Segurança de Dados Distribuída em Saúde Digital: Identidade Auto Soberana, Controle de Acesso e Registros de Logs baseados em *Blockchain*

Yago de R. dos Santos[1], Guilherme N. N. Barbosa[1], Lucio Henrik A. Reis[1], Nicollas R. de Oliveira[1], Ana Carolina R. Mendes[1], Dianne S. V. Medeiros[1], Diogo M. F. Mattos[1]

[1] LabGen/MídiaCom – TET/IC/PPGEET/UFF
Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

Abstract. *The expansion of Digital Health brings increasing data privacy and security challenges, especially due to data collection by service providers and third parties. The decentralized approach of Self-Sovereign Identity emerges as a solution, offering users direct control over their data. This paper extends the SmartMed tool by investigating the use of the Ethereum and Besu blockchain platforms to control access to medical data. The proposal integrates smart contracts to control access and maintain activity records, highlighting the detailed analysis of performance on both platforms with different consensus protocols. The results reveal the superiority of the Besu platform in relation to Ethereum, indicating a lower computational cost per transaction. This proposal innovates by proposing a system based on smart contracts to guarantee the authenticity of medical data, complemented by the use of Keycloak in managing access to healthcare systems.*

Resumo. *A expansão da Saúde Digital traz desafios crescentes de privacidade e segurança de dados, especialmente devido à coleta de dados por parte de provedores de serviço e terceiros. A abordagem descentralizada da Identidade Auto Soberana surge como solução, oferecendo controle direto aos usuários sobre seus dados. Este artigo estende a ferramenta SmartMed, investigando o uso das plataformas de* blockchain *Ethereum e Besu para controle de acesso a dados médicos. A proposta integra contratos inteligentes para controlar o acesso e manter registros de atividades, destacando-se pela análise detalhada do desempenho nas duas plataformas com protocolos de consenso distintos. Os resultados revelam a superioridade da plataforma Besu em relação à Ethereum, indicando um custo computacional inferior por transação. Esta proposta inova ao propor um sistema baseado em contratos inteligentes para garantir a autenticidade dos dados médicos, complementado pelo uso do Keycloak na gestão de acesso aos sistemas de saúde.*

1. Introdução

Em 2023, houve uma expansão significativa da Saúde Digital no Brasil, com mais de 1,4 mil municípios adotando programas de telessaúde e registrando mais de 950 mil

Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ e RNP e Prefeitura de Niterói/FEC/UFF (Edital PDPA 2020).

telediagnósticos, além de um aumento expressivo no número de exames registrados na Rede Nacional de Dados em Saúde (RNDS), atingindo a marca de 70 milhões de exames somente naquele ano[1]. No entanto, à medida que o cenário da internet evolui em direção à Web 3.0, as preocupações com a privacidade e segurança dos dados tornam-se mais prementes, especialmente em relação à coleta e exploração de dados dos usuários por diversas entidades, incluindo provedores de serviços de Internet (ISPs) e plataformas de terceiros [Popa et al., 2023]. A falta de transparência nas práticas de tratamento de dados e o potencial de exploração sem consentimento do usuário destacam a necessidade de estruturas robustas de gestão de identidade. Em resposta a esses desafios, tecnologias descentralizadas como *blockchain* oferecem soluções promissoras, fornecendo armazenamento e mecanismos de transação seguros e transparentes. No entanto, a aplicação específica dessas tecnologias na área da saúde introduz complexidades adicionais, especialmente na definição e gestão de identidades distribuídas em espaços federados de dados de saúde [Sahi et al., 2023].

Os sistemas tradicionais de identidade de saúde, normalmente centralizados e de propriedade do provedor de Identidades, criam identidades redundantes de pacientes em diferentes sistemas, dificultando a consolidação e a interoperabilidade de dados. O surgimento da Identidade Auto Soberana (SSI) através de tecnologias descentralizadas apresenta uma mudança de paradigma, capacitando os indivíduos com controle total sobre os seus dados pessoais e permitindo o compartilhamento seletivo. No contexto dos cuidados de saúde, a SSI oferece uma abordagem segura e descentralizada à verificação e autorização de identidade, concedendo aos pacientes e aos prestadores autoridade direta sobre as reivindicações de identidade. Aproveitando a *blockchain*, a SSI garante armazenamento e gerenciamento seguro de dados, preservando a privacidade do paciente e permitindo o compartilhamento seguro de dados entre partes autorizadas. No entanto, persistem desafios na integração do SSI nos sistemas de saúde existentes e na garantia da conformidade com os regulamentos de privacidade, como a *General Data Protection Regulation* (GDPR), destacando a necessidade de estruturas de gestão de identidade inovadoras e interoperáveis, adaptadas ao domínio dos cuidados de saúde [Spanakis et al., 2023].

Este artigo expande o escopo da ferramenta SmartMed [Santos et al., 2023] e investiga as implicações da utilização das plataformas de *blockchain* Ethereum e Besu no controle de acesso a dados médicos. Foram desenvolvidos contratos inteligentes para regulamentar o acesso e manter registros de atividades (logs) de sistemas médicos em ambas as plataformas de *blockchain*. Esses ambientes foram integrados à ferramenta SmartMed, permitindo uma avaliação abrangente de seu desempenho. As contribuições principais deste estudo incluem: (i) uma análise detalhada do desempenho dos contratos propostos nas plataformas Ethereum e Besu; e (ii) a incorporação de contratos inteligentes, conforme proposto pelo HyperLedger Indy, para facilitar a provisão de Identidade Auto Soberana em um autenticador KeyCloak. Para tanto, foi elaborado um produto mínimo viável da ferramenta SmartMed, integrando o autenticador às duas plataformas de *blockchain*. Os resultados demonstram que a plataforma Besu apresenta um desempenho superior em relação à Ethereum, com um custo computacional inferior por transação.

Trabalhos anteriores exploram o uso da tecnologia *blockchain* em aplicações médicas, enfocando o compartilhamento seguro de Registros Médicos Eletrônicos

[1]Disponível em `https://www.gov.br/saude/pt-br/assuntos/balanco-2023`.

(EMRs). Soluções comerciais, como o Medicalchain [Albeyatt, 2018], oferecem controle de dados médicos aos usuários, mas não abordam o acesso multinível. Propostas acadêmicas, como AuditChain [Anderson, 2018], FHIRChain [Zhang et al., 2018] e Ancile [Dagher et al., 2018], implementam contratos inteligentes para controle multinível, porém enfrentam desafios como custos elevados e complexidade. Este trabalho propõe um sistema baseado em contratos inteligentes na *blockchain* para garantir a autenticidade dos dados médicos, usando o Keycloak para gerenciar o acesso aos sistemas de saúde.

O restante do artigo está organizado da seguinte forma. A Saúde Digital é abordada na Seção 2. A Seção 3 discute os trabalhos relacionados. A Seção 4 aborda os principais desafios e oportunidades para controle de acesso utilizando *blockchain*. Na Seção 5, é apresentado a arquitetura da solucao proposta. A Seção 6 apresenta os resultados. A Seção 7 conclui o artigo.

2. Desafios de Privacidade e Identificação para a Saúde Digital Distribuída

A digitalização de dados, sobretudo pessoais, vem se tornando um dos principais desafios relacionados à segurança. Com a pandemia do COVID-19, foi necessário acelerar o processo de digitalização de dados médicos, através de registros médicos eletrônicos. Diversas legislações abordam esse tema, tais como a Lei Geral de Proteção de Dados (LGPD) e a *General Data Protection Regulation* (GDPR). Esses dados possuem características distintas dos demais dados pessoais, uma vez que são considerados sensíveis por ambas as legislações. Nos Estados Unidos, por usa vez, existe a *Health Insurance Portability and Accountability Act* (HIPAA), uma legislação específica para dados de saúde. A HIPAA fornece diretrizes para coleta, armazenamento e transmissão das informações de saúde protegidas (*Protected health information - PHI*) por meio de tecnologia, mas carece de detalhes práticos de implementação de medidas de segurança [Shah e Khan, 2020]. Em todos os casos, existe uma necessidade de garantir que as informações, sejam resguardadas de violações, isto é, que não sejam vazadas, sobretudo para fins comerciais. A rastreabilidade do compartilhamento de dados pessoais é uma tarefa extremamente desafiadora de se praticar, uma vez que os dados podem circular por uma variedade de ferramentas sem deixar registros, e muitas vezes sem o conhecimento ou consentimento do proprietário dos dados. Esse fluxo indiscriminado afeta diretamente a privacidade dos indivíduos. Nesse contexto, as leis que regulam a proteção de dados tornaram-se vitais para atribuir responsabilidades, contudo, carecem de mecanismos técnicos robustos para garantir seu efetivo cumprimento.

Os dados de saúde digital são armazenados digitalmente através dos Registros Médicos Eletrônicos (*Electronic Medical Records* - EMRs) e, normalmente, estão distribuídos através de silos de dados, resultando em informações fragmentadas [Tuler De Oliveira et al., 2022]. A diversidade de registros e a fragmentação criam desafios no processamento desses dados [Telenti e Jiang, 2020], além de dificultar a garantia da privacidade, tornando praticamente impossível detectar possíveis violações. Juntamente com as preocupações relacionadas à privacidade, o particionamento dos dados pode resultar na duplicação e perda de dados. Além disso, existem desafios técnicos e tecnológicos para o controle de acesso a dados de pacientes a partir de unidades de saúde remotas. Em alguns casos, existe uma cultura interna às unidades de saúde de compartilhamento indevido de credenciais de acesso entre profissionais de uma mesma equipe, o que propicia a construção de um ambiente no qual os registros de atividades (*logs*) de

acesso não são confiáveis e dificulta a auditoria. Outro fator importante é que em diversos hospitais o controle de acesso a dados de pacientes é baseado em papéis (*Role Based Access Control* - RBAC) [Xu et al., 2023], o que propicia que médicos, que não estão em atendimento a um paciente, tenham acesso às suas informações privadas do prontuário.

Nos Estados Unidos, a *Office of the National Coordinator for Health Information Technology* (ONC) é a entidade do governo responsável por coordenar os esforços para implementar e utilizar tecnologias aplicadas a dados de saúde. Foram propostas diretrizes e regulamentos para garantir que o acesso aos dados médicos seja controlado, abordando questões de segurança e privacidade. Dentre os regulamentos, um deles é responsável pela Verificação e Autenticação de Identidade, na qual a autenticação do paciente desempenha um papel crítico nas instituições de saúde, visando preservar os dados e evitar fraudes [Sookhak et al., 2021]. Utilizar tecnologias computacionais para controlar o acesso aos dados é essencial devido ao cenário complexo da privacidade dos registros médicos e às exigências cada vez mais rigorosas das legislações. Um dos principais desafios enfrentados pela instituições de saúde é garantir que o acesso aos dados seja concedido apenas a profissionais autorizados, baseado em um determinado contexto. No entanto, o principal objetivo de um sistema EMR é disponibilizar os dados do paciente e, portanto, o controle de acesso não deve impedir solicitações legítimas no melhor interesse do paciente [de Oliveira et al., 2023]. Nesse sentido, torna-se indispensável a existência de um sistema de controle de acesso confiável, auditável e distribuído para acesso aos dados. A tecnologia *blockchain* implementa mecanismos de segurança que garantem a imutabilidade, o não repúdio, a integridade e a auditabilidade do acesso aos registros médicos eletrônicos.

No cenário da saúde digital, a gestão das identidades assume um papel cada vez mais crucial. Os sistemas tradicionais de identidade, muitas vezes centralizados e controlados por entidades governamentais ou privadas, apresentam diversas limitações que suscitam crescentes preocupações, especialmente em relação à privacidade e segurança no acesso aos dados associados às credenciais. O controle centralizado e a falta de interoperabilidade entre sistemas de identidade diferentes agravam essas preocupações. A Identidade Autos Soberana (*Self-Sovereign Identity* - SSI) surge como um paradigma alternativo, oferecendo aos indivíduos um controle sem precedentes sobre seus dados pessoais e autonomia inigualável na forma como os compartilham [Galdi et al., 2021]. A SSI se diferencia dos sistemas tradicionais de identidade ao se basear em princípios inovadores em relação ao controle do usuário, descentralização de gerenciamento da identidade e credenciais criptograficamente verificáveis.

A implementação em larga escala da SSI pode trazer diversos benefícios para a sociedade, em especialmente para sistemas de saúde. No contexto de saúde digital, um dos maiores benefícios da SSI é colocar o controle dos dados nas mãos dos indivíduos, permitindo que eles decidam quais informações compartilhar e com quem. Isso protege a privacidade individual e reduz o risco de roubo de identidade e outras formas de fraude [Siqueira et al., 2023]. No âmbito da segurança, a natureza descentralizada da SSI a torna mais resistente a ataques cibernéticos e fraudes de identidade, protegendo informações valiosas contra acessos não autorizados. As credenciais criptograficamente verificáveis garantem a autenticidade e confiabilidade das identidades, dificultando a falsificação ou manipulação de dados. A SSI promove um ambiente digital mais seguro

para todos os usuários [Galdi et al., 2021].

Devido à sua natureza descentralizada e maior controle por parte do usuário, a implementação da Identidade Auto Soberana em sistemas de saúde enfrenta desafios significativos [Shuaib et al., 2023], que precisam ser cuidadosamente considerados para garantir a segurança, privacidade e eficiência. Embora o objetivo principal da adoção de identidades auto soberanas seja empoderar os pacientes com controle total sobre suas informações de identidade, há obstáculos a superar. Nos modelos centralizados tradicionais, os provedores de serviços de saúde são responsáveis pela proteção da privacidade dos pacientes, mas isso requer confiança total dos pacientes nos provedores. Além disso, esses modelos podem ser suscetíveis a perda de dados e violações de segurança. A SSI baseada em *blockchain* oferece uma solução potencial, permitindo que os pacientes controlem suas informações e garantindo sua segurança. No entanto, ainda há incertezas sobre a definição e aplicação precisas da SSI, bem como desafios técnicos na implementação eficaz, como a identificação descentralizada e a interoperabilidade. Para avançar na adoção da SSI no setor da saúde, é crucial resolver essas questões e garantir conformidade com regulamentações de privacidade, como a LGPD no Brasil, a GDPR na Europa e as definições da ONC nos EUA.

3. Trabalhos Relacionados

A utilização da tecnologia *blockchain* em aplicações médicas tem ganhado destaque, especialmente pela sua capacidade de gerar evidências computacionais irrefutáveis e armazená-las de forma distribuída. Essa característica é particularmente valiosa em soluções de compartilhamento de Registros Médicos Eletrônicos (*Electronic Medical Records* - EMRs), em que a rastreabilidade dos dados acessados é crucial. Nesse cenário, várias soluções baseadas em *blockchain* são propostas na literatura e algumas estão disponíveis comercialmente, como a solução Medicalchain [Albeyatt, 2018].

Essa solução usa *blockchain* para desenvolver aplicativos médicos que permitem aos usuários controlar seus dados médicos e optar pelo compartilhamento com profissionais qualificados. São utilizados *tokens* para gerenciar o acesso aos dados. A plataforma **Medicalchain**[2] implementa duas cadeias de blocos. A primeira é usada para controle de acesso aos dados médicos e é construída utilizando a plataforma HyperLedger Fabric. A geração dos *tokens* é responsabilidade da segunda *blockchain*. Medicalchain utiliza para esse fim o ERC20 (*Ethereum Request for Comments 20*) da plataforma Ethereum. A distribuição dos *tokens* é controlada por um contrato inteligente armazenado na *blockchain* Ethereum. Não há armazenamento de dados nos blocos da cadeia. Essa solução não conta com acesso multinível.

A proposta **AuditChain** fornece controle de acesso multinível para pacientes, médicos, enfermeiros e administradores hospitalares para o gerenciamento de EMRs [Anderson, 2018]. A proposta implementa contratos inteligentes utilizando a plataforma HyperLedger Fabric [Rebello et al., 2019, Agrawal et al., 2022]. A assinatura digital da transação usa criptografia de chave pública e serve como um *token* virtual para controle de acesso. Contudo, por utilizar a chave pública, está sujeito ao alto custo de processamento. Zhang *et al.* propõem o FHIRChain, uma arquitetura baseada em *blockchain* que incorpora o padrão HL7 FHIR *Fast Healthcare Interoperability Resources* (FHIR)

[2]Disponível em `https://medicalchain.com/en/`.

para dados clínicos compartilhados [Zhang et al., 2018]. O controle de acesso é realizado por meio de contratos inteligentes na rede pública Ethereum, garantindo maior disponibilidade. No entanto, o uso da rede pública implica custos monetários para a execução do contrato. A **Ancile**, desenvolvida por Dagher *et al.*, é uma *blockchain* baseada em Ethereum usada para gerenciar registros médicos. Ela emprega contratos inteligentes para controlar o acesso e proteger os dados, mantendo os registros nos bancos de dados existentes dos provedores [Dagher et al., 2018].

Em um trabalho anterior, foi proposta a SmartMed, uma ferramenta baseada em contratos inteligentes em uma *blockchain* privada para controlar o acesso a dados médicos distribuídos, promovendo interoperabilidade e conformidade com regulamentos de privacidade [Santos et al., 2023, Tuler De Oliveira et al., 2022]. Os contratos inteligentes garantem segurança e rastreabilidade nas transações de acesso aos dados confidenciais e realiza a integração com sistemas de prontuário eletrônico através do protocolo OAuth2.0. Contudo, a SmartMed foca somente no controle de acesso de dados médicos através de uma *blockchain* privada Ethereum. Este trabalho estende o sistema de controle de acesso amparado por contratos inteligentes da SmartMed, provendo suporte à plataforma Besu, com foco na garantia da autenticidade e não refutabilidade dos eventos de acessos a dados médicos. Ademais, este trabalho também propõe a integração de contratos inteligentes para a realização de Identidades Auto Soberanas no autenticado KeyCloak. Diferentemente dos trabalhos relacionados, o sistema proposto provê um controle de acesso aos dados médicos dos pacientes com alto nível de refinamento, registros de atividades (*logs*) não refutáveis e a integração com a plataforma de Identidade Auto Soberana HyperLedger Indy.

4. *Blockchain* para Controle de Acesso

A tecnologia de cadeia de blocos (*blockchain*) é composta por dois elementos. O primeiro representa uma estrutura de dados para encadeamento de blocos e o segundo, uma rede par-a-par (*peer-to-peer* - P2P) capaz de armazenar as transações de modo ordenado e distribuído [de Oliveira et al., 2023]. A Figura 1 apresenta uma ilustração do funcionamento da *blockchain*. Um dos principais propósitos dessa tecnologia é garantir segurança e resiliência em ambientes nos quais não há confiança mútua entre os participantes da rede, permitindo remover a entidade central que garante a confiança entre as partes [Oliveira et al., 2024]. A *blockchain* tem como característica intrínseca a garantia da integridade dos dados nela armazenados, não havendo possibilidade de remover ou alterar esses dados. Outras propriedades características da *blockchain* são a garantia de transparência e rastreabilidade das informações. Os dados armazenados são acessíveis para todos os participantes da rede par-a-par. Dessa forma, não é recomendado o armazenamento de dados sensíveis não criptografados.

No que diz respeito à taxonomia, as redes de *blockchain* podem ser classificadas como públicas ou privadas, além de serem classificadas em permissionadas ou não permissionadas. O permissionamento define os papéis que os nós podem assumir na rede. Em redes não permissionadas todos os nós possuem o mesmo papel, assumindo as mesmas responsabilidades. Já nas redes permissionadas, nós podem ter papéis distintos e esse papel depende da identificação do nó na rede. A classificação entre pública e privada determina quais nós podem compor a rede par-a-par. Na rede **pública** não existe permissionamento e qualquer nó pode ingressar na rede, fornecendo uma parte de seu poder com-

putacional. A rede pública se caracteriza por ser altamente descentralizada e apresenta diversos desafios relacionados à segurança, pois é possível que nós maliciosos ingressem na rede. Pelo fato de ser pública, a falha em qualquer um dos nós não causa problemas na geração de blocos. Por outro lado, nas cadeias de bloco **privadas** existe controle de acesso à rede, o que resulta em uma rede mais restritiva e controlada. De acordo com essas categorias, as redes de *blockchain* podem ser classificadas em: **Redes Públicas Não Permissionadas**, que não exigem controle de acesso e todos os nós podem gerar novos blocos, havendo uma exigência de mecanismos de consenso mais robustos; **Redes Privadas Não Permissionadas**, que possuem controle de acesso, porém, todos os nós exercem as mesmas funções; **Redes Privadas Permissionadas**, que possuem restrição quanto ao acesso à rede e existem diferenças de funções entre os nós, sendo os nós chamados de mineradores os responsáveis por gerar blocos e participarem do consenso.

As soluções baseadas em *blockchain* tendem a apresentar alta disponibilidade devido ao fato de que todos os nós que participam da rede possuem as mesmas informações, ou seja, uma réplica idêntica da *blockchain*, não havendo, portanto, ponto único de falha. Se um nó ficar inoperante, as informações ainda podem ser acessadas através dos demais nós. Para garantir que as réplicas da *blockchain* sejam idênticas, é necessário aplicar mecanismos de validação e consenso. Uma vez que os blocos da cadeia são compostos por uma sequência de transações a serem executadas, é necessário que um consenso seja alcançado pelos nós e que uma concordância seja estabelecida com relação às transações inseridas no bloco, bem como com a ordem de execução. O processo de validação e ordenação das transações em blocos é conhecido como mineração, uma responsabilidade dos nós mineradores. O mecanismo de consenso utilizado na rede estabelece regras capazes de validar e difundir as transações e blocos, resolvendo potenciais conflitos entre os dados trafegados. Uma vez alcançado o consenso, garante-se a integridade e a imutabilidade da informação.

Entre os principais mecanismos de consenso utilizados em cadeias de blocos no setor de saúde, encontram-se: a Prova de Trabalho *(Proof-of-Work – PoW)*, a Prova de Participação *(Proof-of-Stake – PoS)* e a Prova de Autoridade *(Proof-of-Autorith – PoA)*. **PoW** é um dos principais algoritmos de consenso em cadeias de bloco. Possui sua fundamentação em uma competição entre mineradores através de uma lógica probabilística. Os mineradores, como participantes da rede, buscam resolver desafios criptográficos complexos para registrar transações selecionadas em blocos adicionados à *blockchain*. A resolução dos desafios demanda uma abordagem de força bruta, resultando na descoberta de um valor numérico conhecido como *nonce* criptográfico. O *nonce*, em conjunto com as transações selecionadas, é incorporado ao bloco candidato para subsequente validação pela rede. Esse processo garante segurança ao sistema, uma vez que cada bloco é verificado por múltiplos nós antes de ser aceito como parte integrante da *blockchain*. **PoS** é um mecanismo de consenso, no qual, diferentemente do PoW, o sucesso da mineração de um bloco depende da participação dos nós na rede. Os nós competem entre si para encontrar o valor de resumo criptográfico que seja menor ou igual a um valor alvo, permitindo-lhes minerar um novo bloco. No entanto, a dificuldade de determinar esse resumo criptográfico é inversamente proporcional à riqueza acumulada (conhecida como *coin age*) do nó. A riqueza acumulada é calculada como a quantidade de recursos detidos pelo nó multiplicada pelo período em que o nó manteve esses recursos. Dessa forma, o nó com maior riqueza acumulada terá uma probabilidade maior de validar os próximos

blocos. O **PoA** é um mecanismo de consenso majoritariamente utilizado em redes privadas. Nesse mecanismo, uma entidade central é designada para nomear um conjunto específico de nós com autoridade. Esses nós são responsáveis por gerar novos blocos e validar transações. A inclusão de qualquer bloco na cadeia requer a validação e assinatura por pelo menos um nó com autoridade. A descentralização da rede é assegurada pela necessidade de consenso entre os nós de autoridade em relação ao estado global da cadeia. Para mitigar conflitos e otimizar o uso de recursos, algumas plataformas implementam um esquema rotativo de geração de blocos, garantindo a cada nó de autoridade, um intervalo de tempo exclusivo para realizar essa tarefa.

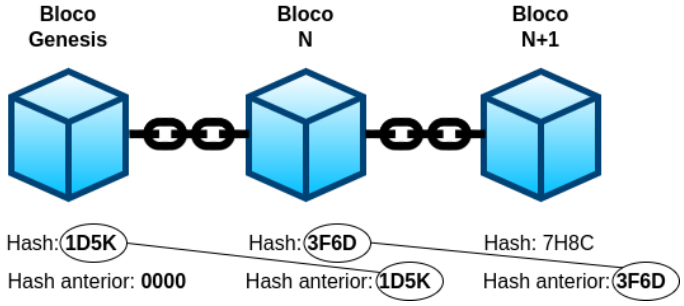


Figura 1. Estrutura da *blockchain*.

Por fim, os contratos inteligentes (*smart contracts*) são aplicações autoexecutáveis armazenadas na *blockchain*. Inicialmente introduzidos na plataforma Ethereum, transformam cláusulas de contratos reais em código e são acessíveis por meio de um endereço conhecido por todos os participantes da rede. Dentro de um contrato inteligente estão as regras acordadas entre as partes, que tornam a violação computacionalmente proibitiva e não vantajosa para potenciais partes maliciosas. Ao contrário dos contratos não determinísticos, que enfrentam dificuldades de consenso devido à aleatoriedade, os contratos inteligentes são naturalmente determinísticos [Mattos et al., 2018].

5. Arquitetura Proposta de Controle de Acesso e *Logs* Verificáveis

A arquitetura proposta visa solucionar desafios relacionados à segurança de registros médicos eletrônicos, implementando controle de acesso a dados médicos distribuídos com regras refinadas e robustas. A Figura 2 apresenta a arquitetura proposta para o sistema. As entidades de saúde interagem com o sistema por meio de uma interface habilitada com OAuth 2.0, solicitando acesso aos dados armazenados em uma base de dados distribuída. As entidades de saúde são representadas por diversos elementos de software de saúde que demandam autenticação e controle de acesso, tais como registros médicos eletrônicos ou ferramentas para a realização de teleconsultas. O protocolo OAuth 2.0 é usado para garantir a interoperabilidade entre sistemas distintos. Esse protocolo permite que usuários concedam a um aplicativo cliente o direito de acessar um sistema ou recursos de terceiros, sem compartilhamento das credenciais do usuário. Para isso, o protocolo usa um *token* de acesso, que representa a autorização para acessar o sistema ou os recursos em nome do usuário. Esse protocolo pode ser implementado por aplicações de EMR, utilizadas pelos usuários para solicitar acesso a dados distribuídos.

As solicitações de acesso são intermediadas pelo sistema proposto, que autoriza ou não o acesso a partir do resultado de interações realizadas com um contrato inteligente que executa na *blockchain*. O sistema implementa o Controle de Acesso Baseado

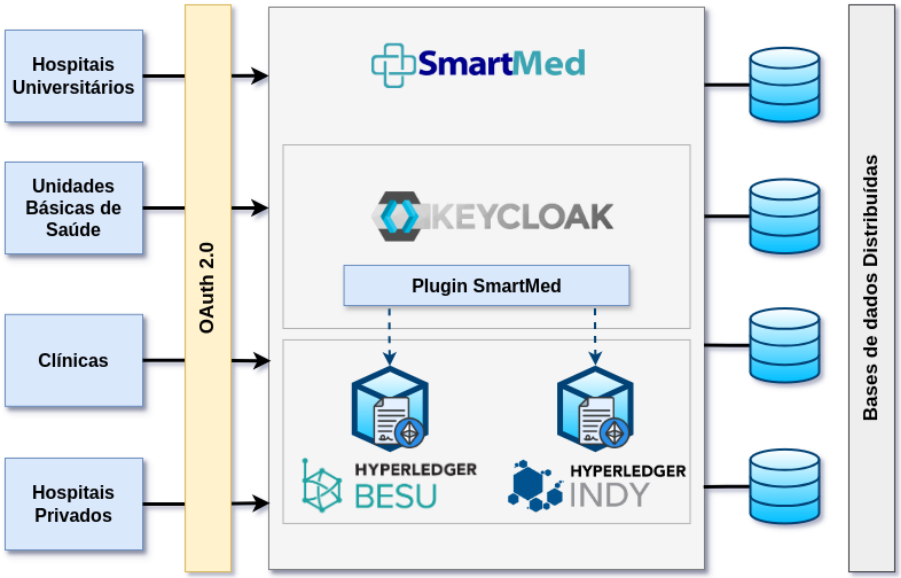


Figura 2. Arquitetura do sistema proposto. Usuários nas entidades de saúde solicitam acesso a bases de dados distribuídas por meio de aplicativos habilitados para OAuth 2.0. As solicitações são intermediadas pelo sistema proposto que determina a autorização de acesso de acordo com o resultado da interação com o contrato inteligente que executa na *blockchain* HyperLedger Besu. Todas as solicitações de acesso negadas e autorizadas, são registradas na *blockchain* de forma imutável.

em Atributos (*Attribute-Based Access Control* - ABAC), que utiliza o conceito ontológico 5W1H (*who, what, where, why, when, and how*) para que as decisões de acesso sejam determinadas a partir da avaliação dos atributos associados ao sujeito solicitante, ao acesso requerido, à operação desejada e, potencialmente, a fatores de contexto da requisição. Ao executar o contrato inteligente, os atributos da solicitação são avaliados e o sistema retorna um *token* de acesso que deve ser consumido para acessar de fato os dados.

Todas as solicitações de acesso são armazenadas em uma *blockchain*, formando um registro auditável e imutável. O sistema proposto implementa duas cadeias de blocos. A primeira executa sobre a plataforma HyperLedger Besu e todas as transações de autorização de acesso são registradas nessa *blockchain*, garantido assim a rastreabilidade do acesso. A segunda *blockchain* executa sobre a plataforma HyperLedger Indy que tem como responsabilidade a gestão de Identidade Auto Soberana, garantindo aos usuários controle total sobre suas informações.

O sistema proposto integra autenticação, autorização e registro de atividades (*logs*) com as cadeias de blocos por meio de *plugin* para o autenticador KeyCloak [3]. O *plugin* desenvolvido estende Keycloak, um software de código aberto para gerenciamento de identidade e de acesso, possibilitando a interação com o contrato inteligente armazenado na *blockchain*. As principais funcionalidades do *plugin* são: (i) encaminhar eventos de *log* específicos para a rede; (ii) encaminhar eventos de solicitação de autorização ou controle de acesso para um contrato inteligente responsável pela avaliação da solicitação; e (iii) receber e interpretar as respostas das transações, devolvendo-as ao Keycloak.

A implantação do sistema em hospitais universitários ou qualquer outra instituição de saúde, possibilita que toda a movimentação de dados médicos, armazenados local ou

[3]Disponível em `https://www.keycloak.org/`.

remotamente, seja centrada no paciente e registrada na rede de forma imutável. O sistema proposto permite também o acompanhamento visual do fluxo de solicitações de acesso através de painéis interativos e possibilita a edição de políticas adaptadas ao perfil de acesso de cada instituição.

6. Resultados Experimentais

Este artigo avalia a viabilidade do sistema proposto por meio da comparação do uso de duas implementações de cadeias de blocos para realizar o controle de acesso e o registro de *logs*. São criadas duas redes de *blockchain* privadas: uma baseada na plataforma HyperLedger Besu e outra, na plataforma Ethereum. Os experimentos são realizados em um notebook equipado com 16 GB de RAM e processador Intel Core i7-10510U, executando o sistema operacional Ubuntu 22.04.4.

A *blockchain* HyperLedger Besu implementa o IBFT 2.0 (*Istanbul Byzantine-fault-tolerant* 2.0), um protocolo de consenso de prova de autoridade (PoA). Já a *blockchain* Ethereum é implementada utilizando o algoritmo de prova de trabalho (PoW) *Ethash* para o consenso. Ambas as redes iniciam com o mesmo bloco *genesis* e são configuradas com quatro nós interconectados. As redes recebem os contratos inteligentes da ferramenta SmartMed [Santos et al., 2023] que incluem as funcionalidades de registro de atividades (*logs*) e uma política simples de controle de acesso que verifica se o endereço de e-mail do requerente pertence a um domínio preestabelecido.

A Figura 3 mostra o esquema do ambiente de testes. Além de configurar a *blockchain*, o sistema proposto conta com uma aplicação *web* de teste para avaliar o *plugin* SmartMed criado para o *Keycloak*. Essa aplicação utiliza o Python 3 e a biblioteca Django 3.2 para o desenvolvimento. A aplicação de teste inclui uma API REST protegida por um *middleware* executada diretamente no Django. O *middleware* intercepta chamadas para a API REST e constrói uma requisição de acesso, aderindo aos padrões do *Keycloak*, incluindo as informações do *token* de autenticação OAuth 2.0 do usuário, a operação solicitada, tais como leitura ou escrita, e o recurso desejado. Esses dados são enviados para o *Keycloak*, que os encaminha para a política correspondente na *blockchain*. Após a avaliação pela política, o resultado é retornado ao *middleware*, que concede ou nega o acesso ao recurso com base na resposta do *Keycloak*. O *middleware* atua como um

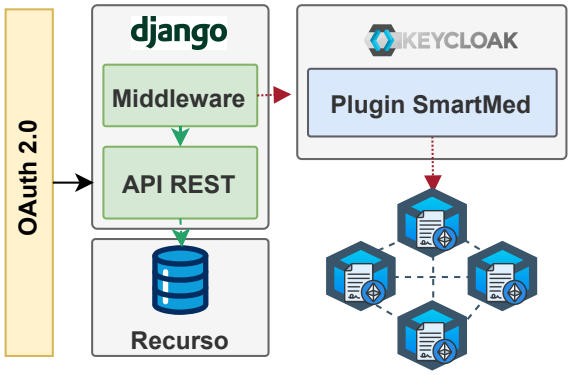
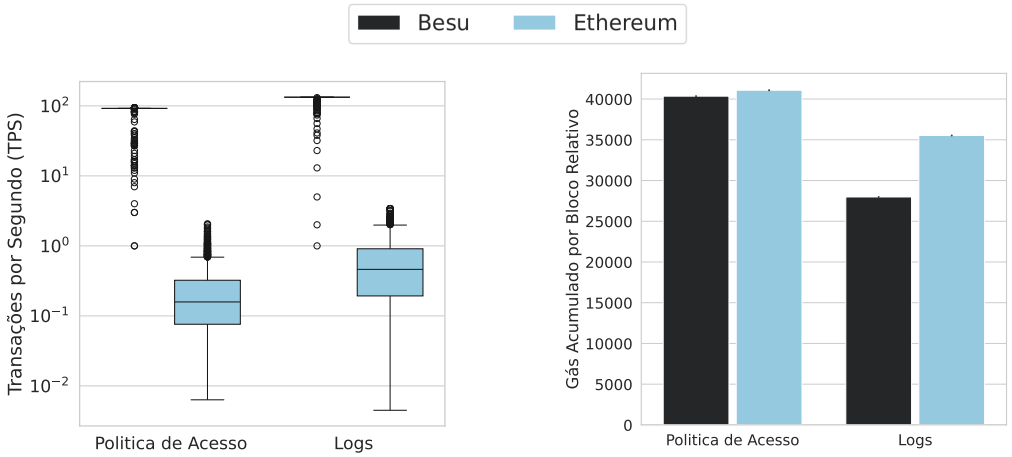


Figura 3. Esquema do ambiente de teste do sistema proposto com uma aplicação *web* baseada na biblioteca Django. O *middleware* direciona solicitações à API REST com informações de autenticação do usuário para o Keycloak, que as envia para um contrato inteligente na *blockchain*. Após avaliação, o *middleware* concede ou nega acesso ao recurso conforme a resposta do Keycloak.



(a) Transações por Segundo (TPS) na execução das funções de controle de acesso e registro de *logs* nos contratos inteligentes.

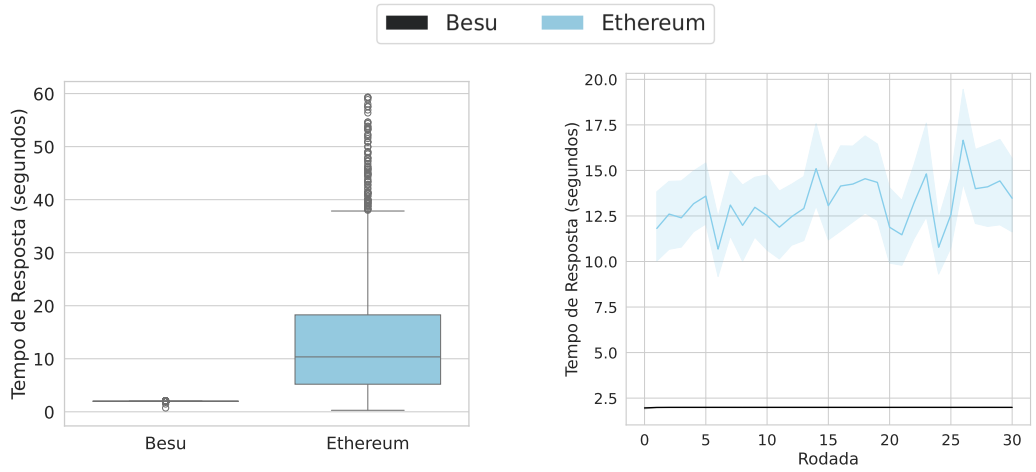
(b) Proporção de gás acumulado por bloco em relação ao número de transações em um bloco.

Figura 4. Desempenho dos contratos inteligentes de política de acesso e registro de *logs*. a) A plataforma Besu teve desempenho, em média, 100 vezes maior que o Ethereum. b) A Plataforma Besu também apresenta menor custo computacional por bloco para operações de registro de *logs*.

gateway para a API, conhecido como *Policy Enforcement Point* (PEP) no padrão XACML utilizado pelo Keycloak. Esse *middleware* intercepta as requisições de acesso aos recursos na API REST e as encaminha ao Keycloak para validação.

O primeiro teste se concentra na avaliação de desempenho das plataformas Ethereum e HyperLedger Besu para a execução de contratos inteligentes em uma rede permissoinada. Avalia-se o número de transações por segundo (*Transactions Per Second* - TPS) e o gás consumido por bloco relativo. O consumo de gás consumido por bloco relativo é a proporção de gás acumulado por bloco em relação à quantidade de transações por bloco. O experimento executa diretamente as funções da política de acesso e de registro de atividades (*logs*) utilizando chamadas JSON-RPC 2.0 para a *blockchain*. A função da política de acesso é testada com o auxílio da biblioteca *Faker*, gerando 9 mil endereços de e-mail bem formados e agrupando-os aleatoriamente com mil instâncias do e-mail correspondente ao domínio esperado pela política, aumentando a desordem e representando um cenário dinâmico. Para a função de registro de atividades, são criadas 10 mil instâncias aleatórias de *logs* seguindo a mesma lógica. As chamadas para as funções são executadas em rajadas de 5 mil requisições sequenciais, e o código de avaliação armazena todos os recibos das transações antes de reiniciar o teste.

O teste é repetido 30 vezes e os resultados são apresentados na Figura 4 com um intervalo de confiança de 95%. Para ambas as funções, a Figura 4(a)mostra que o número médio de transações por segundo na *blockchain* HyperLedger Besu é maior do que na *blockchain* Ethereum. Além disso, a distribuição no HyperLedger Besu é menos dispersa do que no Ethereum, indicando um cenário mais previsível e próximo de um valor constante. Na Figura 4(b), o gás acumulado por bloco relativo na função da política de acesso está muito próximo do limite de gás estipulado para as redes, indicando que ambas as plataformas têm um custo similar para essa função. Por outro lado, a função de *log* apresenta um custo computacional menor no HyperLedger Besu.



(a) Tempo de Resposta (TR) em segundos, da requisição de acesso a um recurso no Besu e no Ethereum.

(b) Tempo de Resposta (TR) em segundos por rodada de execução dos testes.

Figura 5. Desempenho no tempo de resposta da requisição de um recurso. a) A plataforma Besu possui um tempo de resposta de aproximadamente 2 s, e a Ethereum, 10 s. b) O comportamento ao longo do tempo explicita o caráter determinístico do comissionamento das transações na Besu.

O segundo experimento avalia o desempenho de ambas as plataformas no controle de acesso da aplicação de teste. Nesse cenário, são criadas quatro contas de acesso no *Keycloak* para haver variabilidade nas requisições. Mil requisições sequenciais são enviadas para a aplicação utilizando o *token* de acesso de uma das quatro contas previamente autenticadas e selecionadas aleatoriamente a cada requisição. O tempo de resposta de cada requisição é registrado e o experimento é repetido 30 vezes. A Figura 5 apresenta os resultados do experimento com um intervalo de confiança de 95%. A Figura 5(a) mostra o tempo de resposta para cada plataforma, evidenciando que a implementação baseada na plataforma HyperLedger Besu, que utiliza o protocolo de consenso de prova de autoridade IBFT 2.0, mantém um comportamento estável e aproximadamente constante, com tempos de resposta em torno de 2 s. Por outro lado, a abordagem baseada em Ethereum, com protocolo de consenso de prova de trabalho *Ethash*, apresenta grande variação, com uma média em torno de 10 s. Na Figura 5(b), o comportamento estável da HyperLedger Besu é novamente evidenciado, enquanto a abordagem da Ethereum mostra uma grande variação ao longo do tempo, sem indicação de estabilidade.

Os resultados dos experimentos fornecem informações importantes sobre o desempenho das plataformas de *blockchain* avaliadas. É notável a vantagem em utilizar o protocolo de consenso baseado em prova de autoridade em detrimento da prova de trabalho, especialmente em termos de estabilidade e consistência dos resultados. Enquanto a HyperLedger Besu demonstra um comportamento mais previsível e constante, a Ethereum apresenta maior variabilidade, sugerindo desafios potenciais em escalabilidade. Além disso, os resultados indicam que PoA tende a oferecer tempos de resposta mais rápidos em comparação com PoW, destacando seu potencial para aplicações com respostas em quase tempo real. Essas avaliações fornecem uma base sólida para a compreensão do desempenho das diferentes plataformas de *blockchain* e orientam as decisões futuras na evolução e implementação dos sistemas de controle de acesso baseados em *blockchain*.

7. Conclusão

Esse artigo investigou o potencial da tecnologia *blockchain* para gerenciar o acesso aos dados médicos, fornecer uma plataforma confiável para armazenar registros de atividades (*logs*) e estabelecer uma identidade auto soberana na área da Saúde Digital. Para tanto, o artigo estendeu a ferramenta SmartMed e desenvolveu um protótipo de sistema de controle de acesso integrado ao autenticador KeyCloak. A análise do protótipo revelou que a *blockchain*, especialmente amparada pela plataforma HyperLedger Besu, oferece segurança, imutabilidade, auditabilidade e privacidade dos dados de saúde a um custo computacional viável para a sua aplicação. A implementação do sistema, integrado à ferramenta SmartMed e à plataforma de Identidade Auto Soberana HyperLedger Indy, traz diversos benefícios, como o controle dos pacientes sobre seus dados, segurança e privacidade aprimoradas, interoperabilidade e conformidade regulatória com a LGPD e GDPR. Trabalhos futuros visam explorar outros mecanismos de consenso, estratégias de integração com sistemas existentes e avaliar o impacto na qualidade do cuidado.

Referências

Agrawal, D., Minocha, S., Namasudra, S. e Gandomi, A. H. (2022). A robust drug recall supply chain management system using hyperledger blockchain ecosystem. *Computers in biology and medicine*, 140:105100.

Albeyatt, A. (2018). Medicalchain white paper 2.1. Relatório técnico, MedChain White Paper 2.1.

Anderson, J. (2018). Securing, standardizing, and simplifying electronic health record audit logs through permissioned blockchain technology. *UNTHRR*.

Dagher, G. G., Mohler, J., Milojkovic, M. e Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable cities and society*, 39:283–297.

de Oliveira, M. T., Verginadis, Y., Reis, L. H., Psarra, E., Patiniotakis, I. e Olabarriaga, S. D. (2023). Ac-abac: Attribute-based access control for electronic medical records during acute care. *Expert Systems with Applications*, 213:119271.

de Oliveira, N. R., dos Santos, Y. d. R., Mendes, A. C. R., Barbosa, G. N., de Oliveira, M. T., Valle, R., Medeiros, D. S. e Mattos, D. M. (2023). Padroes e soluçoes para armazenamento, compartilhamento e estruturaçao de dados em saúde digital: Privacidade, integraçao e desafios. *Sociedade Brasileira de Computação*.

Galdi, C., Soltani, R., Nguyen, U. T. e An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, 2021:8873429.

Mattos, D. M., Medeiros, D. S., Fernandes, N. C., de Oliveira, M. T., Carrara, G. R., Soares, A. A., Magalhães, L. C. S., Passos, D., Carrano, R. C., Moraes, I. M. et al. (2018). Blockchain para segurança em redes elétricas inteligentes: Aplicações, tendências e desafios. *Sociedade Brasileira de Computação*.

Oliveira, N. R. d., Santos, Y. d. R. d., Mendes, A. C. R., Barbosa, G. N. N., Oliveira, M. T. d., Valle, R., Medeiros, D. S. V. e Mattos, D. M. F. (2024). Storage standards and solutions, data storage, sharing, and structuring in digital health: A brazilian case study. *Information*, 15(1).

Popa, M., Stoklossa, S. M. e Mazumdar, S. (2023). Chaindiscipline - towards a blockchain-iot-based self-sovereign identity management framework. *IEEE Transactions on Services Computing*, 16(5):3238–3251.

Rebello, G., Camilo, G., Silva, L., Souza, L., Guimarães, L., Alchieri, E., Greve, F. e Duarte, O. (2019). Correntes de blocos: Algoritmos de consenso e implementação na plataforma hyperledger fabric. *Sociedade Brasileira de Computação*.

Sahi, N., Liang, A., Van Devanter, W., Oikonomou, K. e Zhang, P. (2023). Self-sovereign identity in semi-permissioned blockchain networks leveraging ethereum and hyperledger fabric. Em *2023 IEEE International Conference on Digital Health (ICDH)*, p. 315–321.

Santos, Y., Reis, L., Barbosa, G., Oliveira, N., Mendes, A., Valle, R., Medeiros, D. e Mattos, D. (2023). Smartmed: Uma ferramenta de controle de acesso a dados de saúde baseado em contratos inteligentes. Em *Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, p. 65–72, Porto Alegre, RS, Brasil. SBC.

Shah, S. M. e Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE Access*, 8:136947–136965.

Shuaib, M., Alam, S., Alam, M. S. e Nasir, M. S. (2023). Self-sovereign identity for healthcare using blockchain. *Materials Today: Proceedings*, 81:203–207.

Siqueira, A., Da Conceição, A. F. e Rocha, V. (2023). Performance evaluation of self-sovereign identity use cases. Em *2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, p. 135–144.

Sookhak, M., Jabbarpour, M. R., Safa, N. S. e Yu, F. R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. *Journal of Network and Computer Applications*, 178:102950.

Spanakis, E. G., Politis, I., Markakis, E., Papatsaroucha, D., Grammatopoulos, A. V., Bolgouras, V., Angelogianni, A., Xenakis, C. e Sakkalis, V. (2023). Towards building a self-sovereign identity framework for healthcare. Em *2023 45th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, p. 1–4.

Telenti, A. e Jiang, X. (2020). Treating medical data as a durable asset. *Nature Genetics*, 52(10):1005–1010.

Tuler De Oliveira, M., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F. e Olabarriaga, S. D. (2022). Smartaccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access*, 10:117836–117854.

Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X. e Deng, R. H. (2023). A secure emr sharing system with tamper resistance and expressive access control. *IEEE Transactions on Dependable and Secure Computing*, 20(1):53–67.

Zhang, P., White, J., Schmidt, D. C., Lenz, G. e Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, 16:267–278.