TENEMOS
MUCHO
QUE HACER
JUNTOS

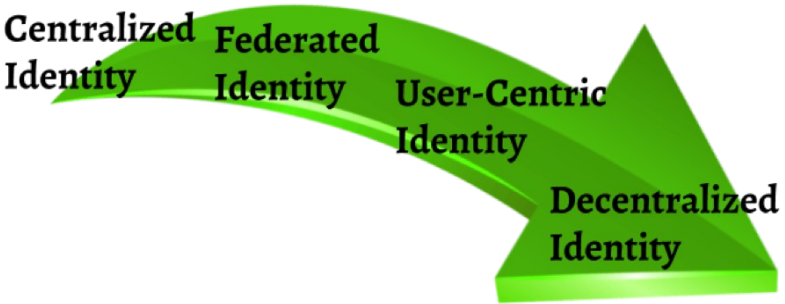
HYPERLEDGER
INDY

tecnalia Inspiring Business


ON THE INTERNET
NOBODY KNOWS YOU'RE A DOG

Un breve repaso histórico

- Identidad Centralizada
- Identidad Federada
  - Misma identidad en múltiples sitios con el consentimiento del usuario
- Identidad Centrada en el Usuario
  - Usuario tiene control sobre su identidad digital repartida entre diversas autoridades
- **Identidad Descentralizada**
  - Decentralized Identity
  - Self-Sovereign Identity (SSI)



Nuevos desafíos de la identidad

- Mantenimiento de IDs y passwords
- Evitar correlación de datos no deseada
  - GDPR
- Data breaches
  - Hackers
- Descentralización
- Evitar la “huella digital”

Identidad en el mundo real

Identity Owner
(Holder)

1. Issuer provee credenciales

2. Owner prueba credenciales

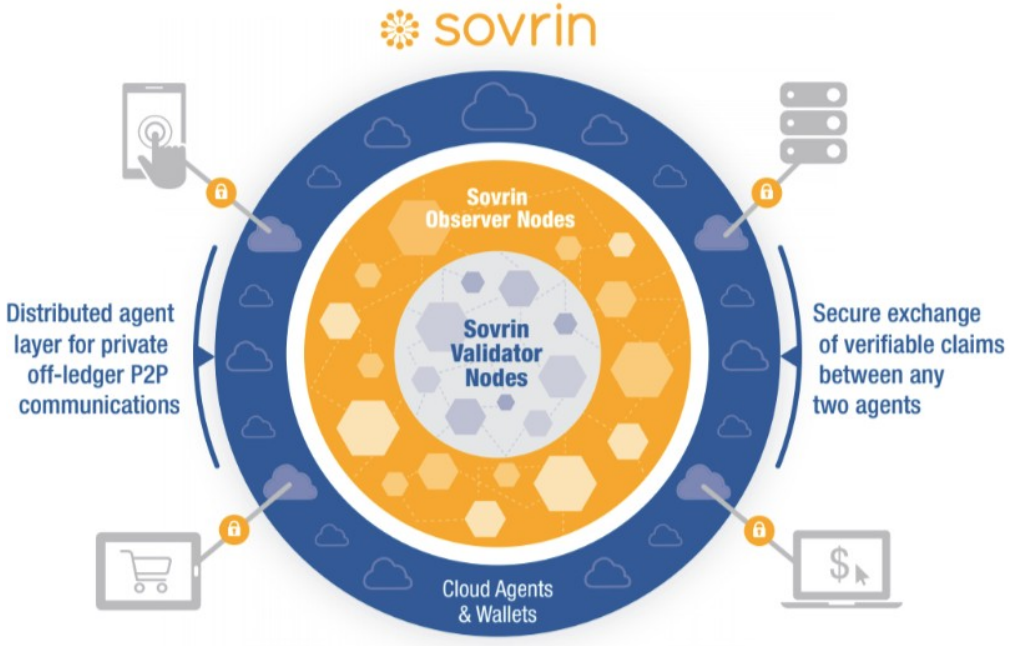
3. Verifier verifica credenciales

Gobierno (Issuer)

Banco (Verifier)

Hyperledger Indy I

- Self-Sovereign Identity
- Blockchain pública permisionada
  - Pública: Sovrin network
  - Permisionada: Nodos validadores permisionados (stewards)



Hyperledger Indy II

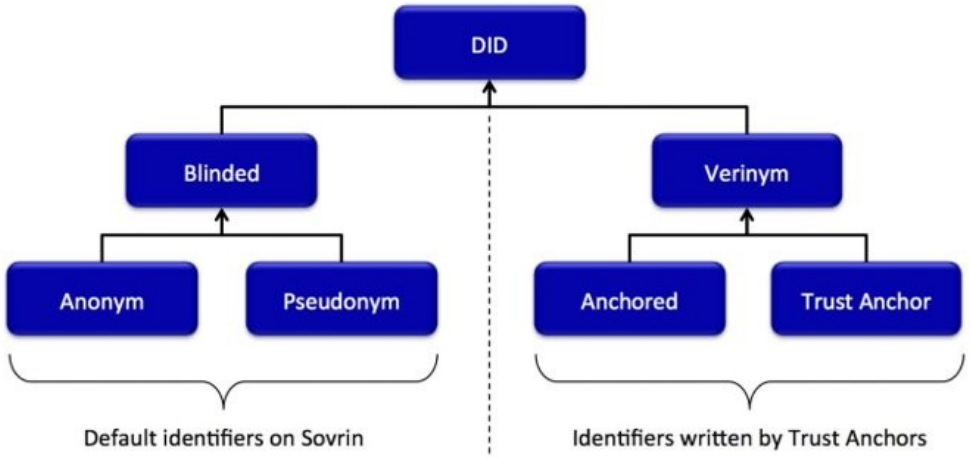
- Nodos
  - Stewards: Todos los nodos con permiso para participar en el proceso de validación
    - https://sovrin.org/stewards/
  - Validator nodes: Subset de stewards participando en el algoritmo de consenso Plenum (RBFT)
  - Observer nodes: Subset de stewards que no participan en el consenso
    - Sirven lecturas
- Trustee: Miembro del Sovrin Foundation Board of Trustees
- Agencies: Proveedores de servicios que gestionan Cloud Agents y pueden provisionar Edge Agents
- Agents: Clientes Indy

Ledger

- 3 ledgers:
  - **Domain ledger**: Identidades (DIDs...)
  - Pool ledger: Validators y observers
  - Config ledger: Configuración
- (Domain) ledger: Sólo información pública
  - DDOs (DID Descriptor Objects)
    - DID
    - Verkey
    - ...
  - Credential schemas
  - Credential definitions (Credential schema + issuer info)
  - Service endpoints
  - Revocation registries

DIDs

- Decentralized IDs
- did:sov:21tDAKCERh95uGgKbJNHYp
- Blinded DIDs:
  - Usados en la interacción entre agentes
  - Evitan correlación
  - Anonym: Un único uso
  - Pseudonym: Para una única relación (Pairwise-Unique Identifier)
- Verinyms:
  - Usados en la interacción con el ledger
  - Asociado con una identidad legal

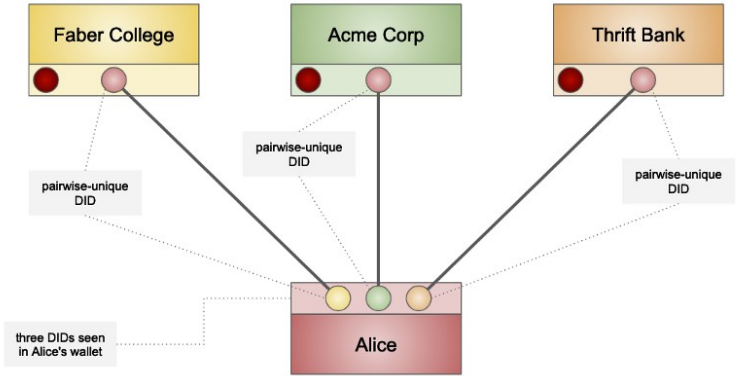


Verifiable Credentials (VCs)

- Credenciales digitales procesadas criptográficamente que prueban afirmaciones (claims) sobre la identidad
- "Equivalentes" a credenciales en papel
- Aseguran:
  - Quién (o quiénes) certifica los claims (el Issuer)
  - Que los claims fueron emitidos a la identidad que los presenta
  - Que los claims no han sido alterados
  - Que la credencial de los claims no ha sido revocada
- Características avanzadas:
  - Divulgación selectiva (Selective Disclosure)
  - Zero Knowledge Proof (ZKP): Ej.: edad > 18 años

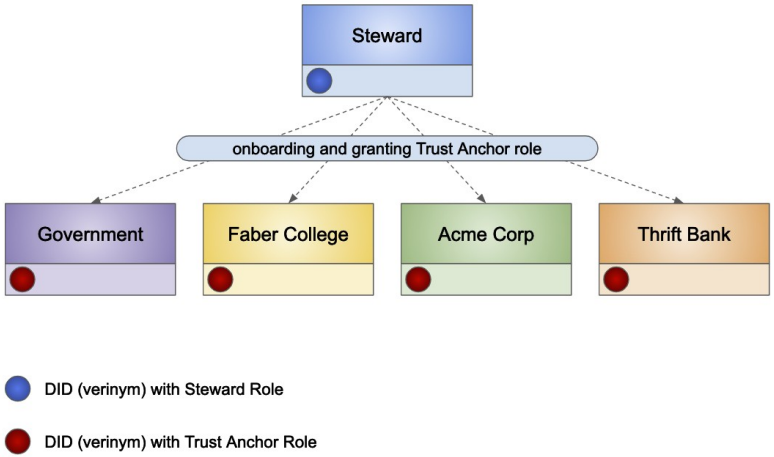
Procesos: Onboarding

- Proceso que implica la creación de un Pairwise-Unique Identifier para la interacción directa entre entre dos actores
- Necesario la primera que vez que se comunican esos 2 actores
- Cada actor genera:
  - DID (pseudonym)
  - Verkey
  - Signing key
- Cada actor mantiene información en un wallet
- Transaction endorser escribe DODs (DID + verkey) en el ledger



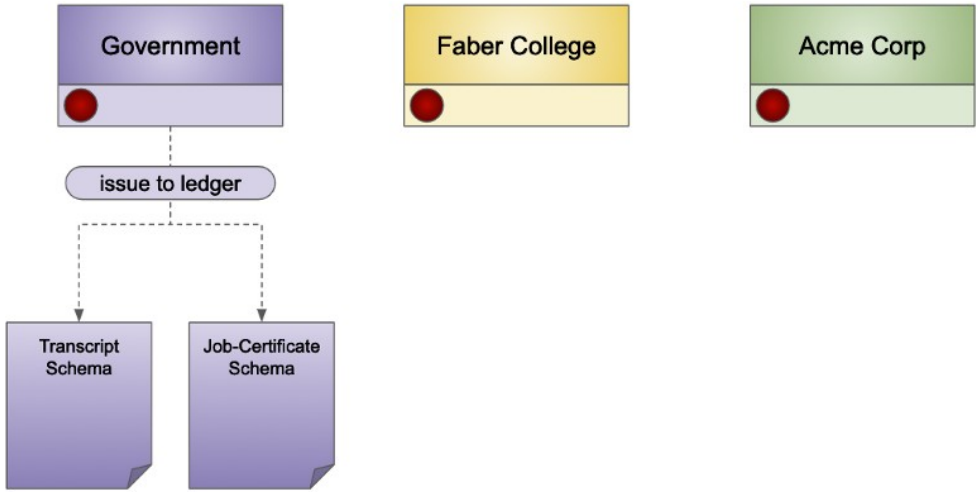
Procesos: Asignación de un verinym

- Requiere Onboarding previo
- Asignación de un DID asociado a una identidad legal para interactuar con el ledger (issuers, verifiers...)
- Sólo un Trust Anchor puede dar de alta un verinym en el ledger
- El identity owner no requiere un verinym (sólo pseudonyms)



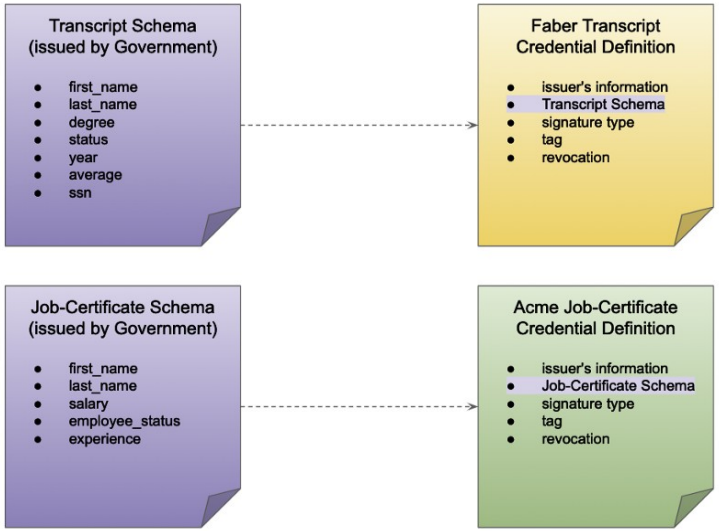
Procesos: Creación de Credential Schemas

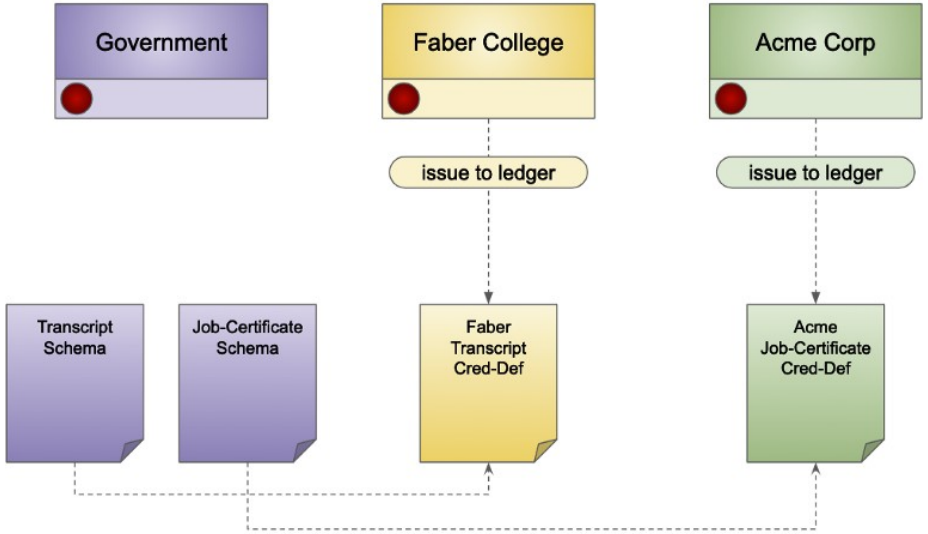
- Definen la estructura de los datos referidos tanto en los Credential definitions como en las propias credenciales
- Almacenados en el ledger



Procesos: Creación de Credential Definitions

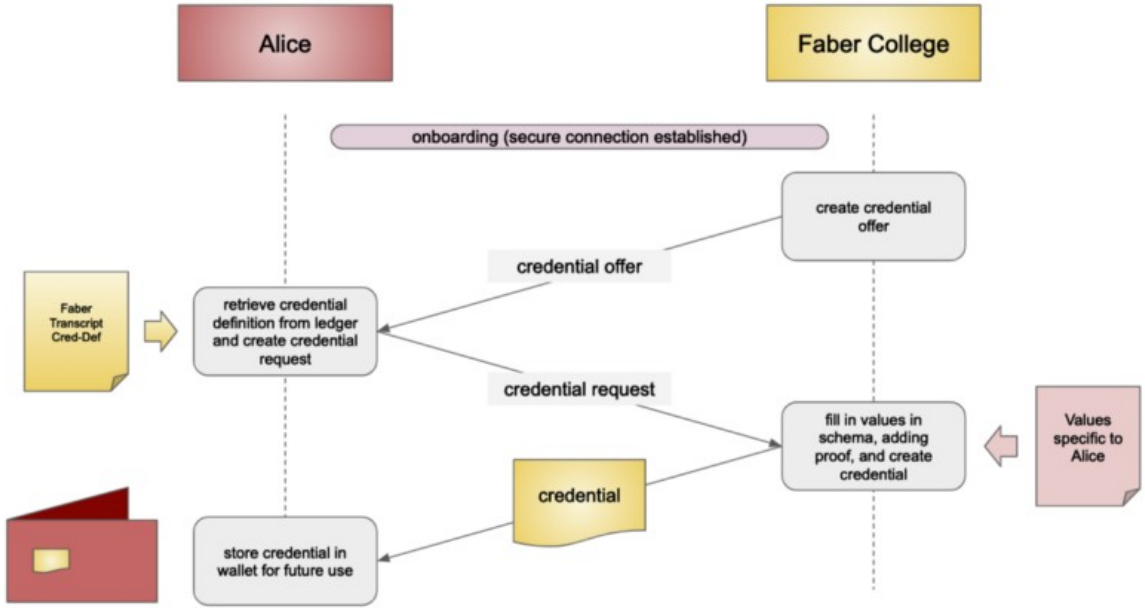
- Los Credential Definitions contienen:
  - El Credential Schema asociado
  - Información sobre el issuer
- Almacenados en el ledger





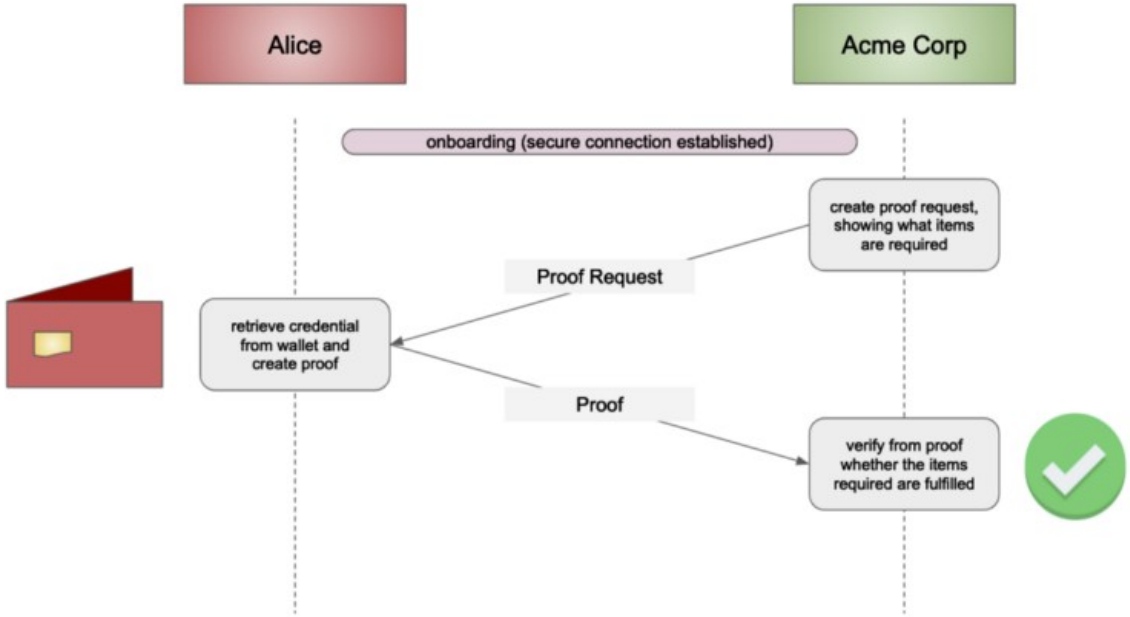
Procesos: Obtención de credenciales

- Requiere Onboarding previo
- Master Secret: Ítem privado que utiliza el individuo para probar que datos de múltiples credenciales tienen un sujeto común

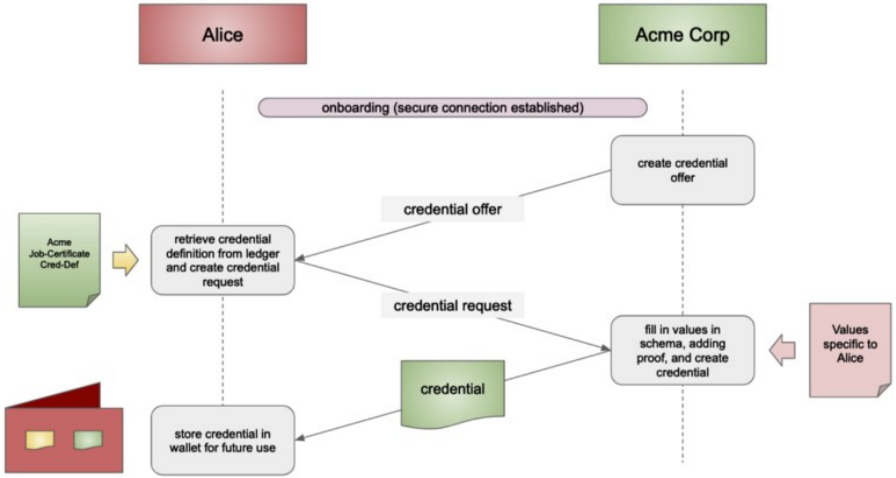


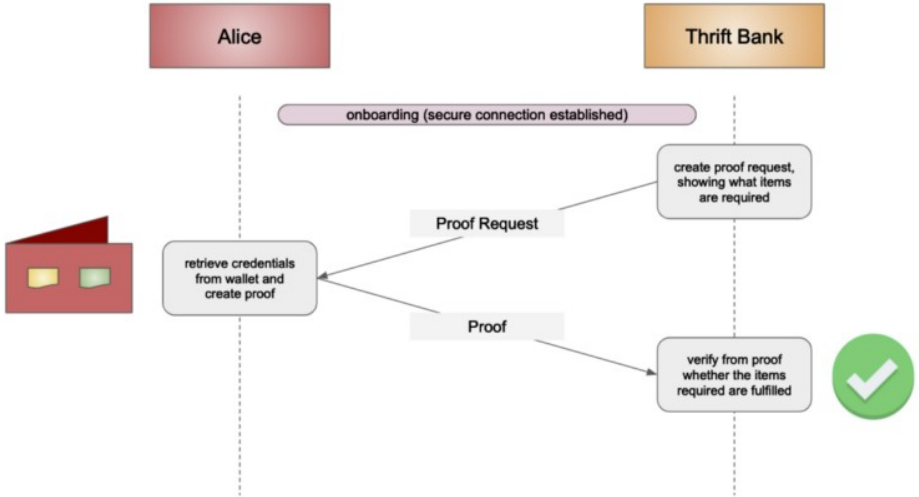
Procesos: Verificación de pruebas

- Requiere Onboarding previo
- No interviene el Issuer



Procesos: Etc.





Agentes Indy

- Tipos:
  - Cloud agents: Issuers, verifiers
  - Edge agents (mobile, etc.): Identity Owners
- Wallets
- Comunicación entre agentes:
  - Definido el formato de los mensajes de la capa de aplicación
  - Pendiente madurar la compatibilidad de las capas inferiores (2019 Q1)
- Libindy: Rust based C-callable library
- Indy SDK: Wrappers: Java, Python, iOS, NodeJS, .Net, Rust
- Indy CLI: Command Line Interface

Sovrin Network

- Red pública Hyperledger Indy
  - https://sovrin.org/
- Trustees:
  - Miembro del Sovrin Foundation Board of Trustees
  - https://sovrin.org/team/
- Stewards:
  - Validator/observer nodes
  - Rol Trust Anchor implícito
  - https://sovrin.org/stewards/
- Alta como Transaction Endorser
  - Issuer/(verifier)
  - https://sovrin.org/issue-credentials/
  - Pricing
    - Roadmap: Indy Token

Item	Price
DID Write	$10
Schema	$50
Credential Definition	$25
Revocation Registry	$20
Revocation Update	$0.10

Hazlo práctico

- Simple PoC:

https://medium.com/@kctheservant/exploring-hyperledger-indy-through-indy-dev-example-10075d2547ae

- Entorno de desarrollo

https://github.com/sovrin-foundation/indy-dev

Preguntas