

Blockchain And Self-Sovereign Identity: A Healthcare Use Case

Matheus Lázaro Honório da Silva¹

Gislainy Velasco¹, Noeli Antônia Pimentel Vaz^{1 2}, Matheus Brito Martins¹,
Pedro Moraes Ribeiro Gonçalves Silva¹, Sergio T. Carvalho¹

¹Instituto de Informática - Universidade Federal de Goiás (UFG)

²Instituto Acadêmico de Ciências Exatas e Tecnológicas - Universidade Estadual de Goiás (UEG)

{matheus.lazaro, gislainycrisostomo, noelivaz}@discente.ufg.br

{matheus.b.m, pedro.ribeiro}@discente.ufg.br

sergiocarvalho@ufg.br

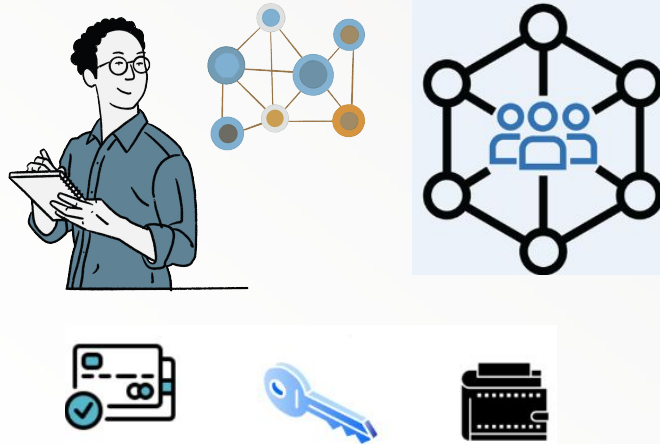
Motivação

1. A **transformação digital** tem provocado mudanças significativas em diversos setores, sendo a saúde um dos mais impactados.
 - a. Tem impulsionado a criação de **sistemas clínicos distribuídos e interoperáveis**.
2. Relaciona-se ao avanço da **digitalização na saúde**, que amplia o compartilhamento de dados, mas também os riscos de **vazamentos, fraudes e falta de controle pelo paciente**.
3. Demandas por **privacidade, rastreabilidade e interoperabilidade** crescem, impulsionadas por normas como a **LGPD/GDPR**.



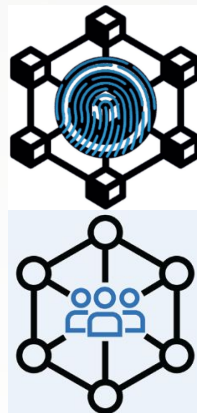
Problema

- **Sistemas centralizados** dificultam a **governança descentralizada** e tornam pacientes **dependentes de intermediários** para acessar ou compartilhar seus dados clínicos. Falta **autonomia**, **privacidade seletiva** e **auditabilidade confiável**.



Objetivo

- Elaborar uma arquitetura híbrida on-chain/off-chain que integra **blockchain permissionada e identidade autossobrerana (SSI)** e, então, permitir que pacientes **controlem, compartilhem e verifiquem credenciais e dados clínicos** com consentimento explícito.

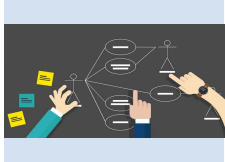


Blockchain em Saúde



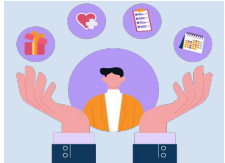
Redes permissionadas

- Participação controlada (leitura, escrita e validação).
- Assegura-se confiança mesmo entre entidades com interesses distintos. Ex.: hospitais, clínicas e laboratórios.
- Hyperledger Fabric é modularizável para diferentes circunstâncias de descentralização de dados e de governança.



Casos de uso já validados

- Prontuários eletrônicos.
- Rastreamento de fármacos.
- Gestão de consentimentos.
- Demonstra-se a viabilidade em auditabilidade e interoperabilidade.



Benefícios

- Transparência e integridade dos registros médicos (funções hash).
- Rastreabilidade.
- Dificulta fraudes ou manipulações.



Desafios

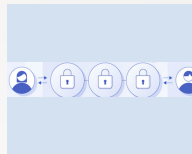
- Escalabilidade técnica e regulatória.
- Interoperabilidade entre redes distintas.
- Busca por um padrão único global para saúde.

Identidade Digital e SSI



Identidade digital

- Base para **autenticação** e **autorização** segura.
- **Representação** de uma pessoa ou dispositivo por meio de atributos verificáveis.



ZKP (Prova de Conhecimento Zero)

- Permite **provar atributos** (ex: maioria) sem expor dados sensíveis (ex: data de nascimento).
- Reforça a **privacidade** dos usuários em **sistemas descentralizados**.

Self-Sovereign
Identity
(SSI)

SSI (Identidade Autossoberana)

- Usuários controlam suas próprias credenciais (**DIDs** e **VCs**), dispensando autoridades centrais.
- **Carteira digital:** consentimento granular e revogação independente de terceiros.



AnonCreds

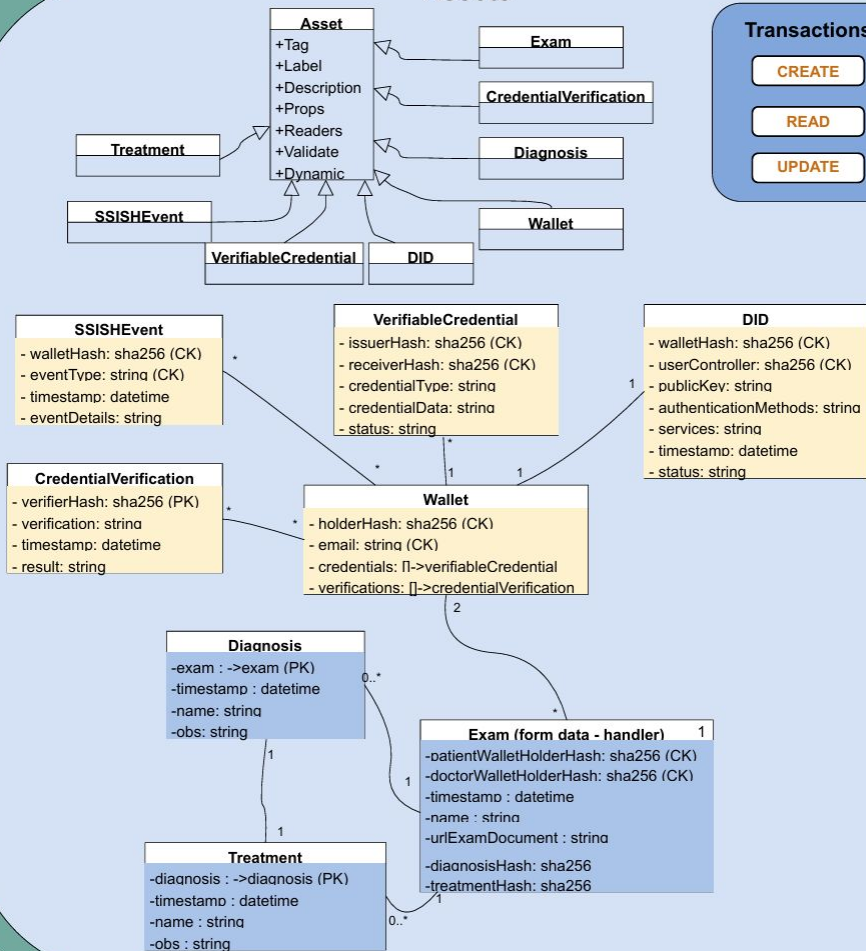
- Modelo com três níveis de atributos: visíveis, comprometidos e predicados com ZKP.
- Adotado por Hyperledger Indy para garantir **verificações criptográficas** e **privacidade seletiva**.

Trabalhos Relacionados

1. Nascimento-Silva-Jr et al.	Propõem blockchain para proteger dados de saúde, destacando riscos de vazamento e fraude. Não abordam SSI, DIDs ou carteiras digitais.
2. Robichez et al	Discutem uso de blockchain na identificação cidadã em governos, com foco em transparência. Não tratam de SSI nem de aplicações clínicas.
3. Leite & Henriques	Analizam a transição de modelos federados para descentralizados, priorizando privacidade. Não apresentam solução prática aplicada à saúde.
4. Wolff & Henriques	Aplicam SSI em contexto acadêmico via RNP (Rede Nacional de Ensino e Pesquisa), com foco técnico e em governança. Não envolvem saúde nem credenciais clínicas.
5. Vora et al. 6. Xu et al	Propõem arquiteturas para consentimento e prontuários com blockchain, mas sem adoção de princípios de SSI como DIDs, VCs ou controle pelo paciente.

Chaincode

Assets



Modelo de dados do Chaincode

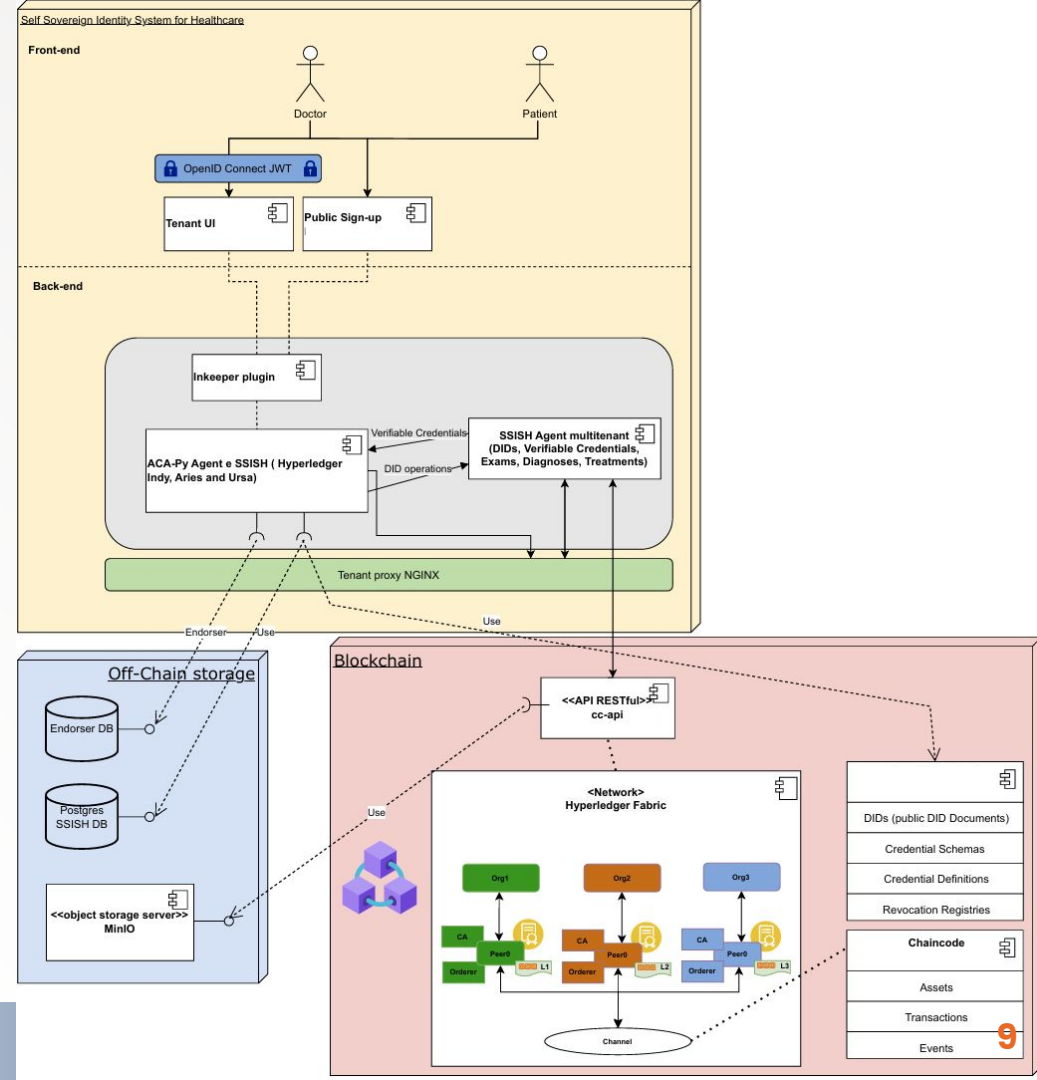
Hyperledger Indy, Aries, Ursa, e integração SSISH

ACA-Py multitenant:

- cada tenant = clínica, médico ou paciente.

Fluxos DIDComm:

- Conexão --> Emissão de credencial --> Solicitação de comprovante/Verificação.

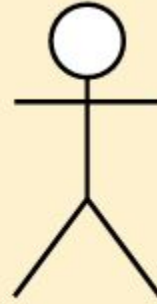


Caso de Uso: Stakeholders



Doctor

Dr. Carlos: médico, emissor e verificador de credenciais.



Patient

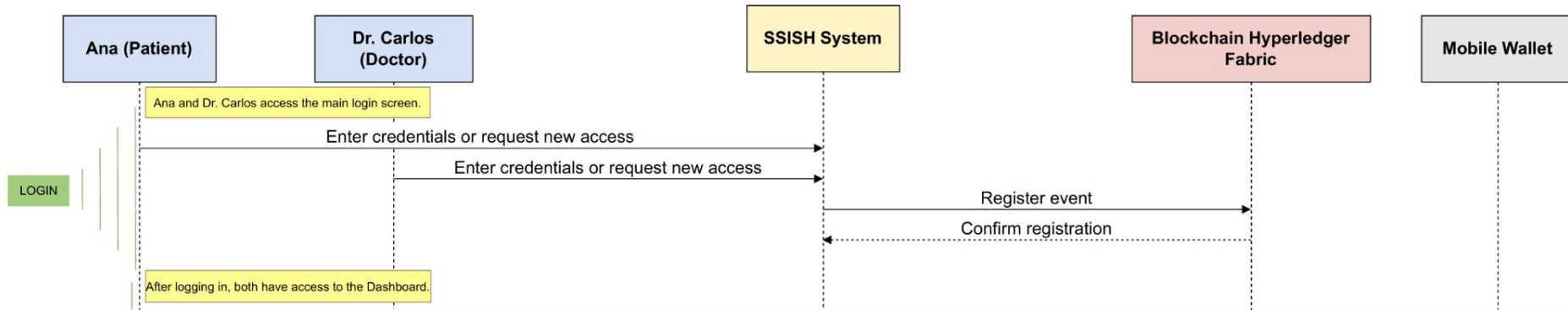
Ana: paciente, quer privacidade e posse do histórico médico.

Laboratórios/Clínicas: emitir laudos;

Seguradoras: verificar carteira digital para receber, armazenar, compartilhar VCs.

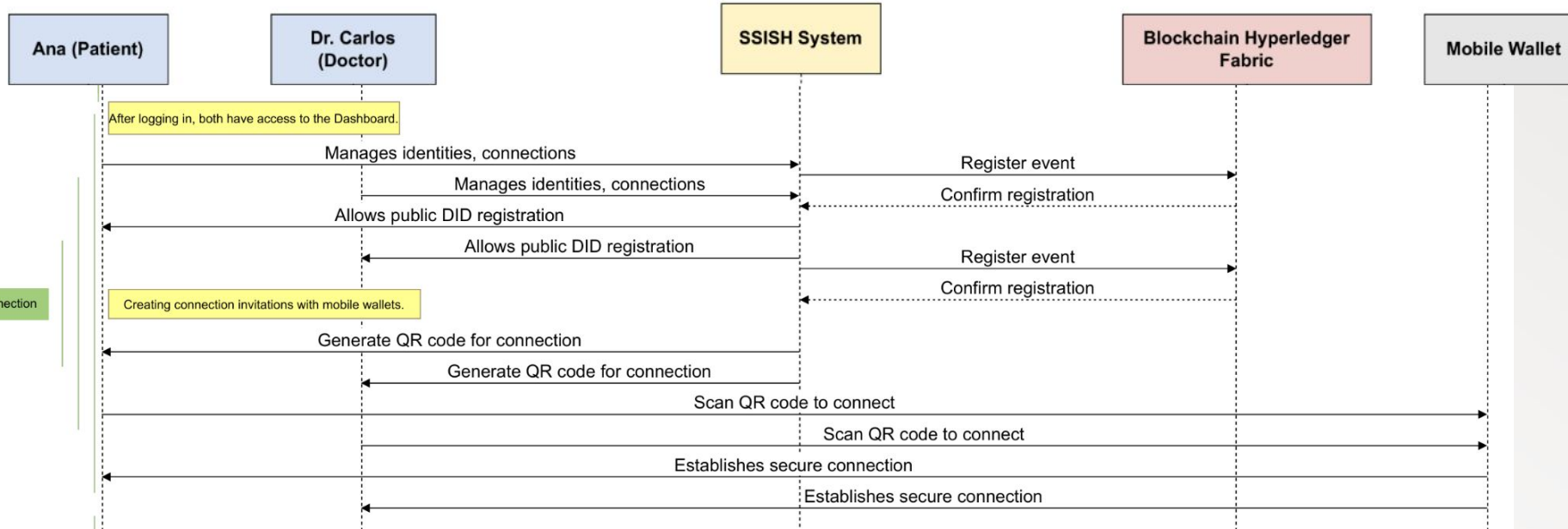
Protótipo SSISH – Fluxo Operacional

Cenário de Login e Registro



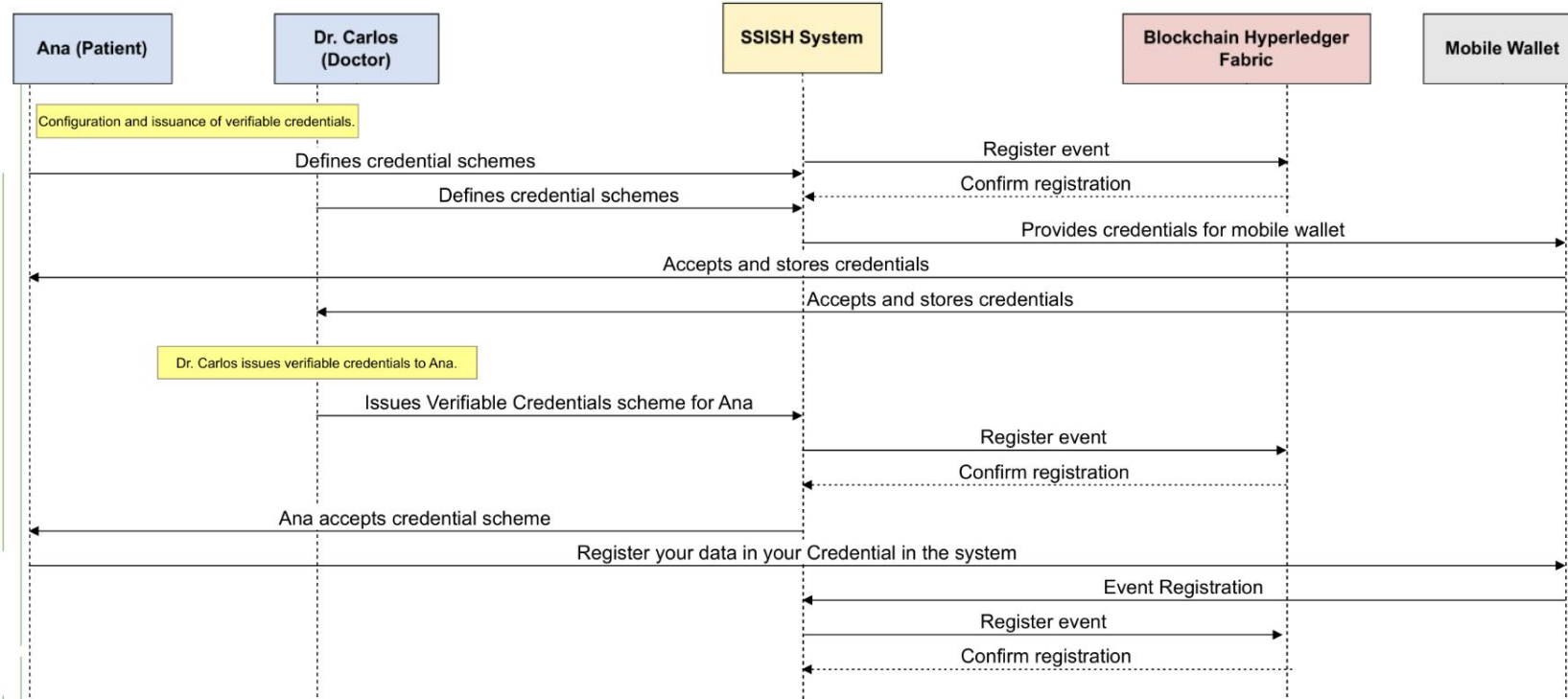
Protótipo SSISH – Fluxo Operacional

Dashboard, DID e Conexão



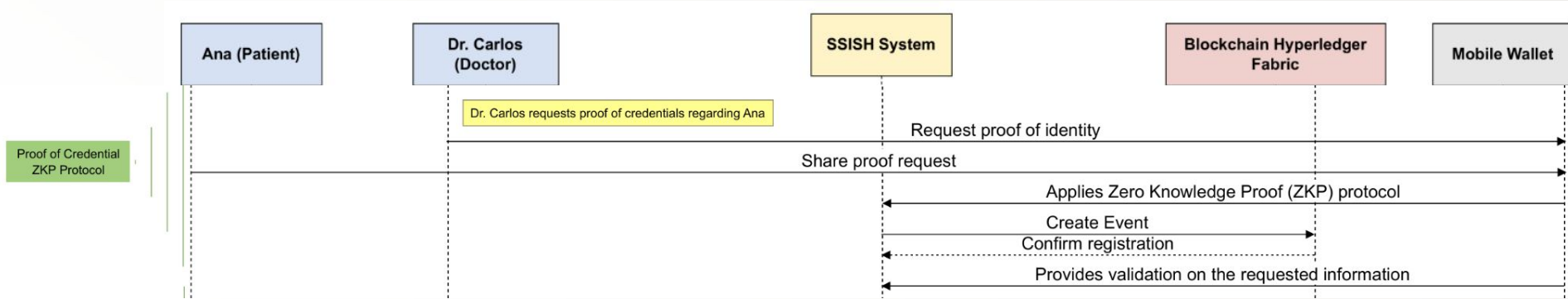
Protótipo SSISH – Fluxo Operacional

Configuração e Emissão de Credenciais Verificáveis



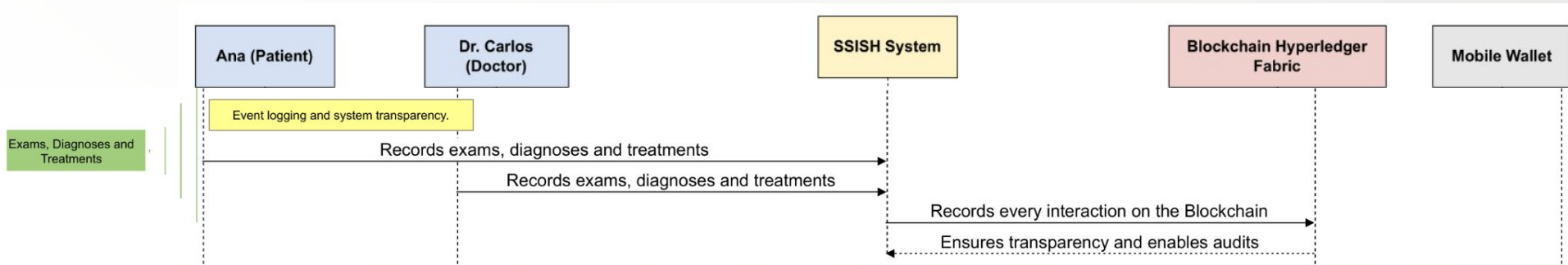
Protótipo SSISH – Fluxo Operacional

Prova de Credencial - Prova de Conhecimento Zero



Protótipo SSISH – Fluxo Operacional

Exames, Diagnósticos e Tratamentos



Benefícios e Limitações

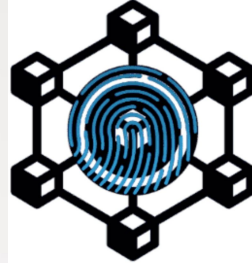


Benefícios observados:

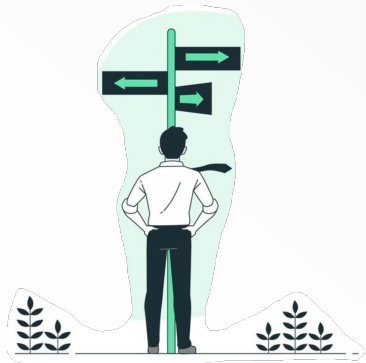
- +Soberania do paciente (gestão própria de dados clínicos e credenciais).
- +Auditoria e rastreabilidade de eventos de saúde (exames, diagnósticos, tratamentos).
- +Confidencialidade com abordagem híbrida e ZKP (verificação sem revelação total).

Limitações identificadas:

- Validação limitada ao ambiente de testes controlado.
- Desafios em orquestração de rede e múltiplas instituições.
- Integração com sistemas legados (como prontuários eletrônicos) demanda padronização.



Próximos passos e Conclusão



Próximos passos:

- Testes de carga para avaliar escalabilidade.
- Suporte a interoperabilidade via FHIR (Recursos rápidos de interoperabilidade em saúde) para integração com sistemas de saúde existentes.
- Exploração de ZKPs avançadas para anonimato verificável em auditorias públicas em saúde.

Conclusão:

- A arquitetura SSISH demonstra que é possível registrar eventos imutáveis e emitir/verificar VCs com privacidade seletiva.
- A integração com agentes ACA-Py simplifica credenciamento e provas criptográficas.



Protótipo SSISH – Capturas de Tela

Dashboard, DID e Conexão

MATHEUS LÁZARO HONÓRIO
DA SILVA

Self Sovereign Identity System for Healthcare

Matheus Lázaro - Ciência da Computação - UFPA

Dashboard

Conexões

Emissão

Verificação

Configuração

Mensagens

Sobre

Dashboard

Exame

Registrar Exame

Listar Exames

Diagnóstico

Registrar Diagnóstico

Listar Diagnósticos

Tratamento

Registrar Tratamento

Listar Tratamentos

Outras ações

Listar Eventos do Sistema

Minhas Credenciais Verificáveis

Minhas Verificações de Credenciais Verificáveis

Minha Carteira

MATHEUS LÁZARO HONÓRIO
DA SILVA

Self Sovereign Identity System for Healthcare

Matheus Lázaro - Ciência da Computação - UFPA

Dashboard

Conexões

Emissão

Verificação

Configuração

Mensagens

Sobre

Perfil do Inquilino

ID do Inquilino

6a14edef-ab26-4537-a3a8-2a9d17d67323

ID da Carteira

x2f43c34-bb5c-43d8-964b-a1fd86329e8e

Nome

Matheus Lázaro Honório da Silva

E-mail de Contato

matheus.lazaro@discente.ufpa.br

Emissor

Livro Razão Atual: bccviri-dev

Aplicador

Connect	Ledger	Alias
Status: active	bccviri-dev	bccviri-dev-endorser
	bccviri-test	bccviri-test-endorser

Endorser Details

DID Public

Register	Ledger Identifier
Ⓢ	bccviri-dev
	bccviri-test

DID Public

FqDw5Sk35yLJabEYTApQ

Public DID Details

Aceitação da TAA

Nenhum Acordo de Autorização de Transação é necessário para este livro razão.

Criado em

May 27 2024, 9:05:19 PM

Atualizado em

May 27 2024, 9:05:19 PM

Registro de DID Público enviado

Ativa DID atualizado com sucesso

Protótipo SSISH – Capturas de Tela

Dashboard, DID e Conexão

MATHEUS LÁZARO HONÓRIO
DA SILVA

Dashboard

Conexões

Conexões

Convites

Emissão

Verificação

Configuração

Mensagens

Sobre

Self Sovereign Identity System for Healthcare

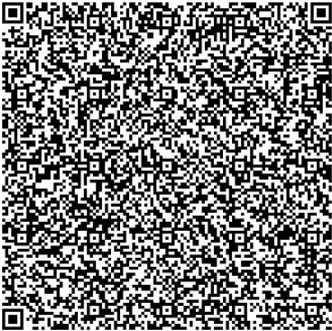
Matheus Lázaro - Ciência da Computação - INF UFG

Convites

Criar Convite

Alíngs da Conexão

Conexão para Paciente - SSISH - Matheus Lázaro



URL do Convite

https://fc8e-177-149-133-164.ngrok-free.app?c_id=

Fechar

Buscar Convites

o de Convite

Protocolo

Criado Em

connections/1.0

May 27 2024, 9:13:58 PM

10

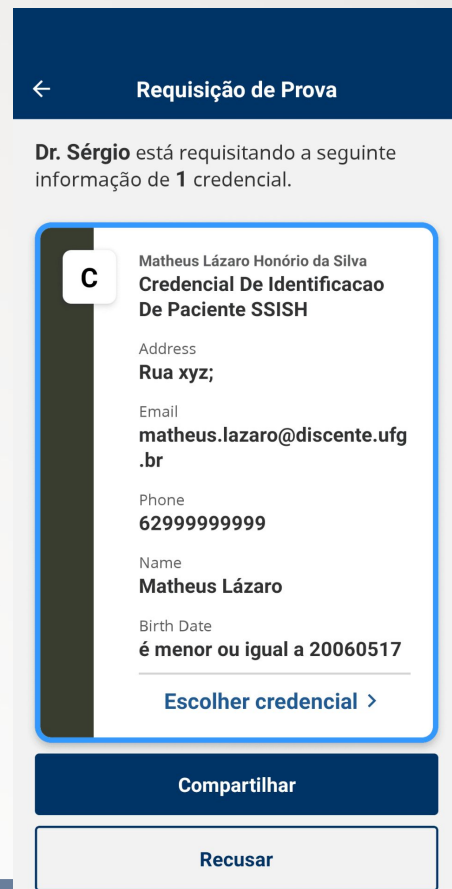
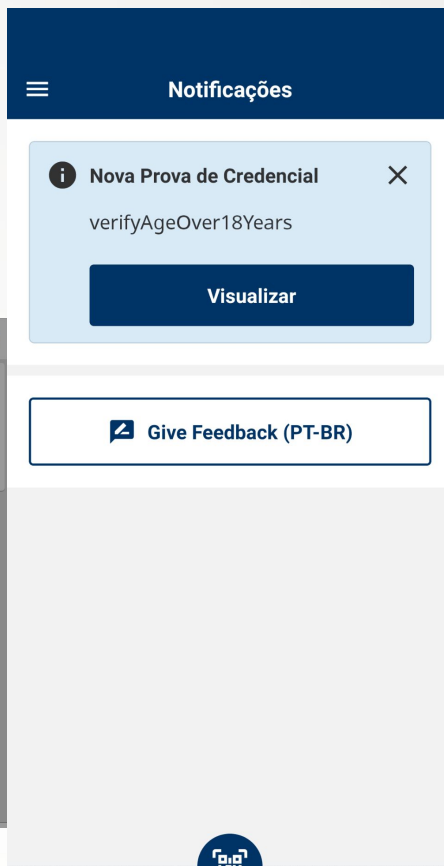
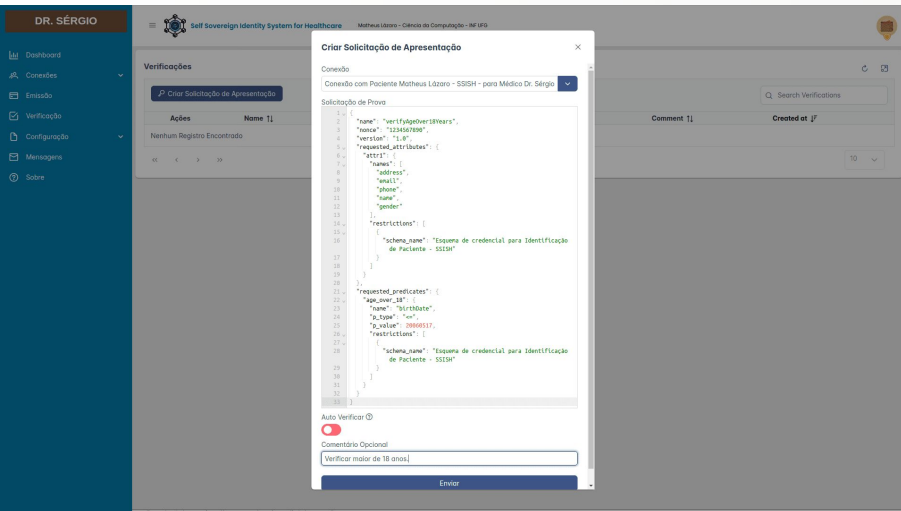
Invitation Created

Evento registrado na Blockchain!

19

Protótipo SSISH – Capturas de Tela

Prova de Credencial - Prova de Conhecimento Zero



Notificações

Scanear

Credenciais

Exames, Diagnósticos e Tratamentos

[illegible]

Protótipo SSISH – Capturas de Tela

Exames, Diagnósticos e Tratamentos

DR. SÉRGIO

Dashboard

Conexões

Emissão

Verificação

Configuração

Mensagens

Sobre

Self Sovereign Identity System for Healthcare

Matheus Lázaro – Clínica de Computação – INF UFS

Registrar Tratamento

🔔 O Diagnóstico deverá ser cadastrado em Dashboard » Diagnóstico » Registrar diagnóstico

Diagnóstico *

Diagnóstico 2 ssish

Nome do Tratamento *

Tratamento 2

Observações

Tratamento para o diagnóstico apontado para o exame oftalmológico do Matheus Lázaro.

Registrar Tratamento

Tratamento registrado com sucesso

Matheus Lázaro Honório da Silva

Dashboard

Conexões

Emissão

Verificação

Configuração

Mensagens

Sobre

Self Sovereign Identity System for Healthcare

Matheus Lázaro – Clínica de Computação – INF UFS

Meus Tratamentos

Tratamento 2

Diagnóstico: Diagnóstico 2 ssish

Data do Tratamento: 27/05/2024, 23:08:27

Observações: Tratamento para o diagnóstico apontado para o exame oftalmológico do Matheus Lázaro.

Tratamento ssish 1

Diagnóstico: Diagnóstico 1 ssish

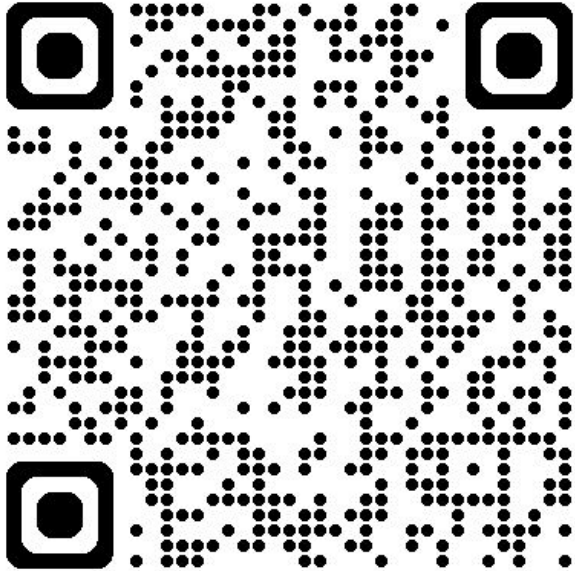
Data do Tratamento: 27/05/2024, 23:03:50

Observações: Obs. tratamento ssish 1.

Código

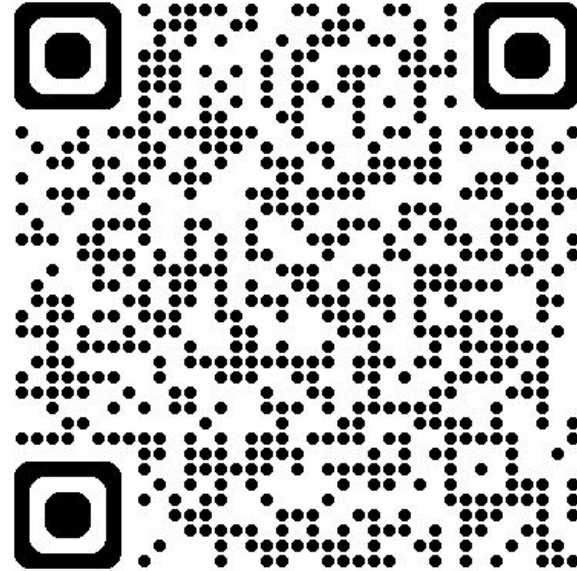
Blockchain Hyperledger Fabric - SSISH

<https://github.com/SelfSovereignIdentity-SystemHealthcare/blockchainFabric-SSISH>



SSISH - Self Sovereign Identity System for Healthcare

<https://github.com/SelfSovereignIdentity-SystemHealthcare/SSISystem>



Perguntas?

Obrigado!