دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

تکلیف چهارم: تهیه ساختار و نگارش گزارش

سپهر مقیسه

شماره دانشجویی:۹۸۳۱۱۰۳

زمستان ۱۴۰۰

فصل دوم

مقدماتی بر بلاک‌چین

۲-۱ توضیحات کلی بلاک‌چین

تکنولوژی بلاک‌چین 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. بلاک‌چین 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 اضافه‌شدن بلاک، بلاک‌چین به سه بخش تقسیم می‌شود:

۱. بخش private
۲. بخش public
۳. بخش permissioned

از فواید بلاک‌چین می‌توان به حافظه بیشتر، امنیت، غیرقابل‌نفوذ بودن، سرعت در پردازش و سیستم غیر کانونی اشاره کرد.

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

این تکنولوژی بر نظام یکپارچگی اما امنیت اشاره دارد. از بلاک‌چین در تکنولوژی‌هایی همانند ارز دیجیتال و برنامه‌های غیر کانونی[1] استفاده می‌شود.

قراردادهای هوشمند وابسته به بلاک‌چین 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 بلاک‌چین قابلیت برطرف ناسازگاری همکاری ایجاد شده در سیستم سلامت را برطرف کند و استاندارد موردنیاز برای برقراری ارتباطی امن میان ارائه‌دهندگان سیستم سلامت، موجودیت‌های سلامتی، و محققین سلامت و دارویی، باشد.

[1] Decentralized-app

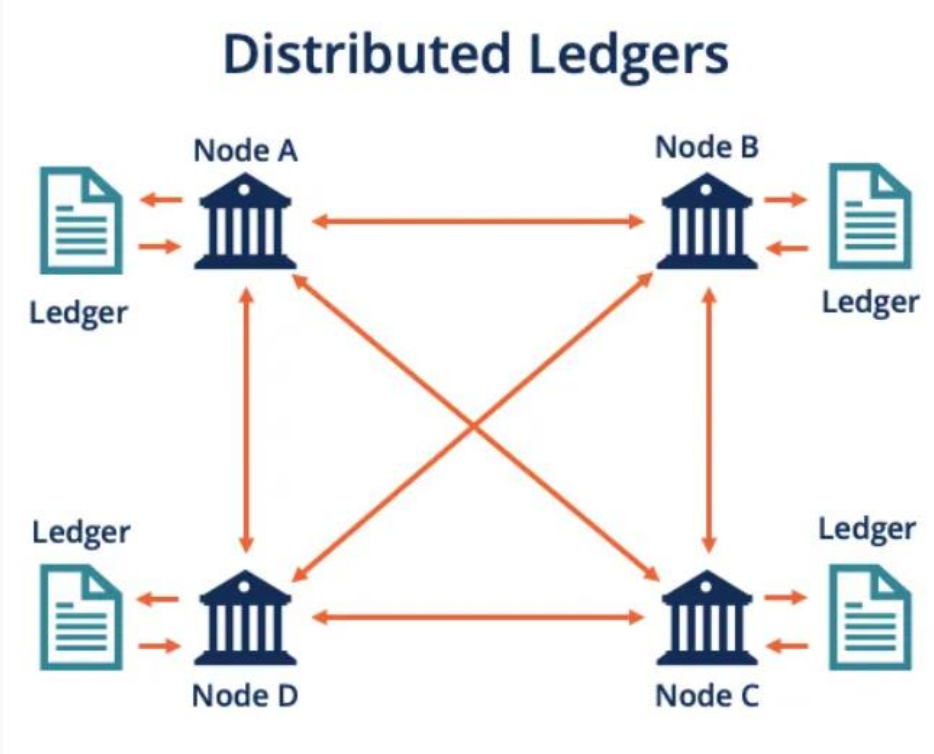
۲-۲ انواع مفهوم‌های مورداستفاده در بلاک‌چین

الگوریتم سکویی[۲]:

در این الگوریتم هر دیتابیس در شبکه نظیر به نظیر به اشتراک گذاشته می‌شوند

در بلاک‌چین دیتابیس برای تمامی مخاطبین شبکه به اشتراک گذاشته می‌شود. هیچ بیگانهٔ 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 بیت‌کوین به اشتراک گذاشته شود.

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



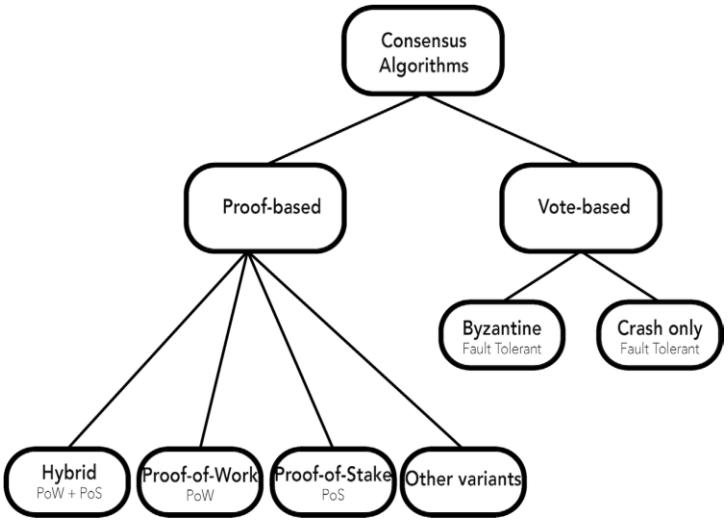
شکل ۱الگوریتم سکویی

[2] distributed ledger

الگوریتم توافق عام[3]:

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

شکل ۲الگوریتم توافق عام



شکل ۳نسخه های مختلف الگوریتم توافق غام

قرارداد هوشمند (smart contract):

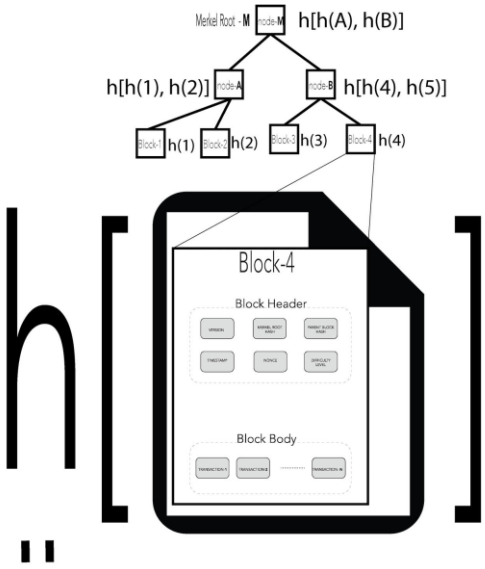
[3] Consensus algorithms

ابزار برنامه‌نویسی شده‌ای که بر روی بلاک‌چین اجرا می‌شود.

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

۲-۳ معماری اصلی بلاک‌چین

ساختار کلی بلاک‌چین به‌صورت شکل زیر است:



شکل ۴ معماری بلاک‌چین

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

[4] hash
[5] header

فصل سوم

تأثیرات بلاک‌چین بر سیستم سلامت

۳-۱ دلایل استفاده از بلاک‌چین در سیستم سلامت[۶]

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 بلاک‌چین به ثبت برساند.

۳-۱-۱ قابلیت همکاری[۷]

این قابلیت بر تکنولوژی اطلاعات همگن اشاره دارد مانند ثبت‌اسناد 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 درنظرگرفتن مهم بودن اشتراک‌گذاری 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[۸] 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 آماده‌شدن، تحویل و دریافت توسط بیمار است. بنا بر قانون ارائه‌دهنده 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 ارائه‌دهنده - محور[۹] است. به همین دلیل به بیمار اجازه کنترل سوابق بیماری خود و مشاهده سابقه دسترسی به آن را نمی‌دهد.

[6] Health care system
[7] Interoperability
[8] Hard disk copies
[9] Provider-centric

قابلیت همکاری به سه مرحله مشاهده شده در جدول زیر تقسیم می‌شود:

جدول ۱سه مرحله قابلیت همکاری

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

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 نه‌تنها به دلیل نحو، بلکه معنایی نیز ترجمه می‌کند.

این سه مرحله تضمین امنیت داده‌ها همراه باکیفیت به همراه دارند.
مرحله پایه‌ای و ساختاری یک پیش‌نیاز برای مرحله معنایی به‌حساب 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 به‌خوبی آن را به انجام رساند که بیش از این در این مقاله به آن نمی‌پردازیم.

۳-۱-۲ سیستم بیمار محور[10]

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 به‌طورکلی 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.

[10] Patient-center care

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 افتا داده‌ها بهای بزرگی را بپردازند.
- **نبود اعتماد میان کارگزاران:** معمولاً کارگزارانی که از یک سیستم سلامت استفاده می‌کنند به یکدیگر اعتماد موردنظر را دارند. اما در زمانی که این سیستم یکی نیست ممکن است اعتماد سخت‌تر میان گروه‌ها ایجاد شود.
- **کمبود حافظه:** اسناد پزشکی معمولاً حجم بالایی دارند. چرا که ممکن است شامل عکس‌های سنگین و یا دیگر اطلاعات پرحجم باشند (در بیماران سرطانی و یا بیماران با مریضی‌های غیرقابل‌درمان شامل این گزینه می‌شوند). این داده‌های پرحجم با تکنولوژی حال حاضر به‌سختی می‌توانند ارسال شوند.

۳-۲ استفاده‌های بلاک‌چین در سیستم سلامت

در این بخش به استفاده‌های بلاک‌چین در سیستم سلامت می‌پردازیم.

جدول ۲ خلاصه کاربرد های استفاده بلاک‌چین 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 داده‌ها برای به‌کاربردن پزشکی در پزشکی از راه دور
۳-۲-۳	به اشتراک گذاشتن داده‌های سرطانی با اجازه بیمار
۳-۲-۴	ثبت داده‌های 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 رخ‌دادن خطا و اشتباه

۳-۱-۱ شناسایی داروی مسکن برای تشخیص احتمال تشنج[11]

همان‌طور که می‌دانید در حال حاضر در آمریکا یک اپیدمی شامل داروی مسکن به وجود آمده است. به همین دلیل استفاده از بلاک‌چین برای قابلیت غیر مرکزی بودن آن و دقیق بودن آن در اینجا امر مهمی به‌حساب می‌آید.

دنیای پزشکی در حال حاضر به‌راحتی مسکن را برای هر دردی تجویز می‌کند. در همین صورت داروخانه‌ها نیز مسکن‌های بیشتری را تولید کرده چرا که هرچه بیشتر فروش داشته باشند، به سهام‌داران داروخانه سود بیشتری می‌رسد. در بعد از عمل‌های جراحی اکثر مواقع برای مقابله با درد حاصل از عمل جراحی افراد ناامید شده و به مسکن‌ها رو می‌آورند. در همین راستا استفاده از تکنولوژی‌های موجود می‌تواند وضع حاصل را بهبود بخشد. این تکنولوژی می‌تواند یک شبکه قابل‌اعتماد برای داروخانه‌ها و بیمارستان‌ها ایجاد کند که هرگونه تجویز نسخهٔ مسکن در آن ثبت شود.

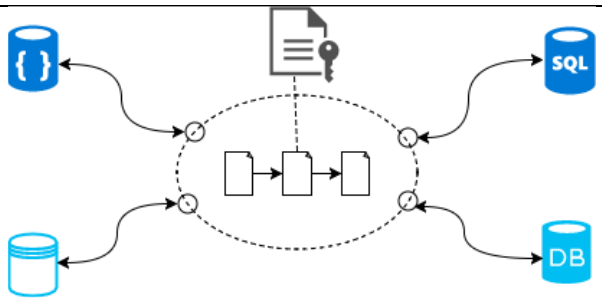
با توزیع خبر این که یک مسکن تجویز شده به‌جای تعریف جز به جز اطلاعت تجویز می‌توان مشکلات مختلفی را در سیستم حال حاضر حل کرد به طور مثال با درنظرگرفتن سوابق تجویز مسکن برای یک بیمار می‌توان از وقوع حادثه‌های ناگوار جلوگیری کرد.

۳-۱-۲ استفاده از داده‌ها برای به‌کاربردن پزشکی در پزشکی از راه دور[12]

به‌طورکلی پزشکی از راه دور به افرادی که در مناطق دورافتاده و یا دارای امکانات پزشکی کم هستند، خدمات پزشکی خوبی را ارائه می‌داد. امروزه در میان بیمارانی که نمی‌خواهند وقت خود را در مطب‌های دکتر بگذراند تا مشکلات کوچک اما اورژانسی را درمان کنند، این عمل معروف شده است. با پیشرفت علم و دسترسی‌های بیشتر به تلفن‌های همراه، شرکت‌های زیادی خدمات ۲۴/۷ را برای دسترسی به موارد پزشکی ارائه می‌دهند؛ همچنین برنامه‌های بسیاری برای کنترل سوابق بیماری و گزارش‌های آن‌ها نیز ایجاد شده است.

خدمات پزشکی از راه دور معمولاً خدمات بیشتری را نسبت به پزشکی سنتی ارائه می‌دهند. اطلاعات پزشکی که در این راستای انجام این عمل ایجاد می‌شود توسط کارگزار اصلی که خدمات پزشکی را ارائه داده است غیرقابل‌دسترسی باشد. برای ازبین‌بردن نیاز به یک عامل سوم[13] و ایجاد رابطه مستقیم میان افراد در کار، بلاک‌چین مانند یک پل عمل می‌کند (نیاز به گفتن است این عمل به‌تنهایی با استفاده از بلاک‌چین انجام نمی‌شود و نیاز به دیگر استانداردهای پزشکی دارد). شکل زیر استفاده از بلاک‌چین برای پل ارتباطی میان سیستم‌های سلامت را به‌خوبی نشان می‌دهد

[11] Opioid Overdose and Over-Prescription
[12] Telemedicine with the use of traditional care
[13] Third party



شکل ۵ پل ارتباطی بلاک‌چین میان سیستم ها و تاریخ انتقالات

هر بانک اطلاعاتی مشخص شده در شکل بالا یک منبع اطلاعاتی جدید ایجاد می‌کند (دایره‌های سفید). یک قرارداد هوشمند (فایل به همراه کلید) برای کنترل انتقال اطلاعات میان این سیستم‌ها و همچنین برای ساخت یک فایل از انتقالات گذشته (غیرقابل‌تغییر)، ایجاد می‌شود.

۳-۱-۳ به اشتراک گذاشتن داده‌های سرطانی با اجازه بیمار [۱۴]

در زمان درمان سرطان به دلیل حساسیت و نوع‌های مختلف غده و یا تومور نکات خاصی لحاظ می‌شود. امروزه در آمریکا یک تخته به نام تخته غدد[۱۵] 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 دررابطه‌با 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 به‌اشتراک‌گذاری اطلاعات بیماران باید نسخه کپی از اطلاعات خود که ممکن است شامل اطلاعات خانوادگی، اطلاعات مراجعه به مرکز سلامت، تجویز نسخه و یا درمان موردنیاز باشد، تهیه کنند. در این زمان کمبود یک مرکز بیمار - محور که بتواند نظرات متعددی را برای شرایط بیمار ارائه دهد، حس می‌شود.

۳-۱-۴ ثبت داده‌های سرطانی [۱۶]

ثبت داده‌های سرطانی امری مهم است چرا که یک درمان برای همه به کار نمی‌رود.

سیستم‌های ثبت نامی وابسته به جمعیت (PBCR) رخداده‌های 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

[14] Patient-Controlled cancer data sharing center
[15] Tumor board
[16] Cancer registry sharing

پیش‌بینی‌شده‌ای برای این واقعه ساخت. در نتیجه می‌توان یک سیستم مناسبت با کمک بلاک‌چین برای درک بهتر این موضع ساخت که به کمک آن بتوان مدل‌های ایجاد شده را به اشتراک گذاشت.

۳-۱-۵ هویت دیجیتال کاربر[۱۷]

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 اطلاعت دارای اشتباه املایی بوده باشند و نیاز به اصلاح داشته باشند. در نتیجه هرچه اطلاعت بیشتری جمع‌آوری شود فرصت بیشتری برای ایجاد اشتباه ساخته می‌شود.

بدون داشتن یک سیستم مشخص برای احراز هویت دیجیتال می‌توان ناسازگاری‌ها و خطاهای متعددی را مشاهده کرد. بلاک‌چین از آدرس‌های کریپتو گرافی شده امن برای احراز هویت استفاده می‌کند. هر آدرس دارای یک کلید خاص است که می‌تواند صاحب هر آدرس را بدون رویت اطلاعات فردی مشخص کند. ویژگی غیر کانونی و خودکار بلاک‌چین به ایجاد یک نمایه احراز هویت کاربر سرتاسر مرکز سلامت در داخل و یا حتی خارج کشور کمک کند.

* در صورت ازدست‌دادن کلید، آدرس‌های جدیدی ایجاد می‌شود.

۳-۱-۶ اسناد پزشکی شخصی[۱۸]

هدف این بخش این است که به بیمار کمک کند تا اطلاعت خود را به‌صورت امن جمع‌آوری، پیدا و یا کنترل کند سند پزشکی شخصی (phr) برنامه‌ای است که به بیمار این اجازه را می‌دهد. کمپانی‌هایی مانند اپل و یا مایکروسافت راه‌حل‌های مرکز محوری را مانند برنامه سلامت اپل[۱۹] و یا مخزن سلامت مایکروسافت[۲۰] را ارائه داده‌اند. اما راه‌حل‌های مرکز محور مشکل اشتراک‌گذاری اطلاعات را حل نمی‌کنند.

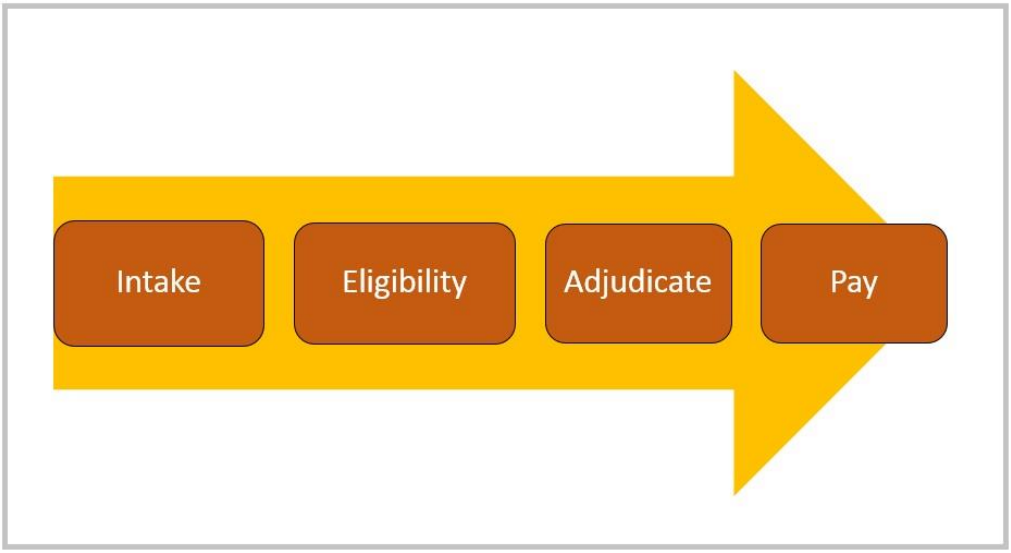
[17] Patient digital identity
[18] Personal health records
[19] Apple health
[20] Health vault

بلاک‌چین از سوی دیگر، اجازه توزیع اطلاعات و کنترل فردی را در یک سیستم غیر مرکز محور می‌دهد. با ایجاد یک برنامه متصل به سیستم سلامت، بیماران می‌توانند تاریخچه پزشکی خود را بدون نیاز به کپی مشاهده کنند. همچنین بلاک‌چین بی‌اعتمادی میان بیمار، مرکز سلامت و فرد سوم را از بین می‌برد چرا که به کمک تلفن‌های همراه هوشمند این عمل را انجام می‌دهد.

۳-۱-۷ داوری حق بیمه[۲۱]

بیمه‌ها برای جبران خسارت‌های ناشی از اتفاق‌های ناگوار، هزینه‌های درمانی و جراحی به وجود آمده‌اند. بیماران بخش کوچکی از هزینه‌ها را پرداخت کرده و باقی هزینه‌ها را بیمه پرداخت می‌کند؛ به این صورت که خدمت ارائه‌دهنده‌ها توسط کمپانی‌ها به کمک "داوری حق بیمه" که وظایف شرکت بیمه و مقدار هزینه‌ای را که می‌پردازد شرح می‌دهد.

در حال حاضر ۲۲ درصد حق بیمه‌ها 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 شفاف‌سازی اطلاعات و اسناد برای شرکت بیمه، کمک می‌کنند. همچنین خطاها را در زمان کمتر شناسایی می‌کنند. مزیت آخر به‌روز نگه‌داشتن افراد داخل شبکه است.



شکل ۶ حق داوری خودکار

[21] Personal health records

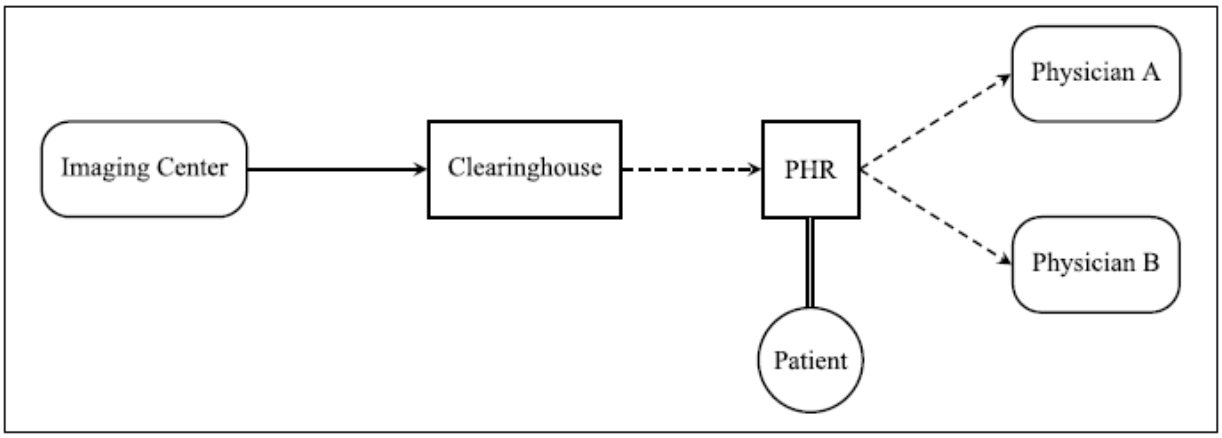
فصل چهارم

چارچوب‌های پیاده‌سازی شده به کمک بلاک‌چین

از بلاک‌چین در چارچوب[22]های مختلفی برای بهبود سیستم سلامت استفاده می‌شود که هرکدام بخشی از کار را آسان‌تر می‌کنند.

۴-۱ چارچوبی برای اشتراک‌گذاری امن داده‌های تصویری - پزشکی

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 ۷مراحل پردازش تصویری داده های پزشکی

۴-۱-۱ معماری ساختمان داده

از بلاک‌چین برای دو 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[23] داریم. داده‌های بلوکی نوع اطلاعاتی که بلاک‌چین در خود ذخیره می‌کند را مشخص می‌کنند.

تصویرسازی بلاک‌چین توسط روش زیر به اشتراک گذاشته می‌شود:

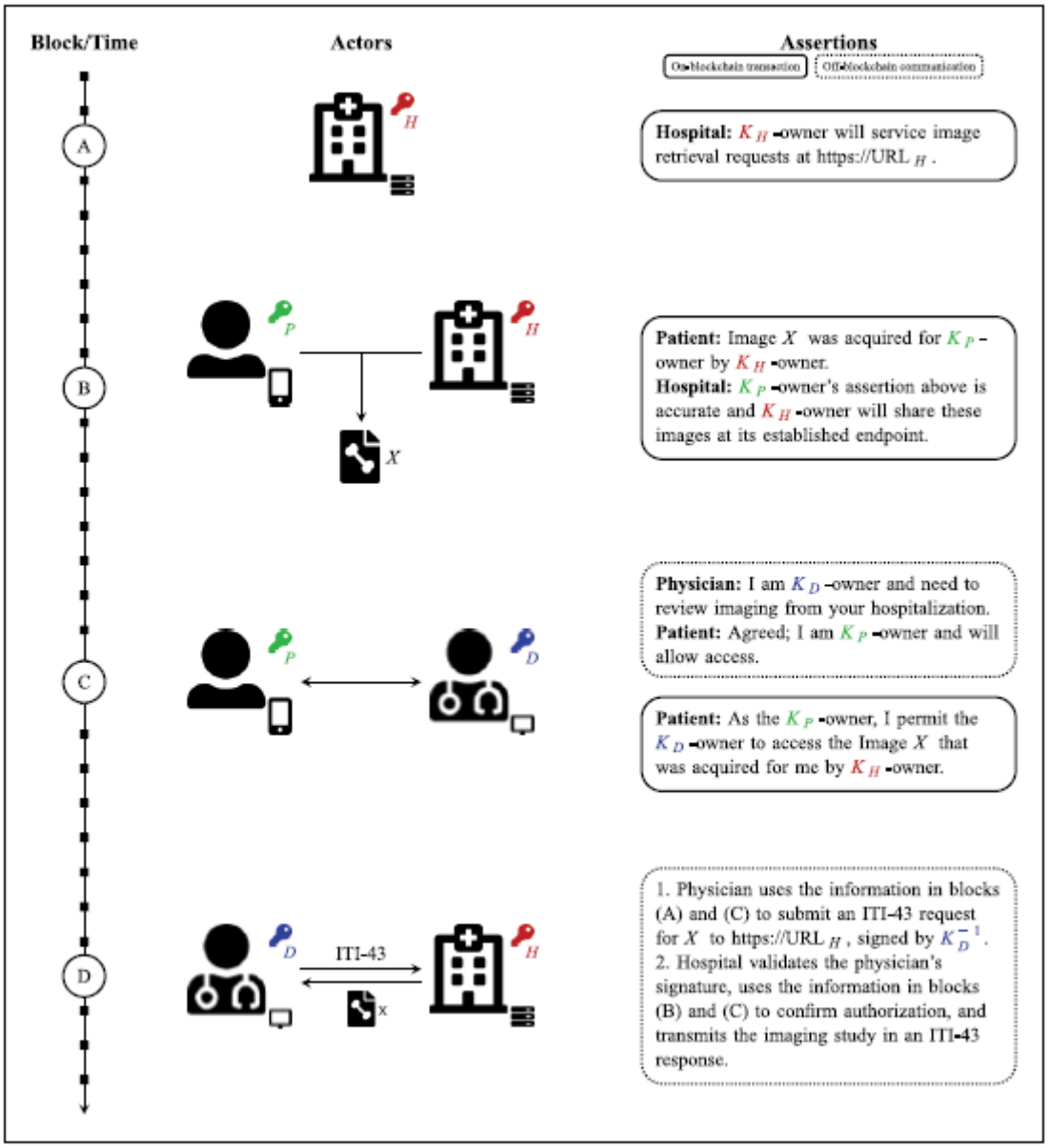
[22] framework
[23] Block data

به‌طورکلی ما انتقال ابر داده‌ها را از بین برده، بیمار pکه برای آزمایش رادیوگرافیکی x به بیمارستان H رفته است و بعدا درخواست دارد تا این عکس ها را با پزشک D بالینی خود به اشتراک بگذارد. مراحل فرآیند را به کمک نماد های قرارداد های امنیتی مانندK_α و k_α^{-1} که نشانه کلید عمومی و خصوصی برای عملگر α هستند و همچنین پیام $\{\mu\}_{\mathrm{k}_\alpha^{-1}}$ زیر نظر کلیدخصوصی ایجاد میشود.

۱. تعریف منبع: این معامله[۲۴] منبع داده‌های تصویری را با کمک یک کلید عمومی به یک آدرس (*url*) وصل می‌کند. در مثال ما بیمارستان یک معامله با به کمک کلید عمومی خود با مقصد نهایی این آدرس که برای نقل داده‌های تصویری به موجودیت‌های مجاز، ثبت می‌کند (فقط یکبار انجام می‌شود). این معامله دوتایی $\{k, URL_H\}_{k_H^{-1}}$ را ایجاد میکند.

۲. معامله بعدی یک منبع به‌عنوان سازنده و یک بیمار به‌عنوان مطالعات رادیوگرافیکی شده باهویت یکتای *UID* ایجاد می‌کند. دوتایی ذخیره زده در بلاک‌چین $\{K_H, \{K_p, K_H, \mathrm{Hash}(\mathrm{UID}_X)\}_{K_P^{-1}}\}_{K_H^{-1}}$ است.

[24] Transaction



شکل ۸مراحلات پردازش تصویری بلاک‌چین

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

$\{K_H, \{K_P, K_H, \text{Hash}(\text{UID}_X)\}_{K_P^{-1}}\}_{K_H^{-1}}$ در یک اجازه دسترسی این رضایت را وارد بلاک‌چین می‌کند. این معامله را بیمار بعد از تأیید حضوری با پزشک خود، ارسال می‌کند. به این صورت پزشک می‌تواند داده درست تصویری بیمار را با اعتماد بیمار دریافت کند.

هیچ تصویری در بلاک‌چین 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.

۲-۴ استفاده از دانش اینترنت نسل پنجم برای ارتباط میان بلاک‌چین و سیستم سلامت

از الگوریتم رمزنگاری منحنی بیضوی[۲۵] 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.

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

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

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

[25] 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

                Retum 1

        else
                Do nothing
        }
}
```

شکل ۹ تابع ایجاد کلید

استفاده از این الگوریتم برای امن‌سازی داده‌ها در تکنولوژی بلاک‌چین در شبکه‌های نسلم پنجم به کمک الگوریتم رمزنگاری منحنی - بیضوی، به کار می‌رود. این روش در مقایسه با روش‌های دیگر مانند الگوریتم ریوست، شمیر و ادلمن[۲۶] و یا الگوریتم دیفی هلمن امن‌تر است.

[26] Rivest, Shamir, Adleman