Revista de Informática Teórica e Aplicada - RITA - ISSN 2175-2745
Vol. 29, Num. 03 (2022) 11-20

RESEARCH ARTICLE

Comparative Analysis of Blockchain-Based Platforms for Managing Electronic Health Records in the Public Healthcare System of Brazil

Análise Comparativa de Plataformas Baseadas em Blockchain para Gerenciamento de Prontuários Médicos Eletrônicos no Sistema de Saúde Público do Brasil

Carlo Kleber da Silva Rodrigues[1]*

Abstract: This article comparatively analyzes two platforms based on Blockchain, aiming at the management of electronic health records in the public healthcare system of Brazil. The difference between the platforms primarily lies in the deployed consensus algorithm. Efficiency, availability, integrity, and confidentiality requirements are evaluated through analytical models and theoretical discussions. Among the obtained results, we highlight the following: (i) the platform with a voting-based consensus algorithm yields a more efficient system, but is more prone to service unavailability, than that of the platform deploying an intensive-compute consensus algorithm; (ii) integrity and confidentiality requirements may be satisfactorily met regardless of the consensus type. As the main contribution, this article provides valuable experimental results and theoretical subsidies, which together complement previous research and help to lay the groundwork for the fruitful development of real projects. Finally, conclusions and future work conclude this article.
Keywords: Blockchain – Platform — Healthcare — Efficiency — Security

Resumo: Este artigo analisa comparativamente duas plataformas baseadas em Blockchain, visando o gerenciamento de prontuários médicos eletrônicos do sistema público de saúde do Brasil. A diferença entre as plataformas reside principalmente no algoritmo de consenso usado. Requisitos de eficiência, disponibilidade, integridade e confidencialidade são avaliados com modelos analíticos e discussões teóricas. Dentre os resultados obtidos, destacam-se: (i) a plataforma com algoritmo de consenso com critério de votação resulta em um sistema mais eficiente, porém mais propenso à indisponibilidade de serviço, que aquele da plataforma com algoritmo de consenso com critério de computação intensiva; (ii) os requisitos de integridade e confidencialidade podem ser satisfatoriamente atendidos independentemente do critério de consenso. Como principal contribuição, este artigo fornece valiosos resultados experimentais e subsídios teóricos, os quais juntos complementam pesquisas anteriores e ajudam a alicerçar o caminho para o desenvolvimento profícuo de projetos reais. Por fim, conclusões e trabalhos futuros encerram este artigo.
Palavras-Chave: Blockchain — Plataforma — Saúde — Eficiência — Segurança

[1] *Centro de Matemática, Computação e Cognição (CMCC), Universidade Federal do ABC (UFABC), Santo André - São Paulo, Brasil*
***Corresponding author**: carlo.kleber@ufabc.edu.br
DOI: http://dx.doi.org/10.22456/2175-2745.125396 • **Received:** 22/06/2022 • **Accepted:** 27/09/2022

1. Introdução

Propostas tradicionais para gerenciamento de Prontuários Médicos Eletrônicos - PMEs (do inglês, *Electronic Health Records* - EHR) [1, 2, 3, 4] usualmente consideram plataformas de arquitetura Cliente/Servidor, em que Unidades de Saúde (USs) acessam informações a partir de múltiplas bases de dados, com baixo nível de compartilhamento e limitada garantia de consistência e integridade. Em seu turno, pesquisas mais recentes admitem arquiteturas baseadas na tecnologia Blockchain [5, 6, 7, 4], em que transações (e.g., busca e inserção de informações) de participantes do sistema (e.g., médicos e enfermeiros) são armazenadas em listas encadeadas de blocos de dados, enquanto PMEs são armazenados em sistemas externos na nuvem. Essa concepção mais recente alia a expectativa de maior segurança de dados, devido ao uso da Blockchain, com a escalabilidade sistêmica, fornecida pela nuvem.

A tecnologia Blockchain tem sua origem no ano de 2008 com o sistema de pagamento eletrônico Bitcoin [8]. Embora o objetivo original tenha sido as transações financeiras,

logo a indústria e a academia identificaram essa tecnologia como uma solução disruptiva possível de ser utilizada em inúmeras outras áreas, incluindo a de sistemas de informação de saúde [9]. Para a submissão de transações sob Blockchain, cada participante possui duas chaves criptográficas: uma privada, que lhe permite assinar a transação, e uma pública, que permite ao sistema confirmar a autoria da transação. As transações são agrupadas em blocos que são validados por uma rede de nós processadores, denominados *mineradores*. Esses nós são interligados em arquitetura *peer-to-peer* (P2P), constituindo a chamada rede de *mineração*. O resultado é uma lista encadeada de blocos que forma o livro razão do sistema (do inglês, *system ledger*). As informações contidas nessa lista são utilizadas para construir e manter a base de dados distribuída do sistema.

Com a tecnologia Blockchain, tem-se a garantia dos seguintes atributos [10, 11, 12]: (i) descentralização, uma terceira parte confiável não é necessária para validar transações, pois as informações são mantidas por múltiplos *mineradores*; (ii) imutabilidade, cada bloco é identificado pelo *hash* de seu cabeçalho, que inclui um resumo das transações nele existentes e o *hash* do cabeçalho do bloco anterior na lista. Com isso, a modificação de um bloco se torna então impraticável, pois levaria à necessidade da alteração de todos os blocos subsequentes; (iii) pseudoanonimato, o participante é identificado apenas por sua chave pública, não havendo associação com sua identificação no mundo real; (iv) transparência, qualquer informação é vinculada a uma exclusiva e imutável transação, que pode ser visualizada pelos participantes de acordo com o controle de acesso; (v) rastreabilidade, como as informações estão associadas a transações, existe a possibilidade de auditoria; (vi) dispensa de confiança mútua, a realização de transações não depende da confiança entre participantes, pois a garantia é dada pelo algoritmo de consenso.

Neste contexto, este artigo analisa comparativamente duas plataformas baseadas em Blockchain, visando o gerenciamento de PMEs de pacientes do sistema público de saúde do Brasil, denominado de Sistema Único de Saúde - SUS [13]. A diferença entre as plataformas reside especialmente no algoritmo de consenso usado. A principal motivação desta pesquisa é a condição de que o SUS tem um gerenciamento ainda pouco efetivo de PMEs, como explicado a seguir. A eficiência (rapidez de processamento de transações) não é adequada, pois as bases de dados individuais não estão integradas. A segurança (tríade: disponibilidade, integridade e confidencialidade [10, 14, 15]) não é apropriada, dado que: (i) a disponibilidade das informações (acessível sempre que necessário) é limitada, pois o compartilhamento de dados entre as USs é restrito; (ii) a integridade das informações (confiável e imutável) não é garantida, pois pode haver inconsistência entre os dados das USs; por fim, (iii) a confidencialidade das informações (visível apenas para participantes autorizados) não é assegurada, pois são empregadas usualmente senhas simples para acesso aos PMEs. Além disso, o paciente não controla seus próprios dados, contrariando a Lei Geral de Proteção de Dados Pessoais - LGPD [16].

A análise comparativa realizada nesta pesquisa é feita por meio de discussão teórica e modelagem analítica baseada em sistemas de filas, com foco nos requisitos de eficiência e segurança. Nesse sentido, a principal contribuição deste trabalho se materializa pela oferta à literatura de valiosos subsídios teóricos e experimentos sob um viés de comparação, o que redunda na complementação de trabalhos anteriores da literatura e, portanto, colabora para o desenvolvimento profícuo de projetos reais de bases de dados sob a tecnologia Blockchain.

O restante deste artigo é organizado como segue. A Seção 2 discorre sobre o projeto genérico de uma plataforma baseada na tecnologia Blockchain. A Seção 3 aborda trabalhos relacionados. Na Seção 4, tem-se a explicação das duas plataformas analisadas nesta pesquisa. A Seção 5 traz a avaliação de desempenho sob viés de comparação. Por fim, conclusões finais e trabalhos futuros constituem a Seção 6.

2. Projeto de Plataforma Baseada em Blockchain

O projeto de uma plataforma baseada na tecnologia Blockchain pressupõe três importantes questões: participantes, permissão de uso, e arquitetura. Os participantes podem ser categorizados como *simples*, *validador* ou *minerador* [11]. *Simples* é aquele participante que utiliza o sistema apenas para realizar transações, aqui também denominado de *ator*. *Validador* é aquele participante que pode realizar e, também, validar transações. Neste caso, o participante tem localmente uma réplica da lista de blocos. Por fim, *minerador* é aquele participante que, além de realizar/validar transações e possuir uma réplica da lista, também pode criar e validar blocos de transações.

Sobre a permissão de uso, o sistema pode ser *não permissionado* ou *permissionado* [17]. No primeiro tipo, também chamado de público, o sistema é aberto para participação. Neste caso, o participante pode exercer o papel de *simples*, *validador* ou *minerador*, e os dados armazenados são visíveis a todos os participantes. No segundo tipo, também chamado de privado, a participação necessita da anuência de uma autoridade predefinida. Neste caso, a visibilidade dos dados é sujeita a direitos de controle de acesso.

Com respeito à arquitetura [9], há dois aspectos a discutir: físico e lógico. O primeiro diz respeito à infraestrutura física, considerando, e.g., as unidades de armazenamento de dados, a topologia física da rede de *mineração*, e os nós processadores. Em seu turno, o aspecto lógico engloba, e.g., o número de listas encadeadas, a topologia lógica de conexão da rede de *mineração*, e o algoritmo de consenso adotado.

Em particular, o número de listas encadeadas define duas categorias [11]: de *lista única* e de *múltiplas listas*. A primeira é de mais simples concepção, resultando em projetos de maior facilidade de implantação. A segunda permite mais efetivamente atender à confidencialidade de dados quando há

diferentes subgrupos de *atores* no mesmo sistema, à custa de maior complexidade de projeto e *overhead* computacional.

Por sua vez, o algoritmo de consenso inclui as regras para validação e criação de blocos de transações. Neste contexto, há três critérios para a seleção dos *mineradores*, que são os responsáveis por estabelecerem o consenso [17, 11]: *computação intensiva*; *capacidade de recursos*; e *votação*. O primeiro critério diz que o *minerador* é aquele que mais rapidamente resolve problemas matemáticos (e.g., desafios criptográficos). O segundo critério assume que o *minerador* é aquele que detém a maior disponibilidade de algum recurso (e.g., espaço em disco). Finalmente, o terceiro critério admite como *minerador* aquele participante que tem a anuência da maioria dos outros *mineradores* do sistema.

3. Trabalhos Relacionados

Esta seção traz algumas das mais importantes e recentes propostas da literatura relacionadas a sistemas de informação de saúde baseados em Blockchain, evidenciando fulcralmente as características de seus respectivos projetos.

Em [18], os autores propõem um sistema interoperável, o qual permite aos profissionais de saúde compartilhar entre si os dados dos pacientes. Em [19, 20], os autores desenvolvem sistemas para acesso a dados que são habilitados por contratos inteligentes. Esses três trabalhos fazem uso do critério de consenso baseado em *computação intensiva*. Em seu turno, as propostas de [21, 22] apresentam sistemas para gerenciamento de dados usando algoritmos de consenso baseado no critério de *votação*.

Em [23, 24, 25, 26], os autores propõem sistemas que se destacam por permitir que pacientes mantenham a administração primária dos próprios dados, i.e., apenas pacientes têm o direito de fazer a submissão de dados na rede; nesses sistemas, os profissionais de saúde estão, portanto, autorizados apenas para acesso a dados. Em [6, 27, 28, 29, 30], os trabalhos trazem sistemas em que tanto profissionais de saúde como pacientes realizam a submissão de dados habilitados por contratos inteligentes.

Os trabalhos supracitados possuem a característica comum de serem de escopo de aplicação mais geral e não tratarem especificamente do SUS, o que termina dificultando inferências concretas sobre a efetividade alcançada se aplicados ao SUS. Por sua vez, os trabalhos de [31, 32, 12] abordam o SUS, conforme discorrido a seguir.

Em [31], os autores apresentam um sistema que tem o gerenciamento de PMEs executado pelos próprios pacientes do SUS. O sistema, porém, é restrito ao atendimento terapêutico de reabilitação física e neurofuncional. Como característica importante, tem-se que seu desenvolvimento é feito sobre a estrutura Ethereum e é usado um consenso baseado no critério de *computação intensiva*. Em que pese a importância do trabalho para a literatura, não há apresentação de resultados de avaliação de desempenho e, além disso, o projeto está aparentemente em estágio inicial de seu ciclo de vida.

Em [32], os autores trazem uma arquitetura de gerenciamento de PMEs usando a estrutura Hyperledger com multicanais, com critério de consenso baseado em *votação*. As transações são guardadas nas listas encadeadas da Blockchain, enquanto os PMEs ficam armazenados em sistemas externos. Embora a proposta não seja exclusiva para o SUS, os experimentos incluem dados do mesmo para avaliação da escalabilidade em termos de volume de dados armazenados. Assim como na proposta de [31], os pacientes têm participação no gerenciamento de seus PMEs. Apesar de os resultados experimentais serem atrativos, não há avaliação dos requisitos de eficiência e segurança, o que acaba impedindo uma conclusão mais contundente sobre a efetividade da proposta.

Em [12], tem-se a proposta de um sistema específico para o SUS. É feita a descrição de toda a plataforma, que faz uso de consenso baseado no critério de *votação*. Como no trabalho de [32], o armazenamento das transações é feito nas listas encadeadas da Blockchain, enquanto os PMEs são guardados em sistemas externos. Os resultados experimentais são bem promissores e se baseiam na avaliação dos requisitos de eficiência, escalabilidade, segurança e custo de implantação. Todavia, não há experimentos de comparação com plataformas afins, o que cria uma lacuna para investigação da efetividade sob o viés de comparação com outras propostas. Neste contexto, menciona-se que uma das plataformas analisadas neste trabalho é a própria proposta de [12], conforme explicado mais adiante na Seção 4.

Ante os trabalhos mencionados, o ineditismo deste artigo se revela, portanto, pela análise comparativa de duas plataformas específicas para o SUS. Neste sentido, tem-se uma valiosa complementação dos trabalhos anteriores da literatura devido aos novos resultados e conclusões aqui obtidos sob viés de comparação, com base no uso de modelos de filas e em discussões teóricas. Existe, portanto, uma sólida contribuição para alicerçar o caminho para o desenvolvimento profícuo de projetos reais sob a tecnologia Blockchain.

4. Plataformas sob Análise

Esta seção explica as duas plataformas analisadas neste trabalho. A primeira plataforma, denominada de Plataforma I, é a mesma apresentada originalmente em [12]. Essa plataforma possui um consenso baseado no critério de *votação* e sua escolha deve-se ao seguinte: (i) é uma proposta bem recente; (ii) apresenta resultados teóricos e experimentais promissores; (iii) é inspirada a partir de reconhecidos trabalhos da literatura (e.g., [11, 17, 33]). Em seu turno, a segunda plataforma, denominada de Plataforma II, é inédita e emprega um algoritmo de consenso baseado no critério de *computação intensiva* [11, 17]. A inspiração para esta proposta também está em trabalhos anteriores da literatura, em que são realizadas discussões teóricas e experimentos de validação (e.g., [9, 17, 4, 34]).

Para fins de organização e facilidade de entendimento, o restante desta seção está dividido em duas subseções, como descrito a seguir. Na Subseção 4.1, discute-se a organização

conceitual das plataformas e as operações então permitidas. Na Subseção 4.2, são explicadas questões de projeto das plataformas e as modelagens analíticas concebidas para fins da realização dos experimentos.

4.1 Organização Conceitual e Operações

As Plataformas I e II têm a mesma organização conceitual e o mesmo conjunto de operações definidos originalmente em [12], que são sucintamente revisados na sequência. A justificativa para tanto é garantir uma análise comparativa justa, pois ambas plataformas ficam, assim, imersas no mesmo cenário de avaliação.

Como ilustrado na Figura 1, a organização conceitual pressupõe três componentes: o primeiro é a US; o segundo é a rede de *mineração*; e o terceiro é a base de dados. O primeiro componente se conecta aos segundo e terceiro componentes por meio de uma rede de acesso (rede de comunicação de dados, e.g., Internet). Não há comunicação direta entre os segundo e terceiro componentes.

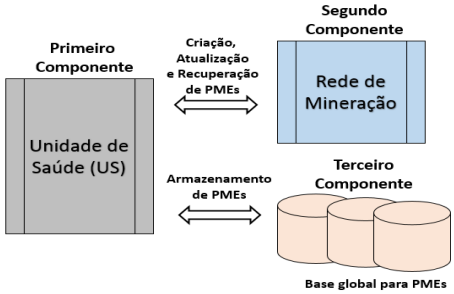

Figura 1. Organização conceitual das plataformas.

O primeiro componente existe em igual número ao total de USs no Brasil. Cada US opera como um participante simples, sob administração da Secretaria de Saúde do município do Brasil onde está localizada. O segundo componente é único, formado por *mineradores*. Sua finalidade é a criação e a validação de blocos de transações (geradas pelas USs). O número de *mineradores* existentes nesse componente é igual ao número de unidades federativas do Brasil. O terceiro componente constitui-se em um armazenamento externo e, também, é único. Sua finalidade é armazenar os PMEs. Os segundo e terceiro componentes são administrados pelo Ministério da Saúde do Brasil. Os componentes se comunicam segundo as quatro operações descritas na Tabela 1.

4.2 Questões de Projeto e Modelagem Analítica

A Tabela 2 informa sobre as questões de projeto e o modelo analítico da rede de *mineração* nas duas plataformas. Como pode ser visto nessa tabela, a diferenciação entre as plataformas reside apenas nos aspectos lógicos e no modelo analítico, os quais são explicados a seguir.

1) Plataforma I

Com respeito aos aspectos lógicos, tem-se o seguinte. O algoritmo de consenso da rede de *mineração* é o *Practical Byzantine Fault Tolerance* – PBFT [35], que é baseado no critério de *votação*. A operação do PBFT ocorre da seguinte forma. A rede de *mineração* tem topologia lógica de um grafo conexo $G = (V, A)$, com $|V| = n$ e $|A| \leq n^2$. Cada nó de G é um *minerador*, e cada aresta é um enlace de comunicação. Um *minerador* é escolhido dentre os n possíveis de forma circular. Se todos os *mineradores* estiverem ocupados, então as transações que chegam são colocadas em espera. As transações recebidas são eventualmente validadas e blocos vão sendo criados.

A criação de um bloco consiste na organização das informações nele contidas (i.e., transações e metadados pertinentes). Após sua criação, o bloco é enviado para os demais *mineradores*. Ao receber um bloco, cada *minerador* verifica as transações nele contidas, calcula o *hash* do bloco, e envia esse *hash* para os demais *mineradores*. Cada *minerador*, que já tenha recebido o bloco, atualiza sua cópia local da lista encadeada se receber o mesmo valor de *hash* desse bloco de, ao menos, $2/3$ dos n *mineradores*. Isso resulta na convergência da base de dados na visão lógica de uma lista única de blocos.

Sobre a modelagem analítica, tem-se o seguinte. Para avaliação de eficiência e disponibilidade da plataforma, mede-se o tempo de resposta, T_R, definido como o intervalo de tempo desde o envio da transação até o recebimento da resposta, medido no primeiro componente da arquitetura (Figura 1). Ressalta-se que o tempo para armazenamento/recuperação de PMEs no terceiro componente não é considerado nesta modelagem, a qual está relacionada à rede de *mineração*, conforme já informado; ademais, note que este tempo independe da tecnologia Blockchain e pode ser assumido, se desejado, como um valor constante adicional em ambas plataformas sob análise.

O valor de T_R é então calculado na Equação 1, onde: T_{AT} é o atraso de transmissão da transação do primeiro componente para o segundo componente; T_{AR} é o atraso de transmissão da resposta do segundo componente para o primeiro componente; e T_P é o tempo de processamento (i.e., validação de transações, criação do bloco, e troca de mensagens na rede de *mineração*) no segundo componente.

$$T_R = T_{AT} + T_{AR} + T_P \tag{1}$$

Os atrasos de propagação na plataforma são desprezados nesta modelagem (sendo sua discussão deixada para trabalhos futuros, em que serão consideradas as distâncias geográficas dos enlaces de comunicação), e $T_{AT} = T_{AR} = D/U$, onde: D é o tamanho da transação; U é a capacidade de transmissão de dados dos enlaces de comunicação entre os componentes. Para o cálculo de T_P, admite-se a visão do *minerador* escolhido, doravante chamado de *líder*. Ao início, o grau do *líder* é $2n/3$, que é o valor mínimo de mensagens de confirmação para adição do bloco à lista encadeada sob PBFT [35]. Se um vizinho do *líder* se torna inalcançável por alguma razão (e.g., ataque de negação de serviço, interrupção do enlace de comunicação, etc.), o grau do *líder* diminui em 1, e a topologia de análise muda: um vizinho é adicionado a um dos vizinhos do *líder* ainda alcançáveis. A partir daí, quando um vizinho do

Tabela 1. Descrição das operações

Operação	Descrição
Criação	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, o segundo componente 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* de PME.
Atualização	Esta operação é semelhante à operação de *Criação*. A diferença é que *Criação* trata sobre a primeira visita do paciente, enquanto que *Atualização* se refere às visitas subsequentes. Ambas operações adicionam informações à base de dados no terceiro componente, e são auditáveis a partir da lista de blocos armazenada no segundo componente.
Recuperação	O primeiro componente envia ao segundo componente uma transação. Esta transação possui 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 em atendimento. O primeiro componente então envia ao terceiro componente o *hash* do PME, junto com a chave pública do paciente. Por fim, após confirmada a integridade do PME, o terceiro componente envia uma cópia do PME ao primeiro componente.
Armazenamento	Esta operação ocorre ao final das operações de *Criação* e de *Atualização*. Porém, para ter-se maior celeridade, também é permitido o seguinte. Quando o PME é criado/atualizado no primeiro componente, seu armazenamento é feito imediatamente no terceiro componente sob o estado de *temporário*. Depois da criação e validação do bloco correspondente, o estado passa então a *permanente*.

Tabela 2. Caracterização das plataformas

Item	Plataforma I	Plataforma II
Permissão de uso	*Permissionado* (privado)	*Permissionado* (privado)
Armazenamento	Externo (nuvem)	Externo (nuvem)
Participantes	*Simples* e *minerador*.	*Simples* e *minerador*.
Aspectos físicos	Rede de *mineração* de topologia P2P; parâmetros da rede de acesso na Tabela 3.	Rede de *mineração* de topologia P2P; parâmetros da rede de acesso na Tabela 3.
Aspectos lógicos	Consenso PBFT; rede de *mineração* de topologia em malha (grafo conexo); lista única.	Consenso PoW; rede de *mineração* de topologia barramento; lista única.
Modelo analítico da rede de *mineração*	Sistema de fila $M/E_k/1/\infty/FIFO$	Sistema de fila $M/M/c/\infty/FIFO$

líder se torna inalcançável, o grau do *líder* diminui em 1, e um vizinho é adicionado ao último vizinho adicionado, formando uma cadeia de nós. Se o número de vizinhos inalcançáveis atinge $(2n/3)$–1, tem-se então o cenário menos eficiente de operação.

Ante o exposto, assume-se então T_P dado pelo tempo de resposta de um sistema de fila, T_{fila}, somado aos atrasos de transmissão de mensagens na rede de *mineração*. O sistema de fila é do tipo $M/E_k/1/\infty/FIFO$ [36, 37], ilustrado na Figura 2. A chegada de blocos segue um processo de Poisson de taxa λ, e o tempo de serviço tem distribuição Erlang com parâmetros $1/(k\mu)$ e k, sendo que: $1/(k\mu)$ é o tempo médio de cada estágio; $k = i+2$; i é o número de vizinhos inalcançáveis pelo *líder*; e $1/\mu$ é o tempo médio de processamento de um bloco (i.e., validação de transações e criação do bloco) sob consenso PBFT [35].

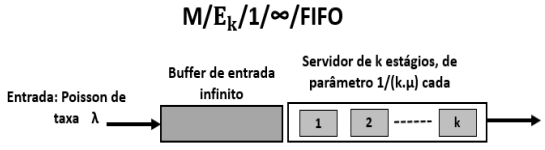

Figura 2. Sistema de fila do tipo $M/E_k/1/\infty/FIFO$.

Daí, a Equação 1 pode ser reescrita na forma da Equação 2, onde: $T_{AB} = B/C$ é o atraso de transmissão do bloco, sendo B o tamanho do bloco, e C a capacidade de transmissão dos enlaces de comunicação entre os *mineradores* do segundo componente; $T_{AH} = H/C$ é o atraso de transmissão do *hash* do bloco, sendo H o tamanho do *hash*. Nesta modelagem, T_{fila} pode ser calculado pela Equação 3 [36, 37], onde: L_{buf} é o número de transações esperando no *buffer* de entrada,

calculada na Equação 4; e $\rho = \lambda/\mu < 1$ (i.e., sistema estável) é a taxa de ocupação. Por fim, a Tabela 3 traz uma síntese dos principais parâmetros utilizados na derivação de T_R sob consenso PBFT.

$$T_R = T_{AT} + T_{AR} + T_{fila} + (i+1)T_{AB} + (\sum_{j=0}^{i}(j+1))T_{AH} \quad (2)$$

$$T_{fila} = \frac{L_{buf}}{\lambda} + \frac{1}{\mu} \quad (3)$$

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

2) Plataforma II

Para esta plataforma, tem-se o emprego do algoritmo de consenso *Proof of Work* – PoW [42]. Esse algoritmo é baseado no critério de *computação intensiva*, destacando-se por ser um dos mais resistentes a fraudes na lista encadeada. Ademais, quanto maior é o número de *mineradores*, menor é a probabilidade de fraudes [9].

Como sob PBFT, a rede de *mineração* sob PoW também possui *n mineradores*. Porém, sob PoW, a rede possui uma topologia em barramento: as transações chegam a um barramento comum a todos os *n mineradores*. O *minerador* que trata as transações é escolhido aleatoriamente. Se todos os *mineradores* estiverem ocupados, então as transações ficam em espera. As transações recebidas são eventualmente validadas e blocos são criados.

Todavia, diferentemente da rede sob PBFT, a criação de um bloco sob PoW inclui, além da simples organização de informações, a solução de um complexo desafio criptográfico, que deve ser obtida em um intervalo de tempo predefinido [12]. O bloco e a solução do desafio são então enviados para todos os demais *mineradores* da rede por meio do barramento comum. Ao receber o bloco, cada *minerador* verifica se a solução do desafio está correta e, em caso positivo, atualiza sua cópia local da lista encadeada, promovendo a convergência da base de dados sob a visão lógica de uma lista única de blocos.

De forma análoga à análise sob PBFT, para a avaliação da eficiência e da disponibilidade sob PoW, mede-se o tempo de resposta, T_R, computado na Equação 1. O que difere na formulação final de T_R, calculada anteriormente sob PBFT, é exclusivamente a derivação do valor de T_P e os atrasos de transmissão de mensagens na rede de *mineração*, como explicado a seguir.

Para conformidade com a operação descrita acima para PoW, assume-se T_P obtido de uma fila $M/M/c/\infty/FIFO$ [36, 37], ilustrada na Figura 3. O processo de chegada se refere a blocos de transações. Esse processo é caracterizado como um processo de Poisson de taxa γ. O serviço é realizado por c servidores independentes, cujos tempos de serviço individuais são idênticos, possuindo cada um deles distribuição exponencial de parâmetro α. Ademais, seja m o número de blocos no sistema (i.e., no *buffer* e em serviço). A taxa de serviço é então $m.\alpha$ (para $0 \leq m < c$) ou $c.\alpha$ (para $m \geq c$), onde: $1/\alpha$ é o tempo médio de processamento de um bloco (i.e., validação de transações e criação do bloco) sob consenso PoW; e $c = n$.

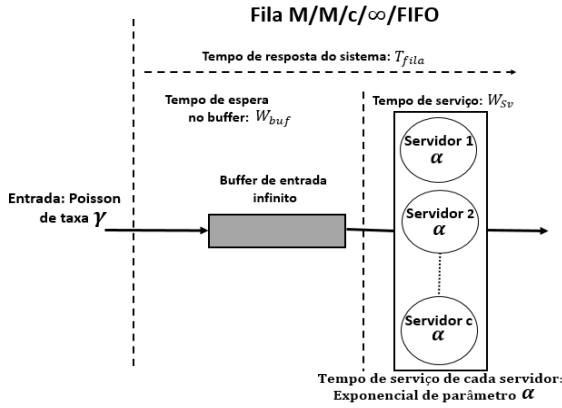

Figura 3. Sistema de filas do tipo $M/M/c/\infty/FIFO$.

Assim, T_P é estimado pelo tempo de resposta, T_{fila}, calculado na Equação 5 [36, 37], onde: W_{buf} é o tempo de espera no *buffer*; W_{Sv} é o tempo de serviço; e N_{buf} é o número de blocos no *buffer* (i.e., aguardando serviço). Em seu turno, o valor de N_{buf} é calculado na Equação 6, onde: $r = \gamma/\alpha$; $\beta = r/c < 1$ (i.e., sistema estável); e P_0 é a probabilidade de não haver blocos no sistema, calculada na Equação 7.

$$T_{fila} = W_{buf} + W_{Sv} = \frac{N_{buf}}{\gamma} + \frac{1}{\alpha} \quad (5)$$

$$N_{buf} = \frac{P_0.r^c}{c!} \cdot \frac{\beta}{(1-\beta)^2} \quad (6)$$

$$P_0 = \frac{1}{\sum_{j=0}^{c-1} \frac{r^j}{j!} + \frac{r^c}{c!(1-\beta)}} \quad (7)$$

Diante do exposto, a Equação 1 é reescrita na forma da Equação 8, onde: T_{AT}, T_{AR} e T_{AB} são calculados como feito na Equação 2, e T_{fila} é dado pela Equação 5. Comparando-se as expressões finais de T_R sob PoW e PBFT, respectivamente, tem-se o seguinte: sob PoW, o atraso de transmissão de bloco na rede de *mineração*, T_{AB}, não é afetado pela indisponibilidade de *mineradores* diferentes daquele que efetivamente *minera* o bloco de transações, pois o bloco de transações *minerado* é sempre enviado diretamente do *minerador* que realizou seu processamento para o primeiro componente (vide Figura 1); e $T_{AH} = 0$, pois não há envio de *hashes* entre *mineradores*. Por fim, na Tabela 3, citada anteriormente, também estão resumidos os principais parâmetros da derivação de T_R, agora sob PoW.

$$T_R = T_{AT} + T_{AR} + T_{fila} + T_{AB} \quad (8)$$

Tabela 3. Síntese dos 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.
D	250 B	Tamanho da transação. A transação é constituída ao menos de: chave pública do paciente (32 B); chave pública do atendente (32 B); tipo de operação e metadados (186 B) [31, 32, 12].
C	7,25 MB/s	Capacidade de transmissão de dados dos enlaces de comunicação entre os *mineradores*. Tem por base estimativas da velocidade de conexão da Internet nas cinco regiões do Brasil [38].
U	2,58 MB/s	Capacidade de transmissão de dados do primeiro componente para o segundo componente da arquitetura. Como no caso do parâmetro C, tem por base estimativas da velocidade de conexão da Internet nas cinco regiões do Brasil [38].
B	2,50 MB	Tamanho do bloco de transações. Assume-se que o bloco contém 10.000 (60.000) transações sob PBFT (PoW), além de metadados pertinentes [35, 9].
n	27	Número de *mineradores* do segundo componente da arquitetura. É estimado pelo número de unidades federativas do Brasil.
λ e γ	variável	Taxa de entrada de blocos no segundo componente da arquitetura (sob PBFT e PoW, respectivamente), medida em blocos por segundo (BPS). É estimada com base na taxa de entrada de transações no segundo componente, ϕ, e no tamanho do bloco de transações, medido em número de transações.
ϕ	variável	Taxa de entrada de transações no segundo componente da arquitetura, medida em transações por segundo (TPS). É estimada com base em projeções da taxa média de visitas de pacientes ao SUS [39] e em projeções do tamanho da população brasileira [40].
$1/\mu$	4 seg	Tempo médio de processamento de um bloco de transações sob consenso PBFT [35].
$1/\alpha$	4 min	Tempo médio de processamento de um bloco de transações sob consenso PoW [41, 9].
k	$i+2$	Número de estágios da distribuição de Erlang na Plataforma I, onde i é o número de *mineradores* inalcançáveis pelo *líder*.
R	25,86 MB	Tamanho do PME. Assume-se que PME é constituído de imagens, filmes e textos [31, 32, 12, 5].
H	32 B	Tamanho do *hash* do bloco. O algoritmo de *hash* utilizado é o conhecido SHA-256.

5. Avaliação de Desempenho

Esta seção faz a avaliação de desempenho das Plataformas I e II, com base nas equações apresentadas na seção anterior e no embasamento teórico da própria tecnologia Blockchain.

A Figura 4 apresenta T_R em função da taxa ϕ, definida na Tabela 3. O intervalo de valores de ϕ abrange o período do ano de 2021 (i.e., $\phi = 45,53$ TPS) até o ano de 2030 (i.e., $\phi = 48,71$ TPS). Em comparação à Plataforma II, a Plataforma I possui valores de T_R sempre bem menores, alcançando uma redução comparativa de até 98,17%. Isso evidencia a maior eficiência da Plataforma I. Ademais, sob o ponto de vista de aplicação prática, é possível conjecturar que a Plataforma I tem um tempo de resposta dentro de uma tolerância aceitável (i.e, $T_R < 4,5$ seg) para serviços usuais de atendimento de pacientes no SUS [13], enquanto a Plataforma II pode vir a se tornar inadequada (i.e., $T_R > 240,0$ seg). Sobre a pouca variabilidade de T_R em cada uma das plataformas, tem-se a justificativa de que a taxa ϕ não aumenta o suficiente para impactar o tempo de processamento dos blocos de transações, tampouco os atrasos de transmissão.

As Figuras 5 e 6 trazem novamente T_R em função da taxa ϕ. Mas, desta vez, são considerados diferentes percentuais de inalcançabilidade de *mineradores*. O intuito é avaliar a disponibilidade do sistema. A Plataforma I é notadamente bem impactada: a variação da inalcançabilidade de 10–50% leva a um aumento de 23,8–209,3% em T_R, implicando a necessidade de *mineradores* de contingência. Diferentemente, a Plataforma II tem significativa resiliência, pois T_R não é

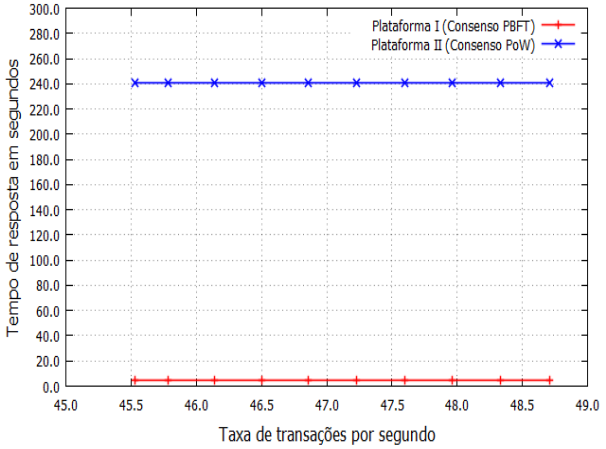

Figura 4. Análise de eficiência.

impactado: os valores de T_R estão sobrepostos, mesmo com 50% de inalcançabilidade. Decorre então que T_R somente seria afetado se a taxa ϕ e/ou o percentual de indisponibilidade de *mineradores* estivessem em patamares de valores acima daqueles que foram investigados. Portanto, sob o requisito de disponibilidade, a Plataforma II é superior à Plataforma I.

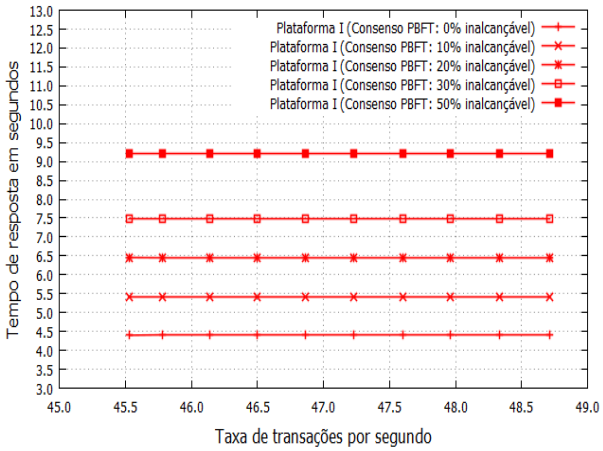

Figura 5. Análise de disponibilidade na Plataforma I.

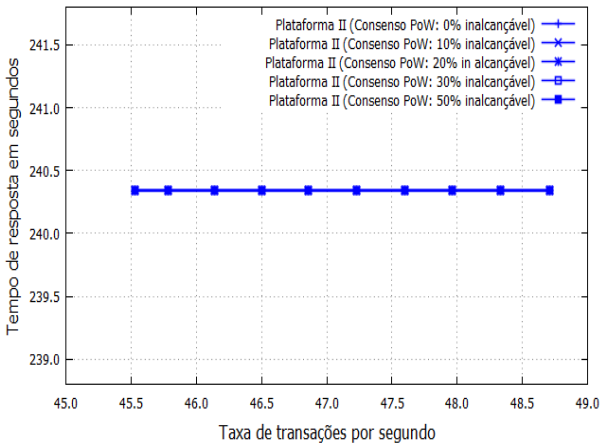

Figura 6. Análise de disponibilidade na Plataforma II.

Sobre a integridade e a confidencialidade, tem-se o seguinte. Ambos requisitos são adequadamente atendidos pela própria concepção teórica da Blockchain nas duas plataformas. Mais precisamente, o atributo sistêmico da imutabilidade garante a integridade, pois, como já mencionado, qualquer mudança em um bloco implica a alteração de todos os blocos subsequentes, o que resulta em uma tarefa computacionalmente difícil. Em seu turno, a confidencialidade pode ser assegurada pela combinação do atributo sistêmico do pseudoanonimato com a possibilidade da cifração das informações com a chave pública do paciente. Neste caso, para leitura dos dados cifrados, o paciente precisa antes conceder autorização por meio de sua chave privada, e.g., inserindo-a no sistema durante a realização de cada atendimento e/ou quando se fizer necessário. O paciente passa, portanto, a ter pleno controle sobre seus próprios dados, em consonância com a LGPD [16].

Ante os resultados obtidos, tem-se então que as Plataformas I e II atendem adequada e igualmente aos requisitos de integridade e confidencialidade. Todavia, a Plataforma I se torna a escolha mais indicada quando o requisito de eficiência é mais importante que o requisito de disponibilidade para o gerenciamento dos PMEs, enquanto que a Plataforma II é a mais indicada em caso contrário.

6. Conclusões e Trabalhos Futuros

Este artigo analisou comparativamente duas plataformas baseadas em Blockchain para o gerenciamento de PMEs do SUS. Por meio de modelos de filas e discussões teóricas, as duas plataformas foram examinadas com foco nos requisitos de eficiência, disponibilidade, integridade e confidencialidade.

Os resultados obtidos mostraram que a plataforma com algoritmo de consenso baseado em *votação* se mostrou mais eficiente, porém menos resiliente à inalcançabilidade de *mineradores*, que a outra com algoritmo de consenso baseado em *computação intensiva*. Ambas plataformas, no entanto, foram capazes de atender adequada e igualmente aos requisitos de integridade e confidencialidade de dados. Assim, a opção por uma plataforma em vez da outra depende da maior prioridade do requisito de operação a ser considerado: eficiência ou disponibilidade. Ainda, como fruto deste trabalho de pesquisa, tem-se que a metodologia baseada em modelos de filas utilizada nos experimentos pode servir como referencial de estudo para construção de novos modelos analíticos, visando avaliar outras plataformas baseadas em Blockchain.

Finalmente, como trabalhos futuros e cientes das limitações desta pesquisa, sugerem-se: (i) análise de plataformas com algoritmo de consenso baseado em *computação intensiva*, buscando obter adequada eficiência de processamento em aplicações de saúde. Para tanto, pode-se experimentar, e.g., diminuir a complexidade do desafio criptográfico e aumentar o número de *mineradores* da plataforma; (ii) propor e analisar alternativas de plataformas com duplo consenso. Por exemplo, para sistemas de saúde podem ser considerados dois tipos de atendimento: emergência e ambulatório. No primeiro, adota-se um consenso baseado em *votação* (para priorizar eficiência) e, no segundo, usa-se um consenso baseado em *computação intensiva* (para priorizar disponibilidade); e (iii) descrever um modelo de ameaças para identificar/tratar vulnerabilidades sistêmicas [43, 44], além de realizar simulações e/ou medições para ratificação dos resultados aqui obtidos e discutidos sobre os requisitos de eficiência e segurança.

Contribuição do autor

Carlo Kleber da Silva Rodrigues: Concepção e elaboração da pesquisa; Realização dos experimentos; Análise e interpretação dos resultados; Redação do manuscrito.

Referências

[1] CHELLADURAI, M. U.; PANDIAN, D. S.; RAMASAMY, D. K. A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. *Health Policy and Technology*, v. 10, n. 4, p. 100513, 2021. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S2211883721000368⟩.

[2] BUTT, N.; SHAN, J. CyberCare: A Novel Electronic Health Record Management System. In: *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. [s.n.], 2016. p. 326–327. Disponível em: ⟨https://doi.org/10.1109/CHASE.2016.52⟩.

[3] AZHAGIRI, M. et al. Secured Electronic Health Record Management System. In: *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*. [s.n.], 2018. p. 915–919. Disponível em: ⟨https://doi.org/10.1109/CESYS.2018.8724010⟩.

[4] ZAABAR, B. et al. HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, v. 200, p. 108500, 2021. ISSN 1389-1286. Disponível em: ⟨https://www.sciencedirect.com/science/article/pii/S1389128621004382⟩.

[5] ISMAIL, L.; MATERWALA, H. Blockchain paradigm for healthcare: Performance evaluation. *Symmetry*, v. 12, n. 8, p. 1–19, julho 2020.

[6] CERCHIONE, R. et al. Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation*, p. 102480–102496, fevereiro 2022.

[7] RAJADEVI, R. et al. Secured Storing and Sharing of Medical Records Based on Blockchain. In: *2022 International Conference on Computer Communication and Informatics (ICCCI)*. [s.n.], 2022. p. 1–5. Disponível em: ⟨https://doi.org/10.1109/ICCCI54379.2022.9741070⟩.

[8] NAKAMOTO, S. *Bitcoin: A peer-to-peer electronic cash system*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 6 de junho de 2022.

[9] RODRIGUES, C. K. da S. Analyzing Blockchain integrated architectures for effective handling of IoT-ecosystem transactions. *Computer Networks*, v. 201, p. 1–12, dezembro 2021.

[10] MINOLI, D.; OCCHIOGROSSO, B. Blockchain mechanisms for IoT security. *Internet of Things*, v. 1-2, p. 1 – 13, setembro 2018.

[11] ISMAIL, L.; MATERWALA, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry*, v. 11, n. 10, p. 1–47, setembro 2019.

[12] RODRIGUES, C. K. da S. Blockchain-Based Platform for Managing Patients' Data in the Public Healthcare System of Brazil . *Revista de Sistemas e Computação (RSC)*, v. 11, n. 3, p. 63–72, dezembro 2021.

[13] FIOCRUZ. *O SUS do Brasil*. 2021. Disponível em: <https://pensesus.fiocruz.br/sus>. Acesso em: 18 de junho de 2022.

[14] ZHANG, K.; JACOBSEN, H. Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. In: *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. [S.l.]: IEEE, 2018. p. 1337–1346.

[15] TAYLOR, P. J. et al. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, v. 6, n. 2, p. 147–156, maio 2020.

[16] Presidência da República do Brasil. *Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei Nº 13.709, de 14 de agosto de 2018*. 2018. Disponível em: <http://www4.planalto.gov.br/legislacao/>. Acesso em: 18 de junho de 2022.

[17] OYINLOYE, D. P. et al. Blockchain Consensus: An Overview of Alternative Protocols. *Symmetry*, v. 13, n. 8, p. 1–35, julho 2021.

[18] AZARIA, A. et al. MedRec: Using Blockchain for Medical Data Access and Permission Management. In: *2016 2nd International Conference on Open and Big Data (OBD)*. [S.l.]: IEEE, 2016. p. 25–30.

[19] DAGHER, G. G. et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, v. 39, p. 283–297, maio 2018.

[20] LI, H. et al. Blockchain-based data preservation system for medical data. *Journal of Medical Systems*, v. 42, n. 141, p. 1–13, junho 2018.

[21] ZGHAIBEH, M. et al. SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities. *IEEE Access*, v. 8, p. 70030–70043, abril 2020.

[22] FAN, K. et al. Medblock: Efficient and secure medical data sharing via blockchain. *Jounal of Medical Systems*, v. 42, n. 8, p. 1–11, junho 2018.

[23] DEY, T. et al. HealthSense: A medical use case of Internet of Things and blockchain. In: *2017 International Conference on Intelligent Sustainable Systems (ICISS)*. Palladam, Índia: IEEE, 2017. p. 486–491.

[24] YUE, X. et al. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *Jounal of Medical Systems*, v. 40, n. 10, p. 1–8, agosto 2016.

[25] TANWAR, S.; PAREKH, K.; EVANS, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, v. 50, p. 1–13, fevereiro 2020.

[26] ASWIN, A. et al. Design of AYUSH: A Blockchain-Based Health Record Management System. In: *Inventive Communication and Computational Technologies*. Singapore: Springer, 2020, (Lecture Notes in Networks and Systems, v. 89). p. 665–672. Disponível em: ⟨https://doi.org/10.1007/978-981-15-0146-3_62⟩.

[27] UDDIN, M. A. et al. Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture. *IEEE Access*, v. 6, p. 32700–32726, julho 2018.

[28] WANG, S. et al. Blockchain-powered parallel healthcare systems based on the acp approach. *IEEE Transactions on Computational Social Systems*, v. 5, n. 4, p. 942–950, dezembro 2018.

[29] KAUR, H. et al. A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. *Journal of Medical Systems*, v. 42, n. 8, p. 1–11, julho 2018.

[30] ROEHRS, A.; COSTA, C.; RIGHI, R. OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, v. 71, p. 70–81, julho 2017.

[31] VIANA, C. et al. Blockchain para gerenciamento de prontuários eletrônicos. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informação*, v. 1, n. 28, p. 177–187, abril 2020.

[32] FERNANDES, A. et al. Scalable Architecture for sharing EHR using the Hyperledger Blockchain. In: *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*. [S.l.]: IEEE, 2020. p. 130–138.

[33] FERDOUS, M. S.; CHOWDHURY, M. J. M.; HOQUE, M. A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, v. 182, p. 1–28, maio 2021.

[34] FAN, C. et al. Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access*, v. 8, p. 126927–126950, julho 2020.

[35] GORKEY, I. et al. *Comparative Study of Byzantine Fault Tolerant Consensus Algorithms on Permissioned Blockchains*. 2020. Disponível em: <http://resolver.tudelft.nl/uuid:01083a4a-900b-4cf9-9746-cb9258c11d9e>. Acesso em: 9 de março de 2022.

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

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

[38] BRANCO, D. C. *Pesquisa mostra qual estado tem maior velocidade de internet do Brasil*. 2021. Disponível em: <https://canaltech.com.br/internet/>. Acesso em: 9 de março de 2022.

[39] Ministério da Sáude do Brasil. *Relatório de Gestão 2018*. 2018. Disponível em: <https://bvsms.saude.gov.br/>. Acesso em: 9 de março de 2022.

[40] Worldometer. *Brazil Population*. 2021. Disponível em: <https://www.worldometers.info/world-population/brazil-population/>. Acesso em: 9 de março de 2022.

[41] BOWDEN, R. et al. *Block arrivals in the Bitcoin blockchain*. 2018. Disponível em: <https://arxiv.org/abs/1801.07447>. Acesso em: 9 de março de 2022.

[42] GERVAIS, A. et al. On the Security and Performance of Proof of Work Blockchains. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Nova York, NY, EUA: Association for Computing Machinery, 2016. p. 3–16.

[43] OTOUM, S.; RIDHAWI, I. A.; MOUFTAH, H. Securing Critical IoT Infrastructures With Blockchain-Supported Federated Learning. *IEEE Internet of Things Journal*, v. 9, n. 4, p. 2592–2601, fevereiro 2022.

[44] TATAM, M. et al. A review of threat modelling approaches for APT-style attacks. *Heliyon*, v. 7, n. 1, p. 1–19, 2021.