Patientory: Sebuah Jaringan Penyimpanan EMR Kesehatan Peer-to-Peer v1.1

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

May 2017

Dokumen ini hanya untuk tujuan informasi dan bukan merupakan upaya atau permintaan untuk menjual saham atau surat berharga di Patientory atau perusahaan terkait atau terkait. Permintaan atau permintaan semacam itu hanya akan dilakukan dengan menggunakan surat pernyataan tertutup dan persyaratan hukum yang berlaku dan sesuai dengan persyaratan semua sekuritas dan undang-undang lainnya yang berlaku.

Abstract

Pertukaran informasi kesehatan bertenaga blockchain (HIE) dapat membuka nilai interoperabilitas dan keamanan cyber sejati. Sistem ini berpotensi menghilangkan gesekan dan biaya perantara pihak ketiga saat ini, when considering population health management. Ada janji untuk meningkatkan integritas data, mengurangi biaya transaksi, desentralisasi dan disintermediasi kepercayaan. Mampu mengkoordinasikan perawatan pasien melalui HIE blockchain pada dasarnya mengurangi layanan yang tidak perlu dan duplikasi tes duplikat dengan menurunkan biaya dan perbaikan dalam efisiensi siklus kontinum, sambil mematuhi semua peraturan dan standar HIPAA. Protokol yang berpusat pada pasien yang didukung oleh teknologi blockchain, Patientory mengubah cara para pemangku kepentingan kesehatan mengelola data medis elektronik dan berinteraksi dengan tim perawatan klinis.

1 Pengantar

1.1 Apakah Blockchain?

Teknologi di balik mata uang digital bitcoin, kelahiran blockchain ditelusuri ke orang, yang tidak dikenal dan dikenal namanya (atau kelompok) yang dikenal sebagai Satoshi Nakamoto. Sejak tahun 2009, blockchain telah mendapatkan penggunaan yang lebih luas di industri keuangan, dengan berbagai blockchain baru yang memungkinkan bisnis dan layanan memasuki pasar. Teknologi Blockchain digunakan untuk berbagi buku besar transaksi di seluruh jaringan bisnis tanpa kendali oleh entitas tunggal manapun. Buku besar yang terdistribusi membuat lebih mudah untuk menciptakan hubungan komersial yang efesien dalam biaya, dimana secara virtual semua hal bernilai dapat dilacak dan diperdagangkan tanpa memerlukan titik pusat kendali. Teknologi ini menempatkan privasi dan kontrol data di tangan para individu

Kepercayaan dan integritas terjalin tanpa ketergantungan pada perantara pihak ketiga.

1.2 Infrastruktur Kesehatan Saat Ini

Penataan kembali dari "prosedur" berdasarkan fokus pada "perawatan holistik individu" memerlukan Penyedia Perawatan membentuk "jaringan" yang bekerja sama menuju tujuan bersama untuk memperbaiki hasil perawatan pasien yang dirawat, untuk episode perawatan akut atau di antara episode perawatan akut. Kebutuhan akan kerja sama antara penyedia layanan kesehatan mulai dari spesialis, dokter perawatan primer, pemberi perawatan dan penyedia layanan kesehatan (seperti perawat nutrisi dan rehabilitasi) menghasilkan peningkatan penggunaan teknologi digital. Meskipun solusi ini secara signifikan memperbaiki pelacakan dan efisiensi untuk memberikan perawatan, namun hasilnya menghasilkan silo informasi kesehatan, terutama dalam sistem rekam medis elektronik (EMR).

Organisasi kesehatan dan pemerintah menghabiskan banyak waktu dan uang untuk menyiapkan dan mengelola sistem informasi dan pertukaran data tradisional; Membutuhkan sumber daya untuk terus memecahkan masalah, memperbarui parameter lapangan, melakukan tindakan cadangan dan pemulihan, dan mengekstrak informasi untuk tujuan pelaporan.

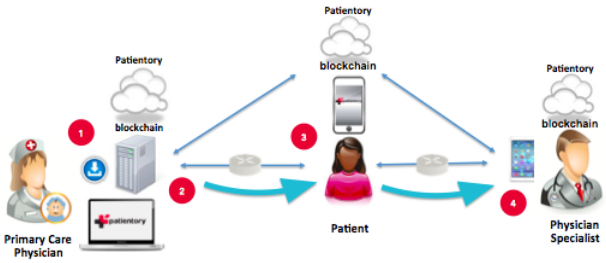
Undang-undang federal dan program insentif telah membuat data perawatan kesehatan lebih mudah diakses, sebagai tanggapan atas dorongan rumah sakit mengenai implementasi EMR. Namun, sebagian besar sistem rumah sakit masih belum dapat dengan mudah (atau aman) membagikan datanya. Akibatnya, dokter menghabiskan lebih banyak waktu mengetik daripada benar-benar berbicara dengan pasien. Tenaga kesehatan atau dokter yang kelelahan melonjak dari 45 menjadi 54 persen antara tahun 2011 dan 2014.[1].

Meskipun ada gagasan tentang informasi kesehatan "individual" baik di bidang klinis maupun kesehatan, ini belum diterjemahkan ke dalam rencana perawatan "personal". Lebih jauh lagi, walaupun ada sejumlah besar data, keseluruhan ekosistem perawatan kesehatan tidak mampu menilai secara memadai nilai atau risiko terhadap data besar untuk membantu memprediksi episode perawatan pasien di masa depan dengan lebih baik.

Oleh karena itu, solusi saat ini yang dilakukan oleh industri Teknologi Perawatan Kesehatan telah menghasilkan pilihan yang sulit antara perawatan dan privasi / kecurangan ekonomi bagi pasien. Kami melihat masalah ini berkembang pesat karena lebih banyak data diciptakan oleh industri. **Sifat teknologi yang aman dan sifat alami terdistribusi dari Blockchain dapat membantu mengurangi biaya dan efisiensi operasi ini serta menyediakan infrastruktur keamanan yang layak.**

1.3 Hubungan Penyedia-Pasien

Paradigma perawatan kesehatan yang baru menuntut kebutuhan akan pemberian perawatan yang efektif dan optimal bagi pasien untuk menghasilkan hasil perawatan yang lebih baik. Hal ini mengharuskan penyedia perawatan utama dapat secara aktif berkoordinasi dan berkolaborasi dengan penyedia layanan perawatan lainnya yang terlibat dan organisasi kesehatan tambahan seperti Laboratorium dan farmasi dalam perawatan. Akhirnya, agar hal ini berhasil catatan pasien perlu diperbarui dan dimodifikasi pada waktu yang tepat.



Gambar 1: Skematik Patientory

Perangkat lunak EMR saat ini melarang hubungan penyedia layanan dan pasien yang efektif. Portal pasien memiliki keterlibatan minimal di antara pasien, sebagai hasil dari pengalaman pasien yang samar. Selanjutnya, perangkat lunak ini hanya menyediakan kemampuan pertukaran informasi yang terbatas dari satu sistem ke sistem lainnya dan biasanya memerlukan individu yang ditunjuk yang mampu melakukan transfer informasi semacam itu. Hal ini menyebabkan meningkatnya jumlah penundaan antara organisasi dalam memberikan perawatan bagi pasien dan juga mengakibatkan penurunan kualitas layanan perawatan secara keseluruhan kepada pasien. Selain itu, karena penyedia layanan kesehatan menghabiskan lebih banyak waktu mereka untuk terlibat dalam koordinasi perawatan, keefektifannya dalam pengobatan pasien dan beban kerja meningkat secara signifikan sehingga menghasilkan dampak kontra-intuitif dalam hasil perawatan bagi pasien.

Selain itu, mengingat banyak dokter tidak ingin pasien mengakses EHRs, pasien mengadopsi peran pasif dalam melacak kesehatan mereka. Hal ini pada akhirnya membuat mereka merasa tidak memiliki kontrol dan kepemilikan kesehatan mereka yang menyebabkan pasien menjadi frustrasi dan terlepas dari perawatan mereka. Meskipun baru-baru ini ada peningkatan dalam aplikasi Perawatan Kesehatan Mobile yang membantu individu melacak parameter vital dan kesehatan mereka, hal yang baru belum diterjemahkan untuk peningkatan perawatan pasien atau kepatuhan dan hasil karena juga menghadapi tantangan untuk diintegrasikan ke dalam EHRs.

2 System Overview

Masalah-masalah ini dapat diselesaikan dengan menggunakan Jaringan Blockchain Patientory. EMR warisan adalah struktur terpusat yang tunduk terhadap peretasan, peraturan keamanan yang ketat, dan biaya overhead yang berat. Dengan menerapkan infrastruktur Patientory Blockchain, penyedia layanan akan melihat pemberantasan pelanggaran layanan kesehatan, saluran untuk fasilitas koordinasi perawatan yang menghasilkan peningkatan kesehatan secara keseluruhan. Di atas adalah skematis yang menggambarkan infrastruktur Blockchain Pasien dan interoperabilitasnya di antara pasien dan para penyedia layanan.

3 Implementasi Sistem

3.1 Peraturan dan Pedoman Kepatuhan HIPAA

Sebelum diskusi implementasi yang berarti, batasan yang diberlakukan oleh mandat dari Health Insurance Portability and Accountability Act of 1996 (HIPAA) harus ditangani. Aturan-aturan yang menjadi perhatian utama adalah Aturan Privasi, aturan Keamanan, dan Pedoman komputasi awan. Maksud dari makalah ini adalah untuk tidak melakukan investigasi penuh terhadap hukum HIPAA. Unsur - unsur yang terkait dengan diskusi pelaksanaan harus didefinisikan dan dibahas lebih lanjut pada saat aplikasi yang relevan.

A. Aturan Privasi

Model bisnis Patientory menetapkan bahwa persyaratan aturan privasi harus diperhatikan karena penyimpanan elektronik dan pengiriman informasi kesehatan privasi. Penerapan aturan privasi diringkas sebagai, "Aturan Privasi. . . (Berlaku) untuk rencana kesehatan, rumah kliring perawatan kesehatan, dan kepada penyedia layanan kesehatan yang mentransmisikan informasi kesehatan dalam bentuk elektronik " [2]. Selain agen ini, pihak-pihak yang bertindak atas nama mereka, sebagai penyedia layanan, juga bertanggung jawab atas kepatuhan HIPAA. Agen tangan kedua ini disebut Business Associates (BA), dan dokumen hukum yang menentukan peraturan dan peraturan yang harus dipatuhi oleh BA disebut Business Associate Contract (BAC). HIPAA menempatkan persyaratan yang ketat mengenai sifat kesepakatan ini.

Poin-poin kelayakan, dari penyelidikan awal, adalah persyaratan yang menentukan otorisasi penggunaan, penggunaan informasi yang tidak teridentifikasi, dan definisi informasi pribadi. Informasi kesehatan swasta (PHI atau ePHI untuk data elektronik) didefinisikan sebagai "semua informasi kesehatan yang diidentifikasi secara individu yang dimiliki atau dikirim oleh entitas yang tercakup atau rekan bisnisnya, dalam bentuk atau media apa pun, baik elektronik, kertas, atau lisan"[2]. Informasikesehatan yang tidak teridentifikasi didefinisikan sebagai "Informasi kesehatan yang tidak mengidentifikasi individu dan yang berkenaan dengan tidak adanya dasar yang masuk akal untuk percaya bahwa informasi tersebut dapat digunakan untuk mengidentifikasi seseorang tidak secara individual mengidentifikasi informasi kesehatan"[2]. Data yang tidak teridentifikasi menggunakan pembatasan yang diringkas sebagai berikut, "Tidak ada batasan penggunaan atau pengungkapan informasi kesehatan yang tidak teridentifikasi. Informasi kesehatan yang tidak diidentifikasikan tidak mengidentifikasi atau menyediakan dasar memadai untuk mengidentifikasi individu " [3]. Batas data yang dapat diidentifikasi ke data yang tidak dapat teridentifikasi didefinisikan sebagai informasi yang mungkin membatasi jumlah individu pada sebuah kumpulan informasi yang terkait dengan kurang dari 0,04% total populasi AS.

B. Aturan Keamanan dan Pedoman Komputasi Awan

Karena panjang konten yang terkait dengan topik ini, hanya elemen-elemen perhatian utama yang diisolasi sebagai referensi. Perhatian utama ini adalah sebagai berikut, "Ketika entitas yang tercakup menjalankan layanan CSP untuk membuat, menerima, memelihara, atau mentransmisikan ePHI (seperti memproses dan / atau menyimpan ePHI), atas namanya, CSP adalah rekan bisnis Di bawah HIPAA. Selanjutnya, ketika rekan bisnis mensubkontrakkan CSP untuk membuat, menerima, memelihara, atau mengirimkan

ePHI atas namanya, subkontraktor CSP itu sendiri adalah rekan bisnis. Hal ini berlaku bahkan jika proses CSP atau hanya menyimpan ePHI terenkripsi dan tidak memiliki kunci enkripsi untuk data. Tidak memiliki kunci enkripsi tidak membebaskan CSP dari status dan kewajiban sebagai rekan bisnis berdasarkan aturan HIPAA. Akibatnya, entitas yang tercakup (atau rekan bisnis) dan CSP harus menandatangani perjanjian bisnis asosiasi HIPAA (BAA), dan CSP bertanggung jawab secara kontrak untuk memenuhi persyaratan BAA dan bertanggung jawab secara langsung untuk mematuhi peraturan persyaratan yang berlaku dari Aturan HIPAA " [3].

Entitas tertutup sering menggunakan penyedia penyimpanan awan (CSPs) untuk menyimpan informasi kesehatan, sering kali menyebutkan bahwa biaya lebih efektif dan ada biaya pengelolaan TI yang lebih rendah. Namun, karena konsumen mengandalkan penyedia awan untuk menyimpan data pribadi, mereka menyerahkan kontrol langsung atas data tersebut dan, akibatnya tidak menyadari siapa yang memiliki akses dan tempat data berada secara geografis. Bahkan jika kesepakatan asosiasi bisnis eksplisit dikembangkan antara BA dan penyedia penyimpanan awan, ini hanya akan memberikan persyaratan siapa yang bertanggung jawab atas privasi dan keamanan data jika terjadi pelanggaran. Konsumen berpotensi memiliki kontrol atas akses ke aliran data ini, namun bergantung pada penyedia penyimpanan awan untuk menerapkan hak istimewa tersebut.

Meskipun penggunaan penyimpanan awan sangat populer, masih ada sejumlah risiko yang dilakukan konsumen saat menggunakan mekanisme ini untuk data pribadi mereka. Dalam arsitektur berbasis awan, data direplikasi dan sering dipindahkan sehingga risiko penggunaan data yang tidak sah meningkat. Selain itu, beberapa individu dengan akses ke data, seperti administrator, insinyur jaringan dan pakar teknis yang mencakup area server yang luas dimana informasi disimpan. Hal ini juga meningkatkan risiko akses dan penggunaan yang tidak sah.

Namun, walaupun data tersebut aman melalui kontrol akses yang ketat dan dienkripsi pada titik asalnya dan saat transit, masih menimbulkan masalah bagi pengembangan Patient-Reported Outcomes Measures (PROMs)(Laporan Hasil Tindakan Pasien). Konsep PROM adalah mengembangkan ukuran yang berfokus pada pasien yang berhubungan dengan area atau fokus yang menjadi perhatian pasien, dan di mana keterlibatan dan umpan balik mereka penting untuk keberhasilan penerapannya. Mengakses data stream yang besar dari berbagai perangkat yang merupakan bagian dari jaringan IoT seperti yang digunakan sekarang bersamaan dengan layanan berbasis awan dapat memberikan landasan untuk mendasarkan PROM, namun sangat sulit untuk mengetahui apakah data tersebut disamarkan di awan akan menghasilkan ukuran yang akan memiliki makna dan relevansi yang diinginkan untuk pasien.

Penerapan teknologi blockchain untuk memastikan dan meningkatkan kerahasiaan data untuk semua catatan medis yang terkait dengan sistem dapat mencapai nol pelanggaran kesehatan dan desentralisasi akhir kepemilikan rekaman. Proses mengenkripsi data saat dikirim ke database menggunakan algoritma yang berbeda dan mendekripsinya selama pencarian akan digunakan.

Berkenaan dengan semakin pesatnya jumlah pelanggaran data yang dihadapi industri perawatan kesehatan, teknologi blockchain membuat kepatuhan HIPAA layak dilakukan bagi pasien dan penyedia layanan.

C. Analisis Sistem Blockchain dari batasan- batasan karena larangan HIPAA

Blockchain Ethereum memfasilitasi beragam subset dari implementasi sistem karena penerapan bahasa pemrograman aplikasi Turing yang lengkap yang dijalankan pada mesin maya Ethereum. Sistem ini memiliki keterbatasan karena mesin virtual tidak memiliki inspeksi langsung ke luar dari internet yang lebih luas kecuali melalui penggunaan Layanan Oracle. Selain itu, keterbatasan penyimpanan blockchain ditegakkan dengan biaya gas untuk penyimpanan dan biaya gas untuk akses terhadap data ini. Pada waktu tulisan ini, waktu blok rantai menetapkan batasan minimum untuk permintaan modifikasi tahap paling sedikit lima belas detik.

Keterbatasan blockchain untuk menghost informasi pribadi dapat diatasi melalui penyangkalan data, seperti enkripsi, namun jika kunci dekripsi tersebut pernah bocor,tidak ada cara untuk menghapus data sensitif itu sendiri dari blockchain. Untuk tujuan data sesuai HIPAA, hal ini berpotensi mengakibatkan kebocoran informasi yang terus-menerus dan tidak dapat diperbaiki karena kekekalan dari blockchain itu sendiri. Meskipun data yang tidak dapat diidentifikasi secara teori dapat disimpan pada Blockchain Publik Ethereum, akan menjadi bencana jika diasumsikan bahwa mekanisme penyaringan data yang tidak teridentifikasi tidak akan pernah gagal, atau bahwa informasi sideband yang terkait dengan interaksi blockchain tidak dapat secara tidak sengaja mengungkapkan identitas. Kesimpulan ini juga dicapai oleh MIT Media Lab selama pembentukan Protokol MedRec dan dirangkum dalam Whitepaper MedRec [3]. Pertambangan informasi sideband ini semudah mengamati cap waktu dan interaksi dengan kontrak penyimpanan data yang diketahui.

Melalui analisis ini, dimungkinkan untuk mengasosiasikan individu dengan institusi, dan yang lebih penting adalah saat mereka berada di sebuah fasilitas. Mengingat sifat khusus dari beberapa fasilitas, ini adalah informasi yang cukup untuk merupakan pelanggaran terhadap kepatuhan HIPAA karena kemampuan pengamat pasif untuk menyimpulkan baik identitas, lokasi, waktu interaksi, dan kemungkinan kelas diagnosis.

Menunda bahwa lokasi ini terpencil sifatnya, pengurangan hingga kurang dari 0,04% populasi AS menjadi sepele. Fakta-fakta ini merupakan kegagalan titik tunggal yang tidak masuk akal yang harus diakui. Selanjutnya, penyimpanan langsung informasi terenkripsi pada blockchain membuat tanggung jawab manajer database untuk masuk ke BAC karena tindakan mereka sebagai fasilitas penyimpanan data HIPAA (lihat bagian berjudul Rule Security and Cloud Computing Guide-lines). Ini adalah ekspektasi yang tidak masuk akal karena setiap penambang, dan bahkan orang-orang yang menjadi host node pasif, perlu mematuhi HIPAA. Karena masalah ini, kami menerapkan mekanisme untuk penyimpanan informasi sensitif yang terus-menerus melalui penerapan blockchain pribadi berbasis Ethereum.

D. Tujuan Pelaksanaan untuk Kegunaan dan Keamanan

Tujuan utama dari setiap sistem keamanan dapat diringkas sebagai tujuan kerahasiaan, integritas, ketersediaan, akuntabilitas dan jaminan informasi / identitas. Untuk mengakomodasi tujuan ini, penyerang dan pengguna harus berada

Masing-masing peran ini menuntut pengakuan atas kemampuan tertentu. Dari perspektif pengguna, sistem perlu transparan sehingga tidak diperlukan pengetahuan lanjutan. Selain itu, karena ketidakmampuan pengguna normal untuk memahami pertimbangan kompleks cybersecurity, prosesnya harus tahan terhadap tindakan pengguna.

Pada saat serangan terjadi, sistem dibuat sedemikian rupa sehingga jumlah biaya yang harus diinvestasikan untuk mengkompromikan sumber daya lebih berharga daripada nilai sumber daya itu sendiri. Hal ini disebabkan oleh kesadaran bahwa sebuah pihak yang maju dengan sumber daya yang cukup akan selalu mampu melakukan pelanggaran terhadap sistem apapun, mengingat usaha dan waktu yang cukup. Secara lebih padat, tidak ada pertahanan yang sempurna. Dengan adanya pembatasan ini, implementasinya sendiri sekarang bisa dibicarakan sehingga kita bisa mencapai semua tujuan yang telah disebutkan sebelumnya.

3.2 Definisi penerapan Perangkat Keras dan Jaringan

Untuk mengakomodasi tujuan desain yang disebutkan di atas, penerapan sistem yang dipilih memerlukan beberapa sistem independen. Setiap sistem membagi otoritas, memastikan hanya entitas yang berwenang yang dapat berinteraksi dengan cara yang disetujui, dan menyediakan mekanisme untuk meningkatkan keamanan sambil mempertahankan keberadaan. Sistem ini juga telah dirancang sedemikian rupa sehingga penskalaan dapat siap dilakukan melalui penambahan skema panggilan hierarkis. Sistem ini dijelaskan sepenuhnya secara rinci di bawah ini.

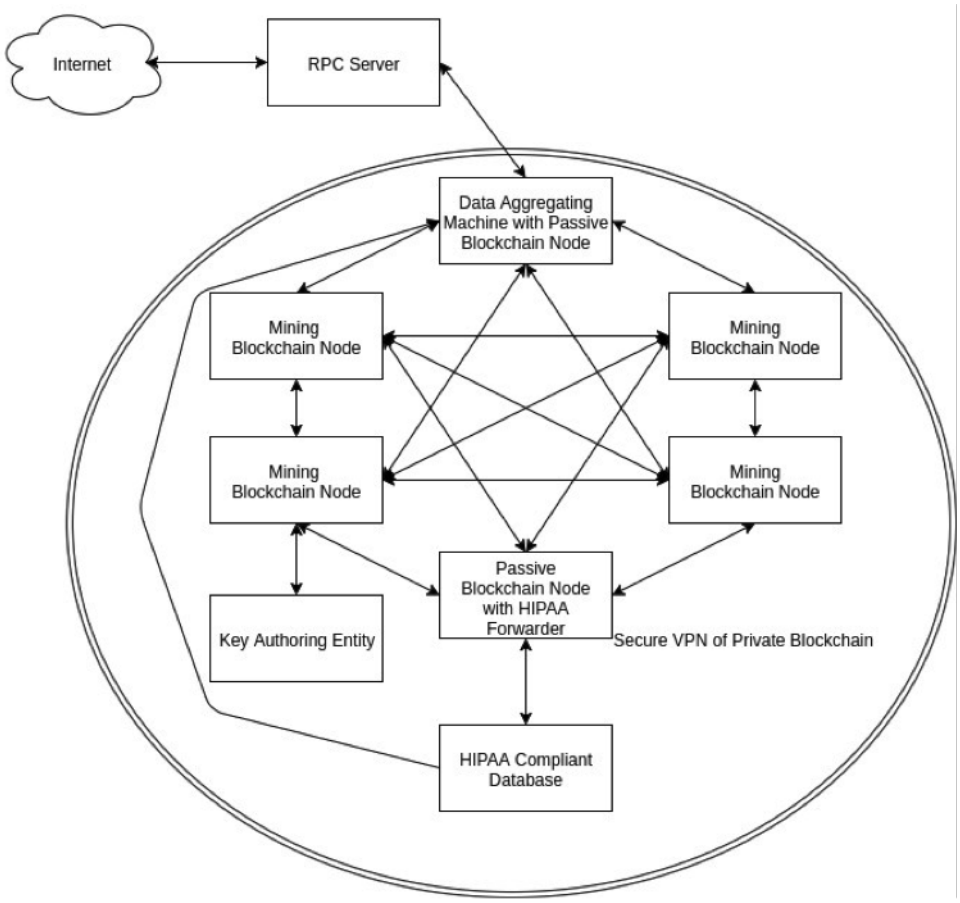
Entitas yang menghadap ke depan adalah Remote Procedure Call (RPC) Server yang bertindak sebagai penghubung ke implementasi pribadi dari Blockchain Ethereum (blockchain yang diizinkan). Jaringan node blockchain ini hanya diotorisasi untuk berinteraksi dengan node blockchain lainnya, entitas pembuat kunci, fasilitas penyimpanan sesuai HIPAA, dan RPC Server. Entitas pembuat kunci adalah sumber daya yang menghasilkan pasangan kunci pribadi/publik untuk digunakan pada blockchain. Fasilitas penyimpanan sesuai HIPAA menampung data aktual yang merupakan informasi kesehatan pribadi elektronik (ePHI= electronic private health information) .

Bila permintaan untuk data terjadi, sistem kepatuhan HIPAA dapat diizinkan untuk berbicara dengan agen penerusan, yang kemudian mengalihkan kembali data ke server RPC. Sebagai alternatif, mungkin terstruktur sedemikian rupa sehingga penyimpanan HIPAA berbicara langsung ke server RPC. Setiap implementasi memiliki manfaat yang harus dipertimbangkan sebelum seleksi akhir. Dalam kedua peristiwa tersebut, fasilitas penyimpanan HIPAA mendekripsi bagian database yang relevan atas permintaan penanganan. Informasi dekripsi ini kemudian dienkripsi ulang dengan menggunakan kunci publik dari pihak yang meminta untuk ditransmisikan. Kunci publik ini juga merupakan kunci publik dari kontrak yang bertindak sebagai antarmuka kontrol dari blockchain ke data HIPAA.

Diagram topologi jaringan yang spesifik dapat dilihat pada gambar 2.

3.3 Definisi Penerapan Perangkat Lunak

Selain isolasi fisik sistem dalam penerapan perangkat keras dan jaringan, kontrol akses perangkat lunak memfasilitasi integritas data dan



Gambar 2: Topografi Jaringan Blockchain Patientory

verifikasi otorisasi untuk entitas peminta. Sistem perangkat lunak, dari perspektif kontrol akses dan enkripsi data dijelaskan di bawah ini.

Database compliant HIPAA hanya akan menerima koneksi inbound dari forwarder HIPAA. Hal ini memastikan bahwa aliran trafik diisolasi ke jalur terkontrol yang diketahui. Forwarder HIPAA hanya akan bertindak untuk meneruskan permintaan ke fasilitas penyimpanan HIPAA sambil menunggu transaksi yang valid telah terjadi pada blockchain tersebut, dan transaksi ini menghasilkan emisi dari sebuah peristiwa permintaan. Forwarder HIPAA hanya akan bertindak untuk meneruskan permintaan ke fasilitas penyimpanan HIPAA sambil menunggu transaksi yang valid telah terjadi pada blockchain tersebut, dan transaksi ini menghasilkan emisi dari sebuah peristiwa permintaan. Peristiwa permintaaan ini harus memuat kunci publik dari pihak yang meminta dan bidang data yang diminta tersebut. Akhirnya, server RPC menggunakan antarmuka program aplikasi akses terkontrol (API) sehingga hanya pengguna yang diketahui dapat berinteraksi dengan server.

Untuk memahami hierarki panggilan sistem, struktur kontrak untuk memfasilitasi kontrol akses harus ditangani terlebih dahulu. Setiap pengguna di sistem memetakan ke alamat pribadi di blockchain pribadi. Setiap alamat pribadi hanya diberi wewenang untuk berbicara langsung dengan SATU kontrak dalam blockchain. Kontrak ini adalah kontrak kelas individu. Institusi, pegawai institusi, dan pelanggan merupakan tingkat kelas objek.

Objek tingkat kelas ini adalah antarmuka berbasis izin. Kontrak Institusi memiliki daftar semua pelanggan yang telah diberikan hak dan setiap kontrak pelanggan memiliki daftar semua institusi yang telah diberi izin. Kontrak yang dipegang oleh institusi ini memiliki fungsi yang memudahkan pencabutan izin kepada institusi, dari pengguna. **Kontrak institusi mungkin tidak mengubah daftar ini sendiri, sehingga mencegah akses tidak sah ke catatan individu.** Sebagai tambahan, Kontrak Institusi memiliki daftar pegawai yang berwenang yang bisa memelihara sepenuhnya. Skema izin ini idealnya harus berfungsi sedemikian rupa sehingga pencabutan izin secara otomatis dilakukan pada interval semi reguler untuk mencegah institusi secara tidak sengaja melestarikan hak akses mantan karyawan.

Dalam sistem ini, semua pihak eksternal berinteraksi melalui penyampaian transaksi yang ditandatangani yang menyandikan permintaan pemanggilan. Transaksi ini disampaikan melalui server RPC pada saat user melakukan validasi. Server RPC mengirimkan permintaan ini ke server agregasi data yang kemudian meneruskan permintaan ini ke penambang berdasarkan mekanisme pembagian beban. Para penambang kemudian memproses permintaan tersebut dengan mengajukan transaksi atas nama pihak yang dipanggil ke kontrak pengendali masing-masing pihak. Kontrak ini memegang hak akses data bahwa entitas berwenang untuk mengakses internal kontrak. Kontrak ini adalah satu-satunya entitas yang akan menerima transaksi dari permintaan dari luar. Dengan demikian, sebuah mekanisme dibentuk untuk sepenuhnya mengendalikan operasi panggilan pada blockchain.

Untuk transaksi tertentu, rekaman yang tidak berubah dari pihak pemanggil dibuat. Ini memastikan bahwa semua upaya untuk mengakses informasi dicatat. Data aktual yang tersimpan dalam kontrak pengguna adalah sistem hash pointer yang ketika diselesaikan oleh server penyimpanan HIPAA menghasilkan pengembalian data yang sesuai. Informasi ini dilontarkan ke forwarder HIPAA dengan melakukan transaksi permintaan yang valid. Mekanisme yang memfasilitasi komunikasi ini tidak langsung dan bermanifestasi melalui sistem pesan event blockchain.

Karena keterbatasan bahwa pemohon hanya bisa mempertanyakan basis data dengan transaksi yang valid, dan pengguna mungkin tidak secara langsung mengubah informasi mereka sendiri, kontrol akses dapat dibuktikan. mekanisme serupa, kecuali kontrak institusi yang menampung daftar pengguna yang dapat meminta data dan daftar pengguna yang mungkin berinteraksi dengan institusi ini sebagai karyawan. Ketika sebuah permintaan transaksi berasal dari kontrak pegawai institusi, kontrak pengontrol memanggil kontrak institusi, yang memanggil kontrak pengguna untuk meminta petunjuk data yang menyelesaikan ePHI. Menunggu institusi tersebut masuk dalam daftar institusi yang disetujui untuk pengguna, kontrak akan mengembalikan pointer hash yang sesuai. Petunjuk ini kemudian diterbitkan sebagai pesan peristiwa yang lagi lagi dilontarkan sampai ke fasilitas penyimpanan HIPAA.

Untuk lebih jelas, proses lengkap dari satu permintaan adalah sebagai berikut: Pihak eksternal meminta data dari layanan tersebut dengan menghubungi server RPC dengan sebuah transaksi yang ditandatangani secara kriptografis untuk diserahkan ke blockchain. Server RPC memverifikasi identitas pihak luar melalui tanda tangan permintaan masuk.

Menunggu tanda tangan cocok dengan entri di database kunci publik yang diizinkan, server RPC menerima permintaan tersebut dan mengajukan permintaan ke Mesin Agregat Data. Mesin Agregat Data kemudian mengajukan permintaan ke verifikator blockchain pribadi. Verifikator menerima permintaan tersebut sebagai panggilan dari akun blokchain terhadap kontrak target. verifikator melakukan panggilan ini, dan jika permintaan tersebut merupakan tindakan yang diijinkan, transaksi akan dimasukkan ke blok berikutnya. Transaksi ini juga menyebabkan terjadinya emisi pesan peristiwa di blockchain. Pesan peristiwa ini diamati oleh HIPAA Forwarder, yang bertindak untuk membuat permintaan terenkripsi terhadap penyimpanan HIPAA berdasarkan hash pesan acara. Pesan ini juga berisi kunci publik dari pihak peminta. Sistem database compliant HIPAA mengamati permintaan ini dan mentransmisikan salinan informasi yang dienkripsi ke server RPC menggunakan kunci publik dari pihak yang meminta. Server RPC kemudian mengembalikan informasi ini ke pihak peminta dengan memetakan ulang IP yang meminta ke kunci publik dalam pesan. Data ini kemudian segera dihancurkan oleh server RPC, sehingga memastikan bahwa server RPC bertindak sebagai saluran yang tidak perlu sesuai dengan HIPAA.

Mekanisme untuk mempublikasikan data bersifat serupa, namun data yang akan disampaikan dienkripsi dengan kunci publik dari fasilitas penyimpanan HIPAA. Operasi lainnya identik kecuali data yang sedang dikirim menggelembung melalui sistem pesan acara. Dengan demikian, karena penggunaan fungsi hash dengan tabrakan yang rendah dan nonces berdasarkan cap waktu, data dapat disimpan dengan kontrak yang mampu menghitung alamat dimana data yang diajukan berada di dalam fasilitas penyimpanan HIPAA.

Akhirnya, distribusi kunci pribadi untuk entitas harus ditangani. Ini dapat difasilitasi melalui sarana optik bagi pengguna smartphone. Ini sama dengan penggunaan kode QR sebagai alamat alamat Ethereum. Cara alternatif juga dapat dibuat menggunakan aplikasi pada kedua komputer desktop

dan perangkat tablet / smartphone. Hilangnya sebuah kunci bukanlah peristiwa bencana, karena kemampuan untuk secara administratif mencabut kontrol akses kontrak pengendali dari satu kunci dan memberikannya kepada yang lain.

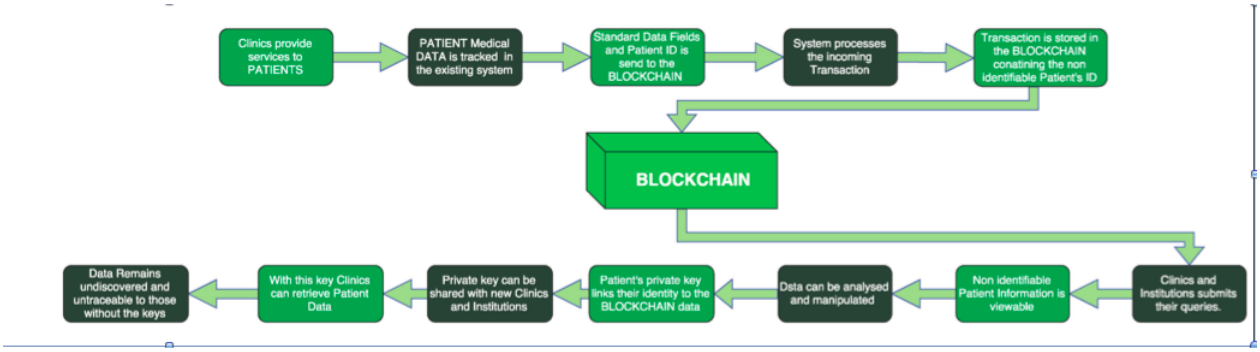
3.4 Interoperabilitas

Sistem EHR didasarkan pada arsitektur validasi credential yang terisolasi dimana data pasien disimpan di masing-masing sistem yang terpisah. Hal ini telah menghasilkan solusi perangkat lunak perawatan "tambahan" satu ke satu untuk sistem ini untuk memungkinkan koordinasi perawatan di seluruh penyedia layanan lainnya dan organisasi kesehatan tambahan. Namun, akses informasi dari organisasi Penyedia utama ke organisasi lain hanya melalui kemampuan terbatas seperti kasus Baca, untuk menyerahkan, untuk mengirim atau untuk pemberitahuan. Selanjutnya, Pasien/Konsumen memiliki interaksi atau keterlibatan yang sangat terbatas dalam pertukaran informasi ini. Selain itu, kelemahan mekanisme pertukaran data ada dalam kesulitan dalam penyempurnaan kesalahan yang terjadi selama proses penyampaian.

Sekali setelah blockchain dan kontrak pintarnya telah dikonfigurasi, parameternya menjadi mutlak. Pasien menjadi perantara utama dalam mengirim dan menerima informasi kesehatan yang meniadakan kebutuhan akan pembaruan dan pemecahan masalah perangkat lunak yang sering terjadi. Karena catatan blockchain juga tidak dapat diubah dan disimpan di semua pengguna yang berpartisipasi, kontinjensi pemulihan tidak diperlukan. Selain itu, struktur informasi transparan blockchain dapat menghapus banyak titik integrasi data dan aktivitas pelaporan yang memakan waktu.

3.5 Proses dan Skalabilitas

Pengguna mengendalikan semua informasi dan transfer mereka yang menjamin data berkualitas tinggi yang lengkap, konsisten, tepat waktu, akurat, dan tersedia secara luas sehingga membuatnya tahan lama dan dapat diandalkan. Karena database terdesentralisasi, blockchain tidak memiliki titik pusat kegagalan dan lebih mampu menahan serangan berbahaya.



Gambar 3: Diagram Alir Proses Blockchain

Di setiap jaringan Perawatan, perlu memastikan bahwa peserta yang bekerja sama dapat saling bergantung satu sama lain untuk memberikan layanan yang diperlukan yang diharapkan dari mereka. Untuk mencapai hal tersebut, harus ada sarana untuk memastikan akuntabilitas tugas dan layanan yang diharapkan dapat disampaikan pada waktu yang tepat dan juga pertanggungjawaban terkait jika tidak disampaikan secara tepat waktu pada tingkat kualitas yang diharapkan. Oleh karena itu, setiap infrastruktur Perawatan Kesehatan harus dapat secara mulus dapat memantau informasi yang diperlukan agar Penyedia Perawatan Primer dapat mengevaluasi jaringan Perawatannya. Lebih jauh lagi, saat jaringan perawatan tumbuh dan interaksi antara penyedia perawatan jaringan ini meningkatkan infrastruktur Perawatan Kesehatan harus mampu menangani skala ini secara efektif.

Aspek kunci untuk membangun sistem pengelolaan kesehatan yang sangat terukur dan terdistribusi adalah kerangka kerja arsitektur peer-to-peer. Kerangka kerja semacam itu telah digunakan di sejumlah segmen industri seperti, media, olahraga, real estat, rantai pasokan, menampilkan blockchain dapat dengan mudah menambahkan konektor perangkat lunak ke kerangka terpusat yang ada [7]. Hal ini telah mendorong kami untuk mengeksplorasi kerangka kerja kerangka blok untuk penerapannya guna membantu memungkinkan kerangka peer-to-peer untuk perawatan kesehatan.

Blockchain memegang janji untuk memvalidasi dua atau lebih entitas yang terlibat dalam "transaksi perawatan kesehatan". Ini menyediakan dua atribut kunci dibandingkan dengan model otentikasi terpusat. Yang pertama, pihak yang berkepentingan dapat saling terlibat dalam "tingkat transaksi" dari "hubungan kepercayaan". Yang kedua adalah bahwa keterpaparan kewajiban dalam hubungan semacam itu terbatas hanya pada keterlibatan "tingkat transaksi". Hal ini sangat berguna karena membatasi akses informasi dan kewajiban antara pihak-pihak yang terlibat dan pada saat yang sama memungkinkan pihak untuk melakukan hubungan transaksi dengan sejumlah penyedia lainnya berdasarkan kemampuan dan jenis perawatan khusus mereka untuk dikirim ke pasien. Ini secara signifikan lebih baik daripada sistem terpusat konvensional yang perlu membatasi jumlah penyedia untuk berbagai kebutuhan pasien karena diperlukan untuk mengelola akses dan liabilitas.

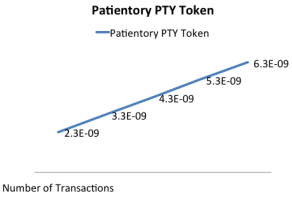
3.6 Pertukaran Informasi Kesehatan dan Token

Token Patientory (PTOY) adalah bahan bakar untuk menggerakkan infrastruktur blockchain. Penggunaan utama token adalah mengatur alokasi penyimpanan jaringan, ukuran kualitas perawatan kesehatan dan siklus pembayaran pendapatan.

Pasien diberikan sejumlah ruang untuk menyimpan informasi secara gratis di jaringan Patientory. PTOY memungkinkan mereka untuk membeli ruang penyimpanan ekstra dari node yang dipasang di sistem rumah sakit. PTOY bisa dibeli melalui platform atau bursa.

Organisasi kesehatan dalam hal ini juga menggunakan PTOY Hal ini juga digunakan dalam pembayaran setelah kontrak cerdas dijalankan dengan perusahaan asuransi kesehatan dan berfungsi sebagai mekanisme untuk mengatur metrik model berbasis nilai.

Agar AS berhasil beralih dari model fee-for-service ke model berbasis nilai saat ini, harus ada infrastruktur TI kesehatan yang memungkinkan organisasi untuk menghubungkan kualitas, nilai dan efektivitas intervensi medis melalui model kompensasi yang memiliki reputasi bagus.



Gambar 4: Nilai Token Patientory sebagai sebuah fungsi dari transaksi

3.7 Akuisisi Token

PTOY dapat diperoleh melalui aplikasi asli Patientory, pasar mata uang kripto dan dari pasien lain, dokter atau perusahaan asuransi melalui transfer. Pengguna platform akan memiliki kemampuan untuk mengakuisisi PTOY dengan mengirim Ether ("ETH") ke kontrak pembuatan PTOY di blockchain selama pra-penjualan. Antarmuka pasien akan mengintegrasikan solusi perdagangan pihak ketiga seperti Shapeshift dan Coinbase untuk pengguna yang tidak memiliki ETH.

Distribusi awal token Patientory akan berupa pra penjualan. Siapa pun akan bisa mendapatkan PTOY dengan harga diskon dengan mengirimkan ETH ke dalam kontrak cerdas penjualan token. Mereka yang memiliki mata uang kripto lain seperti ETC atau BTC dapat menciptakan PTOY melalui layanan konversi pihak ketiga yang akan tersedia di halaman pra-penjualan.

Tim pendiri akan menerima alokasi 10% dari PTOY, menahan selama dua belas bulan. Token ini akan menjadi insentif jangka panjang bagi tim pendiri Patientory. 20% tambahan akan dialokasikan ke dana Yayasan Patientory untuk digunakan dalam penelitian dan pengembangan mengenai teknologi blockchain untuk kasus penggunaan layanan kesehatan.

3.8 Kontrak Cerdas dan proses klaim asuransi

A. Ajudikasi otomatis

Kompleksitas penagihan medis dan proses penggantian pihak ketiga untuk pasien sering menyebabkan kebingungan atau kesalahpahaman antara pasien, penyedia medis, dan perusahaan asuransi. Komplikasi ini menyebabkan beberapa konsumen tidak menyadari kapan, kepada siapa, atau berapa jumlahnya mereka harus membayar tagihan medis atau bahkan apakah pembayaran tersebut merupakan tanggung jawab mereka atau penyedia asuransi.

Patientory adalah platform yang dirancang untuk memanfaatkan baik teknologi blockchain Ethereum dan Fast Healthcare Interoperability Resources (FHIR) compliant application program interfaces (APIs) Meningkatkan efisiensi, memungkinkan klaim ajudikasi waktu singkat yang nyata, memberikan kesepakatan yang transparan antara pemangku kepentingan dan mengurangi kecurangan.

FHIR diciptakan sebagai standar industri untuk memformat data sehingga mengurangi kerumitan integrasi sistem perawatan kesehatan dan asuransi. Aspek penting untuk solusi kami, karena biaya penambahan data ke blockchain, membatasi data tersebut hanya pada apa yang dibutuhkan agar kontrak cerdas dijalankan.

Biaya penagihan dan asuransi terkait diperkirakan akan mencapai 315 Milyar dolar (USD) pada tahun 2018 dan kantor medis menghabiskan 3,8 jam setiap minggu untuk berinteraksi dengan pembayar, platform kami dapat memberikan bantuan yang besar terhadap biaya operasional ini.

Metode yang dapat digunakan untuk analisis korelasi silang untuk informasi diagnostik juga dapat digunakan untuk menganalisis data klaim untuk aktivitas penipuan. Analisis ini mungkin juga mengungkapkan tindakan seperti perilaku mencari obat karena contoh dari beberapa klaim-klaim. Kedua kasus penggunaan ini menambahkan proposisi nilai untuk penggunaan sistem ini oleh perusahaan asuransi, namun manfaat utamanya ada di luar informasi ini.

Karena sistem berbasis aturan yang diterapkan oleh sistem kontrak cerdas, seluruh perjanjian cakupan dapat dikodekan dengan kontrak cerdas yang dirujuk terhadap pengguna akhir. Ini memungkinkan fasilitas medis untuk meminta sistem untuk memverifikasi keberadaan cakupan sebelum pemberian layanan. Penggunaan sistem untuk menghost informasi biaya juga memungkinkan penagihan otomatis antara institusi dan individu sebagai token based debt. Dengan demikian, sebuah institusi dan individu dapat dengan mudah mengetahui biaya yang harus dikeluarkan. Ini menghilangkan beban kerja dari departemen akuntansi, sehingga memberi nilai tambahan pada adopsi sistem.

Untuk alasan ini Patientory adalah sistem pembayaran loop tertutup. Diharapkan hubungan lintas rantai bahkan memungkinkan pertukaran nilai yang aman melalui Blokchain Ethereum publik. Mekanisme ini sudah dipecahkan untuk arbitrase transaksi Bitcoin, walaupun memerlukan entitas tepercaya untuk bertindak sebagai Oracle.

B. Kemungkinan

Dengan menggunakan mekanisme yang ada, arsitektur ini dapat segera dibangun. Salah satu contohnya adalah menghubungkan sistem penyimpanan data HIPAA yang sesuai dengan Amazon Web Service dengan ErisDB yang siap disebarkan. SAAS ini memungkinkan penyebaran dengan cepat sebuah kontrak cerdas Ethereum yang mampu memberi blockchain dengan kontrol akses yang diijinkan sepenuhnya seperti yang disebutkan di atas. Penambahan simpul pasif perlu dibangun, namun ini merupakan biaya pengembangan minimal dibandingkan dengan pengembangan arsitektur yang lengkap.

Dengan arsitektur Smart Contract tiga tingkat, hanya sebagian dari fitur kontrak cerdas yang diterapkan pada blockchain Ethereum. Logika bisnis yang kompleks dihapus dari jalur eksekusi, yang memungkinkan tingkat data dioptimalkan untuk merefleksikan sifat terdistribusi jaringan.

Komponen paket kontrak cerdas yang diterapkan pada blochain Ethereum adalah skema database, validasi dan verifikasi transaksi yang ditambahkan ke buku besar dan logika pengoptimalan pertanyaan untuk membaca buku besar.

Logika bisnis ditarik ke atas blockchain Ethereum dengan lapisan tengah (bisnis) yang terpisah. Kode logika ini mengakses berbagai layanan, termasuk eksekusi yang aman, pengesahan, identitas, dukungan kriptografi, pemformatan data, perpesanan handal, pemicu, dan kemampuan untuk mengikat kode tersebut ke skema dalam kontrak pintar tertentu pada berapapun angka blockchain, yang memungkinkan Patieontory mudah di pasang dan dijalankan ke dalam berbagai konsorsium perawatan kesehatan. Layanan ini disediakan dalam rangka, di mana masing-masing potongan kode yang mendukung kontrak cerdas dapat dijalankan, mengirim transaksi ke node blockchain dan terikat pada skema di tingkat data.

3.9 Manfaat Unik Tambahan

Meskipun sebuah institusi medis, seperti rumah sakit seharusnya tidak memiliki akses terhadap catatan yang belum disetujui secara khusus, dengan meminta pengguna memberi otorisasi atas pembagian informasi dalam keadaan darurat, pengguna akhir dapat memperoleh manfaat tambahan dari partisipasi dalam layanan ini. Dengan pemikiran ini, kebutuhan fasilitas medis untuk mengakses catatan orang yang tidak merespons dalam keadaan darurat merupakan situasi yang memerlukan eskalasi hak istimewa karena pengguna telah memberi izin akses ini sebelumnya. Pada peristiwa seseorang tidak memberi respon, dan ponsel mereka tersedia, institusi tersebut bisa membuktikan kepemilikan perangkat individu dengan menggunakan metode tanda tangan sekunder yang dapat diperoleh dari layar kunci ponsel cerdas. Kunci kedua ini bukan kunci privat yang sama dengan akun utama. Jadi, jika sebuah akun institusi mengajukan permintaan kepada blockchain yang berisi kunci publik seorang individu dan telepon pintar dari orang tersebut telah mengajukan tanda tangan darurat, blockchain tersebut dapat meningkatkan hak istimewa untuk memungkinkan akses ke rekam medis yang tidak dapat diaksesnya. **Kunci pribadi ini harus dianggap mudah terbakar dan diganti oleh individu sesegera mungkin. Dengan cara ini, pertukaran informasi yang aman antara individu dan institusi yang berwenang dapat difasilitasi dalam kondisi darurat.**

Jika sebuah institusi meminta informasi ini tanpa autorisasi yang tepat, individu tersebut akan diberi tahu tentang tindakan tersebut. Jika individu menolak permintaan ini dalam interval ambang batas, data tidak dibagi. Selanjutnya, jika sebuah institusi mencoba beberapa permintaan palsu, institusi tersebut mungkin terkena hukuman dengan mencabut hak istimewa, hukuman moneter, dan / atau tindakan hukum. Kerusakan yang disebabkan oleh kehilangan perangkat selular sangat minim karena kebutuhan akan perangkat seluler dan kunci tingkat institusi. Di masa yang akan datang, semua kartu asuransi bisa disematkan dengan mikrokontroler kriptografi, seperti kartu kredit modern, yang akan memudahkan operasi yang sama tanpa tergantung pada ponsel pintar.

4 Prioritas Perawatan Kesehatan Nasional / Internasional

4.1 Perawatan yang dipersonalisasi

Untuk mencapai perawatan superior yang efektif, pendekatan sentris seseorang penting dilakukan. Pendekatan semacam itu harus memperhitungkan tidak hanya aspek klinis namun faktor sosial dan ekonomi yang menghambat kemampuan seseorang untuk berhasil terlibat dalam kepatuhan perawatan dan hidup sehat untuk menghasilkan kesehatan yang berkelanjutan.

Untuk menghasilkan hasil perawatan yang tepat memerlukan identifikasi hambatan lingkungan kesehatan dan kehidupan pribadi secara jelas. Dengan bertambahnya jumlah pasien yang memiliki komorbiditas 2+, jenis perawatan yang "diam-diam" dalam semua pendekatan pemberian perawatan tidak kondusif dalam memotivasi dan menangani hasil perawatan yang efektif. Dengan bertambahnya jumlah pasien yang memiliki komorbiditas 2+, jenis perawatan yang "diam-diam" dalam semua pendekatan pemberian perawatan, tidak kondusif dalam memotivasi dan menangani hasil perawatan yang efektif. Oleh karena itu, model perawatan yang lebih fleksibel yang disesuaikan untuk mencakup kebutuhan kesehatan dan rasa ingin sehat beragam pasien harus dipertimbangkan. Ini memerlukan rencana perawatan interaktif dinamis yang komprehensif dimana pasien dapat secara aktif melacak, mengelola, dan berpartisipasi dalam perawatan individu adalah vital.

4.2 Hasil Klinis

Patient-related outcome measures (PROMs) Hasil pengukuran terkait pasien yang berfokus pada hasil yang berhubungan langsung dengan pasien, telah mempertimbangkan kepentingan dan signifikansi lebih lanjut dalam beberapa tahun terakhir. Hal ini disebabkan, sebagian, pada perhatian yang meningkat terfokus pada pengalaman perawatan pasien dan untuk memberikan fokus perhatian pada beban dan dampak penyakit pada pasien. PROM dapat mencakup gejala dan aspek lain dari indikator kualitas hidup terkait kesehatan seperti fungsi fisik atau sosial, kepatuhan pengobatan, dan kepuasan dengan pengobatan. Mereka juga dapat memfasilitasi komunikasi pasien-dokter yang lebih akurat dalam hal beban morbiditas terkait pengobatan dengan memberikan evaluasi pengobatan yang lebih rinci dan lengkap untuk kondisi spesifik, seperti kanker atau multiple sklerosis.

PROM berbeda dengan ukuran kelayakan klinis tradisional (misalnya, bertahan hidup dalam kanker, penghentian merokok) karena mereka secara langsung mencerminkan dampak penyakit dan penanganannya dari sudut pandang pasien. Langkah-langkah ini dapat memeriksa keseimbangan antara efisiensi pengobatan dan bebannya terhadap pasien. Hal ini juga efektif untuk melihat area seperti fungsi fisik dan kesejahteraan keseluruhan, dan menyoroti kesesuaian dan keamanan perawatan sehubungan dengan manfaat klinisnya secara keseluruhan. Karena tindakan itu sendiri dikembangkan dari sudut pandang pasien, ia juga dapat memfasilitasi keterlibatan pasien yang lebih besar dalam penanganan keputusan pengobatan serta memberikan panduan untuk dekripsi perawatan kesehatan. Intinya, memperkuat infrastruktur PROM blockchain memperkuat kemampuan untuk memberi insentif kepada penyedia dan pembayar dalam memenuhi standar perawatan.

5 Kesimpulan

Blockchain akan memainkan peran yang semakin penting dalam perawatan kesehatan TI dan membawa gangguan yang bermanfaat dan efisiensi baru kepada setiap pemangku kepentingan di ekosistem. Sangat penting bahwa organisasi perawatan kesehatan memahami inti teknologi blockchain untuk memastikan mereka siap menghadapi perubahan teknologi.

Hasilnya akan menjadi generasi baru dari aplikasi berbasis blockchain yang kuat yang akan membentuk era bisnis berikutnya dalam perawatan kesehatan. Agar blockchain dapat memenuhi potensinya dalam perawatan kesehatan, maka harus didasarkan pada standar untuk memastikan kompatibilitas dan interoperabilitas dalam lanskap sistem perawatan tertutup.

www.patientory.com
Google Slack Twitter Facebook Reddit BitcoinTalk GitHub Telegram Medium

Referensi

[1] "A Begoyan. An overview of interoperability standards for electronic health records." In: (2007.).

[2] Charles N Mead et al. "Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still dicult. do we really need a better mousetrap?" In: (2006.).

[3] Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. "MedRec". In: (2016). URL: www.pubpub.org/pub/medrec.[Accessed:05-Apr-2017].

[4] National Healthcare Ant-Fraud Association. "The Challenge of Health Care Fraud". In: (). URL: https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

[5] Vitalik Buterin. "A next-generation smart contract and decentralized application platform. White Paper". In: (2014.).

[6] Yan-Cheng Chang and Michael Mitzenmacher. "Privacy preserving keyword searches on remote encrypted data.In International Conference on Applied Cryptography and Network Security". In: ().

[7] Mayo Clinic. "Changes in Burnout and Satisfaction With Work-Life Balance in Physicians and the General US Working Population Between 2011 and 2014". In: (). URL: www.mayoclinicproceedings.org.

[8] Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. "Reidao: Digitising Real Estate Ownership". In: (). URL: http://reidao.io/whitepaper.pdf.

[9] et al. Centers for Disease Control Prevention. "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services." In: (2003.).

[10] Roy Thomas Fielding. "Architectural styles and the design of network-based software architectures." In: (2000.).

[11] HHS.gov. "H. H. S. O. of the Secretary Summary of the HIPAA Privacy Rule". In: (2013). URL: www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.[Accessed:04-Apr-2017].

[12] HHS.gov. "Methods for De-identification of PHI". In: (2015). URL: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected.[Accessed:04-Apr-2017].

[13] Alex Mizrahi Iddo Bentov Charles Lee and Meni Rosenfeld. "Proof of activity: Extending bitcoin's proof of work via proof of stake." In: (2014).

[14] Sunny King and Scott Nadal. "PPCoin: Peer-to-peer crypto-currency with proof-of-stake." In: (2012).

[15] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: (2008).

[16] Stean D Norberhuis. In: ().

[17] Pishing Chiang Philip Chuang Maureen Madden Rainer Winnen-burg Rob McClure Steve Emrick Olivier Bodenreider Duc Nguyen and Ivor DSouza. “The NLM Value Set Authority Center.” In: (2013.).

[18] Amit P Sheth. “Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In Interoperating Geographic Information Systems,” in: (1999.).

[19] Nick Szabo. “Formalizing and securing relationships on public networks.” In: (1997.).

[20] “US GPO. CFRx 164 security and privacy. 2008.” In: (). URL: http://www.access.gpo.gov/nara/cfr/waisidx08/45cfr16408.html. Accessed:2016-08-06..