Patientory: Uma rede P2P de Saúde de Armazenamento de Registros Médicos v1.0

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

Abril de 2017

Este documento serve apenas para fins informativos e não constitui uma oferta ou solicitação de venda de ações ou valores mobiliários da Patientory ou de qualquer empresa ligada ou associada. Tal oferta ou solicitação será feita somente por meio de uma nota de oferta confidencial e de acordo com todos os termos de valores mobiliários aplicáveis e outras leis.

Abstrato

Uma troca de informações sobre saúde suportado por uma blockchain (HIE) pode revelar o verdadeiro valor de um sistema interagir e se comunicar com outro, bem como trazer segurança cibernética. Esse sistema tem o potencial de eliminar o atrito e os custos atuais dos intermediários de terceira parte, ao considerar a gestão da saúde da população. Há promessas de melhoria da integridade dos dados, redução dos custos de transação, descentralização e desintermediação da confiança. Ser capaz de coordenar o atendimento ao paciente através de uma blockchain HIE alivia essencialmente serviços desnecessários e duplica testes com redução de custos e melhorias na eficiência do ciclo de cuidado continuo, ao mesmo tempo adere a todas as regras e padrões da HIPAA. Um protocolo baseado no paciente suportado pela tecnologia blockchain, a Patientory está mudando a forma como as partes interessadas dos cuidados da saúde gerenciam registros médicos eletrônicos e interagem com equipes de cuidados clínicos.

1 Introdução

1.1 O que é a Blockchain?

É a tecnologia por trás da moeda digital bitcoin, o nascimento da blockchain é atribuído para o pseudônimo de uma pessoa (ou grupo) não identificada conhecida como Satoshi Nakamoto. Desde 2009 a blockchain ganhou um uso mais generalizado no setor de finanças, com uma variedade de novas blockchains que habilitam negócios e serviços a entrar no mercado. A tecnologia Blockchain é usada para compartilhar um registro de transações em uma rede de negócios sem ser controlada por qualquer entidade. O livro-razão distribuído facilita a criação de relacionamentos comerciais econômicos onde praticamente qualquer coisa de valor pode ser rastreada e comercializada sem exigir um ponto central de controle. A tecnologia coloca privacidade e controle de dados nas mãos do indivíduo. Confiança e integridade é estabelecida sem dependência de terceiros intermediários.

1.2 Infra-estrutura Atual da Saúde

O realinhamento de um enfoque baseado no "procedimento" para o "cuidado integral do indivíduo" exige que os Profissionais da Saúde formem "redes" que trabalhem juntas em direção ao objetivo comum de melhorar o resultado do cuidado dos pacientes sob cuidados, para episódios de cuidados pós-tratamento ou entre episódios de cuidados graves. A necessidade de cooperação entre os profissionais da saúde, desde especialistas, médicos de cuidados primários, cuidadores e prestadores de serviços de saúde (como nutricionistas e enfermeiros de reabilitação) resulta no aumento do uso de tecnologias digitais. Embora essas soluções tenham melhorado significativamente o rastreamento e eficiência da prestação de cuidados, eles resultaram na criação de silos de informações sobre saúde, principalmente pela forma de sistemas de registros médicos eletrônicos (EMR).

As organizações governamentais e de saúde gastam uma quantidade significativa de tempo e dinheiro criando e gerenciando sistemas tradicionais de informação e intercâmbio de dados; exigindo recursos para solucionar problemas continuamente, atualizar parâmetros de campo, executar medidas de backup e recuperação e extração de informações para fins de relatório.

As leis federais e os programas de incentivo tornaram os dados dos cuidados de saúde mais acessíveis, em resposta à rejeição do hospital em relação à implementação dos EMR. No entanto, a grande maioria dos sistemas hospitalares ainda não pode facilmente (ou de forma segura) compartilhar seus dados. Como resultado, os médicos estão gastando mais tempo digitando do que realmente conversando com os pacientes. O esgotamento de médicos saltou de 45 para 54 por cento entre 2011 e 2014 [1].

Embora exista a noção da informação da saúde "individualizada", tanto no plano clínico quanto no bem-estar, estes não se traduzem nos planos de cuidados "personalizados". Além disso, embora haja uma grande quantidade de dados, o ecossistema de saúde global é incapaz de engenhar adequadamente um valor ou risco para grandes dados para ajudar a prever melhor os futuros episódios de cuidados de um

paciente. Consequentemente as atuais soluções buscadas pela indústria de tecnologia de cuidados de saúde resultaram em uma escolha difícil entre cuidados e privacidade/fraude econômica para os pacientes. Nós vemos essa questão se expandindo muito à medida que mais dados estão sendo criados pela indústria. **A tecnologia segura, as propriedades e a natureza distribuída da Blockchain podem ajudar a reduzir o custo e a melhorar a eficiência dessas operações, bem como proporcionar uma infra-estrutura de segurança viável.**

1.3 Relação Paciente-Provedor

O novo paradigma da saúde exige a necessidade de um atendimento eficaz e ideal para que os pacientes obtenham os melhores resultados dos tratamentos. Isso exige que os principais provedores de cuidados são capazes de coordenar ativamente e colaborar com outros provedores de cuidados envolvidos e organizações de saúde auxiliares como laboratórios e farmácias na prestação de cuidados. Em última análise, para que isso tenha sucesso, os registros dos pacientes precisam ser atualizados e modificados em tempo hábil.

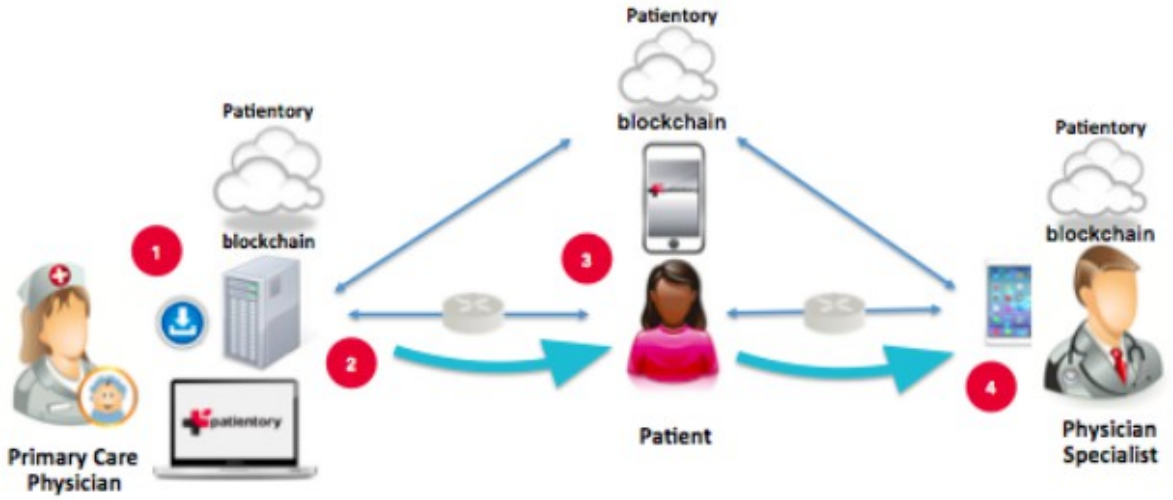

Figura 1: Esquema do paciente

O software de EMR atualmente proíbe a relação efetiva entre paciente e provedor. Os portais dos pacientes têm envolvimento mínimo entre os pacientes, como resultado da experiência do paciente. Além disso, este software apenas fornece uma capacidade limitada de troca de informações de um sistema para outro e geralmente requer um indivíduo designado que seja capaz de realizar tal transferência de informação. Isto levou a uma quantidade crescente de atraso entre as organizações na prestação de cuidados de saúde para o paciente e também resultou na diminuição global da qualidade da prestação de serviços de cuidados ao paciente. Além disso, como os prestadores de cuidados estão gastando mais tempo envolvidos na coordenação dos cuidados do que na eficácia do tratamento de pacientes e sua carga de trabalho tem aumentado significativamente resultando em um impacto contraditório nos resultados dos cuidados para os pacientes.

Além disso, dado que muitos médicos não querem que os pacientes acessem os EHRs, os pacientes adotam um papel passivo no rastreamento de sua saúde. Isto faz com que eles sintam falta do controle e da posse da sua saúde que leva o paciente a ficar frustrado e desalinhado sobre seu tratamento. Embora haja um aumento recente nos aplicativos para celular de cuidados de saúde, ajudando os indivíduos a rastrear suas características vitais e de saúde, a novidade não resultou em melhor atendimento ao paciente ou adesão e resultados, bem como, também enfrenta os desafios de se integrar com os EHRs.

2 Visão Geral do Sistema

Esses problemas atuais são resolvidos usando a Patientory Blockchain Network. O legado da EMR são estruturas centralizadas sujeitas a hackers, estritas regulamentações de segurança e custos gerais pesados. Ao implementar a infra-estrutura da Patientory Blockchain, os prestadores verão a erradicação das brechas da saúde, um canal para a coordenação de cuidados facilitado com resultados na melhoria geral dos resultados da saúde. O que vimos acima é um esquema que descreve a infra-estrutura da blockchain da Patientory e seu sistema que oferece a capacidade entre os pacientes e seus provedores de interagir e se comunicar.

3 Implementação do Sistema

3.1 Regulamentos da HIPAA e Diretrizes de Conformidade

Antes de qualquer discussão significativa sobre implementações, as restrições impostas pelos mandatos da Lei de Portabilidade e Responsabilidade de Seguro de Saúde de 1996 (HIPAA) devem ser tratadas. Essas regras de preocupação primária são a Regra de Privacidade, a Regra de Segurança e as Diretrizes de Computação em Nuvem. A intenção deste artigo não é realizar uma investigação completa da lei HIPAA. Aqueles elementos que são pertinentes para a discussão de implementação devem ser definidos e discutidos mais adiante no momento de uma aplicação relevante.

A. Regra de Privacidade

O modelo de negócios da Patientory prevê que os requisitos da Regra de Privacidade devem ser observados devido ao armazenamento e transmissão eletrônica de informações privadas de saúde. A aplicabilidade da regra de privacidade é resumida como "A Regra de Privacidade. . . (Aplica-se) a planos de saúde, centros de compensação de cuidados de saúde e a qualquer provedor de cuidados de saúde que transmita informações de saúde em formato electrónico" [2]. Além desses agentes, as partes que agem em seu nome, como prestadores de serviços, também são responsáveis pelo cumprimento da HIPAA. Estes agentes de segunda mão são chamados de associados comerciais (Business Associates - BA) e o documento legal que define as regras e os regulamentos que os BA devem aderir é denominado de contrato de associados comerciais (Business Associate Contract - BAC). A HIPAA coloca exigências estritas na

natureza destes acordos.

Os pontos de mérito, a partir de uma investigação inicial, são os requisitos que especificam a autorização de uso, o uso de informações des-identificadas(anônimas) e a definição de informação privada. As informações de saúde privadas (PHI ou ePHI para dados eletrônicos) são definidas como "todas as informações de saúde individualmente identificáveis detidas ou transmitidas por uma entidade coberta ou seu parceiro de negócio, em qualquer forma ou mídia, seja ele eletrônico, papel ou oral". As informações de saúde anônimas são definidas como "As informações de saúde que não identificam um indivíduo e com respeito às quais não há base razoável para acreditar que a informação pode ser usada para identificar um indivíduo não são informações de saúde individualmente identificáveis" [2]. As restrições do uso de dados anônimos são resumidas da seguinte forma: "Não há restrições sobre o uso ou divulgação de informações de saúde anônimas. As informações de saúde anônimas não identificam nem fornecem uma base razoável para identificar um indivíduo" [3]. A fronteira de dados identificáveis para dados des-identificáveis é definida como qualquer informação que possa restringir o possível número de indivíduos que uma coleção de informações está associada a menos de 0.04% da população total dos EUA.

B. Regras de Segurança e Diretrizes de Computação em Nuvem

Devido à extensão do conteúdo associado a este tópico, apenas os elementos de preocupação principal foram isolados para referência. Essas principais preocupações são as seguintes: "Quando uma entidade coberta contrata os serviços de um CSP para criar, receber, manter ou transmitir ePHI (como processar e/ou armazenar ePHI), em seu nome, o CSP é um parceiro de negócios sob a HIPAA. Além disso, quando uma empresa associada subcontrata com um CSP para criar, receber, manter ou transmitir ePHI em seu nome, o próprio CSP subcontratado é um parceiro de negócios. Isso é verdade mesmo se o CSP processar ou armazenar somente o ePHI criptografado e não tiver uma chave de criptografia para os dados. A falta de uma chave de criptografia não isenta um CSP do estado de parceiro de negócios e das obrigações sob as Regras da HIPAA. Consequentemente, a entidade coberta (ou associada) e o CSP devem celebrar um acordo de associação comercial (BAA) em conformidade com a HIPAA e o CSP é tanto contratualmente responsável por cumprir os termos da BAA quanto diretamente responsável pela conformidade com a Requisitos aplicáveis das Regras da HIPAA" [3].

As entidades cobertas geralmente usam provedores de armazenamento em nuvem (CSPs) para armazenar informações de saúde, muitas vezes citando que é mais rentável e há custos mais baixos de gerenciamento de TI. No entanto, como os consumidores dependem de provedores em nuvem para armazenar dados pessoais, eles abandonam o controle direto sobre esses dados e, como resultado, desconhecem quem tem acesso e onde os dados estão localizados geograficamente. Mesmo que um acordo explícito de associação de negócios seja desenvolvido entre o BA e o provedor de armazenamento em nuvem, ele só forneceria os termos de quem assume a responsabilidade da privacidade e segurança dos dados no caso de uma violação ocorrer. O consumidor potencialmente teria controle sobre o acesso a esses fluxos de dados, mas dependeria do provedor de armazenamento em nuvem para impor esses privilégios.

Embora o uso do armazenamento em nuvem seja popular, ainda há uma série de riscos que um consumidor se compromete ao usar esse mecanismo para seus dados pessoais. Na arquitetura baseada em nuvem, os dados são replicados e movidos com freqüência para que os riscos de uso de dados não autorizados não aumentem. Além disso, há vários indivíduos com acesso aos dados, como administradores, engenheiros de rede e especialistas técnicos que cobrem uma ampla área de servidores nos quais as informações são armazenadas. Isso também aumenta o risco de acesso e uso não autorizados.

No entanto, mesmo que os dados sejam seguros através de controlos de acesso rigorosos e criptografados no seu ponto de origem e em trânsito, ainda há um problema para o desenvolvimento das Medidas dos Resultados Relatados pelos Pacientes (PROMs). O conceito do PROM é desenvolver uma medida baseada no paciente que se relaciona com uma área ou foco que seja motivo de preocupação para o paciente e que seu envolvimento e feedback sejam essenciais para sua implementação bem-sucedida. O acesso a grandes fluxos de dados a partir de uma variedade de dispositivos que fazem parte da rede IoT usada agora em conjunto com serviços baseados na nuvem pode fornecer uma base sobre a qual fundamentar uma PROM, mas é difícil saber se os dados armazenados na nuvem produzem uma medida que terá o significado e a relevância pretendidos para um paciente.

A implementação da tecnologia blockchain para garantir e melhorar a segurança de dados para todos os registros médicos associados ao sistema pode atingir zero violações à saúde e definitivamente descentralizar o registro de propriedade. O processo de criptografia de dados quando enviado ao banco de dados usando algoritmos diferentes e descriptografar os dados durante a recuperação será usado.

No que diz respeito ao rápido crescimento do número de violações de dados que o setor de saúde enfrenta, a tecnologia blockchain torna a conformidade da HIPAA viável tanto para pacientes quanto para provedores.

C. Análise das Limitações do Sistema Blockchain devido a Restrições da HIPAA

A Blockchain da Ethereum facilita um subconjunto diverso de implementações do sistema devido à aplicação de uma linguagem de programação de Turing completa que é executada na Ethereum Virtual Machine. Esses sistemas têm limitações em que a máquina virtual não tem inspeção direta além da internet, exceto através do uso de serviços de oráculos. Adicionalmente, as limitações de armazenamento da blockchain são aplicadas pelo custo de gas para armazenar e pelo custo de gas para acessar estes dados. A partir disso, o tempo do bloco estabelece um limite mínimo para solicitações de modificação do estado de pelo menos quinze segundos.

A limitação da blockchain para a hospedar informação privada pode ser superada através do obscurecimento dos dados, como a criptografia, mas no caso da chave de descriptografia já ter sido vazada, não há maneira de remover os próprios dados confidenciais da blockchain. Para efeitos de dados compatíveis com a HIPAA, isto pode potencialmente resultar numa fuga de informação persistente e não corrigível devido à imutabilidade da própria blockchain. Embora os dados de-identificados possam, na teoria, ser armazenados na Blockchain Pública da Ethereum, seria desastroso supor que o

mecanismo de filtragem de de-identification nunca falhará, ou que a informação de banda secundária associada a interações da blockchain não pode revelar identidades inadvertidamente. Esta conclusão também foi alcançada pelo MIT Media Lab durante a formação dos protocolos MedRec e resumida no Whitepaper da MedRec [3]. Minerar esta informação de banda secundária pode ser tão simples quanto observar os carimbos de data/hora e interações com contratos de armazenamento de dados conhecidos.

Através dessa análise, pode ser possível associar um indivíduo a uma instituição e, mais importante, o tempo durante o qual eles estavam presentes em uma instituição. Dada a natureza especializada de algumas instalações, esta informação é suficiente para constituir uma violação da conformidade com a HIPAA devido à capacidade de um observador passivo de deduzir a identidade, a localização, o tempo de interação e, possivelmente, a classe do diagnóstico.

Enquanto esse local é de natureza remota, a redução para menos de 0,04% da população dos EUA torna-se trivial. Esses fatos constituem falhas de ponto único não razoáveis que devem ser reconhecidas. Além disso, o armazenamento direto de até mesmo informações criptografadas sobre a blockchain cria a responsabilidade dos gerentes de banco de dados de entrar em um BAC devido a suas ações como uma instação de armazenamento de dados da HIPAA (consulte a seção Regra de Segurança e Guias de Computação em Nuvem). Esta é uma expectativa irracional, uma vez que todos mineiros, e até mesmo aqueles indivíduos que hospedam nós passivos, precisariam ser compatíveis com a HIPAA. Devido a estas preocupações, implementamos um mecanismo para o armazenamento persistente de informações sensíveis através do uso de uma implementação privada de uma blockchain baseada na Ethereum.

D. Objetivos de implementação para usabilidade e segurança

Os principais objetivos de qualquer sistema seguro podem ser resumidos como os objetivos de confidencialidade, integridade, disponibilidade, responsabilidade e garantia de identidade/informação. Para acomodar esses objetivos, um invasor e usuário devem ser definidos. Cada um desses papéis exige certos reconhecimentos de capacidade. Do ponto de vista do usuário, o sistema precisa ser suficientemente transparente para que nenhum conhecimento avançado seja necessário. Além disso, devido à incapacidade do usuário normal de compreender as considerações complexas de segurança cibernética, o processo precisa ser resistente às ações do usuário.

No caso de ocorrer um ataque, o sistema é criado de tal forma que a quantidade de esforço que deve ser investido para comprometer um recurso custa mais do que o valor do próprio recurso. Isso se deve à constatação de que uma parte suficientemente avançada e com recursos adequados será sempre capaz de violar qualquer sistema, com tempo e esforço suficientes. Em resumo, não há defesa perfeita. Com essas restrições em mente, a implementação em si pode agora ser discutida de modo que possamos atingir todos os objetivos mencionados anteriormente.

3.2 Definição de Hardware e Implementação da Rede

Para acomodar os objetivos de projeto acima mencionados, a implementação do sistema selecionado requer vários sistemas independentes. Cada sistema subdivide a autoridade,

assegura que somente as entidades autorizadas possam interagir de forma aprovada e oferece um mecanismo para aumentar a segurança e manter a disponibilidade. Este sistema também foi concebido de tal modo que o escalonamento pode ser facilmente realizado através da adição de esquemas de chamada hierárquicos. Estes sistemas são completamente descritos em detalhe abaixo.

A entidade que enfrenta o público é um Servidor de Chamada de Procedimento Remoto (Remote Procedure Call - RPC) que atua como uma interface para uma implementação privada da Blockchain da Ethereum (permissionided blockchain). Esta rede de nós da blockchain, só está autorizada a interagir com os outros nós da blockchain, uma entidade de chave autoral, uma instalação de armazenamento compatível com a HIPAA e o Servidor de RPC. A entidade de criação da chave é o recurso que gera pares de chaves públicas/privadas para uso na blockchain. A instalação do armazenamento compatível com a HIPAA hospeda os dados reais que constituem informações eletrônicas privadas de saúde (ePHI).

Quando uma solicitação de dados ocorre, o sistema compatível com a HIPAA pode ser autorizado a falar com o agente de encaminhamento, que re-roteia os dados de volta para o servidor de RPC. Alternativamente, ele pode ser estruturado de modo que o armazenamento da HIPAA fale diretamente com o servidor de RPC. Cada implementação tem benefícios que devem ser considerados antes da seleção final. Em qualquer casos, a instalação de armazenamento da HIPAA descriptografa as porções relevantes da base de dados após a manuseio da solicitação. Esta informação decodificada é então recodificada utilizando a chave pública da parte solicitante para a transmissão. Esta chave pública é também a chave pública do contrato que atua como a interface de controle da blockchain para os dados da HIPAA.

O que se segue é um diagrama da topologia da rede:

3.3 Definição da Implementação do Software

Além do isolamento físico de sistemas na implementação de hardware e rede, o controle de acesso do software facilita a integridade dos dados e a verificação da autorização para entidades solicitantes. O sistema do software, a partir da perspectiva do controle de acesso e da criptografia de dados, é descrito a seguir.

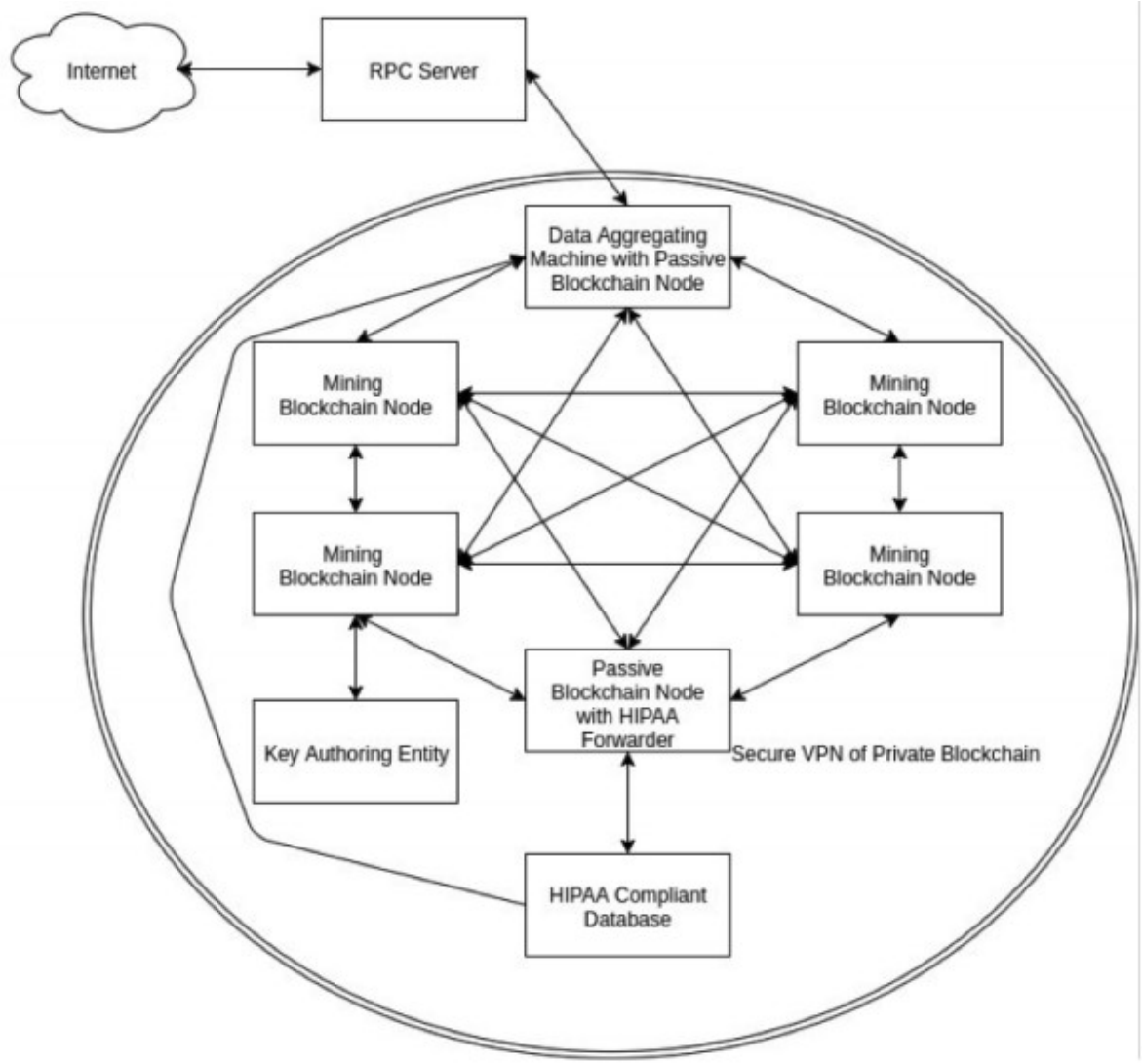

Figura 2: Topografia da Patientory Blockchain Network

O banco de dados compatível com a HIPAA aceitará apenas conexões de entrada do expedidor da HIPAA. Isso garante que o fluxo de tráfego seja isolado para caminhos conhecidos controlados. O expedidor da HIPAA agirá apenas para encaminhar uma solicitação para a instalação de armazenamento da HIPAA enquanto uma transação válida ocorreu na blockchain e essa transação resultou na emissão de um evento solicitante. Este evento solicitante precisa conter a chave pública do solicitante e os campos de dados solicitados. Finalmente, o servidor de RPC usa uma Interface de Programa de Aplicativo (API) controlada por acesso, de modo que somente usuários conhecidos possam interagir com o servidor.

Para entender a hierarquia de chamadas do sistema, a estrutura do contrato para facilitar o controle do acesso deve ser abordada antes. Cada usuário no sistema faz um mapa para um endereço privado na blockchain privada. Todos os endereços privados só estão autorizados a falar directamente com UM contrato na blockchain. Este contrato é o

contrato de classe do indivíduo. Instituições, funcionários da instituição e clientes são objetos de nível de classe.

Esses objetos de nível de classe são interfaces com permissão. O Contrato de Instituição tem uma lista de todos os clientes que concederam privilégios de visualização à instituição e cada contrato de cliente tem uma lista de todas as instituições às quais concedeu permissão. O contrato da instituição possui funções que facilitam a revogação de permissões para a instituição, a partir do usuário. **O contrato institucional não pode alterar esta lista, impedindo assim o acesso não autorizado a registros individuais.** Além disso, o Contrato de Instituição possui uma lista de empregados autorizados que é totalmente capaz de manter. Este esquema de permissão idealmente deveria funcionar de modo que a revogação automática de uma permissão seja realizada em intervalos semi-regulares para evitar que uma instituição inadvertidamente preserve os direitos de acesso de ex-funcionários.

Dentro deste sistema, todas as partes externas interagem através da submissão de transações assinadas que codificam a chamada solicitante. Essas transações são enviadas através do servidor de RPC após a validação do usuário. O servidor de RPC envia essas solicitações para o servidor de agregação de dados que, em seguida, encaminha essas solicitações para os mineiros com base em um mecanismo de compartilhamento de carga. Os mineiros, em seguida, processar o pedido, submetendo a transação em nome do autor da chamada para o contrato de controle da parte respectiva. Este contrato contém as permissões dos dados que a entidade está autorizada a acessar internamente no contrato. Este contrato é a única entidade que aceitará uma transação de um pedido externo. Deste modo, é estabelecido um mecanismo para controlar completamente as operações de chamada na blockchain.

Para qualquer transação, é criado um registro imutável do autor da chamada. Isso garante que todas as tentativas de acesso a informações sejam registradas. Os dados reais armazenados dentro do contrato de usuário é um sistema de indicadores de hash que quando resolvido pelo servidor de armazenamento da HIPAA resultam no retorno dos dados apropriados. Essas informações são borbulhadas até o remetente da HIPAA pela execução de uma transação de solicitação válida. O mecanismo que facilita essa comunicação é indireto e se manifesta através do sistema de mensagens da blockchain. Devido à limitação de que o solicitante só pode consultar o banco de dados por uma transação válida, e o usuário não pode alterar diretamente suas próprias informações, controle de acesso é justificado. Do ponto de vista das instituições, os mecanismos são semelhantes, exceto o contrato de instituição que hospeda uma lista de usuários de quem pode solicitar dados e uma lista de usuários que podem interagir com esta instituição como funcionários. Quando uma transação de solicitação se origina no contrato de um funcionário da instituição, o contrato de controle chama o contrato da instituição, que chama o contrato do usuário para solicitar os indicadores de dados que resolvem o ePHI. Enquanto a instituição estiver na lista de instituições aprovadas para o usuário, o contrato retornará os indicadores de hash apropriados. Estes indicadores são então publicados como uma mensagem de evento que novamente borbulha até a instalação de armazenamento da HIPAA.

Para maior clareza, o processo completo de uma única solicitação é o seguinte: A parte externa solicita dados do serviço chamando o servidor de RPC com uma transação criptograficamente assinada para a submissão para a blockchain. O servidor de RPC verifica a identidade da parte externa através da assinatura de uma solicitação de login.

Enquanto a assinatura corresponder a uma entrada no banco de dados de chaves públicas autorizadas, o servidor de RPC aceita a solicitação e envia a solicitação a Máquina de Agregação de Dados (Data Aggregate Machine). A Máquina de Agregação de Dados então submete os pedidos aos verificadores privados da blockchain. Os verificadores recebem o pedido como uma chamada de uma conta da blockchain contra um contrato de destino. Os verificadores executam essa chamada e, no caso de a solicitação ser uma ação permitida, a transação é inserida no bloco seguinte. Esta transacção também provoca a emissão de uma mensagem de evento na blockchain. Essa mensagem de evento é observada pelo expedidor da HIPAA, que atua para criar uma solicitação criptografada contra o armazenamento da HIPAA com base nos hashes da mensagem de evento. Essa mensagem também contém a chave pública do solicitante. O sistema de banco de dados compatível com a HIPAA observa esse pedido e transmite uma cópia criptografada das informações para o servidor de RPC usando a chave pública do solicitante. O servidor de RPC retorna essas informações para a parte solicitante remapeando o IP solicitante para a chave pública na mensagem. O servidor de RPC transmite essa mensagem sem nunca ter visto os dados subjacentes. Esses dados são imediatamente destruídos pelo servidor de RPC, garantindo assim que o servidor RPC atue como um canal que não precisa ser compatível com a HIPAA.

O mecanismo para publicar os dados é novamente de natureza semelhante, porém os dados a serem enviados são criptografados com a chave pública da instalação de armazenamento da HIPAA. As outras operações são idênticas, exceto os dados que estão sendo postados que borbulham através do sistema de mensagem de evento. Assim, devido ao uso de funções de hashing de colisão baixa e de nonces com carimbos de data/hora, os dados podem ser armazenados com o contrato sendo capaz de computar o endereço em que os dados submetidos estão localizados dentro da instalação de armazenamento da HIPAA.

Finalmente, a distribuição de chaves privadas para entidades deve ser tratada. Isto pode ser facilitado através de meios ópticos para os utilizadores de smartphones. Isto é análogo ao uso de códigos QR como endereços para endereços na Ethereum. Meios alternativos também podem ser estabelecidos usando aplicativos em computadores de mesa e dispositivos tablet/smartphone. A perda de uma chave não é um evento catastrófico, devido à capacidade de remover administrativamente o controle do acesso de um contrato de controle de uma chave e conceder outra.

3.4 Interoperabilidade

Os sistemas de EHR são baseados em uma arquitetura de validação de credenciais isolada na qual os dados do paciente são mantidos separados em cada um dos sistemas. Isto resultou em soluções de "complementos" (add-ons) de software de coordenação de cuidados de saúde de pessoa a pessoa para estes sistemas, para permitir a coordenação

de cuidados entre outros fornecedores e organizações de saúde auxiliares. No entanto, o acesso das informações da principal organização do Provedor às outras organizações é apenas via capacidade limitada em instâncias casos como Ler, Propor, Enviar ou Notificar. Além disso, o Paciente/Consumidor tem muito pouca interação ou envolvimento nessa troca de informações. Além disso, qualquer erro relacionado com a comunicação incorreta ou errada é muito difícil de corrigir.

Uma vez que uma blockchain e seus contratos inteligentes são configurados, os parâmetros tornam-se absolutos. O paciente torna-se o principal intermediário no envio e recebimento de informações de saúde negando a necessidade de atualizações freqüentes e solução de problemas de qualquer software. Como os registros da blockchain também são imutáveis e armazenados por todos os usuários participantes, as contingências de recuperação são desnecessárias. Além disso, a estrutura de informação transparente da blockchain poderia abolir muitos pontos de integração de troca de dados e atividades de relatório demoradas.

3.5 Processos e Escalabilidade

Os usuários estão no controle de todas as suas informações e transferências, o que garante dados de alta qualidade, completos, consistentes, pontuais, precisos e amplamente disponíveis, tornando-os duráveis e confiáveis. Devido à base de dados descentralizada, a blockchain não tem um ponto central de falha e é mais capaz de suportar ataques maliciosos.

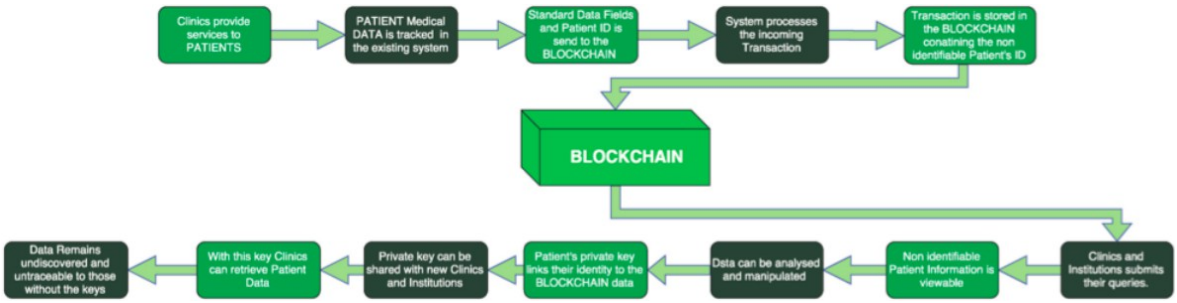

Figura 3: Diagrama de Fluxo do Processo da Blockchain

Em qualquer rede de Cuiados de saúde é necessário garantir que os participantes que estão trabalhando em conjunto podem depender uns dos outros para fornecer os serviços necessários que se espera deles. Para isso, deve haver um meio de assegurar a prestação de contas de tarefas e serviços esperados sejam entregues em tempo hábil e também a responsabilidade associada caso não forem entregues em tempo hábil ao nível de qualidade esperado. Assim, qualquer infra-estrutura de cuidados de saúde tem que ter a competência de perfeitamente ser capaz de monitorar as informações necessárias para permitir que o principal provedor de cuidados avalie a sua rede de cuidados. Além disso, à medida que a rede de cuidados de saúde cresce e essa interação entre as redes de provedores de cuidados aumenta a infra-estrutura dos cuidados de saúde deve ser capaz de abordar esta escala de forma eficaz.

O aspecto chave para a construção de um sistema de Gerenciamento de Cuidados

altamente escalável e distribuído é um quadro arquitetônico peer-to-peer. Essa estrutura já foi usada em vários segmentos da indústria como mídia, esportes, mercado imobiliário, cadeia de suprimentos e outros, a blockchain pode ser facilmente um conector de software complementar para frameworks centralizados existentes[7]. Isto nos levou a explorar a utilização do framework da blockchain para a sua aplicabilidade para ajudar a permitir uma estrutura peer-to-peer para os cuidados de saúde.

A Blockchain tem a promessa de validar duas ou mais entidades envolvidas em uma "transação de saúde". Isso fornece dois atributos-chave em comparação com um modelo de autenticação centralizada. A primeira é que as partes interessadas podem se envolver em um "nível de transação" de "relação de confiança". A segunda é que a exposição da obrigação em tal relação é limitada apenas ao envolvimento de "nível de transação". Isso é muito útil, pois limita o acesso de informações e responsabilidades entre as partes envolvidas e, ao mesmo tempo, permite que uma parte entre em uma relação de transação com um número de outros provedores com base em suas capacidades específicas e tipo de atendimento a ser entregue ao paciente. Isto é significativamente melhor do que os sistemas centralizados convencionais que tem a necessidade de limitar o número de provedores para uma ampla gama de necessidades de pacientes devido ao esforço necessário para gerenciar o acesso e as obrigações.

3.6 Troca de Informação sobre Saúde e Tokens

Para que os EUA se afastem com sucesso do modelo de taxa por serviço para o atual modelo baseado em valores, tem que haver uma infra-estrutura de TI de saúde que permita às organizações vincular qualidade, valor e eficácia de intervenções médicas através de um modelo de remuneração respeitável.

A compensação irá se basear na eficácia da rede dos provedores de serviços em conjunto para garantir a melhoria da qualidade dos cuidados e bem-estar e, ao mesmo tempo, reduzir os custos de cuidados associados. Para incentivar verdadeiramente os diferentes participantes na rede a criar pro-ativamente melhores regimes de assistência, uma compensação baseada no mérito de economias compartilhadas (reembolsos) entra em vigor. A fim de alocar efetivamente uma parte proporcional ao provedor na rede que mais contribuiu para a economia global, um monitoramento claro de sua contribuição é mensurávelmente executado por contratos inteligentes na rede da blockchain.

Outro impacto-chave do novo paradigma de saúde é o modelo de compensação onde os provedores são elegíveis para receber compensação adicional além do cuidado prestado. Esta compensação é o resultado de economias que são geradas com base na forma de quanto os provedores gerenciam os resultados dos cuidados do paciente (incentivos). Qualquer economia gerada através de uma gestão eficiente do cuidado do paciente pode ser mantida pelos provedores e seus parceiros de rede como parte do aspecto de economia compartilhada do novo paradigma de saúde.

Nossa proposta da a capacidade dos pagadores de transferir tokens como incentivos para os provedores que alcançam essas métricas de qualidade. A capacidade de acompanhar e gerenciar contratos inteligentes em que os benefícios podem ser resgatados com facilmente, fornecendo a "cenoura" necessária para provedores e

pacientes participarem ativamente de uma colaboração recíproca. Contrariamente, se um ou mais participantes falharem, penalidades apropriadas por meio de obrigações também podem ser cobradas com a mesma facilidade. Esta aproximação da "cenoura/vara" fornecerá o impulso necessário que é preciso para deslocar a indústria de cuidados médicos de uma mentalidade da gerência da doença a uma mentalidade de estilo de vida bem-estar.

Daí em diante, tokens emitidas pela Patientory (PTY), vão ser o token nativo da plataforma da Patientory. Em troca de tokens PTY, os usuários serão capazes de usar a rede para alugar espaço de armazenamento de informações de saúde, e para executar pagamentos e transações nos contratos inteligentes de saúde.

Acreditamos firmemente que usar um token seja o melhor sistema de pagamento para suportar esta infra-estrutura no futuro próximo. O futuro é um ecossistema vibrante de muitos tokens, para os quais a saúde precisará de um sistema de pagamento em ciclo fechado. O resultado será um ciclo de feedback positivo do círculo de gerenciamento de cuidado eficiente com diminuições significativas em bilhões de dólares atualmente atribuídos à fraude de pagamento de saúde [4].

O sistema também incentiva as grandes organizações com amplo armazenamento de servidores a trocar tokens com organizações de saúde de pequeno e médio porte que precisarão de acesso direto à rede de saúde da blockchain sem a implementação direta de um nó. No entanto, as novas políticas de saúde fornecem o potencial para incentivar os provedores a trabalharem juntos para melhorar as vias de atendimento, as atuais arquiteturas de EHR ficam aquém desta habilidade, assim, a simples concessão ou recebimento de tokens facilita esse processo.

Portanto, o valor dos tokens está vinculado ao volume de transações executadas na rede. À medida que a rede Patientory aumentar consistentemente as transações de tokens, a demanda por token aumenta, resultando em aumento de valor.

3.7 Aquisição de Token

O token PTY pode ser adquirido através do aplicativo nativo da Patientory, do mercado de criptomoedas e de outro paciente, médico ou seguradora por transferência. Os usuários da plataforma terão a capacidade de adquirir PTY enviando Ether ("ETH") para o contrato de criação de PTY na blockchain durante uma pré-venda. A interface da Patientory integrará soluções de negociação de terceiros como a Shapeshift e a Coinbase para usuários que não possuem ETH.

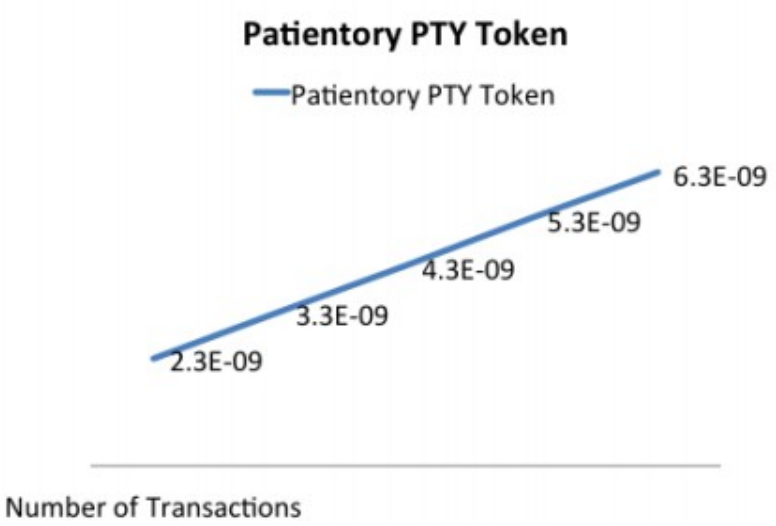

Figura 4: Valor do Token da Patientory Token como Função de Transações

A distribuição inicial do Token da Patientory será sob a forma de uma pré-venda. Qualquer pessoa será capaz de adquirir PTY com uma taxa de desconto penhorando ETH no contrato inteligente de venda do token. Aqueles com outras criptomoedas como ETC ou BTC podem criar PTY através de um serviço de conversão de terceiros que estará disponível na página de pré-venda.

A equipe fundadora receberá uma alocação de 10% de PTY, sujeita a um período de detenção de doze meses. Esses tokens servirão como incentivo de longo prazo para a equipe fundadora da Patientory. 20% adicionais serão alocados ao fundo da Patientory Foundation para ser usado para pesquisa e desenvolvimento com relação à tecnologia blockchain para casos de uso de saúde.

3.8 Contratos inteligentes e Processamento de reivindicação de seguro

A. Auto-arbitragem

A complexidade das faturas médicas e os processos de reembolso de terceiros para os pacientes geralmente levam a confusão ou mal-entendidos entre o paciente, o provedor médico e a seguradora. Essas complicações levam alguns consumidores a não saber quando, a quem, ou que quantia eles devem para uma conta médica ou mesmo se o pagamento era sua responsabilidade ou o provedor de seguros.

A Patientory é uma plataforma projetada para alavancar tanto as tecnologias da blockchain da Ethereum quanto as APIs de Fast Health Interoperability Resources (FHIR) para aumentar a eficiência, permitir a arbitragem de reivindicações em tempo quase real, fornecer acordos transparentes entre as partes interessadas e diminuindo a fraude.

O FHIR foi criado como um padrão da indústria para formatar os dados, reduzindo assim a complexidade da integração para os sistemas legados de saúde e seguros. Um aspecto-chave da nossa solução, devido ao custo de adicionar dados à blockchain, está limitando esses dados apenas ao que é necessário para que os contratos inteligentes sejam executados.

Com os custos relacionados com faturas e seguro, que esperam atingir 315 bilhões de dólares (USD) em 2018 e os consultórios médicos gastam 3,8 horas por semana

interagindo com os pagadores, nossa plataforma pode trazer alívio substancial para esses custos operacionais. Esses mesmos métodos que podem ser utilizados para a análise de correlação cruzada para informação de diagnóstico podem ser utilizados para analisar dados de reivindicação de atividade fraudulenta. Esta análise também pode revelar ações como o comportamento de busca de medicamentos devido à instância de reivindicações múltiplas. Ambos os casos de uso acrescentam propostas de valor para o uso deste sistema pelas companhias de seguros, mas o benefício final está além dessa informação.

Devido ao sistema baseado em regras que é executado pelo sistema de contratos inteligentes, contratos de cobertura inteiros podem ser codificados para contratos inteligentes que são referenciados contra usuários finais. Isso permitiria a uma instituição médica consultar o sistema para verificar a existência de cobertura antes da prestação do serviço. O uso do sistema para hospedar informações de custo também permite a cobrança automática entre instituições e indivíduos como dívida baseada em token. Assim, uma instituição e um indivíduo podem ser facilmente informados dos custos à medida que são apresentaos. Isso remove a carga de trabalho dos departamentos de contabilidade, portanto, um valor adicional para a adoção do sistema.

Por esta razão a Patientory é um sistema de pagamento em ciclo fechado. Espera-se que a ligação de cadeia cruzada possa até mesmo permitir a troca segura de valor através da Blockchain pública da Ethereum. Esse mecanismo já está resolvido para a arbitragem de transações de Bitcoin, embora exija uma entidade confiável para atuar como um oráculo.

B. Viabilidade

Através do uso de mecanismos existentes, esta arquitetura pode ser prontamente construída. Um desses exemplos seria a vinculação do sistema de armazenamento de dados compatível com a HIPAA da Amazon Web Service com o ErisDB que é prontamente implantável. Este SAAS permite a rápido implantação de um contrato inteligente da blockchain da Ethereum com controles de acesso totalmente autorizados, como os mencionados acima. A adição dos nós passivos precisaria ser construída, mas este é um custo de desenvolvimento mínimo em comparação com o desenvolvimento da arquitetura completa.

Com a arquitetura de três níveis do Contrato Inteligente da Patientory, apenas um subconjunto dos recursos de um contrato inteligente é implementado na blockchain da Ethereum. A complexa lógica de negócios é removida do caminho da execução, o que permite que a camada de dados seja otimizada para refletir a natureza distribuída da rede.

Os componentes do pacote de contratos inteligentes implementados na blockchain da Ethereum são o esquema de banco de dados, a validação e verificação de transações que anexam ao livro-razão e a lógica de otimização de consulta para leitura do livro-razão. A lógica de negócios é puxada para cima da blockchain da Ethereum para uma camada intermediária (empresarial) separada. Esse código lógico acessa uma variedade de serviços, incluindo a execução segura, atestado, identidade, suporte criptográfico, formatação de dados, mensagens confiáveis, gatilhos e a capacidade de vincular esse código ao esquema de contratos inteligentes específicos em qualquer número de

blockchains, permitindo que a Patientory encaixe e funcione em vários consórcios de saúde. Esses serviços são fornecidos em uma estrutura, onde as partes individuais do código que suportam os contratos inteligentes podem ser executadas, enviando transações para nós da blockchain e ser vinculados ao esquema na camada de dados.

3.9 Benefícios exclusivos adicionais

Embora uma instituição médica, como um hospital, não devesse ter acesso a registros que não tenham sido especificamente aprovados, o usuário final poderia obter benefícios adicionais pela participação no serviço se os usuários pré-autorizassem o compartilhamento de informações sob circunstâncias de emergência. Com isso em mente, a necessidade de uma aplicação médica para acessar os registros de uma pessoa que não responde em uma situação de emergência constitui uma situação que merece o escalonamento de privilégios dado que o usuário já autorizou esse acesso. No caso de uma pessoa não ser responsável e ter seu telefone celular presente, a instituição pode tomar a posse do dispositivo de um indivíduo usando um método de assinatura secundária disponível na tela de bloqueio de um smartphone. Esta segunda chave não deve ser a mesma chave privada que a conta principal. Assim, se uma conta de instituição submete uma solicitação à blockchain contendo a chave pública de um indivíduo e o smartphone daquele indivíduo envia uma assinatura de emergência, a blockchain pode aumentar o privilégio para permitir o acesso a registros médicos. **O acesso à esta chave privada deve ser considerada queimável e ser substituída pelo indivíduo o mais rapidamente possível. Desta forma, a troca segura de informações entre um indivíduo e uma instituição autorizada pode ser facilitado em situações de emergência.**

Caso uma instituição solicite essas informações sem autorização apropriada, o indivíduo será notificado das ações. Se o indivíduo nega essa solicitação dentro de um intervalo limite, os dados não são compartilhados. Além disso, se uma instituição tentar múltiplas solicitações fraudulentas, a instituição pode ser punida por revogação de privilégio, punição monetária e/ou ações legais. O dano causado pela perda de um dispositivo celular é mínimo devido à necessidade de um dispositivo celular e uma chave de nível de instituição. No futuro próximo, todos os cartões de seguro poderiam ser incorporados com micro-controladores criptográficos, tais como cartões de crédito modernos possuem, que iria facilitar a mesma operação independente de um smartphone.

4 Prioridades Nacionais/Internacionais de Saúde

4.1 Cuidados personalizados

Para alcançar um cuidado superior eficaz, uma abordagem baseada na pessoa é importante. Tal abordagem deve levar em conta não apenas os aspectos clínicos, mas também os fatores sociais e econômicos que impedem a capacidade de se engajar com sucesso na conformidade de cuidados e vida saudável para produzir um bem-estar sustentado.

Para obter resultados de cuidados eficazes é necessário identificar claramente as

barreiras da saúde individual e das situações de vida. Com o crescente número de pacientes com mais de 2 incidência de uma doença, a abordagem "unilateral" de atendimento de todos os tipos de assistência não é propícia para motivar e tratar resultados de cuidados eficazes. Por isso, um modelo de cuidado mais flexível adaptado para incluir as necessidades multifacetadas de saúde e bem-estar dos pacientes deve ser considerado. Isto exige que um plano de cuidados interativo, dinâmico e abrangente, no qual o paciente possa ativamente acompanhar, gerir e participar dos seus cuidados, isso é vital.

4.2 Resultados Clínicos

As Medidas dos Resultados Relatados pelos Pacientes (PROMs), que se concentram em resultados que estão diretamente relacionados com o paciente, assumiram uma importância e significado crescentes nos últimos anos. Isto deve-se, em parte, ao aumento da atenção focada na experiência do paciente e para fornecer uma avaliação baseada no paciente sobre sua obrigação e o impacto da doença. As PROMs podem incluir sintomas e outros aspectos de indicadores de qualidade de vida relacionados à saúde, como a função física ou social, a adesão ao tratamento e a satisfação com o tratamento. Eles também podem facilitar uma comunicação mais precisa entre o médico e o paciente quanto à carga da incidência de uma doença relacionadas ao tratamento, fornecendo uma avaliação mais detalhada e completa de tratamentos para condições específicas, como câncer ou esclerose múltipla.

As PROMs são distintas das medidas de eficácia clínica tradicionais (por exemplo, sobreviventes ao câncer, cessação do tabagismo) porque refletem diretamente o impacto da doença e do seu tratamento do ponto de vista do paciente. Ele pode examinar o equilíbrio entre a eficiência do tratamento e as obrigações do paciente. É também eficaz na observação de áreas como o funcionamento físico e o bem-estar geral e destaca a eficácia e a segurança dos tratamentos em relação ao seu benefício clínico global. Como as próprias medidas são desenvolvidas do ponto de vista do paciente, elas também pode facilitar um maior envolvimento do paciente na tomada de decisão do tratamento, bem como fornecer orientação para decisões de cuidados de saúde. Essencialmente, reforçar uma infra-estrutura de PROM baseada na blockchain reforça a capacidade de incentivar os provedoes e os contribuintes no cumprimento dos padrões de atendimento.

5 Conclusão

A Blockchain desempenhará um papel cada vez mais significativo na TI de cuidados de saúde e trará inovações benéficas e novas eficácias para cada parte interessada no ecossistema. É de vital importância que as organizações de saúde compreendam o núcleo da tecnologia blockchain para garantir que estejam prontas para as mudanças que a tecnologia implica.

O resultado será uma nova geração de poderosos aplicativos baseadas na blockchain que moldarão a próxima era de negócios na área da saúde. Para que as blockchains cumpram seu potencial na área de saúde, devem ser baseadas em padrões que assegurem a compatibilidade e a interoperabilidade dentro do sistema de saúde.

Referências

[1] “A Begoyan. An overview of interoperability standards for electronic health records.” Em: (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?” Em: (2006.).

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

[4] National Healthcare Ant-Fraud Association. “The Challenge of Health Care Fraud”. Em: (). 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 ap- plication platform. White Paper”. Em: (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”. Em: ().

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

[8] Hendrik Tanjaya Tan Darvin Kurniawan David Chandra. “Reidao: Digitis- ing Real Estate Ownership”. Em: (). 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.” Em: (2003.).

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

[11] HHS.gov. “H. H. S. O. of the Secretary Summary of the HIPAA Pri- vacy Rule”. In: (2013). URL: www.hhs.gov/hipaa/for-professionals/ privacy/laws-regulations/index.html. [Acessado:04-04-2017].

[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. [Acessado :04- 04-2017].

[13] Alex Mizrahi Iddo Bentov Charles Lee and Meni Rosenfeld. “Proof of activity: Extending bitcoin’s proof of work via proof of stake.” Em: (2014).

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

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

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

[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.” Em: (2013.).

[18] Amit P Sheth. “Changing focus on interoperability in information sys- tems: from system, syntax, structure to semantics. In Interoperating Ge- ographic Information Systems,” Em: (1999.).

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

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