UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CIÊNCIA DA COMPUTAÇÃO

Thainan Vieira Junckes

Prescrições médicas auto-soberanas: Fortalecendo a segurança e a privacidade

Florianópolis
2023

Thainan Vieira Junckes

Prescrições médicas auto-soberanas: Fortalecendo a segurança e a privacidade

Trabalho de Conclusão de Curso submetido ao Curso de Graduação em Ciência da Computação do Centro Tecnológico da Universidade Federal de Santa Catarina como requisito para obtenção do título de Bacharel em Ciência da Computação.
Orientador: Maurício de Vasconcelos Barros
Coorientador: Jean Everson Martina, Dr.

Florianópolis
2023

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Junckes, Thainan Vieira
Prescrições médicas auto-soberanas : fortalecendo a segurança e a privacidade / Thainan Vieira Junckes ; orientador, Maurício de Vasconcelos Barros, coorientador, Prof. Dr. Jean Everson Martina, 2023.
91 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Tecnológico, Graduação em Ciências da Computação, Florianópolis, 2023.

Inclui referências.

1. Ciências da Computação. 2. Prescrição médica.. 3. Privacidade. 4. Blockchain. 5. Identidade auto-soberana. I. Barros, Maurício de Vasconcelos. II. Martina, Prof. Dr. Jean Everson. III. Universidade Federal de Santa Catarina. Graduação em Ciências da Computação. IV. Título.

Thainan Vieira Junckes

Prescrições médicas auto-soberanas: Fortalecendo a segurança e a privacidade

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Bacharel em Ciência da Computação e aprovado em sua forma final pelo curso de Graduação em Ciência da Computação.

Florianópolis, 29 de Novembro de 2023.

Prof. Lúcia Helena Martins Pacheco, Dra.
Coordenadora do Curso

Banca Examinadora:

Maurício de Vasconcelos Barros
Orientador
Universidade Federal de Santa Catarina

Jean Everson Martina, Dr.
Avaliador
Universidade Federal de Santa Catarina

Lucas Mayr de Athayde
Avaliador
Universidade Federal de Santa Catarina

Gustavo Zambonin
Avaliador
Universidade Federal de Santa Catarina

Dedico esse trabalho aos meus pais, Rosemari e Vanderlei,
que sempre acreditaram no meu potencial.

AGRADECIMENTOS

Agradeço os meus pais e irmã, pelo amor, incentivo e apoio incondicional nos momentos difíceis e compreenderem a minha ausência enquanto eu me dedicava à realização deste trabalho. Ao meu orientador, Maurício de Vasconcelos Barros, pelo empenho dedicado à elaboração deste trabalho. Ao Prof. Dr. Jean Everson Martina pela oportunidade na elaboração deste trabalho. Aos meus colegas de trabalho, que sempre me apoiaram na conclusão do curso em paralelo às atividades profissionais. E a todos aqueles que contribuíram, de alguma forma, para a realização deste trabalho.

“A tecnologia move o mundo.” - Steve Jobs

RESUMO

Nos últimos anos, o compartilhamento crescente de informações pessoais online se intensificou. Isso gerou preocupações sobre a segurança, a privacidade e a propriedade dos dados dos usuários. A virtualização também está levando à transição das identidades físicas para identidades digitais. O paradigma da Identidade Auto-Soberana, que possibilita ao usuário ser o verdadeiro dono de sua identidade e dos dados vinculados, pode ser utilizado para estudar essa questão. Uma série de termos fundamentais ligados ao tema, incluindo Identidade Auto-Soberana, Credenciais Verificáveis, Blockchain e Hyperledger, entre outros, são essenciais para compreender essa nova abordagem. Durante a pandemia, houve um aumento nas consultas médicas virtuais, destacando a importância das prescrições digitais e a necessidade de proteger a privacidade dos pacientes. Este trabalho se propõe a explorar a viabilidade e implicações da tecnologia de Identidade Auto-Soberana na gestão de dados de saúde, usando a emissão de prescrições médicas como estudo de caso.

Palavras-chave: Prescrição médica. Blockchain. Identidade auto-soberana. Privacidade.

ABSTRACT

In recent years, the increasing sharing of personal information online has intensified. This has raised concerns about users' security, privacy, and data ownership. Virtualization is also driving the transition from physical identities to digital identities. The Self-Sovereign Identity paradigm, which allows the user to be the true owner of their identity and linked data, can be used to study this issue. A series of fundamental terms linked to the topic, including Self-Sovereign Identity, Verifiable Credentials, Blockchain and Hyperledger, among others, are essential to understanding this new approach. During the pandemic, there has been an increase in virtual doctor consultations, highlighting the importance of digital prescriptions and the need to protect patient privacy. This work aims to explore the feasibility and implications of Self-Sovereign Identity technology in health data management, using the issuance of medical prescriptions as a case study.

Keywords: Prescription. Blockchain. Self-sovereign identity. Privacity.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A quantidade de informações pessoais compartilhadas online aumentou significativamente nos últimos anos. A combinação de redes sociais e internet móvel é onde muitos desses dados se originam. Nossas rotinas são cada vez mais vividas no mundo virtual, uma tendência que foi acelerada pela pandemia de Covid-19, que obrigou uma parcela da população a trabalhar, estudar e realizar consultas médicas à distância (SCHEFFER et al., 2022). Devido à esse rápido processo de virtualização provocado pela pandemia, por vezes, não houve tempo suficiente para adequar os sistemas a essa nova rotina. Dessa forma, embora a sociedade esteja mais conectada, está também mais exposta.

Nesse cenário, a privacidade dos dados dos usuários é um tópico de discussão. Por vezes, grandes corporações que adquirem dados de usuários o fazem de forma abusiva. A revelação, em 2018, de que o Facebook forneceu à empresa de dados Cambridge Analytica acesso irrestrito e não autorizado a informações de identificação pessoal de mais de 87 milhões de usuários desavisados é um bom exemplo disto (ISAAK; HANNA, 2018).

Para os cidadãos receberem mais garantias acerca de seus dados, em meados de 2020 entrou em vigor no Brasil a Lei Geral de Proteção de Dados (BRASIL, 2018). A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis. Também esclarece que todos os dados tratados, inclusive no meio digital, estão sujeitos à regulação. Além disso, a LGPD estabelece que não importa onde está localizada a organização ou o seu centro de dados: se há o processamento de informações sobre pessoas, a LGPD deve ser cumprida.

Durante a pandemia de Covid-19, cresceu o número de consultas médicas virtuais (Saúde Digital Brasil, 2022). Dessa forma, a emissão de prescrições digitais e a utilização dos dados anonimizados devem ser feitos de forma a respeitar a privacidade dos pacientes atendidos.

Prescrições médicas são documentos criados e emitidos por profissionais de saúde que que contém instruções específicas para o tratamento de um paciente (MARIA; SEBASTIãO, 2011). Tradicionalmente, as prescrições são feitas em papel, onde o médico escreve manualmente as informações necessárias, assina e carimba o documento. A prescrição em papel é entregue ao paciente, que pode levá-la a uma farmácia para obter os medicamentos prescritos. Esse tipo de prescrição ainda é o principal formato de prescrição. Porém, alguns problemas como ilegibilidade, identificação incorreta de medicamento e dosagem podem ocorrer (BABU; THIYAGARAJAN, 2021).

Com o avanço da tecnologia, as prescrições médicas também podem ser feitas de forma digital. Uma prescrição digital é um método em que se utiliza um dispositivo digital onde ocorre trocas de informações entres os envolvidos (ALDUGHAYFIQ; SAMPALLI, 2021). Nesse caso, o médico utiliza um sistema eletrônico de prescrição, onde as informações são inseridas em um software específico e transmitidas eletronicamente para a farmácia. Melhor comunicação entre os envolvidos, aumento da eficiência do processo e diminuição de erros de prescrição são algumas das suas vantagens (BABU; THIYAGARAJAN, 2021). Entretanto, a ameaça à privacidade

e segurança das informações dos pacientes é um fator a ser considerado. A possibilidade de hackers invadirem os sistemas e disponibilizarem esses dados é uma preocupação (MURUGESAN; SORWAR, 2010). Os dados médicos de um paciente são dados sensíveis, e precisam ser tratados de forma cuidadosa.

Com esse processo de virtualização, as identidades e documentos físicos, tradicionalmente em papel, estão sendo transferidas para uma versão digital, conhecida como identidade e documento digital. Um desses modelos de identidade digital é a Identidade Auto-Soberana, um paradigma de gerenciamento de identidade que busca permitir aos usuários possuírem e controlarem totalmente suas identidades digitais, um sistema centrado no usuário (MüHLE et al., 2018). Esse modelo pode ser utilizado em situações onde os dados pessoais são sensíveis, como dados de pacientes atendidos por médicos e farmacêuticos.

Uma forma comum de implementar Identidades Auto-Soberanas é em conjunto com a tecnologia Blockchain devido à sua descentralização, segurança, privacidade, controle do usuário e capacidade de interoperabilidade (FERDOUS; CHOWDHURY; ALASSAFI, 2019). Para isso, o projeto Hyperledger Indy é comumente utilizado. Esse projeto fornece uma infraestrutura robusta e interoperável para a criação de sistemas de identidade digital confiáveis, autônomos e descentralizados (PASTUCHOV; CURRAN, 2019).

Dessa forma, um arranjo que faça uso de Blockchain e Identidade Auto Soberana, é apropriado para o tipo de trato de dados necessários a um sistema de prescrição eletrônica. Lidando com dados sensíveis, o foco desse sistema seria na privacidade, com minimização de dados, tendo maior controle sobre a quantidade de exposição dos dados.

Utilizando a emissão de uma prescrição médica como caso de uso para a criação de um protótipo, este trabalho propõe investigar a viabilidade e implicações da tecnologia utilizada em sistemas de Identidade Auto-Soberana no manejo de dados de saúde.

1.1 OBJETIVOS

1.1.1 Objetivo geral

O objetivo geral desta proposta é realizar um estudo sobre o conceito e as tecnologias associadas ao paradigma da Identidade Auto-Soberana de forma a compreender o seu funcionamento e identificar seus pontos fracos, fortes, desafios e sua viabilidade para o trato de dados sensíveis.

1.1.2 Objetivos Específicos

- Pesquisar os conceitos e tecnologias associadas à identidade auto-soberana e prescrições médicas digitais;
- Implementar um protótipo para emitir e revogar prescrições médicas auto-soberanas com as tecnologias pesquisadas;

- Verificar a viabilidade do protótipo implementado;
- Documentar o processo e os resultados em um formato de apresentação de Trabalho de Conclusão de Curso.

1.2 METODOLOGIA

Buscando atender aos objetivos do trabalho, é utilizado uma abordagem mista de pesquisa teórica e desenvolvimento prático.

1.2.1 Pesquisa Teórica

- Revisão Bibliográfica: Foi realizado uma revisão narrativa da literatura sobre Identidade Auto-Soberana e prescrições médicas digitais. Fontes incluindo artigos acadêmicos, livros, relatórios técnicos, documentação de projetos open-source relevantes, e estudos de caso. Esta revisão visou compreender os conceitos fundamentais, as tecnologias envolvidas, e as tendências atuais nos campos de Identidade Auto Soberana e Prescrições Médicas Eletrônicas.
- Análise de Casos: Foram analisados casos de uso reais e hipotéticos de prescrições médicas digitais, em especial com uso de Blockchain, observando o manejo dos dados de saúde, com foco em entender como a Identidade Auto-Soberana pode ser aplicada para ampliar a privacidade desses dados. Esta análise ajudou a identificar os desafios, oportunidades e limitações práticas da tecnologia.

1.2.2 Desenvolvimento Prático

- Desenvolvimento de Protótipo: Baseado nas análises do casos de uso, e embasado pela revisão bibliográfica a respeito do tema, foi elaborado e implementado um protótipo com o objetivo de emitir e revogar prescrições médicas digitais. Este protótipo utilizou tecnologias associadas à Identidade Auto-Soberana, incluindo soluções Blockchain como o Hyperledger Indy e o Hyperledger Aries. O protótipo conseguiu com sucesso emitir prescrições auto soberanas.

1.2.3 Documentação e Apresentação

- Documentação do Processo: Todo o processo de pesquisa, desenvolvimento, e análise foi documentado. Isso inclui a metodologia adotada, tecnologias e as soluções encontradas.
- Preparação para Apresentação: Os resultados e descobertas foram consolidados em um formato apropriado para a apresentação de um Trabalho de Conclusão de Curso, incluindo relatórios escritos e materiais visuais.

1.3 JUSTIFICATIVA

Com a aceleração da digitalização provocado pela pandemia, o número de consultas e procedimentos realizados via telemedicina aumentou de forma rápida. Essa digitalização incluiu um avanço no uso de Prescrições Médicas Eletrônicas. As prescrições tradicionais em papel, são mais propensas a erros, interpretação equivocada e adulteração. Sua contraparte digital oferece maior controle sobre fraudes e erros. Porém, apesar desses sistemas serem importantes para a redução de erros, os dados de saúde sensíveis inseridos nesses sistemas, necessitam atenção quanto ao armazenamento e manoseio.

Muitas das abordagens de prescrições eletrônicas atuais são centralizadas (GARCIA et al., 2022), tornando-as mais vulneráveis a pontos únicos de falha e questionamentos quanto à privacidade e governança dos dados. Uma alternativa emergente é a adoção da tecnologia Blockchain, oferecendo uma maior afastamento de entidades controladoras únicas, além de segurança, integridade dos dados e aumentando a transparência do processo, assim como um possível redução de custos por meio de um compartilhamento entre os diversos nodos.

Porém esses sistemas ainda podem ser melhorados. O uso de dados de saúde salvos na Blockchain em contratos inteligentes, ainda que criptografados, representam um risco para a preservação futura desses dados. Perante a natureza imutável da Blockchain, esses dados criptografados podem ser salvos e decifrados em algum ponto no futuro. Além disso acaba sendo utilizado uma grande quantidade de processamento na Blockchain, assim como também o processamento para cifragem e decifragem dos dados no armazenamento e transmissão.

É notável que na literatura analisada exista uma falta de abordagens de prescrições eletrônicas com uso do paradigma de Identidades Auto Soberanas, que poderia abordar alguns desses problemas referentes à privacidade e armazenamento dos dados.

Dessa forma o presente trabalho amplia o debate sobre privacidade com o uso de um sistema de prescrição eletrônica com Blockchain e utilizando o paradigma de Identidade Auto Soberana. Um sistema de prescrição com maior privacidade e propriedade dos dados, beneficia o avanço e a transição desses documentos para o meio digital, sem comprometer o devido trato necessário a dados tão sensíveis como são os dados de saúde de indivíduo.

1.4 ORGANIZAÇÃO

Inicialmente é apresentado conceitos chaves que serão tratados, como identidades digitais e Auto-Soberana. Após, o trabalho passa por diversos temas apropriados à tecnologia abordada, como funções Hash, credenciais verificáveis, DIDs, entre outros. Na sequência são abordadas as tecnologias e ferramentas descobertas, como Blockchain, Hyperledger Indy e Hyperledger Aries. Por fim, é exposto a proposta e implementação realizada no presente estudo.

2 IDENTIDADES DIGITAIS

A ISO 24760-1 (ISO, 2019) define identidade digital como um “conjunto de atributos relacionados a uma entidade.”

Maliki e Seigneur (2007) conceituam a Identidade Digital como sendo a representação dessa entidade, vinculada a algum contexto específico (MALIKI; SEIGNEUR, 2007). Gerenciamento de Identidade, ou em inglês, *Identity and Access Management* (IAM), é definido como um conjunto de políticas, processos e tecnologias que auxiliam a identificar entidades e garantir o correto acesso a serviços e recursos.

Começando com o modelo básico e crescendo em vários estágios com a introdução de modelos adicionais, o cenário de gerenciamento de identidade evoluiu ao longo dos anos. É apresentado abaixo os principais modelos de gerenciamento de identidades conhecidos.

2.1 IDENTIDADE ISOLADA

Este modelo de identidade é o mais simples e mais comum, além de ter sido o primeiro criado (FERDOUS; CHOWDHURY; ALASSAFI, 2019). Nele, existem apenas duas partes envolvidas: o provedor de serviço, que possui seu próprio provedor de identidade, e o usuário. Cada provedor de serviço é responsável por fornecer ao usuário (cliente) seu identificador e sua credencial correspondente. Uma desvantagem, segundo Ferdous, Chowdhury e Alassafi (2019), é a necessidade de se autenticar em cada serviço, gerando um acúmulo de identidades de um mesmo usuário, pois cada provedor de serviço possui seu próprio domínio e as operações não são válidas em outros domínios.

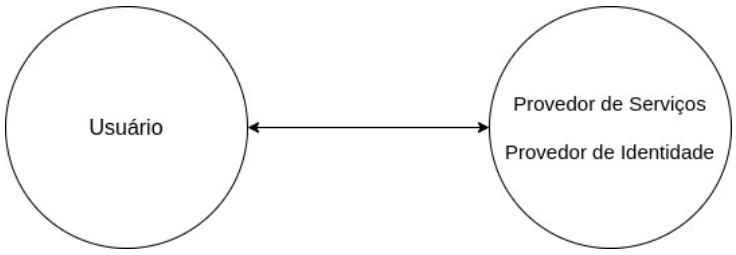


Figura 1 – Modelo de Identidade Isolada

Fonte: Inspirado em (SCHARDONG; CUSTóDIO, 2022)

2.2 IDENTIDADE FEDERADA

Neste modelo, cada domínio de identidade é composto por apenas um provedor de identidade e um ou mais provedores de serviço (FERDOUS; CHOWDHURY; ALASSAFI, 2019). O provedor de identidade emite os identificadores e as credenciais relacionadas ao usuário, e também, autentica o usuário e repassa seus atributos ao provedor de serviço, como

Figura 2 – Modelo de Identidade Federada

Fonte: Inspirado em (FERDOUS; CHOWDHURY; ALASSAFI, 2019)

mostrado na Figura 2. Depois que um usuário é autenticado, ele pode acessar os serviços de todos os provedores de serviços que compartilham o mesmo provedor de identidade. Assim que uma noção de confiança é estabelecida entre o provedor de identidade e o seu provedor de serviço relacionado, temos um domínio de identidade federada.

2.3 IDENTIDADE CENTRADA NO USUÁRIO

O modelo centrado no usuário é parecido com o anterior. Segundo Ferdous, Chowdhury e Alassafi (2019), nesse modelo, vários provedores de serviço podem compartilhar um único provedor de identidade, porém não é necessário haver uma noção de confiança entre as entidades. Sempre que um usuário tenta acessar um serviço através de um provedorde serviço, ele é encaminhado para o provedor de identidade solicitado, onde é feita a autenticação. Sem uma noção de confiança, as entidades neste modelo confiam umas nas outras. Por isso, esse modelo também é conhecido como modelo de confiança aberta. Alguns sistemas baseados no protocolo OAuth, como o Facebook, utilizam esse modelo (ALLEN, 2016).

2.4 IDENTIDADE AUTO-SOBERANA

A definição de identidade auto-soberana ainda é bastante discutida, como é possível ver em Allen (2016) e em Ferdous, Chowdhury e Alassafi (2019). Mas há algo em comum, neste modelo o usuário deve ter o controle total da sua identidade digital. Assim, o usuário tem autonomia para armazenar sua identidade onde queira e apresentar apenas quado necessário.

Christopher Allen propôs dez princípios para identidades auto-soberanas (ALLEN, 2016). Além dos autores citados anteriormente, outros autores como Schardong e Custódio (2021) e Mühle et al. (2018) usam esses princípios como referência na área.

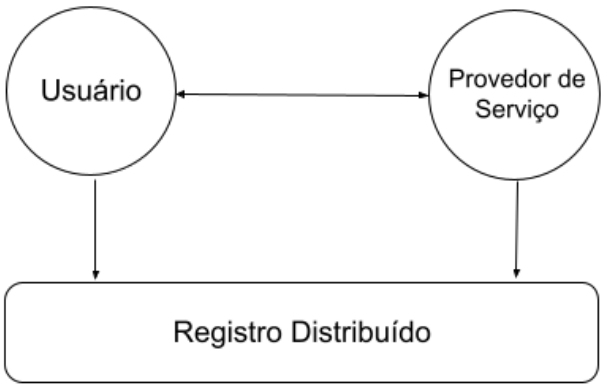
Os dez princípios são:

1. Existência: os usuários devem existir independente do provedor;
2. Controle: os usuários devem controlar suas identidades;
3. Acesso: os usuários devem ter acesso aos seus próprios dados;

4. Transparência: os sistemas devem ser aberto em como funcionam e são atualizados. Os algoritmos devem ser *open-source*;
5. Persistência: as identidades devem ser persistidas;
6. Portabilidade: informações e serviços sobre a identidade devem ser transportáveis;
7. Interoperabilidade: as identidades devem ser tão amplamente utilizáveis quanto possível;
8. Consentimento: os usuários devem concordar com o uso de sua identidade;
9. Minimização: sempre mostrar o mínimo possível de alguma informação necessária;
10. Proteção: os direitos dos usuários devem ser protegidos.

A tecnologia Blockchain possui em comum algumas das propriedades mencionadas por Allen. Segundo Nakamoto (2008), a Blockchain provê essencialmente um domínio descentralizado que não é controlado por nenhuma entidade específica, provendo independência e autonomia para a identidade. Além disso, os dados armazenados estão facilmente disponíveis para qualquer usuário autorizado (FERDOUS; CHOWDHURY; ALASSAFI, 2019). Utilizando o auxílio desta tecnologia, o usuário apresentaria sua credencial e caberia à parte verificadora conferir na Blockchain sua autenticidade, usando o registro distribuído como um agente de confiança, como mostrado na Figura 3.

Figura 3 – Modelo de Identidade Auto-Soberana



Fonte: Inspirado em (NAIK; JENKINS, 2020)

3 PRESCRIÇÕES MÉDICAS DIGITAIS

Uma prescrição médica é um documento escrito por um médico ou outro profissional de saúde, que contém instruções sobre o tratamento de um paciente (MARIA; SEBASTIãO, 2011). Essas instruções normalmente incluem os medicamentos a serem tomados, a dosagem, a frequência e a duração do tratamento. É um componente importante do cuidado de saúde, pois fornece informações detalhadas para o paciente, farmacêutico e outros envolvidos no tratamento. Ela ajuda a garantir que o paciente receba o tratamento adequado e seguro, levando em consideração fatores como a condição médica, histórico de saúde, idade e possíveis interações medicamentosas.

Geralmente, as prescrições são feitas em papel, onde o médico escreve as informações necessárias, assina e carimba a prescrição. Com a prescrição em mãos, o paciente entrega a uma farmácia de confiança para obter os medicamentos prescritos. Entretanto, segundo Babu e Thiyagarajan (2021), esse modelo físico possui algumas desvantagens. A prescrição muitas vezes é ilegível, gerando erros de interpretação. Erros como identificação incorreta do medicamento, dosagem e frequência de uso podem causar danos ao paciente (BABU; THIYAGARAJAN, 2021).

A evolução da tecnologia tem levado ao uso mais frequente de prescrições digitais (MEDICINAS/A, 2021). Segundo Aldughayfiq e Sampalli (2021), uma prescrição digital é um método em que se utiliza um dispositivo digital onde ocorre trocas de informações entres os envolvidos. Nesse modelo, o médico usa um sistema eletrônico de prescrição, onde insere as informações básicas no sistema que posteriormente transmite para a rede de farmácias.

A prescrição digital é mais difícil de ser manipulada, afirma Agrawal (2009), além de diminuir erros de prescrição dos medicamentos. Já Murugesan e Sorwar (2010), ressalta que a prescrição digital fornece uma melhor comunicação entre os envolvidos, aumento da eficiência de todo o processo e ajuda na diminuição de erros. Porém, a ameaça à privacidade e à segurança dos dados dos pacientes bem como a possibilidade de vazamento dos dados por hacker são algumas das limitações apontadas por Murugesan e Sorwar (2010).

Segundo Garcia et al. (2022), grande parte dos sistemas de prescrição digital em uso ainda são centralizados, o que significa que uma entidade centralizada mantém a autoridade sobre o sistema, tornando-o vulnerável a pontos únicos de falha. Além disso, toda a rede é interrompida caso este sistema central seja hackeado.

Com o auxílio da tecnologia Blockchain, é possível armazenar e gerenciar as informações das prescrições médicas de forma segura e confiável. Segundo Lim et al. (2018), o uso de Blockchain possui algumas vantagens como a segurança dos dados pois faz uso de criptografia avançada e distribuição descentralizada. Também permite rastrear todas as interações e transações relacionadas às prescrições, facilitando na redução de fraudes e erros.

Navaratna, Wijesinghe e Pilapitiya (2020) destaca que a utilização de Blockchain traz maior disponibilidade e transparência, pois os custos de manutenção podem ser divididos entre as entidades interessadas. Um alto nível de auditabilidade também pode ser alcançado, afirma

Navaratna, Wijesinghe e Pilapitiya (2020), devido ao fato do registro distribuído da Blockchain ser imutável.

4 PRINCIPAIS CONCEITOS

Para explicar melhor a abordagem do estudo e do protótipo, é apresentado a seguir uma breve introdução aos principais conceitos envolvidos: funções Hash, criptografia assimétrica e Blockchain. Assim como, assinaturas digitais e identidades descentralizadas.

4.1 FUNÇÕES HASH

As funções Hash são muito importantes na criptografia. Principalmente por garantir a integridade de um dado ou informação. Como toda função, cada elemento do seu domínio é mapeado para um elemento da sua imagem.

A função cria um resumo criptográfico único para cada entrada, que pode ser um texto ou arquivo. Além disso, uma pequena alteração resulta em um resumo completamente diferente. Porém, caso não haja alteração, o resumo sempre será o mesmo. Sendo assim, é possível garantir integridade da entrada.

Segundo Yaga et al. (2018), as funções Hash possuem três características importantes:

1. Resistência a pré-imagem: significa que a função é unidirecional, ou seja, é computacionalmente inviável calcular o valor de entrada correto dado algum valor de saída;
2. Resistência a segunda pré-imagem: dado uma entrada específica, é computacionalmente inviável encontrar uma segunda entrada que produz a mesma saída;
3. Resistência a colisão: não é possível encontrar duas entradas que resultem em uma mesma saída.

Na Blockchain as funções Hash são utilizadas para verificar a integridade dos dados. Um algoritmo comumente utilizado é o Secure Hash Algorithm de 256 bits, conhecido como SHA-256 (YAGA et al., 2018).

4.2 CRIPTOGRAFIA ASSIMÉTRICA

Segundo Oliveira (2012), a criptografia assimétrica utiliza duas chaves diferentes, uma pública e outra privada. A chave pública pode ficar disponível para qualquer usuário que deseja se comunicar com outro de maneira segura. Porém, a chave privada deve permanecer em posse apenas do usuário titular.

Segundo Stallings (2015), por meio dessas duas chaves, torna-se viável executar operações criptográficas complementares, como encriptar e decriptar, ou assinar e verificar.

Uma mensagem cifrada com a chave pública só pode ser decifrada com a chave privada. Por outro lado, uma mensagem cifrada com a chave privada poderá ser decifrada por todos que possuem a chave pública, sabendo assim o autor da mensagem (OLIVEIRA, 2012).

4.3 ASSINATURAS DIGITAIS

Assinaturas digitais são mecanismos criptográficos usados para verificar a autenticidade, a integridade e a não repúdio de documentos eletrônicos, mensagens ou transações digitais (STALLINGS, 2015). Elas são baseadas em algoritmos criptográficos assimétricos e funções Hash.

O certificado digital faz a associação entre uma identidade e uma chave pública através de um documento assinado digitalmente por uma entidade responsável por emitir os certificados, a Autoridade Certificadora (STALLINGS, 2015).

Uma infraestrutura de chave pública é necessária para que os sistemas de assinaturas digitais baseadas em chaves assimétricas funcione com validade jurídica. No Brasil, existe a ICP Brasil. Essa infraestrutura é responsável por armazenar, gerenciar, distribuir e revogar os certificados digitais.

Segundo Stallings (2015), com a chave privada do assinante é feita a encriptação do valor de hash do documento, sendo esse hash cifrado a assinatura digital. Com a chave pública em mãos, pode-se decriptar o texto cifrado e obter o hash original da mensagem, garantindo assim autenticidade e integridade.

4.4 IDENTIFICADORES DESCENTRALIZADOS (DID)

Os identificadores descentralizados, também conhecidos como DID, são um tipo de identificador que permite identidades digitais verificáveis e descentralizadas. São projetados para permitir que indivíduos tenham controle sobre sua identidade digital e suas informações pessoais. O DID é um padrão aberto especificado pela W3C (SPORNY et al., 2022).

Conforme a Figura 4, um DID é um texto simples *string* que possui três partes (SPORNY et al., 2022):

1. esquema do DID;
2. método do DID;
3. identificador específico.

Figura 4 – Exemplo de estrutura do DID

Fonte: (SPORNY et al., 2022)

Os DIDs foram concebidos para operar de maneira independente de registros centralizados, provedores de identidade e autoridades certificadoras. Uma entidade pode possuir vários DIDs, cada um destinado a um relacionamento específico com outra entidade.

O DID é ligado a um documento DID e a uma chave verificadora. Um documento DID é um conjunto de dados em JSON que especifica, por exemplo, chaves públicas de uma entidade. Uma entidade costuma ser uma pessoa ou organização (SPORNY et al., 2022).

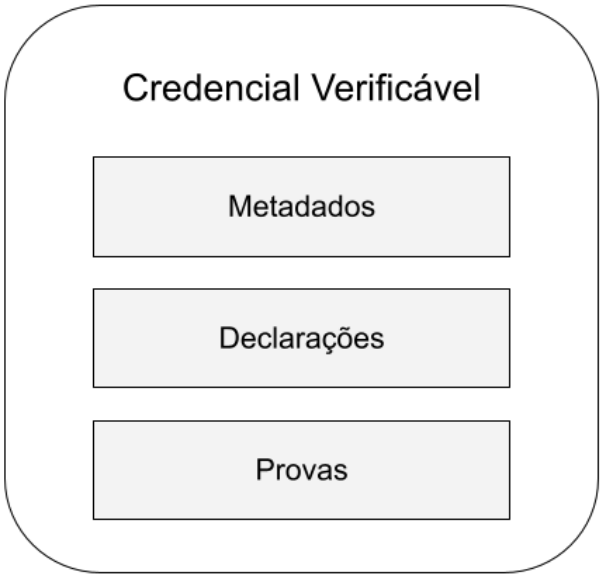
4.5 CREDENCIAIS VERIFICÁVEIS

Uma credencial verificável é, segundo Sporny, Longley e Chadwick (2022), uma estrutura de dados que representa informações sobre um assunto (pessoa, organização, entidade) e é emitida por uma entidade confiável.

Conforme representando na Figura 5, uma credencial verificável possui três partes: declarações, provas, metadados (SPORNY; LONGLEY; CHADWICK, 2022). A declaração possui informações sobre o titular da credencial. Provas são evidências criptográficas que comprovam a autenticidade da declaração. Essas provas são geradas pela entidade emissora da credencial, utilizando chaves criptográficas e algoritmos de assinatura digital. As provas permitem que terceiros verifiquem a integridade e autenticidade da credencial sem a necessidade de confiar na entidade emissora. Quando utilizadas em conjunto com DID e Blockchain, a confiaça pode ser recebida através do DID registrado na Blockchain. Os metadados descrevem propriedades como data de validade, emissor, chave pública etc.

As credenciais verificáveis são projetadas para serem compartilhadas de forma seletiva e controlada pelo titular da credencial. O titular pode apresentar sua credencial verificável a uma parte verificadora, que pode verificar a autenticidade e validade da credencial sem precisar entrar em contato direto com a entidade emissora.

Figura 5 – Estrutura de uma Credencial Verificável



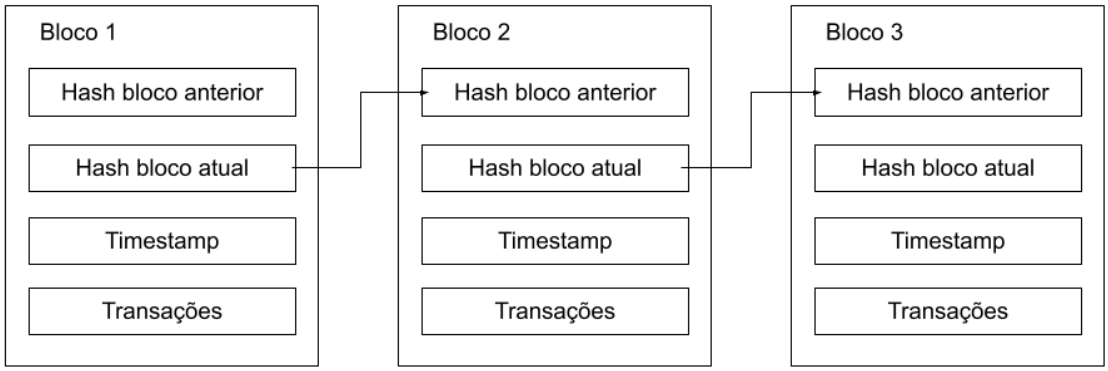
Fonte: Inspirado em (SPORNY; LONGLEY; CHADWICK, 2022)

4.6 BLOCKCHAIN

A tecnologia Blockchain é uma estrutura de dados distribuída e descentralizada que permite o registro e a validação de transações de forma segura. Ela consiste em blocos de informações interligados de forma imutável e cronológica. Esse conceito foi iniciamlmente proposto por Nakamoto em seu artigo sobre Bitcoin (NAKAMOTO, 2008).

Segundo Xu, Weber e Staples (2019), cada rede Blockchain é composta por uma *ledger*, podendo ser uma lista encadeada de blocos. Na *ledger*, cada bloco possui um conjunto de transações realizadas na rede, um valor hash, o endereço do bloco anterior e um *timestamp* que mostra o momento de criação do bloco. Assim, quando um dado precisa ser escrito, um protocolo de consenso é executado para alcançar acordo sobre o estado atual da *ledger* entre diferentes nós (ou participantes) na rede (XU; WEBER; STAPLES, 2019). A Figura 6 ilustra isso.

Figura 6 – Estrutura dos blocos da Blockchain



Fonte: Inspirado em (YAGA et al., 2018)

As redes de Blockchain podem ser públicas ou privadas em relação à validação. Na pública, qualquer usuário pode entrar e participar do processo de consenso e validação de blocos. Na privada, apenas usuários com autorização podem ler ou validar transações, a depender da escolha da autoridade controladora (YAGA et al., 2018).

Para prevenir ataques maliciosos em redes públicas, a tecnologia Blockchain faz uso de um mecanismo de consenso distribuído, onde os participantes da rede realizam um acordo coletivo sobre a veracidade das transações. Assim, não há dependência de uma autoridade central. Alguns exemplos desse mecanismo são o prova de trabalho (*proof of work*) e o prova de participação (*proof of stake*).

4.6.1 Prova de Trabalho (*Proof of Work*)

O *Proof of Work (PoW)* é o algoritmo de consenso mais antigo e também o mais utilizado nas redes Blockchain (LIM et al., 2018). Nele, os usuários da rede disputam entre si

para resolver problemas computacionais e matemáticos de alta complexidade. Esses problemas requerem uma alta quantidade de processamento e consomem bastante energia. Segundo Yaga et al. (2018), o usuário responsável por solucionar o problema, e consequentemente publicar o próximo bloco, costuma receber uma recompensa pelo trabalho.

Um exemplo de uso desse algoritmo é na rede do Bitcoin (NAKAMOTO, 2008). Lá é necessário executar a função Hash diversas vezes no cabeçalho do bloco e encontrar um resultado de hash com um determinado número de zeros no início. Porém, a cada 2016 blocos a dificuldade do problema é ajustada. Após encontrada a solução, o usuário envia o bloco para os outros usuários da rede, que por sua vez, adicionam esse novo bloco à sua cópia da Blockchain.

4.6.2 *Byzantine Fault Tolerant* (BFT)

O BFT é um protocolo de consenso distribuído para garantir que, mesmo na presença de nodos maliciosos o sistema possa funcionar corretamente e chegar a um consenso. Um tipo de protocolo de tolerância a falha bizantina chamada *Practical Byzantine Fault Tolerance* (PBFT) é utilizada pela Hyperledger Indy (NGUYEN; KIM, 2018).

Segundo Nguyen e Kim (2018), no PBFT, existem dois tipos de nós: um nó líder e alguns pares (nós) de validação; e esses pares executarão algumas rodadas para anexar um bloco à cadeia. Inicialmente, os clientes enviam suas solicitações de transações aos pares validadores correspondentes. A partir daqui, o par receptor validará as transações e depois as transmitirá para outros pares, incluindo o líder. Após o número de transações atingir um limite denominado tamanho do lote, ou após um intervalo, o nó líder ordenará as transações pelo horário de criação, colocando-as em um bloco. Posteriormente, são executadas três fases do PBFT. Primeiramente, na fase de pré-preparação, o líder transmite sua proposta de bloco para outros pares. Eles receberão e armazenarão o bloco localmente. Então, para ter certeza de que o bloco recebido do líder é o mesmo, eles fazem uma verificação dupla, transmitindo-o na fase Preparar e na fase Confirmar. Após a fase de Preparação, se algum nó receber os blocos iguais aos que armazenou localmente antes, de mais de 2/3 de todos os nós, ele executará a fase de Commit. Em seguida, o mesmo procedimento é registrado após a fase Commit, que é o requisito para qualquer nó executar as transações no bloco proposto e anexá-lo às suas cadeias atuais.

5 HYPERLEDGER INDY

Hyperledger Indy é um projeto de código aberto que faz parte da iniciativa Hyperledger, uma comunidade colaborativa liderada pela Linux Foundation, focada no desenvolvimento de tecnologias de blockchain para uso empresarial (FOUNDATION, 2015). Com o Hyperledger Indy é possível gerenciar identidades auto-soberanas baseadas em Blockchain.

5.1 REGISTRO DISTRIBUÍDO INDY

O Registro Distribuído Indy é formado por outros dois projetos: Indy-Plenum e Indy-Node. No Indy-Plenum é implementado o algoritmo de consenso. Já no Indy-Node é feita a implementação das transações relacionadas à identidade (SHCHERBAKOV, 2019).

O Indy-Plenum utiliza um algoritmo de consenso chamado Plenum Byzantine Fault Tolerant (BFT) (PASTUCHOV; CURRAN, 2019). Ele é projetado para ser altamente tolerante a falhas bizantinas, que são situações em que os nodos podem se comportar de maneira maliciosa, enviando informações falsas ou comprometendo a integridade da rede.

O Registro Distribuído Indy é público permissionado (SHCHERBAKOV, 2019). O acesso à leitura é aberto, porém é preciso permissão para escrever e validar as transações. Apenas dados públicos são escritos na Blockchain, como DIDs, chaves e esquemas de credenciais.

5.2 CONJUNTO DE NODOS (*NODE POOL)*

O Registro Distribuído possui dois conjuntos de nodos: *Validators* e *Observer*. Essa divisão de conjuntos permite uma maior flexibilidade na configuração da rede e na distribuição de funções (PASTUCHOV; CURRAN, 2019).

O conjunto *Validators* é composto por nodos que desempenham um papel ativo no processo de consenso e validação das transações. Esses nodos têm a responsabilidade de chegar a um acordo sobre a ordem e a validade das transações, garantindo assim a segurança e a integridade da rede. É aqui que o Indy-Plenum está implementado. Além disso, nesse conjunto, durante o processo de consenso, todos os nodos assinam em conjunto no momento da escrita. Essa assinatura serve para verificação de dados.

Segundo Pastuchov e Curran (2019), o conjunto *Observer* consiste em nodos que não participam diretamente do processo de consenso e validação das transações, mas acompanham e recebem atualizações da rede. Esses nodos desempenham um papel de observadores na rede, permitindo monitorar e verificar as transações sem a necessidade de realizar o trabalho intensivo de validação. Os nodos do *Observer* recebem cópias dos blocos validados pelos nodos do *Validators*.

5.3 TIPOS DE REGISTROS DISTRIBUÍDOS

O Hyperledger Indy possui quatro Registros: Config Ledger, Pool Ledger, Domain Ledger e Audit Ledger (HYPERLEDGER, 2018b).

5.3.1 Config Ledger

No Config Ledger ficam registrados informações sobre as validações de transações e políticas de autorização (HYPERLEDGER, 2018a). Todos os nodos devem conhecer em consenso sobre essas informações. Para isso, os nodos fazem a leitura desse Registro.

5.3.2 Pool Ledger

No Pool Ledger, as informações sobre o estado atual do Conjunto de Nodos são registradas (HYPERLEDGER, 2018a). Quem são os nodos e suas chaves públicas são algumas dessas informações. As transações são adicionadas nesse Registro, desde que envolva adição, remoção ou edição nos nodos.

5.3.3 Domain Ledger

O principal Registro é o Domain Ledger. Aqui ficam as transações específicas de identidade e de aplicação (HYPERLEDGER, 2018a). Para escrever no Registro, é imprescindível possuir uma identidade com permissão de escrita. Todavia, todas as informações relativas às identidades estão armazenadas no próprio Domain Ledger. Se o Registro estiver vazio, não é possível criar novas identidades, pois não há autorização para efetuar escritas no Registro.

5.3.4 Audit Ledger

O Audit Ledger é o Registro encarregado da sincronização entre as diversas Ledgers. Monitorando as outras Ledgers, ele organiza todas as transações de todos os registros em uma sequência que reflete ordenadamente todas as transações do sistema (HYPERLEDGER, 2018b). Esse Registro é fundamental para a recuperação do sistema, conduz auditorias externas e promove controle e coesão interna no sistema.

6 HYPERLEDGER ARIES

O Hyperledger Aries é um projeto da Hyperledger que visa fornecer uma infraestrutura e conjuntos de ferramentas para credenciais verificáveis (HYPERLEDGER, 2019a). O Hyperledger Aries também colabora com outros projetos e tecnologias relacionadas, como o Hyperledger Indy.

Ele fornece uma base para o desenvolvimento de aplicativos e soluções que envolvem identidade digital, interações ponto-a-ponto (*peer-to-peer*) e transações confidenciais. Também possui uma camada de interface para criar, assinar e ler transações na Blockchain.

6.1 ARIES AGENTS

Um agente é responsável por interagir com outras entidades. Segundo Curran (2021), uma instância de um agente possui duas partes: o agente em si e o controlador.

O agente lida com todas as funcionalidades principais do Aries, como interagir com outros agentes, gerenciar armazenamento seguro, enviar notificações de eventos e receber orientações do controlador. O controlador fornece a lógica de negócios que define como essa instância específica do agente se comporta, como responder a eventos no agente e quando acionar o agente para iniciar eventos (CURRAN, 2021).

6.2 DIDCOMM

O DIDComm (DID Communication) é um mecanismo de mensagens que permite a comunicação entre agentes Aries (HYPERLEDGER, 2021). Além disso, o DIDComm permite uma troca assíncrona e segura de mensagens encriptadas ponto-a-ponto.

O mecanismo emprega uma instância do método did:peer DID method, que utiliza DIDs não publicados na Blockchain, sendo usados exclusivamente de maneira privada entre os dois agentes que estão em comunicação.

Existem alguns protocolos padrões que estabelecem um conjunto de mensagens para executar uma tarefa específica:

- O protocolo “estabelecer conexão” permite dois agentes se conectarem através de algumas mensagens: convite, requisição de conexão e resposta da conexão;
- O protocolo “emitir credencial” permite um agente emitir uma credencial verificável para outro agente;
- O protocolo “revogar credencial” permite um agente revogar uma credencial verificável previamente emitida para outro agente.

7 SOLUÇÕES PARA IDENTIDADES AUTO-SOBERANAS BASEADAS NA BLOCKCHAIN

Neste capítulo serão abordadas outras soluções relevantes para Identidades Auto-Soberanas baseadas na Blockchain, tais como uPort, Sovrin e EverID.

7.1 UPORT

A uPort é uma solução de código-aberto baseada na Ethereum (PANAIT; OLIMID; STEFANESCU, 2020). Seu objetivo é fornecer uma identidade descentralizada. Uma identidade é criada pelo usuário por meio de um aplicativo móvel dedicado que armazena todos os dados de identidade do usuário, incluindo as chaves privadas usadas para assinar e compartilhar reivindicações. Depois que o usuário cria uma identidade, dois contratos inteligentes *controller* e *proxy* são automaticamente inseridos no Blockchain Ethereum.

Segundo Panait, Olimid e Stefanescu (2020), o contrato *proxy* referencia o endereço do contrato *controller*. As funções do *proxy* só podem ser executadas pelo *controller*. O endereço do *proxy* possui um identiicador uPort exclusivo do usuário. Um usuário pode criar vários identificadores não vinculáveis.

O mapeamento de atributos de identidade para um identificador específico é feito através da implementação de um contrato inteligente de registro. Este registo pode ser consultado por qualquer entidade, no entanto, apenas o seu proprietário pode atualizar os seus atributos. Como a Blockchain não é dedicada a armazenar grandes quantidades de dados, é feito o hash do JSON do atributo e depois armazenada no registro.

Segundo Dib e Toumi (2020), a principal limitação do uPort é a falta de portabilidade devido ao fato de apenas outras identidades do uPort serem capazes de certificar. A questão da interoperabilidade também é um problema, uma vez que é baseada na Ethereum.

Além disso, Dib e Toumi (2020) destaca que embora o processo de recuperação social permita recuperar a propriedade de um identificador comprometido ou perdido, o conjunto de administradores pode ser uma porta de ataque se decidirem conspirar contra um usuário. Se um aplicativo uPort for comprometido e a lista de administradores for alterada maliciosamente, o identificador será permanentemente comprometido.

Por último, pelo uPort ser baseado principalmente em contratos inteligentes, Dib e Toumi (2020) ressalta que um nodo malicioso na Blockchain pode rastrear e vincular todas as atividades relacionadas a um identificador. Assim, a verdadeira identidade do usuário, bem como, todas as ações associadas poderão ser conhecidas. Isto pode comprometer a privacidade dos usuários.

7.2 SOVRIN

A Sovrin é uma rede de identidade descentralizada de código aberto construída sobre uma *ledger* distribuída permissionada (SOVRIN, 2023). A Sovrin é pública no sentido de que qualquer pessoa pode enviar transações de leitura, porém, apenas instituições confiáveis podem ter nodos que participam do protocolo de consenso, assim o acesso de escrita é permitido apenas a esses nodos.

Na Sovrin são utilizados um aplicativo móvel e um agente para permitir interações entre o usuário e o resto da rede. Esses itens também ajudam os usuários a gerenciar chaves criptográficas. Por ter uma comunicação entre agentes sem depender da *ledger*, ela proporciona mais confidencialidade e privacidade.

Segundo Dib e Toumi (2020), o principal problema na Sovrin é a presença de instituições pré-definidas como *middlewares* entre o usuário e a *ledger*. Isso pode acarretar no acesso indevido à informações sobre a identidade dos usuários. Dib e Toumi (2020) também afirma que princípios da Identide Auto-Soberana como consentimento e proteção podem ser comprometidos. O uso e transações na Sovrin geram taxas.

7.3 EVERID

O EverID é um sistema de Identidade Auto-Soberana baseado em Blockchain (EVEREST,). Com ele é possível armazenar atributos de identidade e certificações. O EverID facilita o processo de verificação de identidade dos usuários e permite uma transferência segura de valor entre os membros da rede. Ele também utiliza contratos inteligentes para fornecer propriedade de dados pessoais, através dos quais o usuário controla como os atributos de identidade são compartilhados.

O usuário do sistema não precisa possuir um dispositivo móvel, pois o documento de identidade governamental, os dados biométricos e as certificações de terceiros podem ser armazenados na nuvem. Porém, Dib e Toumi (2020) afirma que o princípio de minimização não é totalmente respeitado. Quando uma informação de identidade é necessária para verificar uma reivindicação, o usuário não tem escolha a não ser divulgar todos os dados. O EverID também não é *open-source*, o que compromete o princípio de transparência de uma Identidade Auto-Soberana.

8 TRABALHOS CORRELATOS

Neste capítulo serão apresentados trabalhos correlatos que contemplam o estado da arte no que tange implementação de prescrições médicas digitais com o uso de Blockcahin.

8.1 A BLOCKCHAIN-BASED DATA GOVERNANCE WITH PRIVACY AND PROVENANCE: A CASE STUDY FOR E-PRESCRIPTION

O artigo (GARCIA et al., 2022) apresenta um *framework* de governança de dados descentralizado baseado em Blockchain e reencriptação de proxy para garantir a privacidade, gerenciamento de consentimento e proveniência de dados para prescrição digital. O *framework* ajuda o paciente a armazenar, gerenciar e compartilhar dados da prescrição com outras partes interessadas através de uma *tamper-proof ledger*. Também protege a privacidade dos pacientes armazenando dados de prescrição criptografados na *ledger*. Outra funcionalidade é o suporte à proveniência de dados, assim permite que os proprietários e consumidores de dados monitorem com eficiência os registros históricos dos dados e sua origem, incluindo quem acessou os dados e para quais finalidades.

A implementação usa CosmWasm para os contratos inteligentes e Tendermint para o consenso da Blockchain. Os resultados mostram que a arquitetura proposta pode proteger a privacidade dos proprietários de dados e governar o acesso a dados sensíveis com um mínimo de sobrecarga.

A proposta salva dados sensíveis de identificação de forma criptografada em contratos inteligentes na Blockchain.

8.2 A NEW BLOCKCHAIN-BASED ELECTRONIC MEDICAL RECORD TRANSFERRING SYSTEM WITH DATA PRIVACY

O artigo (LI, 2020) apresenta um sistema de prescrição médica baseado em Blockchain que pode fornecer processamento de prescrições digitais com armazenamento seguro, verificação de identidade e direitos de acesso. Além disso, o sistema adota o método de proteção k-anonimato baseado na privacidade diferencial no caso de emissão de prescrições eletrônicas, para que a segurança dos dados seja efetivamente melhorada, mantendo a privacidade dos dados.

O artigo também descreve um modelo de contrato inteligente para implementar o sistema de prescrições em uma Blockchain genérica. O modelo teria contratos de pacientes, contratos de médicos, contratos de pesquisadores e contratos de tratamento de casos. É utilizada a relação entre contratos para descrever a lógica estrutural do sistema na Blockchain, representando os dados a serem armazenados e os serviços que podem ser prestados em todo o sistema.

Os dados da prescrição são salvos em formato criptografado no contrato inteligente, sendo uma chave privada usada para descriptografar e acessar esses dados. Também é necessá-

rio o consentimento explícito do paciente para acessar seus dados.

8.3 A SECURE BLOCKCHAIN-BASED PRESCRIPTION DRUG SUPPLY IN HEALTHCARE SYSTEMS

O artigo (YING et al., 2019) apresenta uma proposta de arquitetura segura baseada em Blockchain para o fornecimento de medicamentos prescritos em sistemas de saúde. A proposta visa autenticar partes não confiáveis através do registro distribuído e proteger a privacidade do paciente com um modelo de identidade dinâmico, garantindo transações seguras de medicamentos. O trabalho salva dados de identificação de forma criptografada em contratos inteligentes.

O texto afirma que é resistente a vários tipos de ataques e fornece um serviço confiável pois emprega um protocolo de autenticação eficiente para validar a legitimidade do usuário, além de utilizar identidade dinâmica para proteger a anonimidade dos usuários. Além disso, a proposta emprega um controle de acesso baseado em função para garantir que apenas usuários autorizados possam acessar informações confidenciais. Uma análise de segurança presente no artigo mostra que o protocolo é resistente a ataques de falsificação de usuário e de comprometimento de banco de dados. O artigo não indica nenhuma Blockchain específica para sua implementação.

8.4 AUTHENTIC DRUG USAGE AND TRACKING WITH BLOCKCHAIN USING MOBILE APPS

O artigo (BENITA et al., 2020) discute o uso da tecnologia Blockchain no rastreamento do uso de medicamentos e na gestão da cadeia de suprimentos. A implementação da tecnologia Blockchain, especificamente por meio do uso de contratos inteligentes na rede Ethereum, aborda esses desafios.

Segundo o texto, o contrato inteligente ajuda a rastrear o movimento dos medicamentos desde o fabricante até o fornecedor, revendedor, farmácias e finalmente até os pacientes. Ele garante que apenas medicamentos autênticos sejam vendidos e que os pacientes possam comprar apenas medicamentos com uma receita válida de um médico autenticado.

O texto afirma que o sistema proposto é transparente, seguro e descentralizado, com dados armazenados de forma redundante em vários bancos de dados para garantir disponibilidade e imutabilidade. Além disso, é fornecido um pseudocódigo para a implementação, juntamente com uma visão geral do Ethereum, contratos inteligentes do Ethereum e a linguagem de programação Solidity.

Os dados são salvos em formato criptografado no contrato inteligente, sendo uma chave privada usada para descriptografar e acessar esses dados. Nenhum dado pessoal é salvo.

8.5 RXBLOCK: TOWARDS THE DESIGN OF A DISTRIBUTED IMMUTABLE ELECTRONIC PRESCRIPTION SYSTEM

O artigo (THATCHER; ACHARYA, 2020) discute o design e implementação de um sistema de prescrição eletrônica distribuído chamado RxBlock, que utiliza tecnologia Blockchain. O objetivo do sistema é fornecer uma maneira segura e eficiente de gerenciar prescrições eletrônicas.

O sistema utiliza uma Blockchain Ethereum privada e contratos inteligentes para facilitar o processo de prescrição eletrônica. O sistema é composto por várias interfaces de usuário, incluindo a interface de registro, a interface de prescrição e a interface de preenchimento de prescrições. A interface de prescrição permite que os médicos criem novas prescrições para seus pacientes. Eles inserem o nome do paciente e o medicamento prescrito por meio de um formulário web. Após a submissão, o médico recebe uma notificação para confirmar a transação. Também há uma interface que exibe um registro histórico de todas as prescrições preenchidas e não preenchidas no sistema RxBlock. Além dos dados da prescrição, essa interface mostra o médico que originou a prescrição e o farmacêutico que a preencheu.

Uma avaliação sobre o sistema é feita em um centro regional de trauma com cerca de 600 leitos e mais de 30 clínicas associadas. Os resultados confirmam que a proposta demonstra o potencial para aliviar a crise de overdose de medicamentos nos EUA e permite a concepção de um sistema de monitoramento de prescrição digital eficaz e responsável.

Vale ressaltar que todos os dados são salvos em texto claro, destacando assim que a proposta não se preocupa com a privacidade dos usuários.

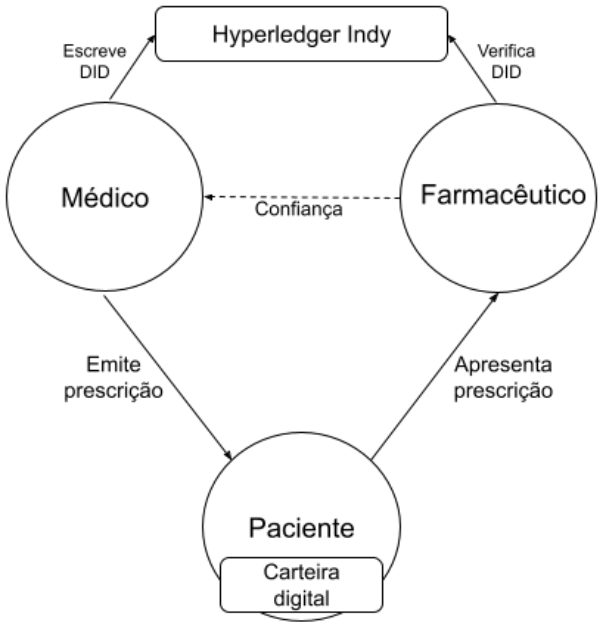
9 PROPOSTA

Com base nos conceitos e tecnologias analisados, na revisão da literatura e casos de uso, é realizado a proposta de um protótipo para emissão e revogação de prescrições médicas digitais baseado em Blockchain, que possa aprimorar os modelos existentes, adicionando maior controle dos dados por parte do paciente. Ao contrário de modelos centralizados e dos modelos descentralizados com Blockchain analisados, a proposta mantém os dados sensíveis em posse do paciente, oferecendo maior propriedade sobre seus dados. A proposta possui seus papéis conforme mostrado na Figura 7.

Ao chegar na consulta médica, o médico convida o paciente para se conectar através de um código QR. Em sua carteira digital no celular, o paciente escaneia o código. Com a conexão confirmada, o médico estará apto para emitir uma prescrição através de seu agente Aries local. O médico emite a prescrição para o paciente, preenchendo todos os campos necessários, a qual é armazenada na carteira digital do paciente. A partir disso, o paciente poderá ir na farmácia de sua preferência retirar o medicamento prescrito.

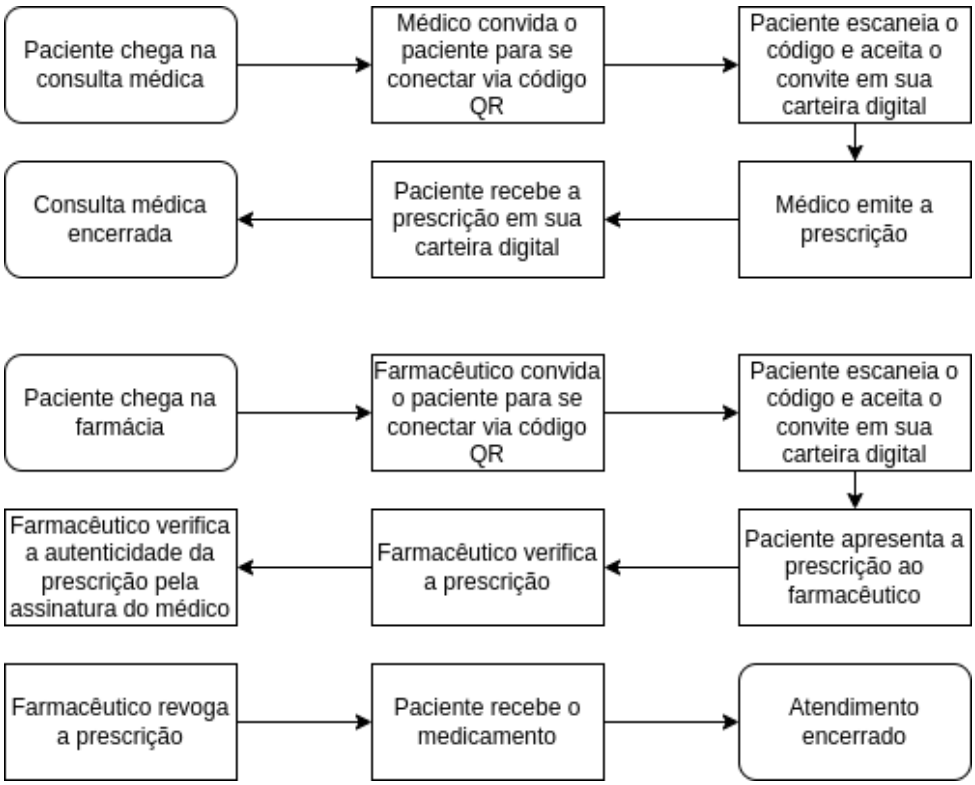
Ao chegar na farmácia, o paciente aceita o convite do farmacêutico através de um código QR. Com ambos conectados, o paciente apresenta a prescrição ao farmacêutico, que verifica a credencial e confirma a autenticidade da prescrição por meio da assinatura digital do médico. Tal assinatura pode ser verificada através do DID do médico no registro distribuído. O registro distribuído fornece a confiança para que o farmacêutico confie que aquela prescrição foi emitida por um médico habilitado. Em seguida, o farmacêutico realiza a revogação da prescrição e entrega o medicamento ao paciente. Todo esse fluxo pode ser visualizado na Figura 8.

Figura 7 – Papéis da proposta



Fonte: O autor

Figura 8 – Fluxograma da proposta



Fonte: O autor

A tecnologia Blockchain oferece algumas vantagens neste caso de uso. A utilização de criptografia avançada e consenso distribuído protege as informações registradas. As informações registradas são imutáveis e não podem ser alteradas retroativamente, garantindo integridade e confiança. Também é possível rastrear e auditar cada transação e modificação feita nas prescrições médicas. Os dados sensíveis são mantidos pelo paciente, oferecendo maior controle sobre suas informações de saúde.

Embora sistemas de prescrições com Blockchain possam ser implementados com contratos inteligentes, em plataformas como Ethereum ou Hyperledger Fabric, foi escolhido a Hyperledger Indy e a Hyperledger Aries. A escolha da Indy se deve ao fato de ser uma Blockchain específica para Identidades Auto-Soberanas, além de ser um projeto *open-source* e com um desenvolvimento maduro. No Registro Distribuído da Indy ficam salvos os esquemas de credenciais, as definições de credenciais, DIDs públicos, chaves públicas, além de acumuladores criptográficos para revogação de credenciais. Esses DIDs serão posteriormente utilizados para verificar as assinaturas dos emissores.

Por se compatível com a Hyperledger Indy e ser integrada à mesma anteriormente, o Hyperledger Aries é uma opção viável. É responsável por fazer a camada de comunicação entre as entidades que usam DID, assim como na Indy. Além disso, a emissão e gerenciamento de credenciais é de sua responsabilidade.

Com uma lógica distribuída, dentro do contexto brasileiro, os nodos de tal sistema poderiam ficar espalhados entre organizações de interesse tais como o Conselho Federal de

Medicina (CFM), o Conselho Federal de Farmácia (CFF), a Agência Nacional de Vigilância Sanitária (ANVISA) e o Sistema Único de Saúde (SUS). Esse modelo pode distribuir os custos de manutenção do sistema entre os participantes.

9.1 FERRAMENTAS UTILIZADAS

Para a implementação de uma instância local da Hyperledger Indy é utilizado o projeto VON Network (COLUMBIA, 2021). É um projeto de código aberto que permite criar uma rede Indy de desenvolvimento. Com ele é possível criar uma rede Indy própria e registrar as credenciais, DIDs e chaves públicas.

Para criar e emitir credenciais verificáveis é utilizado a biblioteca Aries Cloud Agent Python (ACA-Py) (HYPERLEDGER, 2019b) como nosso agente Àries. ACA-PY é um projeto de código aberto que permite criar ecossistemas de credenciais verificáveis. Sua escolha foi devido à compatibilidade com o projeto VON Network, além de ser um projeto bem estabelecido. Com ele podemos criar agentes Aries tanto para o médico, o paciente e o farmacêutico.

A revogação das credenciais é feito por meio de acumuladores criptográficos, com o auxílio do projeto Indy Tails Server (COLUMBIA, 2022). É um projeto de código aberto compatível com os outros dois citados anteriormente. Ele utiliza o registro de revogação da credencial para revogá-la na rede Indy.

Existem outras alternativas ao projetos escolhidos. Uma delas é a rede Sovrin (SOVRIN, 2023). Ela é a implementação da Hyperledger Indy mais madura em produção. Porém, ela é voltada para projetos mais robustos e possui taxas de uso.

9.2 PROTÓTIPO E RESULTADOS

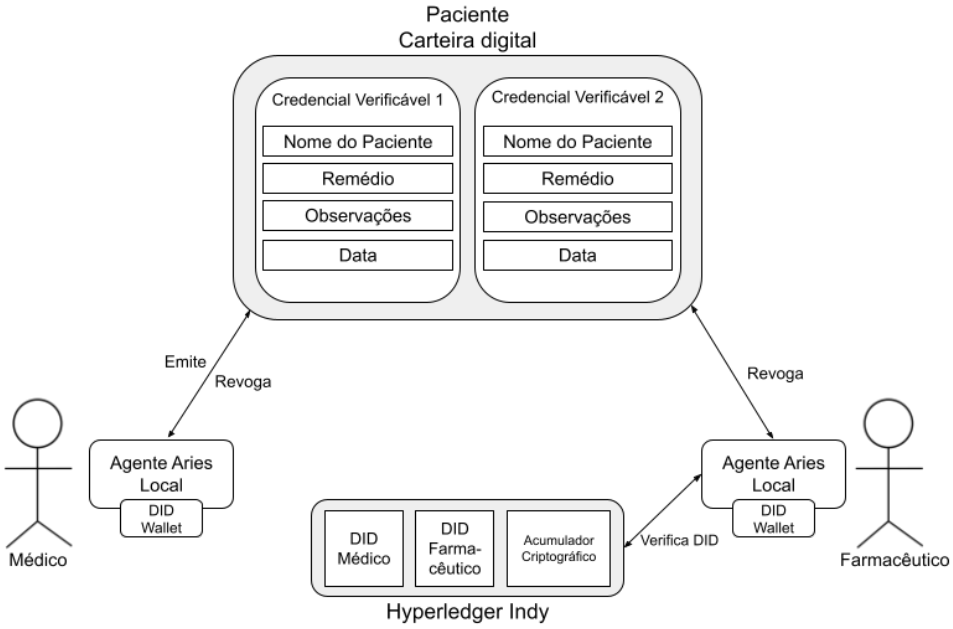
Com as ferramentas citadas acima é possível criar um pequeno protótipo para a emissão e revogação das credenciais verificáveis. O código-fonte e as instruções do protótipo estão em um repositório público no GitHub (JUNCKES, 2023).

A arquitetura ideal da proposta fica tal como na Figura 9. O médico e o farmacêutico têm um agente Aries local, assim podem se comunicar com outros agentes e realizar funções como emissão e revogação de credenciais. Porém, devido à dificuldades na comunicação entre o agente e a rede, o protótipo não possui um agente Aries dedicado ao farmacêutico. Portanto, apenas o médico realiza revogação no protótipo atual.

Na versão atual do protótipo, o paciente também é implementado através de um agente Aries local. Isso ocorre pois não é possível configurar a rede Indy local com os aplicativos móveis de carteiras digitais disponíveis atualmente no mercado. Apenas redes Indy maduras, como a Sovrin, estão habilitadas nos aplicativos testados.

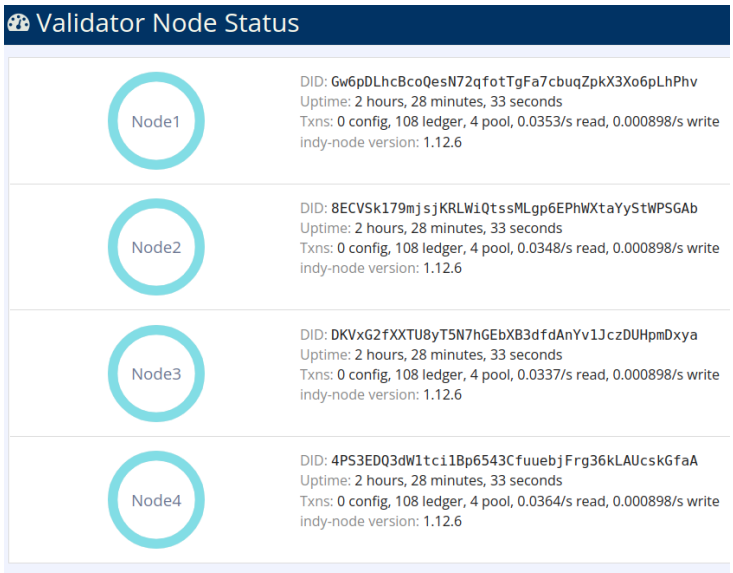
Após inicializada a rede local Indy, podemos verificar o status dos nodos *Validators* conforme a Figura 10.

Figura 9 – Arquitetura da proposta



Fonte: O autor

Figura 10 – Status dos nodos da rede Indy

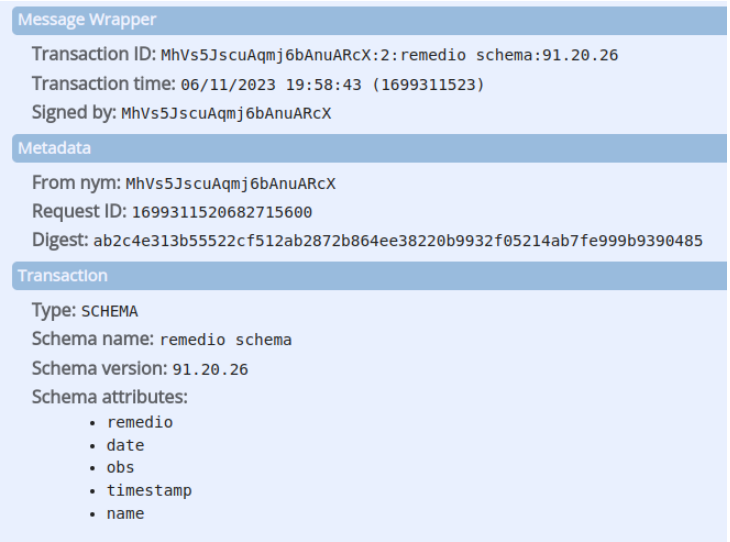


Fonte: O autor

Ao iniciar o agente Aries do médico, é criado o esquema da credencial com quatro campos: o nome do paciente (name), o remédio (remedio), a data da emissão (date) e observações (obs). A Figura 11 mostra a transação na rede Indy com o esquema da credencial criado.

Depois de inicializado o agente Aries do médico, é apresentada a sua tela inicial, como visto na Figura 12. Essa tela contem o código QR e JSON para convidar o paciente. O paciente, por sua vez, irá colocar o convite em sua aplicação e, consequentemente, estabelecer uma conexão com o médico via protocolo DIDComm.

Figura 11 – Esquema da credencial criado na rede Indy



Fonte: O autor

Figura 12 – Tela inicial do médico

Fonte: O autor

Ao iniciar o agente Aries do paciente, a tela inicial solicita o convite JSON do médico para realizar a conexão. Após conectado, conforme a Figura 13, um menu de interação é observado. Nele é possível enviar uma mensagem ao médico e inserir um novo convite. Por outro lado, na tela do médico podemos visualizar, conforme a Figura 14, um menu com as seguintes opções: Emitir prescrição, Enviar mensagem, Criar novo convite, Revogar prescrição, Publicar revogação e Sair.

Com ambos conectados, o médico pode emitir a prescrição em formato de uma cre-

dencial verificável. Ele precisa preencher quatro campos: o nome do paciente, a data, o remédio prescrito e observações. Ao completar o preenchimento dos campos, a credencial é enviada para a carteira digital do paciente. A Figura 15 exemplifica a emissão da prescrição com os campos preenchidos. A prescrição é recebida pelo paciente e armazenada em sua carteira digital conforme mostrado na Figura 16.

A prescrição pode ser emitida de forma que cada medicação seja uma credencial verificável diferente, provendo a opção para o paciente dispensar cada medicamento em farmácias ou em momentos diferentes. Isso gera uma maleabilidade e um controle maior para a dispensação. Atualmente nos modelos de receitas manuais, onde a prescrição fica retida, não existe a opção de dispensação em diferentes ocasiões.

O médico também pode revogar uma prescrição previamente emitida, tornando-a inutilizável novamente. Para isso, ele precisa inserir a *revocation registry ID* da credencial, conforme a Figura 17. A transação da revogação da credencial na rede Indy é mostrada na Figura 18.

O paciente poderá ir na farmácia de sua preferência para adquirir os medicamentos prescritos. O farmacêutico, que também faz uso de um agente Aries, gerará um código QR para se comunicar com o paciente. Depois de estabelecida a conexão, é responsabilidade do farmacêutico verificar a autenticidade da assinatura do emissor pelo DID registrado na Indy. Caso confirmada, ele irá revogar a credencial, tornando-a inutilizável, e entregará os medicamentos ao paciente.

Essa revogação é feita por meio de uma mensagem enviada ao Agente Aries do médico, pedindo a revogação. Em um implementação mais robusta, um Agente Aries em um servidor na nuvem poderia realizar a intermediação entre a comunicação do Agente Aries do farmacêutico e do médico. Na proposta realizada, a revogação pode ser feita por meio de um comunicação direta entre o Agente do farmacêutico e do médico. O paciente pode então dispensar uma segunda medicação, ou ir a uma segunda farmácia e realizar o processo novamente.

A apresentação da prescrição para o farmacêutico segue o paradigma da Identidade Auto Soberana, utilizando a minimização de dados e divulgação seletiva. Dessa forma, é possível por exemplo apresentar apenas o campo da medicação, sem precisar mostrar nenhum dado pessoal do paciente. Porém, certos tipos de prescrições/medicamentos exigem alguma identificação. Uma forma privativa seria a identificação por biometria (em carteiras digitais em *smartphones*), autenticando o paciente sem a necessidade de expor dados pessoais. Caso um arranjo por biometria não esteja disponível, o paciente terá que se autenticar de forma tradicional, idealmente, sem que seus dados sejam registrados em nenhum tipo de sistema, ou registrado de forma pseudo-anônima.

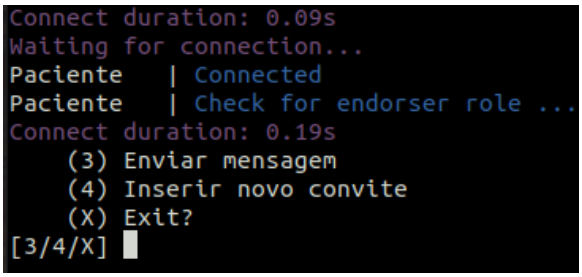


Figura 13 – Tela inicial do paciente

Fonte: O autor

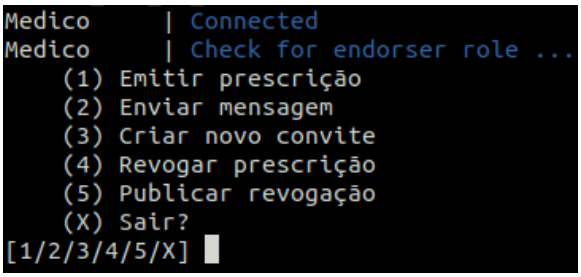
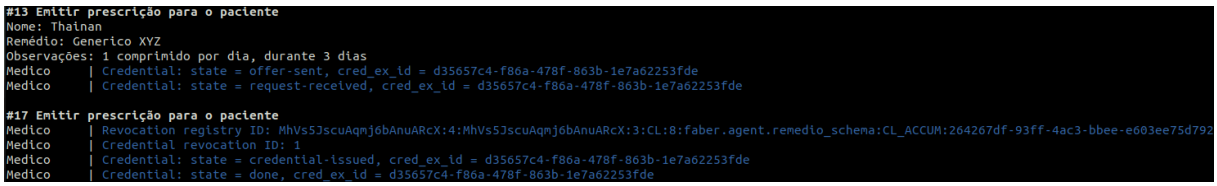


Figura 14 – Menu de opções do médico

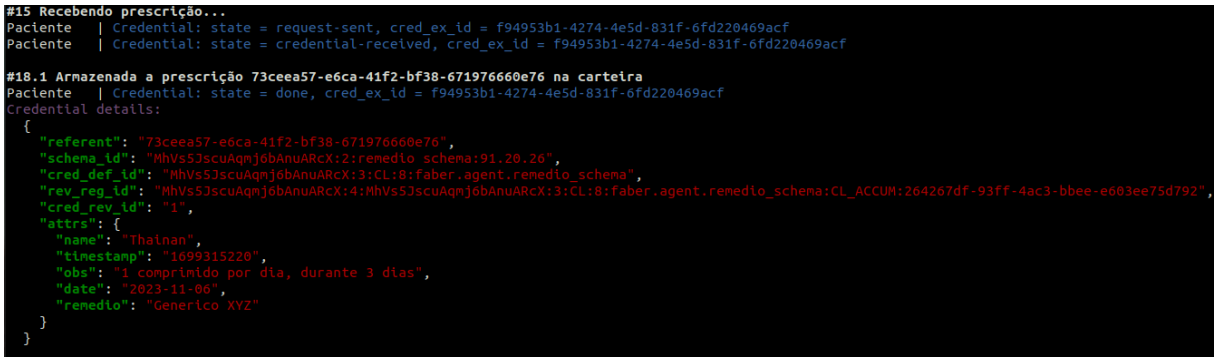
Fonte: O autor

Figura 15 – Exemplo de emissão de prescrição



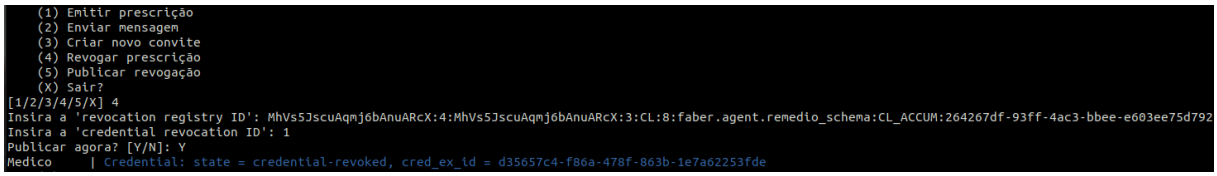
Fonte: O autor

Figura 16 – Exemplo de recebimento de prescrição



Fonte: O autor

Figura 17 – Exemplo de revogação de prescrição



Fonte: O autor

Figura 18 – Transação da revogação na rede Indy

Fonte: O autor

10 DESAFIOS

A implementação de prescrições médicas digitais, aliada à tecnologia Blockchain e Identidade Digitais, representa um avanço significativo no setor de saúde, promovendo uma abordagem inovadora e segura para a gestão de informações médicas. Porém, essa integração enfrenta alguns desafios, que vão desde a usabilidade dos sistemas até as dificuldades das identidades online atuais.

Segundo Schäffner (2019), os modelos atuais de identidade digitais não satisfazem a demanda futura dos usuários de controlar sua própria identidade. O autor afirma que o principal dilema é que o usuário pega emprestada a conta do provedor de identidade que representa a identidade do usuário. Então, mesmo que os atributos da conta possam ser modificados pelo usuário a qualquer momento, não é possível garantir que a identidade fornecida permaneça válida ou não será removida pelo provedor de identidade. Isso não permite aos usuários outra escolha a não ser confiar totalmente no serviço e no provedor de identidade escolhido. Nesse sentido a proposta atual é um avanço.

Schäffner (2019) também afirma que devido à falta de reutilização das identidades já existentes, os serviços online armazenam as informações pessoais dos seus usuários nos seus próprios servidores para determinar quem são eles. Às vezes, os dados fornecidos podem não estar corretos, pois os usuários podem fornecer dados falsos no momento do registo para ocultar a sua identidade real. Isto leva a outro desafio, pois a verificação dos usuários é muito complexa e cara.

Através de um estudo sobre a usabilidade de soluções já existentes de gerenciamento de identidades descentralizadas, Khayretdinova et al. (2022) encontrou alguns desafios acerca do tema. Para gerenciar as identidades de forma eficaz, os usuários precisam compreender como a tecnologia funciona. Porém, o estudo realizado por Khayretdinova et al. (2022) mostra que a mentalidade dos usuários não está alinhada com os desenvolvedores que já são familiarizados com tais tecnologias. Casos de uso como emissão e verificação de credenciais já demonstraram ser um problema para os usuários. A recuperação e o *backup* dos dados também são um desafio.

Khayretdinova et al. (2022) conclui que as soluções que existem atualmente precisam fornecer uma base explicativa e orientar cuidadosamente o usuário com uma boa experiência de uso, por exemplo através da sua interface.

Embora abordagens como a proposta por esse trabalho sejam promissora na ampliação da privacidade e propriedade dos dados, ainda mais em contextos de dados sensíveis, como são os dados de saúde, desafios de usabilidade e também delegação de identidades para crianças e incapazes devem ser levados em conta na criação de sistemas que visam ampliar e melhorar a fronteira das identidades e documentos digitais

11 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

11.1 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo investigar tópicos, ferramentas e tecnologias que viabilizam a aplicação do modelo de Identidade Auto-Soberana no manejo de dados de saúde. O uso da ferramenta Hyperledger Indy para o registro distribuído contribui para a descentralização. A Indy oferece a capacidade de estabelecer confiança, onde o emissor das credenciais verificáveis tem seu DID e chave de verificação registrados na Blockchain, sujeitos à verificação pelo receptor. Enquanto a rede distribuída estiver operacional, o registro permanecerá acessível.

Por ser um sistema distribuído, evita-se (ou dificulta-se) pontos únicos de falha e perda de dados, proporcionando maior disponibilidade ao sistema. Os dados dos pacientes em sua carteira digital oferece controle e privacidade, sendo também uma forma eficiente de transporte desses dados. Os dados em posse do paciente podem ser transportado entre diferentes agentes de saúde, ou estados e até países. Nenhum dado pessoal é guardado nos registros distribuídos.

O protótipo pode ser facilmente adaptado para emitir a prescrição em algum formato para Interoperabilidade, tal como o padrão para troca de dados de saúde FHIR (Health Level Seven International, 2023), que é utilizado pela Rede Nacional de Dados de Saúde (Rede Nacional de Dados em Saúde, 2023).

Outras implementações de prescrições médicas que utilizam Blockchain, como em Garcia et al. (2022), Li (2020), Ying et al. (2019) e Benita et al. (2020) salvam os dados de saúde pessoais de forma criptografada diretamente nos registros distribuídos. Porém, a criptografia que é segura hoje, pode ser quebrada no futuro, expondo esses dados escritos em um registro permanente. A escolha de manter os dados pessoais todos fora dos registros distribuídos evita esses esquemas de criptografias elaborados e garante maior adequação aos processos legais.

Os protocolos do Hyperledger Aries oferecem uma interface que facilita a interação entre distintos participantes, possibilitando a emissão e gestão de credenciais verificáveis. Através desses projetos, várias implementações de modelos de Identidade Auto-Soberana podem coexistir. Esses novos modelos promovem maior privacidade, segurança e controle de propriedade sobre os dados dos usuários.

Outro ponto da proposta é o armazenamento dos dados de forma distribuída em posse dos pacientes, oferecendo a possibilidade de extensão para outros dados (boletins médicos, exames, históricos) sem que o sistema em si precise ampliar sua capacidade de armazenamento.

Ao empregar esse modelo, este trabalho conseguiu estabelecer, com sucesso, um protótipo para a emissão e revogação de prescrições médicas eletrônicas no formato de credenciais verificáveis, fundamentado na tecnologia Blockchain e Identidade Auto Soberana, fornecendo meios para o manejo adequado de dados sensíveis tais quais os dados de saúde de um indivíduo. Esse protótipo resultou na criação de uma prescrição médica que assegura mecanismos de divulgação seletiva. A prescrição, sob a custódia do paciente, proporciona uma utilização da

prescrição com privacidade de seus dados.

Com o tempo, é possível que mais pessoas perceberão a importância de cuidar bem das suas informações digitais. É provável que ainda tenhamos um extenso percurso a percorrer para aprimorar a gestão de nossos dados, que incluirá modelos de administração de identidades digitais, como o de Identidade Auto-Soberana. No futuro , é provável que novas políticas, mecanismos e paradigmas para o gerenciamento de dados serão desenvolvidos. Tecnologias, como a Blockchain, e ferramentas, como Hyperledger Indy e Aries, se tornarão parte integrante desse futuro, provavelmente crescendo e se fortalecendo à medida que nos adaptamos à vida online.

11.2 TRABALHOS FUTUROS

Podemos citar como possíveis trabalhos futuros:

- Aperfeiçoamento do protótipo, adicionando o agente Aries do farmacêutico para se comunicar com o paciente e a rede;
- Implementar uma interface gráfica do usuário para facilitar o uso;
- Adicionar a compatibilidade com aplicativos móveis de carteiras digitais, assim os usuários podem utilizar seus celulares.
- Oferecer a emissão da credencial verificável em um formato JSON FHIR (Rede Nacional de Dados em Saúde, 2023), de forma a ser compatível com a Rede Nacional de Dados de Saúde.
- Aprimorar o processo de revogação por meio de um agente Aries em um servidor na nuvem, facilitando a comunicação entre os agentes do farmacêutico e do médico.

REFERÊNCIAS

AGRAWAL, A. Medication errors: prevention using information technology systems. **British Journal of Clinical Pharmacology**, v. 67, n. 6, p. 681–686, 2009. Disponível em: https://bpspubs.onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2125.2009.03427.x. Acesso em: 03 dez. de 2023.

ALDUGHAYFIQ, B.; SAMPALLI, S. Digital health in physicians' and pharmacists' office: A comparative study of e-prescription systems' architecture and digital security in eight countries. In: . [S.l.: s.n.], 2021. v. 25, n. 2, p. 102–122.

ALLEN, C. **The Path to Self-Sovereign Sdentity**. 2016. Disponível em: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Acesso em: 23 mai. de 2023.

BABU, G. K.; THIYAGARAJAN, P. The current state of prescriptions and potential enhancements using blockchain. In: **2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)**. [S.l.: s.n.], 2021. p. 1–6.

BENITA, R. et al. Authentic drug usage and tracking with blockchain using mobile apps. **International Journal of Interactive Mobile Technologies (iJIM)**, v. 14, n. 17, p. pp. 20–32, Oct. 2020. Disponível em: https://online-journals.org/index.php/i-jim/article/view/16561. Acesso em: 24 nov. de 2023.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 nov. de 2022.

COLUMBIA, P. of B. **VON Network**. 2021. Disponível em: https://github.com/bcgov/von-network/tree/main. Acesso em: 25 jun. de 2023.

COLUMBIA, P. of B. **Indy Tails Server**. 2022. Disponível em: https://github.com/bcgov/indy-tails-server. Acesso em: 02 nov. de 2023.

CURRAN, S. **Aries Cloud Agent Internals: Agent and Controller**. 2021. Disponível em: https://github.com/hyperledger/aries-cloudagent-python/blob/main/docs/GettingStartedAriesDev/AriesAgentArchitecture.md. Acesso em: 22 jun. de 2023.

DIB, O.; TOUMI, K. Decentralized identity systems: Architecture, challenges, solutions and future directions. **Annals of Emerging Technologies in Computing**, v. 4, p. 19–40, 12 2020.

EVEREST. **Everest**. Disponível em: https://everest.org/. Acesso em: 02 dez. de 2023.

FERDOUS, M. S.; CHOWDHURY, F.; ALASSAFI, M. O. In search of self-sovereign identity leveraging blockchain technology. **IEEE Access**, v. 7, p. 103059–103079, 2019.

FOUNDATION, L. **Hyperledger**. 2015. Disponível em: https://www.hyperledger.org/. Acesso em: 22 jun. de 2023.

GARCIA, R. D. et al. A blockchain-based data governance with privacy and provenance: a case study for e-prescription. In: **2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)**. [S.l.: s.n.], 2022. p. 1–5.

Health Level Seven International. **Welcome to FHIR**. 2023. Acesso em: 25 de novembro de 2023. Disponível em: https://www.hl7.org/fhir/.

HYPERLEDGER. **Welcome to Hyperledger Indy Node's documentation!** 2018. Disponível em: https://hyperledger-indy.readthedocs.io/projects/node/en/latest/index.html. Acesso em: 11 nov. de 2023.

HYPERLEDGER. **Welcome to Indy Plenum's documentation!** 2018. Disponível em: https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/index.html. Acesso em: 22 jun. de 2023.

HYPERLEDGER. **Hyperledger Aries**. 2019. Disponível em: https://github.com/hyperledger/aries. Acesso em: 22 jun. de 2023.

HYPERLEDGER. **Hyperledger Aries Cloud Agent - Python**. 2019. Disponível em: https://github.com/hyperledger/aries-cloudagent-python/tree/main. Acesso em: 25 jun. de 2023.

HYPERLEDGER. **Becoming an Indy/Aries Developer**. 2021. Disponível em: https://github.com/hyperledger/aries-cloudagent-python/tree/main/docs/GettingStartedAriesDev. Acesso em: 11 nov. de 2023.

ISAAK, J.; HANNA, M. J. User data privacy: Facebook, cambridge analytica, and privacy protection. **Computer**, v. 51, n. 8, p. 56–59, 2018.

ISO. **IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts**. [S.l.], 2019. Disponível em: https://www.iso.org/standard/77582.html. Acesso em: 12 nov. de 2023.

JUNCKES, T. V. **Prescrições Médicas Auto-Soberanas**. 2023. Disponível em: https://github.com/thainan1208/prescricao-medica. Acesso em: 11 dez. de 2023.

KHAYRETDINOVA, A. et al. Conducting a usability evaluation of decentralized identity management solutions. In: ____. [S.l.: s.n.], 2022. p. 389–406. ISBN 978-3-658-33305-8.

LI, J. A new blockchain-based electronic medical record transferring system with data privacy. In: **2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT)**. [S.l.: s.n.], 2020. p. 141–147.

LIM, S. Y. et al. Blockchain technology the identity management and authentication service disruptor: a survey. **International Journal on Advanced Science, Engineering and Information Technology**, Insight Society, v. 8, n. 4-2, p. 1735–1745, 2018.

MALIKI, T. E.; SEIGNEUR, J.-M. A survey of user-centric identity management technologies. In: **The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)**. [S.l.: s.n.], 2007. p. 12–17.

MARIA, C.; SEBASTIãO, E. **Manual de orientações básicas para prescrição médica**. 2. ed. [S.l.]: Conselho Regional de Medicina do Estado da Paraíba/Conselho Federal de Medicina, 2011.

MEDICINAS/A. **A aceleração da digitalização das receitas médicas no Brasil**. 2021. Disponível em: https://medicinasa.com.br/levantamento-memed/. Acesso em: 30 jun. de 2023.

MURUGESAN, S.; SORWAR, G. Electronic medical prescription: An overview of current status and issues. **Biomedical Knowledge Management: Infrastructures and Processes for E-Health Systems**, p. 61–81, 2010.

MüHLE, A. et al. **A Survey on Essential Components of a Self-Sovereign Identity**. [S.l.]: arXiv, 2018.

NAIK, N.; JENKINS, P. Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. In: **2020 IEEE International Symposium on Systems Engineering (ISSE)**. [S.l.: s.n.], 2020. p. 1–6.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 22 jun. de 2023.

NAVARATNA, L.; WIJESINGHE, N.; PILAPITIYA, U. Providing electronic health care services through a private permissioned blockchain. In: **2020 2nd International Conference on Advancements in Computing (ICAC)**. [S.l.: s.n.], 2020. v. 1, p. 144–149.

NGUYEN, T.; KIM, K. A survey about consensus algorithms used in blockchain. **Journal of Information Processing Systems**, v. 14, p. 101–128, 01 2018.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Segurança Digital [Revista online]**, v. 31, p. 11–15, 2012.

PANAIT, A.-E.; OLIMID, R. F.; STEFANESCU, A. Analysis of uport open, an identity management blockchain-based solution. In: **Trust and Privacy in Digital Business**. [S.l.: s.n.], 2020. p. 3–13.

PASTUCHOV, A.; CURRAN, S. **Introduction to Hyperledger Indy**. 2019. Disponível em: https://github.com/hyperledger-archives/education/blob/master/LFS171x/docs/introduction-to-hyperledger-indy.md. Acesso em: 22 jun. de 2023.

Rede Nacional de Dados em Saúde. **Tecnologias - Rede Nacional de Dados em Saúde (RNDS)**. 2023. Disponível em: https://rnds-guia.prod.saude.gov.br/docs/rnds/tecnologias/#: :text=FHIR%20%C3%A9%20um%20padr%C3%A3o%20 Acesso em: 24 nov. de 2023.

Saúde Digital Brasil. **Atendimentos via telemedicina para casos de Influenza e COVID-19 dobram a cada 36 horas**. 2022. Disponível em: https://saudedigitalbrasil.com.br/press/atendimentos-via-telemedicina-para-casos-de-influenza-e-covid-19-dobram-a-cada-36-horas. Acesso em: 06 nov. de 2023.

SCHARDONG, F.; CUSTóDIO, R. Self-sovereign identity: A systematic review, mapping and taxonomy. **Sensors**, v. 22, n. 15, 2022. ISSN 1424-8220. Disponível em: https://www.mdpi.com/1424-8220/22/15/5641.

SCHEFFER, M. et al. The multiple uses of telemedicine during the pandemic: the evidence from a cross-sectional survey of medical doctors in brazil open access. **Globalization and Health**, v. 18, p. 81, 09 2022.

SCHäFFNER, M. **Analysis and Evaluation of Blockchain-based Self-Sovereign Identity Systems**. 2019.

SHCHERBAKOV, A. **Hyperledger Indy Public Blockchain Node with Alexander Shcherbakov**. 2019. Disponível em: https://youtu.be/UJbJRqur4ng. Acesso em: 22 jun. de 2023.

SOVRIN. **Sovrin**. 2023. Disponível em: https://sovrin.org/. Acesso em: 06 nov. de 2023.

SPORNY, M.; LONGLEY, D.; CHADWICK, D. **Verifiable Credentials Data Model v1.1**. 2022. Disponível em: https://www.w3.org/TR/vc-data-model/. Acesso em: 19 jun. de 2023.

SPORNY, M. et al. **Decentralized Identifiers (DIDs) v1.0**. 2022. Disponível em: https://www.w3.org/TR/did-core/. Acesso em: 18 jun. de 2023.

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e práticas**. 6. ed. [S.l.]: Pearson Education do Brasil, 2015.

THATCHER, C.; ACHARYA, S. Rxblock: Towards the design of a distributed immutable electronic prescription system. **Network Modeling Analysis in Health Informatics and Bioinformatics**, v. 9, 12 2020.

XU, X.; WEBER, I.; STAPLES, M. **Architecture for Blockchain Applications**. [S.l.]: Springer Cham, 2019.

YAGA, D. et al. **Blockchain technology overview - NISTIR 8202**. 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf. Acesso em: 08 jun. de 2023.

YING, B. et al. A secure blockchain-based prescription drug supply in health-care systems. In: **2019 International Conference on Smart Applications, Communications and Networking (SmartNets)**. [S.l.: s.n.], 2019. p. 1–6.

APÊNDICE A – ARTIGO SBC

Prescrições médicas auto-soberanas: Fortalecendo a segurança e a privacidade

Thainan Vieira Junckes

[1]Departamento de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC)

Abstract. *In recent years, the increasing sharing of personal information online has intensified. This has raised concerns about users' security, privacy, and data ownership. Virtualization is also driving the transition from physical identities to digital identities. The Self-Sovereign Identity paradigm, which allows the user to be the true owner of their identity and linked data, can be used to study this issue. A series of fundamental terms linked to the topic, including Self-Sovereign Identity, Verifiable Credentials, Blockchain and Hyperledger, among others, are essential to understanding this new approach. During the pandemic, there has been an increase in virtual doctor consultations, highlighting the importance of digital prescriptions and the need to protect patient privacy. This work aims to explore the feasibility and implications of Self-Sovereign Identity technology in health data management, using the issuance of medical prescriptions as a case study.*

Resumo. *Nos últimos anos, o compartilhamento crescente de informações pessoais online se intensificou. Isso gerou preocupações sobre a segurança, a privacidade e a propriedade dos dados dos usuários. A virtualização também está levando à transição das identidades físicas para identidades digitais. O paradigma da Identidade Auto-Soberana, que possibilita ao usuário ser o verdadeiro dono de sua identidade e dos dados vinculados, pode ser utilizado para estudar essa questão. Uma série de termos fundamentais ligados ao tema, incluindo Identidade Auto-Soberana, Credenciais Verificáveis, Blockchain e Hyperledger, entre outros, são essenciais para compreender essa nova abordagem. Durante a pandemia, houve um aumento nas consultas médicas virtuais, destacando a importância das prescrições digitais e a necessidade de proteger a privacidade dos pacientes. Este trabalho se propõe a explorar a viabilidade e implicações da tecnologia de Identidade Auto-Soberana na gestão de dados de saúde, usando a emissão de prescrições médicas como estudo de caso.*

1. Introdução

A quantidade de informações pessoais compartilhadas online aumentou significativamente nos últimos anos. A combinação de redes sociais e internet móvel é onde muitos desses dados se originam. Nossas rotinas são cada vez mais vividas no mundo virtual, uma tendência que foi acelerada pela pandemia de Covid-19, que obrigou uma parcela da população a trabalhar, estudar e realizar consultas médicas à distância [Scheffer et al. 2022]. Devido à esse rápido processo de virtualização provocado pela pandemia, por vezes, não houve tempo suficiente para adequar os sistemas a essa nova rotina. Dessa forma, embora a sociedade esteja mais conectada, está também mais exposta.

Nesse cenário, a privacidade dos dados dos usuários é um tópico de discussão. Por vezes, grandes corporações que adquirem dados de usuários o fazem de forma abusiva. A revelação, em 2018, de que o Facebook forneceu à empresa de dados Cambridge Analytica acesso irrestrito e não autorizado a informações de identificação pessoal de mais de 87 milhões de usuários desavisados é um bom exemplo disto [Isaak and Hanna 2018].

Para os cidadãos receberem mais garantias acerca de seus dados, em meados de 2020 entrou em vigor no Brasil a Lei Geral de Proteção de Dados [Brasil 2018]. A lei define o que são dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis. Também esclarece que todos os dados tratados, inclusive no meio digital, estão sujeitos à regulação. Além disso, a LGPD estabelece que não importa onde está localizada a organização ou o seu centro de dados: se há o processamento de informações sobre pessoas, a LGPD deve ser cumprida.

Durante a pandemia de Covid-19, cresceu o número de consultas médicas virtuais [Saúde Digital Brasil 2022]. Dessa forma, a emissão de prescrições digitais e a utilização dos dados anonimizados devem ser feitos de forma a respeitar a privacidade dos pacientes atendidos.

Prescrições médicas são documentos criados e emitidos por profissionais de saúde que que contém instruções específicas para o tratamento de um paciente [Maria and Sebastião 2011]. Tradicionalmente, as prescrições são feitas em papel, onde o médico escreve manualmente as informações necessárias, assina e carimba o documento. A prescrição em papel é entregue ao paciente, que pode levá-la a uma farmácia para obter os medicamentos prescritos. Esse tipo de prescrição ainda é o principal formato de prescrição. Porém, alguns problemas como ilegibilidade, identificação incorreta de medicamento e dosagem podem ocorrer [Babu and Thiyagarajan 2021].

Com o avanço da tecnologia, as prescrições médicas também podem ser feitas de forma digital. Uma prescrição digital é um método em que se utiliza um dispositivo digital onde ocorre trocas de informações entres os envolvidos [Aldughayfiq and Sampalli 2021]. Nesse caso, o médico utiliza um sistema eletrônico de prescrição, onde as informações são inseridas em um software específico e transmitidas eletronicamente para a farmácia. Melhor comunicação entre os envolvidos, aumento da eficiência do processo e diminuição de erros de prescrição são algumas das suas vantagens [Babu and Thiyagarajan 2021]. Entretanto, a ameaça à privacidade e segurança das informações dos pacientes é um fator a ser considerado. A possibilidade de hackers invadirem os sistemas e disponibilizarem esses dados é uma preocupação [Murugesan and Sorwar 2010]. Os dados médicos de um paciente são dados sensíveis, e precisam ser tratados de forma cuidadosa.

Com esse processo de virtualização, as identidades e documentos físicos, tradicionalmente em papel, estão sendo transferidas para uma versão digital, conhecida como identidade e documento digital. Um desses modelos de identidade digital é a Identidade Auto-Soberana, um paradigma de gerenciamento de identidade que busca permitir aos usuários possuírem e controlarem totalmente suas identidades digitais, um sistema centrado no usuário [Mühle et al. 2018]. Esse modelo pode ser utilizado em situações onde os dados pessoais são sensíveis, como dados de pacientes atendidos por médicos e farmacêuticos.

Uma forma comum de implementar Identidades Auto-Soberanas é em conjunto

com a tecnologia Blockchain devido à sua descentralização, segurança, privacidade, controle do usuário e capacidade de interoperabilidade [Ferdous et al. 2019]. Para isso, o projeto Hyperledger Indy é comumente utilizado. Esse projeto fornece uma infraestrutura robusta e interoperável para a criação de sistemas de identidade digital confiáveis, autônomos e descentralizados [Pastuchov and Curran 2019].

Dessa forma, um arranjo que faça uso de Blockchain e Identidade Auto Soberana, é apropriado para o tipo de trato de dados necessários a um sistema de prescrição eletrônica. Lidando com dados sensíveis, o foco desse sistema seria na privacidade, com minimização de dados, tendo maior controle sobre a quantidade de exposição dos dados.

Utilizando a emissão de uma prescrição médica como caso de uso para a criação de um protótipo, este trabalho propõe investigar a viabilidade e implicações da tecnologia utilizada em sistemas de Identidade Auto-Soberana no manejo de dados de saúde.

2. Identidades Digitais

A ISO 24760-1 [ISO 2019] define identidade digital como um "conjunto de atributos relacionados a uma entidade."

Maliki e Seigneur (2007) conceituam a Identidade Digital como sendo a representação dessa entidade, vinculada a algum contexto específico [El Maliki and Seigneur 2007]. Gerenciamento de Identidade, ou em inglês, *Identity and Access Management* (IAM), é definido como um conjunto de políticas, processos e tecnologias que auxiliam a identificar entidades e garantir o correto acesso a serviços e recursos.

Começando com o modelo básico e crescendo em vários estágios com a introdução de modelos adicionais, o cenário de gerenciamento de identidade evoluiu ao longo dos anos.

2.1. Identidade Auto-Soberana

A definição de identidade auto-soberana ainda é bastante discutida, como é possível ver em Allen (2016) e em Ferdous, Chowdhury e Alassafi (2019). Mas há algo em comum, neste modelo o usuário deve ter o controle total da sua identidade digital. Assim, o usuário tem autonomia para armazenar sua identidade onde queira e apresentar apenas quado necessário.

Christopher Allen propôs dez princípios para identidades auto-soberanas [Allen 2016]. Além dos autores citados anteriormente, outros autores como Schardong e Custódio (2021) e Mühle et al. (2018) usam esses princípios como referência na área.

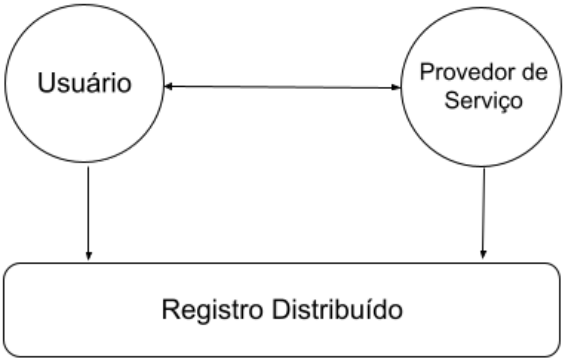
Os dez princípios são:

1. Existência: os usuários devem existir independente do provedor;
2. Controle: os usuários devem controlar suas identidades;
3. Acesso: os usuários devem ter acesso aos seus próprios dados;
4. Transparência: os sistemas devem ser aberto em como funcionam e são atualizados. Os algoritmos devem ser *open-source*;
5. Persistência: as identidades devem ser persistidas;
6. Portabilidade: informações e serviços sobre a identidade devem ser transportáveis;

7. Interoperabilidade: as identidades devem ser tão amplamente utilizáveis quanto possível;
8. Consentimento: os usuários devem concordar com o uso de sua identidade;
9. Minimização: sempre mostrar o mínimo possível de alguma informação necessária;
10. Proteção: os direitos dos usuários devem ser protegidos.

A tecnologia Blockchain possui em comum algumas das propriedades mencionadas por Allen. Segundo Nakamoto (2008), a Blockchain provê essencialmente um domínio descentralizado que não é controlado por nenhuma entidade específica, provendo independência e autonomia para a identidade. Além disso, os dados armazenados estão facilmente disponíveis para qualquer usuário autorizado [Ferdous et al. 2019]. Utilizando o auxílio desta tecnologia, o usuário apresentaria sua credencial e caberia à parte verificadora conferir na Blockchain sua autenticidade, usando o registro distribuído como um agente de confiança, como mostrado na Figura 1.

Figura 1. Modelo de Identidade Auto-Soberana



Inspirado em [Naik and Jenkins 2020]

3. Hyperledger Indy

Hyperledger Indy é um projeto de código aberto que faz parte da iniciativa Hyperledger, uma comunidade colaborativa liderada pela Linux Foundation, focada no desenvolvimento de tecnologias de blockchain para uso empresarial [Foundation 2015]. Com o Hyperledger Indy é possível gerenciar identidades auto-soberanas baseadas em Blockchain.

3.1. Registro Distribuído Indy

O Registro Distribuído Indy é formado por outros dois projetos: Indy-Plenum e Indy-Node. No Indy-Plenum é implementado o algoritmo de consenso. Já no Indy-Node é feita a implementação das transações relacionadas à identidade [Shcherbakov 2019].

O Indy-Plenum utiliza um algoritmo de consenso chamado Plenum Byzantine Fault Tolerant (BFT) [Pastuchov and Curran 2019]. Ele é projetado para ser altamente tolerante a falhas bizantinas, que são situações em que os nodos podem se comportar de maneira maliciosa, enviando informações falsas ou comprometendo a integridade da rede.

O Registro Distribuído Indy é público permissionado [Shcherbakov 2019]. O acesso à leitura é aberto, porém é preciso permissão para escrever e validar as transações. Apenas dados públicos são escritos na Blockchain, como DIDs, chaves e esquemas de credenciais.

4. Hyperledger Aries

O Hyperledger Aries é um projeto da Hyperledger que visa fornecer uma infraestrutura e conjuntos de ferramentas para credenciais verificáveis [Hyperledger 2019a]. O Hyperledger Aries também colabora com outros projetos e tecnologias relacionadas, como o Hyperledger Indy.

Ele fornece uma base para o desenvolvimento de aplicativos e soluções que envolvem identidade digital, interações ponto-a-ponto (*peer-to-peer*) e transações confidenciais. Também possui uma camada de interface para criar, assinar e ler transações na Blockchain.

4.1. Aries Agents

Um agente é responsável por interagir com outras entidades. Segundo Curran (2021), uma instância de um agente possui duas partes: o agente em si e o controlador.

O agente lida com todas as funcionalidades principais do Aries, como interagir com outros agentes, gerenciar armazenamento seguro, enviar notificações de eventos e receber orientações do controlador. O controlador fornece a lógica de negócios que define como essa instância específica do agente se comporta, como responder a eventos no agente e quando acionar o agente para iniciar eventos [Curran 2021].

5. Trabalhos Correlatos

Neste capítulo serão apresentados trabalhos correlatos que contemplam o estado da arte no que tange implementação de prescrições médicas digitais com o uso de Blockcahin.

5.1. A Blockchain-based Data Governance with Privacy and Provenance: a case study for e-Prescription

O artigo [Garcia et al. 2022] apresenta um *framework* de governança de dados descentralizado baseado em Blockchain e reencriptação de proxy para garantir a privacidade, gerenciamento de consentimento e proveniência de dados para prescrição digital. O *framework* ajuda o paciente a armazenar, gerenciar e compartilhar dados da prescrição com outras partes interessadas através de uma *tamper-proof ledger*. Também protege a privacidade dos pacientes armazenando dados de prescrição criptografados na *ledger*. Outra funcionalidade é o suporte à proveniência de dados, assim permite que os proprietários e consumidores de dados monitorem com eficiência os registros históricos dos dados e sua origem, incluindo quem acessou os dados e para quais finalidades.

A implementação usa CosmWasm para os contratos inteligentes e Tendermint para o consenso da Blockchain. Os resultados mostram que a arquitetura proposta pode proteger a privacidade dos proprietários de dados e governar o acesso a dados sensíveis com um mínimo de sobrecarga.

A proposta salva dados sensíveis de identificação de forma criptografada em contratos inteligentes na Blockchain.

5.2. A New Blockchain-based Electronic Medical Record Transferring System with Data Privacy

O artigo [Li 2020] apresenta um sistema de prescrição médica baseado em Blockchain que pode fornecer processamento de prescrições digitais com armazenamento seguro, verificação de identidade e direitos de acesso. Além disso, o sistema adota o método de

proteção k-anonimato baseado na privacidade diferencial no caso de emissão de prescrições eletrônicas, para que a segurança dos dados seja efetivamente melhorada, mantendo a privacidade dos dados.

O artigo também descreve um modelo de contrato inteligente para implementar o sistema de prescrições em uma Blockchain genérica. O modelo teria contratos de pacientes, contratos de médicos, contratos de pesquisadores e contratos de tratamento de casos. É utilizada a relação entre contratos para descrever a lógica estrutural do sistema na Blockchain, representando os dados a serem armazenados e os serviços que podem ser prestados em todo o sistema.

Os dados da prescrição são salvos em formato criptografado no contrato inteligente, sendo uma chave privada usada para descriptografar e acessar esses dados. Também é necessário o consentimento explícito do paciente para acessar seus dados.

5.3. A Secure Blockchain-based Prescription Drug Supply in Health-care Systems

O artigo [Ying et al. 2019] apresenta uma proposta de arquitetura segura baseada em Blockchain para o fornecimento de medicamentos prescritos em sistemas de saúde. A proposta visa autenticar partes não confiáveis através do registro distribuído e proteger a privacidade do paciente com um modelo de identidade dinâmico, garantindo transações seguras de medicamentos. O trabalho salva dados de identificação de forma criptografada em contratos inteligentes.

O texto afirma que é resistente a vários tipos de ataques e fornece um serviço confiável pois emprega um protocolo de autenticação eficiente para validar a legitimidade do usuário, além de utilizar identidade dinâmica para proteger a anonimidade dos usuários. Além disso, a proposta emprega um controle de acesso baseado em função para garantir que apenas usuários autorizados possam acessar informações confidenciais. Uma análise de segurança presente no artigo mostra que o protocolo é resistente a ataques de falsificação de usuário e de comprometimento de banco de dados. O artigo não indica nenhuma Blockchain específica para sua implementação.

5.4. Authentic Drug Usage and Tracking with Blockchain Using Mobile Apps

O artigo [Benita et al. 2020] discute o uso da tecnologia Blockchain no rastreamento do uso de medicamentos e na gestão da cadeia de suprimentos. A implementação da tecnologia Blockchain, especificamente por meio do uso de contratos inteligentes na rede Ethereum, aborda esses desafios.

Segundo o texto, o contrato inteligente ajuda a rastrear o movimento dos medicamentos desde o fabricante até o fornecedor, revendedor, farmácias e finalmente até os pacientes. Ele garante que apenas medicamentos autênticos sejam vendidos e que os pacientes possam comprar apenas medicamentos com uma receita válida de um médico autenticado.

O texto afirma que o sistema proposto é transparente, seguro e descentralizado, com dados armazenados de forma redundante em vários bancos de dados para garantir disponibilidade e imutabilidade. Além disso, é fornecido um pseudocódigo para a implementação, juntamente com uma visão geral do Ethereum, contratos inteligentes do Ethereum e a linguagem de programação Solidity.

Os dados são salvos em formato criptografado no contrato inteligente, sendo uma chave privada usada para descriptografar e acessar esses dados. Nenhum dado pessoal é salvo.

5.5. RxBlock: Towards the design of a distributed immutable electronic prescription system

O artigo [Thatcher and Acharya 2020] discute o design e implementação de um sistema de prescrição eletrônica distribuído chamado RxBlock, que utiliza tecnologia Blockchain. O objetivo do sistema é fornecer uma maneira segura e eficiente de gerenciar prescrições eletrônicas.

O sistema utiliza uma Blockchain Ethereum privada e contratos inteligentes para facilitar o processo de prescrição eletrônica. O sistema é composto por várias interfaces de usuário, incluindo a interface de registro, a interface de prescrição e a interface de preenchimento de prescrições. A interface de prescrição permite que os médicos criem novas prescrições para seus pacientes. Eles inserem o nome do paciente e o medicamento prescrito por meio de um formulário web. Após a submissão, o médico recebe uma notificação para confirmar a transação. Também há uma interface que exibe um registro histórico de todas as prescrições preenchidas e não preenchidas no sistema RxBlock. Além dos dados da prescrição, essa interface mostra o médico que originou a prescrição e o farmacêutico que a preencheu.

Uma avaliação sobre o sistema é feita em um centro regional de trauma com cerca de 600 leitos e mais de 30 clínicas associadas. Os resultados confirmam que a proposta demonstra o potencial para aliviar a crise de overdose de medicamentos nos EUA e permite a concepção de um sistema de monitoramento de prescrição digital eficaz e responsável.

Vale ressaltar que todos os dados são salvos em texto claro, destacando assim que a proposta não se preocupa com a privacidade dos usuários.

6. Proposta

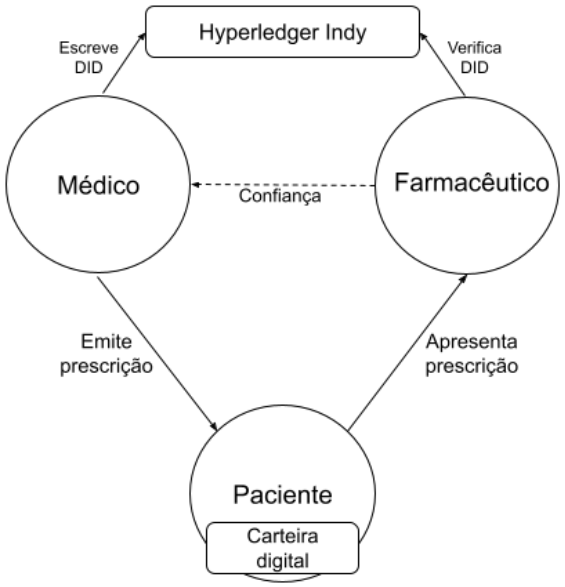
Com base nos conceitos e tecnologias analisados, na revisão da literatura e casos de uso, é realizado a proposta de um protótipo para emissão e revogação de prescrições médicas digitais baseado em Blockchain, que possa aprimorar os modelos existentes, adicionando maior controle dos dados por parte do paciente. Ao contrário de modelos centralizados e dos modelos descentralizados com Blockchain analisados, a proposta mantém os dados sensíveis em posse do paciente, oferecendo maior propriedade sobre seus dados. A proposta possui seus papéis conforme mostrado na Figura 2.

Ao chegar na consulta médica, o médico convida o paciente para se conectar através de um código QR. Em sua carteira digital no celular, o paciente escaneia o código. Com a conexão confirmada, o médico estará apto para emitir uma prescrição através de seu agente Aries local. O médico emite a prescrição para o paciente, preenchendo todos os campos necessários, a qual é armazenada na carteira digital do paciente. A partir disso, o paciente poderá ir na farmácia de sua preferência retirar o medicamento prescrito.

Ao chegar na farmácia, o paciente aceita o convite do farmacêutico através de um código QR. Com ambos conectados, o paciente apresenta a prescrição ao farmacêutico, que verifica a credencial e confirma a autenticidade da prescrição por meio da assinatura

digital do médico. Tal assinatura pode ser verificada através do DID do médico no registro distribuído. O registro distribuído fornece a confiança para que o farmacêutico confie que aquela prescrição foi emitida por um médico habilitado. Em seguida, o farmacêutico realiza a revogação da prescrição e entrega o medicamento ao paciente.

Figura 2. Papéis da proposta



O autor

A tecnologia Blockchain oferece algumas vantagens neste caso de uso. A utilização de criptografia avançada e consenso distribuído protege as informações registradas. As informações registradas são imutáveis e não podem ser alteradas retroativamente, garantindo integridade e confiança. Também é possível rastrear e auditar cada transação e modificação feita nas prescrições médicas. Os dados sensíveis são mantidos pelo paciente, oferecendo maior controle sobre suas informações de saúde.

Embora sistemas de prescrições com Blockchain possam ser implementados com contratos inteligentes, em plataformas como Ethereum ou Hyperledger Fabric, foi escolhido a Hyperledger Indy e a Hyperledger Aries. A escolha da Indy se deve ao fato de ser uma Blockchain específica para Identidades Auto-Soberanas, além de ser um projeto *open-source* e com um desenvolvimento maduro. No Registro Distribuído da Indy ficam salvos os esquemas de credenciais, as definições de credenciais, DIDs públicos, chaves públicas, além de acumuladores criptográficos para revogação de credenciais. Esses DIDs serão posteriormente utilizados para verificar as assinaturas dos emissores.

Por se compatível com a Hyperledger Indy e ser integrada à mesma anteriormente, o Hyperledger Aries é uma opção viável. É responsável por fazer a camada de comunicação entre as entidades que usam DID, assim como na Indy. Além disso, a emissão e gerenciamento de credenciais é de sua responsabilidade.

Com uma lógica distribuída, dentro do contexto brasileiro, os nodos de tal sistema poderiam ficar espalhados entre organizações de interesse tais como o Conselho Federal de Medicina (CFM), o Conselho Federal de Farmácia (CFF), a Agência Nacional de Vigilância Sanitária (ANVISA) e o Sistema Único de Saúde (SUS). Esse modelo pode distribuir os custos de manutenção do sistema entre os participantes.

6.1. Ferramentas Utilizadas

Para a implementação de uma instância local da Hyperledger Indy é utilizado o projeto VON Network [of British Columbia 2021]. É um projeto de código aberto que permite criar uma rede Indy de desenvolvimento. Com ele é possível criar uma rede Indy própria e registrar as credenciais, DIDs e chaves públicas.

Para criar e emitir credenciais verificáveis é utilizado a biblioteca Aries Cloud Agent Python (ACA-Py) [Hyperledger 2019b] como nosso agente Àries. ACA-PY é um projeto de código aberto que permite criar ecossistemas de credenciais verificáveis. Sua escolha foi devido à compatibilidade com o projeto VON Network, além de ser um projeto bem estabelecido. Com ele podemos criar agentes Aries tanto para o médico, o paciente e o farmacêutico.

A revogação das credenciais é feito por meio de acumuladores criptográficos, com o auxílio do projeto Indy Tails Server [of British Columbia 2022]. É um projeto de código aberto compatível com os outros dois citados anteriormente. Ele utiliza o registro de revogação da credencial para revogá-la na rede Indy.

Existem outras alternativas ao projetos escolhidos. Uma delas é a rede Sovrin [Sovrin 2023]. Ela é a implementação da Hyperledger Indy mais madura em produção. Porém, ela é voltada para projetos mais robustos e possui taxas de uso.

6.2. Protótipo e Resultados

Com as ferramentas citadas acima é possível criar um pequeno protótipo para a emissão e revogação das credenciais verificáveis.

A arquitetura ideal da proposta fica tal como na Figura 3. O médico e o farmacêutico têm um agente Aries local, assim podem se comunicar com outros agentes e realizar funções como emissão e revogação de credenciais. Porém, devido à dificuldades na comunicação entre o agente e a rede, o protótipo não possui um agente Aries dedicado ao farmacêutico. Portanto, apenas o médico realiza revogação no protótipo atual.

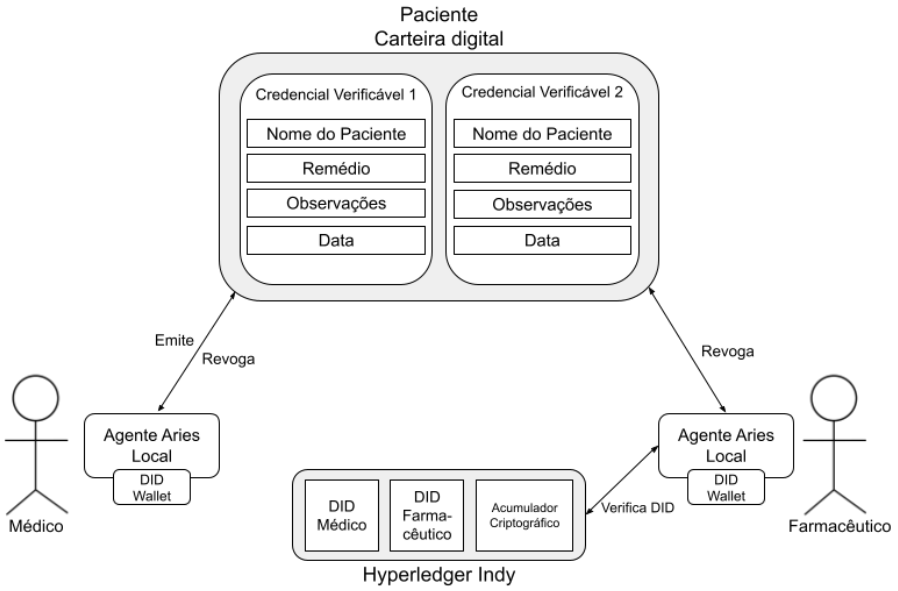
Na versão atual do protótipo, o paciente também é implementado através de um agente Aries local. Isso ocorre pois não é possível configurar a rede Indy local com os aplicativos móveis de carteiras digitais disponíveis atualmente no mercado. Apenas redes Indy maduras, como a Sovrin, estão habilitadas nos aplicativos testados.

Ao iniciar o agente Aries do médico, é criado o esquema da credencial com quatro campos: o nome do paciente (name), o remédio (remedio), a data da emissão (date) e observações (obs).

Depois de inicializado o agente Aries do médico, é apresentada a sua tela inicial. Essa tela contem o código QR e JSON para convidar o paciente. O paciente, por sua vez, irá colocar o convite em sua aplicação e, consequentemente, estabelecer uma conexão com o médico via protocolo DIDComm.

Ao iniciar o agente Aries do paciente, a tela inicial solicita o convite JSON do médico para realizar a conexão. Após conectado, conforme a Figura 4, um menu de interação é observado. Nele é possível enviar uma mensagem ao médico e inserir um novo convite. Por outro lado, na tela do médico podemos visualizar, conforme a Figura 5, um menu com as seguintes opções: Emitir prescrição, Enviar mensagem, Criar novo

Figura 3. Arquitetura da proposta



O autor

convite, Revogar prescrição, Publicar revogação e Sair.

Com ambos conectados, o médico pode emitir a prescrição em formato de uma credencial verificável. Ele precisa preencher quatro campos: o nome do paciente, a data, o remédio prescrito e observações. Ao completar o preenchimento dos campos, a credencial é enviada para a carteira digital do paciente. A Figura 6 exemplifica a emissão da prescrição com os campos preenchidos. A prescrição é recebida pelo paciente e armazenada em sua carteira digital conforme mostrado na Figura 7.

A prescrição pode ser emitida de forma que cada medicação seja uma credencial verificável diferente, provendo a opção para o paciente dispensar cada medicamento em farmácias ou em momentos diferentes. Isso gera uma maleabilidade e um controle maior para a dispensação. Atualmente nos modelos de receitas manuais, onde a prescrição fica retida, não existe a opção de dispensação em diferentes ocasiões.

O médico também pode revogar uma prescrição previamente emitida, tornando-a inutilizável novamente. Para isso, ele precisa inserir a *revocation registry ID* da credencial, conforme a Figura 8. A transação da revogação da credencial na rede Indy é mostrada na Figura 9.

O paciente poderá ir na farmácia de sua preferência para adquirir os medicamentos prescritos. O farmacêutico, que também faz uso de um agente Aries, gerará um código QR para se comunicar com o paciente. Depois de estabelecida a conexão, é responsabilidade do farmacêutico verificar a autenticidade da assinatura do emissor pelo DID registrado na Indy. Caso confirmada, ele irá revogar a credencial, tornando-a inutilizável, e entregará os medicamentos ao paciente.

Essa revogação é feita por meio de uma mensagem enviada ao Agente Aries do médico, pedindo a revogação. Em um implementação mais robusta, um Agente Aries em um servidor na nuvem poderia realizar a intermediação entre a comunicação do Agente Aries do farmacêutico e do médico. Na proposta realizada, a revogação pode ser feita por

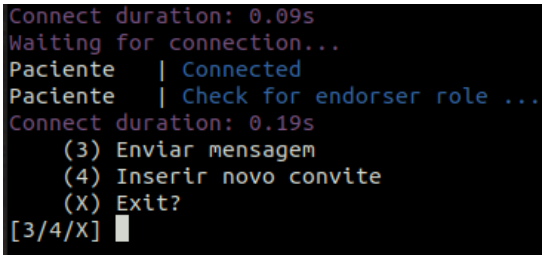


Figura 4. Tela inicial do paciente
O autor

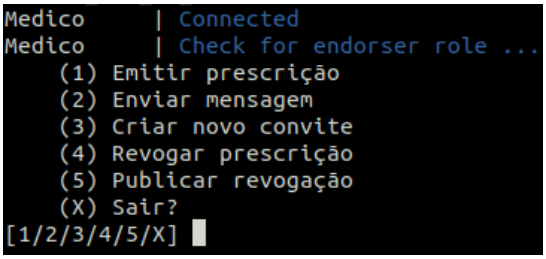
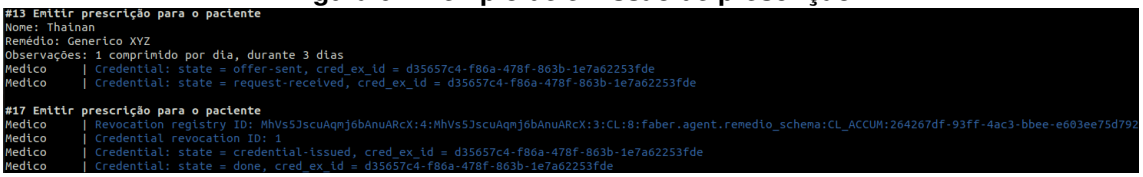


Figura 5. Menu de opções do médico
O autor

meio de um comunicação direta entre o Agente do farmacêutico e do médico. O paciente pode então dispensar uma segunda medicação, ou ir a uma segunda farmácia e realizar o processo novamente.

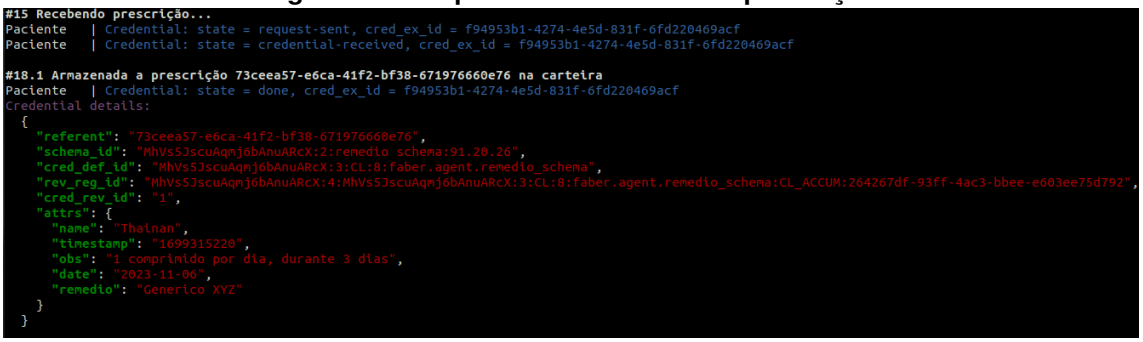
A apresentação da prescrição para o farmacêutico segue o paradigma da Identidade Auto Soberana, utilizando a minimização de dados e divulgação seletiva. Dessa forma, é possível por exemplo apresentar apenas o campo da medicação, sem precisar mostrar nenhum dado pessoal do paciente. Porém, certos tipos de prescrições/medicamentos exigem alguma identificação. Uma forma privativa seria a identificação por biometria (em carteiras digitais em *smartphones*), autenticando o paciente sem a necessidade de expor dados pessoais. Caso um arranjo por biometria não esteja disponível, o paciente terá que se autenticar de forma tradicional, idealmente, sem que seus dados sejam registrados em nenhum tipo de sistema, ou registrado de forma pseudo-anônima.

Figura 6. Exemplo de emissão de prescrição



O autor

Figura 7. Exemplo de recebimento de prescrição

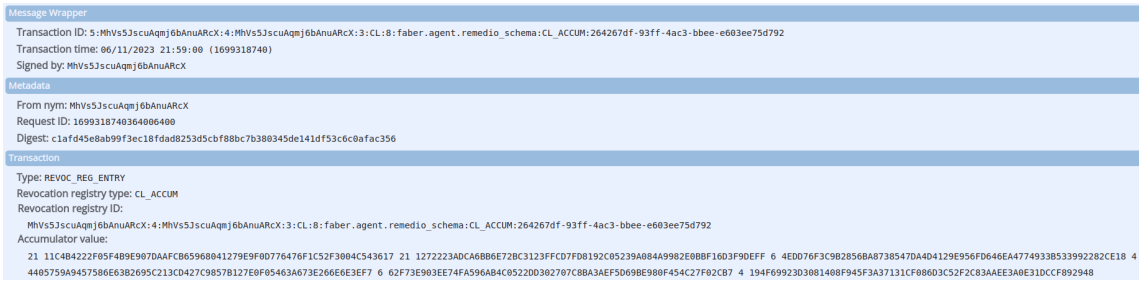


O autor

Figura 8. Exemplo de revogação de prescrição

O autor

Figura 9. Transação da revogação na rede Indy



O autor

7. Considerações Finais e Trabalhos Futuros

7.1. Considerações Finais

Este trabalho teve como objetivo investigar tópicos, ferramentas e tecnologias que viabilizam a aplicação do modelo de Identidade Auto-Soberana no manejo de dados de saúde. O uso da ferramenta Hyperledger Indy para o registro distribuído contribui para a descentralização. A Indy oferece a capacidade de estabelecer confiança, onde o emissor das credenciais verificáveis tem seu DID e chave de verificação registrados na Blockchain, sujeitos à verificação pelo receptor. Enquanto a rede distribuída estiver operacional, o registro permanecerá acessível.

Por ser um sistema distribuído, evita-se (ou dificulta-se) pontos únicos de falha e perda de dados, proporcionando maior disponibilidade ao sistema. Os dados dos pacientes em sua carteira digital oferece controle e privacidade, sendo também uma forma eficiente de transporte desses dados. Os dados em posse do paciente podem ser transportado entre diferentes agentes de saúde, ou estados e até países. Nenhum dado pessoal é guardado nos registros distribuídos.

O protótipo pode ser facilmente adaptado para emitir a prescrição em algum formato para Interoperabilidade, tal como o padrão para troca de dados de saúde FHIR [Health Level Seven International 2023], que é utilizado pela Rede Nacional de Dados de Saúde [Rede Nacional de Dados em Saúde 2023].

Outras implementações de prescrições médicas que utilizam Blockchain, como em A1, A2, A3 e A4 salvam os dados de saúde pessoais de forma criptografada diretamente nos registros distribuídos. Porém, a criptografia que é segura hoje, pode ser quebrada no futuro, expondo esses dados escritos em um registro permanente. A escolha de manter os dados pessoais todos fora dos registros distribuídos evita esses esquemas de criptografias elaborados e garante maior adequação aos processos legais.

Os protocolos do Hyperledger Aries oferecem uma interface que facilita a intera-

ção entre distintos participantes, possibilitando a emissão e gestão de credenciais verificáveis. Através desses projetos, várias implementações de modelos de Identidade Auto-Soberana podem coexistir. Esses novos modelos promovem maior privacidade, segurança e controle de propriedade sobre os dados dos usuários.

Outro ponto da proposta é o armazenamento dos dados de forma distribuída em posse dos pacientes, oferecendo a possibilidade de extensão para outros dados (boletins médicos, exames, históricos) sem que o sistema em si precise ampliar sua capacidade de armazenamento.

Ao empregar esse modelo, este trabalho conseguiu estabelecer, com sucesso, um protótipo para a emissão e revogação de prescrições médicas eletrônicas no formato de credenciais verificáveis, fundamentado na tecnologia Blockchain e Identidade Auto Soberana, fornecendo meios para o manejo adequado de dados sensíveis tais quais os dados de saúde de um indivíduo. Esse protótipo resultou na criação de uma prescrição médica que assegura mecanismos de divulgação seletiva. A prescrição, sob a custódia do paciente, proporciona uma utilização da prescrição com privacidade de seus dados.

Com o tempo, é possível que mais pessoas perceberão a importância de cuidar bem das suas informações digitais. É provável que ainda tenhamos um extenso percurso a percorrer para aprimorar a gestão de nossos dados, que incluirá modelos de administração de identidades digitais, como o de Identidade Auto-Soberana. No futuro , é provável que novas políticas, mecanismos e paradigmas para o gerenciamento de dados serão desenvolvidos. Tecnologias, como a Blockchain, e ferramentas, como Hyperledger Indy e Aries, se tornarão parte integrante desse futuro, provavelmente crescendo e se fortalecendo à medida que nos adaptamos à vida online.

7.2. Trabalhos Futuros

Podemos citar como possíveis trabalhos futuros:

- Aperfeiçoamento do protótipo, adicionando o agente Aries do farmacêutico para se comunicar com o paciente e a rede;
- Implementar uma interface gráfica do usuário para facilitar o uso;
- Adicionar a compatibilidade com aplicativos móveis de carteiras digitais, assim os usuários podem utilizar seus celulares.
- Oferecer a emissão da credencial verificável em um formato JSON FHIR [Rede Nacional de Dados em Saúde 2023], de forma a ser compatível com a Rede Nacional de Dados de Saúde.
- Aprimorar o processo de revogação por meio de um agente Aries em um servidor na nuvem, facilitando a comunicação entre os agentes do farmacêutico e do médico.

Referências

Aldughayfiq, B. and Sampalli, S. (2021). Digital health in physicians' and pharmacists' office: A comparative study of e-prescription systems' architecture and digital security in eight countries. volume 25, pages 102–122.

Allen, C. (2016). The path to self-sovereign sdentity.

Babu, G. K. and Thiyagarajan, P. (2021). The current state of prescriptions and potential enhancements using blockchain. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–6.

Benita, R., S., G. K., B., M., and A, M. (2020). Authentic drug usage and tracking with blockchain using mobile apps. *International Journal of Interactive Mobile Technologies (iJIM)*, 14(17):pp. 20–32.

Brasil (2018). Lei n° 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd). *Diário Oficial [da] República Federativa do Brasil*.

Curran, S. (2021). Aries cloud agent internals: Agent and controller.

El Maliki, T. and Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. In *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, pages 12–17.

Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access*, 7:103059–103079.

Foundation, L. (2015). Hyperledger.

Garcia, R. D., Sankar Ramachandran, G., Jurdak, R., and Ueyama, J. (2022). A blockchain-based data governance with privacy and provenance: a case study for e-prescription. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–5.

Health Level Seven International (2023). Welcome to fhir. Acesso em: 25 de novembro de 2023.

Hyperledger (2019a). Hyperledger aries.

Hyperledger (2019b). Hyperledger aries cloud agent - python.

Isaak, J. and Hanna, M. J. (2018). User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, 51(8):56–59.

ISO (2019). It security and privacy – a framework for identity management – part 1: Terminology and concepts. Standard, International Organization for Standardization.

Li, J. (2020). A new blockchain-based electronic medical record transferring system with data privacy. In *2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT)*, pages 141–147.

Maria, C. and Sebastião, E. (2011). *Manual de orientações básicas para prescrição médica*. Conselho Regional de Medicina do Estado da Paraíba/Conselho Federal de Medicina, 2 edition.

Murugesan, S. and Sorwar, G. (2010). Electronic medical prescription: An overview of current status and issues. *Biomedical Knowledge Management: Infrastructures and Processes for E-Health Systems*, pages 61–81.

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity.

Naik, N. and Jenkins, P. (2020). Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. In *2020 IEEE International Symposium on Systems Engineering (ISSE)*, pages 1–6.

of British Columbia, P. (2021). Von network.

of British Columbia, P. (2022). Indy tails server.

Pastuchov, A. and Curran, S. (2019). Introduction to hyperledger indy.

Rede Nacional de Dados em Saúde (2023). Tecnologias - rede nacional de dados em saúde (rnds).

Saúde Digital Brasil (2022). Atendimentos via telemedicina para casos de influenza e covid-19 dobram a cada 36 horas.

Scheffer, M., Cassenote, A. J., Alves, M. T., and Russo, G. (2022). The multiple uses of telemedicine during the pandemic: the evidence from a cross-sectional survey of medical doctors in brazil open access. *Globalization and Health*, 18:81.

Shcherbakov, A. (2019). Hyperledger indy public blockchain node with alexander shcherbakov.

Sovrin (2023). Sovrin.

Thatcher, C. and Acharya, S. (2020). Rxblock: Towards the design of a distributed immutable electronic prescription system. *Network Modeling Analysis in Health Informatics and Bioinformatics*, 9.

Ying, B., Sun, W., Mohsen, N. R., and Nayak, A. (2019). A secure blockchain-based prescription drug supply in health-care systems. In *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, pages 1–6.