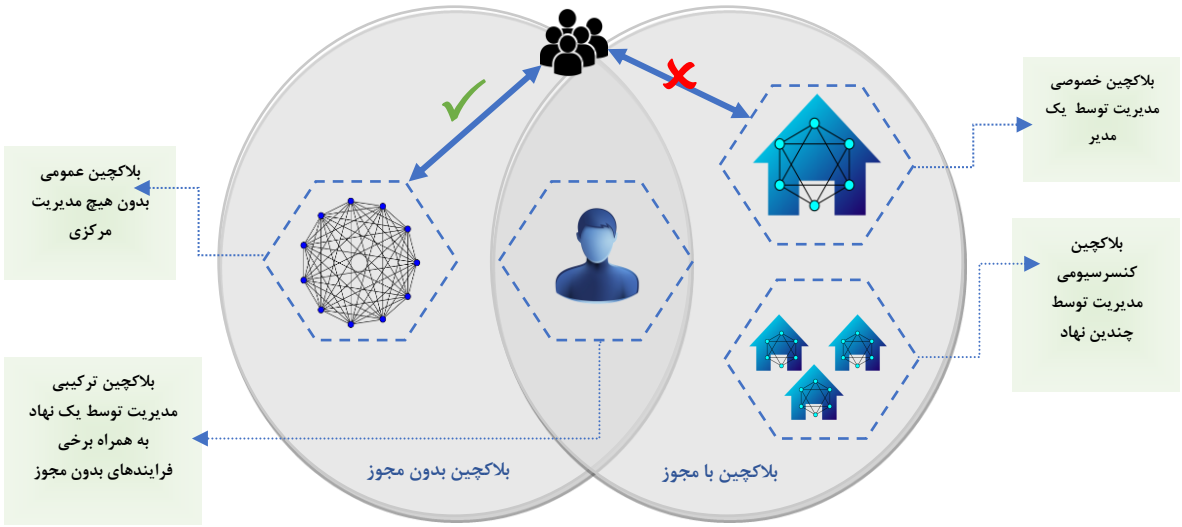
همه گیری جهانی کووید-۱۹ تمام جنبه‌های زندگی بشر را تغییر داد. در این راستا، فناوری اطلاعات به طور قابل توجهی برای مدیریت و کنترل انتقال، آزمایش و واکسیناسیون مورد استفاده قرارگرفت. برای مدیریت همه‌گیری این بیماری، که یک بحران پزشکی فوق‌العاده بود، تمرکز متخصصین حوزه سلامت دیجیتال، بر ارائه راهکارهای سلامت بالقوه جهت کاهش تأثیر این مساله معطوف شد [۲۷]. برخی از راه‌حل‌ها شامل ایجاد سیستم‌های نظارت قابل اعتماد و سلامت از راه دور، ابزارهای

تشخیصی و تصمیم‌گیری بالینی نوآورانه، استفاده از فناوری‌های پوشیدنی برای ردیابی شاخص‌های فیزیولوژیکی، و ایجاد سرویس‌های چت تعاملی برای انتشار اطلاعات درباره بیماری به عموم مردم بود.

۵. طبقه‌بندی بلاکچین

بلاکچین‌ها به دو دسته کلی «بلاکچین بدون مجوز» و «بلاکچین با مجوز» تقسیم می‌شوند. بلاکچین بدون مجوز یک بلاکچین عمومی است که از طریق شبکه برای همه در دسترس است. بلاکچین بدون مجوز به هرکسی اجازه پیوستن و مشارکت در شبکه می‌دهد. هر تراکنش توسط شرکت‌کنندگان از طریق یک الگوریتم اجماع، تایید و پردازش می‌شود. هر فردی که یک کامپیوتر و اتصال به اینترنت داشته باشد می‌تواند به عنوان یک گره ثبت نام کند و یک رکورد کامل بلاکچین را دریافت کند. بلاکچین با مجوز، سیستمی با کاربر مشخص است و دسترسی به انجام اقدامات متنوع در بلاکچین را محدود می‌کند. تراکنشها فقط در صورتی تایید و پردازش می‌شوند که شرکت‌کنندگان قبلاً عضو دفترکل شده باشند. هر بلاکچین با مجوز، خصوصی است و هر بلاکچین بدون مجوز، عمومی است. واژه «عمومی» به معنای «عمومی برای استفاده» است و نه «عمومی برای مشاهده تاریخچه تراکنش ها» و واژه «خصوصی» اشاره به«عمومی برای مشاهده» دارد، و نه «عمومی برای استفاده» [۲۸].

شکل۲ وجه تمایز این دو نوع بلاکچین را نشان می‌دهد. یک بلاکچین فدرال (بلاکچین کنسرسیومی) ترکیبی از بلاکچین‌های عمومی و خصوصی است. درواقع یک بلاکچین نیمه غیرمتمرکز است که سازمان‌های مختلف با یکدیگر همکاری می‌کنند تا در مورد نحوه ارائه خدمات بلاکچین به کاربران تصمیم گیری کنند. بلاکچین فدرال با بلاکچین خصوصی متفاوت بوده و فقط برای یک گروه بسته قابل دسترسی است. بلاکچین خصوصی دارای مدیریت متمرکز با یک مدل رمزنگاری دقیق برای اعتبارسنجی تراکنش‌ها است. بلاکچین ترکیبی، یک نوع بلاکچین منحصربه‌فرد و تحت کنترل یک نهاد واحد است که تمام مزایای یک بلاکچین عمومی از جمله امنیت، شفافیت، تغییر ناپذیری و غیرمتمرکز بودن را دارد. هرچند دسترسی به تراکنش‌ها، نماها و تغییرات را کنترل می‌کند.



شکل ۲- طبقه‌بندی بلاکچین [۳۳]

۶. الگوریتم‌های پیشنهادی اجماع [۹] بلاکچین در سیستم‌های مراقبت بهداشتی

مکانیسم اجماع بلاکچین، یکی از عناصر کلیدی سیستم‌های مراقبت بهداشتی مبتنی بر بلاکچین است. مکانیسم‌های اجماع [۲۹] در سال‌های اخیر مرکز توجه پژوهشگران بوده است. از طریق یک الگوریتم اجماع، همتایان توزیع شده برای اعتبارسنجی تراکنش، رضایت خود را اعلام می‌کنند. تاکنون الگوریتم‌های اجماع متعددی ایجاد شده‌اند. با این حال، تا به امروز مکانیسم اجماعی وجود ندارد که برای تمام مسائل و بویژه سیستم‌های مراقبت بهداشتی مناسب باشد. در ادامه برخی از الگوریتم‌های معروف اجماع مناسب سیستم های مراقبت بهداشتی معرفی می‌شوند.

۶-۱. الگوریتم اثبات سهام Proof-of-stake (PoS)

اثبات سهام، یک الگوریتم اجماع است که اعتباردهنده‌ها برای ایجاد بلوک‌های جدید در زنجیره، بر اساس تعداد سکه‌هایی که به عنوان وثیقه در میان گذاشته‌اند انتخاب می‌شوند. برخلاف الگوریتم اثبات‌کار که استخراج‌کنندگان را ملزم به حل مسائل پیچیده ریاضی برای اعتبارسنجی تراکنش‌ها و ایجاد بلوک‌های جدید می‌کند، PoS اجازه می‌دهد تا این فرایندها توسط یک اعتبارسنجی تصادفی انتخاب شده بر اساس سهم آنها در شبکه، انجام شود.

۶-۲. الگوریتم اثبات سهام نیابتی Delegated Proof-of-Stake (DPoS)

درDPoS، دارندگان توکن به انتخاب گروهی از «نمایندگان» که مسئول اعتبارسنجی تراکنش‌ها و ایجاد بلوک‌های جدید از طرف شبکه هستند رأی می‌دهند. نمایندگان بر اساس سهم آنها در شبکه یا شهرت آنها ، انتخاب می‌شوند. هر چه یک نماینده توکن‌های بیشتری در اختیار داشته باشد یا مورد اعتماد بیشتر از سوی شبکه باشد، شانس انتخاب شدن بیشتری دارد. هنگامی که نمایندگان انتخاب می‌شوند، به نوبت بلوک‌های جدید ایجاد می‌کنند و تراکنش‌ها را تأیید می‌کنند. نمایندگان تشویق می‌شوند تا به نفع شبکه عمل کنند زیرا هر گونه رفتار مخرب می‌تواند منجر به از دست دادن موقعیتشان گردد.

۶-۳. الگوریتم اثبات سهام استیجاری Leased Proof-of-Stake (LPoS)

درLPoS ، دارندگان توکن می‌توانند توکن‌های خود را به اعتباردهنده اجاره دهند. اعتباردهنگان می‌توانند از توکن‌های اجاره‌ای برای اعتبارسنجی تراکنش‌ها و ایجاد بلوک‌های جدید از طرف شبکه استفاده کنند. برخلافPoS ، که در آن اعتبارسنج‌ها برای شرکت در اعتبارسنجی بلوک نیاز به داشتن یک میزان حداقلی سهام دارند، LPoS به دارندگان توکن کوچک اجازه می‌دهد تا با اجاره دادن توکن‌های خود به اعتبارسنج، در اعتبارسنجی بلوک شرکت کنند. این امکان، منجر به غیرمتمرکزتر شدن شبکه می‌شود؛ چراکه شرکت‌کنندگان بیشتری می‌توانند در فرآیند اعتبار سنجی مشارکت کنند. در LPoS، مقدار توکن‌های اجاره‌شده، وزن اعتباردهنده در شبکه را تعیین می‌کند. هر چه یک اعتبارسنج توکن‌های بیشتری را کنترل کند، وزن بیشتری در شبکه داشته و شانس انتخاب شدن برای اعتبارسنجی تراکنش‌ها و ایجاد بلوک‌های جدید، بیشتر می‌شود.

۶-۴. الگوریتم اثبات اهمیت Proof-of-Importance (PoI)

در PoI ، گره‌ها بر اساس سهم کلی آنها در شبکه، تاریخچه تراکنش، تعداد اتصالات و مقدار توکن‌های نگهداری شده، امتیازی را از آن خود می‌کنند. هر چه امتیاز بالاتر باشد، احتمال بیشتری وجود دارد که یک گره برای اعتبارسنجی تراکنش‌ها و ایجاد بلوک‌های جدید انتخاب شود. این سیستم به کاربران انگیزه می‌دهد تا فعالانه در شبکه شرکت کنند. یکی از مزایای اصلی PoI این است که به کاربران کوچکتر اجازه می‌دهد تا تأثیر بیشتری بر شبکه، نسبت به سایر الگوریتم‌های اجماع، داشته باشند. با در نظر گرفتن سهم کلی کاربر در شبکه، به جای تعداد توکن‌هایی که دارند، PoI تمرکززدایی را ترویج می‌کند و به همه کاربران فرصتی برای مشارکت در اعتبارسنجی بلوک می‌دهد.

۶-۵. الگوریتم تحمل خطای بیزانسی کاربردی Practical Byzantine Fault Tolerance (PBFT)

درPBFT ، تمام گره‌های شبکه در چند دور با یکدیگر ارتباط برقرار می‌کنند تا در مورد وضعیت فعلی دفترکل به یک اجماع برسند. هر دور از چند مرحله‌ی درخواست، پیش آماده سازی، آماده سازی و تعهد تشکیل شده است. در طول هر مرحله، گره‌ها، پیام‌ها را مبادله می‌کنند و به اعتبار یک تراکنش یا بلوک خاص رأی می‌دهند. اگر تعداد کافی گره در مورد اعتبار یک تراکنش به توافق برسند، آن را به زنجیره بلوکی اضافه می‌کنند. این الگوریتم به گونه‌ای طراحی شده است که مقاوم در برابر خطا بوده و قادر است تا یک سوم گره‌های شبکه را که به‌طور مخرب یا ناموفق رفتار می‌کنند، مدیریت کند. PBFT به سطح معینی از تمرکز نیز نیاز دارد؛ چراکه گره‌ها برای برقراری ارتباط موثر، باید هویت تمام گره‌های دیگر در شبکه را بدانند. در نتیجه، PBFT معمولاً در شبکه‌های بلاکچین بامجوز، که هویت تمام شرکت‌کنندگان مشخص است، استفاده می‌شود.

۶-۶. پروتکل اجماع ستاره ای Stellar Consensus Protocol (SCP)

الگوریتم اجماع SCP در چند مرحله کار می‌کند. از مرحله نامگذاری شروع می‌شود، جایی که هر گره مقداری را برای توافق تعیین می‌کند. سپس مرحله رأی گیری اجرا می‌شود، که در آن گره‌ها روی مقادیر معین رأی می‌دهند. در نهایت، یک مرحله پذیرش وجود دارد که در آن گره‌ها مقدار را به عنوان مقدار نهایی می‌پذیرند که رأی کافی برای توافق را دریافت کرده است. در بلاکچین مبتنی بر الگوریتم استلار، اعتبارسنج‌ها، هیچ پاداش مالی دریافت نمی‌کنند. در عوض، اعضا تشویق می‌شوند تا به‌عنوان اعتبارسنج ثبت‌نام کنند؛ چراکه امنیت و انعطاف‌پذیری شبکه را افزایش می‌دهند. SCP به دلیل ملاحظات امنیتی و حفظ حریم خصوصی، یکی از گزینه‌های خوب برای سیستم‌های مراقبت بهداشتی مبتنی بر بلاکچین است.

۶-۷. الگوریتم Paxos و Multi-paxos

Paxos واژه‌ایست که به رسیدن به اجماع در شرایط نامشخص اشاره دارد. در صورت پارتیشن‌بندی شبکه یا قطع شدن سرور، سیستم‌های توزیع شده می‌توانند به طور قابل پیش‌بینی با الگوریتم Paxos به کار خود ادامه دهند. ذخیره‌سازی توزیع‌شده می‌تواند به اندازه یک ساختار داده ایمن رشته‌ای قابل پیش‌بینی عمل کند تا زمانی که یک برنامه مشتری بتواند با نقش‌های مهم در یک سیستم توزیع شده ارتباط برقرار کند. Paxos اغلب در مواقعی استفاده می‌شود که مجموعه داده‌های

عظیمی مانند فایل‌ها یا پایگاه‌های داده نیاز به تکرار داشته باشند و ویژگی دوام نیز ضروری باشد. پروتکل تلاش می‌کند حتی زمانی که تعداد محدودی از تکرارها پاسخگو نیستند، پیشرفت کند. سربار محاسبه الگوریتم Paxos زیاد است. در اثر توسعه Paxos ، نسخه‌ای به نام پکسوس چندگانه به وجود آمد. یک راهبر توسط Multi-Paxos انتخاب و مناقصه آغاز می‌شود. استفاده از چند پکسوس، کارایی بلاکچین را با تراکنش‌های متعدد بهبود می‌بخشد.

۶-۸. الگوریتم Raft

Raft جانشین الگوریتم Paxos است و یک الگوریتم اجماع مبتنی بر راهبر است که برای مدیریت شبکه‌های با مقیاس بزرگتر طراحی شده است. در یک محیط بسته توزیع شده، سرور اصلی به عنوان راهبر در نظر گرفته شده و سایر گره‌های باقی‌مانده دنبال‌کننده نامیده می‌شوند. راهبر، مسئول به روزرسانی داده‌ها و تکرار گزارش انتقال است. Raft با هدف آسان نمودن درک کلی سیستم، اجزای اساسی اجماع، مانند انتخاب رهبر، تکرار گزارش و ایمنی را از هم جدا می‌کند. همچنین سطح بالاتری از انسجام را برای به حداقل رساندن تعداد حالت‌هایی که باید در نظر گرفته شوند، اعمال می‌کند. ورودی‌های جدید توسط راهبر به گزارش اضافه می‌شوند و داده‌ها از راهبر به سرورهای دیگر جاری می‌شوند.

۶-۹. الگوریتم ZAB (ZooKeeper Atomic Broadcast)

در یک سیستم مبتنی برZab ، یک گره به عنوان راهبر انتخاب می‌شود و مسئول پیشنهاد به روزرسانی به سایر گره‌های شبکه است. گره‌های دیگر، که دنبال‌کننده نامیده می‌شوند، به روزرسانی پیشنهادی را بر اساس دیدگاه خود از وضعیت فعلی سیستم می‌پذیرند یا رد می‌کنند. هنگامی که اکثر دنبال‌کنندگان یک به روز رسانی را پذیرفتند، راهبر آن را برای بقیه شبکه منتشر می‌کند. ویژگی پخش اتمی Zab تضمین می‌کند که همه یا هیچ یک از شرکت‌کنندگان یک به‌روزرسانی را اعمال نمی‌کنند، و از ناهماهنگی‌های ممکن در اثر به‌روزرسانی‌های جزئی جلوگیری می‌کند. این الگوریتم مورد اعتماد سیستم‌های توزیع شده با قابلیت تحمل خطا است.

۶-۱۰. الگوریتم اثبات یادگیری عمیق Proof-of-deep-learning (PoDL)

برای پشتیبانی از برنامه‌های محاسبات لبه‌ای با دسترسی چندگانه multi-access edge computing (MEC) و تضمین امنیت و حریم خصوصی، یک الگوریتم اجماع اثبات یادگیری عمیق توسعه داده شد [۳۰]. این الگوریتم از یادگیری عمیق برای نگهداری بلاکچین‌ها به جای محاسبات هش بیهوده استفاده می‌کند.

۶-۱۰. الگوریتم اثبات اعتبار توزیع‌شده مبتنی بر راستگویی Honesty-based distributed proof of authority (HDPoA)

یکی از مسائل مربوط به الگوریتم‌های اجماع که در فضای اینترنت اشیا استفاده می‌شوند این است که برخی از دستگاه‌ها فاقد منابع و قدرت محاسباتی هستند. استفاده از بلاکچین در اینترنت اشیا مزایای متعددی را نسبت به سیستم‌های سنتی دارد. از جمله این مزایا می‌توان به افزایش امنیت از طریق تضمین یکپارچگی داده‌ها و مسئولیت‌پذیری و کنترل قابلیت اعتماد بر روی دستگاه‌های متعدد اشاره کرد. برای افزایش یکپارچگی و امنیت داده ها، الگوریتم HDPoA پیشنهاد شد[۳۱].

الگوریتم پیشنهادی هنگام استقرار در چندین دستگاه، عملکردی بهبود یافته را از نظر مصرف انرژی و قدرت هش نشان داد. تجزیه و تحلیل های امنیتی نشان داد که HDPoA ایمن و مناسب برای برنامه‌های کاربردی اینترنت اشیا با بلاکچین است. بنابراین پیش‌بینی می‌شود که این الگوریتم، انتخاب مناسبی در صنعت ۴.۰ باشد.

۷. داده‌کاوی با بهره‌گیری از فناوری بلاکچین

تکنیک‌های داده‌کاوی را می‌توان به طور کلی به یادگیری تحت نظارت و بدون نظارت طبقه بندی کرد. یادگیری نظارت شده شامل آموزش مدلی بر روی داده های برچسب گذاری شده است، در حالی که یادگیری بدون نظارت شامل کشف الگوها در داده های بدون برچسب است [۳۲]. ما چارچوبی را برای استفاده از الگوریتم‌های اجماع در برنامه‌های داده کاوی پیشنهاد می‌کنیم. اولین قدم، شناسایی یک وظیفه خاص در داده‌کاوی است. این گام می‌تواند هر فرایندی از پیشبینی ریزش مشتریان دفاتر بیمه سلامت تا شناسایی تراکنش‌های تقلبی در دعاوی بیمه باشد. هنگامی که وظیفه شناسایی شد، الگوریتم داده کاوی مناسب را می‌توان انتخاب کرد. گام بعدی تعیین این است که کدام الگوریتم اجماع برای کار مورد نظر مناسب‌تر است. به عنوان مثال، اگر این کار شامل پردازش سریع مقادیر زیادی از داده ها باشد، ممکن است PoW به دلیل نیازهای محاسباتی بالا، بهترین انتخاب نباشد. از سوی دیگر، اگر کار شامل تصمیم گیری بر اساس مقدار کمی داده باشد، PoS یا DPoS ممکن است مناسب تر باشند. هنگامی که الگوریتم اجماع انتخاب شد، می‌توان آن را در فرآیند داده‌کاوی ادغام کرد. به عنوان مثال، در یک سیستم مبتنی بر PoW، گره‌ها می توانند برای حل یک مشکل داده‌کاوی خاص به منظور افزودن یک بلوک جدید به زنجیره رقابت کنند. در یک سیستم مبتنی بر PoS، گره‌هایی با بیشترین ارز دیجیتال می‌توانند برای اعتبارسنجی تراکنش‌های جدید و اضافه کردن آنها به دفتر کل انتخاب شوند.

در [۳۳] یک مدل تشخیص بیت‌کوین بر اساس الگوریتم اجماع PoW بر اساس سه متد مطرح داده‌کاوی شامل SVM، AdaBoost و جنگل تصادفی پیشنهاد شده است که عنوان شده الگوریتم AdaBoost عملکرد بهتری به لحاظ مقایسه معیار پوشش (Recall)داشته است.

۸. بحث‌ها، چالش‌ها و فرصت‌های پژوهشی

در این بخش چالش‌ها و فرصت‌های تحقیقاتی این حوزه بر اساس مرور ادبیات ارائه شده در این مقاله ارائه شده است. حفظ حریم خصوصی داده‌ها، تعیین اندازه بلوک، مقیاس‌پذیری، تعداد گره‌ها و پاسخگویی سیستم، انجام تجزیه و تحلیل و تجسم داده‌ها، انتخاب الگوریتم اجماع، مدیریت هزینه انتقال داده ها، مدیریت فرآیندهای تجاری و مصائب موجود در قوانین و مقررات جوامع با وجود این فناوری، از جمله چالش‌هایی هستند که همچنان نیاز است تا محققان و متخصصان به بررسی آنها بپردازند.

- **مقیاس‌پذیری**: یکی از چالش‌های اصلی شبکه‌های بلاکچین، مقیاس‌پذیری است. همانطور که تراکنش‌های بیشتری در شبکه پردازش می‌شود، استفاده از آن کندتر و گران‌تر می‌شود.
- **قابلیت همکاری**: در حال حاضر، اغلب شبکه‌های بلاکچین ، مستقل از یکدیگر عمل می‌کنند که در نتیجه انتقال داده‌ها بین آنها را دشوار می‌کند. تلاش‌هایی برای توسعه استانداردهایی در حال انجام است که به بلاکچین‌های مختلف اجازه برقراری ارتباط و همکاری دوجانبه بدهد.

- **حریم خصوصی**: در حالی که تمام تراکنش‌های بلاکچین به صورت عمومی قابل مشاهده هستند، برخی از پروژه‌ها در حال بررسی راه‌هایی در راستای ارائه حریم خصوصی بیشتر برای کاربران هستند. این ارتقا می‌تواند شامل استفاده از فناوری‌هایی مانند اثبات دانش صفر یا رمزگذاری هومومورفیک برای فعال کردن تراکنش‌های خصوصی در بلاکچین های عمومی باشد.
- **حکمرانی**: با غیرمتمرکز شدن شبکه‌های بلاکچین، نیاز به توسعه ساختارهای حاکمیتی مؤثر برای اطمینان از توسعه و پایداری مداوم آنها وجود دارد.

پایداری: مصرف انرژی مورد نیاز برای تامین انرژی برخی از شبکه‌های بلاکچین نگرانی‌هایی را در مورد تاثیرات زیست محیطی آنها ایجاد کرده است.

۹. نتیجه

در حال حاضر، فناوری بلاکچین در مقایسه با گذشته نقش مهمی را در IoMT و مراقبت‌های بهداشتی ایفا می‌کند. در گذشته، داده‌های مراقبت‌های بهداشتی عمدتاً در سرورهای متمرکزی که در برابر تهدیدات سایبری آسیب‌پذیر بودند، ذخیره می‌شد. این مسئله منجر به نگرانی‌هایی در مورد حریم خصوصی و امنیت بیمار و همچنین چالش‌هایی در اشتراک گذاری و دسترسی به داده‌های بیمار شده است. با این حال، با ظهور فناوری بلاکچین، تغییر قابل توجهی به سمت اشتراک‌گذاری داده‌های غیرمتمرکز، ایمن و شفاف در مراقبت‌های بهداشتی صورت گرفته است. فناوری دفترکل غیرقابل تغییر بلاکچین یک رکورد ضددستکاری از داده‌های پزشکی را ارائه می‌دهد که توسط اشخاص مجاز می‌تواند به طور ایمن و کارآمد قابل دسترسی باشد. این امر امنیت داده ها را افزایش، قابلیت همکاری را بهبود و به اشتراک‌گذاری یکپارچه داده‌ها در بین ارائه دهندگان مراقبت‌های بهداشتی را تسهیل می‌کند. امروزه در زمینه IoMT ، فناوری بلاکچین امکان تراکنش‌های داده‌ای امن و خودکار را بین دستگاه‌های متصل و ارائه دهندگان مراقبت‌های بهداشتی فراهم می‌کند. این یک اکوسیستم مراقبت‌های بهداشتی منسجم‌تر و کارآمدتر ایجاد می‌کند، جایی که داده‌ها در زمان واقعی منتقل می‌شوند و منجر به تشخیص سریع‌تر و بهبود نتایج بیمار می‌شود. علاوه بر این، فناوری بلاکچین بیماران را قادر می‌سازد تا کنترل بیشتری بر روی داده‌های سلامتی خود داشته باشند و به آنها این امکان را می‌دهد تا آن‌ها را با هر فردی که انتخاب می‌کنند به اشتراک بگذارند. درحالی که در گذشته بیماران کنترل کمی بر داده‌های سلامتی خود داشتند و نمی‌توانستند به راحتی به داده‌های خود دسترسی داشته باشند یا آن‌ها را به اشتراک بگذارند. به طور کلی، فناوری بلاکچین می‌تواند صنعت مراقبت‌های بهداشتی را با افزایش امنیت داده‌ها، بهبود قابلیت همکاری و توانمندسازی بیماران متحول سازد.

فناوری بلاکچین و داده‌کاوی دو حوزه مهم با کاربردهای بالقوه فراوان هستند. با ترکیب این دو زمینه می‌توان ابزارهای قدرتمند جدیدی برای تجزیه و تحلیل و پردازش داده‌ها به صورت امن و غیرمتمرکز ایجاد کرد. چارچوب پیشنهادی نقطه شروعی برای کاوش در فصل مشترک الگوریتم‌های اجماع بلاکچین و داده‌کاوی فراهم می‌کند و انتظار داریم در سال‌های آینده شاهد پیشرفت‌های هیجان‌انگیز زیادی در این زمینه باشیم.

با نگاهی به آینده، چندین گام موثر وجود دارد که می تواند قابلیت‌های فناوری بلاکچین را بیشتر افزایش دهد. یکی از امیدوارکننده‌ترین آنها، توسعه برنامه‌های مالی غیرمتمرکز است که از بلاکچین برای ایجاد محصولات و خدمات مالی فارغ از واسطه‌های سنتی استفاده کند. یکی دیگر از زمینه‌های نوآوری، توسعه سیستم های مدیریت زنجیره تامین مبتنی بر بلاکچین است که می‌تواند به افزایش شفافیت و قابلیت ردیابی در زنجیره‌های تامین جهانی کمک کند. در نتیجه، در حالی که فناوری بلاکچین هنوز با چالش‌هایی مواجه است، پتانسیل بسیار زیادی برای رشد صنایع و برهم زدن مدل‌های تجاری سنتی دارد.

همانطور که این فناوری به رشد و تکامل خود ادامه می‌دهد، می‌توان انتظار داشت که در سال‌های آینده شاهد ظهور موارد استفاده نوآورانه‌تر باشیم.

مراجع

1. Zhang, Q., He, Y., Lai, R., Hou, Z. and Zhao, G. (2023). A survey on the efficiency, reliability, and security of data query in blockchain systems. Future Generation Computer Systems.
2. Zhang, P., Schmidt, D.C., White, J. and Lenz, G. (2018). Blockchain technology use cases in healthcare. In Advances in computers, Vol. 111, pp. 1-41.
3. Ramachandran, A. and Kantarcioglu, D. (2017). Using blockchain and smart contracts for secure data provenance management. arXiv preprint arXiv:1709.10000.
4. Zhu, L., Wu, Y., Gai, K. and Choo, K.K.R. (2019). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 91, 527-535.
5. Shah, Z., Ullah, I., Li, H., Levula, A., and Khurshid, K. (2022). Blockchain based solutions to mitigate distributed denial of service (ddos) attacks in the internet of things (iot): A survey. Sensors, 22(3), 1094.
6. Khatri, S., Alzahrani, F. A., Ansari, M. T. J., Agrawal, A., Kumar, R., and Khan, R.A. (2021). A systematic analysis on blockchain integration with healthcare domain: scope and challenges. IEEE Access, 9, 84666-84687.
7. Islam, A. and Soo Y.S. (2020). "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things." *Computers & Electrical Engineering* 84 : 106627.
8. Gökalp, E., Gökalp, M.O., Çoban, S., and Eren, P.E. (2018). Analysing opportunities and challenges of integrated blockchain technologies in healthcare. *Information Systems: Research, Development, Applications, Education: 11th SIGSAND/PLAIS EuroSymposium 2018, Gdansk, Poland, Proceedings 11*, 174-183.
9. Agbo, C.C., Mahmoud, Q.H. and Eklund, J.M. (2019). Blockchain technology in healthcare: a systematic review. *In Healthcare*, Vol. 7, No. 2, p. 56.
10. McGhin, T., Choo, K.K.R., Liu, C.Z. and He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*, 62-75.
11. Kuo, T.T., Kim, H. E. and Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211-1220.
12. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 21260.
13. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*, 1-32.
14. Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A.M. (2016). Using blockchain for medical data access and permission management'. In *2nd International Conference on Open and Big Data* .pp. 1-2.

15. Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M. and Khan, M. I.A. (2022). Blockchain technology in healthcare: A systematic review. *Plos one*, *17*(4), e0266462.
16. Linn, L.A. and Koo, M.B. (2016, September). Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST* (pp. 1-10).
17. Agrawal, D., Minocha, S., Namasudra, S. and Gandomi, A.H. (2022). A robust drug recall supply chain management system using hyperledger blockchain ecosystem. *Computers in biology and medicine*, *140*, 105100.
18. Anik, F.I., Sakib, N., Shahriar, H., Xie, Y., Nahiyan, H.A. and Ahamed, S.I. (2023). Unraveling a blockchain-based framework towards patient empowerment: A scoping review envisioning future smart health technologies. *Smart Health*, 100401.
19. Aliakbarpoor, Y., Comai, S. and Pozzi, G. (2017). Designing a HL7 compatible personal health record for mobile devices. In *2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI)* (pp. 1-6). IEEE.
20. Singh, A.P., Pradhan, N.R., Luhach, A.K., Agnihotri, S., Jhanjhi, N.Z., Verma, S. and Roy, D. S. (2020). A novel patient-centric architectural framework for blockchain-enabled healthcare applications. *IEEE Transactions on Industrial Informatics*, 17(8), 5779-5789.
21. Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y. and Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE access*, *9*, 9728-9743.
22. Omar, I. A., Jayaraman, R., Salah, K., Yaqoob, I. and Ellahham, S. (2021). Applications of blockchain technology in clinical trials: review and open challenges. *Arabian Journal for Science and Engineering*, *46*, 3001-3015.
23. Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G. and Al-Khateeb, H. (2019). Blockchain and clinical trial. *Adv Sci Technol Secur Appl*, *1*(1), 6-10.
24. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A. and Islam, A.N. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *Journal of Parallel and Distributed Computing*, *172*, 69-83.
25. Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R.M., Salem, M., Alzahrani, A.A. and Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, *65*, 263-274.
26. Raikwar, M., Mazumdar, S., Ruj, S., Gupta, S. S., Chattopadhyay, A. and Lam, K.Y. (2018, February). A blockchain framework for insurance processes. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-4). IEEE.
27. Kapoor, A., Guha, S., Das, M. K., Goswami, K.C. and Yadav, R. (2020). Digital healthcare: The only solution for better healthcare during COVID-19 pandemic?. *Indian Heart Journal*, 72(2), 61-64.
28. Solat, S., Calvez, P. and Naït-Abdesselam, F. (2021). Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *J. Softw.*, *16*(3), 95-106.
29. Yadav, A. S., Singh, N. and Kushwaha, D. S. (2023). Evolution of Blockchain and consensus mechanisms & its real-world applications. *Multimedia Tools and Applications*, 1-46.

30. Chenli, C., Li, B., Shi, Y. and Jung, T. (2019, May). Energy-recycling blockchain with proof-of-deep-learning. In *2019 IEEE International Conference on Blockchain and Cryptocurrency*, pp. 19-23.
31. Andrew, J., Isravel, D. P., Sagayam, K.M., Bhushan, B., Sei, Y. and Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, 103633.
32. Hewage, U. H. W. A., Sinha, R., & Naeem, M. A. (2023). Privacy-preserving data (stream) mining techniques and their impact on data mining accuracy: a systematic literature review. *Artificial Intelligence Review*, 1-38.
33. Dong, Z. (2023). Application of Big Data Mining Technology in Blockchain Computing. *International Journal of Informatics and Information Systems*, *6*(2), 81-88.

[1] Internet of Medical Things
[2] Peer-to-Peer
[3] Proof-of-Work
[4] Proof-of-Stake
[5] Electronic Health Records (EHRs)
[6] Personal Health Records (PHRs)
[7] Self-care Management
[8] Correlation
[9] Consensus Algorithms