

*Blockchain
em evolução.*



Meta 5

**META 5 - Pesquisa e
Desenvolvimento em
Identidade Digital
Descentralizada**

Campinas 25-02-2026
Antonio Mateus de Sousa

Meta 5 – Agenda

- Objetivos da meta
- Equipe atualizada
- Entregas realizadas
- Lições aprendidas e *insights*



Meta 5 – Descrição de Meta

- Foram Desenvolvidos arquitetura e componentes do metassistema de Identidade Digital Descentralizada (IDD).
- Realização de prospecção tecnológica, testes de desempenho e escalabilidade.
- Participação de grupos de padronização (ABNT, ITU, DIF, ToIP).
- Monitoramento de evolução de aspectos regulatórios no Brasil e no exterior.

Meta 5 – Equipe Atualizada

Equipe CPQD

- Antonio Mateus de Sousa
- Bruno Evaristo
- Rayan Jucá
- Fernanda Jordão
- Ismael Ávila
- Lesandra Kobus
- Silvia Marion

Apoio Técnico da RNP

- Michelle Wangham



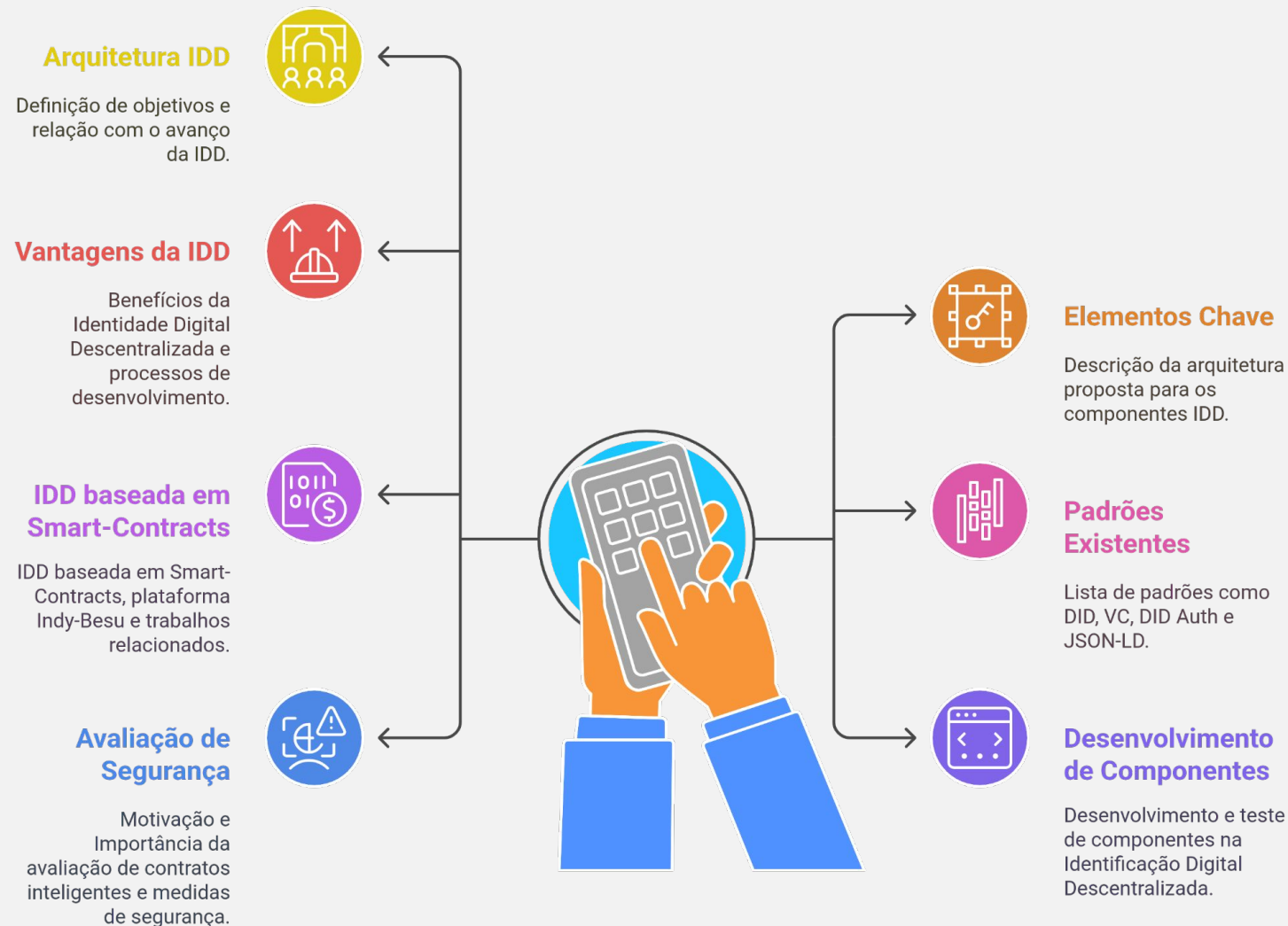
Meta 5 – Entregas Realizadas

- Meta 5.1: Prospeção tecnológica, padronização e aspectos legais em identidade digital descentralizada



Meta 5 – Entregas Realizadas

- Meta 5.2: Definição de arquitetura, desenvolvimento e testes de componentes IDD



Meta 5 – Entregas Realizadas

- Meta 5.3:

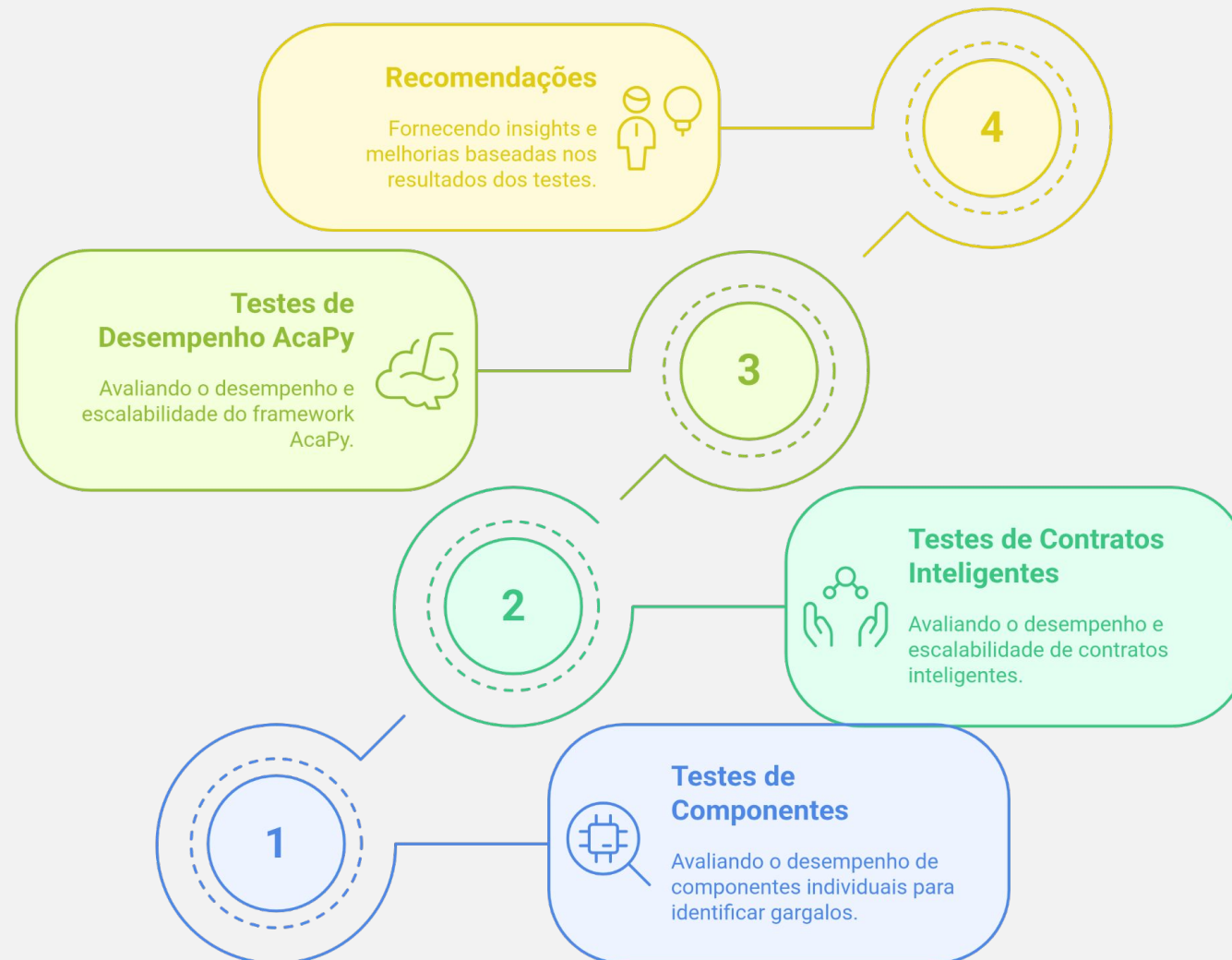
Desenvolvimento

de aplicações de IDD



Meta 5 – Entregas Realizadas

- Meta 5.4: Testes de desempenho e escalabilidade dos componentes e aplicação IDD



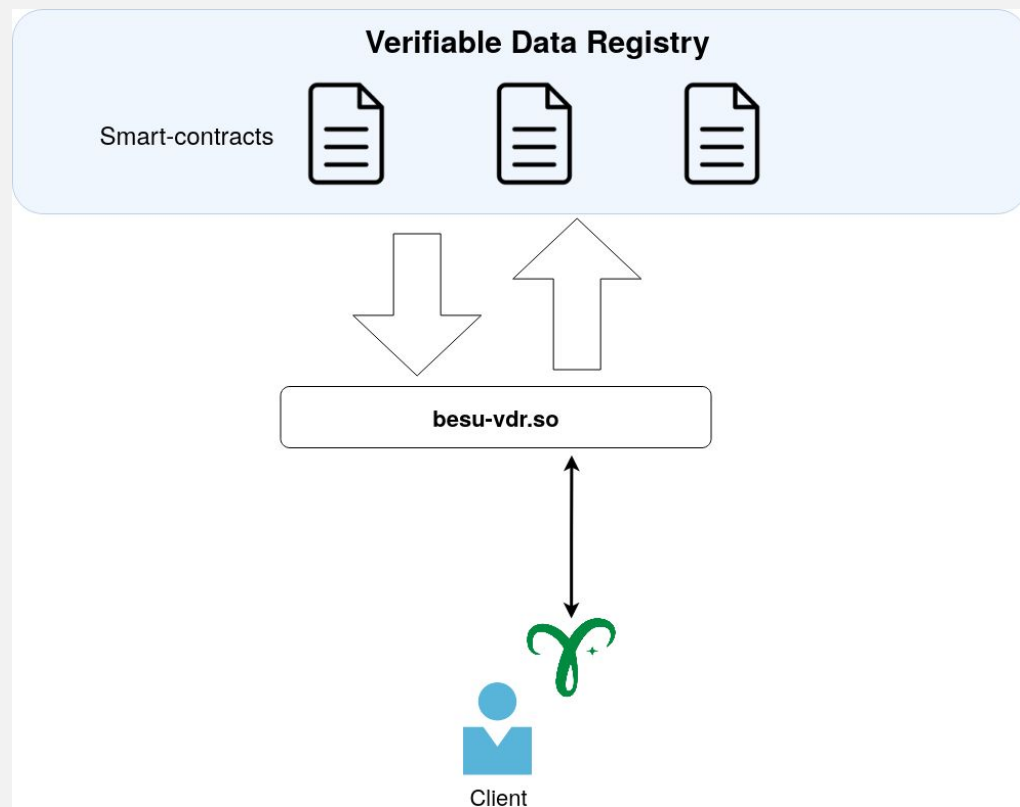
Meta 5 – Entregas Realizadas

- Levantamento de protocolos e especificações de IDD (ex.: DIDs, VCs, DIDComm).
- Comparativo entre Hyperledger Besu x Indy, com escolha do Besu.
- Análise de modelos de governança (eIDAS 2.0, EBSI).
- Acompanhamento e análise de padrões da OpenID Foundation, Linux Foundation e OpenWallet Foundation.
 - EU Digital Identity Wallet e Self-Issued OpenID Provider v2 (OIDF)
 - Hyperledger Aries, Indy Besu, CREDEBL e Hyperledger Identus (LFDT)
 - Credo e Bifold (OWF)
- Descrição de *Mobile Documents* e *Mobile Drive Licenses*.
- Seleção da tecnologia AnonCreds para credenciais com privacidade aprimorada.

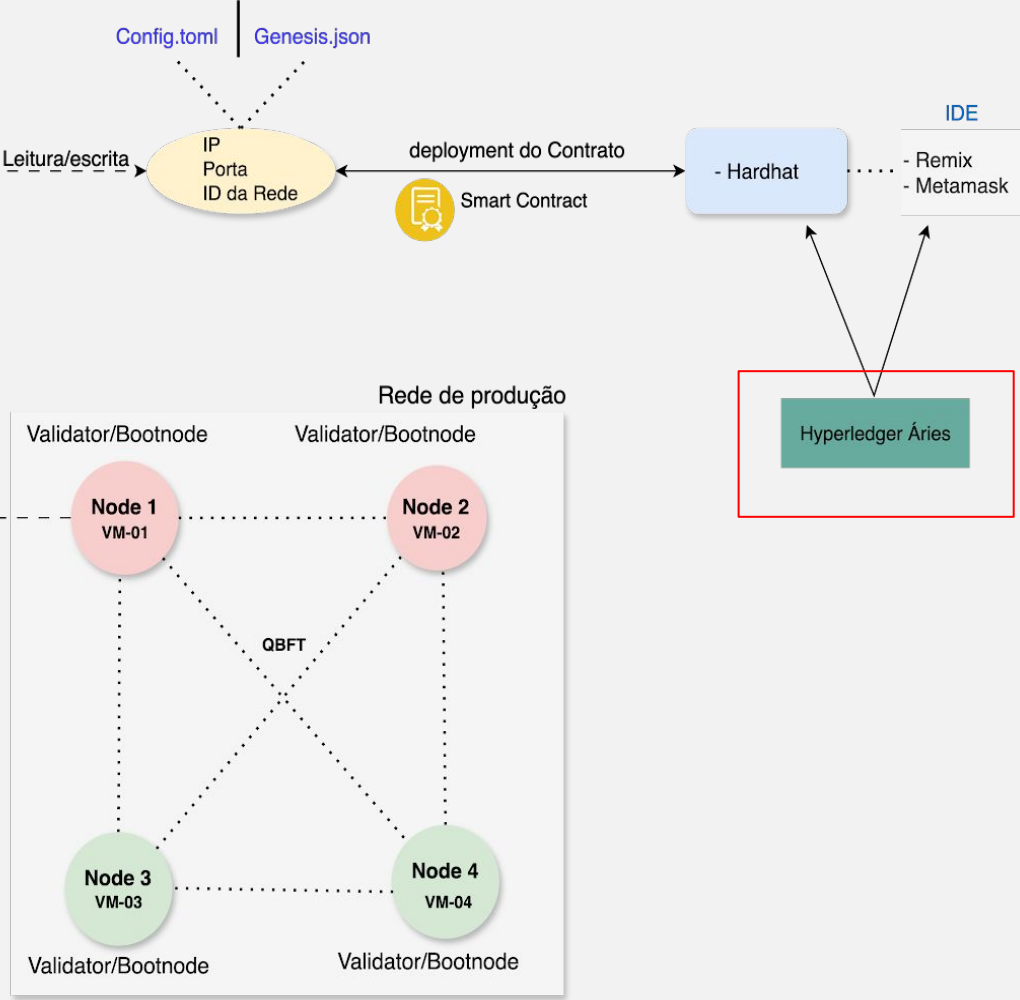
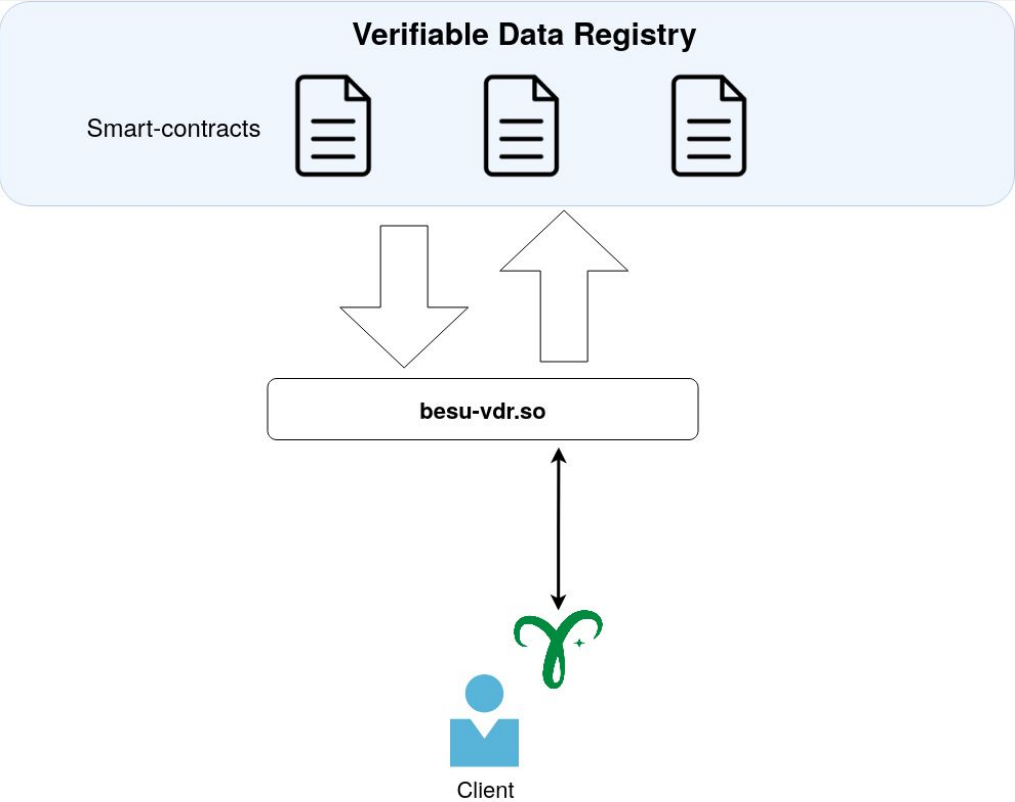
Meta 5 – Resultados

- Implementação completa do plugin Indy-Besu no Aca-py, que aumenta significativamente a adotabilidade e interoperabilidade do protocolo Aries.
- Implementação do plugin para HSMs também no Aca-py, preservando a segurança e integridade de chaves durante todo o ciclo de vida.

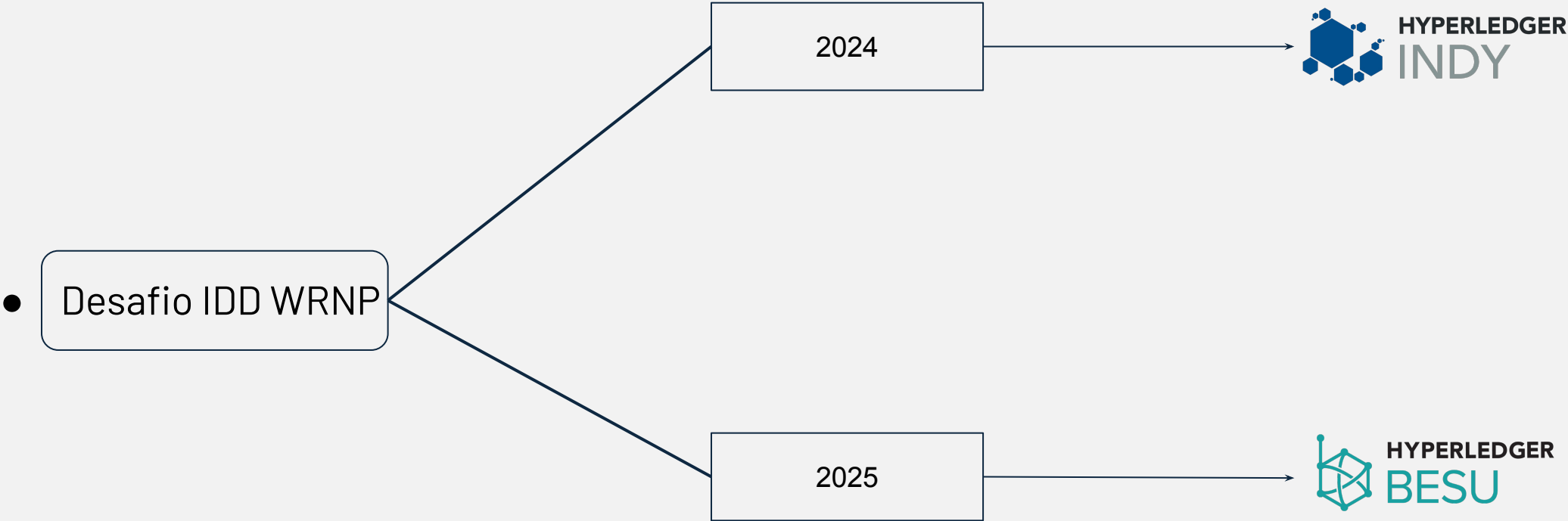
Meta 5 – Resultados



Meta 5 – Resultados

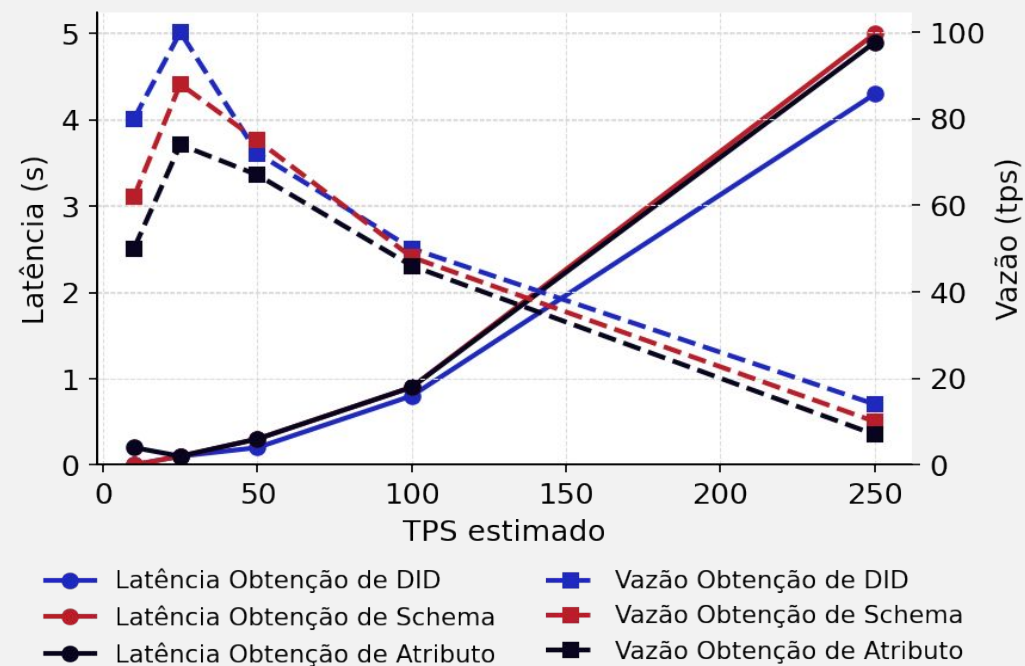
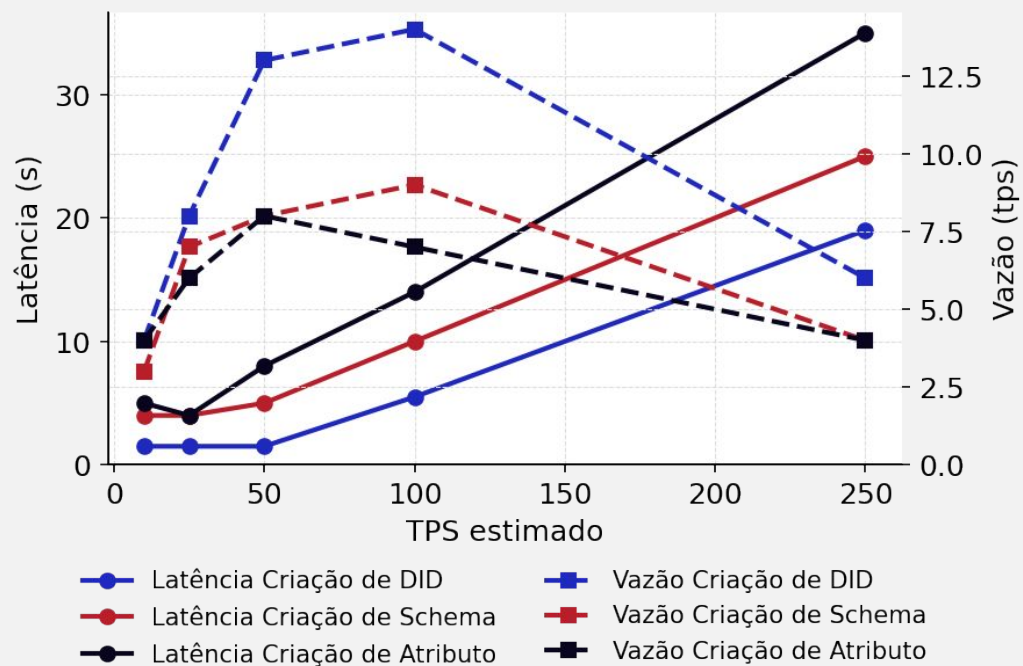


Meta 5 – Resultados

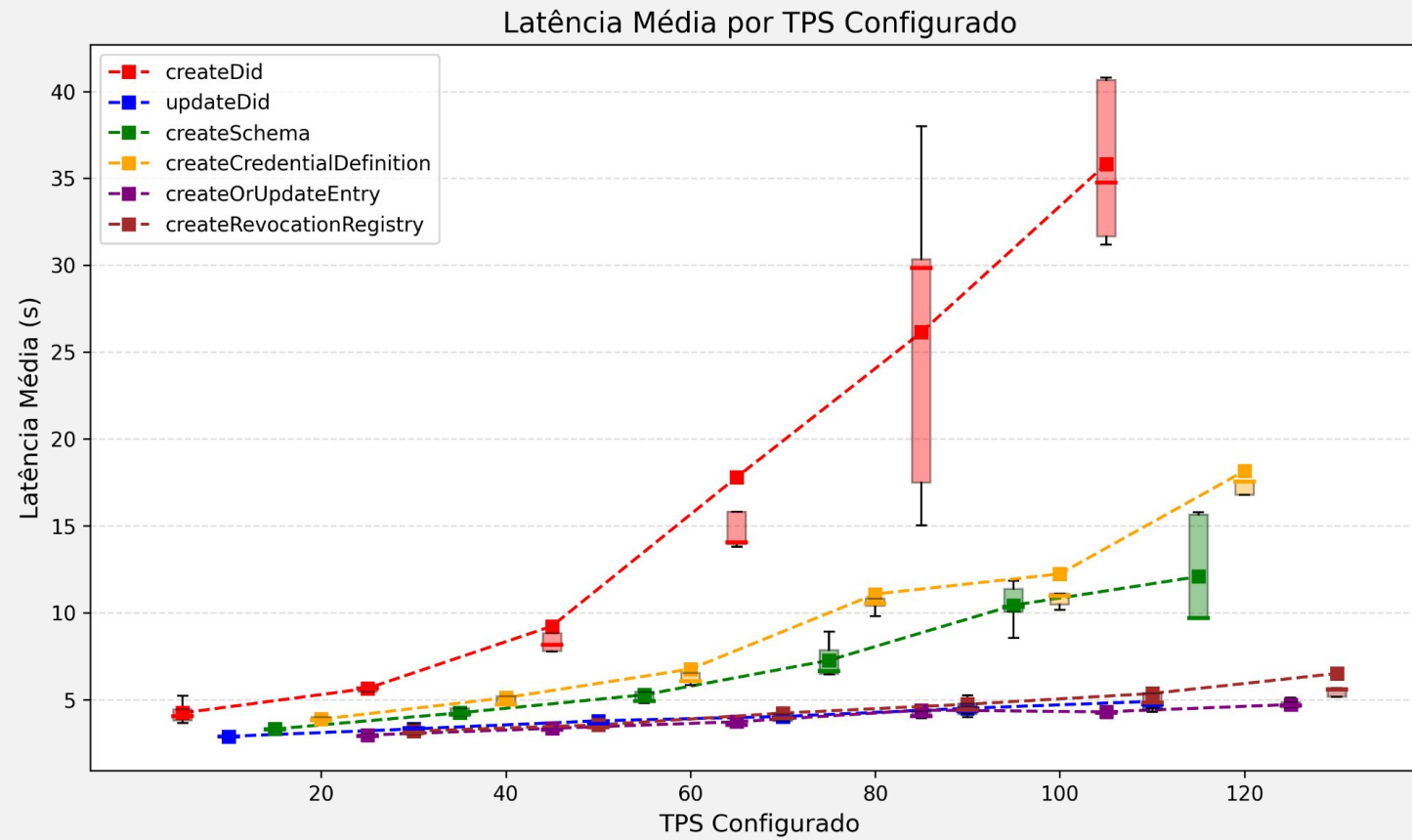


Meta 5 – Resultados

- Artigos Submetidos
 1. Estrutura de governança orientada por regras programáveis com suporte de identidade digital descentralizada (SBSeg - Wgid)
 2. Integração de Verifiable Credentials em Sistemas Web: Estudo de Caso com o SOU iD (SBSeg - Wgid)
- 3. Governança Digital que se Explica: Interação Segura com Regras Programáveis (IHC)
 4. Interação e Privacidade por Design: Navegando com Verifiable Credentials no SOU iD (IHC)
- Projetos realizados
 - WRNP Game: evolução do "Desafio IDD" realizado no WRNP 2024 migrando para *Hyperledger Besu*
 - Avaliação de contratos inteligente utilizando o Hyperledger Caliper
 - Funções de criação de dids, schemas e credenciais
 - Testes de desempenho do agente ACA-Py



Comparação de latência e vazão das operações de criação e obtenção na rede Indy. Adaptado de Bastos et al. (2024) e Veloso et al. (2024)



Comparação de latência entre funções na rede Besu

Meta 5 – Lições aprendidas

- Organizações e Frameworks de Padronização:
 - OpenID Foundation: Desenvolvimento de padrões como OpenID4VC (para VCs), SIOPv2 (provedor autoemitido) e OpenIDIDComm.
 - Linux Foundation Decentralized Trust: Projetos como Hyperledger Aries, AnonCreds (privacidade com ZKP), CREDEBL e Hyperledger Identus.
 - Open Wallet Foundation: Promoção de carteiras digitais interoperáveis, incluindo os projetos Credo e Bifold.



Meta 5 – Lições aprendidas

- Tecnologias de Registros Distribuídos (DLT): Analisam plataformas blockchain para soluções de IDD, com foco comparativo entre o Hyperledger Besu (compatível com EVM e versátil) e o Hyperledger Indy (específico para identidade digital).
- Interoperabilidade e Padrões: Tratam da capacidade de DIDs serem reconhecidos em diferentes redes, garantindo conformidade com padrões globais do W3C e integração de chaves criptográficas.



Meta 5 – *Insights*

- Padrões a serem considerados W3C VCs (em adoção na EU)
- Eidas2.0
- Blockchain pós-quântica (*Q day*)
- OpenID4VCI e OpenID4VCP
- Identidade para agentes IA
- Reputação baseada em credenciais



Meta 5 – O que fazer com o legado?

- Expansão dos laboratórios (mais experimentos e PoCs no ambiente)
- Elaboração de manuais de uso do ambiente IDD (Padrões e tecnologias)
- Realizar treinamentos práticos voltados para IDD em parceria com universidades
- Escrita de artigos científicos



Obrigado.

