

Providing and Implementing the Secure Structure of the Waiting List Management System for Organ Transplantation Patients with Blockchain Technology based on IPFS

Mohamahd Amin Samsami¹, Parviz Rashidi-Khazaei^{2*}, Omid Reza Boloki Speily²

1. MA Student, Department of Information Technology and Computer Engineering, Urmia University of Technology, Urmia, Iran

2. PhD in Information Technology Engineering, Assistant Professor, Department of Information Technology and Computer Engineering, Urmia University of Technology, Urmia, Iran

ARTICLE INFO:

Article History:

Received: 26 Jan 2024

Accepted: 11 Sep 2024

Published: 21 Sep 2024

*Corresponding Author:

Parviz Rashidi-Khazaei

Email:

p.rashidi@uut.ac.ir

Citation: Samsami MA, Rashidi-Khazaei P, Boloki OR. Providing and Implementing the Secure Structure of the Waiting List Management System for Organ Transplantation Patients with Blockchain Technology based on IPFS. Journal of Health and Biomedical Informatics 2024; 11(2): 101-114. [In Persian]

Abstract

Introduction: In recent decades, the medical field has faced many challenges in managing and maintaining information security on waiting lists for organ transplantation patients. The lack of trust of the participants in this process, which requires more efforts to ensure the security and privacy of patients and donors, highlights the necessity for finding new security solutions.

Method: In this study, a safe and reliable method was presented and implemented using blockchain technology based on the Network Distributed File System (IPFS) to improve waiting list management and solve the challenge of maintaining voluminous medical documents. In this method, patient information is anonymized using appropriate algorithms, and then, stored and linked to the blockchain network.

Results: The implemented system provides an integrated and innovative method in organ transplantation management, which not only comprehensively provides the security and privacy of patients, but also reduces social inequalities and increases trust in the organ donation process, as well as fair management of patient waiting lists.

Conclusion: The proposed system has provided a scalable and efficient system using microservices architecture and can be provided as a reliable tool for medical stakeholders.

Keywords: Blockchain, Organ Transplant Waiting List, Anonymization of Medical Documents, Storage of Patients' Medical Documents, Patient Privacy security



CrossMark

مقاله پژوهشی

ارائه ساختار امن سامانه مدیریت لیست انتظار بیماران پیوند عضو مبتنی بر فناوری بلاکچین و ذخیره سازی توزیع شده پرونده

محمد امین صمصامی^۱، پرویز رشیدی خزاعی^{۲*}، امیدرضا بلوکی اسپیلی^۲

۱. دانشجوی کارشناسی ارشد، مهندسی فناوری اطلاعات و کامپیوتر، دانشکده علوم و فناوری های نوین، دانشگاه صنعتی ارومیه، ارومیه، ایران

۲. دکتری تخصصی مهندسی فناوری اطلاعات، استادیار، گروه مهندسی فناوری اطلاعات و کامپیوتر، دانشکده علوم و فناوری های نوین، دانشگاه صنعتی ارومیه، ارومیه، ایران

چکیده

مقدمه: مدیریت و حفظ امنیت اطلاعات لیست انتظار بیماران نیازمند پیوند عضو در دهه های اخیر با چالش های متعددی مواجه بوده است. عدم اعتماد بین مشارکت کنندگان و نگرانی ها درباره حفظ حریم خصوصی بیماران و اهداکنندگان، لزوم یافتن راهکارهای امنیتی جدید را برجسته کرده است.

روش کار: در این مطالعه روشی امن و قابل اعتماد برای بهبود مدیریت لیست انتظار پیوند عضو با استفاده از فناوری بلاکچین و شبکه سیستم پرونده توزیع شده مبنی بر IPFS ارائه و پیاده سازی شده است که علاوه بر ذخیره سازی امن اطلاعات، چالش نگهداری اسناد پزشکی حجیم را نیز حل نموده است. در ساختار پیشنهادی اطلاعات بیمار با کمک الگوریتم های مناسب، گمنام سازی و سپس ذخیره سازی شده و به شبکه بلاکچین نیز متصل می شوند.

یافته ها: پس از بررسی روش های مشابه، چالش های موجود (حفاظت از هویت بیماران، نگهداری امن اسناد پزشکی و ...) شناسایی و سپس روشی یکپارچه و نوآورانه در مدیریت پیوند عضو با کمک الگوریتم های رمزنگاری و شبکه IPFS پیشنهاد و فراهم نموده که نه تنها امنیت و حریم خصوصی بیماران را به صورت جامع تأمین می کند، بلکه باعث کاهش نابرابری های اجتماعی و افزایش اعتماد به فرآیند اهدای عضو نیز می شود و به مدیریت عادلانه لیست انتظار بیماران پیوند عضو و حل چالش های اساسی حوزه پزشکی کمک می کند.

نتیجه گیری: سیستم پیشنهادی با به کارگیری معماری میکروسرویس، یک سیستم مقیاس پذیر و کارا را فراهم نموده است و می تواند به عنوان ابزاری مطمئن در اختیار دست اندرکاران قرار گیرد.

کلیدواژه ها: بلاکچین، لیست انتظار پیوند عضو، گمنام سازی اسناد پزشکی، ذخیره سازی اسناد پزشکی بیماران، امنیت حریم خصوصی بیماران

اطلاعات مقاله

سابقه مقاله

دریافت: ۱۴۰۲/۱۱/۶

پذیرش: ۱۴۰۳/۶/۲۱

انتشار برخط: ۱۴۰۳/۶/۳۱

*نویسنده مسئول:

پرویز رشیدی خزاعی

ایمیل:

p.rashidi@uut.ac.ir

ارجاع: صمصامی محمد امین،

رشیدی خزاعی پرویز، بلوکی اسپیلی امیدرضا. ارائه ساختار امن سامانه مدیریت لیست انتظار بیماران پیوند عضو مبتنی بر فناوری بلاکچین و ذخیره سازی توزیع شده پرونده. مجله انفورماتیک سلامت و زیست پزشکی ۱۴۰۳؛ ۱۱(۲): ۱۰۱-۱۱۴.

مقدمه

پیوند عضو به معنای انتقال عضو یا بافت از یک فرد به فرد دیگر است که به عنوان آخرین راه حل برای بسیاری از مشکلات پزشکی در نظر گرفته می شود و هدف آن بهبود وضعیت سلامت بیمار است [۱]. از زمان اولین پیوند موفقیت آمیز عضو بدن انسان در سال ۱۹۵۴، پیوند عضو به عنوان یک رشته جدید و مهم با تمرکز بر نوآوری در طراحی دارو و جراحی پزشکی مدرن ظاهر شد [۲]، ولی به دلیل کمبود عضو پیوندی، بیمار برای دریافت عضو مورد نیاز خود در لیست انتظار عضو قرار می گیرد. در بسیاری از موارد، زمان انتظار برای یافتن یک عضو مناسب برای بیماران بسیار طولانی است و باعث ایجاد مشکلات بزرگی در سراسر جهان شده است [۳].

با افزایش تعداد بیماران در لیست انتظار و تقاضای روزافزون برای اعضای پیوندی، چالش هایی مانند مدیریت عادلانه لیست انتظار، حفظ حریم خصوصی بیماران و جلوگیری از سوءاستفاده های احتمالی به مشکلاتی اساسی تبدیل شده اند. اهمیت امنیت و حریم خصوصی داده های بیماران، به دلیل حساسیت این اطلاعات و پیامدهای احتمالی نقض آن ها، امری ضروری است که نباید نادیده گرفته شود [۴]. با ظهور فناوری های نوین مانند بلاک چین و IPFS (Inter Planetary File Shystem) این امکان فراهم شده است که داده های پزشکی به صورت غیرمتمرکز، امن و با حفظ حریم خصوصی ذخیره و مدیریت شوند تا از مشکلاتی مانند حمله باج افزار به سیستم های سلامت پیشگیری نماید و فرآیند عمل پیوند را آسان تر کند. به کارگیری فناوری بلاک چین می تواند علاوه بر اشتراک گذاری و نگهداری ایمن داده های لیست بیماران، امنیت و عدالت لازم را برای اهداکنندگان و گیرندگان فراهم کند [۵].

Zouarhi یک سیستم اهدای کلیه تحت وب مبتنی بر بلاک چین به نام "Kidner" پیشنهاد داده است. این سیستم، راهکار جدیدی را به جای ساختار متمرکز مدیریت لیست انتظار پیوند کلیه ارائه می دهد. هدف سیستم پیشنهادی شناسایی و تطبیق اهدا کننده و گیرنده سازگار در سراسر جهان است [۶]. Dajim و همکاران، یک برنامه غیرمتمرکز تحت وب مبتنی بر بلاک چین برای ثبت اطلاعات بیماران از جمله شناسه پزشکی، نوع عضو و گروه خونی پیشنهاد کرده اند که فرآیند اهدای عضو را ایمن تر و خودکار می کند و از هرگونه امکان دستکاری جلوگیری می کند [۷]. در سیستم پیشنهادی Soni و Kumar بیمار با وضعیت بحرانی به صورت جداگانه مورد بررسی و ارزیابی قرار می گیرد و به جستجو، تطبیق دهنده و گیرنده کمک می کند [۸]. Hawashin و همکاران، یک برنامه اهدا و پیوند عضو مبتنی بر بلاک چین اتریوم پیشنهاد دادند که بر اساس اطلاعات ثبت شده، اهداکننده را با گیرنده مناسب مطابقت می دهد [۹].

در روش پیشنهادی Alandjani، فرآیند اهدای عضو با امضای یک قرارداد هوشمند توسط اهداکننده و گیرنده شروع می شود. سپس اسناد ارسال و توسط پزشک مجاز مراقبت های بهداشتی تأیید می شوند. در صورت عدم تطابق، پزشک یک جفت عدم تطابق ایجاد و در شبکه پخش می کند. شبکه یک تطابق مناسب جستجو می کند و برای تأیید به پزشک ارسال می گردد سپس اطلاعات اهداکننده و گیرنده که تأیید شده اند در بلاک چین ثبت می شوند [۱۰].

Yahaya و همکاران روشی برای ذخیره سازی و اشتراک سوابق پزشکی بیماران در شبکه زنجیره ای مبتنی بر بلاک چین پیشنهاد داده اند که با استفاده از یک سرویس مشتری اختصاصی، کاربران مختلف می توانند با بلاک چین تعامل داشته باشند. هنگام اضافه کردن سوابق، محدودیت های کنترل دسترسی به عنوان بخشی از منطق قرارداد هوشمند اجرا می شود تا اهدا کننده دیگری را از دیدن یا تولید اسناد برای بیمارانی که به آن ها مجوز ندارد، منع کند [۱۱]. Daniel و همکاران سیستمی برای ثبت، ذخیره سازی و تضمین مالکیت سوابق پزشکی بیماران مبتنی بر IPFS ارائه داده اند [۱۲].

بررسی هایی که پژوهشگران انجام داده اند به این نتیجه رسیده اند که در ایران و جهان، سازمان ها و مراکز درمانی برای پیوند عضو فاقد شفافیت و امنیت هستند و نظارت بر آن ها کاری بسیار دشوار است [۹]. در کشور ایران و اکثر کشورهای در حال توسعه، مشکلات متعددی برای شناسایی اهداکنندگان و اتصال آن ها به گیرندگان دارای اولویت در لیست انتظار پیوند وجود دارد و این مشکلات عبارتند از: ۱- نبود زیر ساخت مناسب ۲- عدم وجود نظام منسجم برای پیوند عضو ۳- عدم وجود بانک اطلاعاتی کامل در زمینه پیوند عضو ۴- عدم مشارکت اهداکنندگان به دلیل نبود اطمینان در خصوص محافظت از اطلاعات محرمانه [۱۳]. لازم است برای اجرای عدالت در تخصیص عضو پیوندی مکانیزم هایی برای مدیریت لیست گیرندگان در نظر گرفته شود و از طرفی عدم حفظ محرمانگی داده های اشخاص اهداکننده و گیرنده بر میزان تمایل افراد برای مشارکت تأثیر منفی می گذارند [۱۴]. سیستم های فعلی باعث سوء استفاده و

تبعیض بین بیماران خواهد شد که در نتیجه منجر به آسیب رساندن بیشتر به گیرنده‌های با توان مالی پایین‌تر، اما با الویت نیاز بالاتر به پیوند عضو، می‌شود.

بررسی و مقایسه پژوهش‌های انجام شده در جدول ۱ نشان داد که چگونه فناوری بلاک‌چین می‌تواند راه‌حل‌های مدیریت پیوند عضو را بهبود بخشد؛ اما این پژوهش‌ها همه معیارهای لازم برای فرآیند ثبت داده‌های حجیم پزشکی به صورت کاملاً محرمانه در لیست پیوند عضو را در نظر نمی‌گیرند. در این پژوهش، ساختاری امن برای ذخیره‌سازی و اشتراک‌گذاری داده‌های لیست انتظار بیماران پیوندی در جهت برطرف شدن بخشی از چالش‌ها مانند: ۱- دستکاری لیست پیوند عضو ۲- عدم امکان ذخیره‌سازی اسناد پزشکی حجیم در بلاک‌چین ۳- پیوست نشدن اسناد پزشکی بیمار در لیست پیوند ۴- عدم محافظت از حریم خصوصی اطلاعات بیماران در اسناد پزشکی ذخیره شده ۵- نبود یک سیستم یکپارچه غیرمتمرکز برای مدیریت لیست بیماران پیوندی، ارائه شده است. فناوری بلاک‌چین به عنوان یک فناوری نوآورانه، می‌تواند به حل بخشی از مشکلات فوق کمک نماید و اشتراک‌گذاری داده‌ها را ایمن‌تر و فرآیندهای اهدا عضو را آسان‌تر می‌کند [۱۵]. در این پژوهش با به کارگیری بلاک‌چین و شبکه IPFS، به دنبال ارائه و پیاده‌سازی ساختاری مناسب برای مدیریت لیست بیماران پیوندی هستیم تا بتوان محرمانگی داده‌ها را تضمین کند و اعضا بتوانند با اعتماد بیشتری در آن مشارکت داشته باشند.

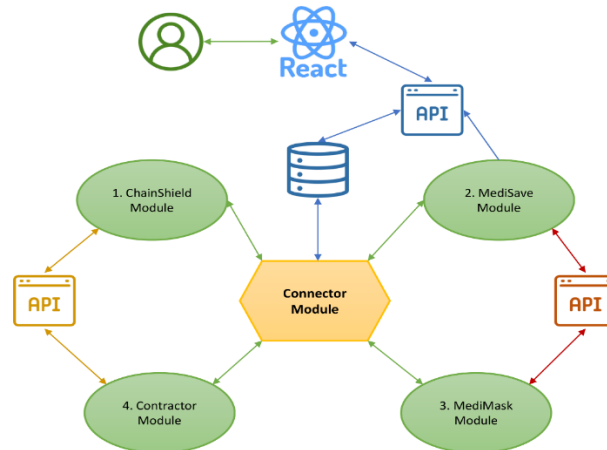
روش کار

این پژوهش از نوع کاربردی و بنیادی می‌باشد و به صورت گذشته نگر انجام گرفته است. روش‌های ارائه شده طی ده سال گذشته در جدول ۱ جمع‌آوری و ویژگی‌های مهم آن‌ها با یکدیگر مقایسه شده است و نقاط ضعف و قوت آن‌ها به‌طور کامل مورد مطالعه کیفی و بررسی قرار گرفته است. برای غلبه بر چالش‌ها و مشکلات روش‌های قبلی، ساختاری مطابق شکل ۱ پیشنهاد شده است که با استفاده از ماژول‌های مختلف، لیست کاملی از اهداکنندگان و گیرندگان، همراه با اسناد پزشکی بیماران را می‌توان با امنیت بیشتری ذخیره و نگهداری کرد. استفاده از این ساختار باعث کاهش خطاهای پزشکی در فرآیند انتخاب عضو و عمل پیوند شده و به حل چالش ناعدالتی‌های اجتماعی در لیست انتظار پیوند عضو کمک می‌نماید.

جدول ۱: مرور کلی آخرین روش‌های انجام شده مرتبط

سال	مرجع	نوع شبکه بلاک‌چین	استفاده از IPFS	دسترسی بیمار به اطلاعات خود	هدف اصلی	نقاط قوت	نقاط ضعف
۲۰۲۲	Hawashin و همکاران [۹]	خصوصی	NA	×	اهدای عضو و پیوند عضو به صورت هوشمند از طریق یک برنامه غیرمتمرکز	یکپارچه سازی ردیابی فرایند پیوند عضو اهدایی	عدم ذخیره‌سازی اسناد پزشکی بیماران
۲۰۲۱	Soni و Kumar [۸]	هایبرید	NA	✓	ایجاد یک برنامه غیر متمرکز با رویکرد FIFO برای انتخاب اهداکننده و گیرنده عضو	استفاده از الگوریتم‌های رمزنگاری مختلف و ایجاد عدالت در لیست انتظار	روش پیشنهادی در بستر بلاک‌چین زمان‌بر و کند است
۲۰۲۱	Yahaya و همکاران [۱۱]	خصوصی	نامشخص	✓	مدیریت اطلاعات و جلوگیری از دسترسی غیرقانونی یا نادرست به داده‌های اهدا کننده و گیرنده	احراز هویت بالای سیستم و امنیت بالای کاربران	نا مشخص بودن روش ذخیره‌سازی سوابق پزشکی بیماران
۲۰۲۰	Daniel و همکاران [۱۲]	خصوصی	IPFS	×	ذخیره‌سازی اسناد پزشکی بیماران نیازمند عضو با فناوری بلاک‌چین	استفاده از فناوری IPFS برای ذخیره‌سازی اسناد پزشکی	عدم محافظت از هویت بیماران در اسناد پزشکی ذخیره‌سازی شده
۲۰۱۹	Dajim و همکاران [۷]	خصوصی	NA	×	فرایند اهدای عضو را با کمک فناوری بلاک‌چین، ایمن و خودکار می‌کند	سیستم امن برای مدیریت لیست انتظار گیرندگان عضو	عدم ذخیره‌سازی اسناد پزشکی بیماران
۲۰۱۹	Alandjani [۱۰]	عمومی	NA	✓	راهنمایی یک سیستم غیرمتمرکز برای تعامل و تبادل اطلاعات بین اهداکننده عضو و بیمار	یکپارچه سازی فرایند انتقال عضو و ارتباط دیجیتالی بین اهداکنندگان و گیرندگان	تعامل کند سیستم به علت ماهیت فناوری بلاک‌چین
۲۰۱۷	Zouarhi [۶]	خصوصی	NA	×	انتخاب عضو از میان اهداکنندگان با روش کدین در یک برنامه غیرمتمرکز	پیدا کردن مناسب‌ترین عضو برای جراحی پیوند عضو	تأخیر در دسترسی به داده‌های پزشکی

ساختار راه حل پیشنهادی بر مبنای معماری میکروسرویس می‌باشد و شامل پنج ماژول: ۱- ماژول Coordinator، ۲- ماژول ChainShield (Chain Shield)، ۳- ماژول MediSave (Medical Save)، ۴- ماژول MediMask (Medical Mask) و ۵- ماژول Contractor می‌باشد که ارتباط بین ماژول‌ها در شکل ۱ نشان داده شده است.



شکل ۱: ماژول‌های ساختار پیشنهادی

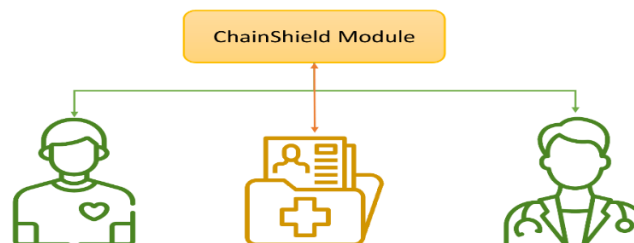
الف) ماژول رابط (coordinator)

ماژول Coordinator به عنوان هسته مرکزی، وظیفه ارتباط و هماهنگی سایر ماژول‌ها را بر عهده دارند و برای اتصال به پایگاه داده‌های مختلف استفاده می‌شود. با استفاده از Coordinator، شما می‌توانید به راحتی با هر پایگاه داده‌ای از طریق (دپ Dapp (Decentralized Applications ارتباط برقرار کنید.

با رشد محاسبات اینترنتی، به ویژه بلاکچین و قراردادهای هوشمند، دپ به نوع جدیدی از برنامه‌ها تبدیل شده است. از این طریق کاربران می‌توانند بدون درگیر شدن با جزئیات پیچیده برنامه‌های سروری مانند IPFS و ... از این سرویس استفاده نموده و در عین حال داده‌ها و نتایج عملیات اصلی در قراردادهای هوشمند در یک زنجیره بلوکی را ذخیره نمود. دپ‌ها از طریق تراکنش‌ها، با قراردادهای هوشمند تعامل دارند و بر اساس آن‌ها خدمات ارائه می‌دهند [۱۶] و ماژول مشخص می‌کند بخش‌های مختلف چگونه به هم دیگر متصل شوند.

ب) ماژول سپر زنجیره‌ای (ChainShield Module)

ماژول ChainShield یک سپر زنجیره‌ای است که از فناوری بلاکچین در جهت افزایش امنیت و حفظ حریم خصوصی کاربران استفاده می‌کند.

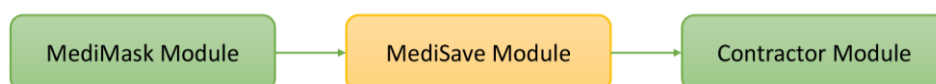


شکل ۲: ذخیره‌سازی و نگهداری مشخصات پزشکان و بیماران در ماژول ChainShield Module

همان طور که در شکل ۲ مشاهده می شود، ماژول ChainShield بر مبنای فناوری بلاک چین عمل می کند که امکان ذخیره سازی و تبادل اطلاعات بدون نیاز به واسطه دسترسی به دیتابیس توزیع شده را فراهم می کند. در فناوری بلاک چین با استفاده از رمزنگاری و توزیع داده ها، امکان هک، حذف و دستکاری اطلاعات ثبت شده، تا حد زیادی کاهش می یابد و با موفقیت در حوزه های مختلفی استفاده شده است [۱۷]. به این ترتیب، هر گونه تغییر یا دسترسی غیرمجاز به اطلاعات بیمار، برای دیگر اعضای شبکه قابل رؤیت خواهد بود و با تعریف سطح دسترسی برای هر یک از اعضای شبکه [۱۸] می تواند اطلاعات پزشکی افراد را به صورت امن در سیستمی توزیع شده ذخیره کند. به این ترتیب، هر گونه تغییر یا دسترسی غیرمجاز به اطلاعات پزشکی، برای دیگران امکان پذیر نخواهد بود. در ChainShield، هر پزشکی که در شبکه بلاک چین عضو می شود، باید هویت خود را تأیید کند این روش می تواند به تضمین امنیت در ارائه خدمات پزشکی کمک کند.

پ) ماژول ذخیره سازی اسناد پزشکی (MediSave Module)

ذخیره سازی اسناد پزشکی بیماران و نگهداری آن ها از وظایف اصلی ماژول MediSave می باشد. در شکل ۳، این ماژول با ارتباط بین ماژول MediMask و ماژول Contractor اسناد حجیم پزشکی را که قابلیت ذخیره سازی در قراردادهای هوشمند ندارند را در IPFS ذخیره سازی می کند.



شکل ۳: ارتباط ماژول MediSave با دیگر ماژول ها

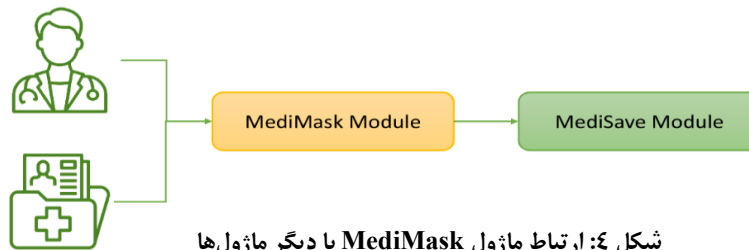
شبکه IPFS به عنوان یک پروتکل انتقال و ذخیره سازی فایل های دیجیتالی معرفی شده است. در این شبکه، بدون نیاز به سرور مرکزی فایل ها به صورت قطعات (chunk) ذخیره می شوند و هر قطعه با یک شناسه یکتا مانند یک هش مشخص می شود. این شبکه امکان ذخیره سازی فایل های بزرگ و حجیم را فراهم می کند و باعث می شود که اسناد پزشکی بدون محدودیت در اینترنت قابل دسترس باشند. همچنین با استفاده از IPFS، از گم شدن و از بین رفتن اسناد پزشکی جلوگیری می شود [۱۹] و امکان دسترسی به آن ها برای مراکز درمانی مختلف به صورت سریع و آسان فراهم می شود و از سرعت و کارایی بالای این ماژول تحت شبکه IPFS برای این منظور بهره برده می شود. همچنین استفاده از MediSave باعث می شود زمانی یکی از سرورهای که در این شبکه اطلاعات را ذخیره کرده است خراب شود، دسترسی به اطلاعات از طریق سرورهای دیگر امکان پذیر شود.

با استفاده از IPFS در این ماژول، اطلاعات پزشکی بیماران می تواند به صورت توزیع شده و در اختیار چندین سازمان و دستگاه پزشکی قرار گیرد. در این حالت، اطلاعات پزشکی بیماران به صورت متمرکز در یک سرور نگهداری نمی شود و هر بخش مربوطه به صورت مستقل و مستقل از سایر بخش ها از اطلاعات بیماران استفاده می کند [۲۰].

ت) ماژول گمنام سازی اسناد پزشکی (MediMask Module)

برای حفظ محرمانگی اطلاعات بیماران از روش گمنام سازی (Anonymization) قبل از ذخیره سازی اسناد پزشکی استفاده می شود. در این ساختار، اطلاعات شخصی بیماران از جمله نام، شماره تماس، آدرس و ... از اسناد پزشکی بیمار حذف می شود و فقط اطلاعات پزشکی مرتبط با بیمار باقی می ماند. در این حالت، اسناد پزشکی بیماران با حفظ حریم شخصی و امنیت اطلاعات، در دسترس مراکز پزشکی مختلف قرار می گیرد [۲۱].

در شکل ۴ ماژول MediMask برای حفظ حریم خصوصی بیماران، ابتدا به پزشکی که در این سرویس توسط سازمان یا مرکز درمانی که اجازه بارگذاری داده‌های پزشکی را داده است، از پزشک، اسناد پزشکی بیمار را دریافت می‌کند و سپس مشخصات بیمار را از آن اسناد حذف می‌کند و یک هش یا شناسه رمزنگاری شده به اسناد پیوست می‌کند و در نهایت اسناد را در اختیار MediSave قرار می‌دهد.

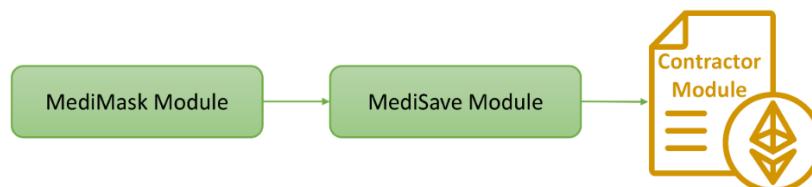


شکل ۴: ارتباط ماژول MediMask با دیگر ماژول‌ها

با گمنام‌سازی اسناد پزشکی بیماران، از اطلاعات شخصی و حساس آن‌ها در مواقعی که به دسترسی اطلاعات پزشکی آن‌ها احساس می‌شود، جلوگیری می‌شود. همچنین، با این روش، امکان مقایسه اطلاعات پزشکی بیماران با یکدیگر به منظور بهبود خدمات پزشکی امکان‌پذیر است. همچنین با استفاده از MediMask می‌توان تمام داده‌های بیماران را برای مراکز تحقیقاتی جمع‌آوری کرد که آن‌ها با دسترسی به این داده‌ها بتوانند راه‌حل‌های بهتری برای درمان بیماران ارائه دهند. برای رمزنگاری و گمنام‌سازی داده از تابع درهم‌سازی SHA3 به عنوان آخرین نسل الگوریتم SHA که، غیر قابل رمزگشایی بوده و برگشت پذیر نمی‌باشد و در اغلب در پروتکل‌های ارتباطی امن، مانند TLS (Transport Layer Security) (امنیت لایه حمل و نقل)، برای ارائه رمزنگاری و تأیید اعتبار پیام استفاده می‌شوند، استفاده خواهد شد [۲۲]. در این ماژول اطلاعات بیمار شامل: ۱- نام بیمار، ۲- تاریخ تولد بیمار، ۳- شماره تماس بیمار و ... توسط الگوریتم SHA3 هش می‌شوند و به اسناد بیماران تگ می‌شوند. سپس اسناد پزشکی بیماران به همراه تگ رمزنگاری شده توسط ماژول MediMask به ماژول MediSave برای ذخیره‌سازی انتقال داده خواهد شد.

ث) ماژول قرارداد هوشمند (Contractor Module)

همان‌طور که در شکل ۵ مشخص است، ماژول Contractor یک قرارداد هوشمند بین پزشکان و مراکز پزشکی است که برای ثبت اطلاعات پزشکی بیمار ایجاد می‌شود. برای ساخت این قرارداد هوشمند، از بلاک‌چین اتریوم استفاده می‌شود که امکان ذخیره‌سازی امن و تغییر ناپذیری اطلاعات را فراهم می‌کند. با استفاده از این ماژول، پزشکان می‌توانند اطلاعات پزشکی بیمار خود را به صورت الکترونیکی در قرارداد هوشمند ثبت کنند و بیمار دسترسی به این اطلاعات را دارد [۲۳]. همچنین، با استفاده از این قرارداد هوشمند، پزشکان می‌توانند تشخیص‌های خود را به همراه اسناد پزشکی و نتایج آزمایش‌های بیماران ثبت کنند و به صورت الکترونیکی با آن‌ها ارتباط برقرار کنند. با توجه به این که اطلاعات پزشکی بسیار حساس است، استفاده از این ماژول باعث افزایش امنیت و حریم خصوصی بیماران می‌شود.



شکل ۵: ارتباط ماژول Contractor با دیگر ماژول‌ها

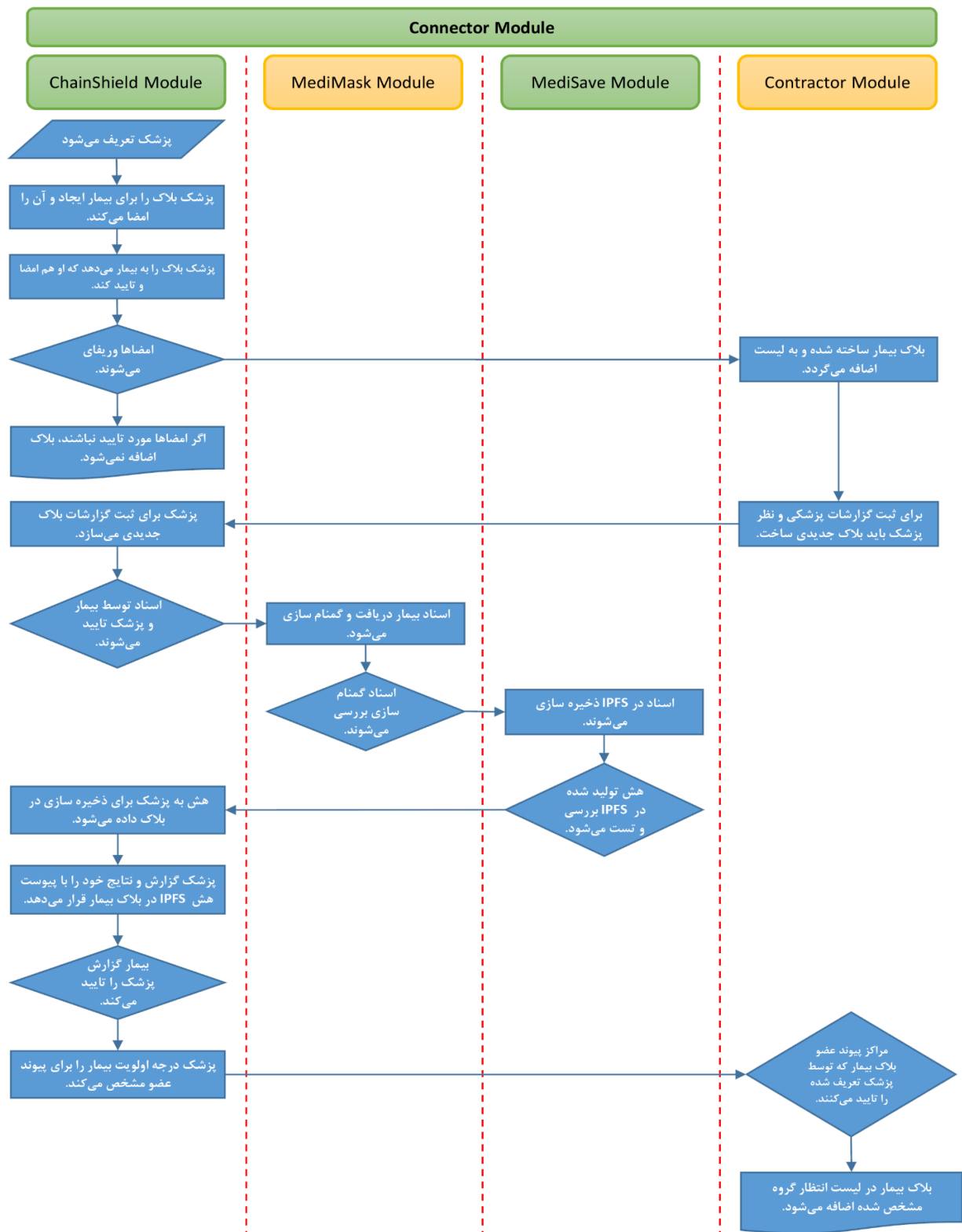


ساختار مبتنی بر قرارداد هوشمند برای اشتراک‌گذاری داده‌های بیماران، می‌تواند به عنوان یک راه حل امن و شفاف برای انتقال اطلاعات پزشکی و بهبود هماهنگی بین مراکز درمانی و نهادهای پزشکی مورد استفاده قرار گیرد. در این ساختار، یک قرارداد هوشمند برای اشتراک‌گذاری داده‌های پزشکی بین مراکز مختلف توسط پزشک بیمار ایجاد می‌شود. این قرارداد، شامل شرایط و معیارهایی است که توسط مراکز پزشکی تعیین می‌شود. در این ساختار، اطلاعات پزشکی بیماران در قرارداد هوشمند قرار می‌گیرد و تنها در صورتی که تمامی معیارها و شرایط توافق شده در قرارداد هوشمند بین مراکز پزشکی و پزشکان برآورده شود، به اشتراک گذاشته می‌شود. این معیارها و شرایط شامل اجازه دسترسی به اطلاعات پزشکی بیماران، نحوه استفاده از این اطلاعات، تضمین امنیت و حفظ حریم شخصی و محرمانگی اطلاعات پزشکی بیماران می‌باشد. در الگوریتم جدول ۴ نحوه ایجاد قرارداد هوشمند برای لیست انتظار پیوند عضو و اضافه کردن بیماران در لیست نشان داده شده است.

استفاده از Contractor به کاهش سرعت اطلاعات پزشکی، کاهش خطاهای ثبت اسناد پزشکی و کارآمدی در بخش پزشکی، بهبود امنیت و حریم شخصی بیماران و بهینه‌سازی مدیریت اطلاعات پزشکی کمک می‌کند. همچنین، این روش، تعامل بین مراکز درمانی را هماهنگ‌تر می‌کند و کیفیت درمان بهتر می‌شود، همچنین اعتماد بیماران به بخش نگهداری‌های سوابق پزشکی سازمان‌های سلامت افزایش می‌یابد.

ج) پیکربندی ساختار پیشنهادی

شکل ۶ فرآیند کلی عملکرد سامانه را نشان می‌دهد. در این ساختار ابتدا به پزشک دسترسی داده می‌شود که بتواند گیرندگان را ثبت نام کند. در مرحله نخست پزشک برای ثبت گزارش خود و اضافه کردن بیمار به لیست انتظار، ابتدا گروه انتظاری که باید بیمار در آنجا ثبت شود را مشخص و انتخاب می‌کند. سپس پزشک برای تکمیل و تأیید اطلاعات بیمار جهت امضا، بلاک را به بیمار می‌دهد که امضا کند. پس از آن که امضاها اعتبارسنجی شدند، بلاک بیمار جدید به زنجیره بلاک‌ها متصل خواهد شد. در مرحله بعد برای ثبت نظر پزشک و گزارش‌های بیمار در بلاک جدید ابتدا نیاز است که اسناد پزشکی بیمار گمنام‌سازی شود و سپس در سامانه جهت ذخیره‌سازی در IPFS بارگذاری می‌گردد. شبکه IPFS یک هش به پزشک می‌دهد و پزشک هش را در قرارداد هوشمند به همراه نظر خود در رابطه با بیمار ثبت می‌کند. بیمار هم مالکیت گزارش‌های نوشته شده توسط پزشک را تأیید می‌کند. پس از تکمیل فرآیند ثبت گزارش داده‌های بیمار و مشخص شدن درجه اولویت بیمار توسط پزشک، قرارداد هوشمند وارد فرآیند تأیید نهایی خواهد شد. برای ثبت قرارداد هوشمند در لیست انتظار پیوند، لازم است که مراکز پیوند عضو، قرارداد نوشته شده توسط پزشک را امضا کنند. سپس بیمار به لیست انتظار برای دریافت عضو اضافه می‌شود.



شکل ۶: دیاگرام نحوه ثبت بیمار توسط پزشک و اضافه شدن به لیست انتظار پیوند عضو



نتایج

برای گمنام سازی اسناد پزشکی الگوریتمی مبتنی بر SHA3 در جدول ۳ ارائه داده شد که با استفاده از آن ابتدا اطلاعات بیمار گمنام می‌شود و سپس سند پزشکی در شبکه IPFS ذخیره‌سازی می‌گردد.

جدول ۳: الگوریتم رمزنگاری SHA3 برای گمنام‌سازی داده‌های بیماران

Algorithm 1 Compute SHA-3 Hash

Require: String to be hashed: `string_to_hash`

Ensure: SHA-3 Hashed String: `hashed_string`

- 1: Initialize a SHA-3 hash object: `sha3_hash`
 - 2: Update the hash object with the input string encoded in UTF-8:
`sha3_hash.update(string_to_hash.encode('utf-8'))`
 - 3: Compute the hashed string in hexadecimal format: `hashed_string = sha3_hash.hexdigest() = 0`
-

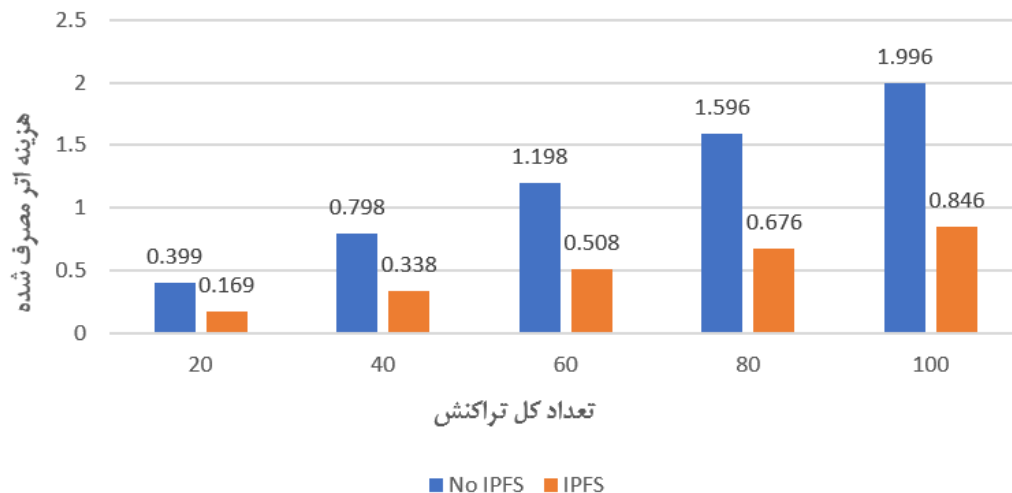
پس از گمنام‌سازی اسناد، اطلاعات بیماران در قراردادهای هوشمند ذخیره‌سازی می‌گردد. جدول ۴ الگوریتم پیاده‌سازی شده برای ایجاد، ذخیره‌سازی و مدیریت لیست انتظار بیماران پیوند را ارائه داده است.

جدول ۴: الگوریتم سیستم پیشنهادی برای قرارداد هوشمند لیست انتظار پیوند عضو

Algorithm 2 Contract Organ transplant waiting list

- 1: **Variables:**
 - 2: $PatientCount \leftarrow 0$
 - 3: $Patients$ is a mapping from *uint* to *Patient*
 - 4: **Struct List:**
 - 5: $id : uint$
 - 6: Doctor's Report : string
 - 7: $complete : bool$
 - 8: **procedure** CONSTRUCTOR
 - 9: Call ADDPATIENT with 'test Report'
 - 10: **end procedure**
 - 11: **Status:** ADDEDPATIENT with *uint* id, *string* content, *bool* complete
 - 12: **Status:** THE TRANSPLANT IS COMPLETED with *uint* id, *string* content, *bool* complete
 - 13: **procedure** ADDPATIENT($_content$: string)
 - 14: $PatientCount \leftarrow PatientCount + 1$
 - 15: $tasks[PatientCount] \leftarrow PATIENT(PatientCount, _content, false)$
 - 16: Emit ADDEDPATIENT($PatientCount, _content, false$)
 - 17: **end procedure**
 - 18: **procedure** TOGGLECOMPLETED(id : uint)
 - 19: $t \leftarrow Patients[id]$
 - 20: $t.complete \leftarrow true$
 - 21: $Patients[id] \leftarrow t$
 - 22: Emit TRANSPLANTATION WAS DONE($id, Patients[id].content, true$)
 - 23: **end procedure**
-

نگهداری اسناد حجیم پزشکی در بلاک چین از مشکلات اصلی به کارگیری شبکه بلاک چین برای مدیریت پرونده های پزشکی می باشد که در این تحقیق برای حل این چالش از شبکه IPFS استفاده شد. شکل ۴ نشان داد شد که استفاده از IPFS منجر به کاهش قابل توجه هزینه های انجام تراکنش در شبکه اتریوم منجر شده است. برای راه اندازی و انجام تراکنش در قرارداد هوشمند باید گس (Gas) صرف شود. نرخ گس، هزینه ای است که یک کاربر باید به ازای هر واحد گس پرداخت کند. نرخ گس با توجه به ازدحام شبکه تعیین می شود [۲۴]. همان طور که در شکل ۷ نشان داده شد استفاده از IPFS در آزمایش های انجام شده منجر به کاهش شدید هزینه های ذخیره سازی شد.



شکل ۷: هزینه های ذخیره سازی اسناد پزشکی در سیستم پیشنهادی با IPFS در مقابل بلاک چین

ذخیره سازی و اشتراک گذاری داده های لیست بیماران پیوندی در سیستم های متمرکز با تهدیدهای امنیتی برای نفوذ غیرقانونی، سرقت اطلاعات بدون اطلاع کاربران یا اجرای سایر اقدامات مخرب همراه است. به طور کلی استفاده از سیستم های متمرکز برای ذخیره سازی داده های محرمانه کاربران مناسب نیست، چرا که این سیستم ها امنیت بسیار پایینی دارند و همچنین مدیریت لیست انتظار پیوند در سیستم های فعلی شفافیت لازم را ندارند و باعث می شوند که انتقال عضو به صورت عادلانه بین گیرندگان با اولویت بالا تخصیص پیدا نکند. در تلاش برای حل این چالش ها و بهبود کیفیت و امنیت لیست انتظار پیوند عضو، مطالعه حاضر یک رویکرد نوین مبتنی بر فناوری بلاک چین ارائه می دهد.

بحث و نتیجه گیری

هدف این پژوهش ارائه و پیاده سازی یک سامانه امن و مقیاس پذیر برای مدیریت لیست انتظار بیماران پیوند عضو با استفاده از فناوری بلاک چین و ذخیره سازی توزیع شده است که امنیت، حریم خصوصی و عدالت در دسترسی را بهبود بخشد. این پژوهش در مقایسه با سیستم های مشابه که از فناوری بلاک چین استفاده کرده اند، با افزودن الگوریتم گمنام سازی و IPFS به عنوان بستر ذخیره سازی، مشکلات مربوط به مدیریت داده های حجیم پزشکی را نیز برطرف کرده است. به علاوه، پیوست اسناد پزشکی به لیست پیوند عضو به صورت امن و غیرقابل تغییر از دیگر مزایای این سیستم است که در مقایسه با پژوهش های قبلی برتری دارد.

همان طور که در جدول ۵ مشاهده شد، این راهکار با ارائه سیستمی غیرمتمرکز، توانایی حفظ امنیت داده ها و شفافیت را بهبود بخشیده و به ویژه در انتقال عضو، عدالت تخصیص عضو را بهبود می بخشد. فناوری بلاک چین با ویژگی هایی چون تغییرناپذیری داده ها و توزیع شده بودن، به عنوان پایه ای قوی برای ایجاد یک سیستم امن و شفاف انتقال عضو عمل می کند.

جدول ۵: مقایسه روش پیشنهادی با روش‌های مشابه

سال	مرجع	نوع شبکه بلاک چین	سکو بلاک چین	فرداد هوشمند	ذخیره سازی اسناد پزشکی	فناوری ذخیره سازی اسناد	گمنام سازی اسناد پزشکی	دسته بندی بر اساس تایپ باقت عضو در یک بلاک چین
۲۰۲۳	راه حل پیشنهادی	هایبرید	اتریوم	✓	✓	IPFS	✓	✓
۲۰۲۲	Hawashin و همکاران [۹]	خصوصی	اتریوم	✓	×	NA	×	×
۲۰۲۱	Kumar و Soni [۸]	هایبرید	اتریوم	✓	×	NA	×	×
۲۰۲۱	Yahaya و همکاران [۱۱]	خصوصی	نامشخص	✓	✓	بلاک چین	×	×
۲۰۲۰	Daniel و همکاران [۱۲]	خصوصی	اتریوم	✓	✓	IPFS	×	×
۲۰۱۹	Dajim [۷]	خصوصی	نامشخص	✓	×	NA	×	×
۲۰۱۹	Alandjani [۱۰]	عمومی	نامشخص	✓	×	NA	×	×
۲۰۱۷	Zouarhi [۶]	خصوصی	اتریوم	✓	×	NA	×	×

این پژوهش با استفاده از IPFS ذخیره سازی اسناد پزشکی که دارای حجم بالایی هستند را در سیستم های غیرمتمرکز امکان پذیر می کند. در ساختار پیشنهادی با استفاده از روش گمنام سازی برای اسناد پزشکی باعث می شود سطح محرمانگی هویت بیماران ارتقاء پیدا کنند و از حریم خصوصی بیماران محافظت خواهد شد. به علاوه، روش پیشنهادی با پیوست شدن اسناد پزشکی بیمار باعث می شود از ذخیره سازی نتایج و نسخه پیچی اشتباه برای بیماران توسط پزشکان یا مراکز درمانی کاهش یابد. در روش پیشنهادی می توان با پیوست اسناد پزشکی بیماران توسط پزشکان، آزمایشگاه ها و مراکز درمانی، خطاهای نتیجه گیری از گزارش های اشتباه پزشکی را کاهش داد. با این حال، روش پیشنهادی با چالش هایی نیز روبه رو است. اصلاح داده های پزشکی پس از ثبت در بلاک چین به دلیل ماهیت غیرقابل تغییر بودن آن، کاری دشوار و زمان بر است. همچنین، سرعت پایین ثبت داده ها به دلیل نیاز به تأیید بلاک ها توسط مراکز درمانی، ممکن است در شرایط اضطراری مشکل ساز باشد.

برای تحقیقات آینده، پیشنهاد می شود که راهکارهایی برای بهبود سرعت عمل ثبت و تطبیق داده ها و تسهیل در اصلاح اطلاعات پزشکی بررسی شود. بهبود این موارد می تواند باعث پذیرش گسترده تر این سیستم در مراکز درمانی و افزایش کارایی آن در مدیریت لیست انتظار بیماران پیوند عضو شود.

سیستم پیشنهادی می تواند به عنوان ابزاری مطمئن در دسترس تصمیم گیران قرار گیرد تا فرآیند پیوند عضو را بهبود داده و اعتماد عمومی به این فرآیند حیاتی را افزایش دهد.

در این پژوهش، با بهره گیری از فناوری بلاک چین و IPFS، روشی نوآورانه برای مدیریت لیست انتظار بیماران پیوند عضو ارائه شده است. روش پیشنهادی از طریق گمنام سازی اطلاعات بیماران و ذخیره سازی امن اسناد پزشکی، توانسته است مشکلات مربوط به حریم خصوصی و امنیت داده ها را حل کند. این رویکرد با استفاده از ساختار غیرمتمرکز، امکان دستکاری و سوء استفاده از اطلاعات حساس بیماران را به حداقل می رساند. پژوهش حاضر با ارائه ساختاری امن و مقیاس پذیر، توانسته است نیازهای مهمی از جمله حفظ حریم خصوصی و عدالت در فرآیند پیوند عضو را پاسخ دهد. با استفاده از این سیستم، بیماران و اهداکنندگان می توانند با اعتماد بیشتری در این فرآیند مشارکت کنند و از صحت و امنیت اطلاعات خود اطمینان حاصل نمایند.

تعارض منافع

نویسندگان تأیید می کنند که تعارض منافع وجود ندارد.

حمایت مالی

این کار در قالب پایان نامه کارشناسی ارشد دانشگاه صنعتی ارومیه انجام شده است و فاقد حمایت مالی می باشد.

کد اخلاق

دانشگاه های صنعتی فاقد فرایند صدور کد اخلاق می باشند. پروپوزال پایان نامه مرتبط در مدیریت امور پژوهشی دانشگاه صنعتی ارومیه در تاریخ ۱۴۰۲/۰۱/۱۹ به شماره ۸۶۱۰۲/۳۵۵ مصوب گردیده است.

سهام مشارکت نویسندگان

تمامی نویسندگان در بخش های مختلف فعالیت داشته و از سهم مساوی برخوردار می باشند.

References

- [1]. Fishman JA. Infection in organ transplantation. American Journal of Transplantation 2017;17(4):856-79. <https://doi.org/10.1111/ajt.14208>
- [2]. Merrill JP, Murray JE, Harrison JH, Guild WR. Successful homotransplantation of the human kidney between identical twins. Journal of the American Medical Association 1956;160(4):277-82.
- [3]. LI PK, Chu KH, Chow KM, Lau MF, Leung CB, Kwan BC, et al. Cross sectional survey on the concerns and anxiety of patients waiting for organ transplants. Nephrology 2012;17(5):514-8. <https://doi.org/10.1111/j.1440-1797.2012.01615.x>
- [4]. Haleem A, Javaid M, Singh RP, Suman R, Rab S. Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks 2021;2:130-9. <https://doi.org/10.1016/j.ijin.2021.09.005>
- [5]. Tagde P, Tagde S, Bhattacharya T, Tagde P, Chopra H, Akter R, et al. Blockchain and artificial intelligence technology in e-Health. Environ Sci Pollut Res Int 2021;28(38):52810-31. doi: 10.1007/s11356-021-16223-0
- [6]. Zouarhi S. Kidner – A Worldwide Decentralised Matching System for Kidney Transplants. Journal of the International Society for Telemedicine and EHealth 2017; 5:e62:1-4.
- [7]. Dajim LA, Al-Farras SA, Al-Shahrani BS, Al-Zuraib AA, Mathew RM. Organ donation decentralized application using blockchain technology. 2nd International Conference on Computer Applications & Information Security (ICCAIS); 2019 May 1-3; Riyadh, Saudi Arabia: IEEE; 2019. p. 1-4. doi: 10.1109/CAIS.2019.8769459
- [8]. Soni A, Kumar SG. Creating organ donation system with blockchain technology. European Journal of Molecular & Clinical Medicine 2021;8(03):2021.
- [9]. Hawashin D, Jayaraman R, Salah K, Yaqoob I, Simsekler MC, Ellahham S. Blockchain-based management for organ donation and transplantation. IEEE Access 2022;10:59013-25. doi: 10.1109/ACCESS.2022.3180008
- [10]. Alandjani G. Blockchain based auditable medical transaction scheme for organ transplant services. 3C Tecnología 2019;31(2):41-63.
- [11]. Yahaya CA, Firdaus A, Khen YY, Yaakub CY, Abd Razak MF. An Organ Donation Management System (ODMS) based on Blockchain Technology for Tracking and Security Purposes. International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM); 2021 Aug 24; Pekan, Malaysia: IEEE; 2021. p. 377-82. doi: 10.1109/ICSECS52883.2021.00075
- [12]. Daniel IA, Pop C, Anghel I, Antal M, Cioara T. A blockchain based solution for managing transplant waiting lists and medical records. 16th International Conference on Intelligent Computer Communication and Processing (ICCP) 2020 Sep 3-5; Cluj-Napoca, Romania: IEEE; 2020. p. 505-10. doi: 10.1109/ICCP51029.2020.9266214
- [13]. Kiani M, Abbasi M, Ahmadi M, Salehi B. Organ transplantation in Iran; current state and challenges with a view on ethical consideration. J Clin Med 2018;7(3): 45. <https://doi.org/10.3390/jcm7030045>
- [14]. Kumari S, Dixit T, Prakash P, Sharma V. Public Fund Care Tracking System based on Blockchain. 2nd Asian Conference on Innovation in Technology (ASIANCON); 2022 Aug 26; Ravet, India: IEEE; 2022. p. 1-5. doi: 10.1109/ASIANCON55314.2022.9908651
- [15]. Hussien HM, Yasin SM, Udzir NI, Ninggal MI, Salman S. Blockchain technology in the healthcare industry: Trends and opportunities. Journal of Industrial Information Integration 2021;22:100217. <https://doi.org/10.1016/j.jii.2021.100217>
- [16]. Wu K. An empirical study of blockchain-based decentralized applications. arXiv preprint arXiv:1902.04969. 2019. <https://doi.org/10.48550/arXiv.1902.04969>



- [17]. Johari R, Kumar V, Gupta K, Vidyarthi DP. BLOSOM: BLockchain technology for Security of Medical records. ICT Express 2022;8(1):56-60. <https://doi.org/10.1016/j.ict.2021.06.002>
- [18]. Wu H, Dwivedi AD, Srivastava G. Security and privacy of patient information in medical systems based on blockchain technology. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM). 2021;17(2s):1-7. <https://doi.org/10.1145/3408321>
- [19]. Azbeg K, Ouchetto O, Andaloussi SJ. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egyptian Informatics Journal 2022;23(2):329-43. <https://doi.org/10.1016/j.eij.2022.02.004>
- [20]. Kumar R, Marchang N, Tripathi R. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. International Conference on Communication Systems & Networks (COMSNETS) 2020 Jan 7-11; Bengaluru, India: IEEE; 2020. p. 1-5. doi: 10.1109/COMSNETS48256.2020.9027313
- [21]. Olatunji IE, Rauch J, Katzensteiner M, Khosla M. A review of anonymization for healthcare data. Big Data 2022. doi: 10.1089/big.2021.0169
- [22]. Long S. A comparative analysis of the application of hashing encryption algorithms for MD5, SHA-1, and SHA-512. Journal of Physics Conference Series 2019;(1):012210. doi:10.1088/1742-6596/1314/1/012210
- [23]. Nishi FK, Shams-E-Mofiz M, Khan MM, Alsufyani A, Bourouis S, Gupta P, et al. [Retracted] Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. Journal of Sensors 2022;2022(1):7299185. <https://doi.org/10.1155/2022/7299185>
- [24]. Koutmos D. Network activity and ethereum gas prices. J. Risk Financial Manag 2023;16(10): 431. <https://doi.org/10.3390/jrfm16100431>