بسم الله الرحمن الرحیم

اولین همایش ملی هوش مصنوعی و محاسبات نرم در علوم انسانی (AISCH-2019)
دانشگاه علامه طباطبائی- تهران، ایران

ارائه یک راهکار بومی برای حفظ حریم خصوصی در پرونده الکترونیک سلامت با استفاده از فن آوری زنجیره بلوک و قراردادهای هوشمند

پژوهشگران:

عزیز صداقت، نیلوفر مظفری، علی حمزه

آبان ۱۳۹۸

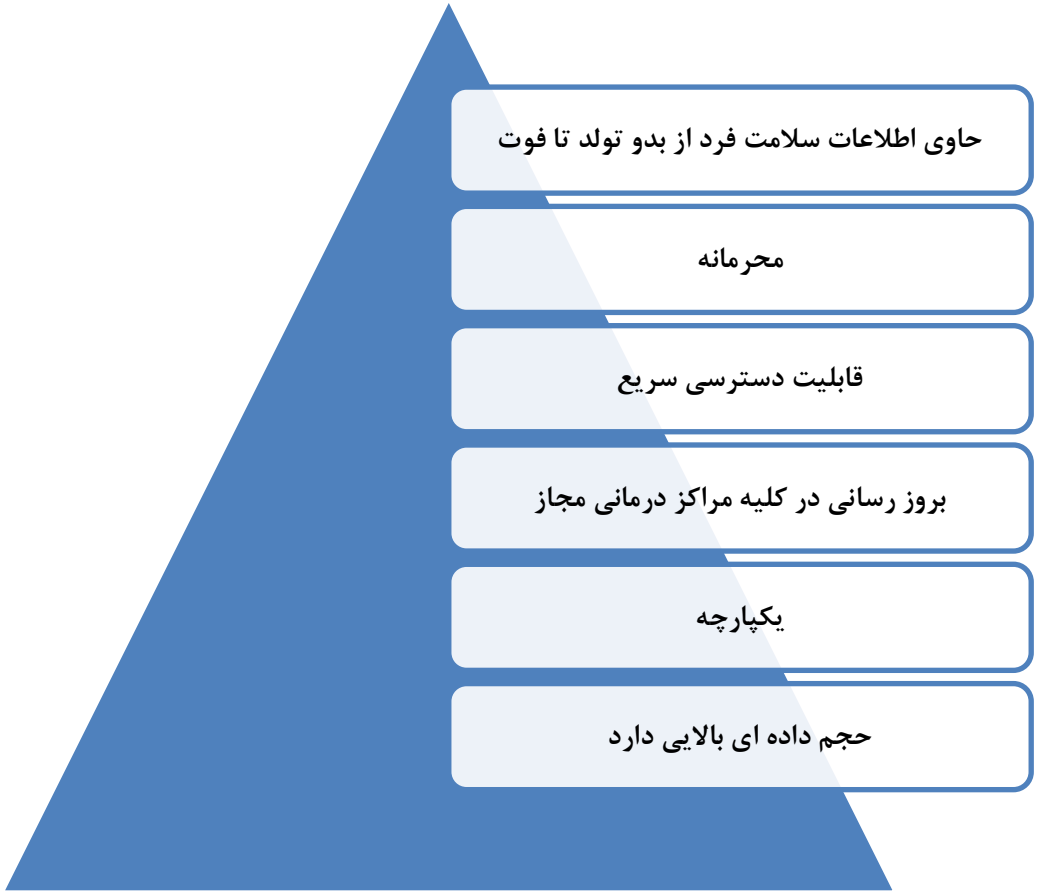
عناوین

- مقدمه
- تعریف مساله
- پیشینه پژوهشی
- روش پیشنهادی
- بحث
- جمع بندی و کار آینده

پرونده الکترونیک سلامت

چکیده خواص پرونده الکترونیک سلامت طبق تعاریف:

- سازمان بهداشت جهانی
- مکلندون و همکاران
- صیدی و همکاران



مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

حریم خصوصی؛ یک الزام در پرونده الکترونیک سلامت

مقدمه

تعریف مساله

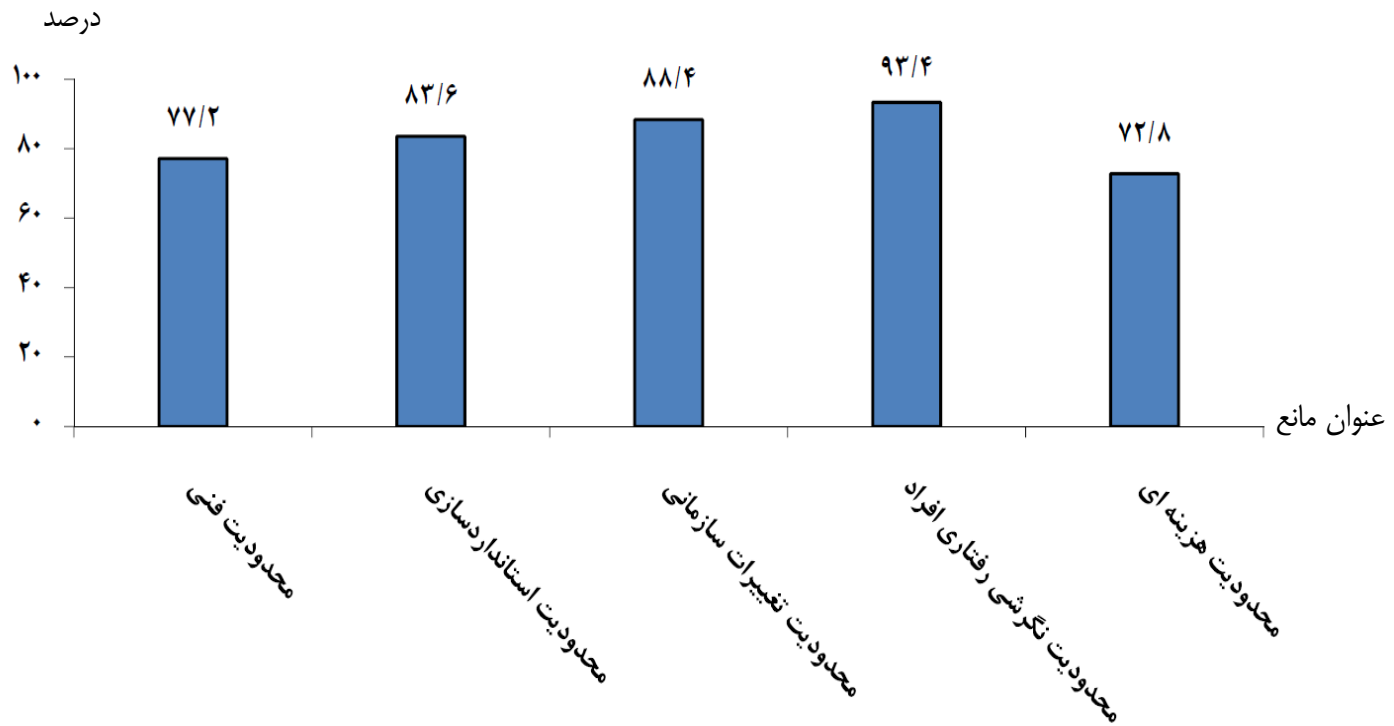
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

نتایج پژوهش جبراییلی و همکاران در خصوص موانع تحقق پرونده الکترونیک سلامت در ایران



عدم رعایت حریم خصوصی یکی از مصادیق محدودیت های رفتاری؛
دغدغه ۸۶,٤٪ جامعه پژوهشی

حریم خصوصی؛ یک الزام در پرونده الکترونیک سلامت

مقدمه

تعریف مساله

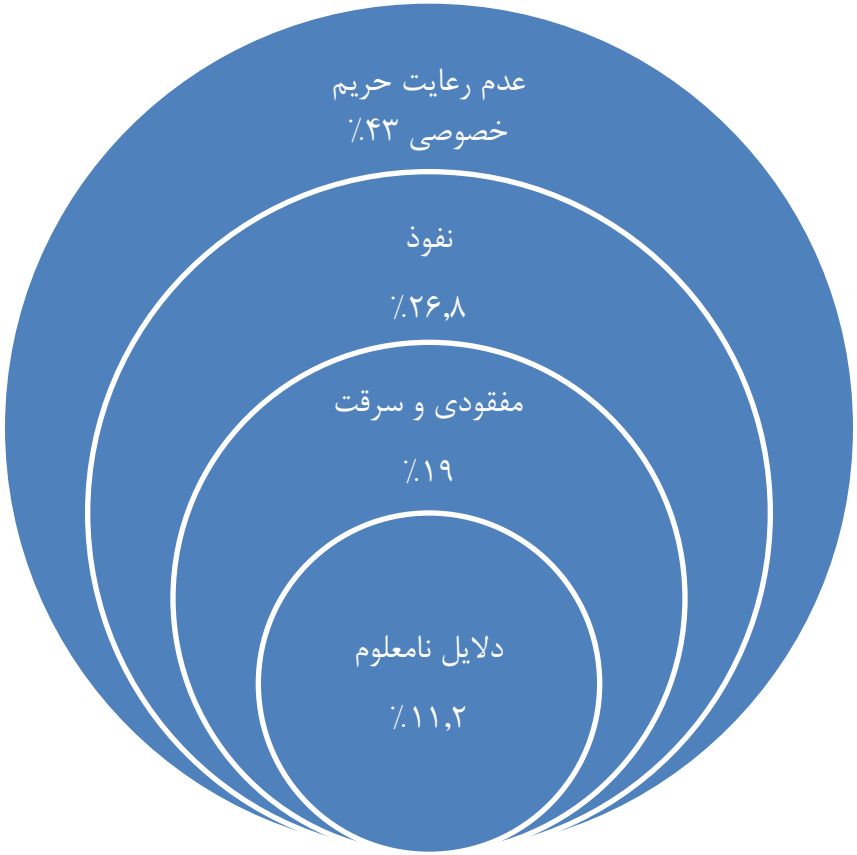
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

رخدادهای منجر به شکست حفاظتی داده های بیماران در سال ۲۰۱۶



گزارش موسسه Protenus

یکپارچگی پرونده سلامت؛ چالش مهم پیاده سازی

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

چالش های یکپارچگی پرونده سلامت		
پراکندگی جغرافیایی مراکز درمانی	بروزرسانی	هزینه

اظهارات متعدد مقامات وزارت بهداشت و درمان کشور بیانگر وجود این چالش هاست

صورت مساله

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

سیستم PIMED

Privacy and **I**ntegrity Management of Electronic **MED**ical Records using Blockchain Technology

راهکاری منطبق بر قوانین ایران

جهت غلبه بر چالش حریم خصوصی
و
یکپارچگی پرونده الکترونیک سلامت

برپایه زنجیره بلوک و قراردادهای هوشمند

فعالیتهای مرتبط

ژنگ (۲۰۱۸)	•موارد کاربرد زنجیره بلوک در حوزه سلامت
کلاوسن (۲۰۱۸)	•کاربرد بلاکچین در زنجیره تامین صنعت سلامت
کئو (۲۰۱۷)	•دلایل برتری بلاکچین بر سایرگزینه ها برای سیستم غیرمتمرکز سلامت
ماتیو هوی (۲۰۱۷)	•قابلیت زنجیره بلوک در زنجیره تامین دارو
متلر (۲۰۱۶)	•قابلیتهای زنجیره بلوک در حوزه درمان
لین(۲۰۱۶)	•گستردن حوزه داده های ورودی پرونده به سنسورهای پوشیدنی سلامت •ایده دادن جهت استفاده از زنجیره بلوک در حوزه تحقیقات پزشکی
الکساندر سامارین (۲۰۱۶)	•ذخیره پرونده در ابر •دسترسی تنها توسط بیمار
کالور(۲۰۱۷)	•مبتنی بر زنجیره بلوک •فقط بیماران و ارائه دهندگان حضور دارند
MedRec (2016)	•راهکاری برای حفظ حریم خصوصی با استفاده از زنجیره بلوک •قراردادهای هوشمند
Ancile (2018)	•راهکاری برای حفظ حریم خصوصی با استفاده از زنجیره بلوک •قراردادهای هوشمند

یافته های مشترک در MedRec و Ancile

مقدمه

تعریف مساله

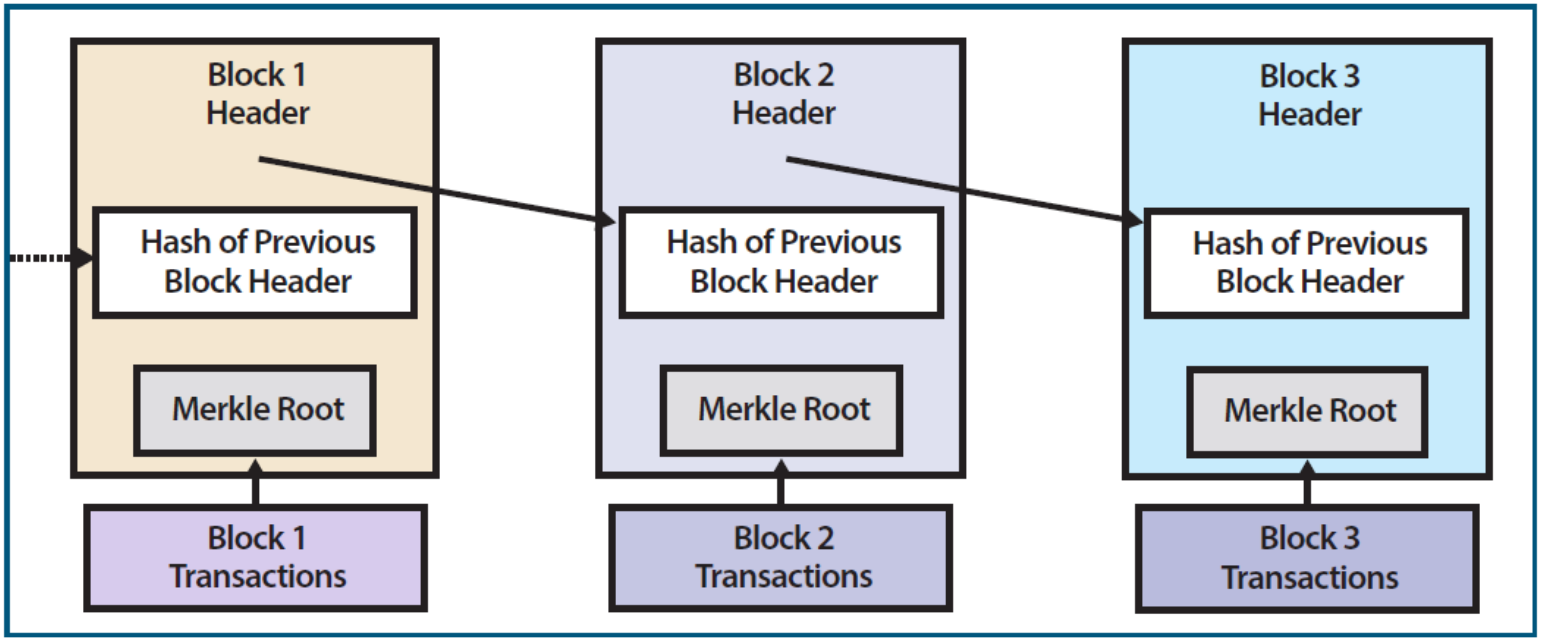
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

زنجیره بلوک



کپی نسخه واحد در کل گره ها

دفترکل توزیع شده

نظیر به نظیر

زیرساخت کلیدعمومی

کاربردهای تراکنشی

استخراج رمزارز

براساس مقاله S. Nakamoto

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

بیت کوین

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

- ✓نخستین رمزارز دیجیتال
- ✓معرفی در سال ۲۰۰۹
- ✓مبتنی بر زنجیره بلوک
- ✓حذف بانک از تراکنشات مالی
- ✓تایید تراکنشات مالی توسط همگان
- ✓شفافیت تراکنشات

براساس مقاله S. Nakamoto

اتریوم

- ✓ دومین ارز دیجیتال پلتفرم بزرگ بازار بـا هـدف هوشـمند سـازی فراینـدها و فضایی برای اجرا برنامه های غیرمتمرکز و خودکار
- ✓در سال ۲۰۱۵ به سرپرستی ویتالیک بوترین معرفی شد
- ✓یک زنجیره بلوک خصوصی درعین داشتن خواص عمومی زنجیره بلوک
- ✓تعداد محدودی از گره ها اجازه استخراج یا تغییر و یا خواندن زنجیره بلـوک را دارند

براساس مقاله V. Buterin

مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

مقایسه بیت کوین و اتریوم

پارامتر	بیت کوین	اتریوم
محدودیت سکه	۲۱ میلیون	نامحدود
پرتکل زنجیره بلوک	اثبات انجام کار	اثبات انجام کار
موارد استفاده	ارز دیجیتالی	ارز دیجیتالی – قرارداد هوشمند
حریم خصوصی	بالا	بالا
اسم و واحد ارز	بیت-کوین	اتر
نماد ارز	BTC	ETH
الگوریتم هش	SHA-256	ETHASH
زمان تولید بلوک	حداقل ۱۰ دقیقه	حدود ۱۴ ثانیه
استخراج	استخراج کننده ASIC	GPU + CPU

مقدمه

تعریف مساله

پیشینه پژوهشی

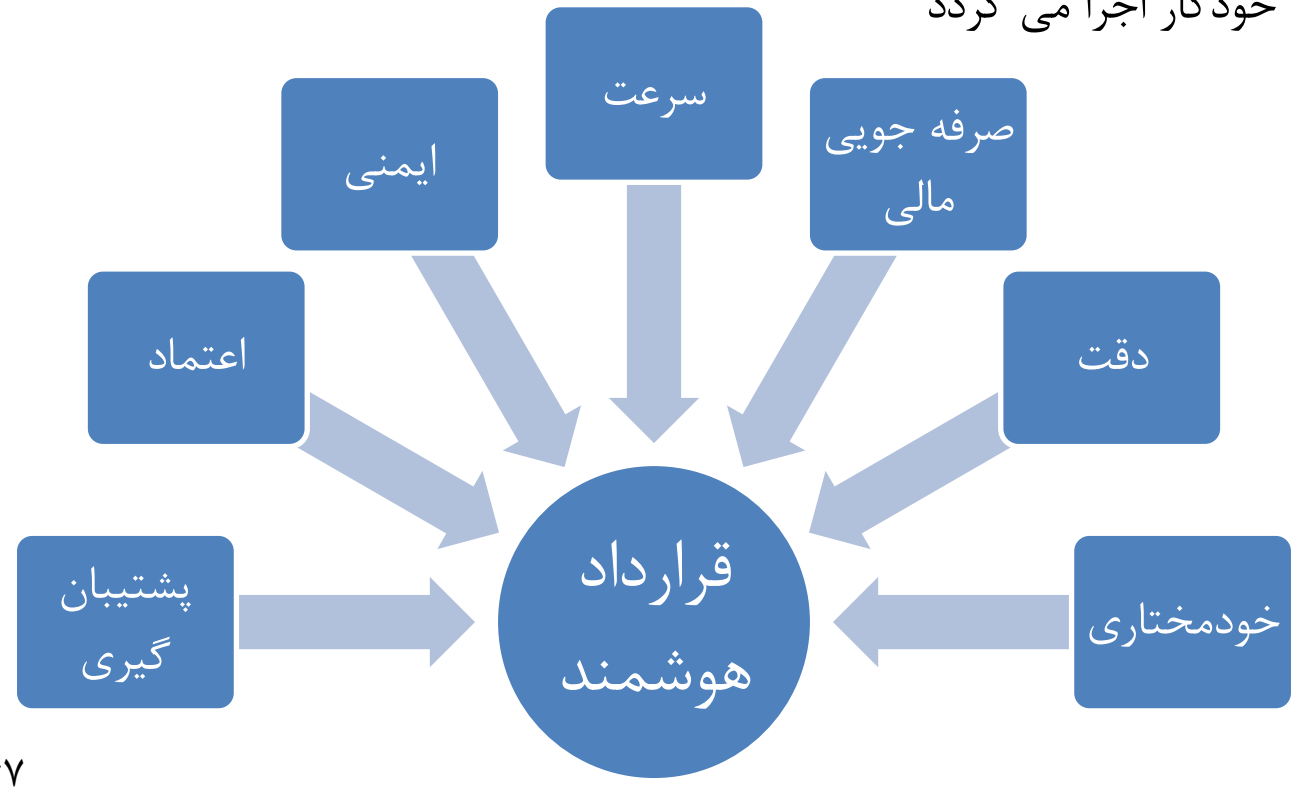
روش پیشنهادی

بحث

جمع بندی

قرارداد هوشمند

- ✓یک قرارداد هوشمند، یک پروتکل ویژه است که برای مشارکت، تأیید یا اجرای مفاد یک قرارداد خاص، فعال می شود
- ✓ماهیت قرارداد هوشمند اسکریپتی است که تحت برقراری شرایط خاص بطور خودکار اجرا می گردد



مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

زنجیره بلوک؛ انتخابی مناسب در بین گزینه های غیرمتمرکز

نظیر به نظیر بودن	• استقلال بیمار و ارائه دهنده
تغییرناپذیری	• دفترکل فقط خواندنی • مناسب جهت دعاوی بیمه
قابلیت دسترسی	• انتشار کپی پرونده در کل گره ها
امنیت و محرمانگی	• الگوریتم های رمزنگاری
یکپارچگی	• هش داده ها

یافته های پژوهش Kuo و همکاران

مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

مفروضات

مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

- زنجیره بلوک پیشنهادی، اتریوم است چون خصوصیات امن تری را با توجه به امکان خصوصی سازی آن نسبت به سایر زنجیره های بلوک در اختیار قرار می نهد.

- بیماران و ارائه کنندگان کیف پول اتریوم را بر روی دستگاه خود نصب نموده اند (بدین طریق همگی دارای آدرس اتریوم هستند)

- قوانین استفاده شده در این سیستم، برگرفته از منشور حقوق بیمار در ایران و راهنمای عمومی اخلاق حرفه‌ای اعضای سازمان نظام پزشکی می باشد.

قانون HIPAA

مقدمه

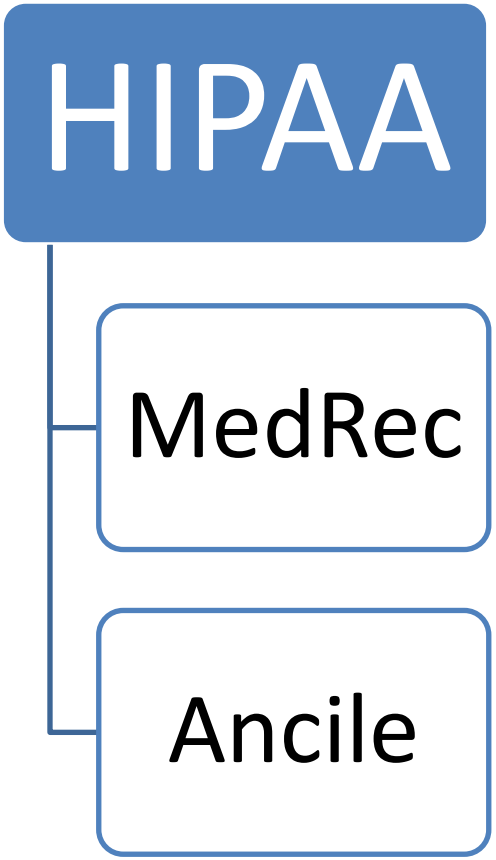
تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

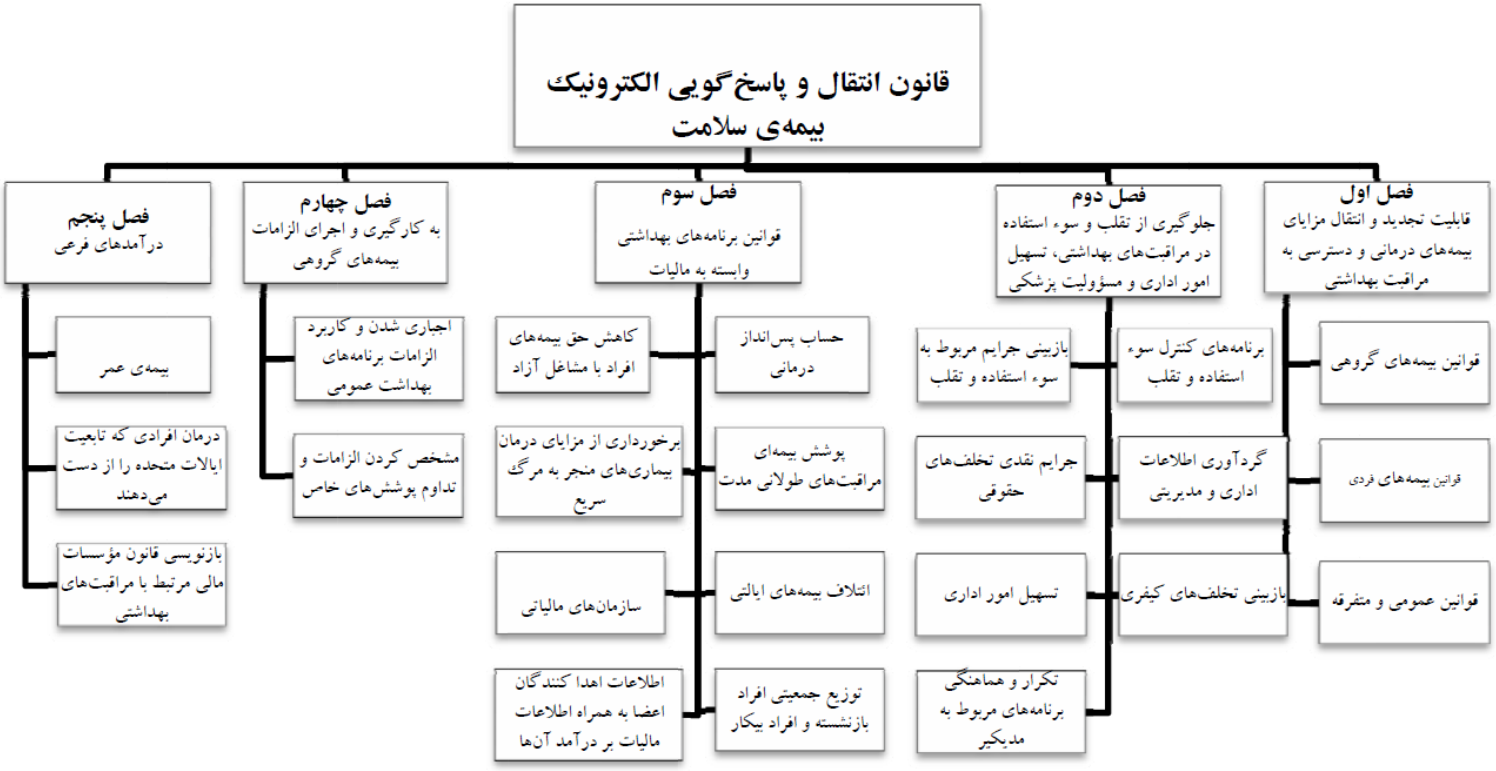
بحث

جمع بندی



قانون انتقال و پاسخ گویی الکترونیک بیمه ی سلامت آمریکا

قانون HIPAA



مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

قوانین رعایت حریم خصوصی بیماران در ایران

مقدمه

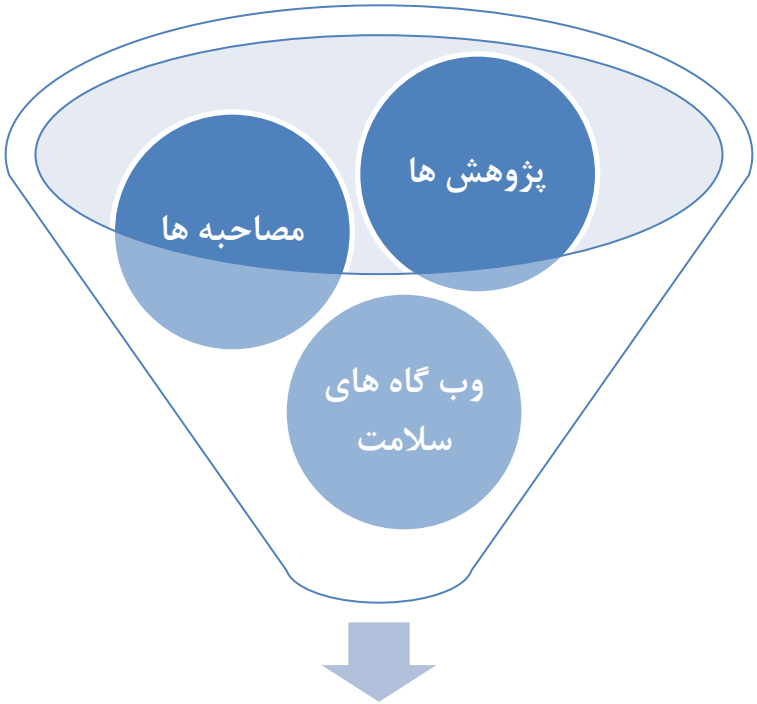
تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی



منشور حقوق بیمار + راهنمای اخلاق حرفه ای سازمان نظام پزشکی

قوانین رعایت حریم خصوصی بیماران در ایران

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

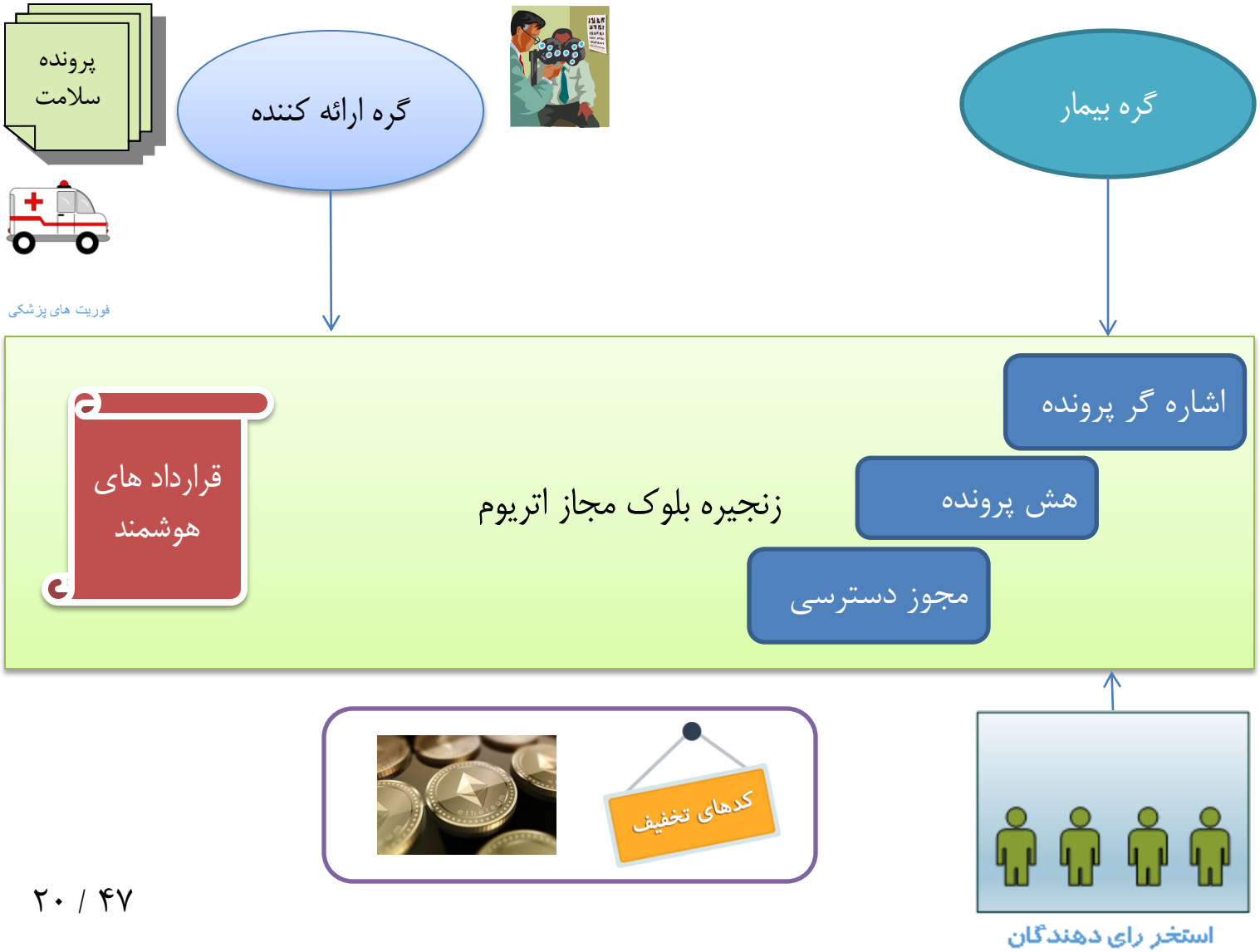
منشور حقوق بیماران

- بکارگیری کلیه امکانات جهت رعایت حریم خصوصی بیماران
- دسترسی به داده ها صرفا محدود به بیمار و افرادی که در قانون مجاز شمرده شده اند
- حق بیمار برای همراهی شخص معتمد(مثلا والدین کودک) محفوظ است

سازمان نظام پزشکی

- محدوده حریم خصوصی شامل اطلاعات حساس و غیر حساسی است که به هر شکل در مراحل مختلف تشخیصی و درمانی جمع آوری می‌شود
- افراد صرفا به دلیل پزشک بودن یا عضویت در زمره حرفه‌مندان پزشکی برای دسترسی به اطلاعات بیماران مجاز شمرده نمی‌شوند.
- در موارد خاص، بیمار تا جایی که امکان دارد باید در جریان الزام قانونی نقض اصل رازداری قرار گیرد و سپس اطلاعات از وی دریافت شود

شماتیک کلی سیستم PIMED



مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

گره های سیستم PIMED

مدیر پایگاه داده: یک واسط برای اجرا کردن پرس و جو بر روی پایگاه ارائه کننده پس از کنترل مجوز دسترسی درخواست دهنده، ذخیره اطلاعات پرونده شخصی در سمت پایگاه داده محلی بیمار

کلاینت اتریوم: اتصال به شبکه نظیر به نظیر، رمزگذاری و ارسال تراکنش ها، تایید تراکنش ها و نگهداری یک کپی محلی تاییدشده زنجیره بلوک

برنامه کاربردی کاربر:
نسخه بیمار بازیابی اطلاعات، دریافت درخواستهای دسترسی به پرونده و نمایش برای بیمار، ارائه امکانات به اشتراک گذاری داده ها و امکانات جستجو
نسخه ارائه دهنده برنامه کاربردی رابط کاربر، قادر به ثبت و بازیابی اطلاعات، دریافت درخواستهای دسترسی به پرونده و نمایش برای ارائه دهنده و امکانات جستجو

قراردادهای هوشمند PIMED

قرارداد فوریت های پزشکی
- خصوصی

قرارداد پرونده
- خصوصی

قرارداد سابقه
- خصوصی

قرارداد ثبت نام
- عمومی

قرارداد اجماع
- عمومی

مقدمه

تعریف مساله

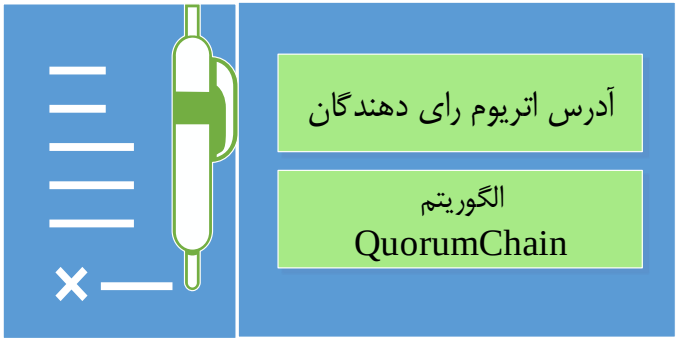
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

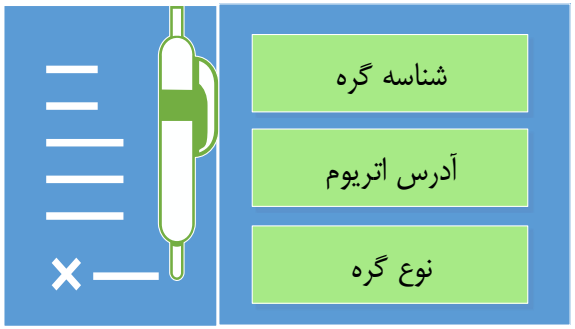
قرارداد اجماع



- ذخیره آدرس های اتریوم گره هاییکه اجازه رای برای استخراج دارند
- دخالت مستقیم در فرآیندهای استخراج و ثبت نام
- حصول اطمینان از مجاز بودن گره های ثبت نام کننده
- امکان اعمال سیاست گذاریهای وزارت بهداشت

مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

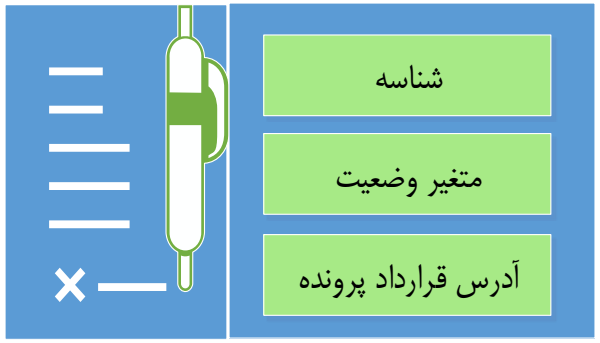
قرارداد ثبت نام



- ثبت اطلاعات گره بیمار یا ارائه کننده خدمات درمانی
- مقادیر عنصر نوع: بیمار و ارائه دهنده
- جلوگیری از ثبت نام دوگانه
- حذف فرآیند اجماع در ارجاعات بعدی به گره ها

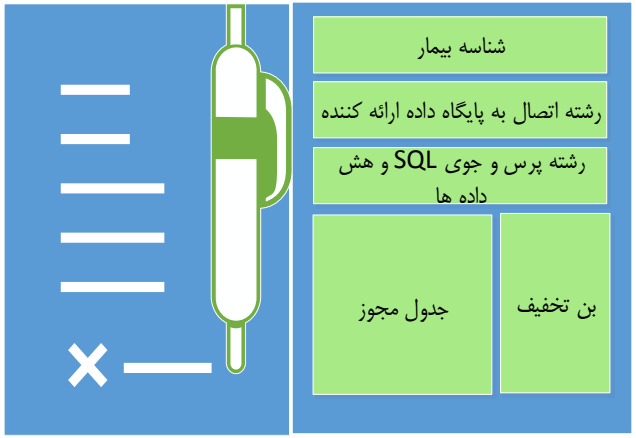
مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

قرارداد سابقه



- مسئول نگهداری سوابق مراجعات بیمار به ارائه کنندگان خدمات درمانی و بالعکس
- مقادیر عنصر وضعیت : انتظار، تایید و مردود
- بیمار مدام متغیر وضعیت خود را چک می کند و بمحض بروزرسانی آگاه می شود

قرارداد پرونده



❖نگهداری ارجاعات و آدرس محل اصلی نگهداری پرونده، مجوزهای دسترسی، هش رکورد مربوطه و نیز یک بن تخفیف استفاده از خدمات درمانی ارائه دهنده برای استخراج کننده بلوک

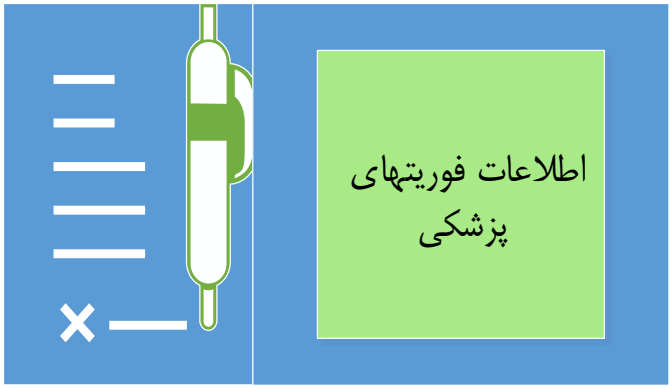
❖ارائه دهنده مخیر است در مواردیکه آگاهی بیمار از اطلاعات پزشکی اش براساس قانون برای وی مضر باشد، در قسمت شرط پرس و جو اطلاعات ممنوعه را فیلتر نماید

❖مقداردهی اولیه جدول مجوز:

شناسه	رشته پرس و جو	سطح دسترسی
شناسه بیمار	رشته کامل با فیلتر موارد خاص	مالکیت
شناسه ارائه کننده	رشته کامل بدون شرط	خواندن/نوشتن

مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

قرارداد فوریت های پزشکی



- اطلاعات آن توسط بیمار تکمیل می گردد(حیطه اطلاعات فوریت پزشکی را بیمار تعیین می نماید)
- اطلاعات با کلید K_EMRG بصورت متقارن رمز شده اند
- رمز کردن داده و ارسال به این قرارداد مشترکا توسط مدیر برنامه های کاربردی و کلاینت اتریوم گره بیمار انجام می شود
- قرارداد فوریت های پزشکی برای هر گره بیمار در زمان افزوده شدن به سیستم ایجاد می گردد اما به روزرسانی آن توسط خود بیمار انجام می گردد
- وزارت بهداشت آدرس قرارداد فوریت های پزشکی، کلید K_EMRG منتسب به آن بهمراه کدملی و اثر انگشت بیمار را در قالب یک جدول در اختیار مدیر پایگاه داده کلیه مراکز فوریت های پزشکی قرار می دهد

انواع تراکنشات PIMED

مقدمه

تعریف مساله

پیشینه پژوهشی

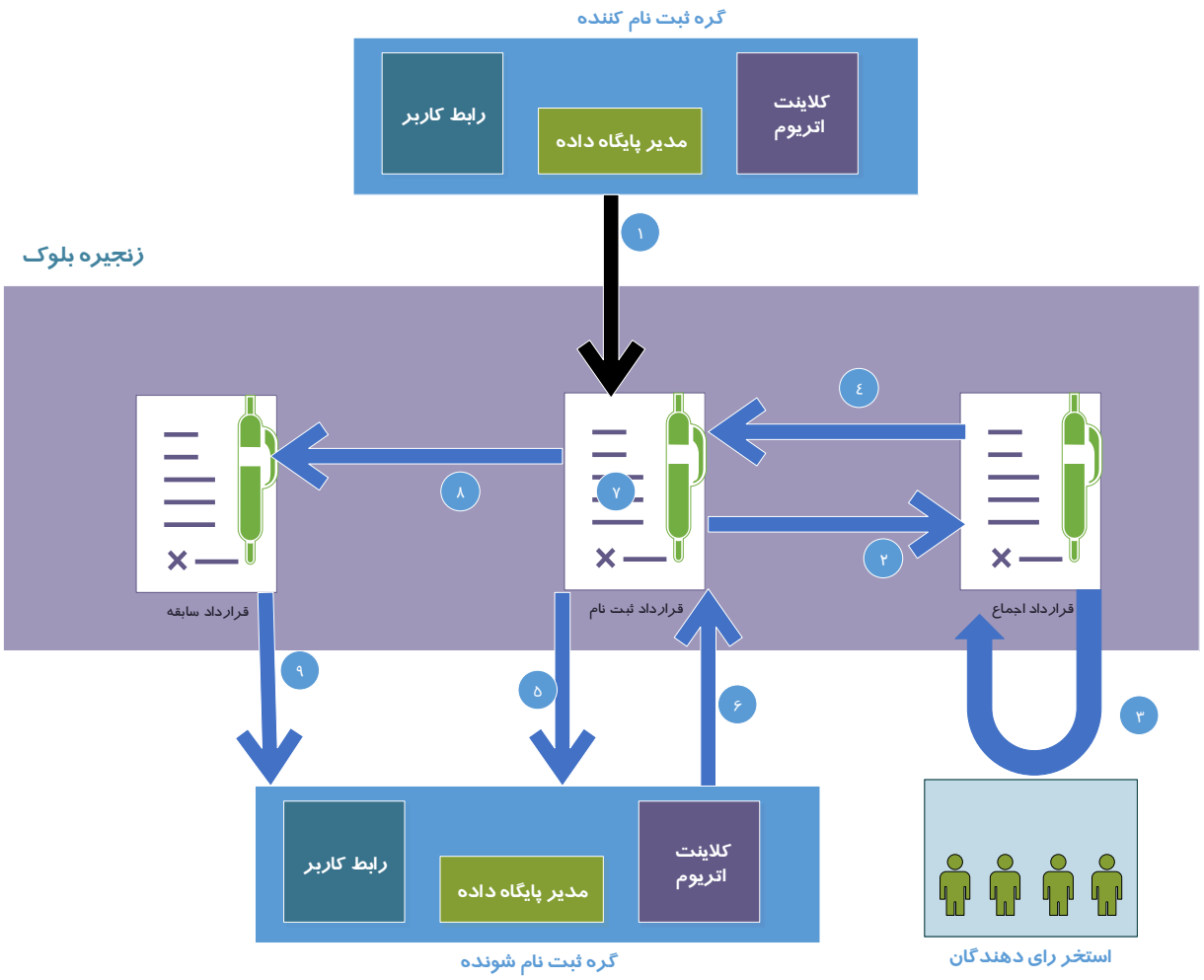
روش پیشنهادی

بحث

جمع بندی

تراکنش عادی	Eth_Call	تراکنش داخلی
•باید توسط بازیگر خارجی ارسال گردد •در زنجیره بلوک ذخیره می شود	•تنها توسط گره های محلی اجرا می گردند •در زنجیره بلوک ذخیره نمی شود	• تراکنشات بین قراردادهای هوشمند • در زنجیره بلوک ذخیره نمی شود

فرآیندها : افزودن گره جدید



مقدمه

تعریف مساله

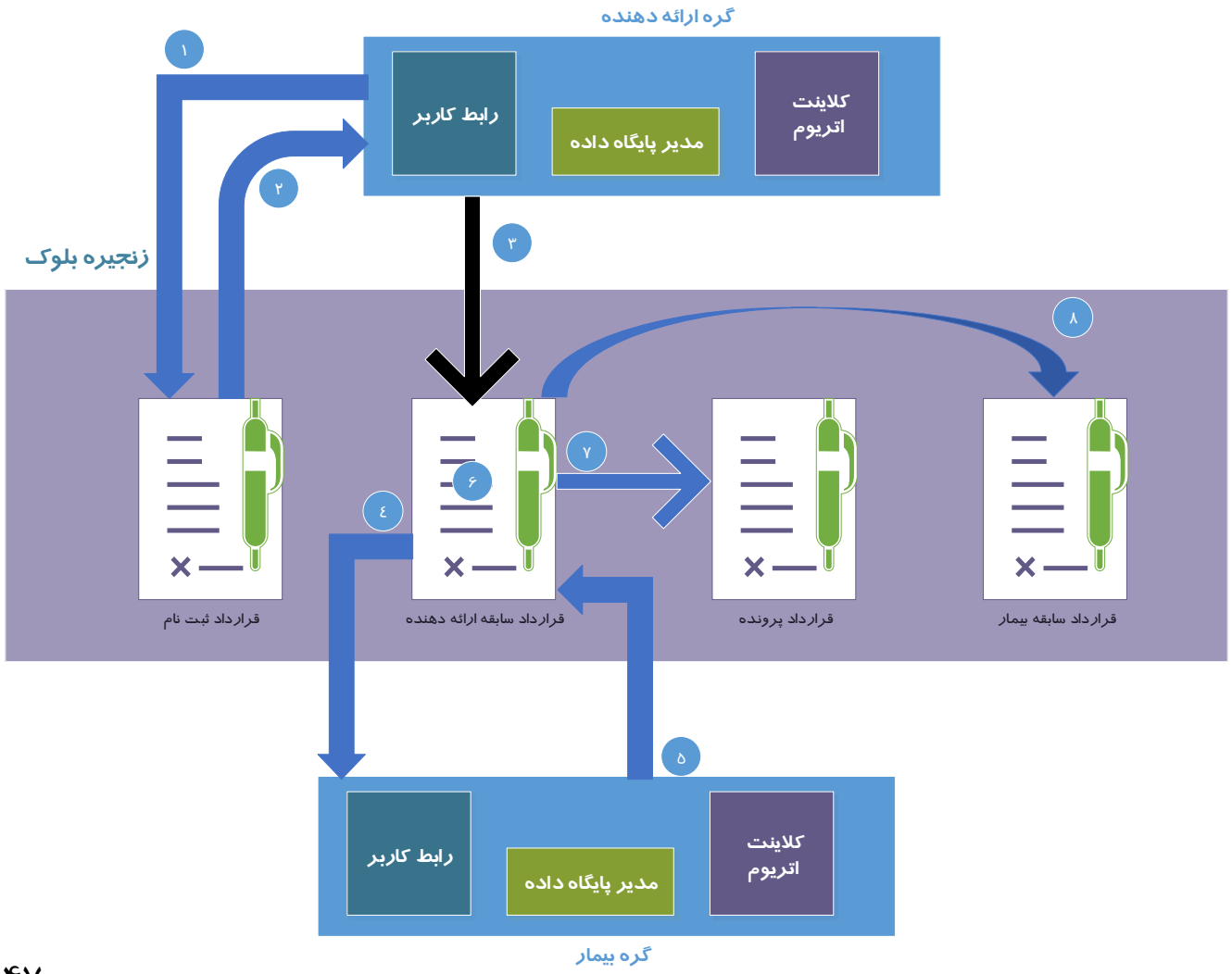
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

فرآیندها : ثبت نام (ایجاد پرونده)



مقدمه

تعریف مساله

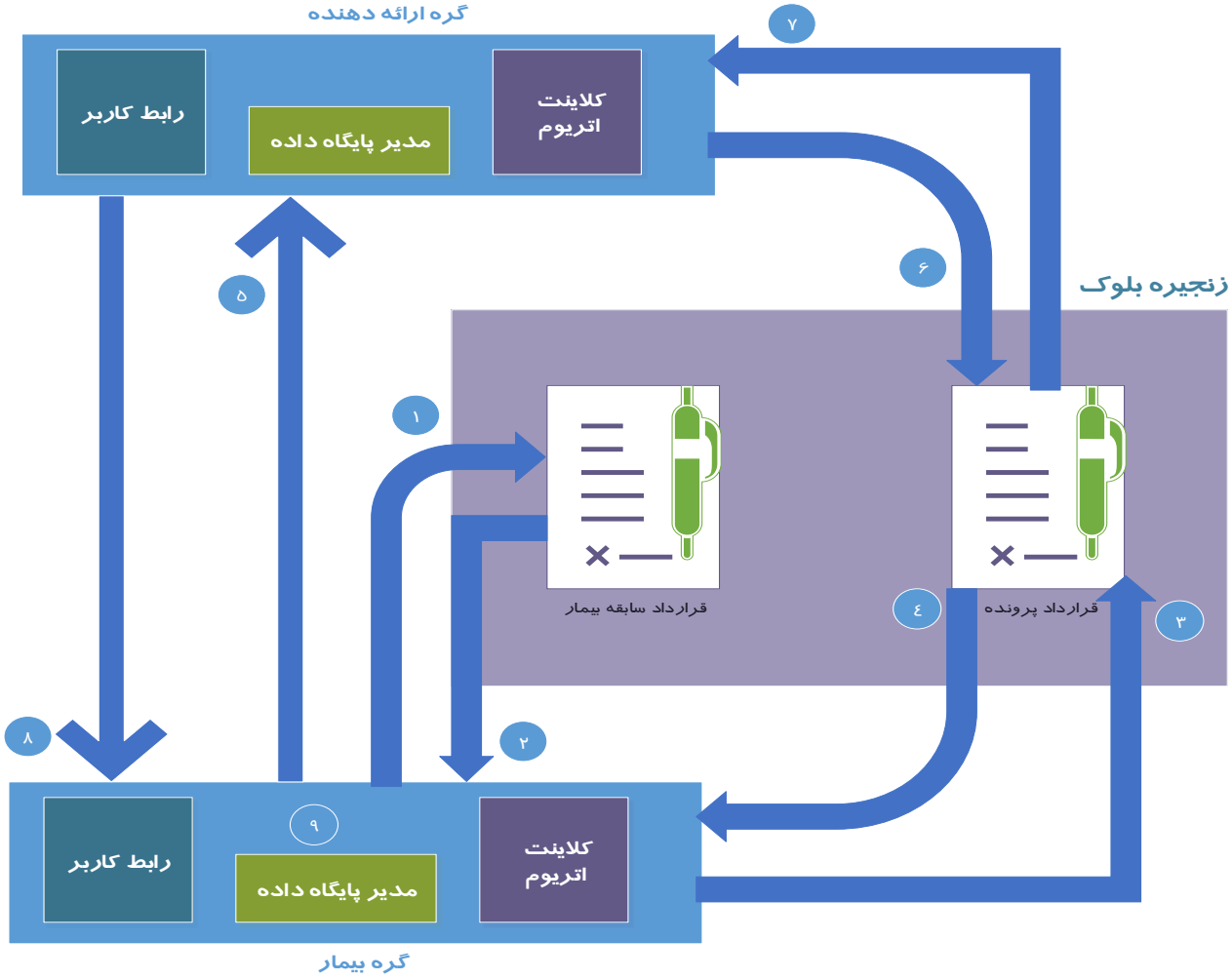
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

فرآیندها : دستیابی به اطلاعات پرونده



مقدمه

تعریف مساله

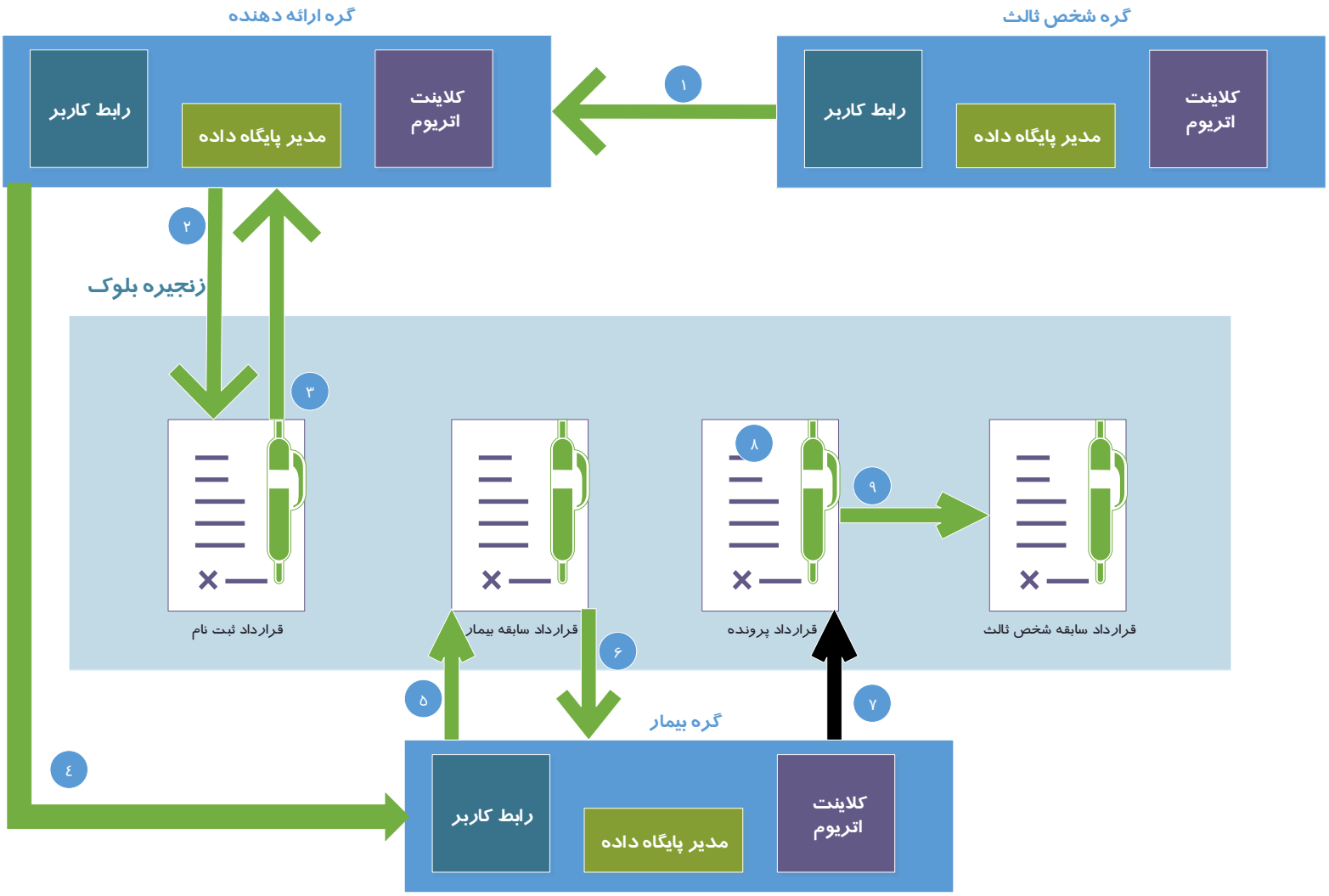
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

فرآیندها : اعطای مجوز به شخص ثالث



مقدمه

تعریف مساله

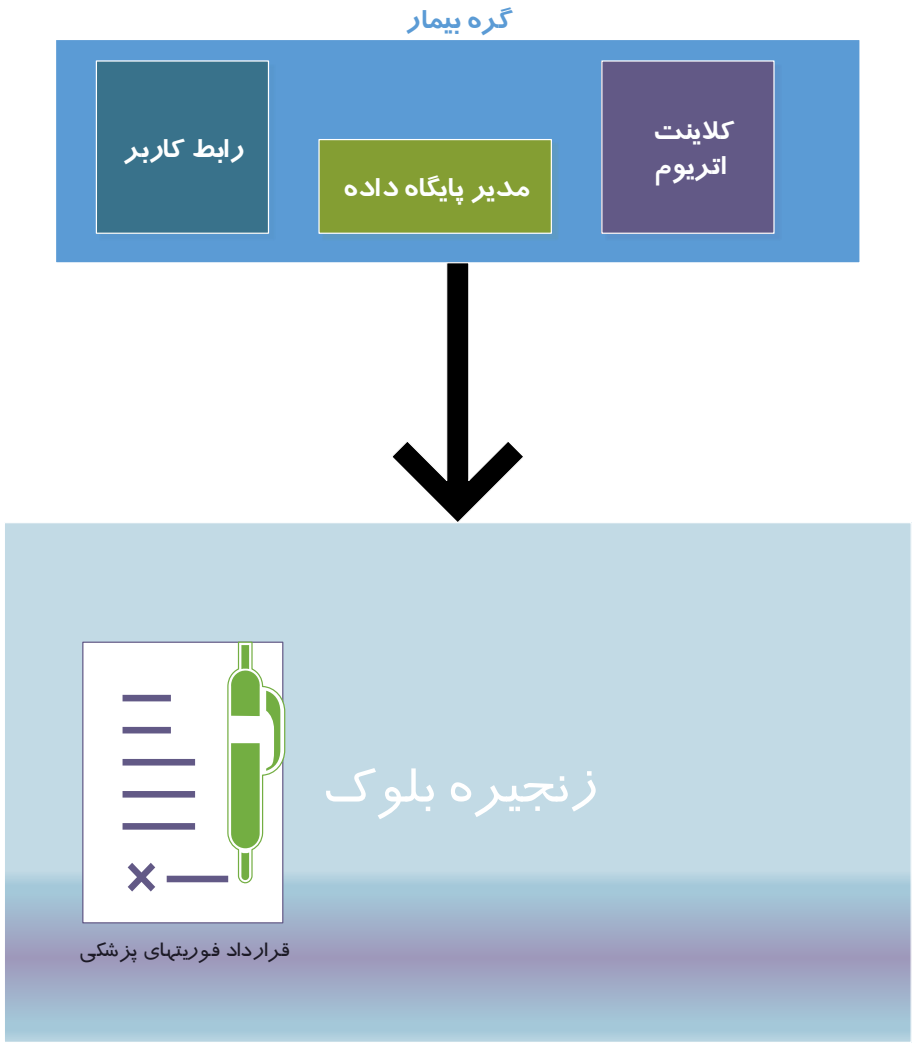
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

فرآیندها : ثبت اطلاعات فوریت های پزشکی



مقدمه

تعریف مساله

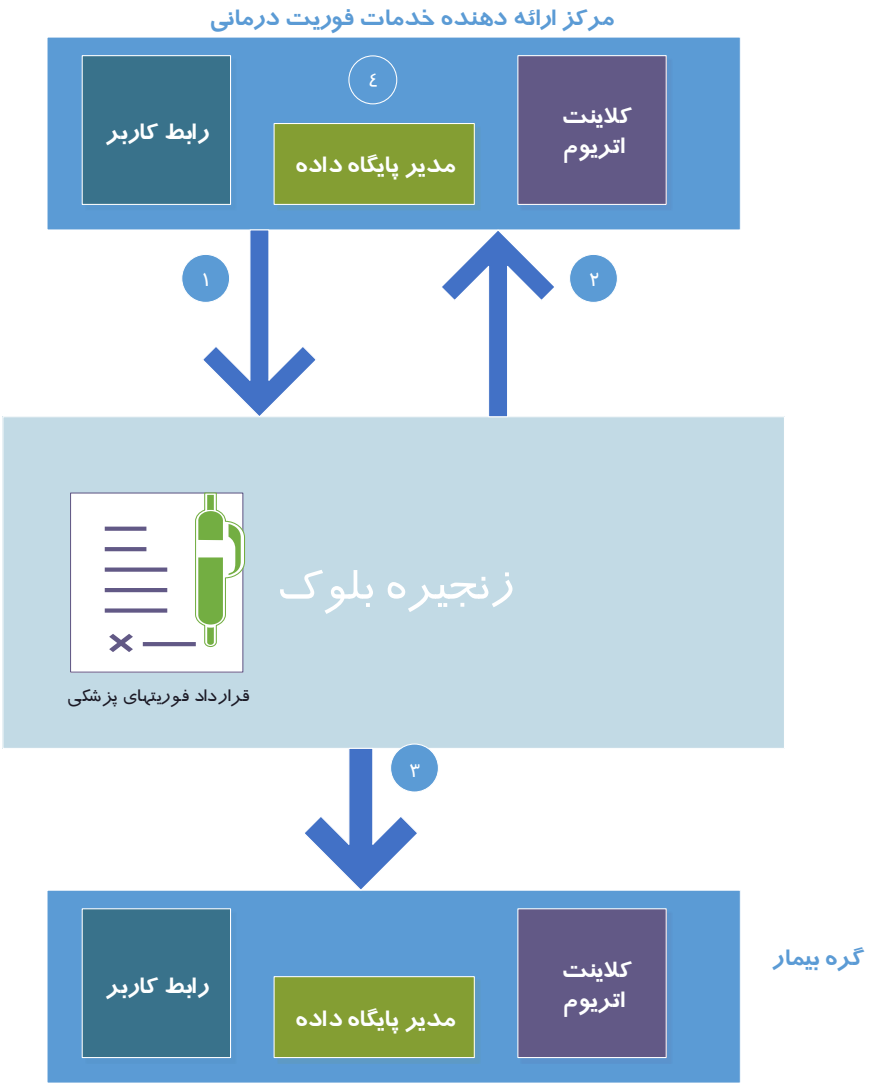
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

فرآیندها : خواندن اطلاعات فوریت های پزشکی



مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

استخراج

مقدمه

تعریف مساله

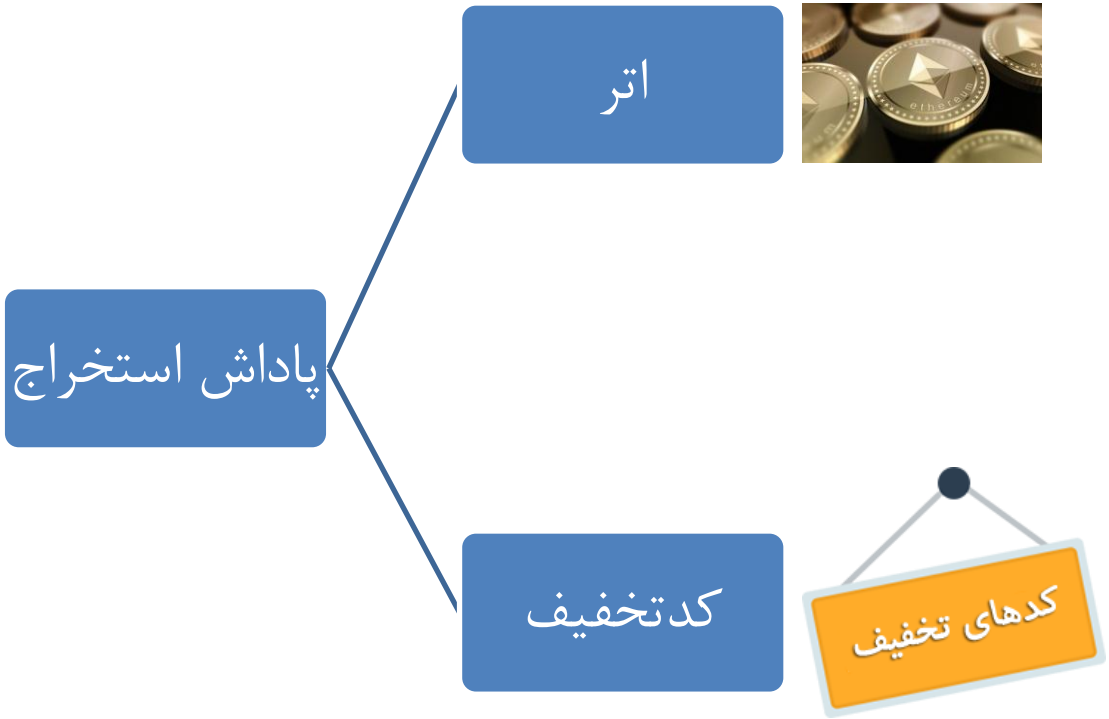
پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

اتر: پاداش ذاتی استخراج در شبکه اتریوم



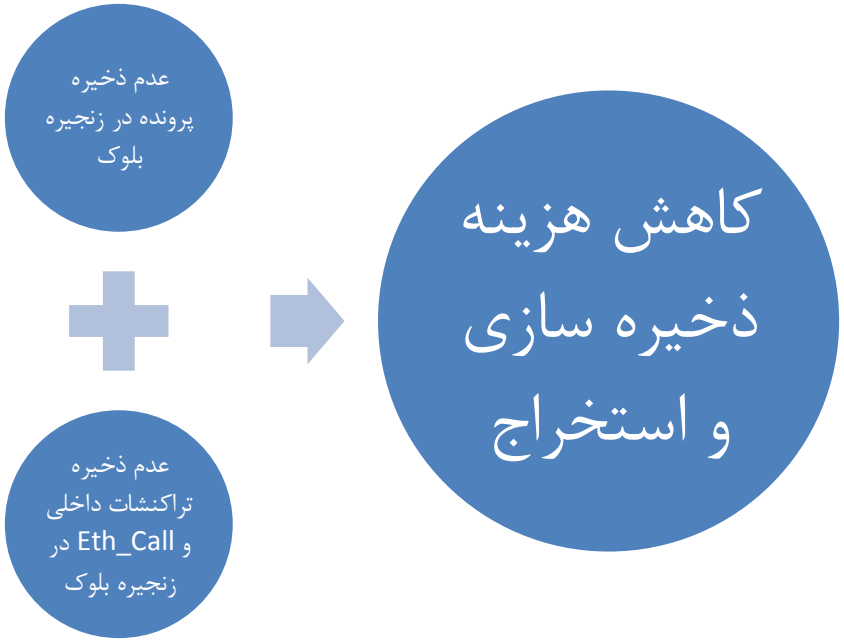
کد تخفیف : اجرای تابعی در قرارداد پرونده به محض استخراج تراکنش مرتبط به بروزرسانی پرونده و نسبت دادن کد تخفیف به استخراج کننده در پایگاه داده ارائه دهنده

مقایسه و ارزیابی

معیار	MedRec	Ancile	PIMED
تعداد اجزای نرم افزاری گره ها	۴	۳	۳
تعداد قرارداد هوشمند	۳	۶	۵
مشوق استخراج	دارد	ندارد	دارد
دسترسی مستقیم به پرونده فوریت پزشکی بیمار در زمان بروز فوریتهای درمانی	ندارد	ندارد	دارد
تعداد مراحل افزودن گره	بیان نشده	۱۲	۹
تعداد مراحل ایجاد پرونده	۹	۲۱	۸
تعداد مراحل بازیابی اطلاعات پرونده	بیان نشده	۹	۸
تعداد مراحل اعطای مجوز دسترسی	بیان نشده	۱۰	۹

مقیاس پذیری

- کپی اطلاعات در کل گره ها
- عدم ذخیره سازی اطلاعات پرونده در زنجیره بلوک
- عدم به مخاطره افتادن حریم خصوصی در عین مقیاس پذیری



مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

انطباق PIMED با قوانین بومی سلامت

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

۱	۲	۳	۴	۵	۶
زنجیره بلوک	ایجاد پرونده پس از تایید بیمار	انعطاف در ایجاد دسترسی به والدین در قرارداد پرونده	پوشش کل داده های تولیدشده توسط ارائه دهندگان خدمات درمانی	لزوم تایید بیمار برای دسترسی فرد ثالث	اطلاع رسانی در زمان بروز فوریت ها

جمع بندی و کار آینده

جمع بندی

- حذف هزینه های سیستم متمرکز
- سطح اعتماد بالاتر
- انعطاف در پیاده سازی
- منطبق بر قوانین حریم خصوصی
- یکپارچگی

کار آینده

- بهبود امنیتی: احتمال تحلیل تراکنشات بیماران
- ابهام در استقبال کاربران
- محدودیتهای فنی: حمله ۵۱٪

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی

با تشکر از توجه شما

الگوریتم اثبات کار

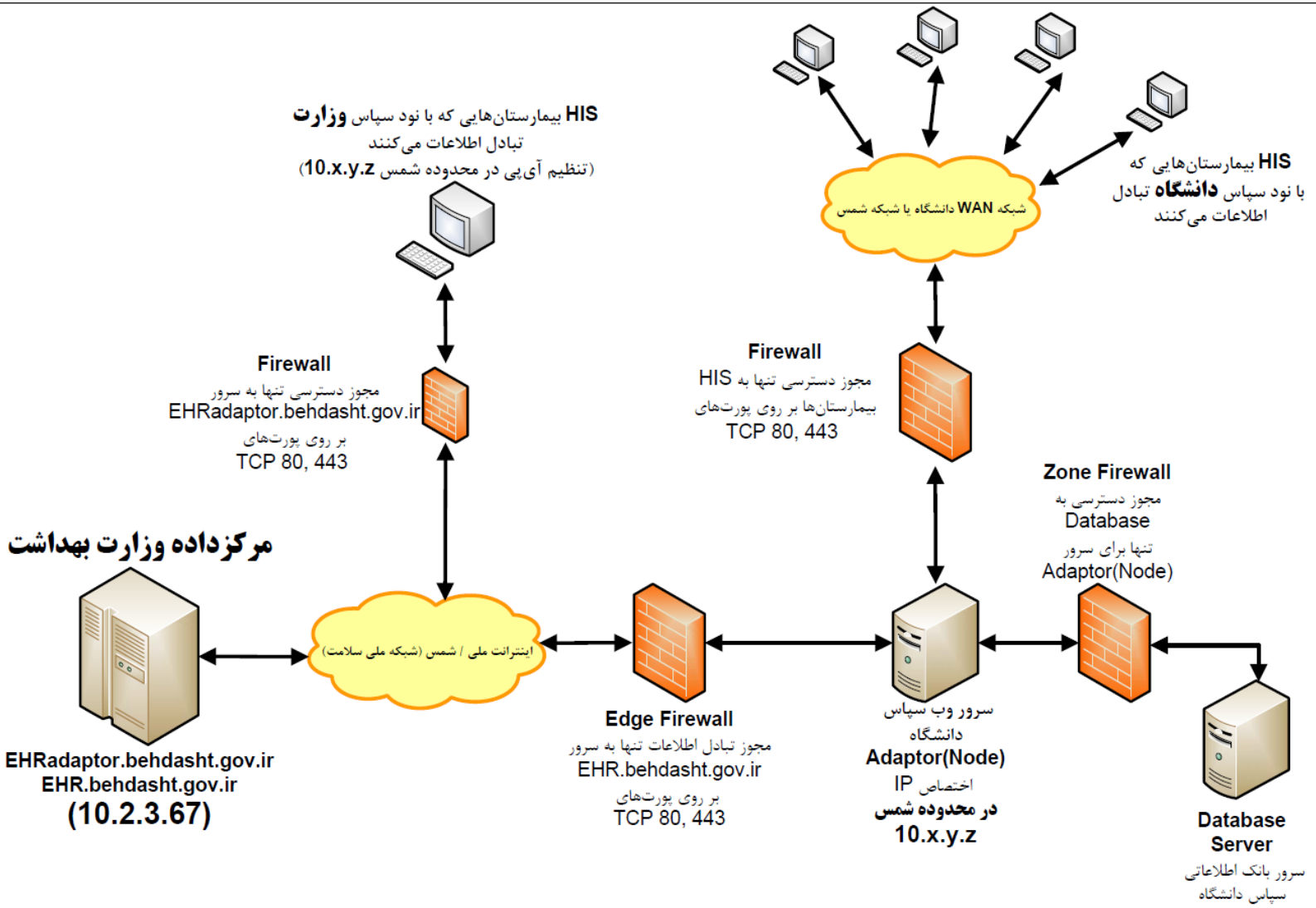
مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

۱) از سرآیند (header) بلاک یک هش تولید کنید.
۲) یک عدد تصادفی به انتهای هش تولیدشده اضافه کنید.
۳) خروجی بدست آمده را دوباره هش کنید.
۴) خروجی مرحله ۳، باید از میزان سختی شبکه که یک عدد مشخص-شده توسط سیستم است کمتر باشد. در غیر اینصورت باید یکی به عدد تصادفی افزوده و به مرحله دوم برگردید و دوباره سعی کنید.
۵) به همه اطلاع بدهید که موفق شده اید و مقدار تصادفی، هش بدست آمده و بلاک را برای همه کسانی که با آن ها در ارتباط هستید بفرستید.
۶) با استفاده از هش بدست آمده و اطلاعاتی که وجود دارد بسته بعدی را تولید کنید.

قرارداد هوشمند

مقدمه
تعریف مساله
پیشینه پژوهشی
روش پیشنهادی
بحث
جمع بندی

- مثال : دستگاه های فروش خودکار
- تفاوت فرایند قرارداد های هوشمند با فرایند های معمولی در اینترنت، غیرمتمرکز بودن و عدم بازگشت آن است. مثلا تراکنش های بانکی به صورت هوشمند انجام می گیرند اما مثلا بانک مرکزی میتواند از انجام یک تراکنش جلوگیری کند. در قرارداد های هوشمند شخص یا نهادی قادر به کنترل یک قرارداد نیست و وقتی مفاد یک قرارداد صحیح باشد، این قرارداد به صورت کاملا خودکار اجرا می شود.


HIS بیمارستان‌هایی که با نود سپاس وزارت
تبادل اطلاعات می‌کنند
(تنظیم آی‌پی در محدوده شمس 10.x.y.z)
HIS بیمارستان‌هایی که
با نود سپاس دانشگاه تبادل
اطلاعات می‌کنند
شبکه WAN دانشگاه یا شبکه شمس
Firewall
مجوز دسترسی تنها به سرور
EHRadaptor.behdasht.gov.ir
بر روی پورت‌های
TCP 80, 443
Firewall
مجوز دسترسی تنها به HIS
بیمارستان‌ها بر روی پورت‌های
TCP 80, 443
Zone Firewall
مجوز دسترسی به
Database
تنها برای سرور
Adaptor(Node)
مرکزداده وزارت بهداشت
اینترانت ملی / شمس (شبکه ملی سلامت)
EHRadaptor.behdasht.gov.ir
EHR.behdasht.gov.ir
(10.2.3.67)
Edge Firewall
مجوز تبادل اطلاعات تنها به سرور
EHR.behdasht.gov.ir
بر روی پورت‌های
TCP 80, 443
سرور وب سپاس
دانشگاه
Adaptor(Node)
اختصاص IP
در محدوده شمس
10.x.y.z
Database
Server
سرور بانک اطلاعاتی
سپاس دانشگاه

معماری شبکه بهینه برای پرونده سلامت: متمرکز یا غیرمتمرکز؟

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

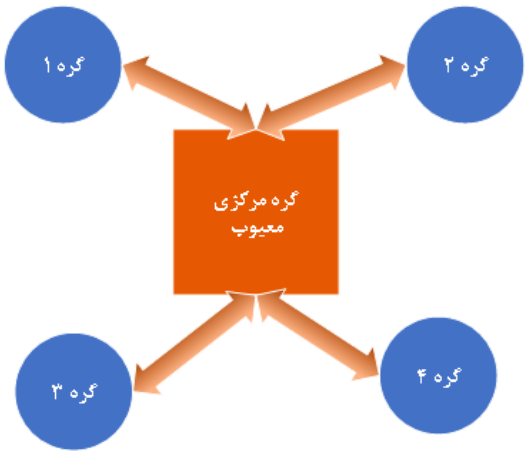
جمع بندی

مزایای معماری غیرمتمرکز(Kuo و همکاران):

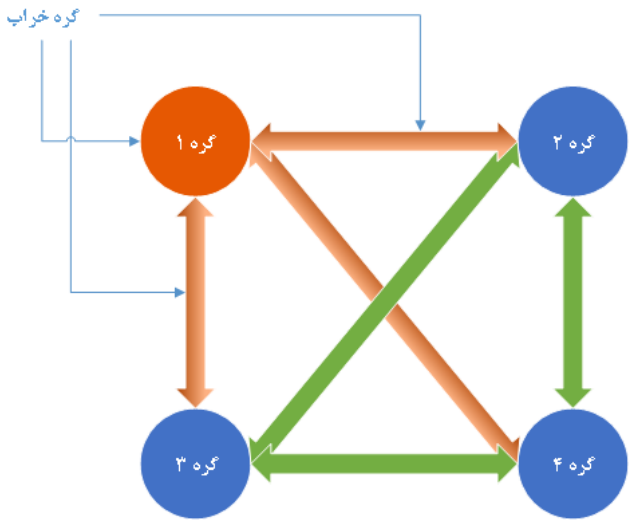
۱. هزینه کمتر

۲. سرعت بیشتر دسترسی به اطلاعات

۳. عدم وجود نقطه واحد شکست



روش متمرکز



روش غیرمتمرکز

توصیه های پیاده سازی PIMED

برنامه نویسی گره

- Geth Ethereum Client
- Web based interface on Flask(a Python micro framework)
- SQL Lite interface

قرارداد هوشمند

- Solidity on EVM
  - Remix
  - Ether atom
  - Visual Studio

مقدمه

تعریف مساله

پیشینه پژوهشی

روش پیشنهادی

بحث

جمع بندی