

Chaincode con datos privados de transacciones



Contenido

- Introducción
- Canales vs. colecciones de datos privados
- Canales
- Colecciones de datos privados
 - Difusión de datos privados
 - Colecciones implícitos y explícitos
- Demo



Introducción

¿Por qué necesitamos datos privados?

Mantener información sensible off-chain pero con integridad y relacionada a una transacción

Publicar información de forma inmutable sin de revelar la información mismo

Para pre-aprobar transacciones con ciertos parámetros acordados privadamente

Compartir información de transacciones solamente con un grupo selecto de participantes

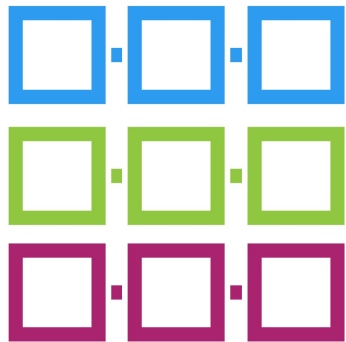
...



Canales vs. colecciones de datos privados

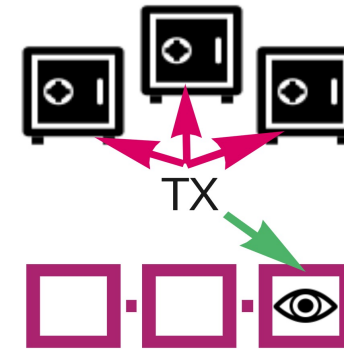
Dos soluciones para diferentes escenarios

Canales



Transacciones completamente privadas de otros canales

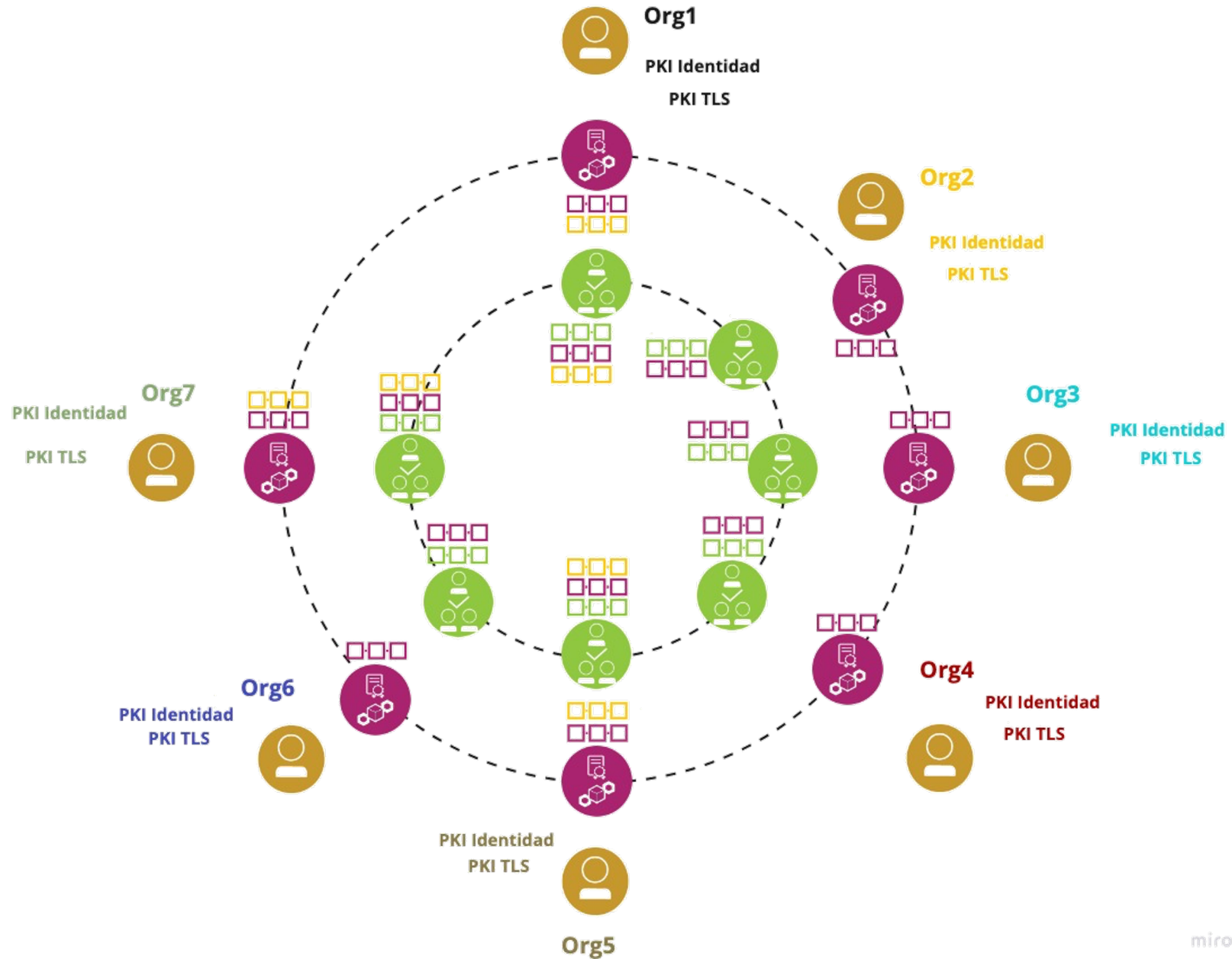
Colecciones



Transacciones públicamente compartidas en mismo canal con cierta información privada compartida y guardada *off-chain*

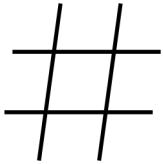


Canales



Colecciones de datos privados

Funciones hash



Integridad de información

Datos privados

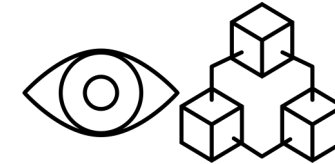
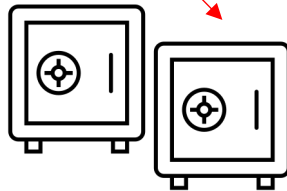
Hash

Hola, comunidad Hyperledger Latam!

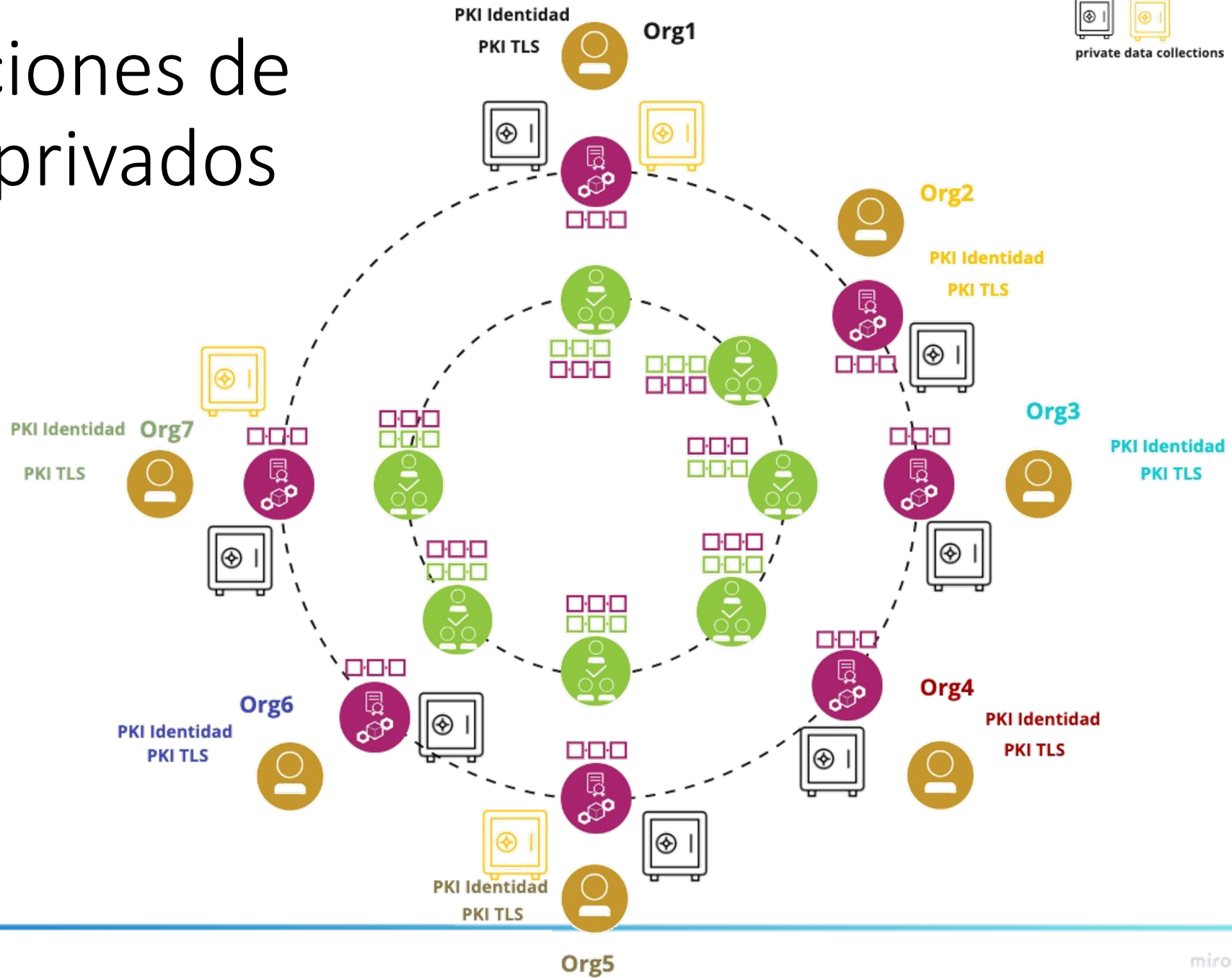
Hash(mensaje)

3a7af2f7d2a0a31ac06a446b24233ef8f9591b332d172ea7b146b39217804aeb

miro



Colecciones de datos privados



Colecciones de datos privados

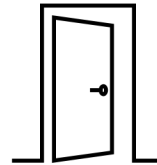
Difusión de datos privados

Anchor peers



Comunicación directo entre peers de diferentes organizaciones

External Endpoints



Políticas de endorsement correctos



Aprobaciones de las transacciones sin de compartir los datos privados con organizaciones no autorizados



Colecciones implícitos y explícitos

Colecciones implícitos

Datos privados guardados por una sola organización. No se tienen que definir explícitamente, Fabric ya crea una colección por cada organización.

Útil en el momento de querer compartir datos privados directamente con una sola organización

Colecciones explícitos

Grupos de miembros de que es previamente conocido que todos en el grupo tienen que recibir los mismos datos privados de ciertas transacciones

! Numero de organizaciones en una colección tiene que ser igual o mayor al numero de *endorsements* necesarios para las transacciones!

