DOI: 10.36558/rsc.v11i3.7541

Blockchain-Based Platform for Managing Patients' Data in the Public Healthcare System of Brazil

Carlo Kleber da Silva Rodrigues
Centro de matemática, Computação e Cognição (CMCC)
Universidade Federal do ABC (UFABC)
Santo André, SP, Brasil
carlo.kleber@ufabc.edu.br

ABSTRACT

The public healthcare system of Brazil must serve a population of around 214 million citizens, spread across 27 federative units covering a territory of over 8.5 million km^2. One of the pivotal bottlenecks for its effective operation lies in the management of patients' health data, which are consolidated in medical records. Intrinsically distributed and decentralized, the aforementioned data management raises deep concerns regarding efficiency, security, and scalability, besides economic cost. In this context, the Blockchain technology has been envisioned as a promising solution. This article therefore proposes a Blockchain-based platform for managing medical records. Its effectiveness is herein attested by conceptual discussion plus analytical modeling. As the main contribution, we thus provide the literature with theoretical subsidies and experiments that may underpin and guide the development of real projects. At last, conclusions and future works close this article.

CCS Concepts

•**Networks** → **Network performance analysis;** *Network algorithms;*

Keywords

Blockchain; Platform; Scalability; Efficiency; Security.

1. INTRODUÇÃO

Sistema Único de Saúde (SUS) é a denominação do sistema público de saúde brasileiro. Foi instituído pela Constituição Federal de 1988, em seu artigo 196. Com sua implantação, a população brasileira, com mais de 214 milhões de habitantes [44], passou a ter direito à saúde gratuita [15].

Ante a abrangência do SUS, a gestão de dados de seus pacientes redunda em um complexo processo que inclui ações como armazenar, atualizar e analisar milhões de prontuários médicos. Isso com o intuito, e.g., de melhorar os tratamentos oferecidos, rastrear as causas de enfermidades, direcionar a fabricação de medicamentos e, ainda, estabelecer uma agenda de medicina preventiva para o País [28, 29].

Por definição, o prontuário médico documenta, por exemplo, queixas, sintomas, exames, diagnósticos, tratamentos adotados e medicamentos prescritos, que são usualmente registrados de forma escrita (i.e., manualmente) durante o atendimento do paciente, gerando assim um arquivo em papel. Todavia, é fato que já existe um esforço para que essas informações também possam ser inseridas por meio de sistemas informatizados, possibilitando a criação dos denominados prontuários médicos eletrônicos (PMEs) [28, 29].

A expectativa natural é que os prontuários em papel sejam substituídos em sua totalidade pelos PMEs [28]. Para tanto, é imprescindível que os PMEs sejam consolidados em uma robusta base de dados, possibilitando o compartilhamento entre diferentes atores do SUS (e.g., clínicas, hospitais, etc.) e, também, entre o SUS e diferentes atores externos (e.g., laboratórios privados, centros de pesquisa, etc.). Esse compartilhamento impõe um sério desafio tecnológico, pois pressupõe uma base de dados com estritos requisitos de eficiência, segurança e escalabilidade [28, 29, 37, 46, 39]. Neste cenário, a principal questão que se apresenta é: Que tecnologia utilizar para construção e manutenção dessa base de dados?

O exposto acima é a motivação deste artigo, cujo objetivo é propor uma plataforma baseada na tecnologia Blockchain para gerenciamento de PMEs de pacientes do SUS. Esta tecnologia surgiu em 2008 com a proposta do sistema de pagamento eletrônico Bitcoin [34, 25]. Embora o foco original tenha sido as transações financeiras, logo a indústria e a academia identificaram Blockchain como uma solução disruptiva, baseada em técnicas criptográficas, possível de ser utilizada em inúmeras outras áreas, e.g., cidades inteligentes, logística, indústria, saúde e eleições (e.g., [42, 23, 8, 35]).

A Blockchain preconiza que as transações dos atores do sistema precisam ser inicialmente agrupadas em blocos que são validados por uma rede de nós processadores interligados sob arquitetura *peer-to-peer* (P2P). O resultado final é uma lista encadeada de blocos de transações, constituindo o livro razão do sistema (do inglês, *ledger*). As informações desta lista encadeada são então utilizadas para construir e manter a base de dados distribuída do sistema [34, 7, 8].

A análise da efetividade da plataforma aqui proposta é feita por discussão conceitual e modelagem analítica baseada em sistemas de filas, com foco nos requisitos de eficiência, segurança e escalabilidade, ademais de custo financeiro. Neste contexto, a principal contribuição desta pesquisa se revela pela oferta inédita de subsídios teóricos sólidos e experimen-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

tos para o desenvolvimento de projetos reais de uma base de dados para o SUS, baseada na tecnologia Blockchain.

O restante deste artigo é organizado como segue. A Seção 2 caracteriza um sistema baseado em Blockchain. Na Seção 3, apresenta-se o gerenciamento de PMEs no SUS. A Seção 4 revisa a literatura. Na Seção 5, tem-se a proposta da nova plataforma. A Seção 6 realiza a avaliação de desempenho. Por fim, conclusões e trabalhos futuros estão na Seção 7.

2. CARACTERIZAÇÃO: BLOCKCHAIN

2.1 Participantes e Permissão de Uso

Há três tipos de participantes: *simples*, *validador* e *minerador* [22, 31]. O primeiro é um usuário final, que utiliza o sistema para realizar transações. O segundo pode realizar e validar transações. Neste caso, o participante possui uma réplica da lista encadeada de blocos. Por fim, além de realizar/validar transações e ter uma réplica da lista encadeada, o terceiro tipo pode ainda criar e validar os blocos de transações que são eventualmente adicionados à lista encadeada.

Quanto à permissão de uso, o sistema pode ser do tipo *não permissionado* ou *permissionado* [31, 47]. No primeiro tipo, também nomeado de *público*, o sistema é aberto para participação. Neste caso, o participante opera sob um pseudônimo, podendo exercer o papel de *simples*, *validador* ou *minerador*. Os dados armazenados são visíveis para todos participantes. No segundo tipo, também chamado de *privado*, a participação necessita da anuência de uma autoridade predefinida. Neste caso, a visibilidade dos dados está sujeita a direitos de controle de acesso. De forma geral, o sistema *permissionado* possui comparativamente um menor número de *mineradores*, além de oferecer melhores níveis de eficiência e segurança à custa de menor descentralização.

2.2 Principais Atributos do Sistema

Os principais atributos são os seguintes [22, 23, 47]:

- Descentralização: uma terceira parte confiável para validação das transações não é necessária, pois a lista encadeada é mantida por múltiplos nós através da troca de mensagens e emprego de um algoritmo de consenso. Este algoritmo define as regras sobre as mensagens a serem trocadas e sobre quais e/ou quantos *mineradores* estão aptos a criar e validar os blocos de transações.

- Imutabilidade: A identificação de um bloco é feita a partir de seu cabeçalho, que inclui o *hash* criptográfico de seu conteúdo e a identificação do bloco anterior na lista. Qualquer modificação em um bloco, portanto, modifica todos os blocos subsequentes na lista. Isso torna a adulteração de um bloco computacionalmente difícil, conforme maior seja o tempo decorrido desde sua adição à lista, além do fato de existirem múltiplas réplicas da lista. No caso da inserção de informações incorretas ou da existência de atualizações, é necessário que novas transações sejam executadas com tal intento.

- Transparência: Qualquer mudança nas informações está vinculada a uma exclusiva e imutável transação, a qual pode ser visualizada por todos os participantes por meio das réplicas da lista encadeada.

- Rastreabilidade: Como todas as informações estão associadas a transações, que são imutáveis e visíveis por todos os participantes, há a possibilidade de verificação de todo o ciclo de vida das informações: desde a inserção até as eventuais atualizações e correções. Isso resulta em um efetivo mecanismo de auditoria sistêmica.

- Dispensa de Confiança Mútua: A execução de transações no sistema independe da confiança existente entre os participantes diretamente envolvidos (e.g., uma transferência financeira entre dois clientes de um banco). A confiança sistêmica entre todos os participantes é garantida pelo algoritmo de consenso adotado.

2.3 Fluxo da Execução de Transação

Uma transação é uma ação executada por um participante do sistema, usando criptografia assimétrica, que resulta na modificação da base de dados. O fluxo de execução de uma transação t, de um participante P, é dado a seguir [22, 47].

1. Submissão de t: P realiza o *hash* de t, obtendo H_t. P utiliza sua chave privada, K_{pv}, para encriptar H_t, obtendo $K_{pv}(H_t)$, que é a sua assinatura digital. P envia a concatenação $K_{pv}(H_t) + t$ em *broadcast* pela rede.

2. Validação de t: é feita por *validadores*. Consiste na autenticação da identidade de P, e na verificação da integridade de t. Para autenticação, desencripta-se $K_{pv}(H_t)$, recebido pela rede, usando a chave pública K_{pb} de P, obtendo-se: $K_{pb}(K_{pv}(H_t)) = H_t$. Se a desencriptação é exequível, então a identidade está autenticada. Para integridade, faz-se o *hash* de t, recebido pela rede, obtendo-se: H'_t. Daí, se $H_t = H'_t$, então t está íntegra e é enviada em *broadcast* para os *mineradores*.

3. Criação de blocos: o *minerador* agrupa as transações validadas em blocos, que são criados em acordo com as regras do protocolo adotado. Cada bloco tem um tamanho limite e é formado por um cabeçalho seguido por um conjunto de transações. As informações do cabeçalho variam em função da aplicação, mas usualmente são no mínimo: instante da criação; versão do protocolo; raiz da árvore de Merkle das transações; e *hash* do cabeçalho do bloco anterior. O bloco é então enviado em *broadcast* para outros *mineradores*.

4. Replicação: os *mineradores* verificam a validade dos blocos recebidos, conforme algoritmo de consenso adotado. Geralmente, essa verificação consiste ao menos em analisar as seguintes informações: *hash* do bloco, carimbo de tempo, *hash* do bloco anterior, validade das transações, e raiz da árvore de Merkle das transações. Uma vez verificada a validade, as ações subsequentes dependem do consenso adotado, e.g., adição do bloco à cópia local da lista, e envio de confirmação.

3. GERENCIAMENTO DE PMES NO SUS

3.1 Unidades de Sáude

O atendimento do paciente é feito em uma unidade de saúde (US), classificada em um dos tipos a seguir [15, 28]. A Unidade Básica de Saúde (UBS) atende a uma região geográfica de um município, contemplando o local de residência do

paciente. Nas UBSs são realizadas consultas ambulatoriais agendadas. A Unidade de Pronto Atendimento (UPA) é a unidade para onde o paciente se dirige em casos de emergência e/ou urgência. O Hospital/Clínica/Laboratório Público (HCL) é a unidade para onde o paciente também pode se dirigir em caso de emergência e/ou urgência (como no caso da UPA), ou onde o paciente realiza procedimentos médicos específicos, continuados e/ou de maior complexidade. Por fim, tem-se a Instituição Médica Conveniada (IMC), a qual é similar à HCL, diferindo apenas por ser uma entidade privada contratada pelo SUS.

3.2 Utilização dos PMEs

Cada paciente possui um único e exclusivo PME [15, 28]. Sua criação e manipulação é realizada por profissionais credenciados pelo SUS usando uma aplicação de *software* padronizada. A criação do PME ocorre quando o paciente visita alguma US pela primeira vez. Após isso, sempre que um paciente visita uma US para atendimento, os profissionais credenciados envolvidos nesse atendimento têm então acesso ao seu PME para manipulação, mediante o uso de senhas.

3.3 Eficiência, Segurança e Escalabilidade

A eficiência se traduz pela celeridade com que as operações realizadas na base de dados são atendidas. O tempo de resposta para obtenção dos resultados esperados deve estar dentro de limiares de tempo satisfatórios. Este requisito não é possível ser devidamente avaliado na corrente forma de gerenciamento. Isso porque não há ainda uma plena integração da base de dados. Em verdade, as USs ainda trabalham de forma parcialmente ou totalmente isoladas [15, 28, 29].

A segurança se traduz pela seguinte tríade: disponibilidade (i.e., os dados são acessíveis sempre que necessário), integridade (i.e., os dados armazenados não podem ser adulterados), e confidencialidade (i.e., os dados estão disponíveis apenas quando autorizados) [46, 39]. Na corrente forma de gerenciamento, a segurança está comprometida. Isso porque a disponibilidade é limitada, pois a base de dados não está integrada. Ainda, a integridade dos dados não é garantida, pois pode haver inconsistência entre dados redundantes [15, 28, 29]. Por fim, a confidencialidade é fragilmente assegurada, pois apenas há o uso simples de senhas de acesso [15, 28, 29]. Além disso, o próprio paciente não tem controle assertivo com respeito à divulgação de seus dados (armazenados no PME), o que termina indo de encontro à Lei Geral de Proteção de Dados Pessoais (LGPD) [32].

A escalabilidade se refere à capacidade de crescimento da base de dados sem comprometimento da sua efetividade, observando os requisitos discutidos anteriormente. O nível de escalabilidade da corrente base de dados não é possível ser avaliado apropriadamente. Isso porque a não integração da base de dados obstaculiza uma visão sistêmica [15, 28, 29]. Para efeito desta avaliação, neste trabalho são então estimados o volume de tráfego na rede e o tamanho da base de dados, ademais de custo financeiro de armazenagem.

4. REVISÃO DA LITERATURA

Os trabalhos seminais de gerenciamento de PMEs apontam para arquiteturas Cliente/Servidor, em que a US acessa os dados a partir uma base local. Essa base de dados armazena conjuntamente as transações (i.e., metadados) dos atores e os dados dos pacientes (i.e., prontuários médicos). Já os trabalhos mais recentes admitem arquiteturas em que as transações são armazenadas nas listas encadeadas da tecnologia Blockchain, enquanto os dados dos pacientes são armazenados em sistemas externos, e.g., servidores na nuvem. Essa concepção mais recente alia a segurança dos dados, provida pela Blockchain, com a escalabilidade do sistema, em termos de volume de dados armazenados, provida pela nuvem (e.g., [45, 16, 22]).

Ademais da permissão de uso explicada na Subseção 2.1, a distinção entre os trabalhos mais recentes fulcralmente reside nos seguintes dois pontos gerais. O primeiro é o número de listas encadeadas para armazenamento das transações. Isso define duas categorias de arquitetura [3]: lista única e múltiplas listas. A primeira é de mais simples concepção, resultando em projetos de maior facilidade de implantação. A segunda permite, à custa de maior complexidade de projeto e *overhead* computacional, mais efetivamente atender à confidencialidade dos dados quando há diferentes subgrupos de atores de negócio no mesmo sistema [20, 22].

O segundo ponto é o algoritmo de consenso para seleção dos *mineradores*. Há três critérios [31, 21, 13]: poder de processamento; capacidade de recursos; e votação. O primeiro reflete a celeridade para resolver problemas matemáticos (e.g., desafios criptográficos). O segundo se refere a algum recurso que o *minerador* possui (e.g., espaço em disco). O terceiro é um acordo em que um nó se torna *minerador* quando recebe o apoio da maioria dos outros *mineradores*. A escolha do critério de consenso depende da aplicação proposta, devendo estabelecer um compromisso entre eficiência e segurança: um consenso mais simples (complexo) implica maior (menor) celeridade e menor (maior) segurança.

Sob um viés comparativo, algoritmos que usam os critérios poder de processamento e capacidade de recursos são usualmente empregados para sistemas *não permissionados*, enquanto que aqueles baseados em votação são para sistemas *permissionados*. Ademais, o critério de poder de processamento usualmente está associado a um maior consumo de energia elétrica e limitada escalabilidade [31, 21, 13].

Na atualidade já existe um considerável número de *surveys* e *reviews* (e.g., [19, 23, 18, 6]) sobre sistemas de saúde baseados em Blockchain, em que plataformas, arquiteturas, aplicações, taxonomia, etc. são discutidas em um mesmo trabalho de pesquisa. Alternativamente, tencionando uma visão mais pontual, na sequência são então caracterizadas algumas das mais recentes e importantes propostas realizadas. O objetivo é prover ao leitor uma visão do estado da arte de propostas sob o tema de pesquisa aqui em análise.

Em [5], os autores propõem uma aplicação interoperável baseada em Blockchain, a qual permite aos profissionais de saúde credenciados compartilharem entre si os dados dos pacientes. Em [9, 27], os autores propõem uma estrutura de Blockchain para acesso a dados médicos habilitados por contrato inteligente. No caso desses três trabalhos, usa-se um mecanismo de consenso que considera o critério poder de processamento.

Em [1, 45], os autores desenvolvem uma estrutura de Blockchain para registros médicos usando um mecanismo de consenso baseado em votação. Em [10, 2, 36, 4], os sistemas de saúde baseados em Blockchain se destacam por permitir que os pacientes mantenham a administração primária dos seus dados, i.e., apenas os pacientes têm o direito de fazer a submissão de dados na rede. Nesses sistemas, os profissionais de saúde credenciados estão, portanto, habilitados apenas

para acesso aos dados dos pacientes. Em [40, 43, 24, 33], os autores propõem sistemas de saúde baseados em Blockchain com profissionais de saúde (credenciados) e pacientes habilitados para atualização de dados.

Com respeito especificamente ao SUS, não há, contudo, uma grande diversidade de obras. Neste contexto, apenas dois trabalhos recentes e mais relacionados são discorridos detalhadamente na sequência. Em [41], os autores apresentam um sistema baseado em Blockchain que tem o gerenciamento de PMEs executado pelos próprios pacientes, o que não é uma característica do SUS. Ademais, o sistema é restrito apenas ao atendimento terapêutico de reabilitação física e neurofuncional. Seu desenvolvimento é feito sobre a plataforma Ethereum. Os autores alertam sobre a necessidade de uma regulamentação governamental específica no setor de saúde, ainda não existente. Por fim, não há apresentação de resultados de avaliação de desempenho, e o respectivo projeto está aparentemente em estágio inicial de sua evolução.

Em [14], os autores propõem uma arquitetura para gerenciamento de PMEs usando a plataforma Hyperledger com multicanais. As transações são armazenadas nas listas encadeadas da Blockchain e os PMEs em sistemas externos. Embora a proposta não seja específica para o SUS, os experimentos incluem dados do mesmo para avaliação da escalabilidade em termos volume de dados armazenados. Assim como em [41], os pacientes têm participação no gerenciamento de seus PMEs, o que não é uma característica do SUS. Por fim, não há avaliação de requisitos de segurança e eficiência, o que termina impedindo uma conclusão mais contundente sobre a efetividade da proposta apresentada.

Ante os trabalhos relacionados, que estão sumarizados na Tabela 1, o ineditismo deste artigo se materializa pela proposta de uma plataforma dedicada ao SUS, bem como sua avaliação por meio de modelagem analítica usando teoria das filas. A avaliação realizada é ampla, incluindo requisitos de eficiência, segurança e escalabilidade, ademais do custo financeiro da armazenagem dos dados.

5. PROPOSTA DA PLATAFORMA

5.1 Arquitetura

Uma visão geral da arquitetura é apresentada na Fig. 1. Há três componentes constituintes: o primeiro se refere à US; o segundo é a rede de *mineração*; o terceiro é a base global de dados. O primeiro componente se comunica com os segundo e terceiro componentes por meio de uma rede de comunicação de dados (e.g., Internet). Não há comunicação direta entre os segundo e terceiro componentes.

O primeiro componente na prática existe em igual número ao total de US no Brasil. Cada US opera como um participante *simples*, administrado pela Secretaria de Saúde do município onde está localizado. O segundo componente é único, constituído por *mineradores*. Sua finalidade é a criação e a validação de blocos de transações, geradas pelas USs. O terceiro componente, que é um armazenamento externo, também é único. Sua finalidade é armazenar PMEs. Os segundo e terceiro componentes são administrados pelo Ministério da Saúde.

A comunicação entre os componentes ocorre conforme operações descritas a seguir, em que apenas as essencialidades do processo são abordadas (para detalhamento das transações, vide Subseção 2.3). Ademais, por objetividade, o tratamento de exceções e inconsistências é deliberadamente omitido.

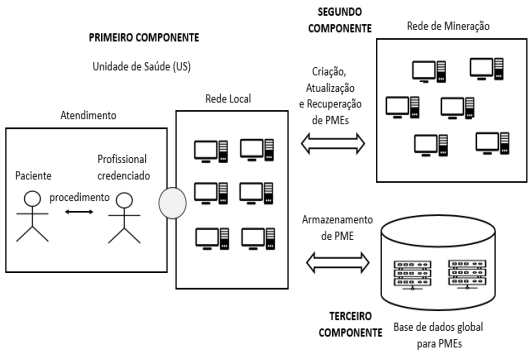

Figura 1: Visão geral da arquitetura.

- Criação de PME: o primeiro componente cria um novo PME no primeiro atendimento de um paciente. O primeiro componente então envia ao segundo componente uma transação. Esta transação contém o *hash* do PME e as chaves públicas do paciente e do atendente, respectivamente. Após a criação e a validação de um bloco contendo a transação em questão, o segundo componente então notifica o primeiro componente. O primeiro componente então envia ao terceiro componente o PME, o *hash* do PME, e as chaves públicas do paciente e do atendente, respectivamente. Esta última interação é a operação de Armazenamento.

- Atualização de PME: esta operação é semelhante à operação de Criação. A diferença é que Criação se refere à primeira visita do paciente, enquanto que Atualização se refere às visitas subsequentes. Ambas operações adicionam informações à base de dados externa (no terceiro componente), e são auditáveis a partir da lista encadeada de blocos (no segundo componente).

- Recuperação de PME: o primeiro componente envia ao segundo componente uma transação. Esta transação contém a chave pública do paciente. Após realizar uma busca exitosa na lista encadeada, o segundo componente envia ao primeiro componente o *hash* do PME do paciente. O primeiro componente então envia ao terceiro componente o *hash* do PME, junto com a chave pública do paciente. Por fim, confirmada exitosamente a integridade do PME a partir do *hash* informado, o terceiro componente envia uma cópia do PME ao primeiro componente.

- Armazenamento de PME: esta operação ocorre ao final das operações de Criação e Atualização. Porém, para maior celeridade, também é permitido o seguinte. Quando o PME é criado/atualizado no primeiro componente, o seu armazenamento é feito imediatamente no terceiro componente sob o *status* de temporário, mesmo antes da criação e validação do bloco correspondente no segundo componente. Mais tarde, após a criação e a validação do bloco, o *status* de armazenamento passa ao *status* de permanente.

Tabela 1: Síntese de trabalhos relacionados

Referências	Tipo de pesquisa	Caracterização principal	Principal limitação
[19, 23, 18, 6]	*Surveys* e *reviews*	Conceitos, taxonomia, comparações, estudos de caso, etc.	Baseado em trabalhos anteriores, sem apresentação de novas propostas
[5, 9, 27]	Propostas de aplicações	Compartilhamento de dados do paciente. Uso de contratos inteligentes. Consenso baseado em poder de processamento.	Consenso pode comprometer eficiência e escalabilidade.
[1, 45]	Propostas de aplicações	Consenso baseado em votação.	Consenso pode aumentar complexidade de implantação e operação.
[10, 2, 36, 4]	Propostas de aplicações	Administração primária dos dados por parte dos pacientes.	Administração de dados pode dificultar interoperabilidade dos dados entre unidades de saúde.
[40, 43, 24, 33]	Propostas de aplicações	Pacientes e profissionais credenciados estão habilitados para atualização de dados.	Administração de dados pode comprometer segurança e confidencialidade de dados
[41]	Propostas de aplicações	Refere-se ao SUS. Dados gerenciados pelos pacientes. Atendimento terapêutico de reabilitação física e neurofuncional.	Sem resultados de avaliação de desempenho. Projeto em estágio inicial de sua evolução e de escopo restrito.
[14]	Propostas de aplicações	Refere-se (parcialmente) ao SUS. Dados gerenciados pelos pacientes. As transações são armazenadas nas listas encadeadas da Blockchain e os dados dos pacientes em sistemas externos.	Como em [41], sem resultados de avaliação de desempenho. Projeto em estágio inicial de sua evolução e de escopo restrito.

Menciona-se ainda que a arquitetura assume a operação do sistema na categoria *permissionado*. A escolha dessa categoria se dá pelo fato de o SUS não poder prescindir de uma política de segurança austera quanto à participação de atores. Isso devido à sensibilidade das informações dos pacientes [32].

5.2 Algoritmo de Consenso

O algoritmo de consenso é o Practical Byzantine Fault Tolerance (PBFT). Este algoritmo é do tipo baseado em votação e, no caso de sistemas *permissionados*, se apresenta como um dos mais competitivos para adequado compromisso entre eficiência e segurança, especialmente quando o número de *mineradores* da rede é inferior a 200 [21, 14].

A operação do PBFT é como segue. Seja M_j o j-ésimo *minerador* da rede, com $1 \leq j \leq n$ e n o número de unidades federativas do Brasil. Um *minerador* líder é escolhido dentre os n possíveis de forma circular. Este líder recebe todas as transações originadas pelo primeiro componente (i.e., participantes *simples*). As transações recebidas são validadas e um bloco é criado. O bloco é então enviado em *broadcast* para os demais *mineradores*. Ao receber o bloco, cada *minerador* verifica as transações contidas, calcula o *hash* do bloco, e envia esse *hash* em *broadcast* para os demais *mineradores*. Cada *minerador* então atualiza sua cópia de lista encadeada se receber o mesmo valor de *hash* de ao menos $\frac{2n}{3}$ *mineradores*, promovendo assim a convergência global da base de dados.

6. AVALIAÇÃO DE DESEMPENHO

6.1 Eficiência e Disponibilidade

Para avaliação da eficiência e da disponibilidade, mede-se o tempo de resposta, T_R, que corresponde ao intervalo de tempo desde o envio da transação até o recebimento da resposta, pelo primeiro componente. T_R é calculado em (1), onde: T_1 é o atraso de transmissão da transação do primeiro componente para o segundo componente; T_2 é o atraso de transmissão da resposta do segundo componente para o primeiro componente; e T_P é o tempo de processamento no segundo componente.

$$T_R = T_1 + T_2 + T_P \tag{1}$$

Nesta modelagem, os atrasos de propagação são desprezados e, ainda, tem-se $T_1 = T_2 = D/U$, onde: D é o tamanho da transação; e U é a capacidade de transmissão dos enlaces de comunicação entre os componentes. Para análise de T_P, admite-se a visão do *minerador* líder do segundo componente, considerando os três casos a seguir, ilustrados na Fig. 2

1) Melhor Caso: é o cenário de mínimo T_P, pois todos os *mineradores* estão conectados entre si diretamente. A rede é representada por um grafo completo $G = (V, A)$, com $|V| = n$ e $|A| = n(n-1)/2$. Cada nó é um *minerador*, e cada aresta é um enlace de comunicação. O grau de cada nó é $(n-1)$. T_P é calculado como o tempo de resposta de um sistema de filas, T_{fila}, somado aos atrasos de transmissão de mensagens na rede. O sistema de filas é do tipo $M/E_k/1/\infty/FIFO$ [26, 38, 30] (vide Fig. 3), onde

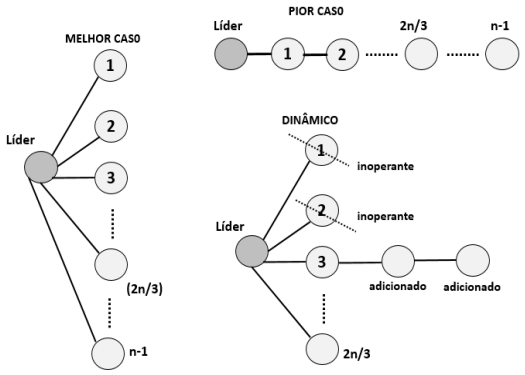

Figura 2: Casos de análise: Melhor, Pior e Dinâmico.

as chegadas de transações seguem um processo de Poisson de taxa λ, e o tempo de serviço tem distribuição Erlang com parâmetros $1/(k\mu)$ e k, sendo $1/(k\mu)$ o tempo médio de cada estágio, e $k = 2$ o número de estágios. A taxa λ é aqui estimada pelo número médio de visitas de paciente ao SUS no período de um ano, e o parâmetro $1/\mu$ é tempo médio de validação de um bloco de transações sob consenso PBFT. Assim, (1) é reescrita como (2), onde: C é a capacidade de transmissão dos enlaces de comunicação entre os *mineradores* do segundo componente; $T_3 = B/C$ é o atraso de transmissão do bloco, sendo B o tamanho do bloco; e $T_4 = H/C$ é o atraso de transmissão do *hash* do bloco, sendo H o tamanho do *hash*. T_{fila} é então calculado em (3), onde: L_{buf} é o número de transações esperando no *buffer* de entrada, calculada em (4); e $\rho = \lambda/\mu < 1$ (i.e., sistema estável) é a taxa de ocupação do sistema.

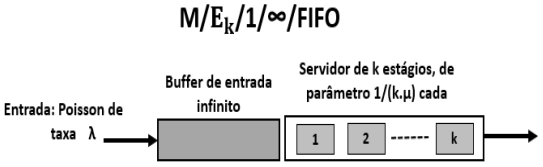

Figura 3: Sistema de filas do tipo $M/E_k/1/\infty/FIFO$.

$$T_R = T_1 + T_2 + T_{fila} + T_3 + T_4 \tag{2}$$

$$T_{fila} = \frac{L_{buf}}{\lambda} + \frac{1}{\mu} \tag{3}$$

$$L_{buf} = \frac{\rho^2(1/k+1)}{2(1-\rho)} \tag{4}$$

2) Pior Caso: é o cenário de máximo T_P. A rede é representada por um grafo conexo $G = (V, A)$, com $|V| = n$ e $|A| = n - 1$. Cada nó é um *minerador*, e cada aresta é um enlace de comunicação. O grau do líder e do n-ésimo nó é 1, e dos demais nós é 2, resultando em um caminho simples desde o nó líder até o n-ésimo nó. T_P é estimado pelo tempo de resposta de um sistema de filas, T_{Fila}, somado aos atrasos de transmissão de mensagens na rede. O sistema de filas é do mesmo tipo que no caso anterior. Mas, devido à diferente topologia da rede, (2) é reescrita como (5), sendo $k = 2/3n + 1$. T_{fila} é obtido usando ainda (3) e (4).

$$T_R = T_1 + T_2 + T_{fila} + (k-1)T_3 + (k-1)T_4 \tag{5}$$

3) Caso Dinâmico: é o cenário usado para verificar a disponibilidade, pois admite a variação do número de mineradores conectados diretamente ao líder. A rede é representada por um grafo conexo $G = (V, A)$, com $|V| = n$ e $|A| \leq n^2$. Cada nó é um *minerador*, e cada aresta é um enlace de comunicação. Ao início, o grau do líder é $\frac{2n}{3}$, que é o valor mínimo de mensagens de confirmação para adição do bloco sob PBFT. Se um vizinho do líder se torna inoperante (ou inalcançavel), o grau do líder diminui em 1, e a topologia de análise muda: um vizinho é adicionado a um dos vizinhos do líder ainda operantes. A partir daí, sempre que um vizinho do líder se torna inoperante (ou inalcançável), o grau do líder diminui em 1, e um vizinho é adicionado ao último vizinho adicionado, resultando em uma lista encadeada de nós. Se o número de vizinhos inoperantes (inalcançáveis) do líder atinge $(\frac{2n}{3} - 1)$, o caso dinâmico se reduz ao pior caso. T_P é estimado pelo tempo de resposta de um sistema de filas, T_{fila}, somado aos atrasos de transmissão de mensagens na rede. O sistema de filas é do mesmo tipo que no caso anterior. Mas, devido à diferente topologia da rede, tem-se que (2) é reescrita como (6), sendo $k = i + 2$, onde i é igual ao número de vizinhos inoperantes (ou inalcançáveis) pelo líder. Por sua vez, T_{fila} é obtido usando ainda (3) e (4).

$$T_R = T_1 + T_2 + T_{fila} + (i+1)T_3 + (\sum_{j=0}^{i}(j+1))T_4 \tag{6}$$

A Tabela 2 resume os principais parâmetros utilizados no cômputo de T_R. Os valores indicados se baseiam em análises anteriores de plataformas de saúde e de consenso PBFT (e.g., [22, 23, 21]). Em seu turno, a Tabela 3 estima a taxa de transações λ e o tamanho do incremento anual da base de dados do terceiro componente, considerando os anos de 2021 a 2030. A estimativa baseia-se na taxa de crescimento anual da população brasileira (pior caso: fixada em 0,78% ao ano [44]) e no número médio de visitas ao SUS realizadas no ano de 2018. Naquele ano, houve cerca de 1,4 bilhão de visitas [29] para uma população de $\approx$ 209,5 milhões de habitantes [44]. Assume-se que cada visita resulta em uma transação, a qual produz um arquivo a ser armazenado no terceiro componente de tamanho igual ao do PME, pois admite-se que a transação realiza a criação do PME (na primeira visita do paciente) ou atualiza o PME (em atendimentos subsequentes).

Para análise da eficiência, tem-se então a Fig. 4. Note a baixa variabilidade de T_R em ambos casos (melhor e pior) no período de 2021 (λ = 45,53 TPS) a 2030 (λ = 48,71 TPS). Numericamente, T_R é $\approx$ 4,40 seg no melhor caso, e $\approx$ 10,25 seg no pior caso. Em conclusão, é possível conjecturar que a eficiência do sistema é adequada, pois T_R está dentro de limites aceitáveis para não comprometer o nível de qualidade de serviço do sistema ou da qualidade de experiência do usuário.

Para análise da disponibilidade, tem-se a Fig. 5. O objetivo é identificar a robustez do sistema ante a inoperância (ou inalcançabilidade) dos *mineradores* da rede. Este cenário supõe, e.g., um ataque de indisponibilidade à rede ou mesmo uma falha de operação dos enlaces de comunicação.

Tabela 2: Síntese de parâmetros.

Parâmetro	Valor	Definição
T_R	Variável	Tempo de resposta em segundos. Corresponde ao intervalo de tempo que decorre desde o envio da transação pelo primeiro componente da arquitetura até o recebimento da resposta pelo mesmo. Varia em função da taxa de transações λ.
D	250 B	Tamanho da transação em bytes. A transação é constituída ao menos de: chave pública do paciente (32 B); chave pública do profissional (32 B); tipo de operação e metadados (186 B).
C	7,25 MB/s	Capacidade de transmissão de dados (em megabytes por segundo) dos enlaces de comunicação entre os *mineradores*. Tem por base estimativas da velocidade de conexão da Internet nas cinco regiões do Brasil [11].
U	2,58 MB/s	Capacidade de transmissão de dados (em megabytes por segundo) do primeiro componente para o segundo componente da arquitetura. Tem por base estimativas da velocidade de conexão da Internet nas cinco regiões do Brasil [11].
B	2,50 MB	Tamanho do bloco de transações em megabytes. Assume-se que o bloco contém 10.000 transações, além de metadados pertinentes.
n	27	Número de *mineradores* do segundo componente. É estimado pelo número de unidades federativas do Brasil.
λ	Variável	Taxa de entrada de transações no segundo componente da arquitetura, medida em transações por segundo (TPS). É estimada pela taxa média de visitas de pacientes ao SUS a cada ano (vide Tabela 3).
$1/\mu$	4 seg	Tempo médio de processamento de um bloco de 10.000 transações sob consenso PBFT, medido em segundos.
k	Variável	Número de estágios da distribuição de Erlang. Seu valor varia em função da topologia da rede.
R	25,86 MB	Tamanho do PME em megabytes. Assume-se que o PME é constituído de imagens, filmes e textos.
H	32 B	Tamanho do *hash* do bloco em bytes. O algoritmo de *hash* utilizado é o conhecido SHA-256.

Tabela 3: Número de visitas e base de dados.

Ano	População (hab)	# Visitas SUS	λ (TPS)	Incremento (PB)
2021	214.367.735	1.432.529.017	45,43	37,04
2022	216.039.803	1.443.702.743	45,78	37,33
2023	217.724.913	1.454.963.624	46,14	37,63
2024	219.423.168	1.466.312.341	46,50	37,91
2025	221.134.668	1.477.749.577	46,86	38,21
2026	222.859.519	1.489.276.024	47,23	38,51
2027	224.597.823	1.500.892.377	47,60	38,81
2028	226.349.686	1.512.599.337	47,96	39,11
2029	228.115.214	1.524.397.612	48,33	39,42
2030	229.894.512	1.536.287.913	48,71	39,72

Como mencionado, o *minerador* líder tem uma conectividade inicial de $\frac{2n}{3}$, que é progressivamente afetada. A partir dos resultados, tem-se que, e.g., para uma perda de 27,8%

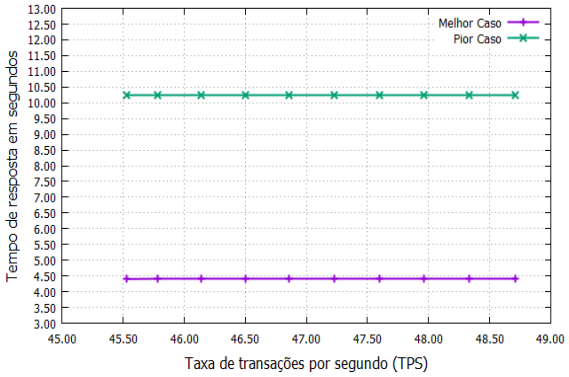

Figura 4: Análise de eficiência: melhor e pior casos.

(i.e., $i = 5$) da conectividade, eleva-se o T_R em 38,9%; e para uma perda de 50% (i.e., $i = 9$), eleva-se o T_R em 70,2%. Em conclusão, conjectura-se que a robustez do sistema não é adequada, pois T_R é significativamente impactado. Como solução, dever haver *mineradores* de contingência, que vão operar estrategicamente quando do impedimento de outros.

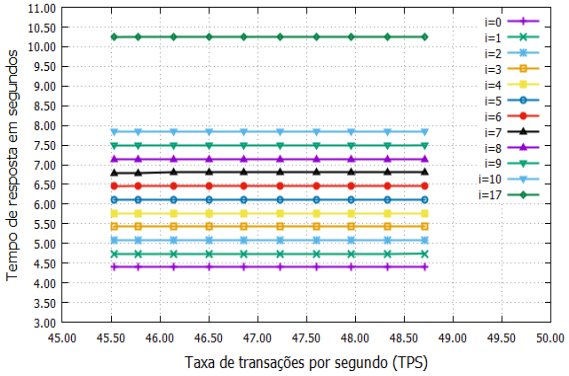

Figura 5: Análise de disponibilidade: caso dinâmico.

6.2 Integridade e Confidencialidade

A integridade e a confidencialidade dos dados são asseguradas pela própria concepção da Blockchain, como explicado a seguir. A integridade é garantida pelo fato de os blocos de transações serem interligados sob a forma de uma lista encadeada, onde o elo de ligação entre os mesmos consiste no *hash* do cabeçalho do bloco anterior, que inclui o conteúdo das transações nele armazenadas. A mudança de alguma dessas transações implica a alteração de todos os blocos subsequentes, o que resulta em uma tarefa computacionalmente difícil (vide Subseção 2.2). Por sua vez, a confidencialidade dos dados do PME pode ser implementada pela cifração do mesmo com a chave pública do paciente. Para acesso aos dados cifrados, o paciente então concede a autorização por meio de sua chave privada, passando a ter controle sobre os dados do seu PME.

6.3 Escalabilidade e Custo

O aumento do tráfego de dados e o aumento do tamanho da base de dados não comprometem a eficiência sistêmica, conforme estimativa de T_R (vide Fig. 4). Ademais, a se-

gurança sistêmica tampouco é afetada (vide Subseção 6.2). Portanto, pode-se conjecturar que o sistema possui adequada escalabilidade. Para o custo da armazenagem, tem-se a Fig. 6. É mostrado o tamanho total em petabytes da base de dados a cada ano, com base nos incrementos anuais da Tabela 3. Para implantação em 2021, haveria um custo de armazenagem mensal de R$ 7,52 milhões, totalizando R$ 90,24 milhões em 12 meses [17]. A cada ano subsequente, haveria um acréscimo de ≈ 38,52 PB, perfazendo um custo de R$ 7,82 milhões ao mês, e de R$ 93,84 milhões ao ano. Assim, teria-se em 2030 um custo anual de R$ 934,9 milhões. Com referência ao orçamento do Ministério da Saúde de R$ 136,76 bilhões em 2021 [12], o custo em 2030 representaria apenas 0,68%. Daí, conjectura-se que o impacto econômico é aceitável.

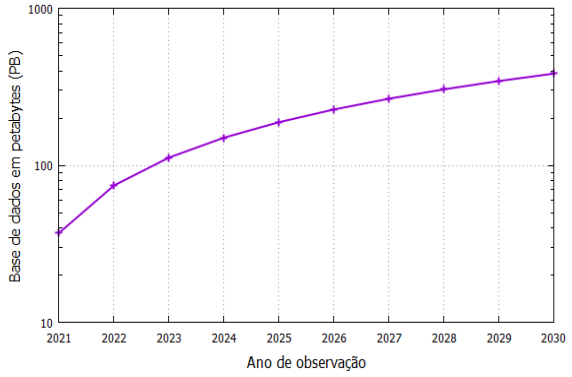

Figura 6: Crescimento da base de dados.

7. CONCLUSÕES FINAIS

Este artigo apresentou uma plataforma baseada em Blockchain para gerenciamento de prontuários eletrônicos médicos de pacientes do SUS. Por meio de modelagem analítica e discussão conceitual, foi possível confirmar uma efetividade adequada da plataforma proposta, sob os requisitos de eficiência, segurança e escalabilidade, bem como um aceitável custo econômico.

Vale ressaltar que a modelagem de filas e toda a metodologia utilizada nos experimentos, pode ser utilizada como base para avaliar diferentes sistemas baseados em Blockchain, inclusive considerando outras áreas de aplicações diferentes da saúde.

Como pesquisas futuras e ante as limitações desta pesquisa, apontam-se: análise de algoritmos de consenso diferentes do Practical Byzantine Fault Tolerance (PBFT); comparação com outras propostas de plataformas semelhantes; estudo de tecnologias de registros distribuídos diferentes da Blockchain; e realização de simulações e medições para retificação e/ou ratificação dos resultados aqui alcançados.

8. REFERÊNCIAS

[1] Fan K., Wang S., Ren Y., Li H., and Yang Y. Medblock: Efficient and secure medical data sharing via blockchain. *Jounal of Medical Systems*, 42(8), 2018. doi:10.1007/s10916-018-0993-7.

[2] Yue X., Wang H., Jin D., Li M., and Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Jounal of Medical Systems*, 40(10), 2016. doi:10.1007/s10916-016-0574-6.

[3] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, Porto, Portugal, 2018. doi:10.1145/3190508.3190538.

[4] Aswin A.V. and Basil K.Y. and Viswan V.P. and Reji B. and Kuriakose B. Design of AYUSH: A Blockchain-Based Health Record Management System. In *Inventive Communication and Computational Technologies*, volume 89 of *Lecture Notes in Networks and Systems*, pages 665–672. Springer, Singapore, 2020. doi:10.1007/978-981-15-0146-3_62.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman. MedRec: Using Blockchain for Medical Data Access and Permission Management. In *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, 2016. doi:10.1109/OBD.2016.11.

[6] K. Azbeg, O. Ouchetto, S. Andaloussi, and L. Fetjah. A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications. *IRBM*, 2021. doi:10.1016/j.irbm.2021.05.003.

[7] F. Casino, T. K. Dasaklis, and C. Patsakis. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36:55–81, 2019. doi:10.1016/j.tele.2018.11.006.

[8] C. K. da Silva Rodrigues. Analyzing Blockchain integrated architectures for effective handling of IoT-ecosystem transactions. *Computer Networks*, 201:108610, 2021. doi:10.1016/j.comnet.2021.108610.

[9] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39:283–297, 2018. doi:10.1016/j.scs.2018.02.014.

[10] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre. HealthSense: A medical use case of Internet of Things and blockchain. In *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, pages 486–491, Palladam, India, 2017. doi:10.1109/ISS1.2017.8389459.

[11] Dácio Castelo Branco. Pesquisa mostra qual estado tem maior velocidade de internet do Brasil, 2021. [Online]. Available at: https://canaltech.com.br/internet/pesquisa-mostra-qual-estado-tem-maior-velocidade-media-de-internet-do-brasil-195456/. Accessed on: Sept. 9th, 2021.

[12] Empresa Brasil de Comunicação. Notícia - Saúde tem previsão de aumento de R$ 10,7 bilhões no Orçamento de 2022, 2021. [Online]. Available at:https://agenciabrasil.ebc.com.br/. Accessed on: Sept. 23rd, 2021.

[13] M. S. Ferdous, M. J. M. Chowdhury, and M. A.

Hoque. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, 182:103035, 2021. doi:10.1016/j.jnca.2021.103035.

[14] A. Fernandes, V. Rocha, A. F. d. Conceição, and F. Horita. Scalable Architecture for sharing EHR using the Hyperledger Blockchain. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*, Salvador, Brazil, 2020. doi:10.1109/ICSA-C50368.2020.00032.

[15] FIOCRUZ. O SUS do Brasil, 2021. [Online]. Available at: https://pensesus.fiocruz.br/sus. Accessed on: July. 10th, 2021.

[16] P. S. R. Garcia and J. H. Kleinschmidt. Sharing Health and Wellness Data with Blockchain and Smart Contracts. *IEEE Latin America Transactions*, 18(06):1026–1033, 2020. doi:10.1109/TLA.2020.9099679.

[17] Google Cloud. Google Cloud Pricing Calculator, 2021. [Online]. Available at:https://cloud.google.com/products/calculator/. Accessed on: Sept. 22nd, 2021.

[18] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab. Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, 2:130–139, 2021. doi:10.1016/j.ijin.2021.09.005.

[19] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag. Blockchain in healthcare and health sciences - A scoping review. *International Journal of Medical Informatics*, 134:104040, 2020. doi:10.1016/j.ijmedinf.2019.104040.

[20] J. J. Hunhevicz and D. M. Hall. Do you need a blockchain in construction? use case categories and decision framework for dlt design options. *Advanced Engineering Informatics*, 45:101094, 2020. doi:10.1016/j.aei.2020.101094.

[21] Isitan Gorkey and Chakir El Moussaoui and Vincent Wijdeveld and Erik Sennema. Comparative Study of Byzantine Fault Tolerant Consensus Algorithms on Permissioned Blockchains, 2020. [Online]. Available at: http://resolver.tudelft.nl/uuid:01083a4a-900b-4cf9-9746-cb9258c11d9e. Accessed on: Aug. 29th, 2021.

[22] L. Ismail and H. Materwala. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry*, 11(10), 2019. doi:10.3390/sym11101198.

[23] L. Ismail and H. Materwala. Blockchain paradigm for healthcare: Performance evaluation. *Symmetry*, 12(8), 2020. doi:10.3390/sym12081200.

[24] Kaur H., Alam M.A., Jameel R., Mourya A.K., and Chang V. . A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *Journal of Medical Systems*, 42(8), 2018. doi:10.1007/s10916-018-1007-5.

[25] P. K. Kaushal, A. Bagga, and R. Sobti. Evolution of bitcoin and security risk in bitcoin wallets. In *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, pages 172–177, Jaipur, India, 2017. doi:10.1109/COMPTELIX.2017.8003959.

[26] L. Kleinrock. *Queuing Systems. Volume I: Theory.* Wiley, New York, 1975.

[27] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu. Blockchain-based data preservation system for medical data. *Jounal of Medical Systems*, 42(141), 2018. doi:10.1007/s10916-018-0997-3.

[28] Ministério da Sáude do Brasil. Plataforma de saúde para o cidadão, profissionais e gestores de saúde, 2021. [Online]. Available at: https://conectesus.saude.gov.br/home. Accessed on: July. 10th, 2021.

[29] Ministério da Sáude do Brasil. Relatório de Gestão 2018, 2021. [Online]. Available at: https://bvsms.saude.gov.br/bvs/publicacoes/relatorio/_gestao/ Accessed on: Sept. 13rd, 2021.

[30] A. G. N. Novaes. *Pesquisa operacional e transportes: modelos probabilísticos*. McGraw-Hill do Brasil, São Paulo, 1975.

[31] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry*, 13(8), 2021. doi:10.3390/sym13081363.

[32] Presidência da República do Brasil. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei Nº 13.853, de 8 de julho de 2019, 2019. [Online]. Available at: http://www4.planalto.gov.br/legislacao/.

[33] A. Roehrs, C. A. da Costa, and R. da Rosa Righi. OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, 71:70–81, 2017. doi:10.1016/j.jbi.2017.05.012.

[34] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Available at: https://bitcoin.org/bitcoin.pdf. Accessed on: July. 10th, 2021.

[35] A. I. Sanka and R. C. Cheung. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, 195:103232, 2021. doi:10.1016/j.jnca.2021.103232.

[36] S. Tanwar, K. Parekh, and R. Evans. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50:102407, 2020. doi:10.1016/j.jisa.2019.102407.

[37] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, 2019. doi:10.1016/j.dcan.2019.01.005.

[38] K. S. Trivedi. *Probability and Statistics with Reliability, Queuing and Computer Science Applications*. John Wiley & Sons, New York, second edition, 2002.

[39] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente. Towards Secure and Decentralized Sharing of IoT Data. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 176–183, July 2019.

[40] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian. Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture. *IEEE Access*, 6:32700–32726, 2018. doi:10.1109/ACCESS.2018.2846779.

[41] C. Viana, A. F. Brandão, D. R. C. Dias, G. Castellano, and M. D. P. Guimaraes. Blockchain para gerenciamento de prontuários eletrônicos. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 1(28):177–187, 2020.

[42] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu. Blockchain for the IoT and industrial IoT: A review. *Internet of Things*, page 100081, 2019.

[43] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang. Blockchain-powered parallel healthcare systems based on the acp approach. *IEEE Transactions on Computational Social Systems*, 5(4):942–950, 2018. doi:10.1109/TCSS.2018.2865526.

[44] Worldometer. Brazil Population, 2021. [Online]. Available at: https://www.worldometers.info/world-population/brazil-population/. Accessed on: Sept. 13rd, 2021.

[45] M. Zghaibeh, U. Farooq, N. U. Hasan, and I. Baig. SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities. *IEEE Access*, 8:70030–70043, 2020. doi:10.1109/ACCESS.2020.2986789.

[46] K. Zhang and H. Jacobsen. Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 1337–1346, July 2018.

[47] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.*, 14:352–375, 2018. doi:10.1504/IJWGS.2018.10016848.