risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 15/11/2022
Aceitação/Acceptance: 20/02/2023

Proposta de um Algoritmo de Consenso para Plataformas *Blockchain* em Sistemas de Gestão de Saúde Privados

Fabricio Rodrigues Freire[1], William Ferreira Giozza[2], Carlo Kleber da Silva Rodrigues[3]

fabricio.freire@redes.unb.br; giozza@unb.br; carlo.kleber@ufabc.edu.br

[1] Programa de pós-Graduação Profissional em Engenharia Elétrica (PPEE), Universidade de Brasília (UnB), Brasília - DF, Brasil

[2] Departamento de Engenharia Elétrica, UnB, Brasília - DF, Brasil

[3] Centro de Matemática, Computação e Cognição, Universidade Federal do ABC (UFABC), Santo André - SP, Brasil

Pages: 103-116

Resumo: Os registros médico-hospitalares relacionados aos pacientes e geridos por sistemas de gestão de saúde necessitam da implementação de controles que garantam a privacidade e segurança das informações. Neste contexto, diversos estudos apontam para viabilidade no emprego de tecnologias como *Blockchain* para o provimento de soluções que vão desde o controle de suprimentos médicos à gerência dos dados de pacientes. A tecnologia *Blockchain* possui diversos elementos para garantia dos requisitos necessários a sistemas de gestão de saúde, e um deles é o algoritmo para consenso entre os participantes da rede. Este artigo propõe um algoritmo de consenso baseado em votação e tolerante a falhas bizantinas aplicado a sistemas de gestão de saúde privados. Essa proposta é resultado de um estudo teórico envolvendo uma análise crítica sobre os requisitos necessários para a implementação de sistemas de gestão da saúde baseados em plataformas *Blockchain* privadas. Por fim, conclusões gerais e sugestões para trabalhos futuros encerram este artigo.

Palavras-chave: *Blockchain*; Algoritmos de Consenso; Sistemas de Gestão de Saúde; Segurança da Informação.

Blockchain Consensus Algorithm Proposal for Healthcare Management Systems

Abstract: Medical-hospital records related to patients and managed by health management systems require the implementation of controls that provide the privacy and security of information. In this context, many studies report to the feasibility of using technologies such as Blockchain to provide solutions ranging from the control of medical supplies to the management of patient data. Blockchain technology has many elements to guarantee the necessary requirements for health management systems, and one of them is the algorithm for consensus among

network participants. This article proposes a based-voting-and-byzantine-fault-tolerant consensus algorithm intended for application in private health systems. This proposal results from a theoretical study concerning the main requirements for the implementation of Blockchain platforms for private health systems. Finally, general conclusions and suggestions for future work close this article.

Keywords: Blockchain, Consensus Algorithm, Healthcare Management Systems, Information Security.

1. Introdução

Sistemas dedicados à gestão das informações médico-hospitalares advindas de pacientes devem fornecer condições para o armazenamento e análise dos registros, além de proverem subsídios para a definição de um tratamento mais adequado às suas condições sanitárias (Huru *et al,* 2022; Adere, 2022; Ismail & Materwala, 2020). Esses sistemas de gestão de saúde foram ganhando complexidade ao longo do tempo (Reibling et al, 2019; Dabbagh, 2021). Além da necessidade de garantir integridade, confidencialidade e disponibilidade nos prontuários médicos, esse tipo de sistema deve prover um processamento eficiente em razão do grande volume de dados gerado (Kaur, 2018).

Uma tecnologia de segurança da informação bastante promissora para a implementação de sistemas de gestão das informações médico-hospitalares é a *Blockchain,* que pode ser definida como uma base de dados distribuída onde os registros são armazenados em blocos (Zheng, 2018), embutindo elementos como criptografia, livro-razão (*ledger*) e algoritmo de consenso (Greve *et al*, 2018). Os elementos constituintes da *Blockchain* garantem suas propriedades tais como imutabilidade, integridade, atualidade, transparência, disponibilidade, descentralização e desintermediação (Hasan *et al*, 2022).

O uso da tecnologia *Blockchain* em sistemas para gestão da saúde permite por exemplo a implantação de mecanismos para a rastreabilidade e o controle de entrada e saída de insumos, evitando vultosos desperdícios de recursos (Brasil, 2021). Percebe-se então que os requisitos necessários para implementação de sistemas de gestão de saúde vão ao encontro das características dessa tecnologia (Qahtan, 2022; Sy, 2022; Ghayvat, 2021).

Um dos grandes desafios de sistemas construídos sobre plataformas baseadas em *Blockchain* é a obtenção de um acordo, ou consenso, entre participantes da corrente sobre a validade de um conjunto de transações para garantia da consistência dos registros ali contidos. Esse consenso pode ser alcançado com uma estratégia de comunicação baseada em algoritmos que permitem a partes desconhecidas entre si, que podem ser até adversárias, chegarem a um acordo sobre o estado atual e passado das informações armazenadas na base de dados. Existem dois modelos de decisão de consenso para correntes *Blockchain*: probabilístico para correntes públicas e determinístico para correntes privadas (Rodrigues e Silva, 2019).

No modelo probabilístico usa-se protocolos de consenso baseados em provas como por exemplo a prova de trabalho *(Proof-of-Work* – PoW) (Rodrigues, 2017) onde qualquer nó pode participar do protocolo de consenso e procurar acrescentar blocos, estendendo a corrente de blocos. Nesse modelo de consenso, múltiplas propostas de inserção de novos blocos podem ser feitas concorrentemente e gerar bifurcações na corrente, sendo

necessário aplicar uma regra probabilística onde o ramo da bifurcação mais longo ganha (Cao *et al,* 2020).

No modelo determinístico de decisão de consenso, apenas nós autorizados, conhecidos e identificados, executam um protocolo de consenso e devem votar pela aprovação ou rejeição de um bloco, e atingir um consenso antes de adicionar o novo bloco à corrente (Crain *et al,* 2018). O modelo determinístico permite prover um bom desempenho em termos da vazão de transações, mas apresenta limitações quanto à escalabilidade do número de participantes na corrente *Blockchain*.

Dentre os protocolos de consenso baseados em votação, uma classe particularmente interessante para a implementação de sistemas de gestão da saúde é a dos protocolos tolerantes a falhas bizantinas (*Byzantine Fault Tolerant* - BFT) que garantem a consistência da *Blockchain* sob comportamento malicioso (Qin *et al*, 2022).

Este trabalho tem como objetivo apresentar a proposta de um novo algoritmo de consenso denominado *Byzantine Fault Tolerance to Health* – H-BFT, baseado em votação e tolerante a falhas bizantinas, para compor uma plataforma *Blockchain* que atenda adequadamente aos requisitos dos sistemas de gestão de saúde. Essa proposta resulta de um estudo teórico envolvendo quatro dos principais algoritmos de consenso baseados em votação e tolerantes a falhas bizantinas existentes (*Pratical Byzantine Fault Tolerance* - pBFT, *Federated Byzantine Agreement* - FBA, *Delegated Byzantine Fault Tolerance* - dBFT e PAXOS), onde buscou-se identificar em cada um suas potencialidades e deficiências quando aplicadas ao contexto específico da saúde.

O restante do presente artigo está estruturado da seguinte forma. Na Seção 2 são apresentados os trabalhos relacionados mais relevantes sobre algoritmos de consenso e o emprego da tecnologia *Blockchain* no contexto da saúde. A Seção 3 apresenta um estudo teórico analisando os algoritmos de consenso selecionados e os requisitos de um sistema para gestão da saúde de modo a identificar os principais elementos necessários à especificação de um mecanismo de consenso que possa atender as necessidades existentes no domínio da gestão da saúde. Na Seção 4 é apresentada a proposta do novo algoritmo de consenso H-BFT. Por fim, na Seção 5 são apresentadas as conclusões e direcionamentos para trabalhos futuros.

2. Trabalhos Relacionados

Os dados relacionados a pacientes e médicos são sensíveis e os sistemas que realizam a gestão de saúde necessitam implementar controles que garantam segurança e eficiência exigida a esse domínio informacional. Diversos estudos têm identificado em tecnologias emergentes como *Blockchain*, as características necessárias ao pleno cumprimento desses requisitos de controle (Adere, 2022). Esta Seção apresenta alguns estudos relacionados ao contexto do presente artigo, cujo enfoque são frameworks que empregam *Blockchain* aplicado ao domínio da gestão da saúde, evidenciando a relevância do assunto.

Em (Azbeg, 2022) é proposto o BlockMedCare, um *framework* com foco nos parâmetros segurança, escalabilidade e tempo de processamento, sendo projetado para o suporte ao monitoramento remoto de pacientes. Esse trabalho objetivou resolver o problema da escalabilidade com um banco de dados baseado em *InterPlanetary File System* - IPFS

(Labs P, 2022) e o mecanismo de consenso Clique PoA. Com esse algoritmo buscou-se acelerar o consenso e o consequente armazenamento de dados, uma vez que ele não demanda grandes recursos computacionais.

No *framework* chamado Ancile (Dagher et al, 2018), foram utilizados *Smart Contracts* (SC) para efetuar as operações de Consenso, Classificação, Histórico de Serviço, Propriedade, Permissões e Criptografia. O emprego de SC objetivou uma melhor experiência para o usuário, e a redução de danos à privacidade dos dados. Para tratar a questão do consenso entre os nós da rede, foi escolhido o QuorumChain, que utiliza SC para gerenciar o processo de votação que cada bloco recebe para considerar a validade do mesmo.

Outro *framework* voltado para área médica é definido em (Singh et al, 2022), e utiliza em conjunto as tecnologias IoT, pelo uso de dispositivos para coleta de dados, *Blockchain*, na garantia de compartilhamento seguro dos dados coletados, e *Federated Learning* (FL), para preservação da privacidade, segurança e escalabilidade do sistema. Nesse trabalho, optou-se por um mecanismo de consenso PoW, contudo, chegou-se ao entendimento que era necessário o desenvolvimento de um algoritmo para lidar com os nós do tipo FL.

De forma semelhante é definido o S2HS (Tripathi et al, 2020), um sistema inteligente de saúde que utiliza os recursos de uma arquitetura IoT, agregando os aspectos de segurança da *Blockchain*. Embora estabeleça um modelo robusto para atender as questões relacionadas a temática da saúde, esse trabalho não aborda questões de escalabilidade nem define um algoritmo de consenso para o sistema.

(Bawany et al, 2022) propõe um *framework* denominado BlockHeal, com foco em telemedicina. Foi definido a partir da identificação das fragilidades existentes nesse modelo de comunicação, e procurou explorar características da tecnologia Blockchain, como segurança, tolerância a falhas, transparência e imutabilidade, com uma implementação baseada em *Hyperledger Fabric*, mas não apresenta especificações a respeito do mecanismo de consenso utilizado.

O *framework* hOCBS (Miyachi & Mackey, 2021) é uma proposta para interação de uma *Blockchain* direcionada ao setor da saúde, com recursos *off-chain*, mantendo as características de escalabilidade, menor gasto com armazenamento e melhoria na privacidade dos dados, próprias a esse tipo de sistema, e agregando a recursos da tecnologia *Blockchain*, para montar uma estrutura que garanta um modelo híbrido nesse aspecto.

Em (Rahman *et al,* 2022), há uma especificação de *framework* baseado nas tecnologias *Internet of Medical Things* - IoMT e *Blockchain* sobre uma estrutura de comunicação 5G *Edge*. Esse trabalho buscou estabelecer meios para preservação da privacidade e integridade dos dados, criptografando as informações antes do armazenamento, e apresentou resultados de experimentos que atestaram a viabilidade e eficiência do *framework* proposto.

A Tabela 1 resume os trabalhos avaliados, e é possível observar que a maioria deles traz especificações da arquitetura de um sistema para resolver os problemas inerentes ao tema da gestão da saúde, mas deixa uma lacuna quanto aos critérios para definição dos algoritmos de consenso elencados. Além disso, esses trabalhos estabelecem a

privacidade dos dados médicos como um aspecto preponderante na implementação, não se aprofundando em outras questões que podem ser relevantes, como eficiência e principalmente escalabilidade.

Referência	Aspectos avaliados	Enfoque	Tipo de Algoritmo
(Azbeg, 2022)	*Integridade, privacidade e controle de acesso*	*IoT, Blockchain, Saúde e IPFS*	*Adoção de algoritmo Clique PoA não fundamentada*
(Dagher et al, 2018)	*Privacidade e controle de acesso*	*IoT, Blockchain, Saúde e Smart Contracts*	*Adoção de algoritmo QuorumChain não fundamentada*
(Singh et al, 2022)	*Privacidade, segurança e escalabilidade*	*IoT, Blockchain, Saúde e FL*	*Algoritmo de consenso que envolve gasto computacional*
(Tripathi et al, 2020)	*Confidencialidade e privacidade*	*IoT, Blockchain e Saúde*	*Não definição de um algoritmo para a proposta, e direcionado a um modelo de saúde específico*
(Bawany et al, 2022)	*Segurança, tolerância a falhas, transparência e imutabilidade*	*IoT, Blockchain e Saúde*	*Não define um algoritmo de consenso para plataforma*
(Miyachi & Mackey, 2021)	*Privacidade*	*Blockchain e saúde*	*Não define um algoritmo de consenso para plataforma*
(Rahman et al, 2022)	*Privacidade e integridade*	*IoMT, Blockchain, saúde e 5G Edge*	*Não define um algoritmo de consenso para plataforma*

Tabela 1 – Síntese dos trabalhos relacionados

Todas essas questões deixam clara a necessidade de aprofundamento dos estudos a respeito dos algoritmos de consenso que atendam aos requisitos necessários a sistemas para gestão da saúde, e servem de fundamentação para proposta constante na Seção 4.

3. Estudo Teórico

Nesta Seção é apresentado um estudo teórico analisando os requisitos necessários a um algoritmo de consenso aplicado a sistemas de gestão da saúde. Busca-se identificar os principais elementos necessários à especificação de um mecanismo de consenso que possa atender as necessidades existentes no domínio da gestão da saúde. O estudo é focado em quatro mecanismos de consenso baseados em votação e tolerantes a falhas bizantinas: *Practical Byzantine Fault Tolerance* (pBFT), *Federated Byzantine Agreement* (FBA), *Delegated Byzantine Fault Tolerance* (dBFT) e PAXOS.

Como visto na Seção 2, há uma heterogeneidade quanto ao tipo de algoritmo de consenso utilizado em sistemas de gestão de saúde, contudo, destacam-se algumas características comuns nesse contexto:

Blockchain privada – Dos sete *frameworks* avaliados, apenas um faz referência a uma *Blockchain* pública. Esse fato se justifica pela necessidade de acesso aos dados circulantes apenas por um grupo específico, o próprio paciente e o médico envolvido no processo de avaliação desses registros.

Algoritmo baseado em votação - Algoritmos baseados em provas implicam no recebimento de uma recompensa ao realizar tal esforço e são recomendados em redes que possuem um grande número de participantes. No caso específico dos sistemas de gestão de saúde, imagina-se uma quantidade limitada de nós, o que sugere o emprego de um algoritmo baseado em votação (Zhang e Jacobsen, 2018; Nguyen e Kim, 2018).

Privacidade *versus* Eficiência - Embora a busca pela eficiência seja um fator importante, a literatura indicou a privacidade das informações registradas como o foco da maioria dos sistemas. Tal fato é reforçado pelos dispositivos regulatórios na legislação dos países, como no Brasil (Brasil, 2018[1]; Brasil, 2018[2]).

3.1. Algoritmos de Consenso

A seguir, serão apresentadas algumas das principais características dos algoritmos de consenso avaliados no presente estudo.

Practical Byzantine Fault Tolerance (pBFT)

Proposto em (Castro e Liskov, 1999), é adaptado à comunicação assíncrona entre os nós da rede e direcionado a sistemas distribuídos, que estabelece a replicação de máquinas de estado como princípio para tolerar a falha bizantina.

Com o pBFT, a obtenção do consenso ocorre em três etapas, *pre-prepare*, *prepare* e *commit*. Após uma requisição feita por um cliente C, o líder (réplica 0) propõe uma mudança de estado e os nós realizam uma verificação do conteúdo em suas bases locais (*pre-prepare*) e, caso validado, é enviada para todos os participantes da rede uma mensagem de preparo (*prepare*), onde cada um deles espera o recebimento de $\frac{2n}{3}+1$ mensagens válidas, sendo *n* o número de nós existentes na rede, e após isso é passado para próxima etapa (*commit*), confirmando a transação, para que depois esse estado seja replicado em todas as bases locais.

Os principais fatores limitantes do algoritmo pBFT são a escalabilidade (Xiao *et al*, 2020) e a segurança, especificamente no que se refere ao atraso na conclusão das requisições (Amir *et al*, 2011).

Federated Byzantine Agreement (FBA)

O mecanismo de consenso *Federated Byzantine Agreement* (FBA) propõe que os enlaces entre os participantes da rede sejam definidos por cada um deles, formando a sua própria corrente de modo descentralizado. Esses enlaces são denominados fatias de quórum que se cruzam aos pares para garantir que as informações validadas entre eles não sejam contraditórias (Florian *et al*, 2022; Gaul *et al*, 2019).

Existem duas implementações importantes do algoritmo FBA, os protocolos *Ripple Protocol Consensus Algorithm* e *Stellar Consensus Protocol*, ambas trabalhando com duas etapas para validação de suas transações (Bracciali *et al,* 2021).

Em termos de segurança, o FBA é vulnerável à possibilidade de um nó malicioso causar danos à rede, criando diversas identidades falsas, o Sybil ataque (Iqbal e Matulevičius, 2021), um problema recorrente em algoritmos baseados em votação.

Delegated Byzantine Fault Tolerance (dBFT)

O algoritmo *Delegated Byzantine Fault Tolerance* (dBFT) é uma variação do pBFT que estabelece, em sua versão 2.0, um consenso baseado em três etapas e se propõe a ser mais eficiente por realizar uma votação *real time*, eliminando o tempo de bloqueio e confirmação das transações. O algoritmo dBFT implementa o conceito de consenso rotativo, mas apresenta uma falha de segurança, que se manifesta na possibilidade de um nó malicioso criar mais de um estado para o mesmo bloco (*spork*) (Wang *et al*, 2022).

PAXOS

Esses mecanismos de consenso possuem o algoritmo PAXOS como ancestral comum, com modificações para atender a necessidades específicas do contexto em que são utilizados (Lamport, 1998). Os processos em um algoritmo PAXOS são executados em duas etapas e assumem um ou mais papeis no seu decorrer, identificados como *proposers,* que são responsáveis pela proposição de valores para realizar o consenso; *acceptors são os* elementos responsáveis pela escolha de um valor proposto; e *learners,* que aprendem sobre o valor decidido.

Os quatro algoritmos apresentados possuem uma extensa lista de estudos realizados sobre suas potencialidades e fragilidades ao longo do tempo. Observa-se que a junção de algumas características, associadas à adoção de procedimentos para salvaguarda, permitem a concepção de mecanismos de consenso que garantam a privacidade esperada ao domínio informacional da saúde.

3.2. Requisitos para Sistemas de Gestão de Saúde

A avaliação sobre os estudos referenciados na Seção 2 evidenciou cinco requisitos essenciais ao domínio de sistemas de gestão da saúde, que estabelecem uma trilha para a concepção de um novo algoritmo de consenso. Tais requisitos são descritos a seguir.

Confidencialidade: Como visto na Seção 2, a privacidade é a grande preocupação dos sistemas de gestão de saúde, tanto pela questão regulatória quanto pelos constantes ataques cibernéticos, como o *ransomware*. O conceito de confidencialidade está diretamente ligado à privacidade, pois é a garantia de proteção contra acesso indevido às informações (ISO, 2018; Rodrigues e Silva, 2019; Sy *et al,* 2022).

Disponibilidade: Esse conceito diz respeito à garantia de acesso aos dados a qualquer momento que se faça necessário, e para isso um sistema deve oferecer a continuidade de seus serviços e respostas tempestivas àqueles que podem acessá-los (Sy *et al,* 2022).

Integridade: O conceito de integridade diz respeito à impossibilidade de alteração dos dados por parte de indivíduos não autorizados, visando evitar o prejuízo pela danificação desse ativo (ISO, 2018). Para mitigar esse problema, são empregadas técnicas como versionamento e redundância das informações (*backups*) (Zhang *et al*, 2022).

Escalabilidade: É a capacidade de um sistema entregar um serviço com a mesma qualidade, mesmo que haja uma mudança no cenário de sua inserção ou um acréscimo nos seus clientes (Bouraga, 2021). Algoritmos do tipo BFT possuem escalabilidade limitada, quando comparados a mecanismos de consenso baseados em provas, e

oferecem boas condições de desempenho apenas quando o número de réplicas é limitado (Vukolić, 2016).

Segurança: A tecnologia *Blockchain* possui vulnerabilidades que podem ser exploradas, como o ataque Sybil (Neshenko *et al*, 2019; Hashmat *et al*, 2022). Esse tipo de ataque ocorre quando um ente malicioso tenta controlar a rede criando outros nós vinculados a ele (Iqbal e Matulevičius, 2021), para que ele assuma o controle da rede.

4. Proposta do H-BFT

Esta Seção apresenta uma proposta de mecanismo de consenso baseado em votação e tolerante a falhas bizantinas e voltado a sistemas de gestão de saúde, dentro de um contexto de incertezas quanto à privacidade dos registros médicos de pacientes e dos profissionais de saúde responsáveis pelos diagnósticos.

4.1. Características do algoritmo proposto

O algoritmo proposto, denominado *Byzantine Fault Tolerance to Health* (H-BFT), é um algoritmo de consenso baseado em votação e tolerante a falhas bizantinas, cujas características são descritas a seguir.

Fatiamento contínuo (*continuous slicing*)

A implementação do H-BFT baseia-se no princípio do fatiamento contínuo para obtenção do consenso inspirado na ideia de fatiamento do quórum descrita no algoritmo FBA. O que doravante é proposto pretende estabelecer um quórum mínimo de indivíduos honestos na rede, a partir da lista retornada pelos verificadores. Esse quórum mínimo (*slice*) é expresso por $\frac{T-i}{2}+1$, onde *T* corresponde ao total de participantes verificados e *i* o total de indivíduos já selecionados e, caso o consenso não seja obtido, uma nova rodada é executada. Isso objetiva mitigar possíveis problemas de escalabilidade, comuns em grandes redes que utilizam algoritmos do tipo BFT.

Verificadores (*verifiers*)

No H-BFT, com o intuito de mitigar possíveis ataques do tipo Sybil, foi criado o papel *verifier*, que percorre toda a rede, de forma assíncrona à tentativa de consenso, aplicando um algoritmo de reputação, conforme descrito em (Zhou e Hwang, 2007), para compor uma lista de *acceptors* honestos. Os nós que assumirão o papel de *verifiers* serão responsáveis pela manutenção da lista de indivíduos confiáveis prontos para votar e receberem votos.

Os processos H-BFT podem então assumir os papéis de *leader*, que é responsável pelo recebimento de valores e proposição dos mesmos para estabelecimento de um consenso; *acceptor,* responsável pela escolha de um valor proposto; e *verifier,* que é responsável pela lista de nós idôneos da rede.

Consenso rotativo

O H-BFT implementa o conceito de reputação tal qual o algoritmo dBFT (Wang et al, 2022) que, associado à lista de nós verificados, altera o *leader* continuamente, propondo

um mecanismo de classificação *Peer-to-Peer* (P2P) distribuído de modo a selecionar os nós respeitáveis de forma dinâmica (Zhou & Hwang, 2007).

4.2. Implementação do algoritmo proposto

A Figura 1 exemplifica de forma simples as trocas de mensagens entre os participantes da rede durante a execução do H-BFT, representando a execução para obtenção do consenso entre as partes.

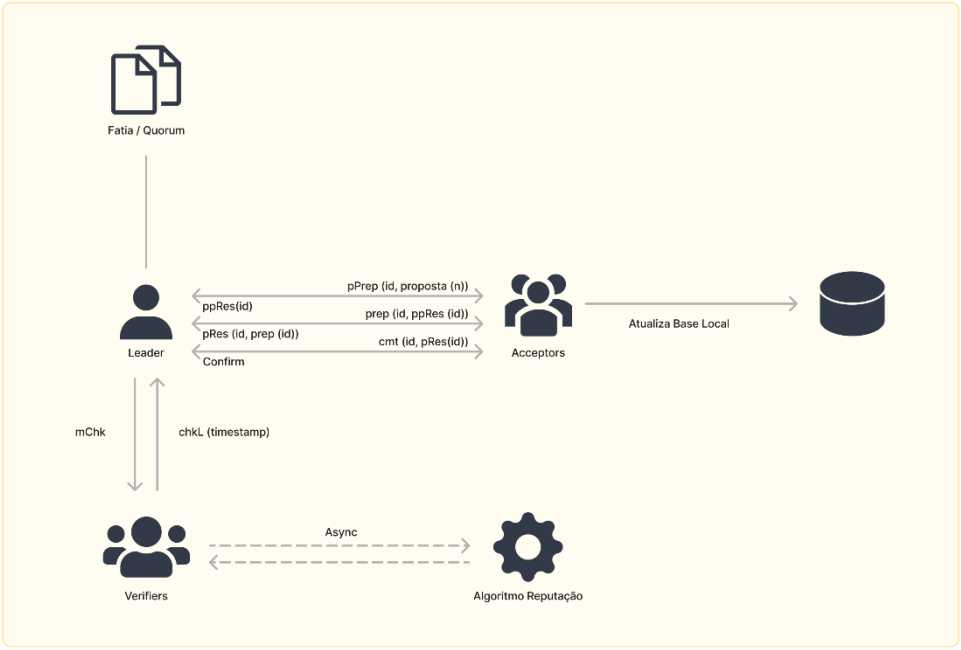

Figura 1 – Fluxo do Algoritmo H-BFT

O funcionamento do H-BFT é descrito detalhadamente na Tabela 2 em termos dos papéis e das respectivas ações nos processos que buscam a obtenção do consenso. A execução básica do algoritmo H-BFT inicia escolhendo-se um *leader* (consenso rotativo).

Papel	Ação
leader	*1. Recebe proposta de um cliente* *2. Envia mChk para os verifiers da rede*
verifier	*3. Recebe mChk* *4. Retorna chkL(timestamp)*
leader	*5. Aguarda chkL dos verifiers* *6. CASO chkL recebida esteja expirada ENTÃO descarta chkL SENÃO atualiza chkL local FIM* *7. Seleciona proposta(n)* *8. Envia pPrep(id, proposta (n)) para acceptors (slice)*

Papel	Ação
acceptor	*9. Recebe pPrep(id, proposta (n))* *10. Verifica sua base de dados local* *11. CASO base esteja correta ENTÃO Envia ppRes(id) para leader FIM*
leader	*12. Recebe ppRes(id)* *13. CASO quórum não seja suficiente para consenso e ainda haja nós honestos na rede ENTÃO Voltar para Ação 2* *SENÃO Envia prep (id, ppRes(id)) a quem respondeu FIM*
acceptor	*14. Recebe prep (id, ppRes(id))* *15. Envia pRes(id, prep(id)) para leader*
leader	*16. Recebe pRes (id, prep(id))* *17. Envia cmt (id, pRes(id)) para quem respondeu*
acceptor	*18. Recebe cmt (id, prep(id))* *19. Confirma a transação (mensagem cRes)* *20. Atualiza base*

Tabela 2 – Especificação do Algoritmo H-BFT

O *leader* ao receber uma proposta para inserção de um novo registro feita por um cliente (ação 1), solicita (ação 2) aos nós *verifiers* por meio de pedido de verificação (*mChk*) uma lista atualizada de nós confiáveis.

Os *verifiers* recebem a mensagem com o pedido de verificação (ação 3) e encaminham (ação 4) uma lista de nós confiáveis (*chkL*) para o *leader*, passando o selo de temporização (*timestamp*) da lista como parâmetro.

O *leader* aguarda as respostas à sua solicitação (ação 5) e ao receber uma lista de nós confiáveis (ação 6), verifica se o *timestamp* de geração da lista é anterior ao da lista em sua posse; se isso for verdade a lista recebida é descartada, caso contrário, ele atualiza a sua lista local. O *leader* então seleciona a proposta(n) (ação 7) e envia (ação 8) uma mensagem de *pre-prepare (pPrep*), contendo o *id* da mesma e a proposta com seu respectivo *id*, para os *acceptors* constantes na fatia de quórum.

Ao receber a mensagem *pPrep* (ação 9), o *acceptor* verifica a sua base de dados local (ação 10) e, caso ela esteja correta, ele responde ao *leader* (ação 11) com uma mensagem *pre-prepare response* (*ppRes*), passando o *id* da mesma como parâmetro.

O *leader* recebe a mensagem *pre-prepare* response (ação 12) enviada por um *acceptor* e avalia o número de respostas recebidas (ação 13). Caso o quórum ainda não seja suficiente para o consenso e ainda haja nós honestos na rede, ele retorna para o início do fluxo (ação 2) e executa a sequência de ações novamente; caso contrário, ele envia uma mensagem *prepare* (*prep*), passando o seu id e a mensagem *prepare response*, para cada *acceptor* que respondeu.

Os *acceptors* recebem (ação 14) a mensagem de *prepare* (*prep*) e retornam (ação 15) suas mensagens *prepare response* (*pRes*) para o *leader*.

O *leader* recebe (ação 16) as respostas (*pRes*) dos *acceptors* e então envia (ação 17) uma mensagem de *commit* (*cmt*) para os *acceptors* que responderam.

Os *acceptors* ao receberem (ação 18) a mensagem de *commit* (*cmt*), confirmam (ação 19) a transação por meio de mensagens *commit response* (*cRes*) e atualizam (ação 20) as suas bases.

A proposta deste algoritmo do consenso teve como referência as características de quatro algoritmos muito utilizados. No entanto, observa-se que os aspectos inseridos para mitigar a ocorrência de erros, atendendo plenamente a uma estrutura voltada ao domínio da gestão da saúde, necessitam da execução de testes para validação de sua efetividade na solução do problema.

5. Conclusões

O presente artigo apresentou uma proposta de algoritmo de consenso baseado em votação, tolerante a falha bizantina e aplicado a sistemas de gestão de saúde, denominado *Byzantine Fault Tolerance to Health* (H-BFT). O algoritmo H-BFT proposto caracteriza-se por uma combinação criteriosa de características dos algoritmos pBFT, FBA, dBFT e PAXOS, além da agregação de elementos para mitigar ataques cibernéticos do tipo Sybil.

Com o H-BFT, foram introduzidos dois conceitos passíveis de implementação: o fatiamento contínuo, destinado à mitigação de fragilidades na escalabilidade em correntes *Blockchain*, e o emprego de validadores com a função de manter uma rede de confiança, diminuindo a possibilidade da atuação de nós maliciosos.

Esta proposta é resultado de um estudo sobre *frameworks* aplicados à gestão de sistemas de saúde, onde identificou-se uma preocupação predominante com os elementos mais sensíveis, como a privacidade dos dados de pacientes e médicos.

Como trabalhos futuros, sugere-se a execução de testes em ambientes simulados, e a implementação do algoritmo com o objetivo de validar os processos aqui estabelecidos.

Referências

Adere, E. (2022). *Blockchain in Healthcare and IoT: A Systematic Literature Review*. *Array* (New York) 14. 100139. Web.

Amir, Y. (2011). *Prime: Byzantine Replication under Attack*. IEEE *Transactions on Dependable and Secure Computing*. vol. 8, no. 4, pp. 564-577, July-Aug. 2011, doi: 10.1109/TDSC.2010.70.

Azbeg, K. *et al.* (2018). *BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security*. *Egyptian Informatics Journal*, Volume 23, issue 2, 2022, pp. 329-343, ISSN 1110-8665.

Bawany, N. *et al.* (2022). *Integrating Healthcare Services Using Blockchain-Based Telehealth Framework*. IEEE *Access* 10 (2022): 36505-6517. *Web*.

Bouraga, S. (2021). *A taxonomy of blockchain consensus protocols: A survey and classification framework*. *Expert Systems with Applications*. vol. 168. 2021.

Bracciali, A., *et al.* (2021). *Decentralization in open quorum systems: Limitative results for Ripple and Stellar*. 2nd *Tokenomics 2020*, pp. 5:1–5:20. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2021)

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da República Federativa do Brasil.

Brasil. (2018). Lei nº 13.787, de 27 de dezembro de 2018. Diário Oficial da República Federativa do Brasil.

Brasil. (2021). Relatório de Auditoria nº 879316 do Ministério da Saúde - Avaliação da Prestação Anual de Contas, CGU. 2021. https://eaud.cgu.gov.br/.

Cao, B. *et al.* (2020). *Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks*. vol. 6. Issue 4. 2020. pp.480-485. https://doi.org/10.1016/j.dcan.2019.12.001

Castro, M. e Liskov, B. (1999). *Practical Byzantine Fault Tolerance. Third Symposium on Operating Systems Design and Implementation*. https://pmg.csail.mit.edu/papers/osdi99.pdf

Crain, T. *et al.* (2018). *DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains*. 2018. IEEE 17th *International Symposium on Network Computing and Applications* (NCA). 2018. pp. 1-8.

Dabbagh, M. *et al. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities*. *Computers Security*. vol. 100, p. 102078, 2021.

Dagher, G. *et al.* (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustainable Cities and Society, vol 39. 2018. pp. 283-297.

Florian, M. *et al.* (2022). *The sum of its parts: Analysis of federated byzantine agreement systems*. Distrib. Comput. 2022.

Gaul, A. *et al.* (2019). *Mathematical Analysis and Algorithms for Federated Byzantine Agreement Systems*. ArXiv. 2019. https://doi.org/10.48550/arxiv.1912.01365

Ghayvat, H. *et al.* (2021). *SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things*. IEEE *Transactions on Industrial Informatics*. vol. 18, no. 8, pp. 5609-5618, 2022.

Greve, F. *et al.* (2018). *Blockchain* e a Revolução do Consenso sob Demanda. Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. ed. XXXVI. c. 5. 2018. Sociedade Brasileira de Computação.

Hasan, K. *et al.* (2022). *A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks*. *Computer Networks*. vol. 211. 2022. https://doi.org/10.1016/j.comnet.2022.109004.

Hashmat, F. *et al.* (2022). *An Automated Context-aware IoT Vulnerability Assessment Rule-set Generator*. *Computer Communications* 186. 2022. 133-52. *Web*.

Huru H. *et al.* (2022). *A novel blockchain-enabled heart disease prediction mechanism using machine learning*. *Computers and Electrical Engineering*. vol. 101, 2022, 108086.

Iqbal, M. e Matulevičius, R. (2021). *Exploring Sybil and Double-Spending Risks in Blockchain Systems*. IEEE *Access*, vol. 9, pp. 76153-76177, 2021.

Ismail, L. e Materwala, H. (2020). *Blockchain paradigm for healthcare: Performance evaluation, Symmetry*, vol. 12, no. 8, 2020.

ISO Central Secretary (2018). *Information technology — security techniques — information security management systems — overview and vocabulary*. *Standard* ISO/IEC TR 27000:2018. *International Organization for Standardization*. Geneva, CH, 2018.

Kaur, H. (2018). *A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment*. *Transactional Processing Systems* (2018). https://doi.org/10.1007/s10916-018-1007-5.

Labs P. (2022). *IPFS Powers the Distributed Web*. *online*. 2022. https://ipfs.io/.

Lamport, L. (1998). *The Part-Time Parliament*. *ACM Transactions on Computer Systems* . 1998. 133-169. *Web*.

Miyachi, K. e Mackey, T. K. (2021). *HOCBS: A Privacy-preserving Blockchain Framework for Healthcare Data Leveraging an On-chain and Off-chain System Design*. *Information Processing & Management*. 2021. 102535. *Web*.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. 2008. https://bitcoin.org/bitcoin.pdf.

Neshenko, N. *et al.* (2019). *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*. IEEE *Communications Surveys and Tutorials*. 2019. Web.

Nguyen, G. e Kim, K. (2018). *A Survey about Consensus Algorithms Used in Blockchain*. *Journal of Information Processing Systems*. v.14. pp.101-128 2018

Qahtan, S. *et al* (2022). *Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry* 4.0 *Systems*. IEEE *Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6415-6423. 2022.

Qin, H. *et al.* (2022). *Weighted Byzantine Fault Tolerance consensus algorithm for enhancing consortium blockchain efficiency and security*, *Journal of King Saud University*. *Computer and Information Sciences*. 2022.

Rahman, M. *et al.* (2022). *Privacy Aware Internet of Medical Things Data Certification Framework on Healthcare Blockchain of* 5G *Edge*. *Computer Communications. vol. 192. pp 373-381.* 2022..Reibling, N. *et al.* (2019). *Worlds of healthcare: A healthcare system typology of oecd countries*. *Health Policy*, vol. 123, no. 7, pp. 611–620, 2019.

Rodrigues, C. K. S. (2021). *Analyzing blockchain integrated architectures for effective handling of iot-ecosystem transactions*. *Computer Networks*. vol. 201. p. 108610. 2021.

Rodrigues, C. K. S. e Silva, P.C. (2019). Uma análise de algoritmos de consenso para *Blockchain* visando à implementação de Sistemas de Informação Distribuídos e Transparentes. Revista de Sistemas e Computação. Salvador. vol. 9, n. 1, p. 163-188. 2019.

Rodrigues, C. K. S. (2017). Uma análise simples de eficiência e segurança da Tecnologia *Blockchain*. Revista de Sistemas e Computação. Salvador, vol. 7, n. 2, p. 147-162. 2017.

Singh, S. *et al.* (2022). *A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology*. *Future Generation Computer Systems*. vol. 129. 2022. pp. 380-388.

Sy, L. *et al.* (2022). *A survey of application research based on blockchain smart contract*. *Wireless Netw*. pp. 635–690. 2022.

Tripathi, G. *et al.* (2020). *S2HS- A blockchain based approach for smart healthcare system*. *Healthcare*. vol. 8. issue 1. 2020.

Vukolić, M. (2016). *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. *Camenisch, J., Kesdoğan, D. (eds) Open Problems in Network Security*. iNetSec 2015. *Lecture Notes in Computer Science*. vol 9591. Springer, Cham. https://doi.org/10.1007/978-3-319-39028-4_9.

Wang, Q. *et al.* (2022). *Formal Security Analysis on dBFT Protocol of* NEO. arXiv. 2022. https://doi.org/10.48550/arxiv.2105.07459.

Xiao, Y. *et al.* (2020). *A Survey of Distributed Consensus Protocols for Blockchain Networks*. IEEE *Communications Surveys & Tutorials*. vol. 22, no. 2, pp. 1432-1465, *Secondquarter*. 2020, doi: 10.1109/COMST.2020.2969706.

Zhang, K. e Jacobsen, H. (2018). *Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains*. 2018. IEEE 38th *International Conference on Distributed Computing Systems* (ICDCS). 2018. pp. 1337-1346.

Zhang, Y, *et al.* (2022). *Distributed data backup and recovery for software-defined wide area network controllers*. *Trans Emerging Tel Tech*. 2022;33(4):e4411. doi:10.1002/ett.4411

Zheng, Z. (2018). *Blockchain challenges and opportunities: a survey*. *International Journal of Web and Grid Services* v. 14, n. 4, pp. 352–375. 2018.

Zhou, R. e Hwang, K. (2007). *PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing*. IEEE *Transactions on Parallel and Distributed Systems*. 2007. Web.