

Interoperabilidade e Segurança de Identidades na Web 3.0: Gestão de Identidade Digital Descentralizada com Blockchain

Diogo Menezes Ferrazani Mattos

menezes@midiacon.uff.br

LabGen/MídiaCom – PPGEET/TCE/IC

Universidade Federal Fluminense (UFF) - Niterói, Brazil

Projeto Ilíada

- **GT-PIDDF:** *Desenvolvimento de uma Plataforma de Identidade Digital Descentralizada com Autenticação Federada*
 - **Coordenador**
 - **Diogo Menezes Ferrazani Mattos**
 - **Vice-coordenadora**
 - **Dianne Scherly Varela de Medeiros**



Diogo Mattos
Coordenador



Dianne Medeiros
Vice-Coordenadora



Nicollas Rodrigues
Pesquisador



Guilherme Nasseh
Desenvolvedor



Yago Rezende
Desenvolvedor



Matheus Belato
Assistente de
Desenvolvimento



Carolina Rocha
Assistente de
Desenvolvimento

Gestão de Identidades Digitais

Cenário Emergente

❖ Web 3.0

- Aumento das transações digitais
- Necessidade crescente de segurança e privacidade

❖ Sistemas Tradicional de Identidade

- Baseados em modelos centralizados
 - Único Provedor de Identidade (IDP)
 - *Única credencial para acessar múltiplos serviços*

❖ Consequências Negativas



Vulnerabilidade a Ataques

- *Aumentando o risco de vazamento de dados*



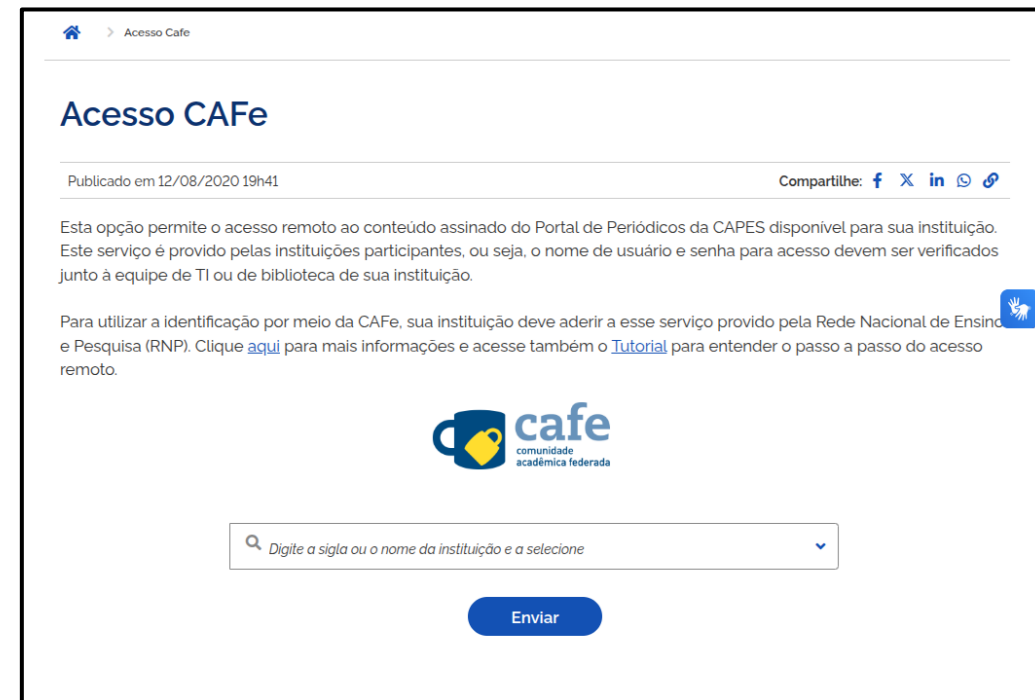
Perda de Controle

- *Os usuários perdem autonomia sobre suas informações no IDP*



Dependência do Provedor

- *A segurança dos dados depende inteiramente do IDP*



Identidade Federada

Centralizada → Federada → Descentralizada

❖ Premissa Básica

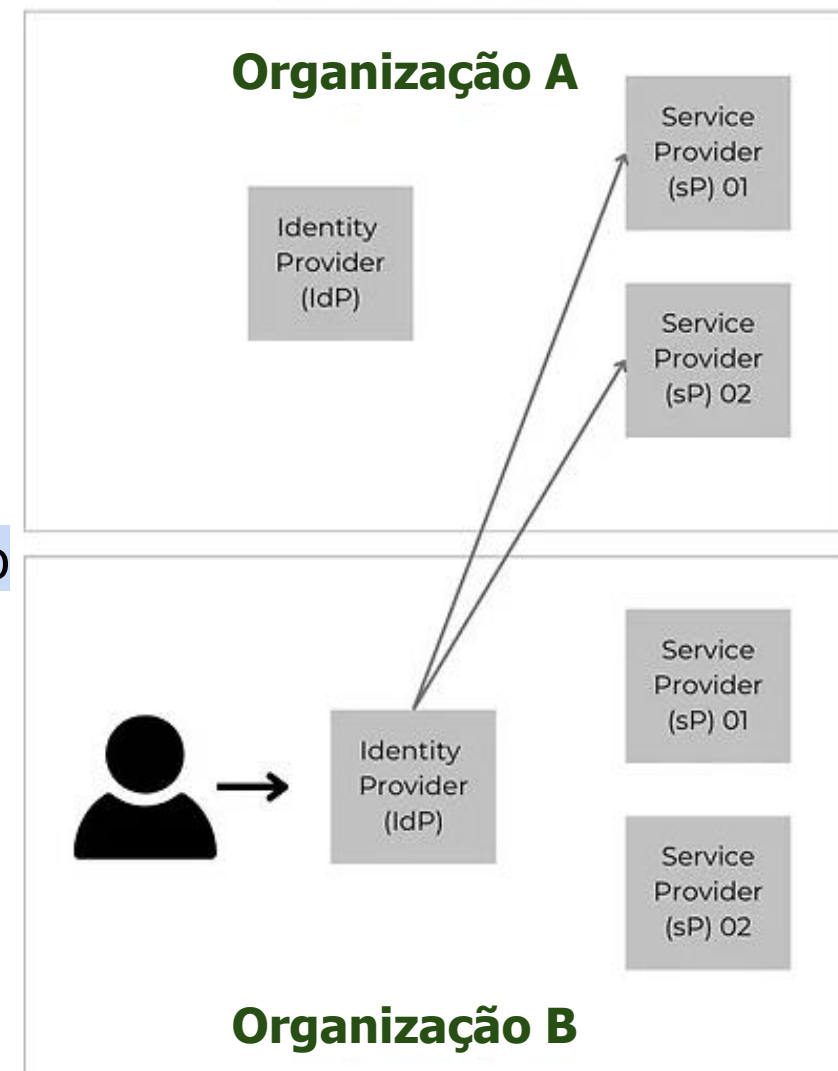
- Vários provedores de identidade colaboram dentro de um círculo de confiança

Consequências

- Usuários podem autenticar-se em MÚLTIPLOS serviços
 - Utilizando uma única credencial provida por um IDP federado → aceita por diversos provedores de serviço

❖ Desafios

- Compatibilidade com regulamentos
 - GDPR e LGPD
- Integração com sistemas legados e IDPs existentes



Plataforma PIDDF

Proposta

PIDDF → Plataforma de **I**dentidade **D**igital **D**istribuída com autenticação **F**ederada

Principais Características

❖ **Gestão Descentralizada de Identidade**

- Utiliza a arquitetura de referência do Trustbloc
 - Garantia do controle e segurança de dados pelos usuários

❖ **Autenticação Federada Avançada**

- Integra Keycloak com suporte ao padrão OAuth 2.0
 - Compatibilidade com sistemas legados → Web 2.0

❖ **Infraestrutura Cloud-Native**

- Adota Kubernetes e Docker para escalabilidade e desempenho robustos

Identidade Autossobrerana - *Conceitos Relacionados* LabGen

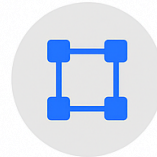
Registros digitais emitidos por uma entidade confiável e verificáveis criptograficamente por qualquer parte interessada.

Usuário controla, gerencia e compartilha seus dados de sem depender de autoridades intermediárias

Identidade Autossobrerana



Credenciais Verificáveis



Blockchain



Identificadores Descentralizados

Identificadores digitais únicos, persistentes e verificáveis, que não dependem de uma autoridade central

Registro distribuído, imutável e seguro que elimina a necessidade de intermediários

❖ Identificadores Descentralizados

- Sequência de texto simples → identificadores únicos globais
 - Detentores são os controladores

➤ Propriedades



Descentralizado

- Independente de uma autoridade central para sua emissão



Persistente

- Continua existindo sem necessidade de uma organização mantenedora



Resolvível

- Permite recuperar metadados associados durante o processo de resolução



Criptograficamente Verificável

- Possibilita comprovar controle e posse por meio de criptografia

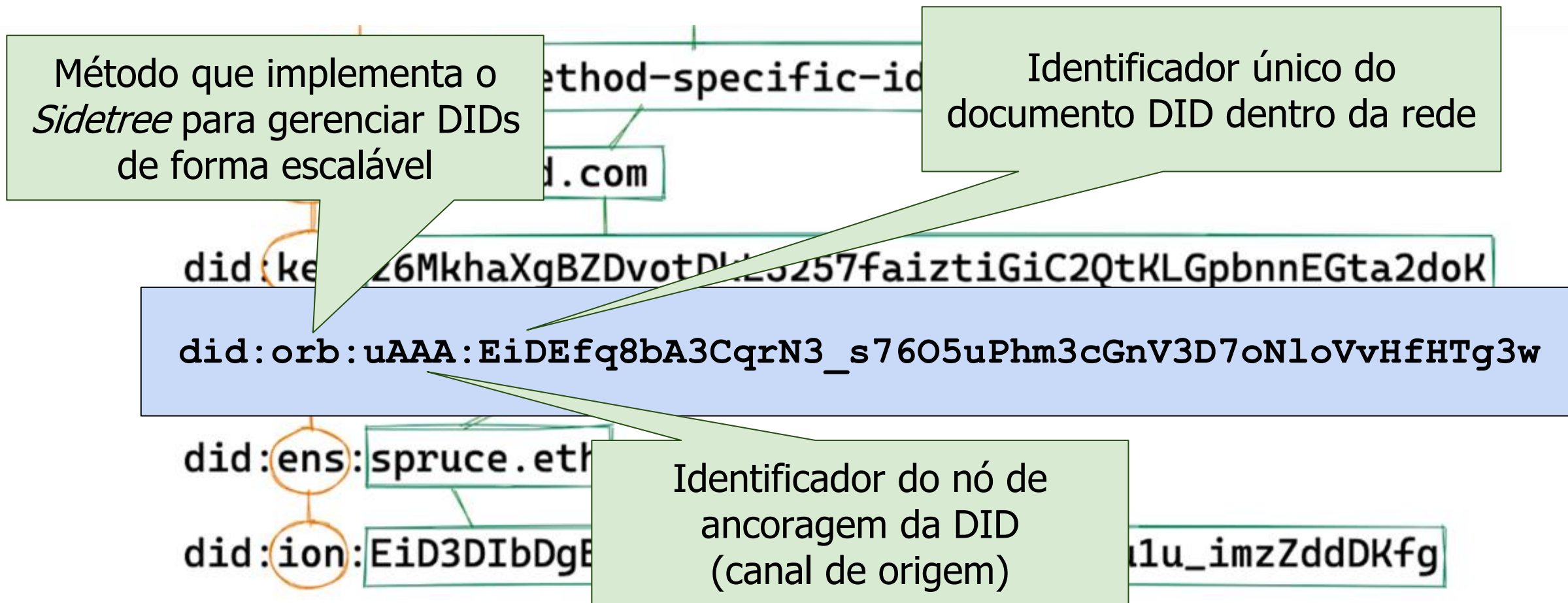
❖ Métodos

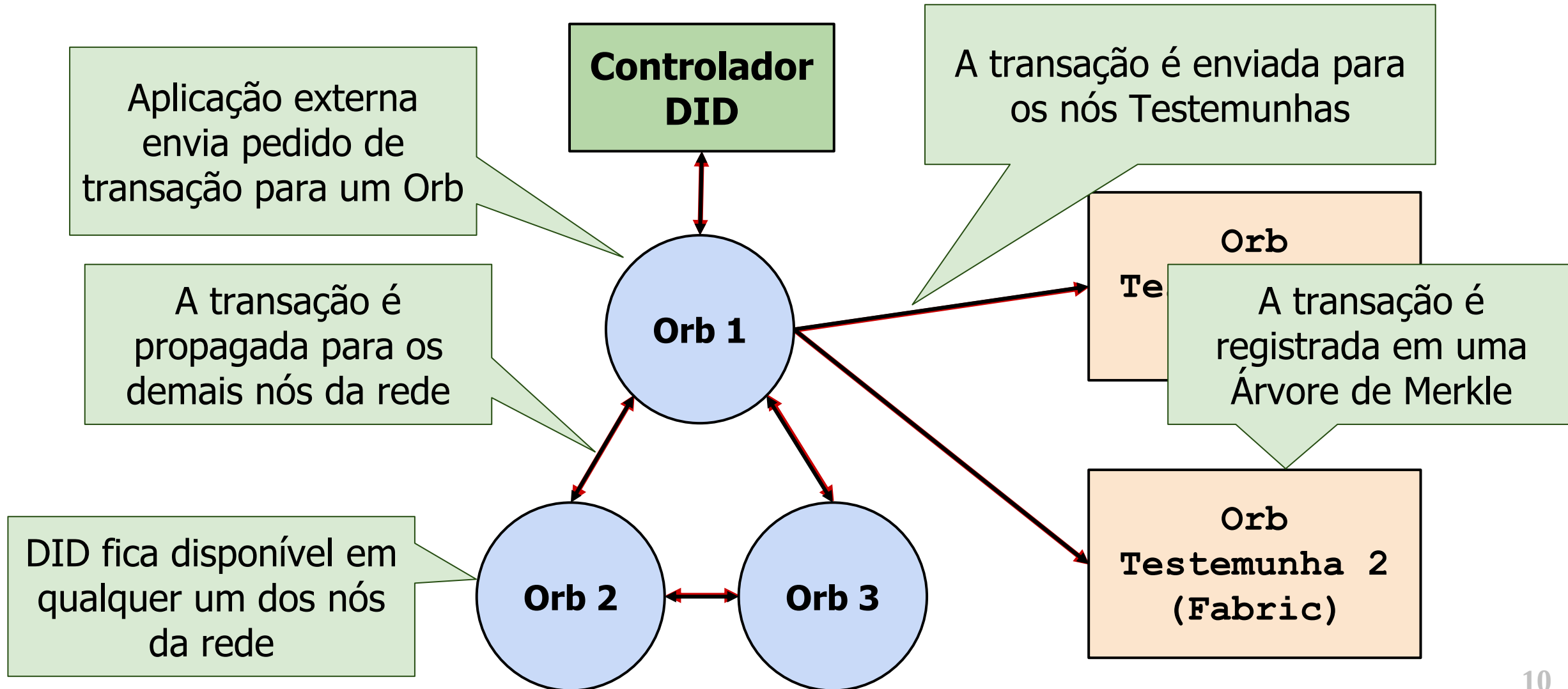
- *"Especificações que definem como um DID é criado, gerenciado e vinculado a um par de chaves pública/privada"*



➤ Sintaxe Básica

- **did**: O prefixo que indica que é um identificador descentralizado
- **<método>**: O método DID que define o funcionamento técnico e a rede associada
 - *Existem atualmente **184** métodos predefinidos*
- **<identificador específico>**: Um identificador único dentro do método

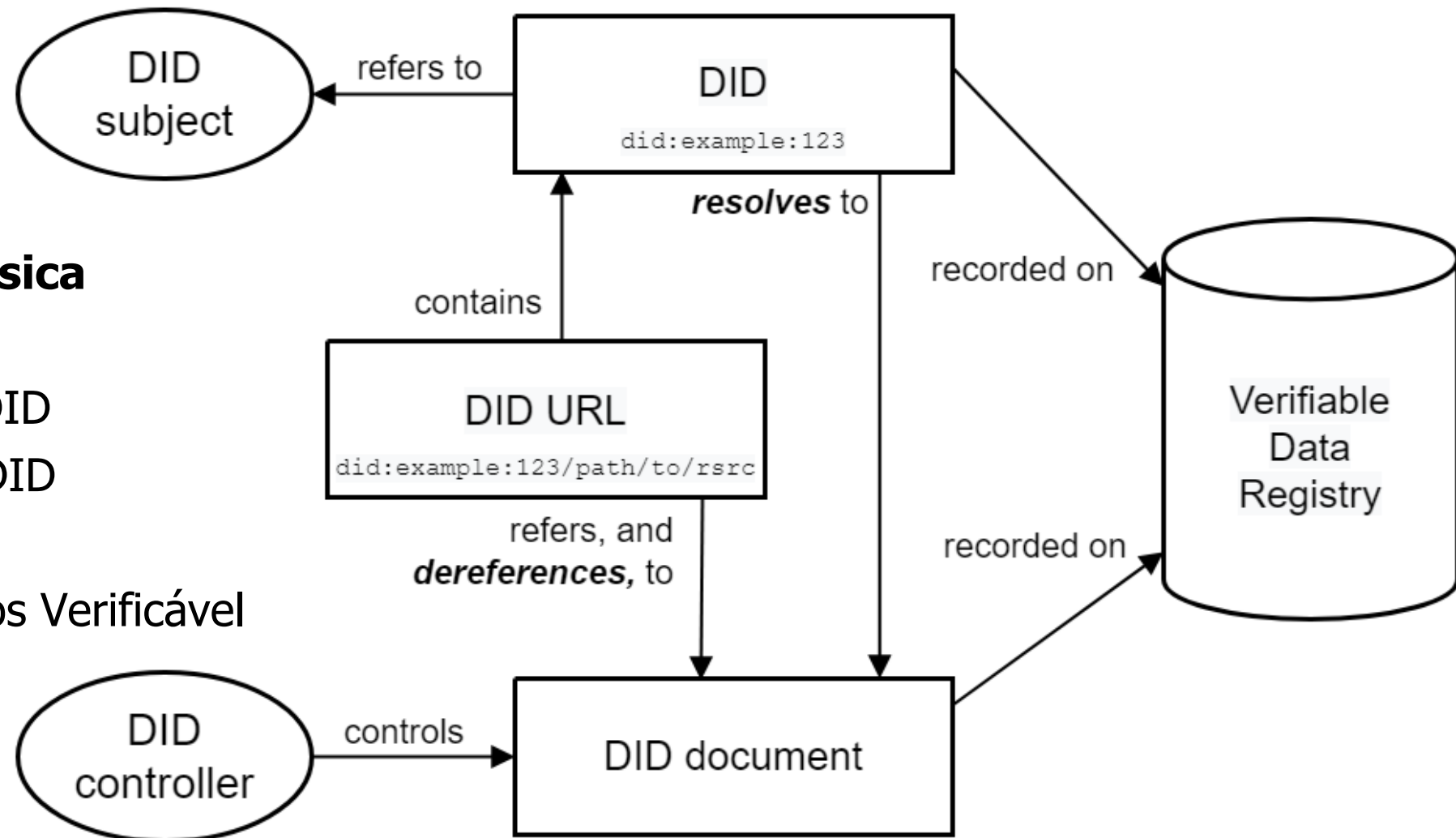




❖ **Arquitetura DID**

➤ **Composição Básica**

- Sujeito DID
- Documento DID
- Controlador DID
- URL DID
- Base de Dados Verificável

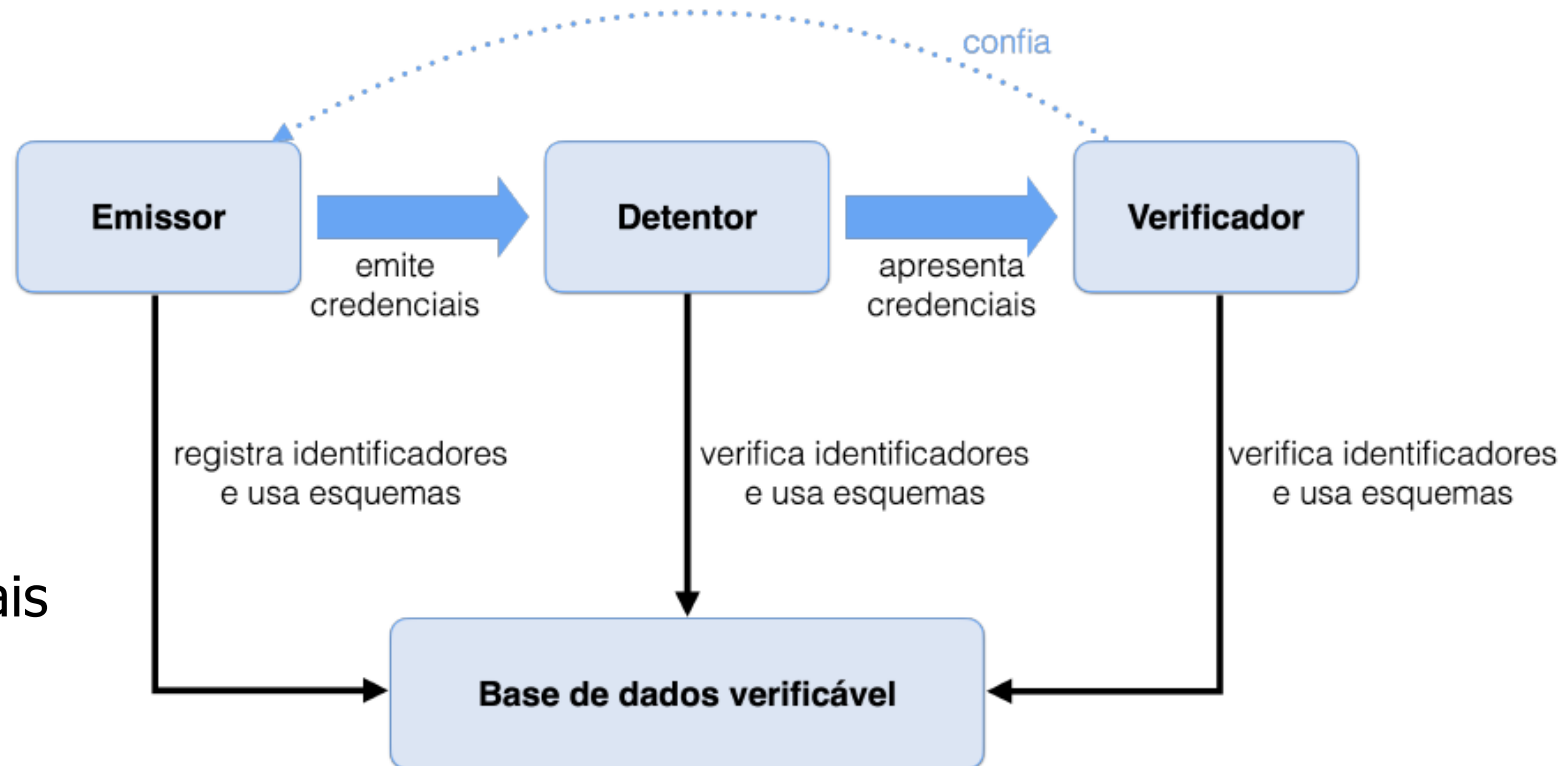


Estado-da-Arte

Verifiable Credentials (VCs)

❖ Credenciais Verificáveis

- Declarações digitais que podem ser verificadas quanto à sua autenticidade e integridade
 - São emitidas por uma autoridade confiável (o emissor) para um titular de credenciais
- Formas de Representação
 - Documentos JSON-LD
 - JSON Web Token (JWT)
 - XML ou RDF
- GT-PIDDF
 - PIDDF-VCS
 - Servidor de Emissão e Verificação de credenciais
 - Base Verificável → ORB



Estado-da-Arte

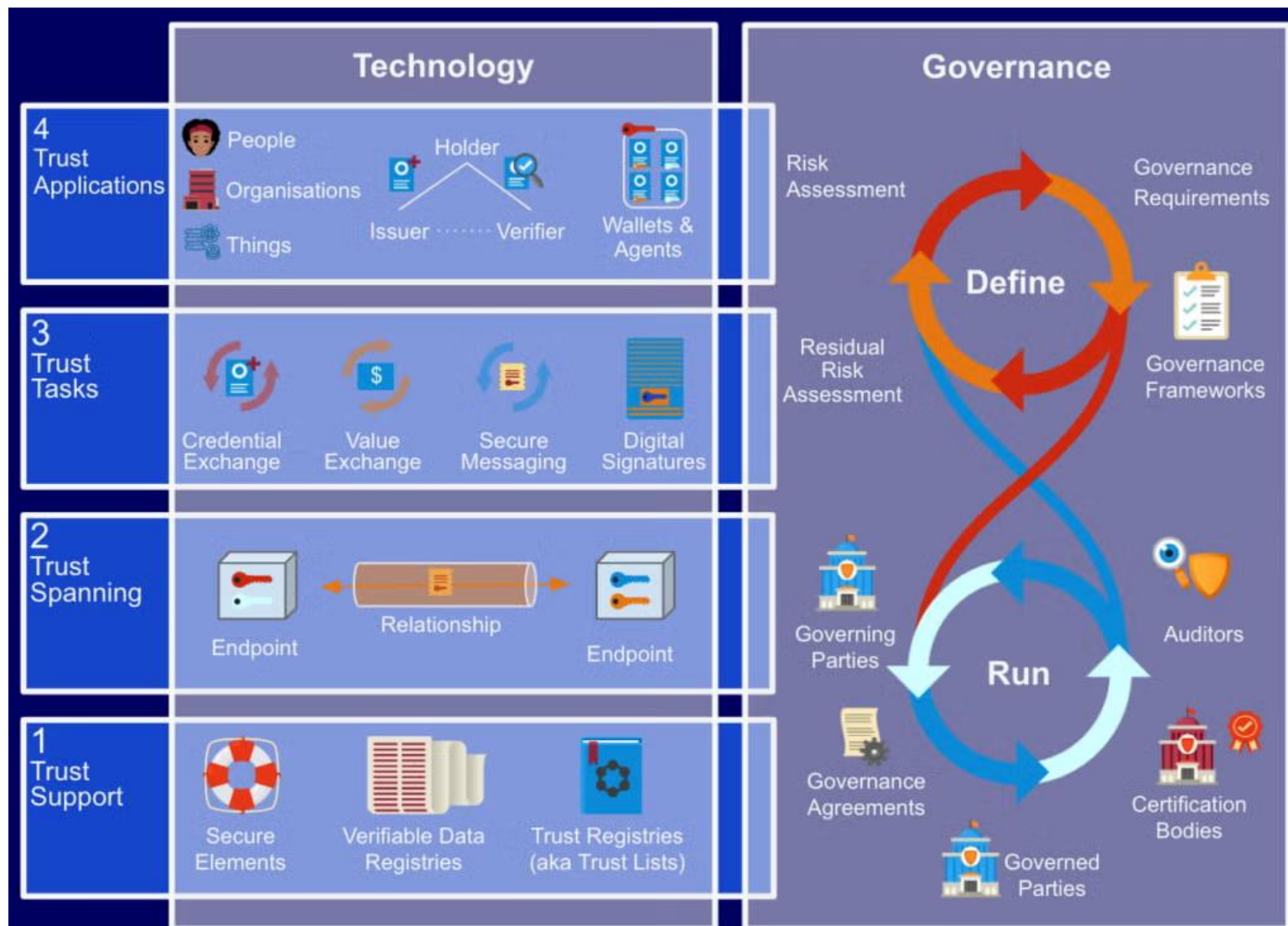
Trust-over-IP (ToIP)

❖ O que é?

- Estrutura em camadas projetada para estabelecer confiança digital
 - Entre indivíduos, organizações e sistemas



TRUST
Over IP
FOUNDATION



❖ Camada de Identificação

- Envolve a criação e verificação das VCs
 - Módulo desenvolvido → PIDDF-VCS

❖ Camada de Autenticação

- Responsável por verificar e validar a identidade do usuário
 - Software Utilizado → *Keycloak*

❖ Camada de Autorização

- Define as regras e permissões para acesso a recursos ou serviços
 - Software Utilizado → *Keycloak Authorization Services + Políticas de Acesso*

❖ Camada de Confiança e Verificação

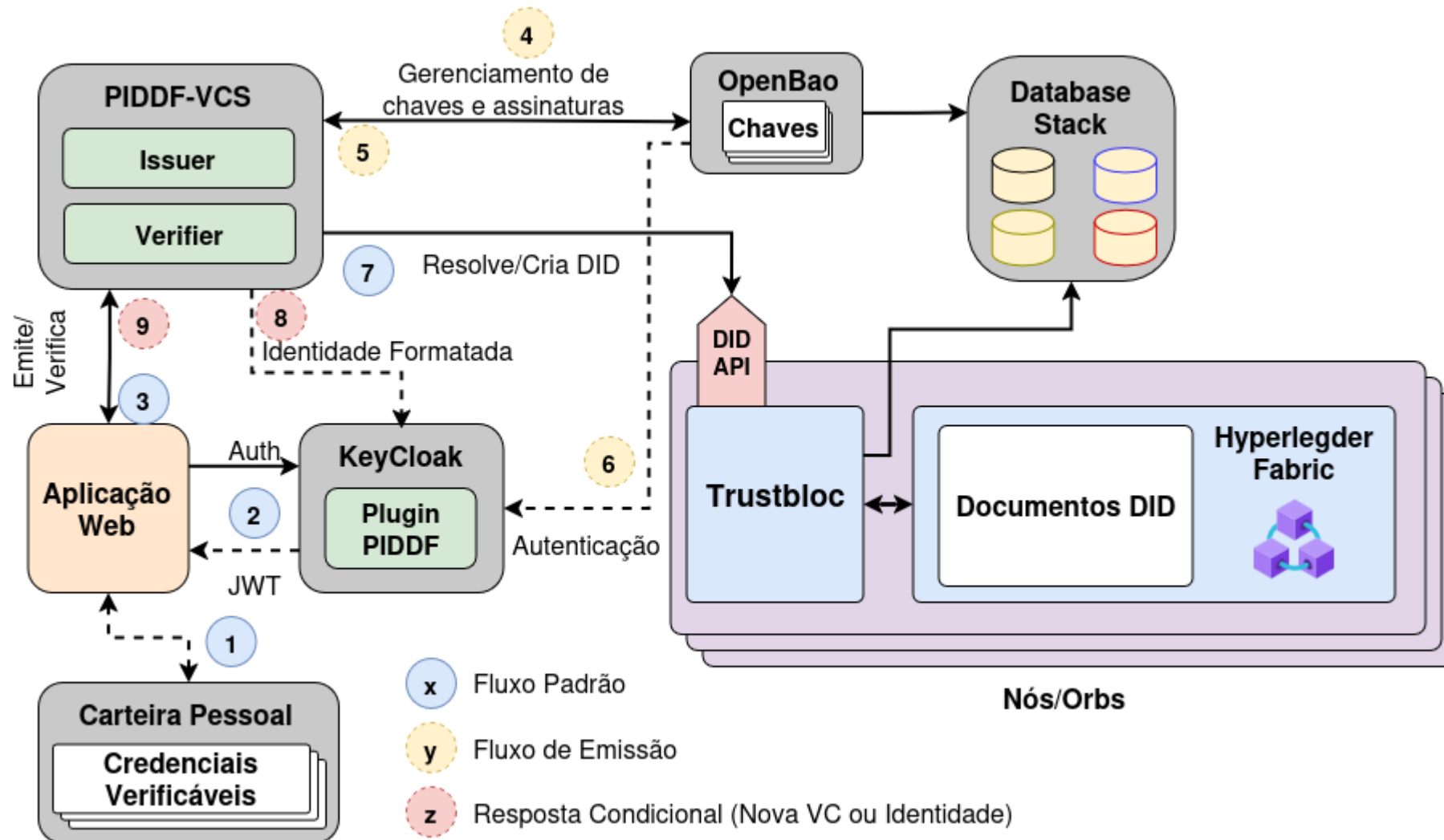
- Atua na garantia da integridade das credenciais e verificações entre as partes envolvidas
 - Software Utilizado → *TrustBloc*

❖ Camada de Interoperabilidade

- Focada na integração entre sistemas e plataformas heterogêneas
 - Software Utilizado → *W3C VC Libraries*

Arquitetura PIDDF

Versão Atual



Composição da Arquitetura

Frameworks Utilizados



OpenBao

❖ **TrustBloc**

- *Framework projetado para facilitar a criação de redes de confiança baseadas em identidades descentralizadas*
- **Principais Vantagens**
 - *Suporte a múltiplos métodos DID*
 - *Documentação atualizada e comunidade ativa*
 - *Suporte completo ao uso de credenciais verificáveis*

❖ **OpenBao**

- *Serviço de gerenciamento de segredos e proteção de dados.*
- **Principais Vantagens**
 - *Compatibilidade com provedores de identidade*
 - *Gerenciamento de credenciais verificáveis*

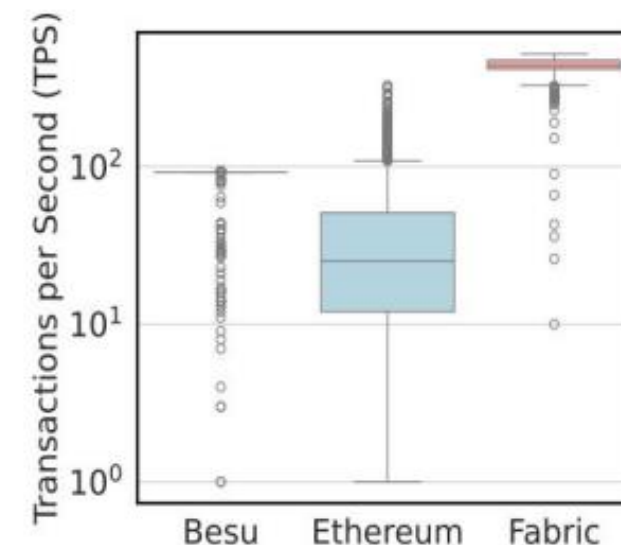
Implantação do Hyperledger Fabric

Por que integrar com Trustbloc?

❖ Outras Blockchains (Bitcoin, Ethereum)

➤ Não Permissionada

- Pares podem participar anonimamente
- Todas as funcionalidades são desempenhadas internamente na infraestrutura das *blockchains*
 - **Consenso e Armazenamento** → realizado por todos os pares
- **Protocolos Pré-Definidos**
 - Consenso
 - Bitcoin → *Proof-of-Work (PoW)*
 - Ethereum 2.0 → *Proof-of-Stake (PoS)*
- **Transações**
 - Geralmente Públicas
 - Baixa vazão de transações



Implantação do Hyperledger Fabric

Por que integrar com Trustbloc?

➤ Características

■ Exclusivamente Permissionada

- **Criação de Canais** → mecanismo para particionar a rede entre organizações
- **Esquema Nativo de Identidade**
 - Cada organização é identificada por certificados x.509
 - Emitidos por CAs e capazes de conter atributos
- **Adoção de Nível de Confiança Prévio**
 - Diminuindo o gargalo do consenso

■ Paradigma Desagregador e Genérico → Foco Enterprise

- **Como?** *Separação do consenso da base de dados*
- **Vantagens** → *Aumentar a eficiência e diminuir o tempo de resposta*
- **Contras** → *Aumentando da complexidade da implementação*
 - Definição de autenticação, validação, base de dados, consenso



Implantação do Hyperledger Fabric

Por que integrar com Trustbloc?



- Por que integrar com Trustbloc?
 - Registro do hash de cada "anchor" do ORB → Auditoria distribuída
 - **Protocolo de Consenso**
 - **Método de Autenticação**
 - **Método de Definição de Canais**

Transição de Paradigma

Recuperação Centralizada → Controle Soberano

❖ Modelo Anterior

- Identidade recuperada de bases de dados centralizadas após a autenticação do usuário
 - *Dependência de repositórios centralizados para o acesso à identidade*

❖ Modelo Atual

- Não haverá recuperação de identidade centralizada
- A identidade reside na posse do cliente
- O próprio usuário "entrega" sua identidade para validação

❖ Consequências no Processo de Autenticação

- Um verificador compara: "Assinatura" do documento vs DID na blockchain
 - *Que verificador? Keycloak*
 - *E o emissor? Cabe integrar um emissor de credenciais verificáveis*
 - **PIDDF - VCS** → módulo implementado
 - *Onde ficam as credenciais? Em posse do usuário*
 - **Wallet do usuário / OpenBao (chaves)**

Plataforma PIDDF

Benefícios



❖ **Segurança**

- Garantia de imutabilidade e verificabilidade dos dados de identidade

❖ **Privacidade**

- Permite que os usuários detenham o controle total de suas informações
 - *Compartilhamento seletivo*

❖ **Interoperabilidade**

- A integração com sistemas legados por meio do protocolo OAuth 2.0

❖ **Escalabilidade**

- Arquitetura cloud-native → baseada em Kubernetes e Docker
 - *Garante alto desempenho*
 - *Capacidade de lidar com grandes volumes de transações*

Impacto no Sistema RNP

Integração com a CAFe

❖ Integração com a CAFe

- Aderência à infraestrutura da Comunidade Acadêmica Federada (CAFe) da RNP

❖ Integração com Keycloak

- Permitirá autenticação federada e consequentemente...
 - Alinhamento aos padrões de segurança e privacidade da LGPD e as políticas de uso da CAFe

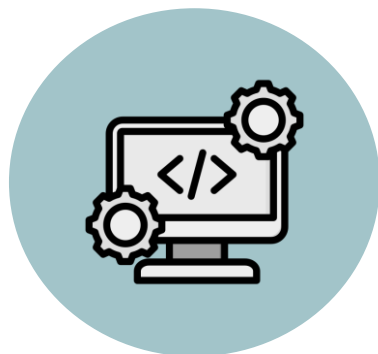
❖ Impacto Potencial

- Alavancar o uso de Identidades Digitais Descentralizadas no contexto da CAFe/RNP



Overview do Desenvolvimento

Tarefas Concluídas, em Andamento e Mapeadas *LabGen*



❖ Etapa de Desenvolvimento

- Implantação do Trustbloc
 - Implantação do HyperLedger Fabric
 - Implantação do VCS
 - Ory OathKeeper e Ory Hydra → *Keycloak*
- Integração Web 2.0 com Web 3.0
- Configuração do *Keycloak*
 - Integração com Identidades Descentralizadas
- Modelagem e Validação da Representação das Identidades
- Desenvolvimento da Lógica de Autenticação e Autorização



Finalizado



Em Andamento



❖ Etapa de Validação e Refinamento

- Desenvolvimento e Teste da Aplicação Cliente
 - Para registro e autenticação
- Avaliação de Métricas de Desempenho e Escalabilidade
 - Dentro do ambiente do testbed

Overview do Desenvolvimento

Etapa de Validação

❖ Metodologia de Testes

- Baseado em Hyperledger Caliper v0.6.0
 - Suporte a redes Hyperledger Fabric (TrustBloc)
- **Cenário** → Simulação de autenticação de usuários
 - Recuperação de DIDs e validação na rede TrustBloc
- **Métricas de Avaliação**
 - Tempo de resposta
 - Taxa de sucesso
 - Consumo de recursos
 - Escalabilidade da solução
- Mensurar impacto da SSI no desempenho de sistemas com padrões tradicionais de autenticação.





- “SANTOS, Y. R. ; BARBOSA, G. N. N. ; REIS, L. H. A. ; OLIVEIRA, NICOLLAS R. DE ; MENDES, A. C. R. ; MEDEIROS, D. S. V. ; MATTOS, D. M. F. . *Segurança de Dados Distribuída em Saúde Digital: Identidade Auto Soberana, Controle de Acesso e Registros de Logs baseados em Blockchain*. In: *Workshop Blockchain: Teoria, Tecnologia e Aplicações*, 2024, Niterói. **Anais do VII Workshop Blockchain: Teoria, Tecnologia e Aplicações (WBlockchain 2024)**. Porto Alegre: Sociedade Brasileira de Computação - SBC, 2024. p. 1-1.



- OLIVEIRA, N. R.; SANTOS, Y. R. ; BARBOSA, G. N. N. ; REIS, L. H. A. ; MENDES, A. C. R. ; OLIVEIRA, M. T. ; MEDEIROS, D. S. V. ; MATTOS, D. M. F. . *Distributed Data Security in Digital Health: Self-Sovereign Identity, Access Control, and Blockchain-based Log Records*. In: **International Conference on Blockchain Computing and Applications (BCCA)**, 2024, Dubai, UAE. (A ser apresentado em Nov/2024), 2024. p. 558.



- DE R. DOS SANTOS, YAGO ; DE OLIVEIRA, NICOLLAS R. ; BARBOSA, GUILHERME N. N. ; REIS, LUCIO HENRIK A. ; MENDES, ANA CAROLINA R. ; DE OLIVEIRA, MARCELA T. ; DE MEDEIROS, DIANNE S. V. ; MATTOS, DIOGO M. F. . *Decentralized security in blockchain-based digital health systems: self-sovereign identity, access control, and auditing with smart contracts*. **Cluster Computing-The Journal of Networks Software Tools and Applications**, v. 28, p. 940, 2025.

Interoperabilidade e Segurança de Identidades na Web 3.0: Gestão de Identidade Digital Descentralizada com Blockchain

Diogo Menezes Ferrazani Mattos

menezes@midiacon.uff.br

LabGen/MídiaCom – PPGEET/TCE/IC

Universidade Federal Fluminense (UFF) - Niterói, Brazil