Patientory: Mạng lưu trữ EMR ngang hàng chăm sóc sức khỏe v1.1

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

Tháng 5 năm 2017

Tóm tắt

Trao đổi thông tin sức khỏe (HIE) dựa trên blockchain có thể mở khóa giá trị thực sự của khả năng tương tác và an ninh mạng. Hệ thống này có tiềm năng loại bỏ sự cản trở và chi phí của các bên trung gian thứ ba hiện tại khi xem xét quản lý sức khỏe dân số. Có những hứa hẹn về tính toàn vẹn của dữ liệu được cải thiện, giảm chi phí giao dịch, phi tập trung hóa và loại bỏ sự trung gian của lòng tin. Khả năng phối hợp chăm sóc bệnh nhân thông qua HIE blockchain về cơ bản sẽ giảm bớt các dịch vụ không cần thiết và các xét nghiệm trùng lặp với việc giảm chi phí và cải thiện hiệu quả của chu trình chăm sóc liên tục, đồng thời tuân thủ tất cả các quy tắc và tiêu chuẩn HIPAA. Một giao thức lấy bệnh nhân làm trung tâm được hỗ trợ bởi công nghệ blockchain, Patientory đang thay đổi cách các bên liên quan trong lĩnh vực chăm sóc sức khỏe quản lý dữ liệu y tế điện tử và tương tác với các nhóm chăm sóc lâm sàng.

1 Giới thiệu

1.1 Blockchain là gì?

Công nghệ đằng sau đồng tiền kỹ thuật số bitcoin, blockchain được bắt nguồn từ một người (hoặc nhóm) ẩn danh, không xác định được gọi là Satoshi Nakamoto.
Từ năm 2009, công nghệ blockchain đã được sử dụng rộng rãi hơn trong ngành tài chính, với nhiều doanh nghiệp và dịch vụ mới hỗ trợ blockchain gia nhập thị trường. Công nghệ blockchain được sử dụng để chia sẻ sổ cái giao dịch trên toàn bộ mạng lưới doanh nghiệp mà không có bất kỳ thực thể nào kiểm soát. Sổ cái phân tán giúp dễ dàng tạo ra các mối quan hệ thương mại hiệu quả về chi phí, nơi hầu như mọi thứ có giá trị đều có thể được theo dõi và giao dịch mà không cần điểm kiểm soát trung tâm. Công nghệ này đặt quyền riêng tư và quyền kiểm soát dữ liệu vào tay

cá nhân. Sự tin tưởng và tính toàn vẹn được thiết lập mà không cần dựa vào bên thứ ba người trung gian.

1.2 Cơ sở hạ tầng chăm sóc sức khỏe hiện tại

Việc điều chỉnh lại từ trọng tâm dựa trên "quy trình" sang "chăm sóc toàn diện cho cá nhân" đòi hỏi các Nhà cung cấp dịch vụ chăm sóc phải hình thành "mạng lưới" cùng nhau làm việc hướng tới một mục tiêu chung là cải thiện kết quả chăm sóc cho bệnh nhân đang được chăm sóc, đối với các đợt chăm sóc sau cấp tính hoặc giữa các đợt chăm sóc cấp tính. Nhu cầu hợp tác giữa những người cung cấp dịch vụ chăm sóc, từ các chuyên gia, bác sĩ chăm sóc chính, người chăm sóc và nhà cung cấp dịch vụ chăm sóc sức khỏe (như chuyên gia dinh dưỡng và y tá phục hồi chức năng) kết quả trong việc sử dụng ngày càng nhiều công nghệ kỹ thuật số. Mặc dù các giải pháp này đã cải thiện đáng kể việc theo dõi và hiệu quả cung cấp dịch vụ chăm sóc, nhưng chúng lại dẫn đến việc tạo ra các kho thông tin y tế, chủ yếu là trong y tế điện tử hệ thống hồ sơ (EMR).

Các tổ chức y tế và chính phủ dành rất nhiều thời gian và tiền thiết lập và quản lý hệ thống thông tin và dữ liệu truyền thống trao đổi; yêu cầu nguồn lực để liên tục khắc phục sự cố, cập nhật trường tham số, thực hiện các biện pháp sao lưu và phục hồi, và trích xuất thông tin cho mục đích báo cáo.

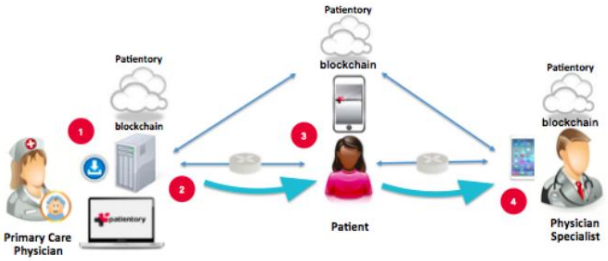
Luật liên bang và các chương trình khuyến khích đã làm cho dữ liệu chăm sóc sức khỏe dễ tiếp cận hơn, để đáp lại sự phản đối của bệnh viện liên quan đến việc triển khai EMR. Tuy nhiên, phần lớn các hệ thống bệnh viện vẫn không thể dễ dàng (hoặc an toàn) chia sẻ dữ liệu của họ. Kết quả là, các bác sĩ dành nhiều thời gian để gõ hơn thực tế nói chuyện với bệnh nhân. Tình trạng kiệt sức của bác sĩ tăng từ 45 đến 54 phần trăm giữa 2011 và 2014 [1].

Mặc dù tồn tại khái niệm về thông tin sức khỏe "cá nhân hóa" cả hai trên phương diện lâm sàng cũng như sức khỏe, những điều này chưa được chuyển thành các kế hoạch chăm sóc "cá nhân hóa" . Hơn nữa, mặc dù có rất nhiều dữ liệu, hệ sinh thái chăm sóc sức khỏe tổng thể không có khả năng thiết kế đầy đủ một giá trị hoặc rủi ro đối với dữ liệu lớn để giúp dự đoán tốt hơn các đợt chăm sóc trong tương lai của bệnh nhân.

Do đó, các giải pháp hiện tại mà ngành công nghệ chăm sóc sức khỏe theo đuổi đã dẫn đến sự lựa chọn khó khăn giữa việc chăm sóc và quyền riêng tư/gian lận kinh tế. cho bệnh nhân. Chúng tôi thấy vấn đề này đang mở rộng đáng kể khi ngành công nghiệp tạo ra nhiều dữ liệu hơn. Công nghệ, thuộc tính và bảo mật của Blockchain bản chất phân tán có thể giúp giảm chi phí và hiệu quả của những hoạt động cũng như cung cấp cơ sở hạ tầng an ninh khả thi.

1.3 Mối quan hệ giữa bệnh nhân và nhà cung cấp

Mô hình chăm sóc sức khỏe mới đòi hỏi nhu cầu chăm sóc hiệu quả và tối ưu cung cấp cho bệnh nhân để mang lại kết quả chăm sóc tốt hơn. Điều này đòi hỏi Hiệu trưởng Các nhà cung cấp dịch vụ chăm sóc có thể chủ động phối hợp và cộng tác với các đơn vị chăm sóc khác các nhà cung cấp liên quan và các tổ chức y tế phụ trợ như Phòng xét nghiệm và Nhà thuốc trong việc cung cấp dịch vụ chăm sóc. Cuối cùng, để điều này thành công, hồ sơ bệnh nhân cần phải được cập nhật và sửa đổi kịp thời.



Hình 1: Sơ đồ bệnh nhân

Phần mềm EMR hiện nay không tạo được mối quan hệ hiệu quả giữa bệnh nhân và nhà cung cấp. Cổng thông tin bệnh nhân có sự tương tác tối thiểu giữa các bệnh nhân, do trải nghiệm của bệnh nhân bị cô lập. Hơn nữa, phần mềm này chỉ cung cấp khả năng trao đổi thông tin hạn chế từ hệ thống này sang hệ thống khác và thường yêu cầu một cá nhân được chỉ định có khả năng chuyển giao thông tin đó.

Điều này dẫn đến sự chậm trễ ngày càng tăng giữa các tổ chức trong việc cung cấp dịch vụ chăm sóc cho bệnh nhân và cũng dẫn đến sự suy giảm chung về chất lượng cung cấp dịch vụ chăm sóc cho bệnh nhân. Ngoài ra, vì các nhà cung cấp dịch vụ chăm sóc dành nhiều thời gian hơn để tham gia vào việc phối hợp chăm sóc, hiệu quả của họ trong việc điều trị bệnh nhân và khối lượng công việc đã tăng lên đáng kể. Điều này dẫn đến tác động phản trực giác trong kết quả chăm sóc cho bệnh nhân.

Ngoài ra, do nhiều bác sĩ không muốn bệnh nhân truy cập EHR, bệnh nhân thụ động trong việc theo dõi sức khỏe của mình. Điều này cuối cùng khiến họ cảm thấy thiếu kiểm soát và sở hữu sức khỏe của mình, dẫn đến bệnh nhân trở nên thất vọng và không tham gia vào việc chăm sóc. Mặc dù gần đây có sự gia tăng các ứng dụng Chăm sóc sức khỏe di động giúp mọi người theo dõi các thông số sức khỏe và các dấu hiệu sinh tồn của họ, nhưng sự mới lạ này không chuyển thành việc cải thiện việc chăm sóc bệnh nhân hoặc tuân thủ và kết quả vì nó cũng phải đối mặt với những thách thức khi tích hợp vào EHR.

2 Tổng quan hệ thống

Những vấn đề hiện tại này được giải quyết bằng cách sử dụng Mạng lưới Blockchain Patientory. EMR cũ là các cấu trúc tập trung dễ bị tấn công, các quy định bảo mật nghiêm ngặt và chi phí quản lý nặng nề. Bằng cách triển khai Blockchain Patientory trong cơ sở hạ tầng, các nhà cung cấp sẽ thấy các vi phạm được giảm thiểu do các thuộc tính kiểm soát truy cập vốn có của hệ thống; một kênh để phối hợp chăm sóc được tạo điều kiện thuận lợi với kết quả là cải thiện tổng thể về kết quả sức khỏe. Trên đây là sơ đồ mô tả cơ sở hạ tầng blockchain Patientory và khả năng tương tác giữa bệnh nhân và nhà cung cấp của họ.

3 Triển khai hệ thống

3.1 Quy định và hướng dẫn tuân thủ HIPAA

Trước bất kỳ cuộc thảo luận có ý nghĩa nào về việc triển khai, các hạn chế được thực thi theo các chỉ thị của Đạo luật về khả năng chuyển đổi và trách nhiệm giải trình bảo hiểm y tế năm 1996 (HIPAA) phải được giải quyết. Các quy tắc quan tâm chính là Quy tắc bảo mật, Quy tắc bảo mật và Nguyên tắc điện toán đám mây. Mục đích của bài viết này không phải là tiến hành điều tra đầy đủ về luật HIPAA. Các yếu tố có liên quan đến thảo luận về việc triển khai sẽ được xác định và thảo luận thêm tại thời điểm áp dụng có liên quan.

A. Quy tắc bảo mật

Mô hình kinh doanh của Patientory quy định rằng các yêu cầu của Quy tắc bảo mật phải được tuân thủ do lưu trữ và truyền thông tin sức khỏe cá nhân qua phương tiện điện tử. Khả năng áp dụng của quy tắc bảo mật được tóm tắt như sau: “Quy tắc bảo mật. . . (áp dụng) cho các chương trình bảo hiểm sức khỏe, trung tâm thanh toán chăm sóc sức khỏe và bất kỳ nhà cung cấp dịch vụ chăm sóc sức khỏe nào truyền thông tin sức khỏe dưới dạng điện tử” [2]. Ngoài các tác nhân này, các bên hành động thay mặt họ, với tư cách là nhà cung cấp dịch vụ, cũng chịu trách nhiệm tuân thủ HIPAA. Các tác nhân thứ cấp này được gọi là Đối tác kinh doanh (BA) và văn bản pháp lý xác định các quy tắc và quy định mà BA phải tuân thủ được gọi là Hợp đồng đối tác kinh doanh (BAC). HIPAA đặt ra các yêu cầu nghiêm ngặt về bản chất của các thỏa thuận này.

Các điểm đáng chú ý, từ một cuộc điều tra ban đầu, là những yêu cầu chỉ định việc cho phép sử dụng, việc sử dụng thông tin ẩn danh và định nghĩa về thông tin riêng tư. Thông tin sức khỏe riêng tư (PHI hoặc ePHI đối với dữ liệu điện tử) được định nghĩa là “tất cả thông tin sức khỏe có thể nhận dạng cá nhân do một thực thể được bảo vệ hoặc đối tác kinh doanh của thực thể đó nắm giữ hoặc truyền đi, dưới bất kỳ hình thức hoặc phương tiện nào, dù là điện tử, giấy tờ hay truyền miệng” [2]. Thông tin sức khỏe ẩn danh được định nghĩa là “Thông tin sức khỏe không nhận dạng một cá nhân và không có cơ sở hợp lý nào để tin rằng thông tin đó có thể được sử dụng để nhận dạng một cá nhân thì không phải là thông tin sức khỏe có thể nhận dạng cá nhân” [2]. Các hạn chế sử dụng dữ liệu ẩn danh được tóm tắt như sau, “Không có hạn chế nào đối với việc sử dụng hoặc tiết lộ thông tin sức khỏe ẩn danh. Thông tin sức khỏe ẩn danh không nhận dạng cũng không cung cấp cơ sở hợp lý để nhận dạng một cá nhân” [3]. Ranh giới giữa dữ liệu có thể nhận dạng và dữ liệu không thể nhận dạng được xác định là bất kỳ thông tin nào có thể hạn chế số lượng cá nhân có thể liên quan đến một bộ sưu tập thông tin xuống dưới 0,04% tổng dân số Hoa Kỳ.

B. Quy tắc bảo mật và hướng dẫn điện toán đám mây Do nội dung

liên quan đến chủ đề này khá dài nên chỉ những yếu tố quan tâm chính mới được tách riêng để tham khảo. Những mối quan tâm chính này như sau: “Khi một thực thể được bảo vệ thuê dịch vụ của CSP để tạo, nhận, duy trì hoặc truyền ePHI (chẳng hạn như để xử lý và/hoặc lưu trữ ePHI), thay mặt cho thực thể đó, CSP là đối tác kinh doanh theo HIPAA. Ngoài ra, khi một đối tác kinh doanh ký hợp đồng phụ với CSP để tạo, nhận, duy trì hoặc truyền

ePHI thay mặt cho mình, bản thân nhà thầu phụ CSP là một đối tác kinh doanh. Điều này đúng ngay cả khi CSP chỉ xử lý hoặc lưu trữ ePHI được mã hóa và không có khóa mã hóa cho dữ liệu. Việc không có khóa mã hóa không miễn trừ CSP khỏi tình trạng và nghĩa vụ của đối tác kinh doanh theo Quy tắc HIPAA. Do đó, thực thể được bảo vệ (hoặc đối tác kinh doanh) và CSP phải ký kết thỏa thuận đối tác kinh doanh (BAA) tuân thủ HIPAA và CSP vừa phải chịu trách nhiệm theo hợp đồng để đáp ứng các điều khoản của BAA vừa phải chịu trách nhiệm trực tiếp để tuân thủ các yêu cầu áp dụng của Quy tắc HIPAA" [3].

Các thực thể được bảo vệ thường sử dụng nhà cung cấp lưu trữ đám mây (CSP) để lưu trữ thông tin sức khỏe, thường trích dẫn rằng nó hiệu quả hơn về mặt chi phí và có chi phí quản lý CNTT thấp hơn. Tuy nhiên, vì người tiêu dùng dựa vào nhà cung cấp đám mây để lưu trữ dữ liệu cá nhân, họ từ bỏ quyền kiểm soát trực tiếp đối với dữ liệu đó và do đó không biết ai có quyền truy cập và dữ liệu nằm ở đâu về mặt địa lý.
Ngay cả khi có thỏa thuận hợp tác kinh doanh rõ ràng giữa BA và nhà cung cấp dịch vụ lưu trữ đám mây, thì thỏa thuận đó cũng chỉ cung cấp các điều khoản về việc ai sẽ chịu trách nhiệm về quyền riêng tư và bảo mật dữ liệu trong trường hợp xảy ra vi phạm. Người tiêu dùng có khả năng kiểm soát quyền truy cập vào các luồng dữ liệu này, nhưng sẽ phải phụ thuộc vào nhà cung cấp lưu trữ đám mây để thực thi các đặc quyền đó.

Mặc dù việc sử dụng lưu trữ đám mây rất phổ biến, nhưng vẫn có một số rủi ro mà người tiêu dùng phải gánh chịu khi sử dụng cơ chế này cho dữ liệu cá nhân của mình. Trong kiến trúc đám mây, dữ liệu được sao chép và di chuyển thường xuyên, do đó rủi ro sử dụng dữ liệu trái phép tăng lên. Ngoài ra, nhiều cá nhân được cấp quyền truy cập tiềm năng vào dữ liệu, chẳng hạn như quản trị viên, kỹ sư mạng và chuyên gia kỹ thuật thực hiện dịch vụ trên hoặc cho máy chủ lưu trữ dữ liệu này. Điều này cũng làm tăng rủi ro truy cập và sử dụng trái phép.

Tuy nhiên, ngay cả khi dữ liệu được bảo mật thông qua các biện pháp kiểm soát truy cập nghiêm ngặt và được mã hóa tại điểm xuất phát và trong quá trình truyền tải, nó vẫn đặt ra vấn đề cho việc phát triển các Biện pháp kết quả do bệnh nhân báo cáo (PROM). Khái niệm về PROM là phát triển một biện pháp tập trung vào bệnh nhân liên quan đến một lĩnh vực hoặc trọng tâm mà bệnh nhân quan tâm và một biện pháp mà sự tham gia và phản hồi của họ là cần thiết để triển khai thành công. Việc truy cập các luồng dữ liệu lớn từ nhiều thiết bị khác nhau là một phần của mạng IoT, như hiện đang được sử dụng, kết hợp với các dịch vụ dựa trên đám mây có thể cung cấp nền tảng để xây dựng PROM, nhưng rất khó để biết liệu dữ liệu đó được lưu trữ trong đám mây có tạo ra một biện pháp có ý nghĩa và mức độ liên quan như mong muốn đối với bệnh nhân hay không.

Việc triển khai công nghệ blockchain để đảm bảo và tăng cường bảo mật dữ liệu cho tất cả hồ sơ y tế liên quan đến hệ thống có thể giảm thiểu vi phạm sức khỏe và phân cấp quyền sở hữu hồ sơ cuối cùng. Quá trình mã hóa dữ liệu khi được gửi đến cơ sở dữ liệu bằng các thuật toán khác nhau và giải mã dữ liệu trong quá trình truy xuất sẽ được sử dụng. Dữ liệu sẽ được mã hóa bằng các thuật toán tuân thủ NIST trong quá trình truyền và truy xuất theo yêu cầu của luật pháp. Do đó, mọi trao đổi thông tin sẽ tuân thủ các thông lệ tốt nhất được nêu trong các thông số kỹ thuật của NIST.

Liên quan đến số lượng vi phạm dữ liệu đang gia tăng nhanh chóng mà ngành chăm sóc sức khỏe phải đối mặt, công nghệ blockchain giúp tuân thủ HIPAA

khả thi cho cả bệnh nhân và nhà cung cấp.

C. Phân tích hệ thống Blockchain về những hạn chế do các hạn chế của HIPAA

Chuỗi khối Ethereum tạo điều kiện cho một tập hợp con đa dạng các triển khai hệ thống do ứng dụng ngôn ngữ lập trình hoàn chỉnh Turing được thực hiện trên Máy ảo Ethereum. Các hệ thống này có những hạn chế trong rằng máy ảo không có sự kiểm tra trực tiếp hướng ra bên ngoài của phần rộng hơn internet ngoại trừ thông qua việc sử dụng Dịch vụ Oracle. Ngoài ra, lưu trữ những hạn chế của blockchain được thực thi bởi chi phí gas của việc lưu trữ và gas chi phí truy cập vào dữ liệu này. Tính đến thời điểm viết bài này, thời gian khối của chuỗi thiết lập một giới hạn tối thiểu cho các yêu cầu sửa đổi của tiểu bang ít nhất là mười lăm giây.

Giới hạn của blockchain trong việc lưu trữ thông tin riêng tư có thể được khắc phục thông qua việc che giấu dữ liệu, chẳng hạn như mã hóa, nhưng trong trường hợp khóa giải mã bị rò rỉ, không có cách nào để xóa dữ liệu nhạy cảm khỏi chuỗi khối. Vì mục đích dữ liệu tuân thủ HIPAA, điều này có thể có khả năng dẫn đến rò rỉ thông tin dai dẳng, không thể sửa chữa được do tính bất biến của chính blockchain. Mặc dù dữ liệu ẩn danh có thể được lưu trữ trên Blockchain Ethereum công khai, nhưng sẽ là thảm họa nếu cho rằng cơ chế lọc nhận dạng sẽ không bao giờ thất bại hoặc thông tin dải phụ liên quan đến tương tác blockchain không thể vô tình tiết lộ danh tính. Kết luận này cũng được đưa ra bởi MIT Media Lab trong quá trình hình thành các Giao thức MedRec và được tóm tắt trong MedRec Sách trắng [3]. Khai thác thông tin dải bên này có thể đơn giản như quan sát dấu thời gian và tương tác với các hợp đồng lưu trữ dữ liệu đã biết.

Thông qua phân tích này có thể liên kết một cá nhân với một tổ chức, và quan trọng hơn là thời gian họ có mặt tại một cơ sở. Với bản chất chuyên môn hóa của một số cơ sở, đây là thông tin đủ để cấu thành hành vi vi phạm tuân thủ HIPAA do người quan sát thụ động có khả năng suy ra cả danh tính, vị trí, thời gian tương tác và có thể là cả lớp chẩn đoán.

Trong khi chờ đợi vị trí này ở xa về bản chất, việc giảm xuống còn ít hơn 0,04% dân số Hoa Kỳ trở nên tầm thường. Những sự thật này cấu thành nên những thất bại đơn lẻ vô lý phải được thừa nhận. Hơn nữa, lưu trữ trực tiếp thậm chí thông tin được mã hóa trên blockchain tạo ra trách nhiệm của người quản lý cơ sở dữ liệu phải nhập vào BAC do hành động của họ như một dữ liệu HIPAA cơ sở lưu trữ (Xem phần có tiêu đề Quy tắc bảo mật và Hướng dẫn điện toán đám mây). Đây là một kỳ vọng vô lý vì mọi thợ đào, và thậm chí cả những người cá nhân lưu trữ các nút thụ động, tất cả đều cần phải tuân thủ HIPAA. Do đối với những lo ngại này, chúng tôi triển khai một cơ chế lưu trữ liên tục thông tin nhạy cảm thông qua việc sử dụng triển khai riêng tư của Ethereum dựa trên blockchain.

D. Mục tiêu triển khai cho khả năng sử dụng và bảo mật

Mục tiêu chính của bất kỳ hệ thống an toàn nào có thể được tóm tắt như sau: về tính bảo mật, tính toàn vẹn, tính khả dụng, tính trách nhiệm và thông tin/nhận dạng đảm bảo. Để đáp ứng được những mục tiêu này, kẻ tấn công và người dùng phải

đã định nghĩa. Mỗi vai trò này đòi hỏi một số sự thừa nhận về khả năng. Theo quan điểm của người dùng, hệ thống cần phải đủ minh bạch để không cần kiến thức nâng cao. Ngoài ra, do người dùng thông thường không thể nắm bắt được những cân nhắc phức tạp về an ninh mạng, nên quy trình cần phải chống lại các hành động của người dùng.

Trong trường hợp một cuộc tấn công xảy ra, hệ thống được tạo ra sao cho lượng công sức phải bỏ ra để xâm phạm một tài nguyên có giá trị hơn giá trị của chính tài nguyên đó. Điều này là do nhận thức rằng một bên đủ tiên tiến với các nguồn lực phù hợp sẽ luôn có khả năng xâm phạm bất kỳ hệ thống nào, nếu có đủ thời gian và công sức. Nói một cách cô đọng hơn, không có biện pháp phòng thủ hoàn hảo nào. Với những hạn chế này trong đầu, bản thân việc triển khai có thể được thảo luận sao cho chúng ta đạt được tất cả các mục tiêu đã đề cập trước đó.

3.2 Định nghĩa về phần cứng và triển khai mạng

Để đáp ứng các mục tiêu thiết kế nêu trên, việc triển khai hệ thống đã chọn đòi hỏi một số hệ thống độc lập. Mỗi hệ thống chia nhỏ thẩm quyền, đảm bảo chỉ những thực thể được ủy quyền mới có thể tương tác theo cách đã được chấp thuận và cung cấp một cơ chế để tăng cường bảo mật trong khi vẫn duy trì tính khả dụng. Hệ thống này cũng đã được thiết kế sao cho việc mở rộng quy mô có thể dễ dàng thực hiện thông qua việc bổ sung các lược đồ gọi phân cấp. Các hệ thống này được mô tả đầy đủ chi tiết bên dưới.

Thực thể công khai là Máy chủ Gọi thủ tục từ xa (RPC) hoạt động như một giao diện với triển khai riêng của Ethereum Blockchain (chuỗi khối được cấp phép). Mạng lưới các nút chuỗi khối này chỉ được phép tương tác với các nút chuỗi khối khác, một thực thể biên soạn khóa, cơ sở lưu trữ tuân thủ HIPAA và Máy chủ RPC. Thực thể biên soạn khóa là tài nguyên tạo cặp khóa riêng tư/công khai để sử dụng trên chuỗi khối.

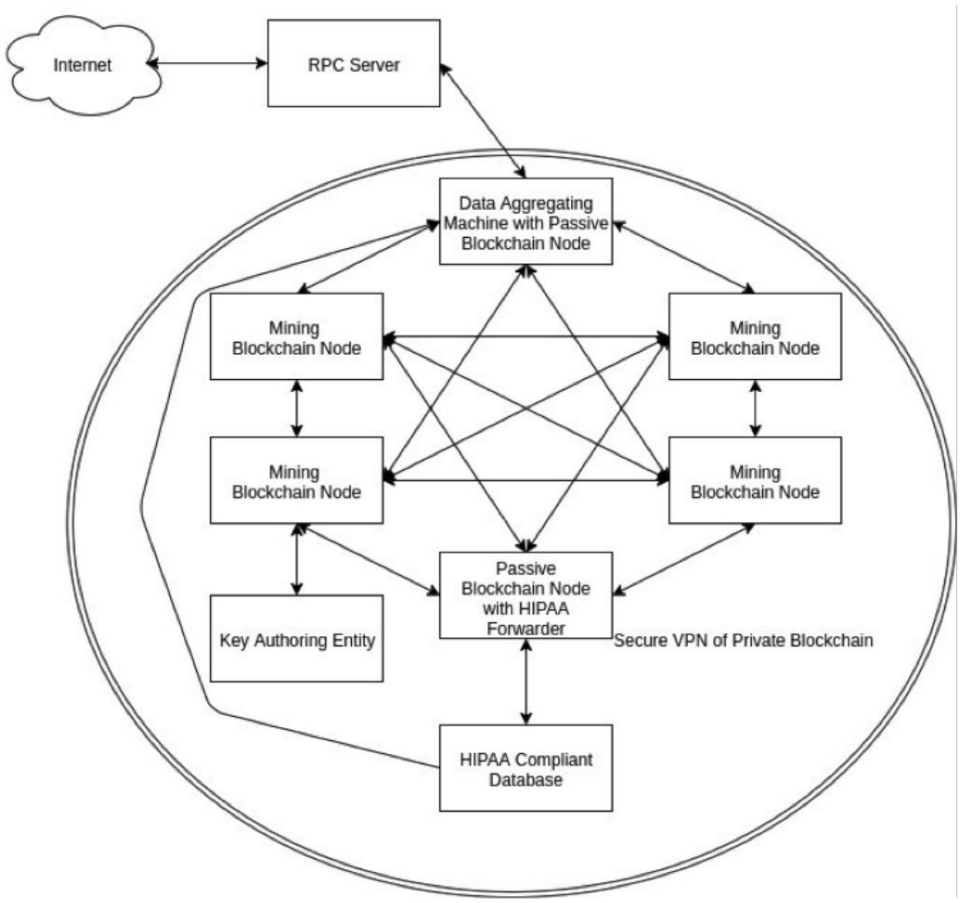
Cơ sở lưu trữ tuân thủ HIPAA lưu trữ dữ liệu thực tế cấu thành thông tin sức khỏe cá nhân điện tử (ePHI).

Khi có yêu cầu dữ liệu, hệ thống tuân thủ HIPAA có thể được ủy quyền để giao tiếp với tác nhân chuyển tiếp, sau đó tác nhân này sẽ định tuyến lại dữ liệu trở lại máy chủ RPC. Ngoài ra, hệ thống có thể được cấu trúc sao cho bộ lưu trữ HIPAA giao tiếp trực tiếp với máy chủ RPC. Mỗi triển khai đều có những lợi ích phải được cân nhắc trước khi lựa chọn cuối cùng. Trong cả hai trường hợp, cơ sở lưu trữ HIPAA sẽ giải mã các phần có liên quan của cơ sở dữ liệu khi xử lý yêu cầu. Sau đó, thông tin đã giải mã này được mã hóa lại bằng khóa công khai của bên yêu cầu để truyền. Khóa công khai này cũng là khóa công khai của hợp đồng đóng vai trò là giao diện điều khiển từ chuỗi khối đến dữ liệu HIPAA.

Sơ đồ cấu trúc mạng được chỉ định có thể được xem ở hình 2.

3.3 Định nghĩa về triển khai phần mềm

Ngoài việc cô lập vật lý các hệ thống trong phần cứng và triển khai mạng, kiểm soát truy cập phần mềm tạo điều kiện thuận lợi cho tính toàn vẹn của dữ liệu và



Hình 2: Địa hình mạng lưới Blockchain của Patientory

xác minh quyền hạn cho các thực thể yêu cầu. Hệ thống phần mềm, theo quan điểm kiểm soát truy cập và mã hóa dữ liệu được mô tả dưới đây.

Cơ sở dữ liệu tuân thủ HIPAA sẽ chỉ chấp nhận các kết nối đến từ bộ chuyển tiếp HIPAA. Điều này đảm bảo rằng luồng lưu lượng được cô lập với các đường dẫn được kiểm soát đã biết. Bộ chuyển tiếp HIPAA sẽ chỉ hoạt động để chuyển tiếp yêu cầu đến cơ sở lưu trữ HIPAA trong khi chờ giao dịch hợp lệ đã xảy ra trên blockchain và giao dịch này dẫn đến việc phát ra sự kiện yêu cầu.

Sự kiện yêu cầu này cần chứa khóa công khai của bên yêu cầu và các trường dữ liệu được yêu cầu. Cuối cùng, máy chủ RPC sử dụng Giao diện chương trình ứng dụng (API) được kiểm soát quyền truy cập sao cho chỉ những người dùng đã biết mới có thể tương tác với máy chủ.

Để hiểu được hệ thống phân cấp cuộc gọi của hệ thống, trước tiên phải giải quyết cấu trúc hợp đồng để tạo điều kiện kiểm soát truy cập. Mỗi người dùng trong hệ thống ánh xạ đến một địa chỉ riêng trên chuỗi khối riêng. Mỗi địa chỉ riêng chỉ được phép nói chuyện trực tiếp với MỘT hợp đồng trên chuỗi khối. Hợp đồng này là hợp đồng lớp của cá nhân. Các tổ chức, nhân viên tổ chức và khách hàng là các đối tượng cấp lớp.

Các đối tượng cấp lớp này là các giao diện dựa trên quyền. Institution Contract có danh sách tất cả khách hàng đã cấp quyền xem cho tổ chức và mỗi hợp đồng khách hàng có danh sách tất cả các tổ chức mà tổ chức đã cấp quyền. Hợp đồng do tổ chức nắm giữ có các chức năng tạo điều kiện cho bất kỳ việc thu hồi quyền nào đối với tổ chức từ người dùng. Hợp đồng của tổ chức không được tự thay đổi danh sách này, do đó ngăn chặn việc truy cập trái phép vào hồ sơ của cá nhân. Ngoài ra, Institution Contract sở hữu danh sách các nhân viên được ủy quyền mà tổ chức có toàn quyền duy trì. Sơ đồ cấp quyền này lý tưởng nhất là phải hoạt động theo cách mà việc thu hồi quyền tự động được thực hiện theo các khoảng thời gian bán đều đặn để ngăn tổ chức vô tình bảo toàn quyền truy cập của các nhân viên cũ.

Trong hệ thống này, tất cả các bên bên ngoài tương tác thông qua việc gửi các giao dịch đã ký mã hóa cuộc gọi yêu cầu. Các giao dịch này được gửi qua máy chủ RPC sau khi người dùng xác thực. Máy chủ RPC đăng các yêu cầu này lên máy chủ tổng hợp dữ liệu, sau đó máy chủ này chuyển tiếp các yêu cầu này đến thợ đào dựa trên cơ chế chia sẻ tải. Sau đó, thợ đào xử lý yêu cầu bằng cách gửi giao dịch thay mặt cho bên gọi đến hợp đồng kiểm soát tương ứng của bên đó. Hợp đồng này nắm giữ các quyền đối với dữ liệu mà thực thể được phép truy cập nội bộ vào hợp đồng. Hợp đồng này là thực thể duy nhất sẽ chấp nhận giao dịch từ yêu cầu bên ngoài. Do đó, một cơ chế được thiết lập để kiểm soát hoàn toàn các hoạt động cuộc gọi trên chuỗi khối.

Đối với bất kỳ giao dịch nào, một bản ghi bất biến của bên gọi được tạo ra. Điều này đảm bảo rằng mọi nỗ lực truy cập thông tin đều được ghi lại. Dữ liệu thực tế được lưu trữ trong hợp đồng người dùng là một hệ thống các con trỏ băm mà khi được máy chủ lưu trữ HIPAA giải quyết sẽ dẫn đến việc trả về dữ liệu phù hợp. Thông tin này được đưa lên bộ chuyển tiếp HIPAA bằng cách thực hiện một giao dịch yêu cầu hợp lệ. Cơ chế tạo điều kiện cho giao tiếp này là gián tiếp và thể hiện thông qua sự kiện blockchain mes-

hệ thống saging. Do hạn chế là người yêu cầu chỉ có thể truy vấn cơ sở dữ liệu bằng giao dịch hợp lệ và người dùng không được trực tiếp thay đổi thông tin của riêng họ, nên có thể chứng minh được quyền kiểm soát truy cập. Theo quan điểm của các tổ chức, các cơ chế tương tự nhau ngoại trừ hợp đồng của tổ chức lưu trữ danh sách người dùng mà hợp đồng có thể yêu cầu dữ liệu và danh sách người dùng có thể tương tác với tổ chức này với tư cách là nhân viên. Khi giao dịch yêu cầu bắt nguồn từ hợp đồng của nhân viên tổ chức, hợp đồng kiểm soát sẽ gọi hợp đồng của tổ chức, hợp đồng này sẽ gọi hợp đồng người dùng để yêu cầu các con trỏ dữ liệu giải quyết ePHI. Trong khi chờ tổ chức nằm trong danh sách các tổ chức được chấp thuận cho người dùng, hợp đồng sẽ trả về các con trỏ băm thích hợp. Sau đó, các con trỏ này được công bố dưới dạng thông báo sự kiện, sau đó lại nổi lên cơ sở lưu trữ HIPAA.

Để rõ ràng hơn, toàn bộ quy trình của một yêu cầu duy nhất như sau: Bên ngoài yêu cầu dữ liệu từ dịch vụ bằng cách gọi máy chủ RPC với giao dịch được ký bằng mật mã để gửi đến blockchain. Máy chủ RPC xác minh danh tính của bên ngoài thông qua chữ ký của yêu cầu đăng nhập.

Trong khi chờ chữ ký khớp với mục nhập trong cơ sở dữ liệu khóa công khai được cấp phép, máy chủ RPC chấp nhận yêu cầu và gửi yêu cầu đến Máy tổng hợp dữ liệu. Sau đó, Máy tổng hợp dữ liệu gửi các yêu cầu đến các trình xác minh chuỗi khối riêng tư. Các trình xác minh nhận yêu cầu dưới dạng cuộc gọi từ tài khoản chuỗi khối đối với hợp đồng mục tiêu. Các trình xác minh thực hiện cuộc gọi này và trong trường hợp yêu cầu là hành động được phép, giao dịch sẽ được nhập vào khối tiếp theo. Giao dịch này cũng gây ra việc phát ra thông báo sự kiện trong chuỗi khối. Thông báo sự kiện này được Bộ chuyển tiếp HIPAA quan sát, bộ phận này sẽ tạo yêu cầu được mã hóa đối với kho lưu trữ HIPAA dựa trên các hàm băm của thông báo sự kiện. Thông báo này cũng chứa khóa công khai của bên yêu cầu. Hệ thống cơ sở dữ liệu tuân thủ HIPAA quan sát yêu cầu này và truyền bản sao thông tin được mã hóa đến máy chủ RPC bằng khóa công khai của bên yêu cầu. Sau đó, máy chủ RPC trả về thông tin này cho bên yêu cầu bằng cách ánh xạ lại IP yêu cầu thành khóa công khai trong thông báo. Máy chủ RPC truyền thông điệp này mà không cần nhìn thấy dữ liệu cơ bản. Dữ liệu này sau đó bị máy chủ RPC hủy ngay lập tức, do đó đảm bảo rằng máy chủ RPC hoạt động như một đường dẫn không cần phải tuân thủ HIPAA.

Cơ chế công bố dữ liệu cũng tương tự về bản chất, nhưng dữ liệu được gửi đi được mã hóa bằng khóa công khai của cơ sở lưu trữ HIPAA. Các hoạt động khác giống hệt nhau ngoại trừ dữ liệu đang được gửi đi sẽ nổi lên thông qua hệ thống tin nhắn sự kiện. Do đó, do sử dụng hàm băm va chạm thấp và nonce có dấu thời gian, dữ liệu có thể được lưu trữ với hợp đồng có khả năng tính toán địa chỉ mà dữ liệu được gửi đi nằm trong cơ sở lưu trữ HIPAA.

Cuối cùng, việc phân phối khóa riêng cho các thực thể phải được giải quyết. Điều này có thể được tạo điều kiện thuận lợi thông qua các phương tiện quang học cho người dùng điện thoại thông minh. Điều này tương tự như việc sử dụng mã QR làm địa chỉ cho các địa chỉ Ethereum. Các phương tiện thay thế cũng có thể được thiết lập bằng cách sử dụng các ứng dụng trên cả máy tính để bàn

và thiết bị máy tính bảng/điện thoại thông minh. Việc mất chìa khóa không phải là sự kiện thảm khốc, do khả năng tước quyền kiểm soát truy cập của hợp đồng kiểm soát từ một chìa khóa và cấp cho chìa khóa khác.

3.4 Khả năng tương tác

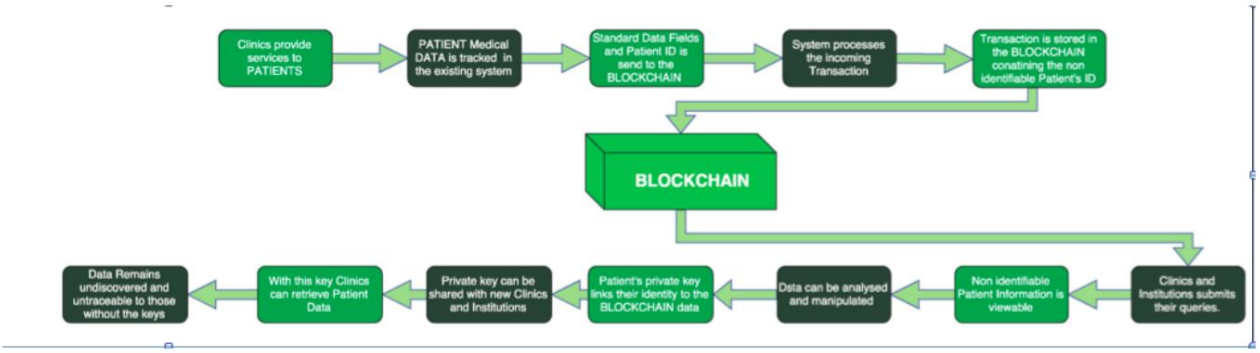
Hệ thống EHR dựa trên kiến trúc xác thực thông tin xác thực riêng biệt trong đó dữ liệu bệnh nhân được lưu giữ trong từng hệ thống riêng biệt. Điều này đã dẫn đến các giải pháp "bổ sung" phần mềm phối hợp chăm sóc một-một cho các hệ thống này để cho phép phối hợp chăm sóc giữa các nhà cung cấp khác và các tổ chức y tế phụ trợ. Tuy nhiên, việc truy cập thông tin từ tổ chức Nhà cung cấp chính đến các tổ chức khác chỉ thông qua khả năng hạn chế trong các trường hợp như Đọc, Gửi, Gửi hoặc Thông báo. Hơn nữa, Bệnh nhân/Người tiêu dùng có rất ít tương tác hoặc sự tham gia vào việc trao đổi thông tin này. Ngoài ra, một nhược điểm đối với các cơ chế trao đổi dữ liệu hiện có là khó khăn trong việc sửa lỗi xảy ra trong quá trình gửi

quá trình.

Khi một blockchain và hợp đồng thông minh của nó được cấu hình, các tham số trở nên tuyệt đối. Bệnh nhân trở thành trung gian chính trong việc gửi và nhận thông tin sức khỏe, phủ nhận nhu cầu cập nhật thường xuyên và khắc phục sự cố của bất kỳ phần mềm nào. Vì hồ sơ blockchain cũng không thể thay đổi và được lưu trữ trên tất cả người dùng tham gia, nên các tình huống bất trắc khi khôi phục là không cần thiết. Hơn nữa, cấu trúc thông tin minh bạch của blockchain có thể xóa bỏ nhiều điểm tích hợp trao đổi dữ liệu và các hoạt động báo cáo tốn thời gian.

3.5 Quy trình và khả năng mở rộng

Người dùng kiểm soát mọi thông tin và chuyển giao của họ, đảm bảo dữ liệu chất lượng cao, đầy đủ, nhất quán, kịp thời, chính xác và có sẵn rộng rãi, do đó làm cho dữ liệu bền vững và đáng tin cậy. Do cơ sở dữ liệu phi tập trung, blockchain không có điểm lỗi trung tâm và có khả năng chống lại các cuộc tấn công độc hại tốt hơn.



Hình 3: Sơ đồ quy trình Blockchain

Trong bất kỳ mạng lưới chăm sóc nào, cần phải đảm bảo rằng những người tham gia đang hợp tác với nhau có thể phụ thuộc vào nhau để cung cấp các dịch vụ cần thiết mà họ mong đợi. Để đạt được điều đó, phải có một phương tiện để đảm bảo trách nhiệm giải trình về nhiệm vụ và dịch vụ được mong đợi sẽ được cung cấp kịp thời và cũng như trách nhiệm liên quan nếu chúng không được cung cấp kịp thời ở mức chất lượng mong đợi. Do đó, bất kỳ cơ sở hạ tầng chăm sóc sức khỏe nào cũng phải có khả năng giám sát thông tin cần thiết một cách liền mạch để cho phép Nhà cung cấp dịch vụ chăm sóc chính đánh giá mạng lưới chăm sóc của mình. Hơn nữa, khi mạng lưới chăm sóc phát triển và sự tương tác giữa các nhà cung cấp dịch vụ chăm sóc trong mạng lưới tăng lên, cơ sở hạ tầng chăm sóc sức khỏe phải có khả năng giải quyết hiệu quả quy mô này.

Yếu tố then chốt để xây dựng một hệ thống Quản lý Chăm sóc có khả năng mở rộng và phân tán cao là một khuôn khổ kiến trúc ngang hàng. Một khuôn khổ như vậy đã được sử dụng trong một số phân khúc công nghiệp như truyền thông, thể thao, bất động sản, chuỗi cung ứng, hiển thị blockchain có thể dễ dàng trở thành một phần mềm kết nối bổ sung cho các khuôn khổ tập trung hiện có[7]. Điều này đã dẫn chúng tôi đến việc khám phá việc sử dụng khuôn khổ chuỗi khối vì khả năng ứng dụng của nó để hỗ trợ cho việc tạo ra một khuôn khổ ngang hàng cho chăm sóc sức khỏe.

Blockchain hứa hẹn sẽ xác thực hai hoặc nhiều thực thể tham gia vào một “giao dịch chăm sóc sức khỏe” . Điều này cung cấp hai thuộc tính chính so với mô hình xác thực tập trung. Đầu tiên là các bên quan tâm có thể tương tác với nhau ở “mức độ giao dịch” của “mối quan hệ tin cậy” .

Thứ hai là việc tiếp xúc với trách nhiệm pháp lý trong mối quan hệ như vậy chỉ giới hạn ở mức độ tham gia “giao dịch” . Điều này rất hữu ích vì nó hạn chế quyền truy cập thông tin và trách nhiệm pháp lý giữa các bên liên quan và đồng thời cho phép một bên tham gia vào mối quan hệ giao dịch với một số nhà cung cấp khác dựa trên năng lực cụ thể và loại hình chăm sóc sẽ cung cấp cho bệnh nhân. Điều này tốt hơn đáng kể so với các hệ thống tập trung thông thường cần hạn chế số lượng nhà cung cấp cho nhiều nhu cầu của bệnh nhân do phải nỗ lực quản lý quyền truy cập và trách nhiệm pháp lý.

3.6 Trao đổi thông tin sức khỏe và mã thông báo

Token Patientory (PTOY) là nhiên liệu thúc đẩy cơ sở hạ tầng blockchain. Mục đích sử dụng chính của token là để điều chỉnh phân bổ lưu trữ mạng, các biện pháp chất lượng chăm sóc sức khỏe và chu kỳ thanh toán doanh thu.

Bệnh nhân được cấp một lượng không gian được phân bổ để lưu trữ thông tin miễn phí trên mạng Patientory. PTOY cho phép họ mua thêm không gian lưu trữ từ các nút được thiết lập trong hệ thống bệnh viện. PTOY có thể được mua thông qua nền tảng hoặc trao đổi.

Các tổ chức chăm sóc sức khỏe cũng sử dụng PTOY trong trường hợp này. Nó cũng được sử dụng trong thanh toán sau khi hợp đồng thông minh được thực hiện với các công ty bảo hiểm chăm sóc sức khỏe và đóng vai trò là cơ chế để điều chỉnh các số liệu mô hình dựa trên giá trị.

Để Hoa Kỳ có thể chuyển đổi thành công từ mô hình trả tiền cho dịch vụ sang mô hình dựa trên giá trị hiện tại, phải có cơ sở hạ tầng CNTT chăm sóc sức khỏe cho phép các tổ chức liên kết chất lượng, giá trị và hiệu quả của y tế.

can thiệp thông qua mô hình bồi thường có uy tín.

Tiền bồi thường sẽ dựa trên mức độ hiệu quả của mạng lưới các nhà cung cấp làm việc cùng nhau để đảm bảo cải thiện chất lượng chăm sóc và kết quả sức khỏe, đồng thời giảm chi phí chăm sóc liên quan. Để thực sự khuyến khích những người tham gia khác nhau trong mạng lưới chủ động tạo ra các chế độ chăm sóc tốt hơn, một khoản bồi thường dựa trên thành tích của các khoản tiết kiệm được chia sẻ (hoàn trả) sẽ có hiệu lực. Để phân bổ hiệu quả một phần chia sẻ tương ứng cho nhà cung cấp trong mạng lưới đóng góp nhiều nhất vào tổng số tiền tiết kiệm, một sự theo dõi rõ ràng về đóng góp của họ có thể đo lường được bằng các hợp đồng thông minh trên mạng blockchain.

Một tác động quan trọng khác của mô hình chăm sóc sức khỏe mới là mô hình bồi thường, trong đó các nhà cung cấp đủ điều kiện để nhận được khoản bồi thường bổ sung ngoài dịch vụ chăm sóc được cung cấp. Khoản bồi thường này là kết quả của khoản tiết kiệm được tạo ra dựa trên mức độ hiệu quả mà các nhà cung cấp quản lý việc chăm sóc kết quả sức khỏe của bệnh nhân (phần thưởng). Bất kỳ khoản tiết kiệm nào được tạo ra thông qua việc quản lý hiệu quả việc chăm sóc bệnh nhân đều có thể được các nhà cung cấp và các đối tác mạng lưới của họ giữ lại như một phần của khía cạnh tiết kiệm được chia sẻ của mô hình chăm sóc sức khỏe mới.

Đề xuất của chúng tôi cung cấp khả năng cho người trả tiền chuyển token như một động lực cho các nhà cung cấp đạt được các số liệu chất lượng này. Khả năng theo dõi và quản lý liền mạch các hợp đồng thông minh trong đó các lợi ích có thể được đổi lại một cách dễ dàng đáng kể cung cấp "củ cà rốt" cần thiết cho các nhà cung cấp và bệnh nhân để tích cực tham gia vào sự hợp tác cộng sinh. Ngược lại, nếu một hoặc nhiều bên tham gia vi phạm, các hình phạt thích hợp, thông qua các khoản nợ phải trả, cũng có thể được áp dụng một cách dễ dàng tương tự. Cách tiếp cận “củ cà rốt/cây gậy” này sẽ cung cấp động lực cần thiết để chuyển ngành chăm sóc sức khỏe từ tư duy quản lý bệnh tật sang tư duy lối sống lành mạnh.

Từ nay trở đi, token do Patientory phát hành (PTOY) là token gốc của nền tảng Patientory. Khi đổi token PTOY, người dùng sẽ có thể sử dụng mạng để thuê không gian lưu trữ thông tin sức khỏe và thực hiện các giao dịch và thanh toán hợp đồng thông minh dành riêng cho sức khỏe.

Chúng tôi tin chắc rằng sử dụng mã thông báo là hệ thống thanh toán tốt nhất để hỗ trợ cơ sở hạ tầng này trong tương lai gần. Tương lai là một hệ sinh thái sôi động của nhiều mã thông báo, trong đó chăm sóc sức khỏe sẽ cần một hệ thống thanh toán vòng kín. Kết quả sẽ là một vòng phản hồi tích cực quản lý chu trình chăm sóc hiệu quả với mức giảm đáng kể hàng tỷ đô la hiện đang được quy cho gian lận thanh toán chăm sóc sức khỏe [4].

Hệ thống cũng khuyến khích các tổ chức lớn có đủ dung lượng lưu trữ máy chủ để giao dịch token với các tổ chức chăm sóc sức khỏe vừa và nhỏ, những tổ chức này sẽ cần truy cập trực tiếp vào mạng lưới sức khỏe blockchain mà không cần triển khai trực tiếp một nút. Mặc dù các chính sách chăm sóc sức khỏe mới có tiềm năng khuyến khích các nhà cung cấp hợp tác để cải thiện các lộ trình chăm sóc, nhưng các kiến trúc EHR hiện tại không thể thực hiện được khả năng này, do đó, chỉ cần cấp hoặc nhận token là có thể tạo điều kiện thuận lợi cho quá trình này.

Do đó, giá trị của các mã thông báo được gắn với khối lượng giao dịch được thực hiện trong mạng. Khi mạng Patientory liên tục tăng lên

giao dịch mã thông báo nhu cầu về mã thông báo tăng lên, dẫn đến giá trị tăng lên.

Hình 4: Giá trị mã thông báo Patientory như một chức năng của giao dịch

3.7 Thu thập mã thông báo

PTOY có thể được mua thông qua ứng dụng gốc của Patientory, thị trường tiền điện tử và từ bệnh nhân, bác sĩ hoặc công ty bảo hiểm khác thông qua chuyển khoản. Người dùng nền tảng sẽ có khả năng mua PTOY bằng cách gửi Ether (“ETH”) vào hợp đồng tạo PTOY trên blockchain trong quá trình bán trước. Giao diện Patientory sẽ tích hợp các giải pháp giao dịch của bên thứ ba như Shapeshift và Coinbase cho những người dùng không có ETH.

Đợt phân phối đầu tiên của Patientory Token sẽ được thực hiện dưới hình thức bán trước. Bất kỳ ai cũng có thể mua PTOY với mức giá chiết khấu bằng cách thế chấp ETH vào hợp đồng thông minh bán token. Những người có các loại tiền điện tử khác như ETC hoặc BTC có thể tạo PTOY thông qua dịch vụ chuyển đổi của bên thứ ba sẽ có trên trang trước khi bán.

Nhóm sáng lập sẽ nhận được 10% phân bổ PTOY, tùy thuộc vào thời hạn nắm giữ mười hai tháng. Các mã thông báo này sẽ đóng vai trò là động lực dài hạn cho nhóm sáng lập Patientory. 20% bổ sung sẽ được phân bổ cho quỹ Patientory Foundation để sử dụng cho nghiên cứu và phát triển liên quan đến công nghệ blockchain cho các trường hợp sử dụng chăm sóc sức khỏe.

3.8 Hợp đồng thông minh và xử lý yêu cầu bảo hiểm

A. Tự động xét xử

Sự phức tạp của việc lập hóa đơn y tế và quy trình hoàn trả của bên thứ ba cho bệnh nhân thường dẫn đến sự nhầm lẫn hoặc hiểu lầm giữa bệnh nhân, nhà cung cấp dịch vụ y tế và công ty bảo hiểm. Những phức tạp này khiến một số người tiêu dùng không biết khi nào, cho ai hoặc số tiền họ nợ hóa đơn y tế hoặc thậm chí là liệu việc thanh toán là trách nhiệm của họ hay của công ty bảo hiểm.

Patientory là một nền tảng được thiết kế để tận dụng cả công nghệ chuỗi khối Ethereum và giao diện chương trình ứng dụng (API) tuân thủ Fast Healthcare Interoperability Resources (FHIR) để tăng hiệu quả, cho phép xử lý khiếu nại gần như theo thời gian thực, cung cấp các thỏa thuận minh bạch giữa các bên liên quan và giảm gian lận.

FHIR được tạo ra như một tiêu chuẩn công nghiệp để định dạng dữ liệu, do đó làm giảm sự phức tạp trong tích hợp cho các hệ thống kế thừa về chăm sóc sức khỏe và bảo hiểm. Một khía cạnh quan trọng đối với giải pháp của chúng tôi, do chi phí thêm dữ liệu vào blockchain, là giới hạn dữ liệu đó chỉ ở mức cần thiết để các hợp đồng thông minh thực hiện.

Với chi phí liên quan đến thanh toán và bảo hiểm dự kiến đạt 315 tỷ đô la (USD) vào năm 2018 và các phòng khám dành 3,8 giờ mỗi tuần để tương tác với bên thanh toán, nền tảng của chúng tôi có thể giúp giảm đáng kể các chi phí hoạt động này.

Các phương pháp có thể được sử dụng để phân tích tương quan chéo cho thông tin chẩn đoán cũng có thể được sử dụng để phân tích dữ liệu khiếu nại về hoạt động gian lận. Phân tích này cũng có thể tiết lộ các hành động như hành vi tìm kiếm thuốc do trường hợp khiếu nại nhiều lần. Cả hai trường hợp sử dụng này đều bổ sung các đề xuất giá trị cho việc sử dụng hệ thống này của các công ty bảo hiểm, nhưng lợi ích cuối cùng nằm ngoài thông tin này.

Do hệ thống dựa trên quy tắc được thực thi bởi hệ thống hợp đồng thông minh, toàn bộ thỏa thuận bảo hiểm có thể được mã hóa thành hợp đồng thông minh được tham chiếu đến người dùng cuối. Điều này sẽ cho phép cơ sở y tế truy vấn hệ thống để xác minh sự tồn tại của phạm vi bảo hiểm trước khi cung cấp dịch vụ. Việc sử dụng hệ thống để lưu trữ thông tin chi phí cũng cho phép tự động lập hóa đơn giữa các tổ chức và cá nhân dưới dạng nợ dựa trên mã thông báo. Do đó, một tổ chức và một cá nhân có thể dễ dàng biết được chi phí khi chúng phát sinh.

Điều này giúp giảm bớt khối lượng công việc cho bộ phận kế toán, do đó tăng thêm giá trị cho việc áp dụng hệ thống.

Vì lý do này, Patientory là một hệ thống thanh toán vòng kín. Người ta hy vọng rằng liên kết chuỗi chéo thậm chí có thể cho phép trao đổi giá trị an toàn thông qua Ethereum Blockchain công khai. Cơ chế này đã được giải quyết để phân xử các giao dịch Bitcoin, mặc dù nó đòi hỏi một thực thể đáng tin cậy để hoạt động như một Oracle.

B. Khả thi Thông qua

việc sử dụng các cơ chế hiện có, kiến trúc này có thể được xây dựng dễ dàng. Một ví dụ như vậy là việc liên kết hệ thống lưu trữ dữ liệu tuân thủ HIPAA của Amazon Web Service với ErisDB có thể triển khai dễ dàng.

SAAS này cho phép triển khai nhanh chóng một blockchain có khả năng hợp đồng thông minh Ethereum với các quyền kiểm soát truy cập được cấp phép đầy đủ như đã đề cập ở trên. Việc bổ sung các nút thụ động sẽ cần phải được xây dựng, nhưng đây là chi phí phát triển tối thiểu so với việc phát triển toàn bộ kiến trúc.

Với kiến trúc Hợp đồng thông minh ba tầng của Patientory, chỉ một tập hợp con các tính năng của hợp đồng thông minh được triển khai trên chuỗi khối Ethereum.

Logic kinh doanh phức tạp được loại bỏ khỏi đường dẫn thực thi, cho phép tối ưu hóa tầng dữ liệu để phản ánh bản chất phân tán của mạng.

Các thành phần của gói hợp đồng thông minh được triển khai trên chuỗi khối Ethereum là lược đồ cơ sở dữ liệu, xác thực và kiểm tra các giao dịch được thêm vào sổ cái và logic tối ưu hóa truy vấn để đọc sổ cái.

Logic kinh doanh được kéo lên trên blockchain Ethereum đến một lớp trung gian (kinh doanh) riêng biệt. Mã logic này truy cập vào nhiều dịch vụ khác nhau, bao gồm thực thi an toàn, xác thực, nhận dạng, hỗ trợ mật mã, định dạng dữ liệu, nhắn tin đáng tin cậy, kích hoạt và khả năng liên kết mã đó với lược đồ trong các hợp đồng thông minh cụ thể trên bất kỳ số lượng blockchain nào, cho phép Patientory cắm và chạy vào nhiều tập đoàn chăm sóc sức khỏe khác nhau. Các dịch vụ này được cung cấp trong một nền tảng, trong đó các đoạn mã riêng lẻ hỗ trợ các hợp đồng thông minh có thể thực thi, gửi giao dịch đến các nút blockchain và được liên kết với lược đồ trong tầng dữ liệu.

3.9 Các lợi ích độc đáo bổ sung

Mặc dù một tổ chức y tế, chẳng hạn như bệnh viện không được phép truy cập vào bất kỳ hồ sơ nào chưa được phê duyệt cụ thể, nhưng bằng cách yêu cầu người dùng ủy quyền trước việc chia sẻ thông tin trong trường hợp khẩn cấp, người dùng cuối có thể nhận được lợi ích bổ sung khi tham gia vào dịch vụ. Với suy nghĩ này, nhu cầu của một cơ sở y tế để truy cập vào hồ sơ của một người không phản hồi trong trường hợp khẩn cấp cấu thành một tình huống xứng đáng được tăng đặc quyền vì người dùng đã ủy quyền truy cập này trước đó. Trong trường hợp một người không phản hồi và có điện thoại di động của họ, tổ chức có thể chứng minh quyền sở hữu thiết bị của một cá nhân bằng cách sử dụng phương pháp chữ ký thứ cấp có sẵn từ màn hình khóa của điện thoại thông minh. Khóa thứ hai này không được là khóa riêng giống với khóa chính của tài khoản. Do đó, nếu một tài khoản của tổ chức gửi yêu cầu đến chuỗi khối chứa khóa công khai của một cá nhân và điện thoại thông minh của cá nhân đó đã gửi chữ ký khẩn cấp, chuỗi khối có thể tăng đặc quyền để cho phép truy cập vào hồ sơ y tế mà nếu không thì nó sẽ không có quyền truy cập. Khóa riêng này nên được coi là có thể ghi và được cá nhân thay thế càng sớm càng tốt. Theo cách này, việc trao đổi thông tin an toàn giữa cá nhân và tổ chức được ủy quyền có thể được tạo điều kiện thuận lợi trong các trường hợp khẩn cấp.

Nếu một tổ chức yêu cầu thông tin này mà không có sự cho phép thích hợp, cá nhân sẽ được thông báo về các hành động. Nếu cá nhân từ chối yêu cầu này trong khoảng thời gian ngưỡng, dữ liệu sẽ không được chia sẻ. Hơn nữa, nếu một tổ chức cố gắng thực hiện nhiều yêu cầu gian lận, tổ chức đó có thể bị trừng phạt bằng cách thu hồi đặc quyền, phạt tiền và/hoặc hành động pháp lý.
Thiệt hại do mất thiết bị di động là tối thiểu do cần cả thiết bị di động và khóa cấp độ tổ chức. Trong tương lai gần, tất cả các thẻ bảo hiểm có thể được nhúng bộ vi điều khiển mật mã, chẳng hạn như thẻ tín dụng hiện đại, giúp thực hiện cùng một hoạt động độc lập với điện thoại thông minh.

4 Ưu tiên chăm sóc sức khỏe quốc gia/quốc tế

4.1 Chăm sóc cá nhân

Để đạt được hiệu quả chăm sóc cao cấp, một cách tiếp cận lấy con người làm trung tâm là rất quan trọng. Một cách tiếp cận như vậy phải tính đến không chỉ các khía cạnh lâm sàng mà còn các yếu tố xã hội và kinh tế cản trở khả năng tham gia thành công vào việc tuân thủ chăm sóc và lối sống lành mạnh để mang lại sức khỏe bền vững.

Để mang lại kết quả chăm sóc hiệu quả đòi hỏi phải xác định rõ ràng các rào cản của tình hình sức khỏe và cuộc sống cá nhân. Với số lượng bệnh nhân mắc 2+ bệnh đi kèm ngày càng tăng, cách tiếp cận cung cấp dịch vụ chăm sóc “cô lập” một loại chăm sóc phù hợp với tất cả không có lợi cho việc thúc đẩy và giải quyết các kết quả chăm sóc hiệu quả. Do đó, cần phải xem xét một mô hình chăm sóc linh hoạt hơn được thiết kế riêng để bao gồm các nhu cầu sức khỏe và thể chất đa diện của bệnh nhân. Điều này đòi hỏi phải có một kế hoạch chăm sóc tương tác toàn diện, năng động trong đó bệnh nhân có thể chủ động theo dõi, quản lý và

tham gia vào việc chăm sóc cá nhân là rất quan trọng.

4.2 Kết quả lâm sàng

Các biện pháp đánh giá kết quả liên quan đến bệnh nhân (PROM), tập trung vào các kết quả có liên quan trực tiếp đến bệnh nhân, đã trở nên quan trọng và có ý nghĩa hơn trong vài năm qua. Một phần là do sự chú ý ngày càng tăng tập trung vào trải nghiệm chăm sóc của bệnh nhân và cung cấp đánh giá tập trung vào bệnh nhân về gánh nặng và tác động của bệnh. PROM có thể bao gồm các triệu chứng và các khía cạnh khác của các chỉ số chất lượng cuộc sống liên quan đến sức khỏe như chức năng thể chất hoặc xã hội, tuân thủ điều trị và sự hài lòng với điều trị. Chúng cũng có thể tạo điều kiện cho việc giao tiếp chính xác hơn giữa bệnh nhân và bác sĩ về gánh nặng của các bệnh liên quan đến điều trị bằng cách cung cấp đánh giá chi tiết và đầy đủ hơn về các phương pháp điều trị cho các tình trạng cụ thể, chẳng hạn như ung thư hoặc đa xơ cứng.

PROM khác với các biện pháp hiệu quả lâm sàng truyền thống (ví dụ, sống sót sau ung thư, cai thuốc lá) vì chúng phản ánh trực tiếp tác động của bệnh và việc điều trị theo quan điểm của bệnh nhân. Các biện pháp này có thể kiểm tra sự cân bằng giữa hiệu quả của việc điều trị và gánh nặng của nó đối với bệnh nhân.
Nó cũng hiệu quả trong việc xem xét các lĩnh vực như hoạt động thể chất và sức khỏe tổng thể, và làm nổi bật hiệu quả và tính an toàn của các phương pháp điều trị liên quan đến lợi ích lâm sàng tổng thể của nó. Vì các biện pháp tự thân được phát triển từ góc nhìn của bệnh nhân, nên nó cũng có thể tạo điều kiện cho bệnh nhân tham gia nhiều hơn vào quá trình ra quyết định điều trị cũng như cung cấp hướng dẫn cho các quyết định chăm sóc sức khỏe. Về cơ bản, việc củng cố cơ sở hạ tầng PROM blockchain củng cố khả năng khuyến khích các nhà cung cấp và bên thanh toán đáp ứng các tiêu chuẩn chăm sóc.

5 Kết luận

Blockchain sẽ đóng vai trò ngày càng quan trọng trong CNTT chăm sóc sức khỏe và mang lại sự gián đoạn có lợi cùng hiệu quả mới cho mọi bên liên quan trong hệ sinh thái.
Điều cực kỳ quan trọng là các tổ chức chăm sóc sức khỏe phải hiểu được cốt lõi của công nghệ blockchain để đảm bảo họ sẵn sàng cho những thay đổi mà công nghệ này mang lại.

Kết quả sẽ là một thế hệ mới các ứng dụng mạnh mẽ dựa trên blockchain sẽ định hình kỷ nguyên tiếp theo của doanh nghiệp trong lĩnh vực chăm sóc sức khỏe. Để blockchain phát huy hết tiềm năng của mình trong lĩnh vực chăm sóc sức khỏe, nó phải dựa trên các tiêu chuẩn để đảm bảo tính tương thích và khả năng tương tác trong hệ thống chăm sóc sức khỏe bị cô lập.
cảnh quan.

Tài liệu tham khảo

[1] “A Begoyan. Tổng quan về các tiêu chuẩn khả năng tương tác cho hồ sơ sức khỏe điện tử.” Trong: (2007.).

[2] Charles N Mead và cộng sự. “Tiêu chuẩn trao đổi dữ liệu trong khả năng tương tác ngữ nghĩa có thể tính toán được của CNTT trong chăm sóc sức khỏe: Hiện có thể thực hiện được nhưng vẫn khó. Chúng ta có thực sự cần một cái bẫy chuột tốt hơn không?” Trong: (2006.).

[3] Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. “MedRec” . Trong: (2016). url: www.pubpub.org/pub/medrec.[Truy cập: 05-04-2017].

[4] Hiệp hội chống gian lận chăm sóc sức khỏe quốc gia. “Thách thức của gian lận chăm sóc sức khỏe” . Trong: (). url: https://www.nhcaa.org/resources/health-care - anti - fraud - resources / the - challenge - of - health - care - fraud.aspx.

[5] Vitalik Buterin. “Một hợp đồng thông minh thế hệ tiếp theo và nền tảng ứng dụng phi tập trung. Sách trắng” . Trong: (2014.).

[6] Yan-Cheng Chang và Michael Mitzenmacher. “Bảo vệ quyền riêng tư khi tìm kiếm từ khóa trên dữ liệu được mã hóa từ xa. Trong Hội nghị quốc tế về mật mã ứng dụng và an ninh mạng” . Trong: ().

[7] Mayo Clinic. “Những thay đổi trong tình trạng kiệt sức và sự hài lòng với sự cân bằng giữa công việc và cuộc sống ở các bác sĩ và dân số lao động nói chung của Hoa Kỳ từ năm 2011 đến năm 2014” . Trong: (). url: www.mayoclinicproceedings.org.

[8] Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. “Reidao: Số hóa quyền sở hữu bất động sản” . TRONG: (). url: http://reidao.io/whitepaper. pdf.

[9] et al. Trung tâm Kiểm soát và Phòng ngừa Dịch bệnh. “Quy tắc bảo mật HIPAA và sức khỏe cộng đồng. Hướng dẫn từ CDC và Bộ Y tế và Dịch vụ Nhân sinh Hoa Kỳ.” Trong: (2003.).

[10] Roy Thomas Fielding. “Phong cách kiến trúc và thiết kế mạng lưới dựa trên kiến trúc phần mềm.” Trong: (2000.).

[11] HHS.gov. “HHSO của Bộ trưởng Tóm tắt Quy tắc bảo mật HIPAA” . Trong: (2013). url: www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.[Truy cập: 04-04-2017].

[12] HHS.gov. “Các phương pháp để hủy nhận dạng PHI” . Trong: (2015). url: https: / / www . hhs . gov / hipaa / dành cho - chuyên gia / quyền riêng tư / chủ đề đặc biệt / hủy nhận dạng/index.html#protected.[Truy cập: 04- tháng 4 năm 2017].

[13] Alex Mizrahi Iddo Bentov Charles Lee và Meni Rosenfeld. “Bằng chứng hoạt động: Mở rộng bằng chứng công việc của bitcoin thông qua bằng chứng cổ phần.” Trong: (2014).

[14] Sunny King và Scott Nadal. “PPCoin: Tiền điện tử ngang hàng với bằng chứng cổ phần.” Trong: (2012).

[15] Satoshi Nakamoto. “Bitcoin: Hệ thống tiền mặt điện tử ngang hàng” . Trong: (2008).

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

[17] Pishing Chiang Philip Chuang Maureen Madden Rainer Winnen-burg Rob McClure Steve Emrick Olivier Bodenreider Duc Nguyen và Ivor DSouza. “Trung tâm thẩm quyền về giá trị NLM.” Trong: (2013.).

[18] Amit P Sheth. “Thay đổi trọng tâm về khả năng tương tác trong các hệ thống thông tin: từ hệ thống, cú pháp, cấu trúc đến ngữ nghĩa. Trong Hệ thống thông tin địa lý tương tác,” trong: (1999.).

[19] Nick Szabo. “Chính thức hóa và bảo đảm các mối quan hệ trên mạng công cộng.” Trong: (1997.).

[20] “US GPO. CFRx 164 bảo mật và quyền riêng tư. 2008.” Trong: (). url: http : / / www . access . gpo . gov / nara / cfr / waisidx08 / 45cfr16408 . html . Truy cập: 2016-08-06..