UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE COMPUTAÇÃO E AUTOMAÇÃO

Beatriz Soares de Souza

PEP+: Um Modelo Blockchain para a Gestão de Casos de Sífilis

Natal

Julho de 2021

Beatriz Soares de Souza

PEP+: Um Modelo Blockchain para a Gestão de Casos de Sífilis

Trabalho de Conclusão de Curso na modalidade Monografia, submetido como parte dos requisitos necessários para conclusão do curso de Engenharia de Computação pela Universidade Federal do Rio Grande do Norte

Universidade Federal do Rio Grande do Norte

Centro de Tecnologia

Departamento de Computação e Automação

Curso de Graduação em Engenharia de Computação

Orientador: Prof. Dr. Ricardo Alexsandro de Medeiros Valentim

Natal

Julho de 2021

Beatriz Soares de Souza
PEP+: Um Modelo Blockchain para a Gestão de Casos de Sífilis/ Beatriz Soares de Souza. – Natal, Julho de 2021-
35 p. : il. ; 30 cm.

Orientador: Prof. Dr. Ricardo Alexsandro de Medeiros Valentim

Trabalho de Conclusão de Curso – Universidade Federal do Rio Grande do Norte
Centro de Tecnologia
Departamento de Computação e Automação
Curso de Graduação em Engenharia de Computação, Julho de 2021.

1. PEP+: Um Modelo Blockchain para a Gestão de Casos de Sífilis.

Beatriz Soares de Souza

PEP+: Um Modelo Blockchain para a Gestão de Casos de Sífilis

Trabalho de Conclusão de Curso na modalidade Monografia, submetido como parte dos requisitos necessários para conclusão do curso de Engenharia de Computação pela Universidade Federal do Rio Grande do Norte

Julho de 2021

Trabalho aprovado. Natal, 14 de Julho de 2021:

Prof. Dr. Ricardo Alexsandro de Medeiros Valentim
Orientador

Me. Fernando Lucas de Oliveira Farias
Convidado

Dr. Philippi Sedir Grilo de Morais
Convidado

Dr. Jailton Carlos de Paiva
Convidado

Esp. Aline Katarine Marques Delgado Freitas
Convidada

Profª. Dra. Karilany Dantas Coutinho
Convidada

Natal
Julho de 2021

Aos meus pais, colegas e orientadores, que
sempre me auxiliaram e apoiaram, dedico este trabalho.

Agradecimentos

À minha família, por confiarem em mim e me apoiarem de todas as formas possíveis.

Aos membros da banca, pela orientação e pela disponibilidade.

Ao LAIS e à UFRN, pela experiência de uma produção compartilhada na qual pude enriquecer minha formação acadêmica.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

CFM Conselho Federal de Medicina

HIV Vírus da Imunodeficiência Humana

HSH Homens Que Fazem Sexo Com Homens

IFRN Instituto Federal de Educação, Ciências e Tenologia do Rio Grande do Norte

IST Infecções Sexualmente Transmissíveis

LAIS Laboratório de Inovação Tecnológica em Saúde

LGPD Lei Geral de Proteção de Dados

MVP Mínimo Produto Viável

NAVI Núcleo Avançado de Inovação Tecnológica

OMS Organização Mundial da Saúde

PEP Prontuário Eletrônico do Paciente

PoA Proof of Authority

PoB Proof of Burn

PoS Proof of Stake

PoW Proof of Work

RGPD Regulamento Geral de Proteção de Dados

SINAN Sistema de Informação de Agravos de Notificação

SUS Sistema Único de Saúde

UFRN Universidade Federal do Rio Grande do Norte

Resumo

O aumento dos casos de sífilis nos últimos anos aponta uma onda epidêmica em diversos países, dentre eles o Brasil. Dessa forma, o Sistema Único de Saúde (SUS) se caracteriza como um forte candidato para a utilização de ferramentas tecnológicas que auxiliem no armazenamento, leitura e acompanhamento de dados de pacientes, em prol de garantir maior eficácia no monitoramento e controle de agravos como a sífilis. Com a crescente busca por tecnologias seguras e auditáveis, a aplicação das redes descentralizadas baseadas em *blockchain* tem progressivamente se apresentado como solução em diversos setores: financeiro, governamental, logístico e de saúde. Com o uso de *blockchain*, o objetivo de acompanhamento dos pacientes com sífilis no SUS pode ser alcançado de maneira segura e interoperável. Neste sentido, o presente trabalho aborda o desenvolvimento de um sistema de prontuário eletrônico centrado na gestão de agravos, com foco em sífilis, utilizando a rede *Ethereum*. A arquitetura do sistema é baseada no algoritmo de consenso *proof-of-authority*, e a interoperabilidade pode ser garantida através da escrita de contratos inteligentes, utilizando a linguagem de programação *Solidity*. Neste contexto, o PEP+ surge como solução tecnológica capaz de garantir transparência, segurança e auditabilidade em dados para prontuário eletrônico no âmbito do SUS.

Palavras-chave: *Blockchain*. Sífilis. Prontuário Eletrônico. *Ethereum*. Sistemas para Saúde.

Resumo

Numbers of syphilis cases have increased markedly in several countries over the last years, Brazil being one of them. Thus, the Brazilian Unified Health System (SUS) could benefit from technologies for storing and reading patient medical records, in order to guarantee effectiveness and better control over diseases such as syphilis. With the growth in searches for safer and more auditable technology, the application of decentralized blockchain networks has progressively presented itself as a solution in the financial, government, logistics and health sectors. The use of a blockchain network allows the monitoring of syphilis data within the SUS safely. Therefore, this work proposes the development of a syphilis electronic medical record system, using the Ethereum network. The system architecture is based on the proof-of-authority algorithm, and smart contract development with Solidity guarantees interoperability. Therefore, PEP+ emerges as a technological solution for ensuring transparency, security and auditability for electronic medical records within the SUS.

Keywords: Blockchain. Syphilis. Electronic Medical Record. Ethereum. SUS.

Sumário

1 INTRODUÇÃO

1.1 Contextualização

De modo hodierno, as Infecções Sexualmente Transmissíveis (IST), se apresentam como um grande desafio epidemiológico global, ao passo que implicam no aumento do risco de aquisição e transmissão do vírus da imunodeficiência humana (HIV). A Organização Mundial da Saúde (OMS) estima a ocorrência de aproximadamente um milhão de casos de ISTs por dia, entre clamídia, gonorreia, tricomoníase e sífilis, essa última atingindo mais de doze milhões de pessoas em todo o mundo por ano (ORGANIZATION et al., 2016).

No Brasil, a taxa de sífilis adquirida apresentou um aumento alarmante nos últimos anos, indo de 12,3 casos a cada 100 mil habitantes em 2011 para 81,4 em 2017, o que indica um aumento de 561%. Em gestantes, o crescimento dos casos nesse mesmo período foi de 660% (SANTOS et al., 2020).

Considerando esta problemática, e com o objetivo de aperfeiçoar a tomada de decisão dos gestores fornecendo informações acuradas e diretas, a Tecnologia da Informação tem contribuído para a melhora nos resultados e no acompanhamento dos casos, com por exemplo, o uso de sistemas de Prontuário Eletrônico do Paciente (CARDOSO, 2018).

Ainda assim, existe uma lacuna quanto à procedência e integração dos dados dos prontuários atuais, e Magalhães et. al (2013), por exemplo, constatou que muitas informações são prejudicadas em análises sobre a epidemia devido às inconsistências de dados encontradas nos prontuários utilizados atualmente.

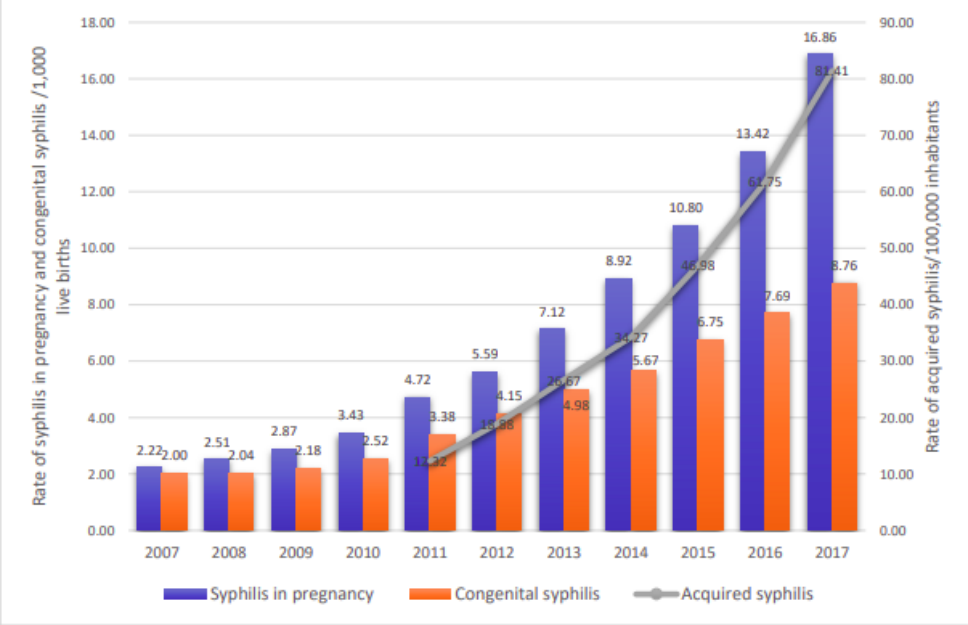
No contexto da sífilis, há diversos estudos atuais (LAFETÁ et al., 2016; MACÊDO et al., 2009; MAGALHÃES et al., 2013) que utilizam dados provenientes de prontuários para acompanhar, monitorar e prevenir a doença. Assim, a implantação de um modelo de prontuário eletrônico seguro, interoperável e congruente com as premissas legais se torna progressivamente mais essencial.

1.2 Referencial Teórico

1.2.1 A sífilis

A sífilis é é uma doença infecto-contagiosa sistêmica com evolução crônica provocada pela espiroqueta *Treponema pallidum*. Nessa patologia, os indivíduos infectados geralmente seguem um curso da doença dividido nos estágios primário, secundário e latente que se manifestam em um período superior a 10 anos (PEELING et al., 2017). Em termos de

Figura 1 – Crescimento dos casos de sífilis gestacional, congênita e adquirida no Brasil.



Fonte – (SANTOS, 2020)

contágio, a transmissão pode ocorrer tanto pela área genital, durante relações sexuais desprotegidas, quanto pelo contato extragenital, a partir de transfusões de sangue e por inoculação acidental, sendo ambas classificadas como sífilis adquirida. Nesse aspecto, a patologia divide-se em sua forma recente, a qual compreende o primeiro ano de evolução da sífilis (incluindo as sífilis primária, secundária e latente recente e tardia), e tardia, após o primeiro ano (incluindo a sífilis latente tardia) (BRASIL, 2010). Há, ainda, o quadro de sífilis congênita cuja transmissão é via vertical, na qual a gestante infectada, quando não tratada ou tratada inadequadamente, dissemina a bactéria por via hematogênica, infectando o feto pela via transplacentária. Tal qual a sífilis adquirida, a sífilis congênita divide-se nas formas precoce, compreendendo a evolução imunitária ocorrida até o segundo ano de vida e pode permanecer assintomática em seus sinais e sintomas, e tardia, cuja evolução ocorre a partir do segundo ano de vida e tem consequências mais específicas com aparecimento de sinais e sintomas característicos da infecção (BRASIL, 2017).

Em 2016, a sífilis foi declarada como um grave problema de saúde pública no Brasil, devido ao constante crescimento dos casos, como observa-se na Figura 1. O combate ao agravamento da epidemia da IST supracitada no país faz parte dos principais instrumentos de gestão estadual, municipal e distrital. A prevenção da transmissão vias vertical e sexual, é prevista como uma prioridade no país (COUTINHO, 2019).

Em todo o território nacional, a notificação de sífilis congênita é compulsória, instituída por meio da Portaria nº 542, de 22 de dezembro de 1986; assim como, a de

sífilis em gestantes, mediante a Portaria nº 33, de 14 de julho de 2005; e, por último, a de sífilis adquirida, por intermédio da Portaria nº 2.472, de 31 de agosto de 2010. No momento presente, vigora a Portaria de Consolidação nº 4, de 28 de setembro de 2017, a qual define a Lista Nacional de Notificação Compulsória de doenças, agravos e eventos de saúde pública nos serviços de saúde públicos e privados em todo o território nacional e dá outras providências. Os dados referentes às notificações de casos da infecção ficam sob responsabilidade do Sistema de Informação de Agravos de Notificação (SINAN) (BRASIL, 2020).

Entretanto, apesar de apresentar-se como uma patologia em situação epidêmica, a sífilis é uma doença curável com tratamento acessível e de baixo custo, com o uso de penicilina (JR, 2017). Consoante a isso, aufere-se o aumento do número de casos aos novos desafios que surgiram ao longo dos anos, seja pela mudança nos grupos de risco, em especial o surgimento da população de homens que fazem sexo com homens (HSH), e mudanças comportamentais na busca de cuidados de saúde para serviços de IST (CHEN, 2017).

1.2.2 *Blockchain*

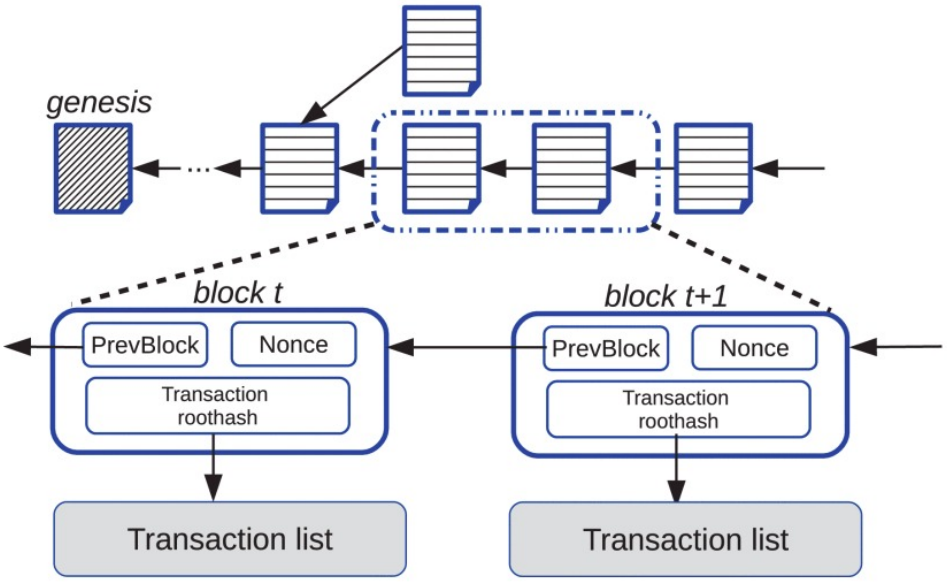
A tecnologia *blockchain* é, conceitualmente, uma lista distribuída de registros, que são compartilháveis, programáveis e seguros. Dessa forma, a *blockchain* pode ser descrita essencialmente como uma cadeia de blocos nos quais todas as informações são escritas, divergindo do conceito clássico de tabelas de um banco de dados onde os registros são armazenados em linhas (NAKAMOTO, 2008). Cada bloco dessa cadeia é formato pelo seu identificador, e pelo *hash* criptográfico do bloco anterior da cadeia, como ilustrado na Figura 2.

Numa rede *blockchain*, as transações são validadas e armazenadas através de algoritmos de consenso, o que descarta a necessidade de uma entidade centralizadora para controle dos dados. Isto é, quando um usuário deseja adicionar uma nova transação na rede, os dados são criptografados e verificados por outros computadores - nós da rede - utilizando estes algoritmos e, se houver consenso entre a maioria deles, um novo bloco de dados será inserido na cadeia e compartilhado com os outros nós (UNDERWOOD, 2016).

Uma vez que qualquer dessas transações é validada consensualmente pelos nós da rede, ela se torna irreversível, verificável, permanente e segura na *blockchain*. Devido a estas características, essa tecnologia tem sido utilizada especialmente na área financeira, na qual se destaca a criação da criptomoeda *Bitcoin*, a primeira moeda digital global e descentralizada (CHEN, 2018).

Quanto às permissões, a *blockchain* pode ser categorizada como pública e não-permissionada, isto é, permite que qualquer usuário a utilize, ou privada e permissionada,

Figura 2 – Estrutura dos dados na *blockchain*



Fonte – (DINH et al., 2018)

na qual apenas um grupo selecionado de usuários pode realizar novas transações na cadeia. Mais especificamente, neste último há um mecanismo de controle de acesso que determina quem pode interagir na rede, o que garante uma autenticação entre os computadores e permite que todos saibam identidade dos outros nós (DINH et al., 2018).

1.2.3 *Ethereum* e os *Smart Contracts*

Em meados de 2013, iniciou-se um projeto denominado *Ethereum*, com a perspectiva de explorar e possivelmente expandir a aplicabilidade das redes *blockchain*, para além do *Bitcoin*. A proposta se baseava em gerar uma plataforma de desenvolvimento genérica, que pudesse ser utilizada para criar aplicações descentralizadas e confiáveis. Destarte, a plataforma *Ethereum* teve leu lançamento em 2015 e desde então tem apresentado um crescimento rápido, com grande potencial de inovação (BUTERIN et al., 2014).

O termo "*Smart Contract*", ou Contrato Inteligente, foi apresentado para indicar que seria possível criar execuções de cotratos a nível computacional sem necessariamente acionar terceiros. O *Ethereum* é uma das tecnologias indicadas no desenvolvimento destes contratos.

Em suma, um *smart contract* é um programa de computador, identificado por um endereço na rede *Blockchain*, que é executado por todos as partes de forma segura, ainda que essas partes não tenham confiança uma nas outras, uma vez que toda a transação é

assegurada pelo código. (SZABO, 2020). Os principais componentes do contrato inteligente são os conjuntos de funções executáveis e variáveis de estado. Durante a execução de uma função, os status das variáveis de estado são alterados dependendo da implementação lógica. Cada contrato recebe um endereço exclusivo da rede Blockchain, e qualquer usuário da rede pode acionar as funções de envio de qualquer tipo de transação. O código do contrato é executado em cada membro do nó na rede Blockchain como parte da verificação de novos blocos (KARAMITSOS et al., 2018).

A execução correta e permissão para execução das funções do contrato se dá por algoritmos de consenso, que serão tratados neste trabalho. Um contrato inteligente, portanto, consiste em três premissas principais, como aponta a Tabela 1.

Tabela 1 – Premissas Principais dos *Smart Contracts*

Premissa	Definição
Acordos contratuais entre as partes	As definições de regras negociais são convertidas em um programa de computador executável, e as partes são identificadas por suas contas na *blockchain* para realizar as transações responsáveis por modificar o estado da cadeia e distribuir para os outros nós.
Governança	Todos os nós participantes da rede podem executar os *Smart Contracts*, porém se submeterão ao processo de validação se as pré-condições foram atendidas ou não.
Execução do contrato	Se as condições e regras forem atendidas, o contrato é executado e as transações são realizadas, garantindo que os *Smart Contracts* sejam autorregulados, isto é, as transações são realizadas de forma autônoma pelo programa desde que os termos do contrato estejam de acordo.

Fonte – (SILLABER; WALTL, 2017)

O código do contrato inteligente é escrito em linguagens de alto nível, como *Solidity* e *Python* para aplicativos *Ethereum*. Como demonstra a Figura 3, cada contrato receberá um endereço exclusivo da rede *Blockchain* e será assinado com a chave pública das partes envolvidas, e o código do contrato será executado nos nós na rede como parte da verificação e validação de novos blocos.

1.2.4 A Lei Geral de Proteção de Dados

Com o avanço tecnológico e a grande massa de dados que são progressivamente disponibilizados na *internet* diariamente por milhões de usuários, garantir a segurança da informação torna-se uma tarefa cada vez mais crítica (ALVES; SOUZA, 2021). Nesse sentido, o *Big Data*, termo que consiste na obtenção e análise de novas informações a partir de uma grande massa de dados, denota, progressivamente, uma constante imersão

Figura 3 – Funcionamento de um Smart Contract.

Fonte – A autora.

na sociedade digital. Além desse fenômeno, essa produção e coleta massiva de dados levou a um outra tendência digital denominada *datafication*, a qual equivale à capacidade de transformar aspectos pessoais em dados que são posteriormente convertidos em informação lida com uma nova forma de valoração, ou seja, é a colheita de informações de qualquer coisa que exista e, por conseguinte, a sua modificação (BOTELHO, 2020).

Sincretizado a esses dois fenômenos, a privacidade informacional e a intimidade dos usuários começam a correr um elevado risco. A partir da *datafication*, o usuário passa a perder o controle individual sobre a colheita e disseminação de informações pessoais. Nessa tendência digital, as empresas coletam, usam e compartilham informações alheias disponíveis online, fazendo com que os usuários percam o controle sobre seus dados pessoais. A privacidade informativa da pessoa natural, cujo significado está relacionado à capacidade de determinar por si mesmo quando, como e em que medida as informações sobre si serão compartilhadas para outras pessoas e organizações, torna-se fragilizada diante desse cenário, resultando em usuários preocupados com sua intimidade online, em especial, com a possibilidade do uso indevido de suas informações pessoais. Consequentemente, voltar o poder de gerenciar e proteger pessoalmente a privacidade online tornou-se um

intento para todos que estão inseridos na sociedade digital (BOERMAN; KRUIKEMEIER; BORGESIUS, 2018).

É nesse contexto que nasce o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, aprovado em 27 de abril de 2016 e em vigor desde de maio de 2018, objetivando a proteção das pessoas físicas com relação ao tratamento de seus dados pessoais e à livre circulação desses dados, conhecido pela expressão *free data flow*. A partir do RGPD, um movimento de formação de regulamentos nacionais para garantir a segurança de informações pessoais passa a atingir diversos países (PINHEIRO, 2020). Dentre esses países, está o Brasil, que em 2018 promulgou a Lei n° 13.709/18 ou, ainda, a Lei Geral de Proteção de Dados (LGPD) em vigor desde agosto de 2020. A lei unificou mais de quarenta normas diferentes que regulam a proteção de dados no país, estabelecendo regras de coleta, tratamento, armazenamento e compartilhamento de dados pessoais pelas organizações, além de garantir direitos aos titulares das informações. A LGPD fundamenta-se pela Constituição Federal de 1988, respeitando as garantias constitucionais de liberdade, privacidade e sigilo de dados, partindo-se da ideia de que todo dado pessoal tem importância e valor (IRAMINA, 2020).

1.2.5 Prontuário Eletrônico do Paciente

Por intermédio da Resolução nº 1.638 de 9 de agosto de 2002, o Conselho Federal de Medicina (CFM) classificou o prontuário do paciente como um documento obrigatório, de caráter legal e sigiloso, fundamental para a prestação da assistência ao paciente, com manutenção realizada apenas por membros da equipe multiprofissional de saúde. Em seu conteúdo há informações referentes à história clínica e social do paciente e todas as assistências prestadas ao mesmo, viabilizando a comunicação entre os profissionais que irão acompanhá-lo (MEDICINA, 2002). O prontuário corresponde não só à ficha clínica ou à ficha de evolução do paciente, como também a todo um conjunto de documentos, como exames complementares, laudos, atestados, prescrições, dentre outros (COLTRI; SILVA, 2019).

Levando em consideração a quantidade de sistemas de saúde no Sistema Único de Saúde (SUS), e a falta de interoperabilidade entre eles, além do grande volume de papel e, principalmente, a dificuldade do paciente, verdadeiro detentor do dado, em ter acesso às suas próprias informações, o legislador brasileiro debruçou-se sobre o tema na Lei nº 13.787, de 27 de dezembro de 2018 ao determinar a transição do modelo manual para digital, dessa forma, implementando o Prontuário Eletrônico do Paciente (PEP). A Lei em questão "dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente", entretanto, como é salientado ainda no Art. 1°, o PEP também é gerido pela LGPD (Lei 13709/18), ao passo que faz-se necessário a seguridade do dado que nele está contido (BRASIL, 2018; PAIVA

et al., 2018).

Dessa forma, problemas com o prontuário em papel, tais como extravio, quebra de privacidade, degradação, dificuldade de recuperação e compartilhamento de informações entre profissionais, são diminuídos ou eliminados com o uso do prontuário eletrônico. Além disso, a utilização do PEP é essencial para questões de acesso rápido e simultâneo às informações por diversos profissionais de saúde, a sua legibilidade, organização sistemática e possibilidade de emissão de relatórios, além de conseguir promover a integração com outros sistemas de informação, com maior agilidade na solicitação e na verificação de exames e de medicações, ampliando a qualidade da informação e, consequentemente, a assistência e a segurança para com o paciente (CRIPPA; DIAS, 2017).

1.3 A proposta

Diante do exposto, este trabalho propõe o desenvolvimento do PEP+: um sistema de prontuário eletrônico do paciente, baseado em *blockchain*, para armazenamento de agravos, utilizando a rede *Ethereum*. De maneira suscinta, o PEP+ permite que os dados do paciente sejam armazenados numa rede descentralizada e segura, em acordo com as premissas da LGPD, e que o paciente seja detentor dos seus próprios dados, podendo compartilhá-los somente quando desejado.

Em termos práticos, o PEP+ é uma implementação de um mínimo produto viável (MVP) que inclui a configuração de uma rede descentralizada *blockchain*, integrada a uma aplicação *web* para interação entre partes via contratos inteligentes, com o intuito de garantir seus três pilares principais:

- Transparência: a *blockchain* é acessível a todas as redes, e quaisquer alterações são registradas em blocos da cadeia;
- Segurança: todos os dados da *blockchain* são criptografados, podendo ser lidos somente por aqueles que possuírem a permissão e a chave para verificação;
- Auditabilidade: os dados armazenados na *blockchain* são imutáveis, garantindo que todo seu histórico possa ser recuperado e auditado.

Este trabalho, com enfoque na sífilis, surge no contexto do projeto "Sífilis Não": uma iniciativa do Ministério da Saúde em parceria com a Universidade Federal do Rio Grande do Norte (UFRN) e concretizado pela Fundação Norte-Rio-Grandense de Pesquisa e Cultura (FUNPEC, 2017).

Neste contexto, o PEP+ surge como solução tecnológica capaz de garantir transparência, segurança e auditabilidade em dados para prontuário eletrônico no âmbito do SUS.

1.4 Objetivos

1.4.1 Geral

Propor e desenvolver o MVP de um sistema integrado a uma rede *Ethereum* para armazenar dados do prontuários eletrônico do paciente relacionados ao diagnóstico de sífilis, de forma segura e auditável.

1.4.2 Específicos

- Configurar uma rede *Ethereum* privada, e prover a comunicação entre diferentes nós, considerando o algoritmo de consenso *Proof of Authority*.
- Desenvolver, lançar e interagir com o *Smart Contract*, registrando novos dados através de transações realizadas com o contrato.
- Criar o *script* de integração para que uma aplicação *Django* possa ler e/ou escrever na rede *blockchain*, salvando dados do paciente.
- Participar de cooperação internacional no âmbito do projeto Sífilis Não juntamente ao Laboratório de Inovação Tecnológica em Saúde (LAIS), com a universidade de Massachusetts para intercâmbio de experiências com pesquisadores da linha de sistemas de informação e diagnóstico de sífilis.

2 MATERIAIS E MÉTODOS

2.1 Metodologia

Esta pesquisa tem a natureza aplicada, com o intuito de gerar conhecimento para a solução do problema da segurança e interoperabilidade dos dados de pacientes quanto à sífilis. O tipo deste trabalho é quali-quantitativo e o objetivo exploratório, uma vez que se trata de um MVP para validar a viabilidade de um sistema baseado em uma rede descentralizada *blockchain* (NASCIMENTO, 2016).

2.2 Estrutura da Rede

2.2.1 Consenso

Para estruturar uma rede descentralizada *Ethereum*, é necessário definir o algoritmo de consenso que será utilizado para validar as transações. No contexto da *blockchain*, o problema do consenso é definido pelos nós da rede, e se baseia em três propriedades: a) concordância, uma vez que a maioria dos nós deve ter acordado na validação do bloco; b) validade, onde o bloco aceito provém de um processo válido; c) terminação, em que todos os processos corretos são eventualmente acrescidos à cadeia principal. É necessário que haja esse protocolo de consenso para que seja garantida a ordenação dos blocos, o que previne concorrência e conflitos nas transações (GRAMOLI, 2020).

Com a evolução das tecnologias de *blockchain*, surgiram diferentes mecanismos para garantir o consenso e a integridade da cadeia e, considerando os diversos algoritmos de consenso existentes (MIERS et al., 2019), podemos citar alguns principais, presentes na Tabela 2.

Dentre os diferentes mecanismos de consenso, observa-se que o mais congruente com a proposta de um prontuário eletrônico seguro para o paciente é o PoA, no qual permissão para criar novos blocos na cadeia está associada diretamente a nós predeterminados, que, em termos práticos, seriam as entidades de saúde do Brasil, como o SUS.

2.2.2 Configuração

O *Ethereum* é um *software* de código aberto, escrito na linguagem *Go*, e que possui uma interface de comunicação denominada *geth*, a qual pode ser executada nos principais sistemas operacionais, como Linux, macOS e Windows (TOYODA et al., 2020). Dessa

Tabela 2 – Principais Algoritmos de Consenso

Algoritmo de Consenso	Conceito
Proof of Work (PoW)	Um dos mais famosos algoritmos de consenso, introduzido no *Bitcoin*, no qual os nós da rede devem manter a segurança através do desenvolvimento de tarefas de alto custo computacional, que geralmente demanda alto poder de processamento e previne que mineradores maliciosos tentem validar e adicionar blocos na cadeia
Proof of Authority (PoA)	Um conjunto de autoridades pré-definido possue a permissão especial para criar novos blocos e gerenciar transações. Esse modelo é utilizado em redes privadas, onde se deseja manter um controle das entidades que poderão realizar qualquer modificação na cadeia. A esses nós, são dadas assinaturas digitais específicas que podem ser rasteráveis e são únicas.
Proof of Burn (PoB)	Os nós mineradores precisam "queimar"(do inglês *burn*) algumas de suas criptomoedas para usá-las como combustível para geração de novos blocos na cadeia, através do envio de ativos para um endereço da blockchain no qual não é possivel recuperar os recursos.
Proof of Stake (PoS)	Este algoritmo segue o mesmo princípio do PoW, porém acrescenta a preferência por nós quem já tenham alta participação na rede, facilitando o processo de minerar e realizar cálculos custosos.

Fonte – (GRAMOLI, 2020)

forma, a primeira etapa da configuração consiste na instalação do geth, que permitirá realizar as seguintes interações com a rede *blockchain* (ETHEREUM, 2019):

- Conectar à rede *blockchain*;
- Baixar e sincronizar os dados (os blocos da cadeia);
- Inserir novos blocos;
- Realizar novas transações;

Após obter o *geth*, é necessário criar o primeiro bloco da blockchain, denominado Genesis. Este bloco será o precursor em comum para todos os blocos da rede, ou seja, qualquer nó que deseje conectar à mesma rede deve utilzar o mesmo arquivo Genesis. Uma blockchain de pelo menos um bloco está na origem de todos os nós sempre, porque dentro do *software* do cliente o bloco Genesis é criptrografado de maneira estática, de forma que não pode ser alterado (BHADORIA; ARORA; GAUTAM, 2020). O arquivo .json do bloco está descrito a seguir:

```
{
        "config": {
                "chainId": 15,
                "clique": {
                        "period": 0,
                        "epoch": 30000
                }
        },
        "difficulty": "1",
        "gasLimit": "22000000000",
        "extraData": "0x000",

        "alloc": {
                "0x<one of your created accounts>": {
                        "balance": "100000000000000000000"
                }
        }
}
```

Os parâmetros deste arquivo são configurados considerando as seguintes chaves:

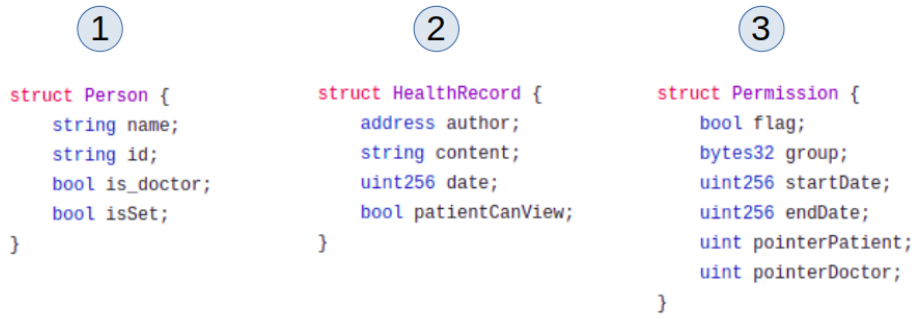
- *extraData*: são os 64 ou 32 bits que podem ser usados para mensagens;
- *difficulty*: define qual será a dificuldade de mineração de um novo bloco;
- *clique*: ao inserir esta chave, está sendo determinado que o algoritmo de consenso utilizado será o *Proof of Authority*, e o *period* igualado a zero infica que não deve haver um período entre as transações e a criação do bloco ao qual elas se referem;
- *alloc*: define um saldo inicial para uma ou mais contas;
- *gaslimit*: a quantidade máxima de saldo (*gas*) que se pode dispender na criação de um novo bloco;

Após a criação do bloco inicial Genesis, é possível inicilizar a rede, utilizando-se de dois comandos pricipais do *geth*. O primeiro deles é o **geth –datadir . init genesis.json**, que irá criar o diretório para armazenamento dos dados da cadeia e também os endereços das contas vinculadas à rede; e o segundo comando **geth –datadir . console** deverá inicializar uma nova sessão na *blockchain* propriamente dita, e que poderá ser conectada a novos nós.

2.3 Criação do *Smart Contract*

O contrato foi escrito na linguagem Solidity, e visa controlar a escrita e leitura dos registros do prontuário eletrônico de um paciente. A premissa principal é de que todas as permissões para o acesso aos dados provém do próprio paciente. O código conta com três *structs* (ou estruturas) que compõem as informações principais do registro, e estão descritas na Figura 4.

Figura 4 – *Structs* principais do contrato.



Fonte – A autora.

A estrutura 1 diz respeito a uma Pessoa, que informa seus dados de nome e identificação (para este contexto, o cpf) com um parâmetro booleano para determinar se é um profissional de saúde. A estrutura 2 é o prontuário propriamente dito, na qual é armazenada a conta do autor do registro, a data, e o conteúdo. Já a estrutura 3 se refere às permissões, que consta o usuário e a durabilidade desta permissão. Essa durabilidade foi implementada para reforçar o controle que o paciente pode ter aos seus próprios dados, podendo inclusive delimitar o tempo que um usuário terá acesso ao seu histórico de agravos.

Dentro do contrato, alguns dicionários de dados também são importantes para fácil acompanhamentos das permissões em vigência e dos grupos de agravos nos quais há registros de dados (como supracitado, este trabalho foi realizado sob o enfoque da sífilis, mas o contrato foi desenvolvido de forma a manter escalável o registro de outras doenças e infecções dentro da rede). O primeiro destes dicionários é o **permissionMap**, que mapeia todas as permissões já concedidas a um PEP, por data e grupo. O segundo é **permissionListPatient** que lista os profissionais de saúde aos quais foram cedidas permissões atualmente, e o terceiro é o **permissionListDoctor** que retorna todos os pacientes aos quais um profissional tem acesso dos registros. Esse mapeamento pode ser visto com mais clareza na Figura 5.

Com a criação do contrato, foi necessário realizar a compilação com o comando **solc -o <pasta> –bin –abi <contrato>.sol** que retorna um identificador do contrato

Figura 5 – Dicionários de dados do contrato.

```
// A person's health record. Each record can be grouped: 'syphilis', 'cancer'...
mapping(address => mapping(bytes32 => HealthRecord[])) public healthRecordMap;

// Who has permission to access each person's data, split by groups
mapping(address => mapping(address => Permission[])) public permissionMap;

// Tracking the doctors each person has granted permission
mapping(address => address[]) public permissionListPatient;

// Tracking the people each doctor has been granted permission
mapping(address => address[]) public permissionListDoctor;
```

Fonte – A autora.

no formato **.abi** e seu arquivo compilado, que é o **.bin**. E assim foi possível lançá-lo na rede *blockchain*, seguindo os seguintes passos:

```
var abi = <abi do contrato>
var bin = 0x + <bin do contrato>
var config = {from:web3.eth.accounts[0],
data: bin,
gas: 4700000
}

var contract_factory = web3.eth.contract(abi)
var contract = contract_factory.new( <argumentos>, config)
```

2.4 Integração

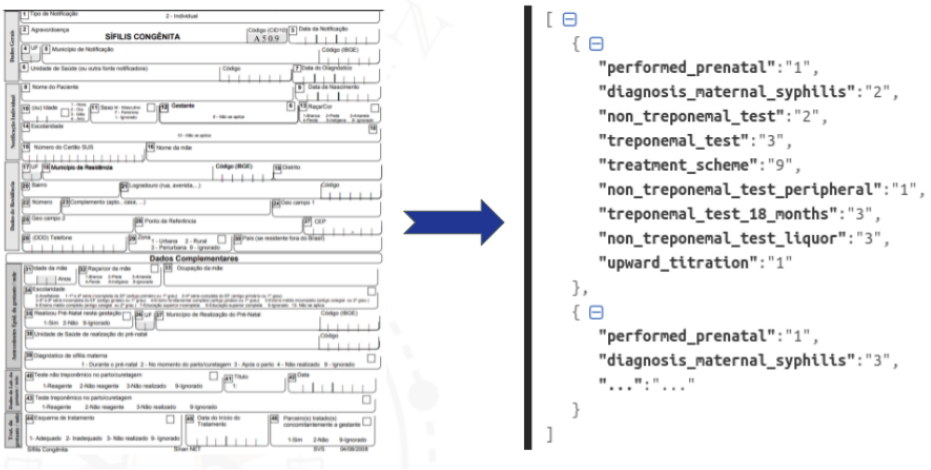
Considerando que a rede teve sua configuração concluída e o *smart contract* foi lançado devidamente na *blockchain*, é necessário realizar a integração do sistema *web* do PEP+, que foi desenvolvido utilizando o *framework* Django, com o contrato.

Para tal, foi utilizada a biblioteca Web3. A Web3.py é uma biblioteca Python para interação com o *Ethereum*, e é geralmente utilizada em aplicativos descentralizados para realizar transações, interagir com contratos, ler dados de bloco e uma variedade de outros casos de uso. A versão original foi derivada da Javascript Web3.js, mas desde então evoluiu em direção às necessidades dos desenvolvedores Python (WEB3, 2018).

A integração é realizada para receber os dados diretamente da aplicação no formato do boletim do SINAN relacionado à sífilis e convertê-lo em um modelo de dicionário no

formado .json, o qual será salvo na rede por intermédio do contrato inteligente, commo ilustrado na Figura 6.

Figura 6 – Boletim do SINAN convertido para JSON.



Fonte – A autora.

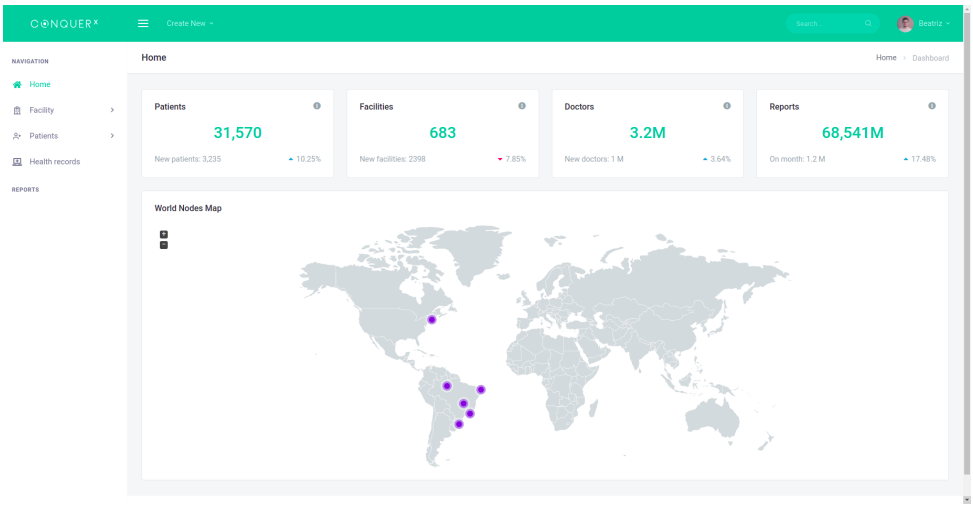
3 Resultados

3.1 A aplicação

Os objetivos do trabalho foram atingidos: o resultado é o MVP de um sistema *web* integrado a uma rede *blockchain* permissionada, capaz de interagir com contratos inteligentes para leitura e/ou escrita de dados de paciente.

O PEP+ conta com uma tela inicial ilustrada na Figura 7, na qual é possível visualizar os pontos geográficos onde há nós ativos da rede blockchain, e alguns *cards* com dados agregados acerca dos quantitativos de pacientes cadastrados, estabelecimentos de saúde, profissionais de saúde e registros.

Figura 7 – Página inicial do PEP+.

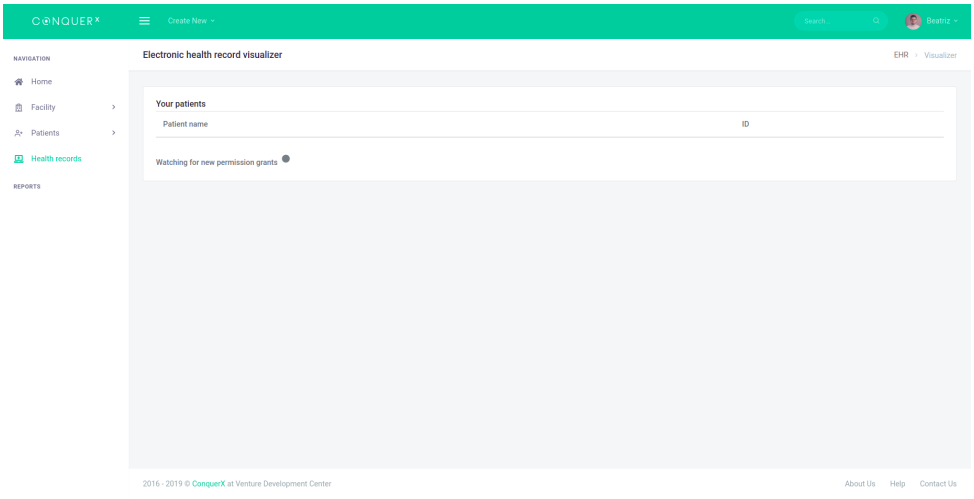


Fonte – A autora.

Na Figura 8 pode-se visualizar a tela de listagem de pacientes ao qual o profissional de saúde terá permissão de leitura/escrita de registros. Esta página é atualizada em tempo real, sempre verificando as permissões da rede para o profissional logado. Ao receber uma nova permissão, é carregado um modal de notificação de nova permissão cedida, como na Figura 9.

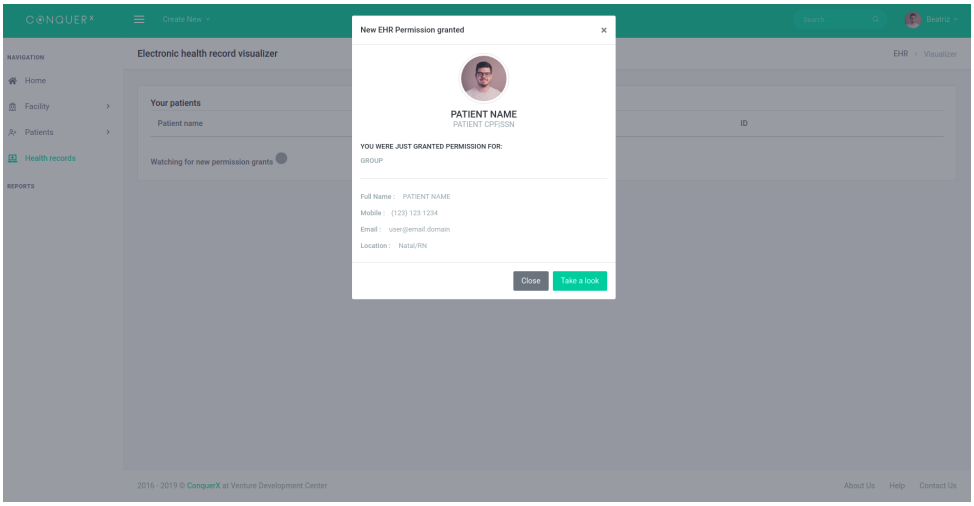
Para usuários administrativos, também é possível cadastrar novos endereços na *blockchain* para novos pacientes, e a partir dele iniciar o fluxo de solicitação de permissões para o profissional de saúde, garantindo que a posse da informação sempre seja do próprio paciente, como mostra a Figura 10.

Figura 8 – Página de acompanhamento de pacientes que permitiram o acesso.



Fonte – A autora.

Figura 9 – Notificação de nova permissão concedida.

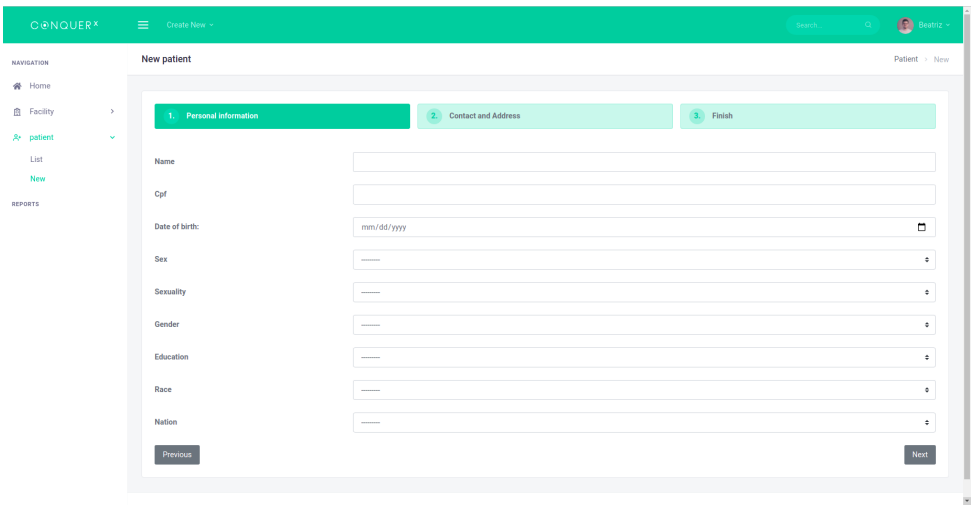


Fonte – A autora.

3.2 Trabalhos Relacionados

Este trabalho foi realizado em cooperação com a Universidade de Massachusetts, e portanto é de suma importância dividir o capital intelectual adquirido a partir desta experiência. Portanto, o processo de desenvolvimento do PEP+ foi compartilhado com a equipe do LAIS no formato de palestras e *workshops*,

Figura 10 – Formulário para criação de novo paciente na rede.



Fonte – A autora.

Figura 11 – Oficinas ministradas no âmbito do sistema PEP+

(a) Primeira oficina no Núcleo Avançado de Inovação Tecnológica (NAVI) do IFRN.

(b) Segunda oficina no Núcleo Avançado de Inovação Tecnológica (NAVI) do IFRN.

(c) Oficina na Secretaria de Educação a Distância (SEDIS) da UFRN.

(d) Oficina na Secretaria de Educação a Distância (SEDIS) da UFRN.

Fonte – O autor

4 CONCLUSÃO

Apresentou-se o projeto e implementação do MVP de um sistema de prontuário eletrônico baseado em *blockchain* para o monitoramento e combate da sífilis de forma transparente e auditável. O resultado desta aplicação é uma ferramenta que provê ao paciente a posse de seus próprios dados, e ao gestor a integridade dos dados relacionados aos pacientes.

Por esse viés, o PEP+ oferece recursos de armazenamento de dados descentralizados, através dos algoritmos de consenso e dos contratos inteligentes, o que propõe automatização na segurança da informação, qualificando-o como forte aliado do gestor para o combate e monitoramento confiável dos dados de sífilis. Desse modo, é possível afirmar que a utilização desta aplicação pode auxiliar no combate de agravos, sob a ótica da sífilis.

4.1 Trabalhos Futuros

Os testes realizados na primeira versão da rede e aplicação implementada demonstram a possibilidade de melhorias nos seguintes aspectos:

- Validar o PEP+ na atenção primária de saúde na gestão de casos da sífilis utilizando *blockchain* para armazenamento dos dados;
- Ampliar o PEP+ para reunir dados de outros agravos;
- Avaliar outras tecnologias descentralizadas para o armazenamento de grandes arquivos, como resultados de exames de imagem;

Referências

ALVES, G. B.; SOUZA, R. T. d. Comércio digital e proteção de dados. *Revista da Defensoria Pública do Distrito Federal*, v. 3, n. 1, p. 99–122, abr. 2021. Disponível em: <http://revista.defensoria.df.gov.br/revista/index.php/revista/article/view/116>. Citado na página 17.

BHADORIA, R. S.; ARORA, Y.; GAUTAM, K. Blockchain hands on for developing genesis block. In: *Advanced applications of blockchain technology*. [S.l.]: Springer, 2020. p. 269–278. Citado na página 23.

BOERMAN, S. C.; KRUIKEMEIER, S.; BORGESIUS, F. J. Z. Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, SAGE Publications, p. 009365021880091, out. 2018. Disponível em: <https://doi.org/10.1177/0093650218800915>. Citado na página 19.

BOTELHO, M. C. A lgpd e a proteção ao tratamento de dados pessoais de crianças e adolescentes. *Revista Direitos Sociais e Políticas Públicas–Unifafibe*, v. 8, n. 2, 2020. Citado na página 18.

BRASIL. *Lei n. 13.787, de 27 de dezembro de 2018*. 2018. Disponível em: <http://www.planalto.gov.br/>. Citado 2 vezes nas páginas 19 e 20.

BRASIL, B. M. da Saúde do. *Nota informativa no 2-SEI/2017. DIAHV/SVS/MS*. 2017. Disponível em: <http://www.aids.gov.br>. Citado na página 14.

BRASIL, B. M. da Saúde do. *Boletim Epidemiológico Sífilis 2020*. 2020. Disponível em: <http://www.aids.gov.br>. Citado na página 15.

BRASIL, M. da Saúde do. *Doenças infecciosas e parasitárias: guia de bolso*. Brasília: [s.n.], 2010. v. 8. Citado na página 14.

BUTERIN, V. et al. A next-generation smart contract and decentralized application platform. *white paper*, v. 3, n. 37, 2014. Citado na página 16.

CARDOSO, J. A. A. Sistemas informatizados de gestão: A contribuição do prontuário eletrônico do paciente no faturamento de um hospital universitário. In: *Congresso de Gestão, Negócios e Tecnologia da Informação–CONGENTI*. [S.l.: s.n.], 2018. Citado na página 13.

CHEN, X.-S. Challenges in responses to syphilis epidemic. *The Lancet. Infectious diseases*, v. 17, n. 8, p. 793–794, 2017. Citado na página 15.

CHEN, Y. Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business horizons*, Elsevier, v. 61, n. 4, p. 567–575, 2018. Citado na página 15.

COLTRI, M. V.; SILVA, R. H. A. da. PRONTUáRIO DO PACIENTE: COMENTáRIOS à LEI nº 13.787/2018. *Revista Brasileira de Odontologia Legal*, Revista Brasileira de Odontologia Legal, p. 89–105, 2019. Disponível em: <https://doi.org/10.21117/rbol.v6i2.253>. Citado na página 19.

COUTINHO, K. M. D. *Telessaúde na formação e qualificação de profissionais para enfrentamento à sífilis*. Dissertação (Mestrado) — Brasil, 2019. Citado na página 14.

CRIPPA, V.; DIAS, D. R. C. VANTAGENS DA IMPLANTAção DO PRONTUáRIO ELETRôNICO NA SEGURANça DO PACIENTE e NA OTIMIZAção DO TRABALHO DO FARMACêUTICO HOSPITALAR. *Infarma - Ciências Farmacêuticas*, Conselho Federal de Farmacia, v. 29, n. 3, p. 199–207, set. 2017. Disponível em: <https://doi.org/10.14450/2318-9312.v29.e3.a2017.pp199-207>. Citado na página 20.

DINH, T. T. A. et al. Untangling blockchain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering*, IEEE, v. 30, n. 7, p. 1366–1385, 2018. Citado na página 16.

ETHEREUM, G. 2019. Disponível em: <https://geth.ethereum.org/>. Citado na página 23.

FUNPEC. *Lembre-se de se cuidar, sífilis: teste, trate e cure.* 2017. Disponível em: <https://www.sifilisnao.com.br/index_desktop.html>. Citado na página 20.

GRAMOLI, V. From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems*, Elsevier, v. 107, p. 760–769, 2020. Citado 2 vezes nas páginas 22 e 23.

IRAMINA, A. Rgpd v. lgpd: Adoção estratégica da abordagem responsiva na elaboração da lei geral de proteção de dados do brasil e do regulamento geral de proteção de dados da união europeia. *Revista de Direito, Estado e Telecomunicações*, v. 12, n. 2, 2020. Citado na página 19.

JR, A. C. W. *Treatment of Early Syphilis in HIV: What Do We Really Know?* [S.l.]: Oxford University Press US, 2017. Citado na página 15.

KARAMITSOS, I. et al. Design of the blockchain smart contract: A use case for real estate. *Journal of Information Security*, Scientific Research Publishing, v. 9, n. 03, p. 177, 2018. Citado na página 17.

LAFETÁ, K. R. G. et al. Sífilis materna e congênita, subnotificação e difícil controle. *Revista Brasileira de Epidemiologia*, FapUNIFESP (SciELO), v. 19, n. 1, p. 63–74, mar. 2016. Disponível em: <https://doi.org/10.1590/1980-5497201600010006>. Citado na página 13.

MACÊDO, V. C. d. et al. Avaliação das ações de prevenção da transmissão vertical do hiv e sífilis em maternidades públicas de quatro municípios do nordeste brasileiro. *Cadernos de Saúde Pública*, SciELO Public Health, v. 25, p. 1679–1692, 2009. Citado na página 13.

MAGALHÃES, D. M. dos S. et al. Sífilis materna e congênita: ainda um desafio. *Cadernos de Saúde Pública*, FapUNIFESP (SciELO), v. 29, n. 6, p. 1109–1120, jun. 2013. Disponível em: <https://doi.org/10.1590/s0102-311x2013000600008>. Citado na página 13.

MEDICINA, C. F. de. *RESOLUÇÃO CFM n. 1.638/2002*. 2002. Disponível em: <https://sistemas.cfm.org.br/>. Citado na página 19.

MIERS, C. et al. Análise de mecanismos para consenso distribuído aplicados a blockchain. SBC, 2019. Citado na página 22.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260, 2008. Citado na página 15.

NASCIMENTO, F. P. d. Classificação da pesquisa. natureza, método ou abordagem metodológica, objetivos e procedimentos. *Metodologia da Pesquisa Científica: teoria e prática–como elaborar TCC. Brasília: Thesaurus*, 2016. Citado na página 22.

ORGANIZATION, W. H. et al. *Global health sector strategy on sexually transmitted infections 2016-2021: toward ending STIs*. [S.l.], 2016. Citado na página 13.

PAIVA, J. C. de et al. SMART: a service-oriented architecture for monitoring and assessing brazil's telehealth outcomes. *Research on Biomedical Engineering*, FapUNIFESP (SciELO), v. 34, n. 4, p. 317–328, out. 2018. Disponível em: <https://doi.org/10.1590/2446-4740.18004>. Citado 2 vezes nas páginas 19 e 20.

PEELING, R. W. et al. Syphilis. *Nature Reviews Disease Primers*, Springer Science and Business Media LLC, v. 3, n. 1, out. 2017. Disponível em: <https://doi.org/10.1038/nrdp.2017.73>. Citado na página 13.

PINHEIRO, P. P. *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD*. [S.l.]: Saraiva Educação SA, 2020. Citado na página 19.

SANTOS, M. M. d. Fragilidades na atenção primária em saúde favorecem o aumento das tendências de sífilis adquirida no brasil. Universidade Federal do Rio Grande do Norte, 2020. Citado na página 14.

SANTOS, M. Marques dos et al. Trends of syphilis in brazil: a growth portrait of the treponemic epidemic. *Plos one*, Public Library of Science San Francisco, CA USA, v. 15, n. 4, p. e0231029, 2020. Citado na página 13.

SILLABER, C.; WALTL, B. Life cycle of smart contracts in blockchain ecosystems. *Datenschutz und Datensicherheit-DuD*, Springer, v. 41, n. 8, p. 497–500, 2017. Citado na página 17.

SZABO, N. The idea of smart contracts. nick szabo's papers and concise tutorials (1997). *URL http://www. fon. hum. uva. nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo. best. vwh. net/smart contracts*, v. 2, 2020. Citado na página 17.

TOYODA, K. et al. Function-level bottleneck analysis of private proof-of-authority ethereum blockchain. *IEEE Access*, IEEE, v. 8, p. 141611–141621, 2020. Citado na página 22.

UNDERWOOD, S. Blockchain beyond bitcoin. *Communications of the ACM*, ACM New York, NY, USA, v. 59, n. 11, p. 15–17, 2016. Citado na página 15.

WEB3. *Introduction*. 2018. Disponível em: <https://web3py.readthedocs.io/en/stable/>. Citado na página 26.