1 Introdução

O ecossistema de saúde pública no Brasil vem sofrendo um processo veloz de digitalização, impulsionado pela consolidação dos prontuários eletrônicos e pela integração nacional via Rede Nacional de Dados em Saúde, em busca de constituir soluções inovadoras, seguras e eficazes, em comparado com diversos gargalos intrínsecos aos modelos tradicionais.

Entretanto, diante da crescente digitalização do SUS, a criticidade acerca da forma com que os dados de saúde dos pacientes, usuários do sistema único de saúde, são colhidos e processados no cenário nacional, vem aumentando exponencialmente. Contudo, além da oferta de benefícios, a aplicação desta tecnologia, em contrapartida, traz uma potencialidade de riscos de vazamentos, fraudes e adulterações, significativa, especialmente em triagem hospitalar, enquanto um dos principais setores das unidades de saúde, responsáveis pela coleta, processamento, armazenamento e compartilhamento de dados.

Diante disso, o objetivo principal deste trabalho é analisar a adoção da tecnologia blockchain no setor de triagem hospitalar do SUS, transpassando desde sua concepção histórica, até a estruturação explorada na atualidade. O problema de pesquisa, portanto, parte do questionamento sobre: Há viabilidade jurídica para o uso da tecnologia blockchain, nas triagens hospitalares do SUS, sem acarretar fricções indevidas e riscos de reidentificação ao fluxo assistencial?

Entretanto, considera-se imprescindível transpassar por etapas estruturadas através do estudo sobre a conceituação e caracterização da tecnologia blockchain; da análise dos fluxos operacionais das triagens hospitalares do SUS, além da sistematização de evidências empíricas sobre incidentes de segurança e vazamentos de dados no setor; e da análise acerca da (in)compatibilidade do uso da tecnologia em comento, em observância aos critérios, requisitos e definições estabelecidos pelos atos normativos vigentes.

Para tanto, adotou-se a metodologia de análise documental e revisão de literatura, com levantamento e exame dos atos normativos vigentes, além da análise multidisciplinar a estudos acadêmicos e a relatórios técnicos sobre segurança da informação em saúde.

Assim, encontrou-se na tecnologia *blockchain* a potencialidade esperada para auxiliar na construção da solução dos problemas em questão, na medida em que detém a capacidade de oportunizar o controle de acesso do sistema, além de âncoras criptográficas das anotações clínicas e das obtenções de consentimentos, estabelecendo, ainda, uma relação de transparência controlada.

Por fim, destaca-se que, o presente estudo sugere, ao final, a elaboração de um modelo de governança e arquitetura, acompanhado de critérios de conformidade e indicadores de desempenho para implantação incremental no SUS.

2 CONCEITUAÇÃO E CARACTERIZAÇÃO DA TECNOLOGIA *BLOCKCHAIN* E DO FLUXO ASSISTENCIAL DE TRIAGEM NO SUS

Com vistas em parametrizar a abordagem em questão, e, assim, oportunizar a devida compreensão sobre o tema em comento, destaca-se que nesta seção serão apresentados um breve histórico sobre a tecnologia *Blockchain*, além da sua conceituação e da sua caracterização, enquanto tecnologia. Em seguida, será analisado o fluxograma assistencial do SUS, com ênfase às atividades desempenhadas em setor de triagem hospitalar.

2.1. A tecnologia *Blockchain* e suas características

A tecnologia *blockchain* consiste, em suma, em uma tecnologia desenvolvida através de uma rede de computação distribuída, na qual os participantes encontram a segurança necessária para se integrarem a outros atores distintos, com os quais não possuem histórico de compartilhamento de dados, recebendo, entretanto, uma garantia técnica de inviolabilidade, transparência, interoperabilidade e imutabilidade dos registros (Conferência Nacional da Indústria, 2021).

Na visão de Aitzhan e Svetinovic (2006), a *blockchain* é interpretada como uma cadeia cronologicamente ordenada de blocos protegidos pela resolução chamada de *Proof-of-Work*, em que há o encadeamento através da utilização do *hash* do bloco anterior junto ao do bloco atual, o que, na prática, faz com que uma transação não possa ser alterada sem alterar as demais.

Calado, Silva e Troccoli (2024), ao beberem na fonte de Moraes, destacam que a blockchain deve ser imaginada como um grande banco de dados ou uma grande planilha, escrita com criptografia, para o registro das transações, onde cada registro parte do registro anterior num encadeamento de blocos.

Merkle (1989), através da materialização da denominada "árvore de *Merkle*", sustenta que cada folha possui relação direta e permanente com a raiz, o que permite, portanto, a integridade dos dados, vinculados e armazenados no âmbito da raiz, considerada *blockchain* .

Galhardo (2021, p. 236), por sua vez, afirma que a tecnologia *blockchain* não foi idealizada para realizar armazenar arquivos, mas apenas "*hashes* e códigos alfanuméricos correspondentes aos endereços ou contas dos usuários".

Em 2008, Satoshi Nakamoto apresentou ao mundo uma tecnologia inovadora, capaz de implementar uma espécie de dinheiro ou moeda eletrônica chamada de *Bitcoin* (token) em um tipo denominado de rede, chamada de *blockchain*, que utilizaria de um protocolo

denominado de *Proof of Work* (PoW) ou "Prova de Trabalho" para validar cada transação *peer-to-peer*, com objetivo de evitar o "gasto duplo" (Silva, 2020; Pinheiro, 2024).

Entretanto, junto a popularização dos criptoativos, a exemplo do *Bitcoin*, foram desenvolvidos os contratos digitais, conhecidos como "smart contracts", mecanismo utilizado como base das transações operadas em *blockchain*, com o objetivo de automatizar e fornecer garantias e seguranças as partes se comparado com contratos tradicionais (Moraes, 2021). No setor de saúde, o uso integrado da *blockchain* e dos *Smart Contracts* revelam a confiabilidade e a capacidade resolutiva na utilização destas ferramentas tecnológicas, em face dos problemas existentes no processamento e no tratamento dos dados sensíveis, coletados em ambiente de triagem hospitalar (Moraes, 2021).

Calado (2024, p. 98), leciona que, diante da versatilidade desta tecnologia, ao longo dos anos, a *blockchain* foi sendo aprimorada e ampliada, a partir da implementação de uma variedade de redes *blockchain*, com característica próprias, mas que se adaptam a diversas necessidades, as quais foram divididas, inicialmente, em *blockchains* não permissionadas, subdividida em *blockchains* públicas, e permissionadas, subdividida em *blockchains* privadas e de consórcio (Yaga, 2018).

Para Pinheiro (2024), as *blockchains* podem ser públicas, quando forem operadas de maneira descentralizada e acessível a todos os usuários. Já as *blockchains* privadas, são operadas de forma centralizada em um usuário ou em um grupo de usuários, com o objetivo de restringir a participação de usuários externos, através de "métodos de consenso diferentes".

Na prática clínica, em que pese as *blockchains* não permissionadas explorem a transparência, enquanto um dos principais benefícios referentes a sua operacionalização, a preferência recai sobre as *blockchain* consideradas permissionadas, uma vez que, por exigirem controle de acesso e confidencialidade, os dados clínicos, enquanto dados sensíveis, são mantidos na forma *off-chain*, ou seja, fora da cadeia (em um bloco específico), de modo a garantir uma relação de transparência e de segurança na relação instituída entre o titular (paciente), operador (profissional de saúde) e o controlador (Poder Público), ficando os demais dados (metadados verificáveis), a serem registrados na forma *on-chain* (Morte *et al*, 2020).

No cenário nacional, o Ministério da Saúde já apresentou iniciativas que visam um projeto de integração nacional na área de Saúde Digital, a exemplo do projeto de unificação do portal "Meu SUS Digital" com a RNDS, em que se objetiva, por exemplo, permitir o compartilhamento integrado dos dados sensíveis, de maneira descentralizadas, além garantir a interoperabilidade entre as instituições, com foco em privacidade e rastreabilidade,

alinhando-se, portanto, ao paradigma de processamento de dados no lugar de origem (off-chain) e de provas de integridade em *on-chain* (Golveia, 2025).

Além disso, Calado, Troccoli e Silva (2024) destacaram que o Brasil agiu na vanguarda a partir da inserção da tecnologia *blockchain* na composição da Rede Nacional de Dados em Saúde (RNDS). Atualmente, o país já acumula mais de 2,2 bilhões de dados em *blockchain*, conforme apresentado no Painel Telebrasil, no ano de 2024 (Cardoso, 2024).

Outrossim, de acordo com a Saúde Business, no corrente ano, o Hospital Edmundo Vasconcelos, em São Paulo/SP, anunciou a adoção de sistema baseado na tecnologia *blockchain*, com o objetivo de centralizar cadastros e agilizar atendimento, com uso de identidade digital e autenticação forte, visando reduzir fraudes, duplicidade de registros e tempo de *check-in* (Santos, 2025).

Entretanto, após a contextualização e apresentação dos potenciais riscos e benefícios desta tecnologia, há de se observar o fluxograma e as normativas de regência dos desenvolvimento das atividades no setor de triagem das unidades de saúde pública do país.

2 A TRIAGEM HOSPITALAR NO SUS.

A triagem em portas de urgência e emergência envolve um processo assistencial inicial, considerado como complexo e sensível, por se tratar do momento em que se coleta a identificação do paciente e dos seus dados sensíveis, dentre eles, dados de identificação, sinais vitais, queixas, histórico, medicamentos em uso, etc., para abertura de ficha (Bárbara *et al,* 2000), além da realização do protocolo de *Manchester*, com o objetivo de materializar a classificação de risco apresentado pelo paciente, e, assim, otimizar a definição da prioridade clínica (Oman *et al,* 2003).

Destarte, esse conjunto de dados e informações colhidas na porta da unidade de saúde inaugura o prontuário do paciente em atendimento, ao passo em que, ao difundir as informações a toda a equipe assistencial da unidade, o referido compartilhamento denota, de maneira intrínseca, riscos à integridade e a confidencialidade dos dados sensíveis, haja vista que, diante do alto fluxo, das pressões operacionais e da heterogeneidade de profissionais de saúde e de sistemas utilizados pelas unidades, há um aumento na probabilidade da existência de problemáticas correlatas a realização de acessos indevidos e de vazamento de dados.

Nos EUA, em 2024, a empresa Change Healthcare, da UnitedHealth Group, foi vítima de um ataque cibernético que alcançou escala sem precedentes e, segundo autoridades, chegou a impactar 192,7 milhões de pessoas, de acordo com informações publicadas no site do Departamento de Saúde e Serviços Humanos dos EUA, em virtude do vazamento de dados

sensíveis e do amplo efeito sistêmico incidente sobre os faturamentos e as autorizações (Schepkov, 2025).

No Brasil, o setor de saúde figura entre os mais visados, com milhares de violações registradas ao longo dos últimos 5 (cinco) anos, além do acúmulo de episódios de indisponibilidade e falhas sistemáticas, que afetam a integridade e a confiabilidade nos diversos sistemas aplicados as unidades de saúde.

Em 2020, por exemplo, o Instituto de Defesa do Consumidor (Idec) apresentou representação perante o Ministério Público Federal (MPF) solicitando a abertura de inquérito para investigar situações que levaram à exposição de dados aproximadamente 16 milhões de brasileiros que tiveram diagnóstico suspeito ou confirmado de COVID-19 (Cambricoli, 2020).

No ordenamento jurídico pátrio, denota-se a robustez necessária para o desenvolvimento do presente estudo, no cenário das triagens hospitalares. A LGPD, por exemplo, classifica os dados de saúde como dados pessoais sensíveis, ao passo em que exige a realização de um tratamento de dados criterioso, comprometido com a segurança e o enfoque estritamente assistencial, em benefício aos interesses dos titulares de dados, sendo vedado, entretanto, a sua utilização e o seu compartilhamento com objetivo de obtenção de vantagem ilícita (Brasil, 2018).

Além disso, a Resolução CFM nº 1.821/2007 aprovou o uso do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, além de admitir o uso de sistemas informatizados, e autorizar a digitalização dos prontuários físicos, visando eliminar registros em papel, desde que os sistemas selecionados observem os requisitos de segurança determinados no Art. 3º da referida Resolução (Brasil, 2007).

Assim, considera-se, em análise preliminar, que, de acordo com as normativas vigentes, a utilização da tecnologia *blockchain* apresenta potencialidade responsiva, as problemáticas que afligem o setor de triagem, com perspectiva de correção e de proteção dos dados compartilhados em toda a unidade de saúde, via prontuário eletrônico.

Considerações finais

Com o advento do presente estudo, observou-se que a adoção da tecnologia *blockchain* na triagem hospitalar das unidades de saúde integrantes do SUS mostra-se juridicamente viável e tecnicamente pertinente quando estruturada em modelos permissionados, com registros clínicos *off-chain* e âncoras criptográficas *on-chain*, visando a garantia de integridade, de imutabilidade e de transparência.

Destarte, constatou-se, em linhas preliminares, a possibilidade de observância às exigências de segurança e a confidencialidade do tratamento de dados sensíveis, sem exigir

mudanças que gerem quaisquer fricções ao fluxo assistencial, desde que a solução preserve o desempenho na porta de entrada e respeite o princípio da minimização de dados.

Por fim, do ponto de vista normativo, a LGPD e os demais atos normativos especiais, a exemplo da Resolução CFM nº 1.821/2007, editada pelo CFM, já oferecem lastro regulatório suficiente para orientar governança de acesso, o armazenamento das informações e a certificação dos sistemas, com o objetivo de eliminar os registros físicos, desde que o uso da tecnologia escolhida decorra de uma avaliação de impacto em proteção de dados, políticas de controle de acesso por perfil e *accountability* contínua, somada a rastreabilidade *by design*, diante aumento exponencial da ocorrência de incidentes cibernéticos em saúde, a fim de reduzir superfície de ataque e acelerar às respostas aos incidentes.

REFERÊNCIAS BIBLIOGRÁFICAS

AITZHAN, N. Z.; SVETINOVIC, D. Security and privacy in decentralized energy trading through multisignatures, blockchain and anonymous messaging streams. **IEEE Transactions on Dependable and Secure Computing,** out. 2016.

ARSENE, Codrin. **Blockchain in healthcare guide**. HEALTHCARE WEEKLY, 2024. Disponível em: https://healthcareweekly.com/blockchain-in-healthcare-guide/. Acesso em: 26 set. 2025.

BÁRBARA, N. R. S. *et al*. **Processo de triagem em serviço de emergência**: estudos de caso. 2000. 63 f. Trabalho de Conclusão de Curso (Especialização em Metodologia da Assistência de Enfermagem) – Universidade do Estado da Bahia, Salvador, 2000.

BIS RESEARCH. **Global blockchain in healthcare market 2025**, 2018. Disponível em: https://bisresearch.com/industry-report/global-blockchain-in-healthcare-market-2025.html. Acesso em: 20 set. 2025.

BRASIL. Conselho Federal de Medicina. **Resolução CFM nº 1.821, de 23 nov. 2007**. Aprova normas técnicas para digitalização e uso de sistemas informatizados no prontuário do paciente. Brasília, DF: CFM, 2007.

BRASIL. Confederação Nacional da Indústria. **A tecnologia blockchain e suas possíveis aplicações no comércio exterior**. Brasília: CNI, 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em:https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 out. 2025.

CALADO, Vinicius de Negreiros. Democracia e tecnologia blockchain: uma análise da produção nacional a partir do Google Acadêmico. **Revista Brasileira de Direito Constitucional**, [S. l.], v. 24, n. 1, p. 96–109, 2024. DOI: 10.62530/rbdcv24n01p096.Disponível em: https://esdc.com.br/ojs/index.php/revista/article/view/359. Acesso em: 18 set.2025.

CALADO, Vinicius de Negreiros; TROCCOLI, Matheus Quadros Lacerda; SILVA, FlaviaValeria. Blockchain e Inteligência Artificial: Potencialidades e Desafios da IntegraçãoTecnológica. In: **Regulação da Inteligência Artificial III** [Recurso eletrônico on-line]organização V Congresso Internacional de Direito e Inteligência Artificial (V

CIDIA).Coordenadores: Gabriel Oliveira de Aguiar Borges, Matheus Antes Schwede e Luiz Felipe deFreitas Cordeiro – Belo Horizonte: Skema Business School, 2024. p. 55-63.

CAMBRICOLI, F. **Idec pede ao MPF que investigue vazamento de dados da saúde; deputado aciona TCU**. Estadão, 2020. Disponível em: https://www.estadao.com.br/saude/idec-pede-ao-mpf-que-investigue-vazamento-de-dados-da-saude-deputado-aciona-tcu/. Acesso em: 12 set. 2025.

GALHARDO, Flaviano; PARO, João P.; NALINI, José R.; AL, et. **Direito Registral e Novas Tecnologias**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9786559641130. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559641130/. Acesso em: 20 set. 2025.

GOLVEIA, Vinicius. **Governo federal confirma pesquisas no SUS com blockchain em nova parceria**. LIVECOINS, 2025. Disponível em: https://livecoins.com.br/governo-federal-confirma-pesquisas-no-sus-com-blockchain-em-nova-parceria/. Acesso em: 20 out. 2025.

MERKLE, R. C. A certified digital signature. In: **Advances in Cryptology**. Berlin: Springer-Verlag, 1989.

MORAES, Alexandre Fernandes D. **Bitcoin e Blockchain**: a revolução das moedas digitais. São Paulo: Editora Saraiva, 2021. 9786558110293. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786558110293/. Acesso em: 25 set. 2025.

MORTE, A. B.; MEIRA, A.; COSTA, R.; MARIZ, D. **Uma análise sobre o uso de DLTs no tratamento de dados pessoais**: aderência aos princípios e direitos elencados na LGPD, 2020.

OMAN, K. S.; KOZIOL-MCLAIN, J. K.; SCHEETZ, L. J. *Segredos em enfermagem de emergência*. Trad. Regina Garcez. Porto Alegre: Artmed, 2003.

PINHEIRO, Talita Cavalvanti. Acesso e compartilhamento de dados de saúde em blockchain usando smart contracts. 66 f. Disserção (Mestrado em Engenharia Elétrica) - Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal do Amazonas, Manaus, 2024.

SANTOS, Juliana. **Hospital Edmundo Vasconcelos adota blockchain para centralizar cadastros e agilizar atendimento**. SAÚDE BUSINESS, 2025. Disponível em: https://www.saudebusiness.com/ti-e-inovao/hospital-edmundo-vasconcelos-adota-blockchain-para-centralizar-cadastros-e-agilizar-atendimento/. Acesso em: 27 set. 2025.

SCHEPKOV, Vlad. **Ataque hacker à Change Healthcare da UnitedHealth afetou 192,7 milhões de pessoas**. Investing.com, 2024. Disponível em: https://br.investing.com/news/stock-market-news/ataque-hacker-a-change-healthcare-da-unitedhealth-afetou-1927-milhoes-de-pessoas-1649410. Acesso em: 19 set. 2025.

SILVA, Rodrigo Cardoso. **Proposta de aplicação para verificação do voto com tecnologia Blockchain**: a abordagem de um modelo E2E verifiability para internet Voting da Estônia. 2020. 159 f. Tese (Doutorado em Tecnologias da Inteligência e Design Digital) - Programa de Estudos Pós-Graduados em Tecnologias da Inteligência e Design Digital, Pontifícia Universidade Católica de São Paulo, São Paulo, 2020.

YAGA, Dylan *et al*. **NIST IR 8202***:* Blockchain technology overview. Gaithersburg: NIST, 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf. Acesso em: 22 out. 2025.