



دانشگاه صنعتی امیر کبیر
(پلی تکنیک تهران)

گزارش نهایی درس روش پژوهش و ارائه
تأثیر بلاک چین بر روی سیستم سلامت و بهبود آن

نگارش

سپهر مقیسه

استاد راهنما

دکتر رضا صفابخش

استاد مشاور

دکتر بابک صادقیان

بهار ۱۴۰۱

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

تقدیم به پدر بزرگوار و مادر مهربانم

آن دو فرشته‌ای که از خواسته‌هایشان گذشتند، سختی‌ها را به جان خریدند و خود را سپربلای مشکلات و ناملایمات
کردند تا من به جایگاهی که اکنون در آن ایستاده‌ام برسم.

سپاس‌گزاری

به مصداق «من لم یشکر المخلوق لم یشکر الخالق» بسی شایسته است از استاد فرهیخته و فرزانه جناب آقای دکتر رضا صفابخش که با کرامتی چون خورشید، سرزمین دل را روشنی بخشیدند و گلشن سرای علم و دانش را با راهنمایی‌های کارساز و سازنده بارور ساختند تقدیر و تشکر نمایم.

سهر مقصیه

ارویشت ۱۴۰۰

چکیده

تکنولوژی بلاک چین در مواردی مانند پرداخت‌های آنلاین، سیستم سلامت، قراردادهای هوشمند و ... به کار می‌رود. در شبکه هر انتقال اطلاعاتی بدون ناظر خاصی ثبت و انجام می‌شود. بلاک چین مجموعه‌ای بلاک‌ها است که به کمک یک زنجیر متصل هستند. یک بلاک بعد از تأیید توسط تمامی بلاک‌ها به این زنجیره اضافه می‌شود. دلیل استفاده از این فناوری، ثبت یک سند از گواهی سلامت و تأییدیه آن‌ها که در آینده کارآمد خواهند بود و به سازمان‌ها اجازه استفاده از آن‌ها در زمان مناسب را می‌دهد. این کار اجازه می‌دهد تا پزشک بتواند اطلاعات خود مانند سند پزشکی، مدرک به پایان رساندن دوره کارآموزی و سایر اطلاعات را در بلاک چین به ثبت برساند.

واژه‌های کلیدی:

بلاک چین، سیستم سلامت، بهبود، قرارداد هوشمند

فهرست مطالب

عنوان	صفحه
۱ مقدمه	۱ -
۱-۱ دنیای سلامت نیازمند یک راهکار جدید است	۲ -
۲ مقدمه‌ای بر بلاک چین	۳ -
۱-۲ توضیحات کلی بلاک چین	۴ -
۲-۲ انواع مفهوم‌های مورد استفاده در بلاک چین	۴ -
۳-۲ معماری اصلی بلاک چین	۷ -
۳ تأثیرات بلاک چین بر سیستم سلامت	۸ -
۱-۳ دلایل استفاده از بلاک چین در سیستم سلامت	۹ -
۱-۱-۳ قابلیت همکاری	۹ -
۲-۱-۳ سیستم بیمار محور	۱۰ -
۲-۳ استفاده‌های بلاک چین در سیستم سلامت	۱۱ -
۱-۲-۳ شناسایی داروی مسکن برای تشخیص احتمال تشنج	۱۱ -
۲-۲-۳ استفاده از داده‌ها برای به کار بردن پزشکی در پزشکی از راه دور	۱۲ -
۳-۲-۳ به اشتراک گذاشتن داده‌های سرطانی با اجازه بیمار	۱۲ -
۴-۲-۳ ثبت داده‌های سرطانی	۱۳ -
۵-۲-۳ هویت دیجیتال کاربر	۱۳ -
۶-۲-۳ اسناد پزشکی شخصی	۱۴ -
۷-۲-۳ دآوری حق بیمه	۱۴ -
۴ چارچوب‌های پیاده‌سازی شده به کمک بلاک چین	۱۶ -
۱-۴ چارچوبی برای اشتراک‌گذاری امن داده‌های تصویری - پزشکی	۱۷ -
۱-۱-۴ معماری ساختمان داده	۱۷ -
۲-۴ استفاده از دانش اینترنت نسل پنجم برای ارتباط میان بلاک چین و سیستم سلامت	۲۰ -



۵ نتیجه گیری - ۲۲ -

منابع - ۲۴ -

فهرست اشکال

عنوان	صفحه
شکل ۱- بلاک چین در سیستم سلامت	۲ -
شکل ۲- الگوریتم سکویی	۵ -
شکل ۳- الگوریتم توافق عام	۶ -
شکل ۴- نسخه های مختلف الگوریتم توافق عام	۶ -
شکل ۵- معماری بلاک چین	۷ -
شکل ۶- پل ارتباطی بلاک چین میان سیستم ها و تاریخ انتقالات	۱۲ -
شکل ۷- حق داوری خودکار	۱۵ -
شکل ۸- مراحل پردازش تصویری داده های پزشکی	۱۷ -
شکل ۹- مراحل پردازش تصویری بلاک چین	۱۹ -
شکل ۱۰- تابع ایجاد کلید	۲۱ -

فهرست جداول

عنوان	صفحه
جدول ۱- سه مرحله قابلیت همکاری	۹ -
جدول ۲- خلاصه کاربرد های استفاده بلاک چین در سیستم سلامت	۱۱ -

فصل اول

مقدمه

بلاک‌چین مجموعه‌ای بلاک‌ها است که به کمک یک زنجیر متصل هستند. یک بلاک بعد از تأیید توسط تمامی بلاک‌ها به این زنجیره اضافه می‌شود. این تکنولوژی با روشی که دارد، مورد توجه سهام‌داران واقع شده است. سیستم الکترونیکی ثبت اسناد داده که در قدیم برای اشتراک‌گذاری میان سهام‌داران سیستم سلامت بکار می‌رفت، به دلیل تمرکز بسیار بر داده‌های مرکزی، امنیت پایین و خطادار بودن مورد انتقاد واقع شده است. [۵]

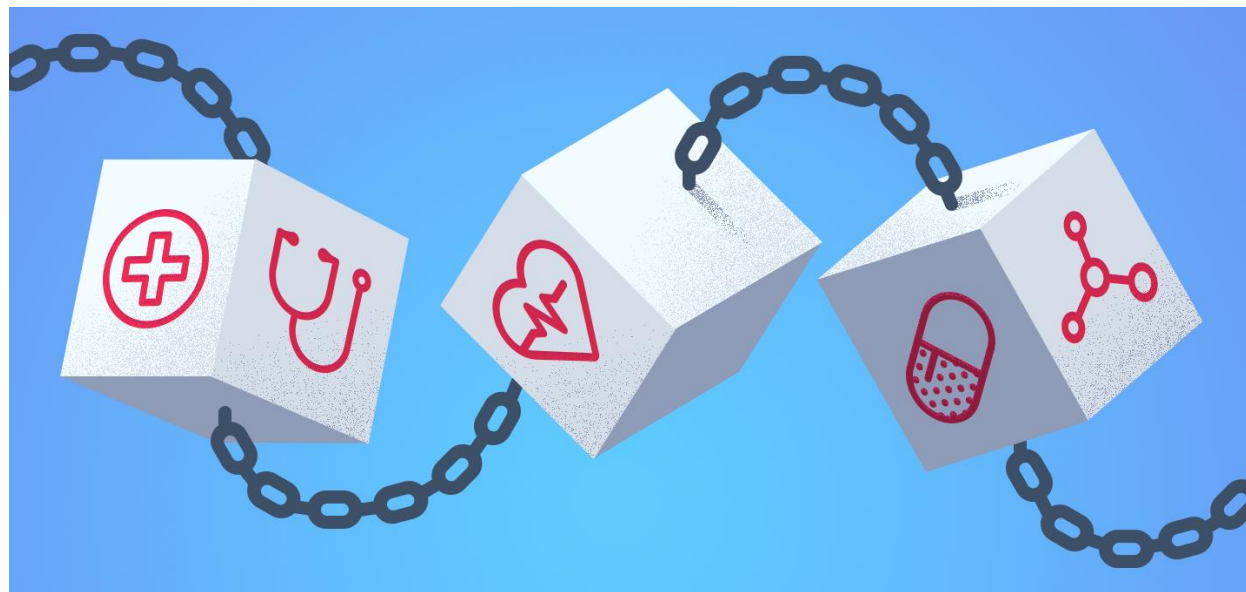
1-1 دنیای سلامت نیازمند یک راهکار جدید است

در حال حاضر دنیا با بحران‌های متعددی نظیر بیماری کرونا روبه‌رو شده است. این بیماری باعث شده مشکلات زیادی از جمله محدودیت‌های سیستم سلامت در رسیدگی به این بیماری، پدیدار شود. بلاک‌چین با فعال کردن اشتراک‌گذاری غیرمرکزی داده‌ها، محافظت از اطلاعات بیماران و مدیریت مطمئن داده‌ها می‌تواند با پاندمی‌ها مقابله کند. [۸]

در حوزه سلامت نقل و انتقالی وجود دارند که نیاز به ثبت دائمی و غیرقابل تغییر دارند. می‌توان به نقل و انتقالی مانند خرید و فروش و یا ارسال مرسولات بهداشتی اشاره کرد.

در حالی که دستگاه‌های متعددی برای نوآوری در داروسازی وجود دارد، برای دیگر نوآوری‌ها دستگاهی وجود ندارد. با در نظر گرفتن مهم بودن اشتراک‌گذاری اطلاعات، جامعه سلامت حال حاضر نیاز به بیمار دارد تا بتواند اسنادی را به اشتراک و یا ثبت برساند. [۱۰]

پس ما در این مقاله در اول به کمبود سیستم سلامت در حال حاضر می‌پردازیم و کمبودها را شناسایی می‌کنیم. در قدم بعدی به این نتیجه می‌رسیم که چرا باید از بلاک‌چین استفاده کنیم و در کدام زمینه‌های سلامتی کاربرد دارد؛ و در انتهای راه چندی از این مثال‌ها را با یکدیگر مرور می‌کنیم و بحث را جمع می‌کنیم.



شکل 1-1 بلاک‌چین در سیستم سلامت

فصل دوم

مقدمه‌ای بر بلاک چین

۱-۲ توضیحات کلی بلاک چین [۱]

تکنولوژی بلاک چین در مواردی مانند پرداخت‌های آنلاین، سیستم سلامت، قراردادهای هوشمند و ... به کار می‌رود در شبکه هر انتقال اطلاعاتی بدون ناظر خاصی ثبت و انجام می‌شود. بلاک چین مجموعه‌ای بلاک‌ها است که به کمک یک زنجیر متصل هستند. یک بلاک بعد از تأیید توسط تمامی بلاک‌ها به این زنجیره اضافه می‌شود. بعد از اضافه شدن بلاک، بلاک چین به سه بخش تقسیم می‌شود:

۱. بخش private

۲. بخش public

۳. بخش permissioned

از فواید بلاک چین می‌توان به حافظه بیشتر، امنیت، غیرقابل نفوذ بودن، سرعت در پردازش و سیستم غیر کانونی اشاره کرد.

هسته بلاک چین گره‌ها، انتقالات، بلاک، و زنجیر هست.

این تکنولوژی بر نظام یکپارچگی اما امنیت اشاره دارد. از بلاک چین در تکنولوژی‌هایی همانند ارز دیجیتال و برنامه‌های غیر کانونی^۱ استفاده می‌شود.

قراردادهای هوشمند وابسته به بلاک چین که مستقیماً کدی را برای کنترل مستقیم مبادلات یا توزیع مجدد دارایی‌های دیجیتال (مانند رمزهای رمزنگاری یا برخی از داده‌ها) بین دو یا چند طرف، طبق قوانین یا توافقاتی که قبلاً بین شرکت‌کنندگان درگیر ایجاد شده است، ارائه می‌دهند.

قراردادهای هوشمند می‌توانند اشیاء داده را ذخیره کرده و عملیات روی داده را تعریف کنند و توسعه را امکان‌پذیر می‌کنند. در حوزه بهداشت و درمان می‌توان از قراردادهای هوشمند برای ایجاد فنی ایمن و مؤثر زیرساخت‌هایی برای افزایش هماهنگی و کیفیت مراقبت و در نتیجه بهبود رفاه افراد و جوامع، استفاده کرد.

در حال حاضر بلاک چین قابلیت برطرف ناسازگاری همکاری ایجاد شده در سیستم سلامت را برطرف کند و استاندارد مورد نیاز برای برقراری ارتباطی امن میان ارائه‌دهندگان سیستم سلامت، موجودیت‌های سلامتی، و محققین سلامت و دارویی، باشد.

۲-۲ انواع مفهوم‌های مورد استفاده در بلاک چین

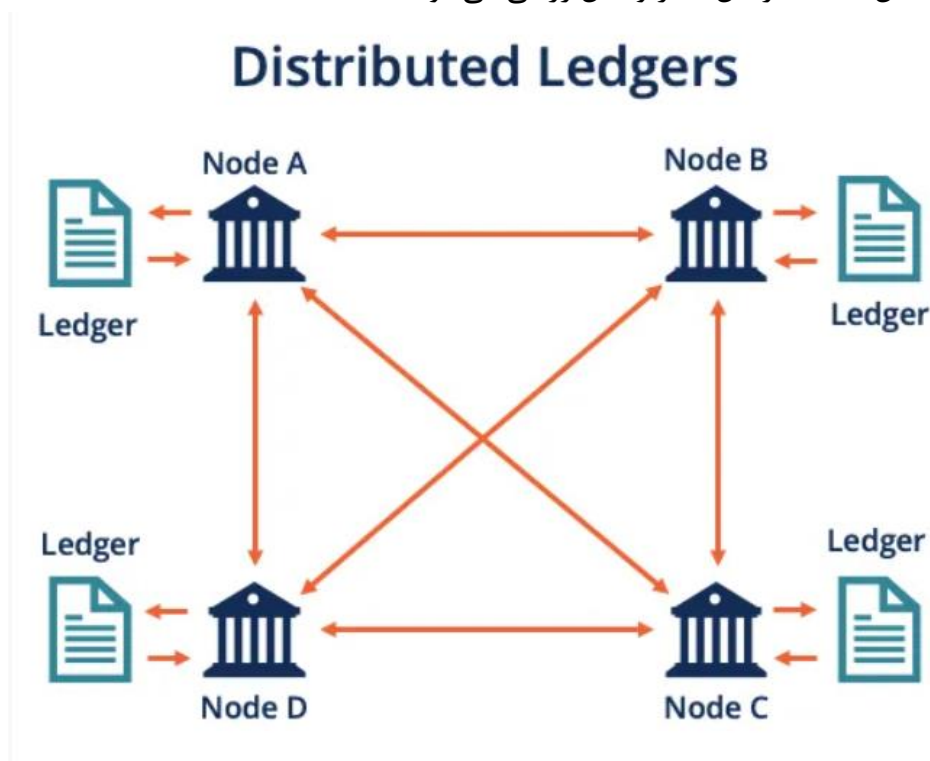
الگوریتم سکویی^۲:

در این الگوریتم هر دیتابیس در شبکه نظیر به نظیر به اشتراک گذاشته می‌شوند در بلاک چین دیتابیس برای تمامی مخاطبین شبکه به اشتراک گذاشته می‌شود. هیچ بیگانه‌ای خارج از شبکه‌ای برای به انجام در آمدن تراکنش‌ها نیاز نیست. هر نقل و انتقالی بدون کمک شی بیگانه‌ای می‌تواند بین دو یا چند مخاطب بیت کوین به اشتراک گذاشته شود.

¹ Decentralized-app

² distributed ledger

هر رکورد دارای یک نشانه امنیتی خاص به همراه خط زمانی مشخصی که زمان دسترسی‌ها را نشان می‌دهد، است. به همین دلیل تخته غیرقابل تغییر و قابل بررسی می‌شود.



شکل ۲-۱/ الگوریتم سکویی

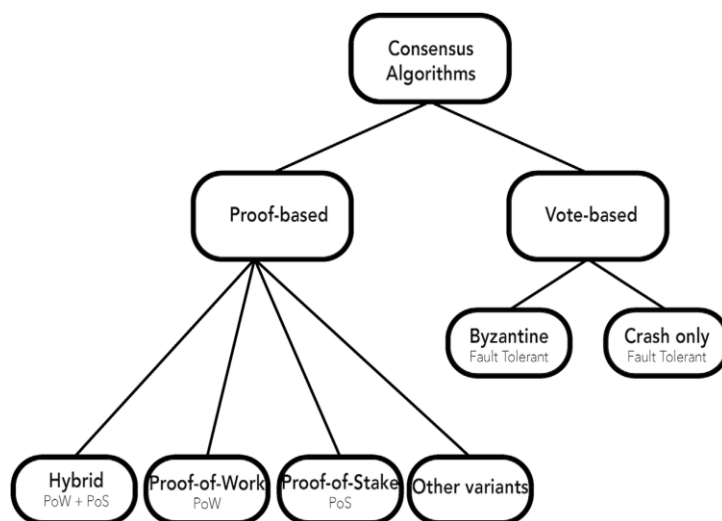
الگوریتم توافق عام^۳:

فرایند یک بلاک تنها در میان چند گره‌ای که به آنها تعلق ندارد اشاره می‌کند. بلاک‌های بلاک‌چین از این نوع الگوریتم بهره می‌گیرند.

³ Consensus algorithms



شکل ۳ الگوریتم توافق عام



شکل ۴ نسخه های مختلف الگوریتم توافق عام

قرارداد هوشمند (smart contract):

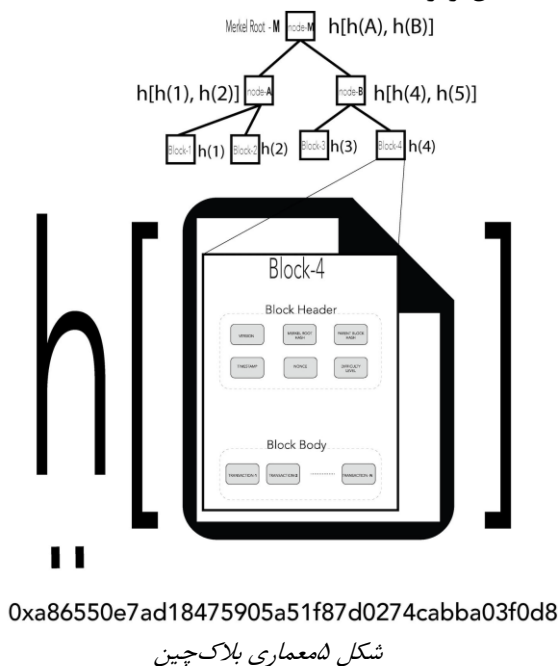
ابزار برنامه‌نویسی شده‌ای که بر روی بلاک‌چین اجرا می‌شود.

بهبود امنیت:

به دلیل رفع اجازه دسترسی اجباری از سوی قدرت مرکزی، هیچ فردی به راحتی نمی‌تواند مشخصات سیستم را برای نفع خود عوض کند.

۲-۳ معماری اصلی بلاک چین^[۵]

ساختار کلی بلاک چین به صورت شکل زیر است:



شکل ۵ معماری بلاک چین

یک بلاک در بلاک چین دارای اطلاعات هش^۴ شده است. این اطلاعات معمولاً دارای یک سر تیتر^۵ و پیام بدنه است. سر تیتر معمولاً نسخه بلاک چین، هش والد، زمان و تاریخ و سطح سختی در خود دارد. بدنه دارای یکلیست از دادوستدهای انجام شده که بلاک چین اجازه انجام داده است را دارد.

^۴ hash

^۵ header

فصل سوم

تأثيرات بلاک چین بر سیستم سلامت

۳-۱ دلایل استفاده از بلاک چین در سیستم سلامت

دلیل استفاده از این فناوری، ثبت یک سند از گواهی سلامت و تأییدیه آن‌ها که در آینده کارآمد خواهند بود و به سازمان‌ها اجازه استفاده از آن‌ها در زمان مناسب را می‌دهد. این کار اجازه می‌دهد تا پزشک بتواند اطلاعات خود مانند سند پزشکی، مدرک به پایان رساندن دوره کارآموزی و سایر اطلاعات را در بلاک چین به ثبت برساند.

۳-۱-۱ قابلیت همکاری^۶ [۴]

این قابلیت بر تکنولوژی اطلاعات همگن اشاره دارد مانند ثبت اسناد الکترونیک سلامت که به اشتراک و یا از داده‌های اشتراکی استفاده می‌کنند. اجازه به سیستم‌های اطلاعاتی برای کار با یکدیگر در محدوده سازمانی مشخص یک عنصر تأثیرگذار در ارتقای کیفیت تحویل اطلاعات به یک جامعه و یا یک فرد، است. با در نظر گرفتن مهم بودن اشتراک گذاری اطلاعات، جامعه سلامت حال حاضر نیاز به بیمار دارد تا بتواند اسنادی را به اشتراک و یا ثبت برساند. این عمل به دو طریق فیزیکی (نسخه کاغذی) و یا نسخه دیسک سخت^۷ به انجام می‌رسد که در حال حاضر بسیار تأثیرگذار نیست. دلایل آن را در زیر مشاهده می‌کنیم:

- **کند است:** چرا که نسخه فیزیک نیاز به آماده شدن، تحویل و دریافت توسط بیمار است. بنا بر قانون ارائه دهنده تا ۳۰ روز فرصت ارائه نسخه فیزیکی را دارد.
 - **ناامن است:** ممکن است در هنگام انتقال به بیمار گم و یا دزدیده شوند.
 - **ناکامل است:** چرا که ممکن است سوابق بیماری شخص در سیستم‌های مختلف توزیع شده باشد و هیچ منبع واحدی برای ثبت تمامی سوابق وجود نداشته باشد. در این صورت فرد بیمار در قبال نگهداری اطلاعات خود مسئولیت دارد.
 - **کمبود محتوا:** چرا که در حال حاضر این سیستم ارائه دهنده - محور^۸ است. به همین دلیل به بیمار اجازه کنترل سوابق بیماری خود و مشاهده سابقه دسترسی به آن را نمی‌دهد.
- قابلیت همکاری به سه مرحله مشاهده شده در جدول زیر تقسیم می‌شود:
- جدول ۱ سه مرحله قابلیت همکاری

تعریف	مرحله همکاری
اشتراک داده‌ها فعال است؛ ترجمه داده‌ها نیاز نیست	پایه‌ای
فرمت‌هایی برای داده‌های اشتراکی تعریف می‌کند	ساختاری
نیاز به ترجمه اطلاعات دارد	معنایی

^۶ Interoperability

^۷ Hard disk copies

^۸ Provider-centric

۱. **پایه‌ای:** اشتراک داده را فعال می‌کند. نیاز به این که خدمت دهنده اطلاعات را دریافت کند ندارد (برای

ترجمه)

۲. **ساختاری:** فرمت‌هایی را برای داده‌های پزشکی تعریف می‌کند و اطمینان حاصل می‌کند که این داده‌ها

در مرحله مرکز داده توانایی ترجمه را با استفاده از فرمت‌های تعریف شده داشته باشند.

۳. **معنایی:** اطلاعات را نه تنها به دلیل نحو، بلکه معنایی نیز ترجمه می‌کند.

این سه مرحله تضمین امنیت داده‌ها همراه با کیفیت به همراه دارند.

مرحله پایه‌ای و ساختاری یک پیش‌نیاز برای مرحله معنایی به حساب می‌آیند. نیاز به ذکر است که مرحله معنایی

سخت‌ترین مرحله برای انجام است اما دارای کیفیت بالایی است. مرحله معنایی نیاز به دانش کلینیکی و پزشکی

است تا بتوان به خوبی آن را به انجام رساند که بیش از این در این مقاله به آن نمی‌پردازیم.

۳-۱-۲ سیستم بیمار محور^۹ [۴]

در این مدل بیمار به روند اشتراک اطلاعات دسترسی دارد و در تصمیمات مربوط به این اسناد کلینیکی توانایی

شراکت دارند. بیماران می‌توانند گزارش‌های سلامتی خود (مانند فشارخون، ضربان قلب و ...) را از تلفن همراه وارد

سابقه بیماری خود کنند.

در این حالت به‌طور کلی سیستم‌های سلامت یادآورهایی را برای بیماران می‌فرستند، تا بیماران بتوانند گزارش‌های

بیماری خود را به‌صورت لحظه‌ای چک کنند. در انتها در این سیستم بسیار مهم است که بیماران بتوانند بر روی

سوابق سلامتی خود، کنترل داشته باشند و مشخص کنند چه کسی به آن‌ها دسترسی داشته باشد.

قابلیت همکاری نیز در راستای سیستم بیمار - محور نیز نقش مهمی را ایفا می‌کند. در عمل محدودیت‌هایی در

سیستم‌های سلامت وجود دارد که مانع همکاری و در نتیجه ایجاد سیستم بیمار - محور می‌شود.

این محدودیت‌ها در زیر مشخص شده‌اند:

• **دلایل امنیتی برای اشتراک‌گذاری اطلاعات:** باید در نظر داشت که با نداشتن یک سیستم امنیتی

قوی احتمال به خطر افتادن اطلاعات کاربر وجود دارد. همچنین ارائه‌دهنده این سیستم‌ها ممکن است با

به خطر افتادن داده‌ها بهای بزرگی را بپردازند.

⁹ Patient-center care

- **نبود اعتماد میان کارگزاران:** معمولاً کارگزارانی که از یک سیستم سلامت استفاده می کنند به یکدیگر اعتماد موردنظر را دارند. اما در زمانی که این سیستم یکی نیست ممکن است اعتماد سخت تر میان گروه ها ایجاد شود.
- **کمبود حافظه:** اسناد پزشکی معمولاً حجم بالایی دارند. چرا که ممکن است شامل عکس های سنگین و یا دیگر اطلاعات پرحجم باشند (در بیماران سرطانی و یا بیماران با مریضی های غیرقابل درمان شامل این گزینه می شوند). این داده های پرحجم با تکنولوژی حال حاضر به سختی می توانند ارسال شوند.

۳-۲ استفاده های بلاک چین در سیستم سلامت [۴]

در این بخش به استفاده های بلاک چین در سیستم سلامت می پردازیم.

جدول ۲ خلاصه کاربرد های استفاده بلاک چین در سیستم سلامت

بخش	خلاصه
۳-۲-۱	شناسایی نسخه تجویز شده در صورت داشتن داروی مسکن برای تشخیص احتمال تشنج
۳-۲-۲	استفاده از داده ها برای به کار بردن پزشکی در پزشکی از راه دور
۳-۲-۳	به اشتراک گذاشتن داده های سرطانی با اجازه بیمار
۳-۲-۴	ثبت داده های سرطانی برای مطالعات در این بخش
۳-۲-۵	احراز هویت دیجیتال بیمار برای تطبیق بهتر اطلاعات
۳-۲-۶	سوابق بیماری شخصی برای مشاهده و کنترل سوابق کامل بیمار
۳-۲-۷	داوری خودکار برای حق بیمه در صورت رخ دادن خطا و اشتباه

۳-۲-۱ شناسایی داروی مسکن برای تشخیص احتمال تشنج^{۱۰} [۴]

همان طور که می دانید در حال حاضر در آمریکا یک اپیدمی شامل داروی مسکن به وجود آمده است. به همین دلیل استفاده از بلاک چین برای قابلیت غیر مرکزی بودن آن و دقیق بودن آن در اینجا امر مهمی به حساب می آید.

دنیای پزشکی در حال حاضر به راحتی مسکن را برای هر دردی تجویز می کند. در همین صورت داروخانه ها نیز مسکن های بیشتری را تولید کرده چرا که هر چه بیشتر فروش داشته باشند، به سهام داران داروخانه سود بیشتری می رسد. در بعد از عمل های جراحی اکثر مواقع برای مقابله با درد حاصل از عمل جراحی افراد ناامید شده و به مسکن ها رو می آورند. در همین راستا استفاده از تکنولوژی های موجود می تواند وضع حاصل را بهبود بخشد. این تکنولوژی می تواند یک شبکه قابل اعتماد برای داروخانه ها و بیمارستان ها ایجاد کند که هر گونه تجویز نسخه مسکن در آن ثبت شود.

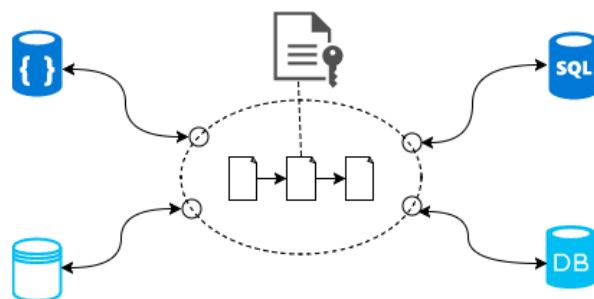
¹⁰Opioid Overdose and Over-Prescription

با توزیع خبر این که یک مسکن تجویز شده به جای تعریف جز به جز اطلاعات تجویز می توان مشکلات مختلفی را در سیستم حال حاضر حل کرد به طور مثال با در نظر گرفتن سوابق تجویز مسکن برای یک بیمار می توان از وقوع حادثه های ناگوار جلوگیری کرد.

۳-۲-۲ استفاده از داده ها برای به کار بردن پزشکی در پزشکی از راه دور^{۱۱} [۴]

به طور کلی پزشکی از راه دور به افرادی که در مناطق دورافتاده و یا دارای امکانات پزشکی کم هستند، خدمات پزشکی خوبی را ارائه می داد. امروزه در میان بیمارانی که نمی خواهند وقت خود را در مطب های دکتر بگذرانند تا مشکلات کوچک اما اورژانسی را درمان کنند، این عمل معروف شده است. با پیشرفت علم و دسترسی های بیشتر به تلفن های همراه، شرکت های زیادی خدمات ۲۴/۷ را برای دسترسی به موارد پزشکی ارائه می دهند؛ همچنین برنامه های بسیاری برای کنترل سوابق بیماری و گزارش های آن ها نیز ایجاد شده است.

خدمات پزشکی از راه دور معمولاً خدمات بیشتری را نسبت به پزشکی سنتی ارائه می دهند. اطلاعات پزشکی که در این راستای انجام این عمل ایجاد می شود توسط کارگزار اصلی که خدمات پزشکی را ارائه داده است غیرقابل دسترسی باشد. برای از بین بردن نیاز به یک عامل سوم^{۱۲} و ایجاد رابطه مستقیم میان افراد در کار، بلاک چین مانند یک پل عمل می کند (نیاز به گفتن است این عمل به تنهایی با استفاده از بلاک چین انجام نمی شود و نیاز به دیگر استانداردهای پزشکی دارد). شکل زیر استفاده از بلاک چین برای پل ارتباطی میان سیستم های سلامت را به خوبی نشان می دهد



شکل ۶ پل ارتباطی بلاک چین میان سیستم ها و تاریخ انتقالات

هر بانک اطلاعاتی مشخص شده در شکل بالا یک منبع اطلاعاتی جدید ایجاد می کند (دایره های سفید). یک قرارداد هوشمند (فایل به همراه کلید) برای کنترل انتقال اطلاعات میان این سیستم ها و همچنین برای ساخت یک فایل از انتقالات گذشته (غیرقابل تغییر)، ایجاد می شود.

۳-۲-۳ به اشتراک گذاشتن داده های سرطانی با اجازه بیمار^{۱۳} [۴]

در زمان درمان سرطان به دلیل حساسیت و نوع های مختلف غده و یا تومور نکات خاصی لحاظ می شود.

¹¹Telemedicine with the use of traditional care

¹² Third party

¹³Patient-Controlled cancer data sharing center

امروزه در آمریکا یک تخته به نام تخته غدد^{۱۴} داریم که متخصصان، پزشکان، جراحان و دیگر افراد مطالعات غددی بیماران را انجام می‌دهند. در مراکز بزرگ این کار بدون هیچ مشکلی انجام می‌شود اما در مراکز کوچک‌تر منابع محدودتر است به همین دلیل حوزه تحقیقاتی در رابطه با تخته غدد محدودتر می‌شود.

در واقعیت بیماران نظر بر این دارند که چند متخصص بر روی سوابق پزشکی ایشان تحقیق کند تا نظر دقیق‌تری را ارائه دهند. در حال حاضر برای به اشتراک‌گذاری اطلاعات بیماران باید نسخه کپی از اطلاعات خود که ممکن است شامل اطلاعات خانوادگی، اطلاعات مراجعه به مرکز سلامت، تجویز نسخه و یا درمان مورد نیاز باشد، تهیه کنند. در این زمان کمبود یک مرکز بیمار - محور که بتواند نظرات متعددی را برای شرایط بیمار ارائه دهد، حس می‌شود.

۳-۲-۴ ثبت داده‌های سرطانی^{۱۵} [۴]

ثبت داده‌های سرطانی امری مهم است چرا که یک درمان برای همه به کار نمی‌رود. سیستم‌های ثبت نامی وابسته به جمعیت (PBCR) رخ داده‌های سرطانی سراسر نقاط را ثبت می‌کنند تا بتوانند برنامه‌ای برای جلوگیری همگانی سرطان از سر بگیرند. سرطان امری حساس است که می‌تواند به بلاک‌چین مربوط شود. باگذشت زمان و دریافت نمونه‌های بیشتر می‌توان با کمک هوش مصنوعی مدل‌های پیش‌بینی‌شده‌ای برای این واقعه ساخت. در نتیجه می‌توان یک سیستم مناسب با کمک بلاک‌چین برای درک بهتر این موضع ساخت که به کمک آن بتوان مدل‌های ایجاد شده را به اشتراک گذاشت.

۳-۲-۵ هویت دیجیتال کاربر^{۱۶}

یک عنصر مهم در اشتراک‌گذاری اطلاعات، احراز هویت فرد است که با کمک سامانه‌های دیجیتال انجام می‌شود. سیستم‌هایی مانند نمایه ارباب - بیمار (mpi) برای این کار ایجاد شده‌اند. با این که عمل‌های مربوط به هویت دیجیتال همچنان در حال پیشرفت هستند، احراز هویت دیجیتال همچنان کاری مشکل است. احراز هویت اشتباه به دسترسی به اطلاعات اشتباه و یا افزونی اطلاعات ختم می‌شود.

به طور تقریب سالانه ۱۹۵ هزار مرگ ناشی از خطای پزشکی اتفاق می‌افتد که بین ۱۰ تا ۱۷ درصد از آن مربوط به خطای "بیمار اشتباهی" مربوط می‌شود که ناشی از هویت دیجیتال است.

با در دسترس نبودن یک استاندارد هویت دیجیتال حتی هویت یک بیمار نیز می‌تواند در بسیاری از زمان‌ها متفاوت باشد. به طور مثال، اطلاعاتی مانند نام، محل تولد، تاریخ تولد و کد ملی برای ثبت بیمار استفاده می‌شود اما همین نام می‌تواند به فرمت‌های مختلف ثبت شود (مانند نام کاربری، نام خانوادگی و ...). مثال دیگری که می‌توان آورد، نشانی منزل نیز ممکن است عوض شد و یا حتی این اطلاعات دارای اشتباه املائی بوده باشند و نیاز به اصلاح داشته باشند. در نتیجه هرچه اطلاعات بیشتری جمع‌آوری شود فرصت بیشتری برای ایجاد اشتباه ساخته می‌شود.

¹⁴ Tumor board

¹⁵ Cancer registry sharing

¹⁶ Patient digital identity

بدون داشتن یک سیستم مشخص برای احراز هویت دیجیتال می توان ناسازگاری ها و خطاهای متعددی را مشاهده کرد. بلاک چین از آدرس های کریپتو گرافی شده امن برای احراز هویت استفاده می کند. هر آدرس دارای یک کلید خاص است که می تواند صاحب هر آدرس را بدون رویت اطلاعات فردی مشخص کند. ویژگی غیر کانونی و خودکار بلاک چین به ایجاد یک نمایه احراز هویت کاربر سرتاسر مرکز سلامت در داخل و یا حتی خارج کشور کمک کند. * در صورت ازدست دادن کلید، آدرس های جدیدی ایجاد می شود.

۳-۲-۶ اسناد پزشکی شخصی^{۱۷} [۴]

هدف این بخش این است که به بیمار کمک کند تا اطلاعات خود را به صورت امن جمع آوری، پیدا و یا کنترل کند سند پزشکی شخصی (p hr) برنامه ای است که به بیمار این اجازه را می دهد. کمپانی هایی مانند اپل و یا مایکروسافت راه حل های مرکز محوری را مانند برنامه سلامت اپل^{۱۸} و یا مخزن سلامت مایکروسافت^{۱۹} را ارائه داده اند. اما راه حل های مرکز محور مشکل اشتراک گذاری اطلاعات را حل نمی کنند. بلاک چین از سوی دیگر، اجازه توزیع اطلاعات و کنترل فردی را در یک سیستم غیر مرکز محور می دهد. با ایجاد یک برنامه متصل به سیستم سلامت، بیماران می توانند تاریخچه پزشکی خود را بدون نیاز به کپی مشاهده کنند. همچنین بلاک چین بی اعتمادی میان بیمار، مرکز سلامت و فرد سوم را از بین می برد چرا که به کمک تلفن های همراه هوشمند این عمل را انجام می دهد.

۳-۲-۷ داوری حق بیمه^{۲۰} [۴]

بیمه ها برای جبران خسارت های ناشی از اتفاق های ناگوار، هزینه های درمانی و جراحی به وجود آمده اند. بیماران بخش کوچکی از هزینه ها را پرداخت کرده و باقی هزینه ها را بیمه پرداخت می کند؛ به این صورت که خدمت ارائه دهنده ها توسط کمپانی ها به کمک "داوری حق بیمه" که وظایف شرکت بیمه و مقدار هزینه ای را که می پردازد شرح می دهد.

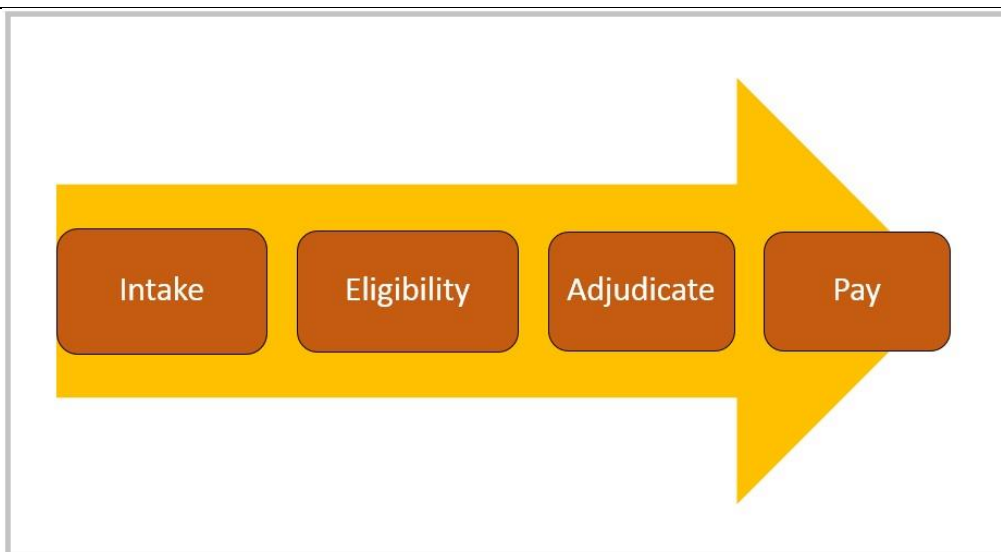
در حال حاضر ۲۲ درصد حق بیمه ها به دلیل این که توسط بیمه دریافت نشده و یا کامل نیستند (شامل اطلاعات اشتباه و یا عدم سند پرداخت). خوشبختانه در حال حاضر قراردادهای هوشمند به کمک خودکارسازی مراحل داوری آمده و با توزیع اطلاعات و در نتیجه شفاف سازی اطلاعات و اسناد برای شرکت بیمه، کمک می کنند. همچنین خطاها را در زمان کمتر شناسایی می کنند. مزیت آخر به روز نگه داشتن افراد داخل شبکه است.

¹⁷Personal health records

¹⁸ Apple health

¹⁹ Health vault

²⁰Personal health records



شکل ۷ حق داور خودکار

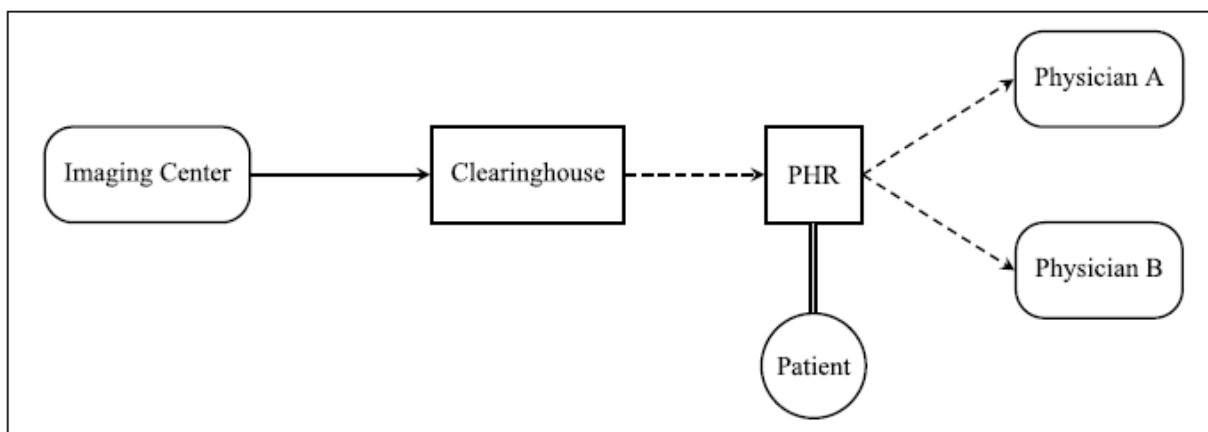
فصل چهارم

چارچوب‌های پیاده‌سازی شده به کمک بلاک چین

از بلاک چین در چارچوب^{۲۱}های مختلفی برای بهبود سیستم سلامت استفاده می‌شود که هر کدام بخشی از کار را آسان تر می‌کنند.

۴-۱ چارچوبی برای اشتراک گذاری امن داده‌های تصویری - پزشکی^[۳]

مطالعات تصویری در حال حاضر یکی از مهم‌ترین حوزه‌های مطالعه برای تصمیمات پزشکی است. اما در حال حاضر روش به کار برده برای انتقال داده‌های تصویری، روشی ناکامل و در بعضی اوقات نادرست است.



شکل ۸-۱ مراحل پردازش تصویری داده‌های پزشکی

۴-۱-۱ معماری ساختمان داده

از بلاک چین برای سه دلیل استفاده می‌کنیم:

۱. ذخیره‌سازی مطالعات تصویری و بیماری که این اطلاعات به آن تعلق دارد.
۲. موجودیت‌هایی که بیمار اجازه دسترسی مطالعات را به آن‌ها داده است.
۳. نقطه نهایی که مطالعات بازیابی می‌شوند.

در بخش‌های قبل در مورد ساختمان بلوک توضیح دادیم؛ بخش دیگری با نام داده‌های بلوکی^{۲۲} داریم. داده‌های بلوکی نوع اطلاعاتی که بلاک چین در خود ذخیره می‌کند را مشخص می‌کنند.

تصویرسازی بلاک چین توسط روش زیر به اشتراک گذاشته می‌شود:

به‌طور کلی ما انتقال ابر داده‌ها را از بین برده، بیمار p که برای آزمایش رادیوگرافیکی x به بیمارستان H رفته است و بعداً درخواست دارد تا این عکس‌ها را با پزشک D بالینی خود به اشتراک بگذارد. مراحل فرآیند را به کمک

²¹ framework

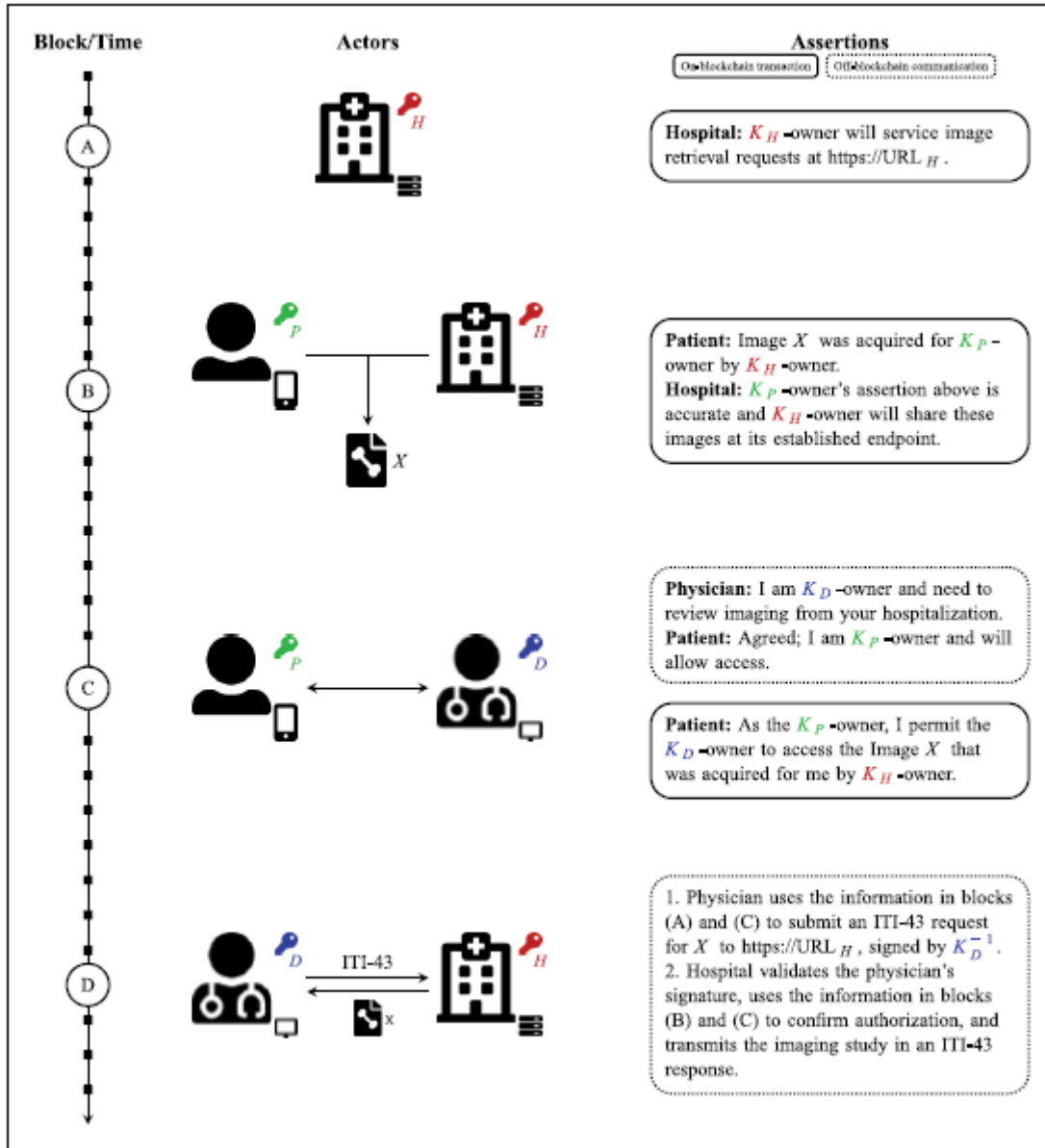
²² Block data

نماد های قرارداد های امنیتی مانند K_α و k_α^{-1} که نشانه کلید عمومی و خصوصی برای عملگر α هستند و همچنین پیام $\{\mu\}_{K_\alpha^{-1}}$ زیر نظر کلید خصوصی ایجاد می شود.

۱. تعریف منبع: این معامله^{۲۳} منبع داده های تصویری را با کمک یک کلید عمومی به یک آدرس (url) وصل می کند. در مثال ما بیمارستان یک معامله با به کمک کلید عمومی خود با مقصد نهایی این آدرس که برای نقل داده های تصویری به موجودیت های مجاز، ثبت می کند (فقط یکبار انجام می شود). این معامله دوتایی $\{k, URL_H\}_{K_H^{-1}}$ را ایجاد میکند.

۲. معامله بعدی یک منبع به عنوان سازنده و یک بیمار به عنوان مطالعات رادیوگرافیکی شده با هویت یکتای UID ایجاد می کند. دوتایی ذخیره زده در بلاک چین $\{K_H, \{K_P, K_H, Hash(UID_X)\}_{K_P^{-1}}\}_{K_H^{-1}}$ است.

²³ Transaction



شکل ۹ مراحل پردازش تصویر بلکچین

۳. اجازه دسترسی: از سوی نقطه نهایی مرکز رادیولوژی به سمت دیگر (بیمار و یا دکتر) اجازه دسترسی به اطلاعات داده می شود. بیمار P به پزشک D اجازه دسترسی می دهد. ماهیت رابطه

این معامله را بیمار بعد از تأیید حضوری با پزشک خود، ارسال می کند. به این صورت پزشک می تواند داده درست تصویری بیمار را با اعتماد بیمار دریافت کند.

هیچ تصویری در بلاک چین ذخیره نشده بلکه زنجیره معاملات فهرستی از دارندگان کلید دارد که بتواند دسترسی داشته باشد. انتقال تصویر نیاز به ارسال درخواست به نقطه نهایی آدرس که این مطالعات تصویری را ایجاد کرده، دارد.

۴-۲ استفاده از دانش اینترنت نسل پنجم برای ارتباط میان بلاک چین و سیستم

سلامت [۱]

از الگوریتم رمزنگاری منحنی بیضوی^{۲۴} که روشی برای کدگذاری داده‌ها با کمک ساخت کلید است، استفاده می‌کنیم.

مراحل این الگوریتم به این صورت است:

به کمک الگوریتم ECC و به کمک مقادیر P & Q امنیت را ایجاد می‌کنیم.

- این دو مقدار دارای کلیدهای A و B هستند.
- P درخواست خود را به Q می‌فرستد.
- Q درخواست را قبول می‌کند.
- مقدار K را حساب می‌کند.

$$K = \frac{Y_B - Y_A}{Z_B - Z_A}$$

- Q مقدار C را از K حساب می‌کند.
- این مقدار را به P می‌فرستد.
- مقدار C از رابطه زیر به دست می‌آید.

$$Z_C = K^2 - Z_A - Z_B$$

$$Y_C = (KZ_A - KY_C) - Y_A$$

- P مقدار C به دست آمده را حساب می‌کند.
- اگر با K برابر بود، اطلاعات را به Q ارسال می‌کند.

²⁴ Elliptic-curve cryptography

```
function Assignkey ()
{
    if patient confirm data over blockchain then
    Generate a key K using ECC
    A<- Get values from ECC_Database
    a sends a Req message with A and B values appended to it

    b computes K from A and B

    b sends a reply with C
    Node a checks the C

    If
    {
        C=A+B
        Return 1
    }
    else
        Do nothing
}
```

شکل ۱۰ تابع/ایجاد کلید

استفاده از این الگوریتم برای امن سازی داده ها در تکنولوژی بلاک چین در شبکه های نسلم پنجم به کمک الگوریتم رمزنگاری منحنی - بیضوی، به کار می رود. این روش در مقایسه با روش های دیگر مانند الگوریتم ریوست، شمیر و ادلمن^{۲۵} و یا الگوریتم دیفی هلمن امن تر است.

²⁵ Rivest, Shamir, Adleman

فصل پنجم

نتیجه گیری

همان‌طور که در فصل‌های قبل اشاره کردیم باگذشت زمان، دیگر روش‌های پیش‌تر جوابگوی نیازهای ما از جمله نیازهای بهداشتی و سلامتی نیست و نیازمند روش‌های جدیدتر هستیم.

در گذشته این روش‌ها به‌صورت مرکزی بود و به‌اصطلاح قدرت در دست چند سهام‌دار و یا چند مقام بالای بیمارستانی بود. اما باگذشت زمان مردم به این‌گونه روش‌ها مخالفت ورزیدند و خواستار تغییر روش به‌طوری‌که علاوه بر سهام‌داران، مردم عادی از جمله خود بیمار بتواند بر اطلاعات و انتقالات نظارت داشته باشد.

الگوریتم بلاک‌چین با قابلیت غیرمرکزی خود روش جدیدی برای نظارت همگانی روی این داده‌ها ارائه داد که باعث می‌شود داده‌ها به‌صورت توزیعی در بلاک‌ها پخش باشند و بیماران و مردم عادی به آن‌ها دسترسی داشته باشند.

بلاک‌چین بر روی بسیاری از موارد سلامت و بهداشت تأثیر گذاشته که می‌توان به مواردی مانند داوری حق بیمه، نظارت بر تجویز مسکن، ثبت داده‌های سرطانی و احراز هویت دیجیتال برای بیماران اشاره کرد.

و در آخر با تمام اطلاعاتی که از فصل‌های پیش‌تر جمع‌آوری کردیم می‌توانیم انواع چارچوب‌های وابسته به بلاک‌چین و یا حتی دخالت هوش مصنوعی را برای راحتی کار در حوزه سلامت ایجاد کنیم. دلیل استفاده از بلاک‌چین در این‌گونه سیستم‌ها به دلیل استفاده راحت‌تر از کلیدهای عمومی و خصوصی است و می‌توان یک نمونه اطلاعات را توسط بیمار، پزشک موردنظر و بیمارستان تأیید کرد.

حال می‌توان این چارچوب را به کمک شبکه اینترنت نسل پنجم فراتر از حد معمول برد و با کدگذاری‌های بهتر امنیت بیشتری را حاصل کرد.

منابع

- [1] suji, H., 2021. Blockchain Based Smart Healthcare Systems in 5G Networks For Preventing Data Forgery. Elsevier, 1(1), pp.2-10.
- [2] Vishal, P., Ronald, R., 2019. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics Journal, 25(4), pp.3-7.
- [3] 101 blockchains, 2021. Top 12 Smart Contract Use Cases. [online] Available at : <https://101blockchains.com/smart-contract-use-cases> [Accessed 28 April 2022].
- [4] Peng, Z., Douglas, C., Jules. W., 2018. Blockchain Technology Use Cases in Healthcare. Elsevier, pp.1-10.
- [5] Emeka, C., Lalit, G., 2020. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. IEEE, pp.1-3.
- [6] Jillian, O., Luke, S., 2019. Opportunities and Challenges of Blockchain Technologies in Health Care. OECD.
- [7] Kanika, G., 2018. Blockchain in Healthcare Frameworks. IJERCSE, 5(4), pp.3-20.
- [8] Jabarulla, M.Y.; Lee, H.-N. A Blockchain and Artificial Intelligence-Based, Patient-Centric Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications. Healthcare 2021, 9, 10 <https://doi.org/10.3390/healthcare9081019>
- [9] Opportunities and Challenges of Blockchain Technologies in Health Care(2020), Paris: OECD
- [10] Priti, T., Sandeep, T., Tanima, B., 2021. Blockchain and artificial intelligence technology in e-Health. Environmental Science and Pollution Research, pp.1-2.