کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش مهارت های کاربردی در تدوین و چاپ مقاله

اصول تنظیم قراردادها

مقاله نویسی علوم انسانی

JCWR2019
کنفرانس بین المللی پنجمین وب پژوهی
٤ و ٥ اردیبهشت ۱۳۹۸: تهران، ایران

Blockchain Solutions for Implementing Electronic Health Record

[1]Mohammad Javad Shayegan Fard, [1]Masoud Barati, [1]Kiarash Shamsi.

[1]Department of Computer Engineering, University of Science and Culture, Tehran, Iran
shayegan@usc.ac.ir, trbarati@gmail.com, kiarash.shamsi@gmail.com

Abstract

Today, data storage and processing play a major role in all areas, including medical topics. Every day, a great deal of information and health records with a secret nature are produced in a distributed manner so providing consensus, storage, integrity, validity and sharing it among different sources, has many challenges.
On the other hand, block chain technology provides us a place for storage and sharing distributed data, which can guarantee the integrity of the data in an integrated network of member nodes. Due to these features, the use of this technology is currently spreading in a variety of fields, including medicine, to overcome the challenges posed. Because of the block chain technology is new and a little ambiguous today and also the importance of privacy in health data issue, this paper attempts to present a variety of options for setting up the block chain system with an electronic health record approach and describing its dimensions. In the end, based on the study and the policy on how to store and process information, the appropriate block chain option is suggested for implementation.

Keywords: Block chain, Electronic health record, DLTs, Data Privacy.

JCWR2019
کنفرانس بین المللی پنجمین وب پژوهی
٤ و ٥ اردیبهشت ١٣٩٨: تهران، ایران

راهکارهایی به منظور پیاده‌سازی پرونده الکترونیک سلامت با استفاده از بلاک‌چین

محمد جواد شایگان‌فرد، مسعود براتی، کیارش شمسی

گروه مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران، ایران
shayegan@usc.ac.ir, rbarati@gmail.com, kiarash.shamsi@gmail.com

چکیده

امروزه ذخیره و پردازش اطلاعات نقش بزرگی در تمامی زمینه‌ها از جمله مباحث پزشکی دارد. هر روزه مقدار بسیار زیادی اطلاعات و پرونده‌های سلامت با ماهیت محرمانه به صورت پراکنده تولید می‌شوند که اجماع، نگه‌داری، تضمین صحت و عدم تغییر محتوای آن و همچنین اشتراک‌گذاری آن بین منابع مختلف دارای چالش‌های فراوانی است. از سوی دیگر فناوری بلاک‌چین بستری را برای ذخیره‌سازی و اشتراک‌داده‌ها به صورت توزیع‌شده برای ما فراهم می‌کند که در آن می‌توان صحت و تغییرناپذیری داده‌ها را در یک شبکه یکپارچه از گره‌های عضو تضمین کرد. به واسطه همین ویژگی‌ها استفاده از این فناوری امروزه در عرصه‌های گوناگونی از جمله پزشکی برای برطرف کردن چالش‌های مطرح‌شده در حال گسترش است. با توجه به نو بودن موضوع بلاک‌چین و وجود ابهامات زیاد در مورد آن و همینطور خاص بودن بحث داده‌های سلامت، این مقاله سعی دارد انواع گزینه‌های موجود برای راه‌اندازی سیستم بلاک‌چین با رویکرد پرونده الکترونیک سلامت را ارائه کرده و ابعاد آن را تشریح نماید. در پایان براساس مطالعه انجام شده و سیاستی که در نحوه ذخیره‌سازی و پردازش اطلاعات وجود دارد گزینه مناسب بلاک‌چین برای پیاده‌سازی پیشنهاد می‌شود.

کلمات کلیدی

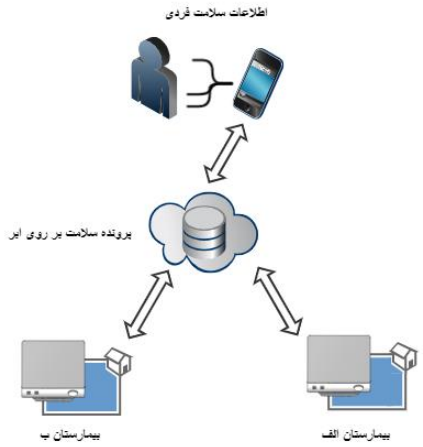
بلاک‌چین، پرونده سلامت، سیستم اطلاعاتی توزیع‌شده، محرمانگی داده

مقدمه

در مبحث سلامت، ذخیره و پردازش اطلاعات نقش بسیار مهمی دارند. برای مثال هنگامی که یک بیمار در بیمارستان تحت معاینات پزشکی قرار می‌گیرد، نتیجه این معاینات اطلاعاتی است که در سیستم سلامت تولید شده، حال این اطلاعات برای تشخیص بیماری او توسط متخصصین مورد استفاده قرار می‌گیرند و پس از آن تحت عنوان سوابق پزشکی ذخیره می‌شوند تا در آینده در همان بیمارستان یا بیمارستان‌های دیگر مورد استفاده قرار گیرند[۱].

ذخیره این سوابق روی کاغذ کاری بسیار سخت و مشکل‌زاست، جابه‌جایی آن‌ها از مرکز پزشکی به مرکزی دیگر دردسرهای خودش را دارد و همچنین امکان گم شدن مدارک در آن‌ها زیاد است. به همین دلایل خیلی سریع پای فناوری به این حوزه باز شد. بسیار واضح است که فناوری می‌تواند راه‌حل‌های بسیاری در حل این مشکلات ارائه دهد که باعث کم شدن هزینه و اتلاف زمان کارمندان شوند. نخستین سیستم‌ها در این حوزه سیستم‌های غیر برخطی بودند که تنها کارایی‌شان تبدیل پرونده‌های کاغذی به الکترونیکی بود. این سیستم‌ها تنها مشکل جاگیر بودن پرونده‌های کاغذی را حل می‌کردند و جابه‌جایی آن‌ها از مرکز پزشکی به مرکزی دیگر را آسان‌تر می‌کردند.

با پیشرفت فناوری در این حوزه مفهوم جدیدی به نام پرونده سلامت شکل گرفت. پرونده سلامت هر فرد عبارت است از مجموع تمام سوابق پزشکی فرد و اطلاعات سلامت فردی که نمونه شماتیک آن را در شکل ۱ مشاهده می‌کنید[۱]. سوابق پزشکی اطلاعاتی هستند که پس از انجام هر معاینه ذخیره



شکل ۱: اکوسیستم پرونده سلامت مبتنی بر ابر، برگرفته از [۱]

می‌شوند و اطلاعات سلامت فردی شامل قد، وزن، مقدار فعالیت در روز و سایر اطلاعاتی است که معمولا توسط سنسورها از فرد جمع‌آوری می‌شوند[۲].

این پرونده‌ها از نظر زمانی کاملا مرتب شده و در نرم‌افزارهای آنلاین و غالبا بر روی ابر نگه‌داری می‌شوند اما باز هم مشکلاتی در مواجهه با آن‌ها وجود دارد[۳]. یکی از این مشکلات تولید داده‌های حجیم برای هر مریض است که کار افزودن داده و فرآیند روی آن را مشکل می‌کند. مشکل دیگر عدم وجود امکان همکاری و اشتراک اطلاعات میان سازمان‌های مختلفی است که به جمع‌آوری پرونده سلامت افراد می‌پردازند، این عدم یکپارچگی میان سازمان‌های جمع‌آوری کننده اطلاعات باعث شده بیشتر این پرونده‌های پزشکی ناقص و در نتیجه تقریبا غیرقابل استفاده شوند. یکی از جدیدترین فن‌آوری‌هایی که در این عرصه وارد شده، فن‌آوری بلاک‌چین یا زنجیره بلوکی است.

امروزه افراد زیادی اسم بلاک‌چین را در حوزه‌ی ارزهای رمزنگاری شده مثل Bitcoin شنیده اند؛ در حالی که، این فناوری قابلیت‌های بسیار وسیع‌تری از توسعه یک سیستم ساده مالی را دارا می‌باشد. از این فناوری به طور کلی در حوزه‌های بسیاری از جمله حوزه‌ی سلامت می‌توان استفاده کرد[۴].

بلاک‌چین یک فناوری برای ساخت پایگاه داده‌های توزیع شده و برخط می‌باشد که از یک ساختار داده‌ای مخصوص به نام بلاک استفاده می‌کنند[۵]؛ مجموعه تمام این بلاک‌ها به صورت توزیع شده و یکسان بین تعداد زیادی از گره‌ها که به آنها دفتر کل (ledger) گفته می‌شود پخش شده و توسط آنها نگهداری می‌گردد. این ویژگی باعث می‌شود تا تمام بلاک‌ها فقط در یک نقطه متمرکز نباشند.

از ویژگی‌های مهم این فناوری می‌توان به عدم از بین رفتن داده‌ها اشاره کرد، همچنین در این سیستم با توجه به وجود گره‌هایی که دفتر کل بوده و حاوی تمام وضعیت شبکه هستند، دستکاری داده‌ها در یک زنجیره نیازمند دستکاری داده در تمام زنجیره‌های موجود در تمام گره‌های دفتر کل است که عملا غیر ممکن است و این ویژگی شبکه باعث می‌شود تا تغییر داده‌های ثبت شده عملا غیر ممکن شود. از آنجایی که این سیستم به یک نوع اعتماد همگانی متکی می‌باشد، کاملا مستقل عمل کرده و نیاز به هیچ شخص و نهاد سومی برای تضمین صحت و سلامت داده‌های موجود در شبکه ندارد[۶].

با توجه به چالش‌های مطرح شده پیرامون ذخیره‌سازی و دسترسی به سوابق پزشکی در بخش‌های قبل و بیان ویژگی‌های کلی شبکه بلاک‌چین می‌توان نتیجه گرفت که این فناوری پتانسیل بلقوه‌ای در استفاده به عنوان بستر سیستم ذخیره‌سازی و استفاده از سوابق پزشکی را خواهد داشت. با توجه به اینکه داده‌های پزشکی داده‌هایی بسیار حساس هستند، دسترسی به این داده‌ها ذاتا به صورت باز و قابل دسترس برای همه امکان‌پذیر نخواهد بود. همچنین تولید این داده‌ها هم مثل شبکه‌های مالی نیست که هر کسی بتواند یک تراکنش بسازد و یا بلاکی را به سیستم اضافه کند، لذا برای شبکه بلاک‌چین سلامت نیازمند مدل‌های خاص و مستقل از مدل شبکه های مالی بلاک‌چین هستیم که هم محاسن این فناوری را برای ما به ارمغان بیاورد و هم چالش‌های موجود را مرتفع سازد.

در این مقاله قصد داریم انواع گزینه های ممکن شبکه بلاک‌چین را با رویکرد نگهداری و پردازش پرونده سلامت مورد مطالعه قرار داده و جوانب مختلف آن را ارزیابی نمائیم.

سیستم پرونده سلامت و بلاک‌چین

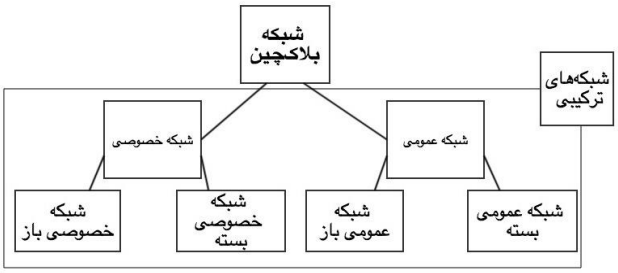
به طور کلی در شبکه های مبتنی بر بلاک‌چین با توجه به نوع دسترسی به شبکه و میزان کنترل اعمال شده روی آن، شبکه به ۲ نوع خصوصی و عمومی تقسیم بندی می‌شود[۷]. در هر کدام از این ۲ مدل، عملکرد و ساختار زنجیره بلوک تفاوتی ندارد، در واقع تفاوت بین آن‌ها در میزان دسترسی به اطلاعات بلوک‌ها و سیاست‌های موجود برای تولید بلوک‌های داده جدید در زنجیره می‌باشد. در مدل اول شبکه برای همه قابل دسترس است و هر کسی می‌تواند وارد شبکه شود به این مدل از شبکه،

مدل شبکه بلاک‌چین عمومی گفته می‌شود[۸]. در مقابل گاهی با توجه به معماری و نیازهای موجود تمایل داریم تا گره‌های موجود در شبکه کاملا در کنترل ما باشند و هر کسی نتواند به این شبکه وارد شده و اطلاعات را مشاهده کند پس برای اضافه کردن گره‌ها به شبکه از یک سیاست گزینش مشخص استفاده کرده و گره‌های خاصی را به شبکه اضافه می‌کنیم. در این مدل اگرچه توسعه شبکه و گسترش آن به هزینه و نظارت بیشتری نیاز دارد اما محدودیت‌های موجود به منظور تامین امنیت داده ها ما را به استفاده از این نوع شبکه ترغیب می‌کند[۸].

یک مدل سیاست گذاری دیگر نیز وجود دارد که بر نحوه‌ی تولید داده، اضافه کردن بلوک به شبکه و فعالیت اعضای شبکه نظارت می‌کند. در واقع در شبکه بلوک چه خصوصی باشد و چه عمومی می‌توان پرسید چه کسی قادر به انجام چه نوع کاری است(؟). اگر پاسخ به این سوال همه و همه‌ی کارهای قابل انجام باشد، شبکه اصطلاحا بدون اجازه (باز) است و اگر پاسخ به این سوال با اعمال یک سری سیاست خاص، هر گره به صورت گزینشی قادر به انجام کارهای مجاز باشد، شبکه اصطلاحا دارای اجازه (بسته) است.

برای اینکه بتوانیم شبکه بلاک‌چین را با رویکرد پرونده سلامت مطالعه کنیم، به این نتیجه رسیدیم که با همین نگاه شبکه خصوصی و عمومی بلاک‌چین بهتر می توان به یک ارزیابی و مقایسه رسید. لذا متدولوژی این مطالعه با این دیدگاه توسعه پیدا کرد. بر این اساس، شکل ۲ استخراج می شود که شبکه بلاک چین به ۴ دسته کلی خصوصی باز (private permission less)، خصوصی بسته (private permissioned)، عمومی بسته (public permissioned) و عمومی باز (public permission less) تقسیم می‌شود.همچنین شبکه ترکیبی می تواند ترکیبی از همه حالت های ممکن با یک معماری جدید باشد.

با توجه به چالش‌های مطرح شده پیرامون ذخیره‌سازی و



شکل۲: شمای کلی انواع شبکه‌های قابل توسعه توسط بلاک‌چین

دسترسی به سوابق پزشکی در بخش‌های قبل و بیان ویژگی‌های کلی شبکه بلاک‌چین می‌توان نتیجه گرفت که این تکنولوژی پتانسیل بلقوه‌ای در استفاده به عنوان بستر سیستم ذخیره‌سازی و استفاده از سوابق پزشکی را خواهد داشت اما استفاده از این فناوری چالش‌های خاص خودش را هم ایجاد می‌کند.

با توجه به اینکه داده‌های پزشکی داده‌هایی بسیار حساس هستند، دسترسی به این داده‌ها ذاتا به صورت باز و قابل دسترس برای همه امکان‌پذیر نخواهد بود. همچنین تولید این داده‌ها هم مثل شبکه‌های مالی نیست که هر کسی بتواند یک تراکنش بسازد و یا بلاکی را به سیستم اضافه کند، لذا برای شبکه بلاک‌چین سلامت نیازمند مدل‌های خاص و مستقل از مدل شبکه‌های مالی بلاک‌چین هستیم که هم محاسن این فناوری را برای ما به ارمغان بیاورد و هم چالش‌های موجود را مرتفع سازد.

با توجه به این توضیحات، به بررسی مدل‌های مختلف پیشنهاد شده در هر نوع از شبکه می‌پردازیم.

۲-۱-شبکه‌های عمومی باز

در این مدل شبکه، هر کسی بدون آنکه نیاز باشد توسط یک سری قوانین احراز هویت شود، قادر خواهد بود وارد شبکه شده و اطلاعات موجود در شبکه را ببیند و به عنوان گره دفتر کل یک کپی از وضعیت شبکه را داشته باشد و در فرآیند اجماع و اعتماد همگانی شرکت کند و همچنین یک بلاک جدید هم به سیستم اضافه کند. در این مدل گره‌های موجود در شبکه هیچ‌گونه شناختی نسبت به هم ندارند. از این مدل بیشتر در ساز و کارهای مالی و پرداختی استفاده می‌شود. در این شبکه فرآیند اجماع بین همه‌ی گره‌های فعال هستند اجرا خواهد شد. اما این شبکه خاصیت توسعه پذیری بسیار بالایی دارد و همچنین با توجه به وجود گره‌های بسیار زیاد و بدون نظارت، خاصیت اجماع و اعتماد همگانی که موجب عدم تغییر داده های ثبت شده می‌شود بسیار بهتر اجرا خواهد شد. همچنین با توجه به وجود کپی‌های بسیار زیاد از بلاک‌ها عملا از بین رفتن داده غیر ممکن است.

اما این مدل شبکه به خودی خود برای نگهداری پرونده‌های سلامت اصلا مناسب نیست زیرا اطلاعات پزشکی دارای خاصیت محرمانگی هستند. از طرف دیگر اطلاعات پزشکی به صورت ذاتی ماهیت تخصصی دارند و هرکسی در این شبکه نباید بتواند هر

مدل داده که بخواهد قرار دهد. پس در صورتی که بخواهیم از این مدل شبکه‌های بلاک‌چین برای حوزه‌ی سلامت استفاده کنیم باید تغییراتی را در آن اعمال کنیم تا بتوانیم با استفاده از مدل عمومی باز مشکلات محرمانگی و درستی داده را نیز حل کنیم.

در این مقاله ۳ روش مطرح که با استفاده از این مدل، در حال توسعه در دنیا است را بررسی خواهیم کرد که علاوه بر استفاده از مزایای این مدل شبکه تا حدی معایب موجود در شبکه برای داده‌های پزشکی را بر طرف می‌سازد.

۲-۱-۱- استفاده از رمزنگاری محتوایی در شبکه عمومی باز

در این روش مشکل محرمانگی داده‌ها با استفاده از رمزنگاری محتوایی بلاک‌ها حل شده است[۹]. فرد سازنده‌ی بلاک در هر بلاک شناسه خود را به صورت باز قرار داده تا مشخص شود بلاک برای اوست و محتویات بلاک را که اطلاعات پزشکی اوست با یک کلید از یک زوج کلید مشخص رمزگذاری می‌کند و در شبکه بلاک‌چین عمومی قرار می‌دهد. حال اعضای شبکه دیگر قادر به دسترسی به اطلاعات بلاک نخواهند بود مگر آنکه کلید دیگر این زوج کلید را داشته باشند[۹]. مکانیزم انتقال کلید می‌تواند یک مکانیزم خارج-بلاکی باشد. در این روش مشکل محرمانگی تا حدی برطرف می‌شود اما چالش‌های فراوانی از جمله مکانیزم ورود اطلاعات، جلوگیری از ساخت بلاک‌های نامعتبر، اعتماد به صحت داده‌های درون هر بلاک و مکانیزم انتقال کلید به وجود می‌آید. شکل ۳ شمایی از این مدل را نشان می‌دهد.

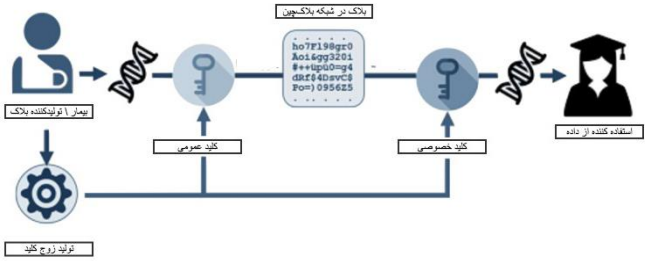
۲-۱-۲ استفاده از فرآیندهای خارج-بلاکی برای ذخیره سازی داده در شبکه بلاک‌چین عمومی باز برای تضمین عدم تغییر داده

در این روش اطلاعات بیمار، به روش‌های مختلف ابری یا غیر ابری در محلی امن ذخیره شده و تنها یک hash از داده‌های آن برروی یک شبکه عمومی باز قرار داده می‌شود. در این روش امنیت اطلاعات و محرمانگی در بخش ذخیره سازی داده تامین شده و فقط یک شبکه بلاک‌چین برای تامین صحت و عدم تغییر داده‌های اصلی تشکیل می‌شود به صورتی که اگر داده تغییر کند hash داده با hash موجود در شبکه یکی نبوده و گره‌ها به اجماع نمی‌رسند و تغییر این بلاک مشخص می‌شود. شکل ۴ نمونه‌ای از این شبکه را نشان می‌دهد. در این روش بلاک‌چین صرفا به عنوان یک بخش کوچک سیستم برای تضمین صحت داده استفاده شده و چالش‌های گذشته مربوط به ذخیره سازی و اشتراک که در بخش قبل شرح داده شد پا برجاست.

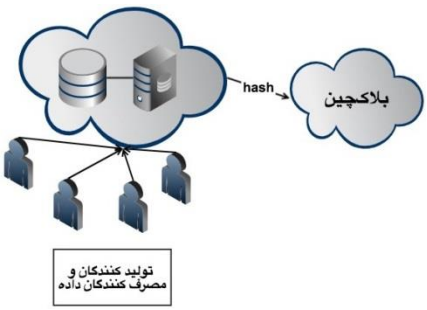
۲-۱-۳- استفاده از قراردادهای هوشمند در شبکه عمومی باز

قراردادهای هوشمند المان‌های جدیدی از شبکه بلاک‌چین هستند که می‌توان آن‌ها را به دستگاه‌های فروش خودکار تشبیه کرد. این قراردادها به صورت هوشمند و بدون نیاز به طرف سومی که آن را اجرا کند در زمان مشخص شده‌ای اجرا خواهند شد[۱۰].

در مورد پرونده‌های سلامت می‌توان از این قراردادها برای اجرای نوعی محرمانگی در کنار قابلیت اشتراک‌گذاری به صورت کنترل‌شده استفاده کرد به صورتی که اطلاعات پزشکی افراد توسط گره‌هایی خاص خارج از شبکه بلاک‌چین تولید و نگهداری می‌شود، این گره‌ها می‌توانند مثلا بیمارستان های مختلف باشند. حال برای آن که بتوان قابلیت اشتراک‌گذاری جهانی و کنترل شده‌ای به آن‌ها اضافه کرد، از یک شبکه بلاک‌چین عمومی باز استفاده می‌کنیم، اما به جای قرار دادن اطلاعات روی شبکه این بار قراردادهای هوشمند روی شبکه قرار می‌گیرند. این قراردادهای هوشمند بین بیمار و شخص مصرف کننده داده‌ی پزشکی او مثلا بیمارستان منعقد شده که توسط آن، بیمارستان



شکل۳: مدل استفاده از رمزنگاری محتوایی در شبکه عمومی باز



شکل ۴: مدل فرآیندهای خارج بلاکی برای ذخیره پرونده سلامت

اجازه‌ی دست‌یابی به اطلاعات ذخیره شده در مرکز مشخصی را تحت شرایط موجود در قرارداد خواهد داشت[۱۱]. استفاده از این مدل محرمانگی را تامین کرده و مشکل اشتراک داده به صورت حفاظت شده را هم حل می‌کند. در شکل ۵ شمای این سیستم را مشاهده می‌کنید

۲-۲-شبکه‌های خصوصی باز

ساختار این مدل از شبکه‌های بلاک‌چین با توجه به تعریف‌هایی که تا به امروز از شبکه‌های بلاک‌چین ارائه‌شده مبهم است. با توجه به ماهیت مبهم و متناقض این شبکه تاکنون مدل پایدار و مشخصی از سیستم‌های ذخیره‌سازی پرونده‌های سلامت برپایه‌ی آن توسعه داده نشده‌است.

۲-۳-شبکه‌های عمومی بسته

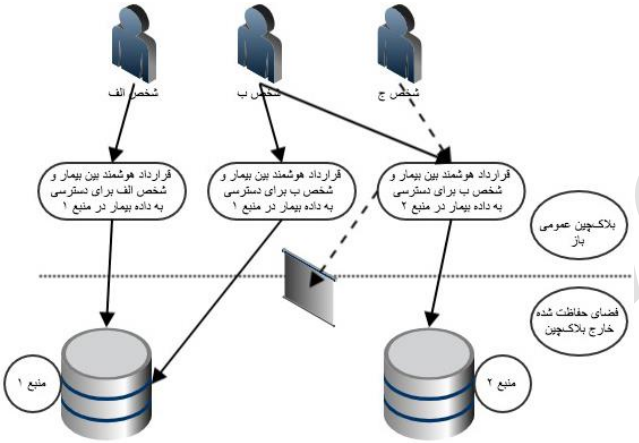
این مدل از شبکه بلاک‌چین حالتی میان بلاک‌چین عمومی و بلاک‌چین خصوصی ایجاد می‌کند. در این شبکه هر گره پس از عضو شدن اعمال محدودتری را برای انجام دارد، در واقع گره‌ها برای انجام هر عملی از جمله خواندن یا نوشتن بر روی شبکه نیاز به مجوز دارند. برای دریافت مجوز، گره نیاز دارد تا توسط شرکت یا مجموعه‌ای از شرکت‌ها که اعضای پایه‌ای آن شبکه هستند احراز هویت شود، برخلاف شبکه‌های عمومی باز که پس از عضو شدن در شبکه، گره قادر به انجام هر عملی از جمله تایید تراکنش‌ها و ذخیره دفتر کل شبکه است. این گونه محدودیت‌ها باعث می‌شود زنجیره بلوکی سیستم فقط برای افراد تایید شده قابل دیدن یا تغییر باشد. تفاوت اصلی این نوع از پیاده‌سازی با شبکه‌های خصوصی در عضویت گره‌هاست؛ در شبکه‌های خصوصی گره‌ها محدود و کاملا شناخته شده هستند اما در این شبکه هر کسی می‌تواند برای عضویت در شبکه تقاضا دهد، حتی در برخی از پیاده‌سازی‌های انجام گرفته از این مدل افراد می‌توانند بدون اجازه برخی اعمال مثل خواندن تراکنش‌ها را قبل از احراز هویت انجام دهند. مهم‌ترین پیاده‌سازی‌های این مدل بلاک‌چین را می‌توان در ارزهای دیجیتال Ripple و EOS دید.

از آن‌جا که در این نوع شبکه، گره‌ها قابل اعتماد به حساب می‌آیند، بارگذاری اطلاعات حساس و خصوصی مانند پرونده سلامت بر روی شبکه بلاک‌چین با ریسک کمتری نسبت به شبکه‌های عمومی باز همراه است اما باز هم متدهای احراز هویت و اعتماد کردن به گره‌های جدید از چالش‌هایی است که این مدل از شبکه‌ها با آن دست و پنجه نرم می‌کنند.

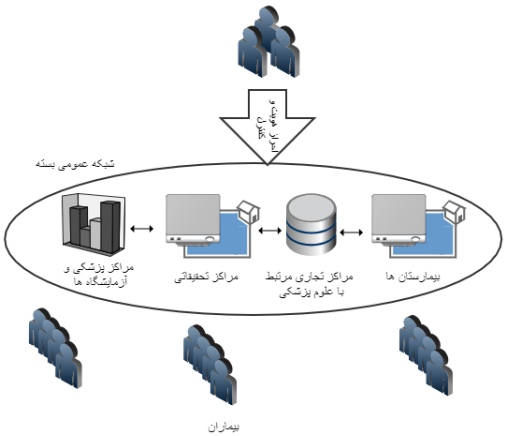
روش ذخیره پرونده سلامت افراد در این نوع شبکه به این شکل است که نهاد رسمی جهانی و مجموعه‌ای از نهادهای کشوری برای ساخت و نظارت بر روی شبکه اقدام می‌کنند، هر گره شبکه یک بیمارستان، آزمایشگاه و یا سایر مراکز پزشکی می‌تواند باشد که پس از ورود به این سامانه برای شرکت در پروتکل های اجماع و یا حتی اضافه کردن داده‌های جدید باید مجوزهای مربوطه را از نهاد کنترل‌کننده کسب کند. شکل ۶ نمونه‌ای از سیستم پزشکی پیاده‌سازی شده در این نوع شبکه است.

۲-۴- شبکه‌های خصوصی بسته

در این مدل شبکه تمامی گره‌هایی که در شبکه شرکت دارند، کاملا یک دیگر را می‌شناسند. در این مدل، شبکه توسط



شکل ۵: استفاده از قراردادهای هوشمند در شبکه عمومی باز برای دسترسی به پرونده‌های سلامت، برگرفته از [۱۱]



شکل ۶: مدل ایجاد پرونده سلامت بر روی بلاک‌چین عمومی بسته

یک نهاد یا ارگان مرکزی به منظور استفاده در یک سیستم خاص پیکربندی می‌شود و تولید اطلاعات و نگهداری آن وظیفه‌ی آن نهاد می‌باشد. از این مدل به منظور راهکاری در توسعه سیستم‌هایی میتوان استفاده کرد که بنا به ماهیتشان می‌بایست کنترل خاصی روی گره‌ها اعمال گردد[۱۲]. به طور کلی از این سیستم‌ها برای مدیریت و توسعه یک بستر برای موجودیت‌های واقعی خارج از بلاک‌چین استفاده می‌شود.

در این مدل، گره‌ها ابتدا توسط نهادی بیرونی که مالک شبکه است، احراز هویت می‌شوند و اجازه‌ی حضور در شبکه را کسب می‌کنند و به همه‌ی گره‌های دیگر شناسانده می‌شود تا بتواند در فرآیند اجماع برای دسترسی به اعتماد همگانی شرکت کند. این گره همچنین می‌تواند در صورت تایید مالک اصلی تولید کننده بلاک باشد. این شبکه برای مدیریت طلاعات پزشکی می‌تواند نقش بسیار موثری بازی کند به صورتی که یک شبکه از مراکز قابل اعتماد توسط نهاد مرکزی سلامت یک کشور تشکیل می‌شود. گره‌های این شبکه می‌توانند تولید کننده یا مصرف کننده اطلاعات باشند مثل بیمارستان‌ها و آزمایشگاه‌ی معتبری که اعتبار آنها توسط نهاد مرکزی تایید می‌شود. این گره‌ها در یک شبکه منسجم داده‌های پزشکی را در یک زنجیره بلوک اختصاصی به اشتراک می‌گذارند و از آنجا که همه‌ی گره‌ها کاملا قابل اعتماد هستند محرمانگی داده کاملا رعایت شده و همچنین اصل تضمین عدم تغییر و صحت داده هم به دلیل ماهیت بلاک‌چین کاملا رعایت می‌شود.

یکی از روش‌های پیاده‌سازی سیستم‌های پرونده سلامت با استفاده از این نوع شبکه‌های بلاک‌چین به این صورت است که یک شبکه در لایه پایین توسط نهاد نظارتی از تعدادی گره شخصی متعلق به خودش شکل می‌گیرد. این نهاد به طور مثال می‌تواند وزارت بهداشت یک کشور باشد. حال تبادل هرگونه اطلاعات با این شبکه به شدت محافظت شده توسط تعدادی دروازه خارج-بلاکی که مربوط به نهاد مرکزی هستند صورت می‌گیرد به صورتی که هر کسی که اطلاعات جدیدی تولید می‌کند مثل بیمارستان، آزمایشگاه یا حتی خود بیمار، اطلاعات خود را به یکی از دروازه‌های مشخص شده تحویل می‌دهد. این دروازه (Gateway) در صورتی که اطلاعات مورد تاییدش باشد آن را در شبکه بلاک‌جین داخلی خودش قرار می‌دهد. برای خواندن اطلاعات هم هر شخصی که بخواهد به اطلاعات دسترسی داشته باشد باید در خواست خود را به دروازه ارسال کند. در صورتی که در خواست او مورد تایید باشد اطلاعات از بلاک‌چین دریافت شده و به او داده می‌شود. در این روش سیاست گذاری بر روی دروازه‌ها بر عهده‌ی نهاد مرکزی است. این نهاد می‌تواند خود بیمار را هم در تصمیم‌گیری ها مشارکت دهد به صورتی که زمانی که یک بیمارستان درخواست دسترسی به اطلاعات را به دروازه می‌دهد، دروازه تا تایید شخص بیمار از دادن این اطلاعات به درخواست کننده خودداری می‌کند[۱۳].

۲-۵ -شبکه‌های ترکیبی

شبکه‌های ترکیبی دسته‌ای جدید در شبکه‌های بلاک‌چین نیستند بلکه در واقع ترکیبی از این دسته‌ها به‌شمار می‌آیند. این ترکیب‌ها به گونه‌ای شکل می‌گیرند که ویژگی‌های هر دو شبکه عمومی و خصوصی بلاک‌چین را به ارمغان بیاورند.

یکی از معماری‌های رایج برای پیاده‌سازی شبکه‌های ترکیبی، معماری لایه‌ای است. در این نوع معماری کل سیستم با توجه به سطح دسترسی‌ها و کاربردهای اطلاعات برای گره‌ها به چند لایه تقسیم می‌شود؛ در هر لایه با توجه به میزان اعتماد به گره‌ها و محرمانگی داده‌ها عمومی یا خصوصی بودن شبکه مشخص می‌شود.

در مبحث مورد نظر ما یعنی پرونده سلامت، شبکه‌های ترکیبی بسیار مفید و کارا هستند و در حال حاضر نیز پیاده‌سازی‌های زیادی در این زمینه در حال اجراست. یک روش پیاده‌سازی پرونده سلامت که تقریبا کاراترین و به‌روزترین روش نیز هست، تقسیم‌بندی سیستم به سه لایه به شرح زیر است:

لایه اول شامل هر بیمار و دستگاه‌ها و سنسورهای اندازه‌گیری اطلاعات سلامتی او است. برای پیاده‌سازی این لایه از بلاک‌چین خصوصی استفاده می‌شود تا خود فرد و یا سنسورها و دستگاه‌های هوشمند مرتبط با او به راحتی و با امنیت بالا بتوانند اطلاعات خود را به شبکه اضافه کنند و فرد یا نهاد دیگری نیز قابل به استفاده از آن‌ها نباشد[۱۴].

لایه دوم شامل مراکز پزشکی مانند بیمارستان‌ها و آزمایشگاه‌هاست که دارای شبکه بلاک‌چین عمومی هستند. اطلاعات در لایه اول ابتدا رمزنگاری می‌شوند و سپس به همراه یک نام مستعار برای هر بیمار به این شبکه فرستاده می‌شوند[۱۴]. گره‌های این شبکه برای دسترسی به داده‌های هر بیمار و یا اضافه کردن اطلاعات به پرونده سلامت، باید کلید عمومی و نام مستعار او را داشته باشند. همچنین برای احراز

هویت و گرفتن دسترسی باید ابتدا به لایه سوم مراجعه کنند.

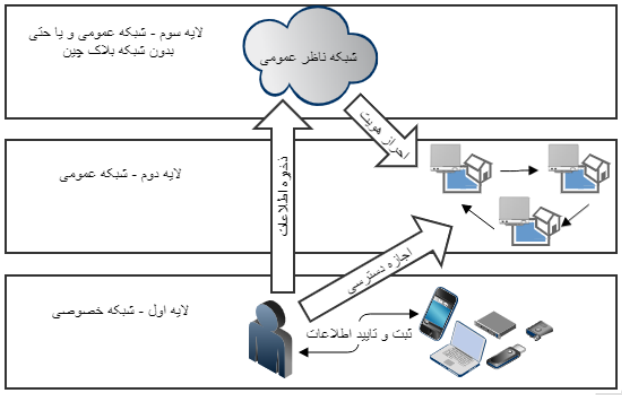
لایه سوم یک شبکه بلاک‌چین عمومی است که یک نسخه از تمامی داده‌های لایه اول و دوم را باز هم با نام مستعار نگه‌داری می‌کند. کاربرد این لایه کنترل گره‌های لایه دوم و همچنین استفاده از پرونده‌های سلامت در علوم داده‌کاوی و استخراج الگوهای مفید است. در بسیاری از پیاده‌سازی‌ها لایه سوم را حتی بدون شبکه بلاک‌چین و تنها با استفاده از ابر نیز پیاده‌سازی می‌کنند[۱۴]. شکل ۷ معماری سه لایه شبکه‌های ترکیبی برای پرونده سلامت را نشان می‌دهد.

۳-بحث

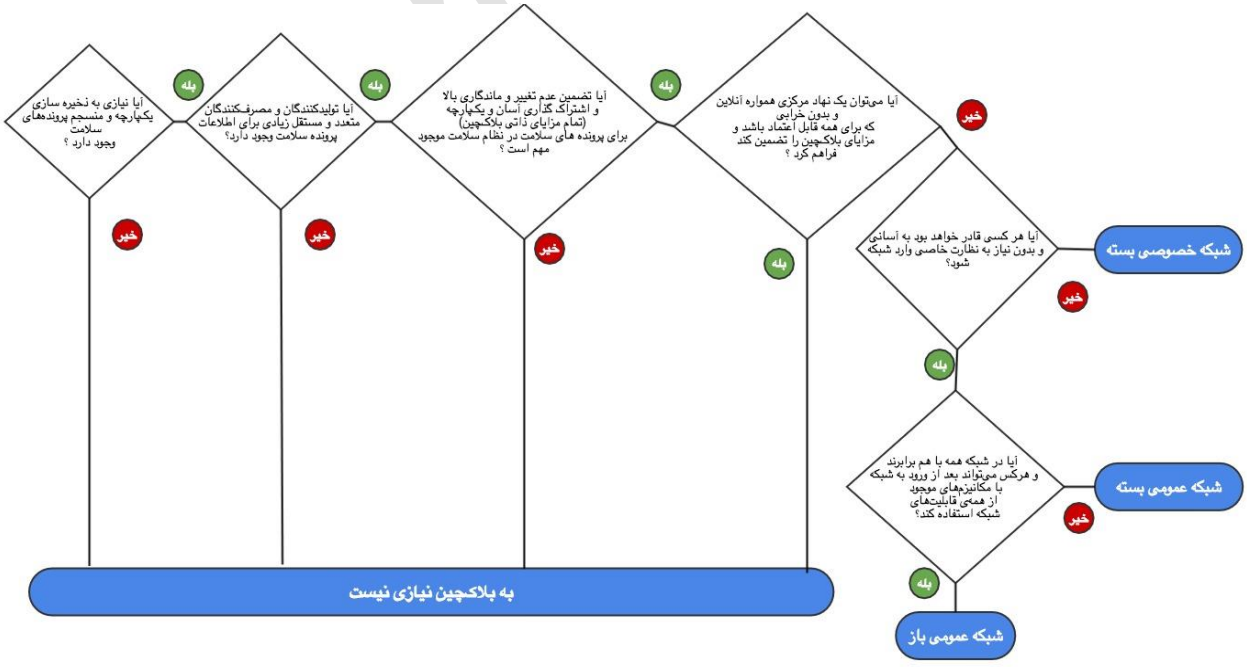
طبق متدولوژی که پیش رفتیم، برای پیاده‌سازی پرونده سلامت در بستر بلاک‌چین چهار گزینه به همراه یک گزینه ترکیبی پیش رو داریم. هر کشور یا سازمان مسئولی باید با توجه به داشته‌ها و نیازهای خود روشی را انتخاب کند. این روش می‌تواند بلاک‌چین و یا روش‌های دیگر پیاده‌سازی باشد. ما در این بخش با توجه به یافته‌هایمان و نمونه کارهای صورت گرفته قبلی فلوچارتی برای نیازسنجی و انتخاب مدل پیاده‌سازی پرونده سلامت تهیه کرده‌ایم. شکل ۸ این فلوچارت را نشان می‌دهد.

۴-نتیجه گیری

هدف این تحقیق مطالعه بر روی راه حل‌های ممکن برای پیاده‌سازی پرونده الکترونیک سلامت در بستر بلاک‌چین بود. در این راستا هم با چالش نو بودن و مبهم بودن مباحث مربوط به بلاک‌چین مواجه بودیم و هم مشکل خاص بودن پرونده الکترونیک سلامت مطرح بود. بنابراین با توجه به ویژگی‌های پرونده الکترونیک سلامت و ابعاد مختلف بلاک‌چین یک رویکرد چهار گزینه‌ای به همراه یک گزینه ترکیبی مورد مطالعه قرار گرفت و ویژگی‌های هریک تشریح گردید. این مقاله کمک می‌کند با توجه به سیاست‌هایی که در نظام پزشکی یک کشور وجود دارد چه نوع سیستم بلاک‌چینی می‌تواند به کار گرفته شود



شکل ۷: نمایی از یک شبکه ترکیبی پرونده سلامت، بر گرفته از [۱۴]



شکل ۸: فلوچارت نیازسنجی و تعیین مدل فناوری مورد استفاده در سیستم‌های پرونده سلامت

مراجع

[1] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?. *IEEE Cloud Computing*, *5*(1), 31-37.

[2] You, I., Choo, K. K. R., & Ho, C. L. (2018). A smartphone-based wearable sensors for monitoring real-time physiological data. *Computers & Electrical Engineering*, *65*, 376-392.

[3] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.

[4] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman.MedRec: Using Blockchain for Medical Data Access and Permission Management. *2nd International Conference on Open and Big Data*, 2016.

[5] Satoshi Nakamoto.Bitcoin:Apeer-to-peer electronic cash system. 2009.

[6] Gavin Wood. Ethereum: A Secure Decentralized Generalized Transaction Ledger. Technical report, Ethereum, August 2017.

[7] Wüst, K., & Gervais, A. (2018, June). Do you need a Blockchain?. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE.

[8] Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2018). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and computer Applications.*

[9] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.

[10] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of medical systems*, *42*(7), 130.

[11] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference* (Vol. 13, p. 13).

[12] Pautasso, and P. Rimba. A Taxonomy of Blockchain-Based Systems for Architecture Design. In 2017 IEEE International Conference on Software Architecture (ICSA), pages 243–252, April 2017.

[13] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*(10), 218.

[14] Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier Blockchain framework for IoT-EHRs systems. *Procedia Computer Science*, *141*, 159-166.

کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش مهارت های کاربردی در تدوین و چاپ مقاله

اصول تنظیم قراردادها

مقاله نویسی علوم انسانی