

Criando Soluções com Hyperledger Indy

Fernando Marino, Blockchain Technical Leader, CPQD



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS





Fernando Marino

CPQD - Blockchain Technical Leader

Pesquisador no CPqD desde 2014, participando de diversos projetos de pesquisa e desenvolvimento de produtos na área de Ciências da Computação, como: mobilidade; visão computacional; IHC (Interação Humano Computador); sistemas acessíveis e mais recentemente Blockchain. Bacharel em Sistemas de Informação pela universidade DeVry Metrocamp em 2014. Atualmente cursa matérias como aluno especial no programa de pós-graduação da Unicamp (Universidade Estadual de Campinas).



HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Agenda



Hyperledger

Hyperledger Greenhouse
Projects

Identidade

Conceitos de Identidade

O Framework

Hyperledger Indy Framework



Agenda



Hyperledger

Hyperledger Greenhouse
Projects



Identidade

Conceitos de Identidade



O Framework

Hyperledger Indy Framework

The Hyperledger Greenhouse



HYPERLEDGER

Community Stewardship and Technical, Legal, Marketing, Organizational Infrastructure

Frameworks



**HYPERLEDGER
BURROW**

Permissionable
smart contract
machine (EVM)



**HYPERLEDGER
FABRIC**

Permissioned
with channel support



**HYPERLEDGER
GRID**

WebAssembly-based
project for building
supply chain solutions



**HYPERLEDGER
INDY**

Decentralized
identity



**HYPERLEDGER
IROHA**

Mobile application
focus



**HYPERLEDGER
SAWTOOTH**

Permissioned &
permissionless support;
EVM transaction family

Tools



**HYPERLEDGER
CALIPER**

Blockchain framework
benchmark platform



**HYPERLEDGER
CELLO**

As-a-service
deployment



**HYPERLEDGER
COMPOSER**

Model and build
blockchain networks



**HYPERLEDGER
EXPLORER**

View and explore data
on the blockchain



**HYPERLEDGER
QUILT**

Ledger
interoperability



**HYPERLEDGER
URSA**

Shared Cryptographic
Library



HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Agenda



Hyperledger

Hyperledger Greenhouse
Projects



Identidade

Conceitos de Identidade



O Framework

Hyperledger Indy Framework

Identidade Digital Centralizada



**Pessoa
(usuário)**



Conta específica para
essa instituição



**Instituição
(serviço)**



HYPERLEDGER

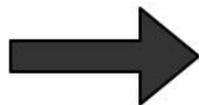
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

CC BY-SA 4.0 - From The Story of SSI Open Standards by Drummond Reed, Chief Trust Officer Evernym and Sovrin Foundation Trustee

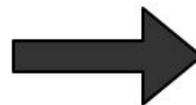
Identidade Federada (IdP - Identity Provider)



**Pessoa
(usuário)**



**Provedor de Identidade
(IdP)**



**Instituição
(serviço)**

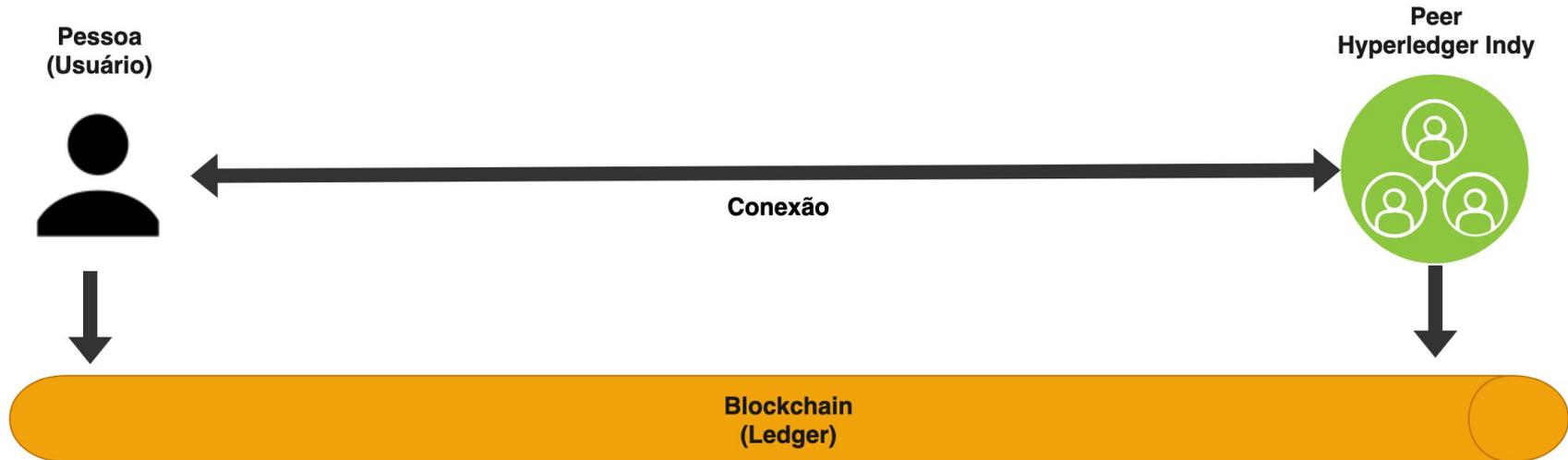


HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

CC BY-SA 4.0 - From The Story of SSI Open Standards by Drummond Reed, Chief Trust Officer Evernym and Sovrin Foundation Trustee

Identidade Descentralizada (Autossoberana)



HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

CC BY-SA 4.0 - From The Story of SSI Open Standards by Drummond Reed, Chief Trust Officer Evernym and Sovrin Foundation Trustee

Agenda



Hyperledger

Hyperledger Greenhouse
Projects



Identidade

Conceitos de Identidade

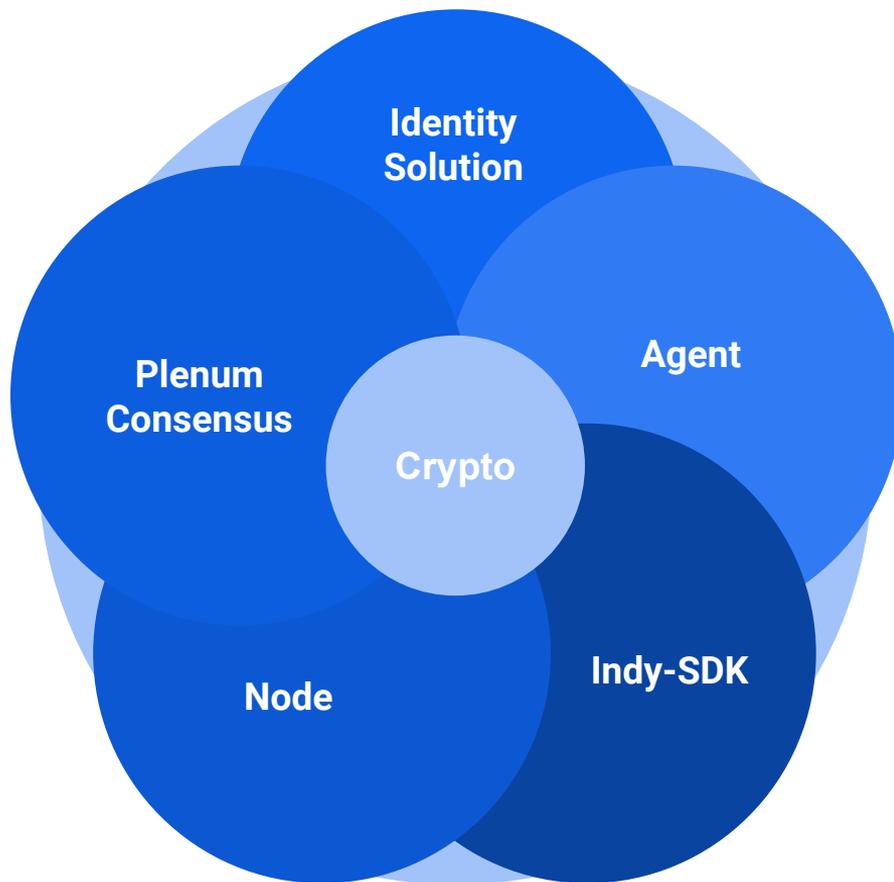


O Framework

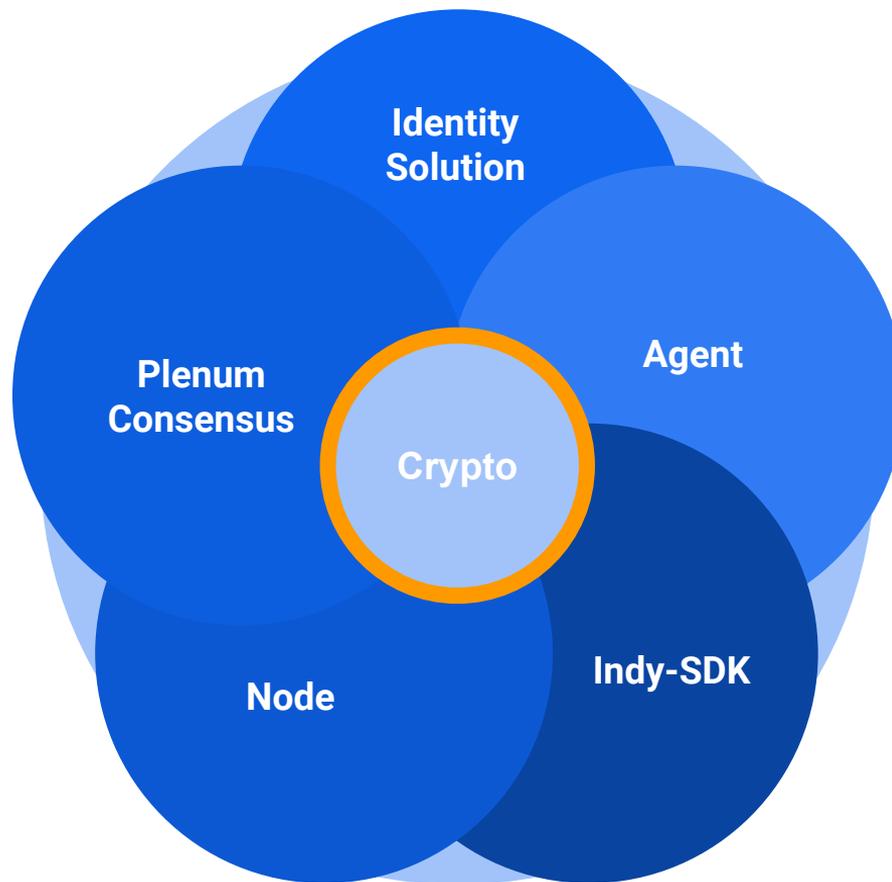
Hyperledger Indy Framework



Conceitos



Crypto

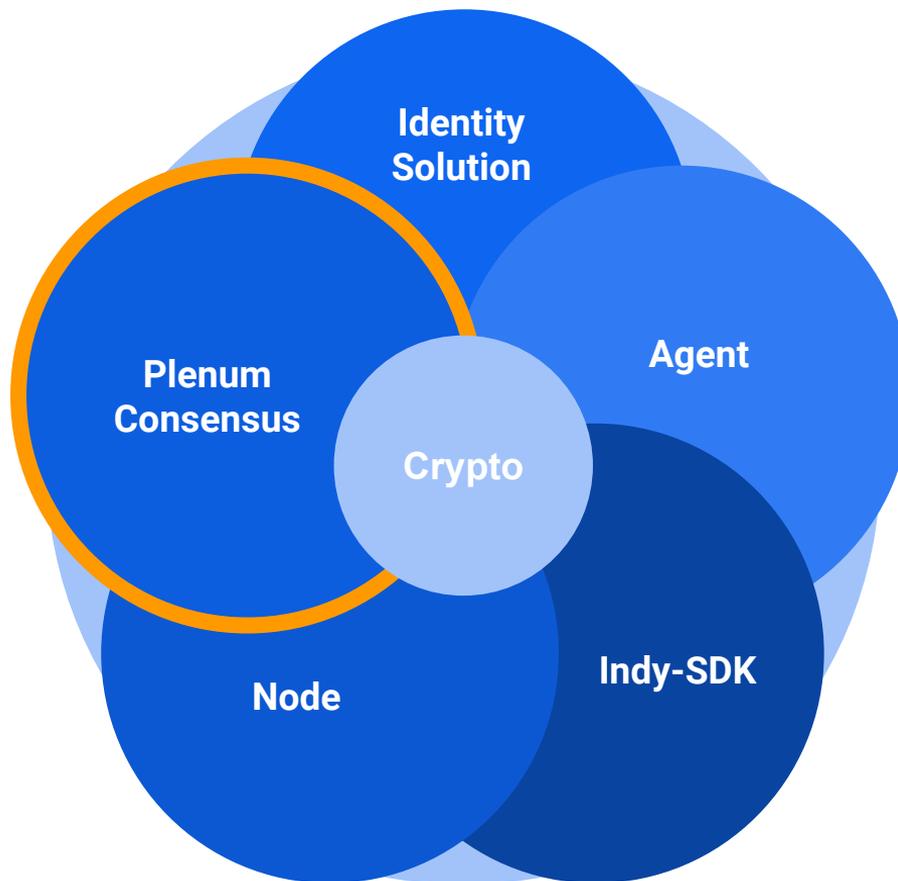


Crypto

- Atualmente usado pelo Hyperledger Indy para ZKPs e assinar "state proofs"
- Inclui esquemas de assinaturas, como Camenisch-Lysyanskaya (CL) Signatures e Boneh–Lynn–Shacham (BLS) signatures
- Desenvolvimento para consolidar crypto com a Hyperledger Ursa



Consenso

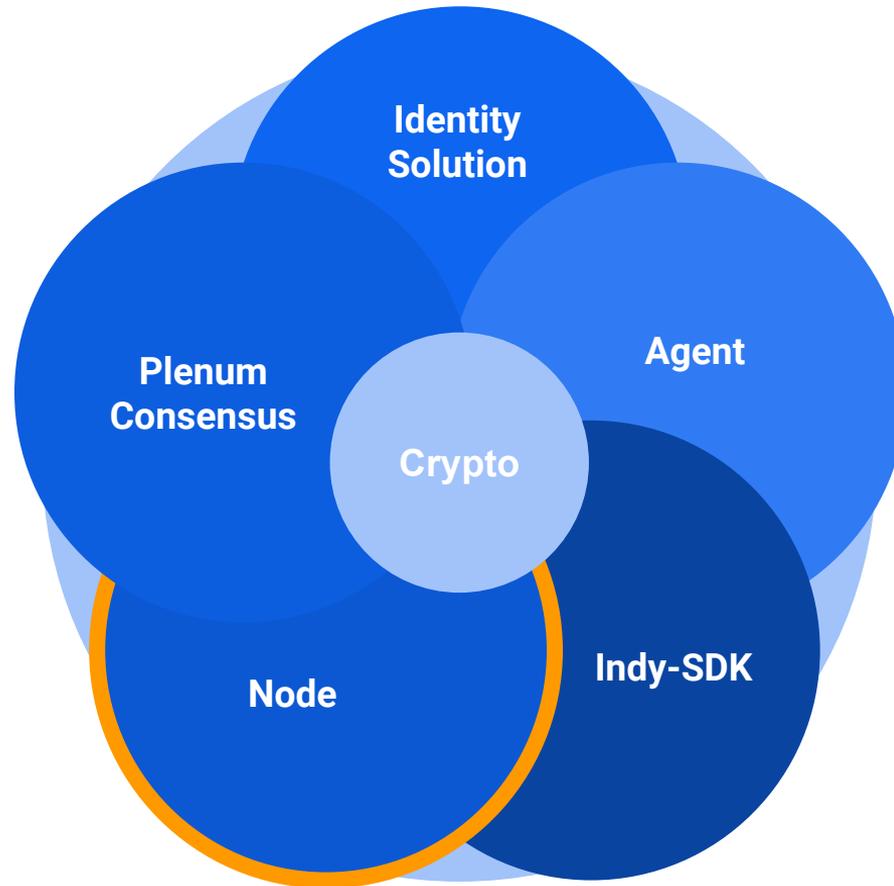


Plenum Consensus

- Baseado no protocolo RBFT ("Redundant Byzantine Fault Tolerance")
- Consenso baseado em líder, com verificações redundantes
- Pode sustentar F falhas, onde $3F + 1$ nós são presentes
 - E.g. pode sustentar 4 falhas quando há 13 nós presentes: $13 \geq 3(4) + 1$



Node

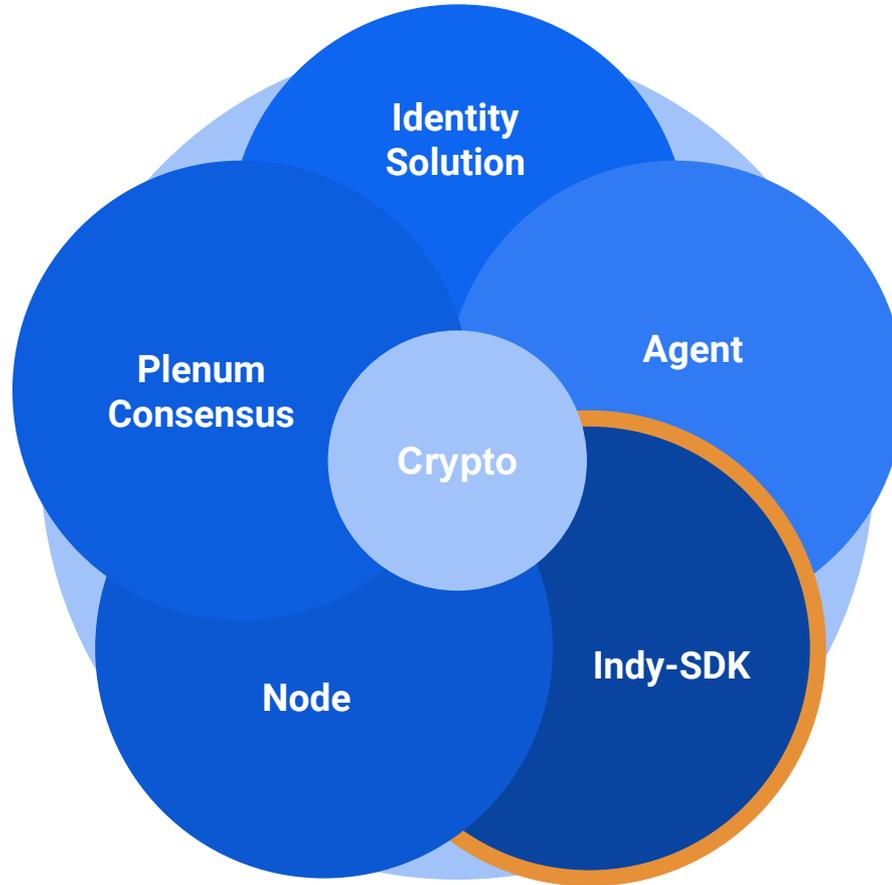


Node

- Transações usadas para identidade
 - Transação de identificadores (NYM)
 - Transações de definição de credencial
 - Transações de Schema
 - Transações de registry
- Faz a validação de que você está fazendo apenas o que deveria
- Executa o algoritmo Plenum consensus



Indy-SDK

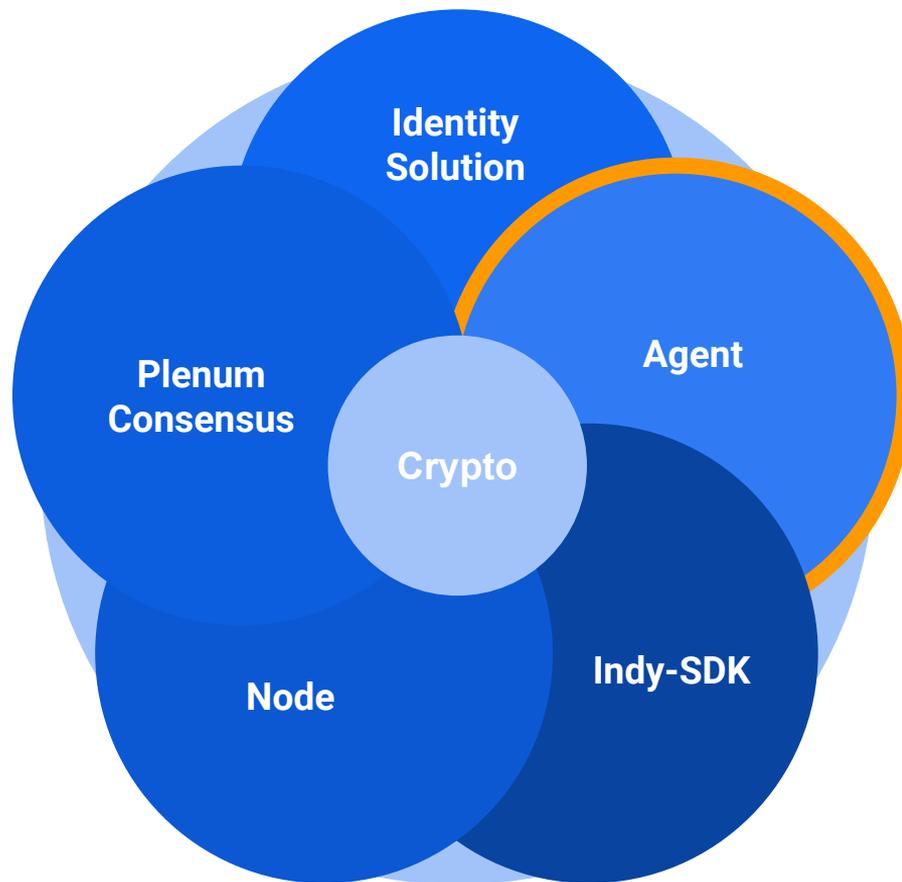


Indy-SDK

- Facilita a interação com a ledger
- Possui uma solução de armazenamento de chaves (Wallet)
- Disponibiliza protocolo "Agent to Agent" para a abstração das interações peer to peer
- Permite recursos avançados de identidade para desenvolvedores criarem agentes e extensões de agente
- Desenvolvido em Rust, com APIs "c-callable"



Agent

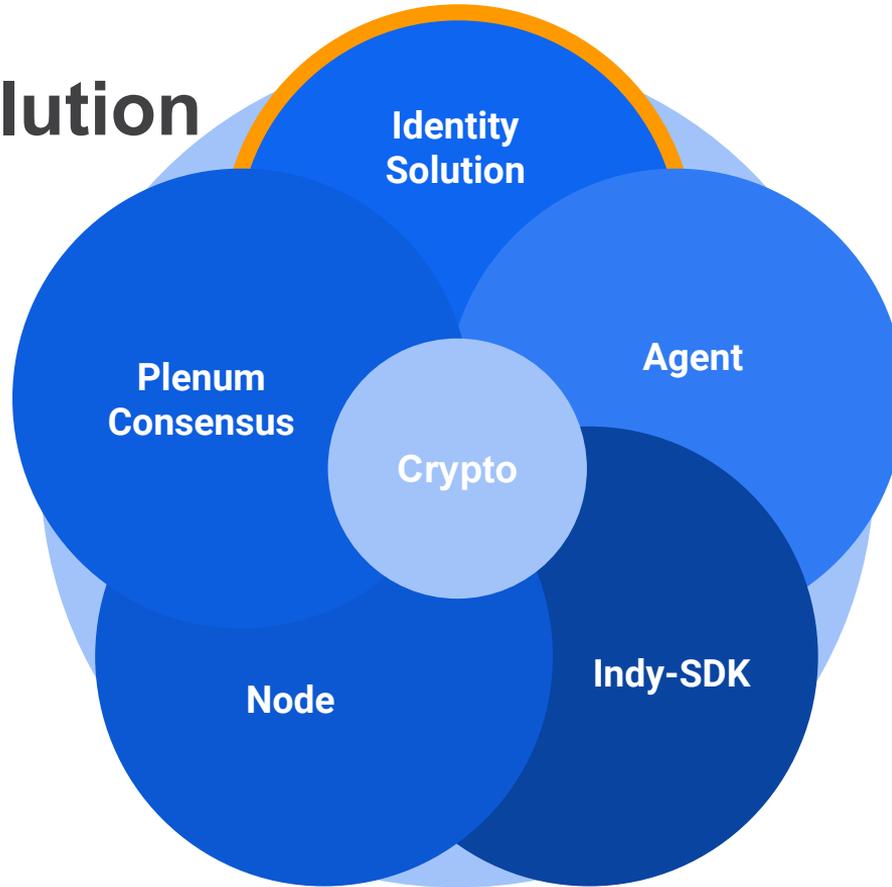


Agent

- Construído usando por meio do Indy-SDK
- Extensível a diferentes "famílias de mensagens", permitindo que os aplicativos sejam construídos em um paradigma orientado à identidade
- Coleção de agentes de referência para a troca de informações de identidade
- Suíte de testes para estabelecer compatibilidade com outros agentes que executam o protocolo A2A



Identity solution

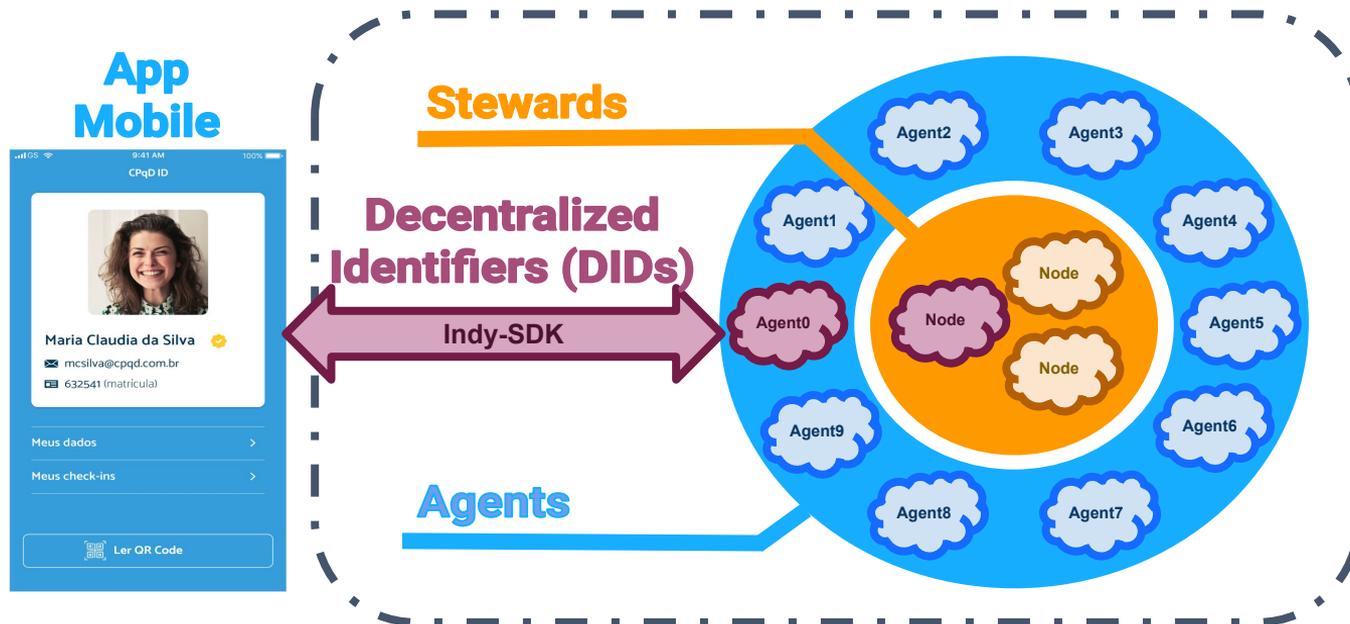


Identity solution

- Maneira fácil de criar o Indy em aplicativos existentes, se um agente já existir no dispositivo
- Extensível através da criação de famílias de mensagens
- Permite que aplicativos e serviços legados se integrem rapidamente ao protocolo A2A
- É nessa camada que desenvolvemos nossas aplicações



Identity solution



Identity solution

Wiki

<https://wiki.hyperledger.org/projects/indy>

GitHub Indy SDK

<https://github.com/hyperledger/indy-sdk>



Obrigado!

Fernando Marino
CPQD - Blockchain Technical Leader
fmarino@cpqd.com.br