

Uma Solução Baseada em Blockchain para Auditoria em Cenários de Telessaúde Emergencial

Victor Octávio Rodrigues Alves¹, Eder John Scheid², Muriel Figueredo Franco¹

¹ Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA)

²Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre — RS — Brasil

{victoralves,muriel.franco}@ufcspa.edu.br, ejscheid@inf.ufrgs.br

Abstract. *Emergency telehealth scenarios combine time-critical clinical decisions, distributed teams, and high volumes of simultaneous records, imposing specific auditability requirements. Traditional health record systems rely on a centralized trust model in which the data custodian is also an interested party. This work proposes an audit layer based on Hyperledger Fabric that provides immutable and verifiable trails for diagnostic events. A Go chaincode and a REST integration layer were implemented and validated on a minimal Fabric network, demonstrating the complete flow from HTTP request to ledger commit and the retrieval of ordered audit trails, including previous values and the author of each change.*

Resumo. *Cenários de telessaúde emergencial reúnem decisões clínicas sob pressão temporal, equipes geograficamente distribuídas e alto volume de registros simultâneos, impondo requisitos específicos de auditabilidade. Os sistemas tradicionais operam sob um modelo de confiança centralizado, no qual o guardião dos dados é também parte interessada. Este trabalho propõe uma camada de auditoria baseada em Hyperledger Fabric, capaz de fornecer trilhas imutáveis e criptograficamente verificáveis. Foram implementados um chaincode em Go e uma camada de integração REST via Fabric Gateway SDK. Os resultados preliminares, obtidos em rede Fabric minificada, demonstram o fluxo completo da requisição HTTP ao registro no ledger e a recuperação de trilhas de auditoria cronologicamente ordenadas, contendo os valores anteriores e a identidade do responsável por cada alteração.*

1. Introdução

A telessaúde consolidou-se como abordagem estratégica na prestação de serviços de saúde, especialmente após a pandemia de COVID-19, que impôs restrições ao atendimento presencial e acelerou a adoção de consultas remotas em escala global [Monaghesh and Hajizadeh 2020]. Nesse contexto, cenários nos quais decisões clínicas precisam ser tomadas rapidamente e envolvem múltiplos profissionais distribuídos geograficamente representam um dos domínios mais críticos e, ao mesmo tempo, mais vulneráveis, já que a urgência do atendimento intensifica o volume de registros gerados e reduz a margem para verificações manuais de integridade e conformidade.

Essa mesma urgência agrava desafios já conhecidos de auditabilidade, segurança e centralização em sistemas de telessaúde [Hathaliya and Tanwar 2020, Severo et al. 2025].

Registros, prescrições e encaminhamentos são gerados em intervalos curtos e armazenados em sistemas centralizados que carecem de interoperabilidade [Vazirani et al. 2020]. Nesses sistemas, a instituição que detém os dados é simultaneamente parte interessada e guardiã dos registros, o que cria um conflito de interesse inerente em que a mesma entidade que poderia ser objeto de auditoria é a que administra os dados a serem auditados [Ahmad et al. 2021]. Somam-se a isso a vulnerabilidade a pontos únicos de falha e a possibilidade de alteração retroativa de registros sem detecção [Yaqoob et al. 2022]. Em disputas médico-legais ou auditorias regulatórias, por exemplo, a impossibilidade de comprovar, de forma irrefutável, a sequência e o conteúdo das decisões tomadas compromete tanto a proteção do paciente quanto a do profissional.

A tecnologia *blockchain* é uma aliada para enfrentar tais limitações. Por meio de estruturas de dados encadeadas criptograficamente e mecanismos de consenso distribuído, ela permite a criação de registros imutáveis e auditáveis, nos quais qualquer tentativa de alteração retroativa é detectável pelos participantes da rede [Scheid et al. 2021]. Contudo, parte significativa das soluções propostas na literatura utiliza *blockchains* públicas, como Ethereum, que apresentam limitações de eficiência, governança de acesso e proteção de dados sensíveis quando aplicadas ao contexto clínico [Tanwar et al. 2020]. Redes permissionadas, nas quais a participação é restrita a entidades previamente autorizadas, mostram-se mais adequadas. O Hyperledger Fabric é uma das plataformas mais maduras dessa categoria, oferecendo contratos inteligentes (*chaincodes*) em linguagens de propósito geral, canais privados de comunicação e políticas configuráveis de endosso [Androulaki et al. 2018].

Este trabalho propõe uma solução baseada em blockchain para a auditabilidade de registros em cenários de telessaúde emergencial. A solução propõe e implementa uma arquitetura em três camadas, que utiliza *smart contracts* executados em uma rede permissionada (*i.e.* Hyperledger Fabric), fornecendo uma camada de auditoria independente para telessaúde que complementa os sistemas já existentes, sem substituí-los.

2. Fundamentação Teórica

Embora o termo “telessaúde emergencial” não esteja formalmente consolidado na literatura como modalidade distinta, principalmente no Brasil, este trabalho propõe sua adoção para designar o conjunto de práticas de telessaúde executadas em cenários clínicos nos quais a pressão temporal é fator determinante e as decisões diagnósticas e terapêuticas envolvem, frequentemente, múltiplos profissionais distribuídos geograficamente. Situações como atendimentos pré-hospitalares, respostas a desastres naturais e urgências em regiões remotas diferenciam-se qualitativamente das demais modalidades de telessaúde, consolidadas sobretudo em contextos eletivos e de acompanhamento a distância.

O conceito encontra aplicação prática no projeto OpenHealth5G¹, desenvolvido no âmbito do programa OpenRAN@Brasil, que tem como um de seus casos de uso prioritários a telessaúde emergencial. Em um dos cenários descritos, uma equipe de primeiro atendimento equipada com câmera 4K, ultrassom portátil e sensores de sinais vitais conectados via 5G transmite dados clínicos em tempo real a especialistas de um centro de referência, que orientam remotamente procedimentos como imobilização e controle de hemorragia.

¹<https://openhealth5g.github.io/>

A partir dessa caracterização, propõem-se os seguintes atributos definidores: (i) **pressão temporal**, com decisões tomadas em minutos ou segundos, sem possibilidade de revisão presencial imediata; (ii) **multiprofissionalidade distribuída**, envolvendo profissionais de organizações distintas que compartilham informações de forma síncrona; (iii) **alto volume e velocidade de registros**, gerados simultaneamente por múltiplas fontes; (iv) **criticidade das decisões**, cujos erros ou atrasos podem ter consequências irreversíveis; e (v) **demanda por auditabilidade robusta**, uma vez que a reconstituição posterior da cadeia de decisões é essencial para fins médico-legais e regulatórios.

3. Trabalhos Relacionados

A Tabela 1 sintetiza os principais trabalhos que exploram aplicações de *blockchain* no domínio da saúde, com foco em auditabilidade e integridade de dados clínicos.

Tabela 1. Comparativo de trabalhos relacionados

Trabalho	Plataforma	Domínio	Finalidade
[Azaria et al. 2016]	Ethereum	Prontuário eletrônico	Gestão descentralizada de permissões e acesso a prontuários
[Tanwar et al. 2020]	Hyperledger Fabric	Prontuário eletrônico	Prontuário eletrônico descentralizado para <i>Healthcare 4.0</i>
[Mole and Shaji 2024]	Ethereum	Prontuário eletrônico	Gerenciamento seguro de prontuários com armazenamento descentralizado
[Ahmad et al. 2021]	Ethereum	Cadeia de suprimentos	Rastreabilidade de equipamentos médicos durante a COVID-19
[Bharathi et al. 2024]	Hyperledger Fabric	Prontuário eletrônico	Compartilhamento de PEP em telemedicina com controle centrado no paciente
[Liang et al. 2024]	Rahasak	Telessaúde	Gestão descentralizada de identidades e comunicação confiável
[Kaushal et al. 2025]	Hyperledger Fabric	Monitoramento remoto (IoT)	Monitoramento remoto integrado a rede permissionada, avaliado via Caliper
Este trabalho	Hyperledger Fabric	Telessaúde emergencial	Auditabilidade de registros por meio de trilhas imutáveis entre organizações

Fonte: elaborada pelos autores.

Soluções baseadas em Ethereum concentram-se em domínios nos quais os requisitos de privacidade são comparativamente menos restritivos. Nesses casos, a transparência inerente às redes públicas é uma vantagem, permitindo verificação independente sem governança centralizada de identidades. Contudo, essas mesmas características tornam-se limitações em domínios clínicos sensíveis: o *throughput* reduzido, a dependência de uma moeda associada à rede e a ausência de mecanismos nativos de controle de acesso por organização comprometem a aplicabilidade em cenários que exigem conformidade regulatória e desempenho previsível.

Em contrapartida, o Hyperledger Fabric predomina em aplicações que envolvem dados clínicos sensíveis e cooperação entre instituições, com viabilidade técnica já demonstrada em redes multi-organizacionais de saúde avaliadas via Hyperledger Caliper [Kaushal et al. 2025], abordagem metodológica que também será adotada neste trabalho. No eixo de telessaúde, o trabalho que aborda o domínio de forma mais direta concentra-se na segurança da comunicação entre participantes, sem tratar da auditabilidade das de-

cisões clínicas, e recorre a uma plataforma pouco difundida na literatura, o que limita a reprodutibilidade [Liang et al. 2024].

Nenhum dos trabalhos analisados trata da telessaúde emergencial: não foram identificadas soluções voltadas à auditabilidade de decisões tomadas sob pressão temporal por equipes multiprofissionais distribuídas, nem aplicações de redes permissionadas nesse contexto.

4. Solução Proposta

A solução proposta organiza-se em três camadas, conforme apresentado na Figura 1: camada do cliente, camada de *gateway* e camada de rede (*i.e.*, *blockchain*).

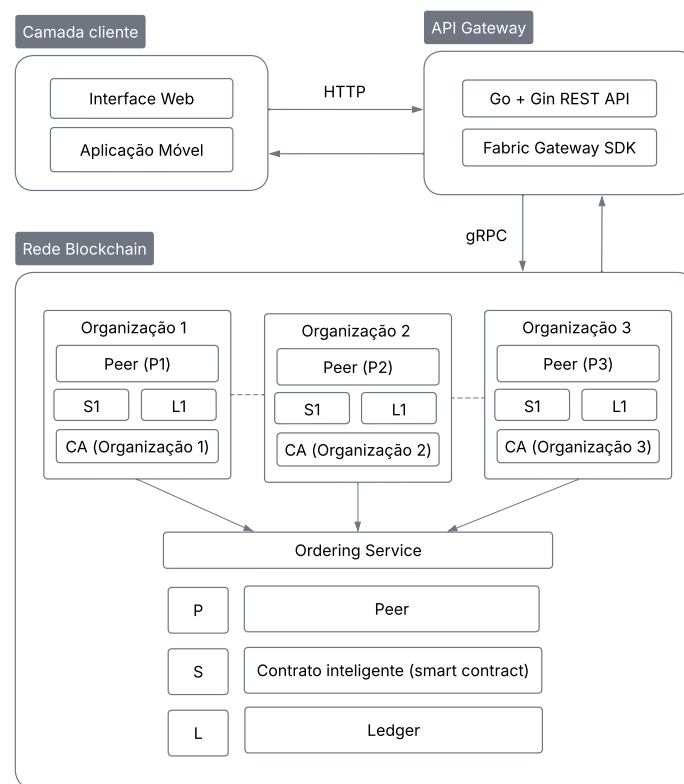


Figura 1. Arquitetura proposta em três camadas

A **camada do cliente** compreende as interfaces de acesso ao sistema, responsáveis por apresentar formulários de registro de eventos, exibir o histórico de alterações e permitir a consulta de trilhas de auditoria. Essa camada não possui qualquer conhecimento sobre a rede subjacente.

A **camada de gateway** é o componente central da arquitetura. Implementada como uma API REST em Go com o *framework* Gin, expõe *endpoints* correspondentes às operações do *chaincode*. Internamente, cada requisição HTTP é traduzida em uma invocação gRPC por meio do Fabric Gateway SDK, que gerencia a conexão com os *peers*, a submissão de propostas de transação e a coleta de *endorsements*. Essa separação de responsabilidades mantém isolada a lógica de comunicação com a *blockchain*, facilitando a evolução independente de cada camada.

A **camada de rede** é composta pela infraestrutura do Hyperledger Fabric. Cada organização participante mantém ao menos um *peer*, que armazena uma réplica local do *ledger* e executa o *chaincode* instalado, além de sua própria *Certificate Authority* para emissão de identidades organizacionais. O *Ordering Service*, compartilhado entre as organizações, estabelece a ordem total das transações e as distribui em blocos aos *peers* do canal. Uma transação só é efetivada após ser endossada pelos *peers* exigidos pela política de endosso do canal.

5. Implementação e Resultados Preliminares

Foi implementado um *chaincode* em Go, utilizando a biblioteca *Hyperledger Fabric Go Contract*, capaz de realizar quatro operações fundamentais sobre registros diagnósticos: inserção, leitura, atualização e consulta de histórico.

O *chaincode* foi implantado e testado em rede Fabric minificada por meio do Microfab, que instancia um *peer*, um ordenador e uma *Certificate Authority* em um único *container* Docker, validando o fluxo completo de submissão, endosso e *commit* de transações. Utilizou-se o Hyperledger Fabric na versão 2.5, com o serviço de ordenação operando em um único nó Raft, mecanismo tolerante a falhas por parada (*Crash Fault Tolerant*, CFT). A operação de consulta de histórico, em particular, demonstrou a capacidade do Fabric de manter uma trilha de auditoria completa e cronologicamente ordenada de todas as alterações realizadas sobre um registro, incluindo os valores anteriores e as identidades dos participantes responsáveis por cada modificação, comportamento que corresponde diretamente ao requisito de reconstituição da cadeia de decisões clínicas.

Sobre essa base, foi desenvolvida a camada de integração. A conexão entre a API REST e a rede Fabric é estabelecida por credenciais TLS e certificados de identidade gerenciados pelo MSP da organização, enquanto o Fabric Gateway SDK abstrai as principais operações dentro da rede. Foram implementados e testados *endpoints* correspondentes às quatro operações do *chaincode*. Embora não reproduza a complexidade de uma rede multi-organizacional, essa configuração valida o fluxo completo, da requisição HTTP ao registro imutável no *ledger*.

6. Conclusões e Trabalhos Futuros

Este trabalho apresentou uma solução de auditoria baseada em Hyperledger Fabric para cenários de telessaúde emergencial, domínio ainda pouco explorado na literatura de *block-chain* aplicada a saúde. Os resultados preliminares validaram o *chaincode* proposto e a camada de integração via Fabric Gateway SDK em rede minificada.

Como trabalhos futuros, prevê-se a expansão para uma topologia multi-organizacional, com políticas de endosso que exijam validação por múltiplas organizações e canais privados para isolar dados sensíveis, de maneira a simular um cenário real. A avaliação de desempenho também será conduzida com o Hyperledger Caliper, medindo latência, vazão (TPS) e taxa de sucesso sob diferentes cargas e números de organizações. O objetivo é verificar se a solução atende aos requisitos temporais do atendimento emergencial, nos quais a latência de registro não pode comprometer o fluxo clínico.

Declaração de uso de IA. Ferramentas de IA generativa foram usadas como apoio à revisão e organização textual, todo o conteúdo foi revisado e validado pelos autores.

Referências

- Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Omar, M., and Ellahham, S. (2021). Blockchain-based forward supply chain and waste management for COVID-19 medical equipment and supplies. *IEEE Access*, 9:44905–44927.
- Androulaki, E., Barger, A., Bortnikov, V., et al. (2018). Hyperledger Fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18)*, pages 1–15. ACM.
- Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30.
- Bharathi Murthy, C. V. N. U. and Lawanya Shri, M. (2024). Secure sharing architecture of personal healthcare data using private permissioned blockchain for telemedicine. *IEEE Access*, 12:106645–106657.
- Hathaliya, J. J. and Tanwar, S. (2020). An exhaustive survey on security and privacy issues in healthcare 4.0. *Computer Communications*, 153:311–335.
- Kaushal, R., Kumar, N., Kukreja, V., and Boonchieng, E. (2025). Hyperledger fabric based remote patient monitoring solution and performance evaluation. *Peer-to-Peer Networking and Applications*, 18.
- Liang, X., Alam, N., Sultana, T., Bandara, E., and Shetty, S. (2024). Designing a blockchain-empowered telehealth artifact for decentralized identity management and trustworthy communication. *Journal of Medical Internet Research*, 26:e46556.
- Mole, J. S. S. and Shaji, R. S. (2024). Ethereum blockchain for electronic health records: securing and streamlining patient management. *Frontiers in Medicine*, 11:1434474.
- Monaghesh, E. and Hajizadeh, A. (2020). The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence. *BMC Public Health*, 20(1):1193.
- Scheid, E. J., Rodrigues, B. B., Killer, C., Franco, M. F., Rafati, S., and Stiller, B. (2021). Blockchains and distributed ledgers uncovered: Clarifications, achievements, and open issues. In *Advancing Research in Information and Communication Technology*, volume 600 of *IFIP Advances in Information and Communication Technology*, pages 289–317. Springer.
- Severo, J., Herbert, J., and Franco, M. (2025). Threat modeling in healthcare: An analysis of trends, gaps, and emerging challenges. In *Anais da XXII Escola Regional de Redes de Computadores*, pages 158–164, Porto Alegre, RS, Brasil. SBC.
- Tanwar, S., Parekh, K., and Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50:102407.
- Vazirani, A. A., O'Donoghue, O., Brindley, D., and Meinert, E. (2020). Blockchain vehicles for efficient medical record management. *npj Digital Medicine*, 3(1):1.
- Yaqoob, I., Salah, K., Jayaraman, R., and Al-Hammadi, Y. (2022). Blockchain for health-care data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34(14):11475–11490.