Decentralized-OpenHealth : Identidade Auto-Soberana e Interoperabilidade FHIR/HL7 no Ecossistema Brasileiro

Antonio Mateus de Sousa[1,2], **Jeffson Celeiro Sousa**[2,3], **Bruno Evaristo**[2,3]

[1] Programa de Pós-Graduação em Ciência da Computação (PGCOMP)
Instituto de Computação – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

[2]Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

[3]Universidade Federal do Pará (UFPA)
Belém – PA – Brasil

{amateus, jcsousa, elderb }@cpqd.com.br

Resumo. *A fragmentação dos dados clínicos no Brasil compromete a interoperabilidade e a privacidade no setor de saúde. Para solucionar este problema, este artigo propõe o Decentralized-OpenHealth (D-OH), uma arquitetura que une a Identidade Digital Descentralizada (DID) ao padrão semântico FHIR/HL7. Sob a governança do Ministério da Saúde e alinhado à Rede Nacional de Dados em Saúde (RNDS), o modelo utiliza Credenciais Verificáveis com assinaturas BBS+ para viabilizar Provas de Conhecimento Zero (ZKPs), garantindo ao cidadão a custódia exclusiva e a divulgação seletiva de seu histórico clínico em conformidade com a LGPD. A avaliação de desempenho em uma rede permissionada (Hyperledger Besu), combinada ao armazenamento híbrido via IPFS para exames densos, demonstrou uma redução superior a 99% no payload das credenciais, atestando a alta escalabilidade e a viabilidade técnica da solução para adoção no Sistema Único de Saúde (SUS).*

Abstract. *The fragmentation of clinical data in Brazil compromises interoperability and privacy in healthcare. To address this issue, this paper proposes Decentralized-OpenHealth (D-OH), an architecture combining Decentralized Digital Identity (DID) with the FHIR/HL7 semantic standard. Under the governance of the Ministry of Health and aligned with the National Health Data Network (RNDS), the model uses Verifiable Credentials with BBS+ signatures to enable Zero-Knowledge Proofs (ZKPs), ensuring citizens have exclusive custody and selective disclosure of their clinical history in compliance with the LGPD. Performance evaluation on a permissioned network (Hyperledger Besu), combined with hybrid IPFS storage for dense medical exams, demonstrated an over 99% reduction in credential payload, proving the solution's high scalability and technical viability for adoption in the Unified Health System (SUS).*

1. Introdução

A digitalização do setor de saúde brasileiro, impulsionada por iniciativas como a Rede Nacional de Dados em Saúde (RNDS), esbarra historicamente na fragmentação dos dados. Hospitais, clínicas e laboratórios operam em silos isolados de informação, limi-

tando a interoperabilidade e retirando do paciente o controle sobre seus registros clínicos [Houtan et al. 2020].

Inspirado no *Open Finance*, o conceito de *OpenHealth* busca resolver esse atrito através de um ecossistema interoperável. Para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD), é fundamental que o cidadão custodie seus dados. A Identidade Digital Descentralizada (DID) e as Credenciais Verificáveis (VCs), aliadas ao padrão semântico *Fast Healthcare Interoperability Resources* (FHIR/HL7), oferecem a infraestrutura criptográfica necessária para viabilizar esse compartilhamento seguro [Phuyal et al. 2026, Spanakis et al. 2025].

Este trabalho propõe e avalia o **Decentralized-OpenHealth (D-OH)**, uma arquitetura nativamente descentralizada para o Brasil. O modelo estabelece o Ministério da Saúde como âncora de confiança e utiliza assinaturas BBS+ para Provas de Conhecimento Zero (ZKP), combinadas ao armazenamento IPFS, garantindo soberania e escalabilidade sem comprometer o desempenho da rede.

2. Trabalhos Relacionados

A literatura recente aborda a Identidade Auto-Soberana (SSI) na saúde [Houtan et al. 2020, Valavan et al. 2024] e a interoperabilidade semântica utilizando VCs e FHIR [Phuyal et al. 2026]. No entanto, a maioria propõe ecossistemas *trustless* desprovidos de hierarquia institucional ou falha ao tratar o armazenamento de ativos densos (como imagens DICOM).

O diferencial do D-OH reside em três pilares: (1) **Governança Institucional**, refletindo as exigências da RNDS/SUS; (2) **Integração Nativa FHIR-VC**, ancorando o formato W3C nas ontologias médicas; e (3) **Armazenamento Híbrido**, mitigando gargalos de *blockchain* ao alocar arquivos pesados *off-chain*.

3. Arquitetura Decentralized-OpenHealth (D-OH)

O modelo D-OH apresentado na Figura 1é composto por três atores principais: o **Emissor** (hospitais/clínicas), o **Titular** (paciente gerenciando sua *HealthDID wallet*) e o **Verificador** (laboratórios/médicos consultivos). O fluxo de confiança não exige integrações ponto a ponto entre os sistemas médicos; a *blockchain* atua unicamente como registro de chaves públicas e âncoras de revogação.

3.1. Modelo de Governança

O Ministério da Saúde atua como a Autoridade Principal (*Trust Anchor*). Ele é responsável por credenciar hospitais e profissionais na *blockchain* (e.g., Rede Blockchain Brasil - RBB), garantindo que uma VC emitida contenha o DID de uma instituição validada.

3.2. Credenciais FHIR Híbridas e ZKP

Para contornar as limitações de armazenamento *on-chain* e o inchaço das carteiras móveis, o D-OH adota uma estratégia híbrida estruturada em FHIR R4.

Imagens médicas pesadas têm seu *hash* SHA-256 extraído e são publicadas no IPFS (*InterPlanetary File System*). A âncora resultante é injetada no atributo `presentedForm` do recurso FHIR `DiagnosticReport`. A credencial final é canonizada e assinada utilizando o padrão `BbsBlsSignature2020`. Esta escolha criptográfica é crucial, pois permite que a carteira derive Provas de Conhecimento Zero (ZKPs) — revelando ao verificador apenas o laudo, omitindo dados sensíveis periféricos.

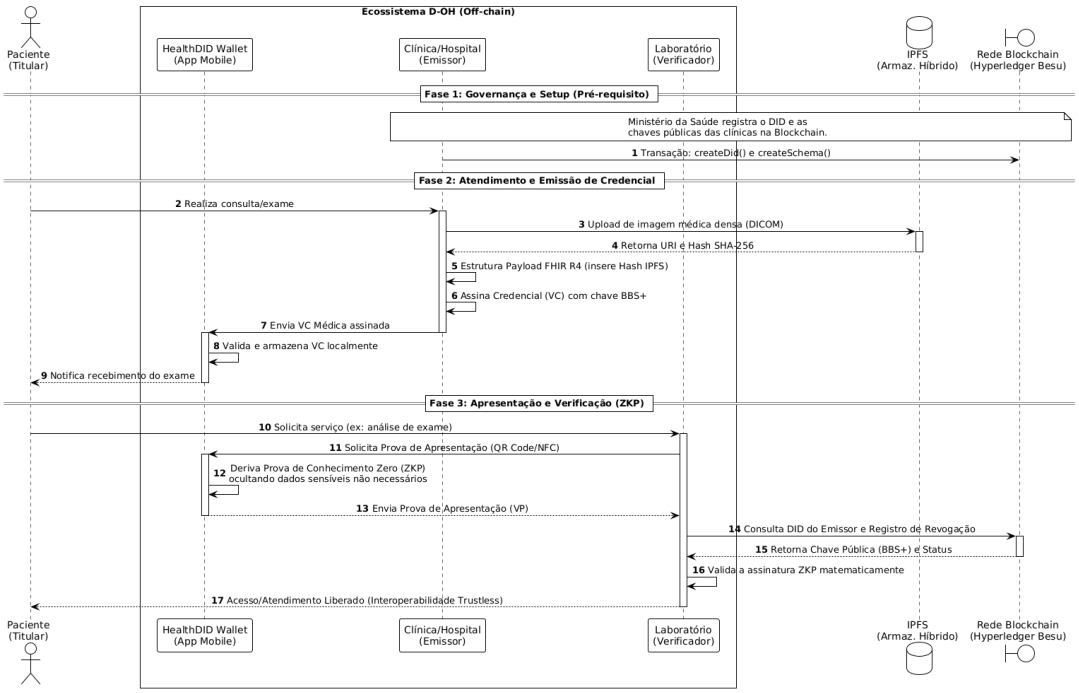

Figura 1. Visão geral da D-OH, projetada para provimento de serviço de openhealth descentralizada.

4. Avaliação de Desempenho e Resultados

Para atestar a viabilidade prática do D-OH, uma Prova de Conceito (PoC) foi executada em contêineres Docker, utilizando o *Aries Cloud Agent Python* (ACA-Py) para a gestão das carteiras e uma rede *Hyperledger Besu* avaliada via *Hyperledger Caliper*.

4.1. Custo Transacional e Latência

A avaliação diferenciou as operações de registro institucional (*on-chain*) da etapa de verificação de exames (*off-chain*). Conforme consolidado na Tabela 1, operações pesadas como o provisionamento (`createDid`, `createSchema`) apresentam latência e custos associados de *gás* mais altos, mas ocorrem tipicamente em *background* ou de forma singular no ciclo de vida da credencial.

Em contrapartida, o fluxo crítico do paciente no momento do atendimento médico (Verificação da VC) possui custo financeiro zero e latência de rede mínima, uma vez que a validação ZKP é integralmente *off-chain* ($\sim$18.5 ms).

Tabela 1. Custo quantitativo e latência por etapa no D-OH.

Etapa (Cadeia / Operação)	Frequência	Custo (Gas)	Latência
Registro de Emissor (`createDid`)	Única	$\sim$682k	Alta ($\sim$4s)
Definição FHIR (`createSchema`)	Única	$\sim$1.13M	Alta ($\sim$5s)
Revogação (`createRevocation`)	Baixa	$\sim$150k	Média ($\sim$3s)
Verificação ZKP (*Off-chain*)	**Alta**	**Zero**	**Baixa ($<$20ms)**

4.2. Eficiência de Armazenamento

O uso da arquitetura híbrida provou-se essencial para a escalabilidade móvel. A injeção direta (*inline*) de uma imagem de 15 MB em Base64 gerou Credenciais Verificáveis

superiores a 20 MB, causando instabilidades de sincronização. Com a adoção do IPFS atrelado ao FHIR, o *payload* da mesma credencial reduziu-se para cerca de 2.5 KB (redução superior a 99%), garantindo a fluidez da *HealthDID wallet*.

5. Conclusão e Trabalhos Futuros

O modelo *Decentralized-OpenHealth* (D-OH) valida a viabilidade de um prontuário eletrônico soberano para o Brasil. Ao unir Identidade Descentralizada, assinaturas BBS+ (ZKP) e ontologias FHIR sob a governança do Ministério da Saúde, a proposta garante interoperabilidade sem violar a LGPD.

A avaliação confirmou que o desacoplamento entre armazenamento denso (IPFS) e âncoras criptográficas (*Hyperledger Besu*) confere escalabilidade ao sistema. Como trabalhos futuros, planeja-se integrar mecanismos de tutela digital para dependentes e viabilizar a interoperabilidade de credenciais FHIR emitidas via dispositivos IoT médicos (*wearables*).

6. Agradecimentos

Os autores agradecem o apoio dado a este trabalho, pelo MCTI-Ministério da Ciência, Tecnologia e Inovação, com recursos financeiros do FUNTTEL e administrados pela FINEP, no âmbito do projeto 5G SAÚDE - Segurança, privacidade, inclusão e qualidade na telemedicina no contexto da Web 3.0, Cotação FT_01.23.0468.00, Referência 0844/23.

Referências

Houtan, B., Hafid, A. S., and Makrakis, D. (2020). A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access*, 8:90478–90494.

Phuyal, S., Bhandari, M., Bista, R., and Ferreira, J. C. (2026). Enabling cross-institution health data sharing in norway: Eudi wallets, on-chain consent, and openehrfhir translation. *IEEE Access*, 14:20309–20327.

Spanakis, E. G., Kung, A., Gyrard, A., Jimenez, D., Rabrait, C., and Sakkalis, V. (2025). Scalable, standards-driven tools for self-sovereign identity and data protection in healthcare clinical decision systems*. In *2025 IEEE International Conference on Imaging Systems and Techniques (IST)*, pages 1–5.

Valavan, P. M., Qurashi, S. N., Sobia, F., Harahsheh, F., Surendran, S., and Mary, S. S. C. (2024). Decentralized identity management using blockchain for healthcare systems. In *2024 IEEE Silchar Subsection Conference (SILCON)*, pages 1–6. IEEE.