



Ecosistema descentralizado,
la evolución de la identidad

Identidad, hoy

Documentos de Identidad

Acta de nacimiento, Credencial de Elector, Pasaporte, Cartilla, CURP



Documentos con relación a la identidad

Recibos de luz, agua, facturas, nómina, estados de cuenta



Identidad biométrica

Rasgos faciales, minucias dactilares, patrones de voz



Rastro Digital

Redes sociales, sitios web, trámites en línea



Identidad móvil

Contraseñas, ubicaciones, preferencias, configuraciones

Problemática

© 1993 The New Yorker Peter Steiner



"On the internet, nobody knows you're a dog."



Problemática

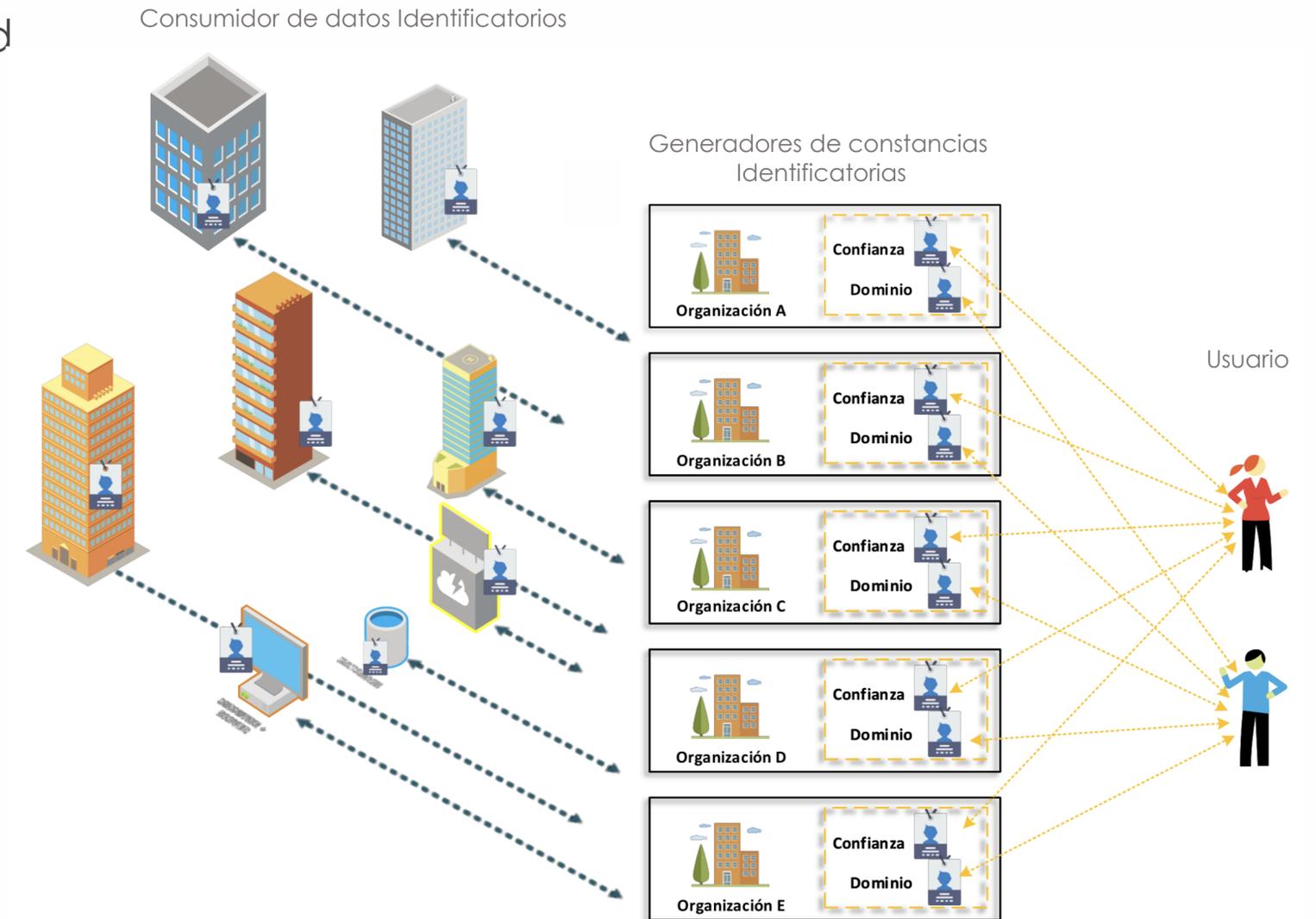
- Conforme avanza el **mundo digital**, la forma de identificarnos se vuelve **más compleja**.
- Un individuo ya **no es representado** sólo por el nombre, género, fecha de nacimiento y dirección.
- **La identidad** ahora incluye detalles como el **empleo, relaciones sociales, financieras e historial médico** entre otros
- Las personas tenemos poca o nula visibilidad del intercambio de atributos de nuestra identidad para la **autenticación, verificación y autorización**



Desafíos

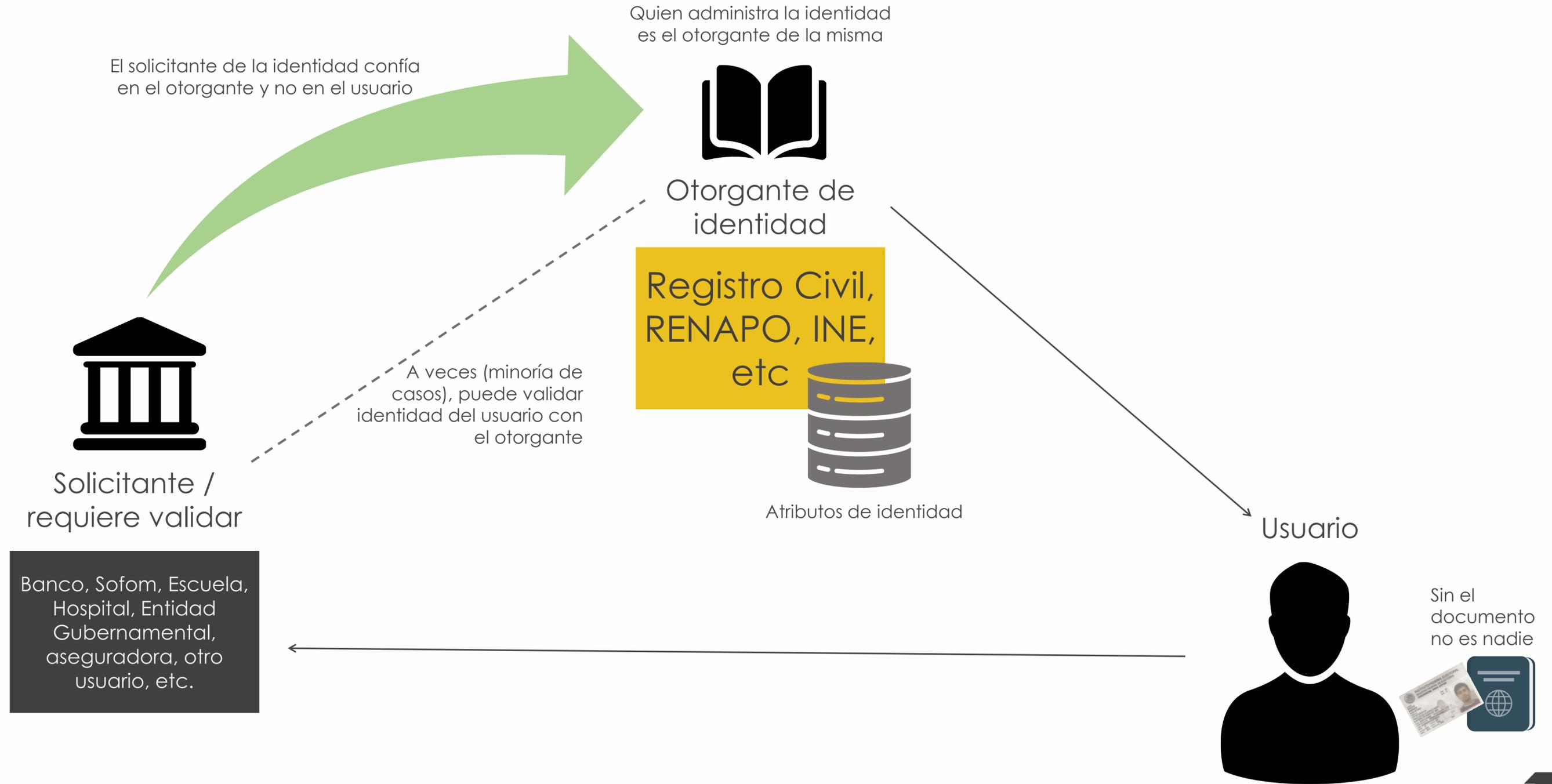
- Para las **personas**:
 - Demasiados pasos y documentos para validar la identidad
 - Sobreexposición de datos en documentación física
 - Control limitado sobre la información
 - Incertidumbre sobre gestión de información compartida
 - Robo de identidad
- Para las **empresas**:
 - Cumplimiento y regulación
 - Fraude y violación de datos
 - Costos, complejidad de gestión y uso
 - Falta de confiabilidad
- Para los **gobiernos**
 - Garantizar la privacidad y seguridad
 - Protección de documentos de identidad contra falsificaciones, alteraciones o robos
 - Aumento de los costos y complejidad en la emisión, renovación, mantenimiento, monitoreo y verificación de la identificación física.

Esquema actual de identidad centralizada



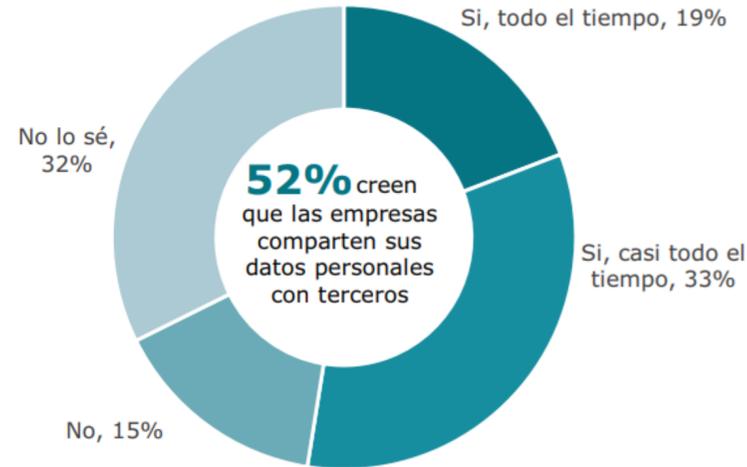
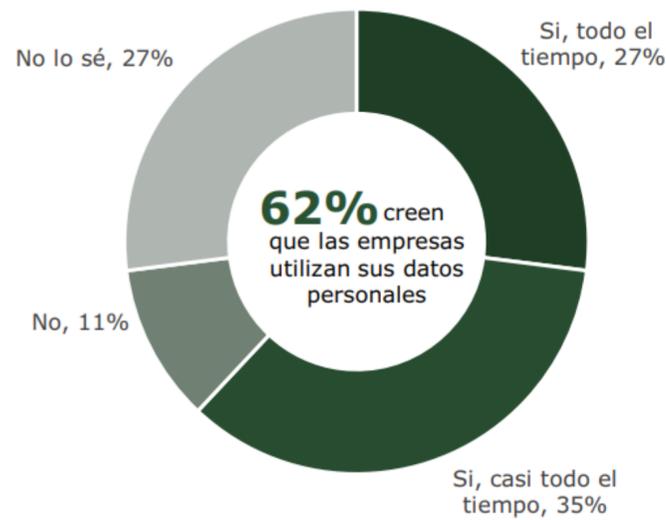
Actualmente se confía en el otorgante de la identificación y no en el usuario

Identidad hoy | Ejemplo conceptual



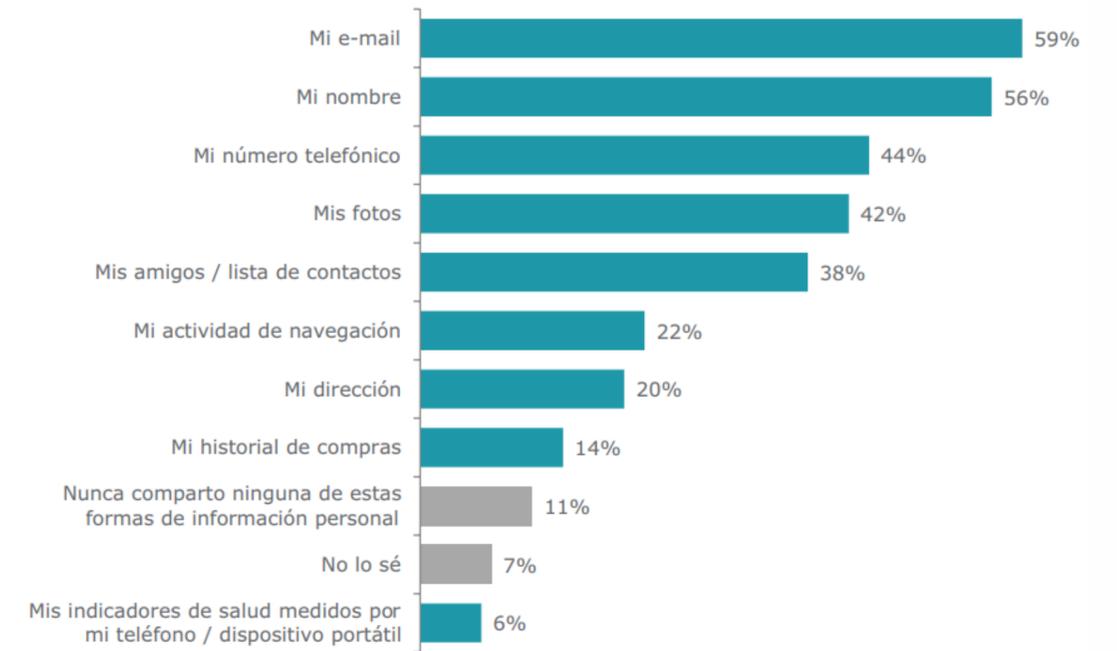
Situación en MX

Encuesta a dueños de teléfonos inteligentes sobre utilización de **datos personales** compartidos a empresas



Fuente: Edición México, Deloitte Global Mobile Consumer Survey, May - Jun 2017
Base: Todos los propietarios de Smartphone de 18-50 años, México, 2017: 1885

Tipo de información compartida en línea



Robo de identidad

01 3er lugar en Latinoamérica

Solo en el primer semestre del 2017 se atendieron **39 mil 758** posibles casos. **22% más** vs mismo periodo en 2016. El monto total por los reclamos asciende hasta **929 millones de pesos**

02 8vo lugar a nivel mundial

En 2016 generaron ingresos de mil 500 a mil 800 millones a los defraudadores

Fraudes cibernéticos

03 Aumentó del 25% en fraudes cibernéticos en 2018 vs el 2017.

04 67% de los casos de robo de identidad ocurren por pérdida de documentos

Uso de smartphone en MX

Usuarios

Actualmente existen 102.9m de teléfonos inteligentes

87.6% de líneas móviles son teléfonos inteligentes

En 2020, el 80% de los celulares vendidos, contarán con un sensor biométrico*

*Fuente: El Economista



18.9m de líneas postpago

01

79.8% redes sociales

02

69.7% apps de contenidos multimedia

03

16% banca móvil y finanzas

04

Evolución de la identidad digital

Bases de información identificatoria centralizadas, controladas por instituciones

1995 - Fase 1:
Identidad centralizada



Identidad pertenece y es administrada por una sola entidad bajo sus propias reglas.

- Funciona bien dentro de dominios propio
- Identificación de usuarios
- Servicios de login fragmentados
- Centrado en proveedores, usuario no es dueño de sus datos
- Borrable

Ejemplo

E-commerce, Redes sociales

2006 - Fase 2:
Identidad Federada



Identidad con cierto grado de portabilidad, permitiendo cierto grado de vinculación de datos y permitiendo acceder a un servicio con las credenciales de otro.

- Perfilamiento de usuarios
- La era de compartir y conectar
- Re-usar autenticación
- Sigue siendo borrable, pero con mayor impacto

Single sign on, login with Facebook...

2016 - Fase 3:
Identidad centrada en el usuario



Usuario participa de manera limitada en la autorización de compartición y gestión de algunos atributos identificatorios

- Identidad permitida por el usuario
- Plataformas de gestión de identidad
- Intercambios digitales continuos
- Bases de datos centralizadas

Hiperconectividad, IoT (reloj inteligente con acceso a geolocalización vinculado a app de salud)

Ahora - Fase 4:
Identidad digital auto-soberana



Identidad controlada por el individuo, seguro, y portabilidad total

Identidad digital auto-soberana

Mundo Antiguo

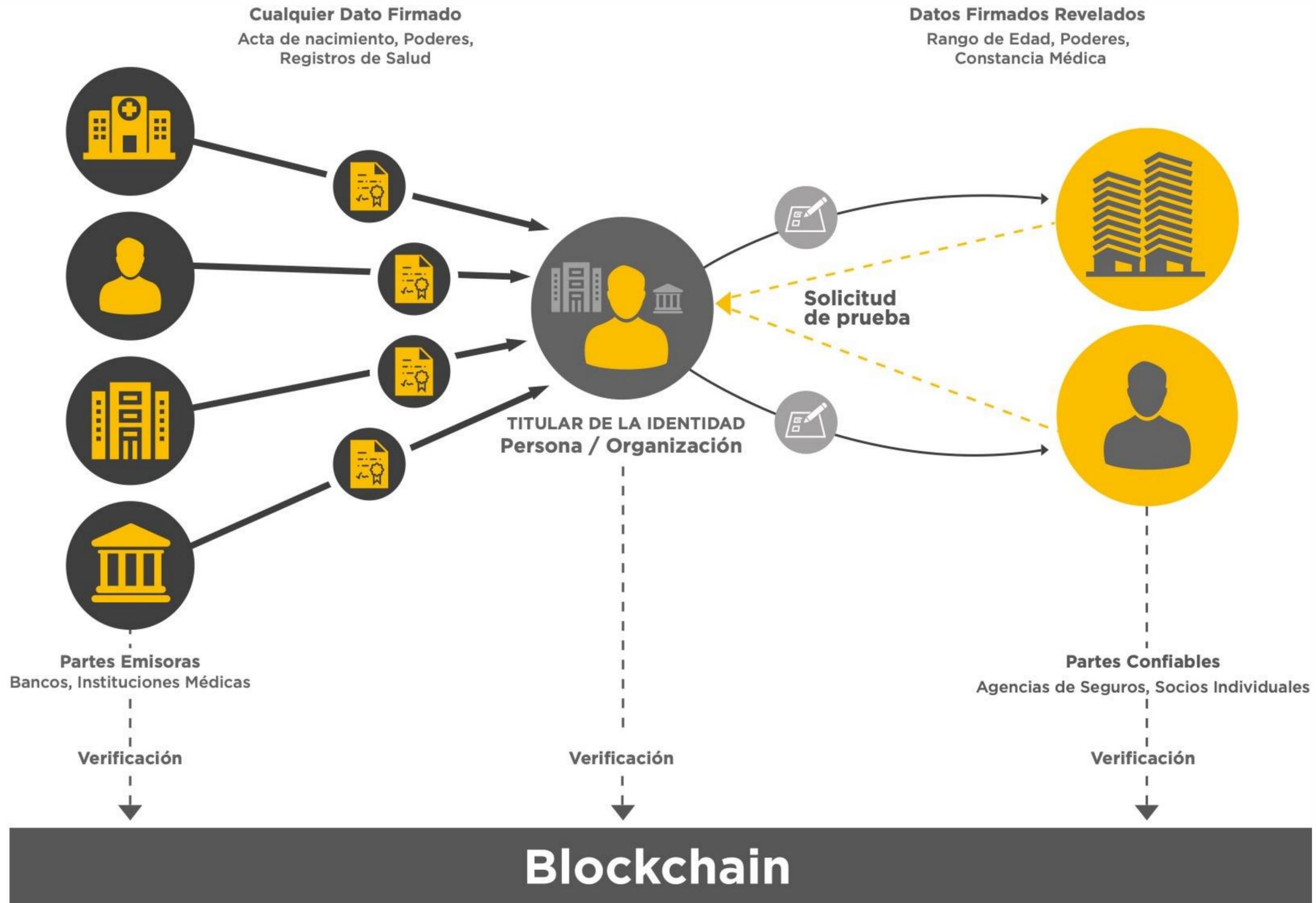


Nuevo Mundo "Post-Silos"



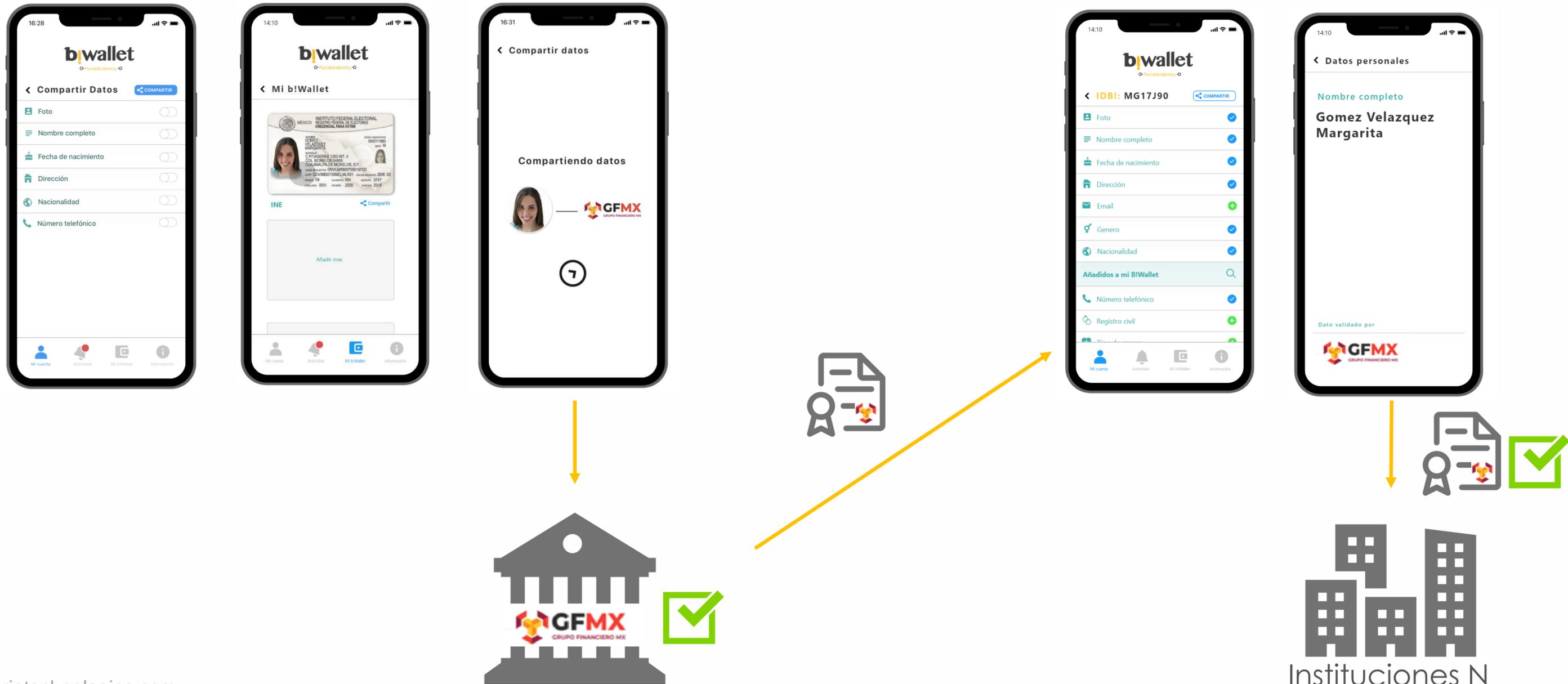
- Diseño centrado en el usuario que le permite controlar sus atributos y perfiles de identidad.
- Permite que los procesos se vuelvan totalmente digitales al tiempo que mantienen la confianza en los elementos de datos.
- Registros auditables para la validación.
- Capacidad de verificar la identidad sin dar a conocer todos los atributos.
- No se puede eliminar
- La existencia de la identidad digital es independiente a cualquier organización
- Usuario decide qué compartir y qué no
- Aseveración de identidad es autoverificable o verificable por un tercero
- De una identidad de silos a un ecosistema de identidades

Binaria Identity - ¿cómo funciona?

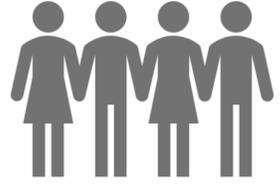


Binaria – identidad controlada por el usuario

Ecosistema colaborativo basado en tecnología Blockchain donde el usuario es dueño de las validaciones de su identidad por parte de terceros y decide qué información validada compartir y con quién.



Binaria – Beneficios



- Comprobación sencilla de identidad
- Control de información compartida
- Revocabilidad de permisos
- Acceso a más trámites en línea
- Aumento de confianza en dato identificatorio entre más se utilice
- Disminución de suplantación
- Posibilidad de identificación paperless



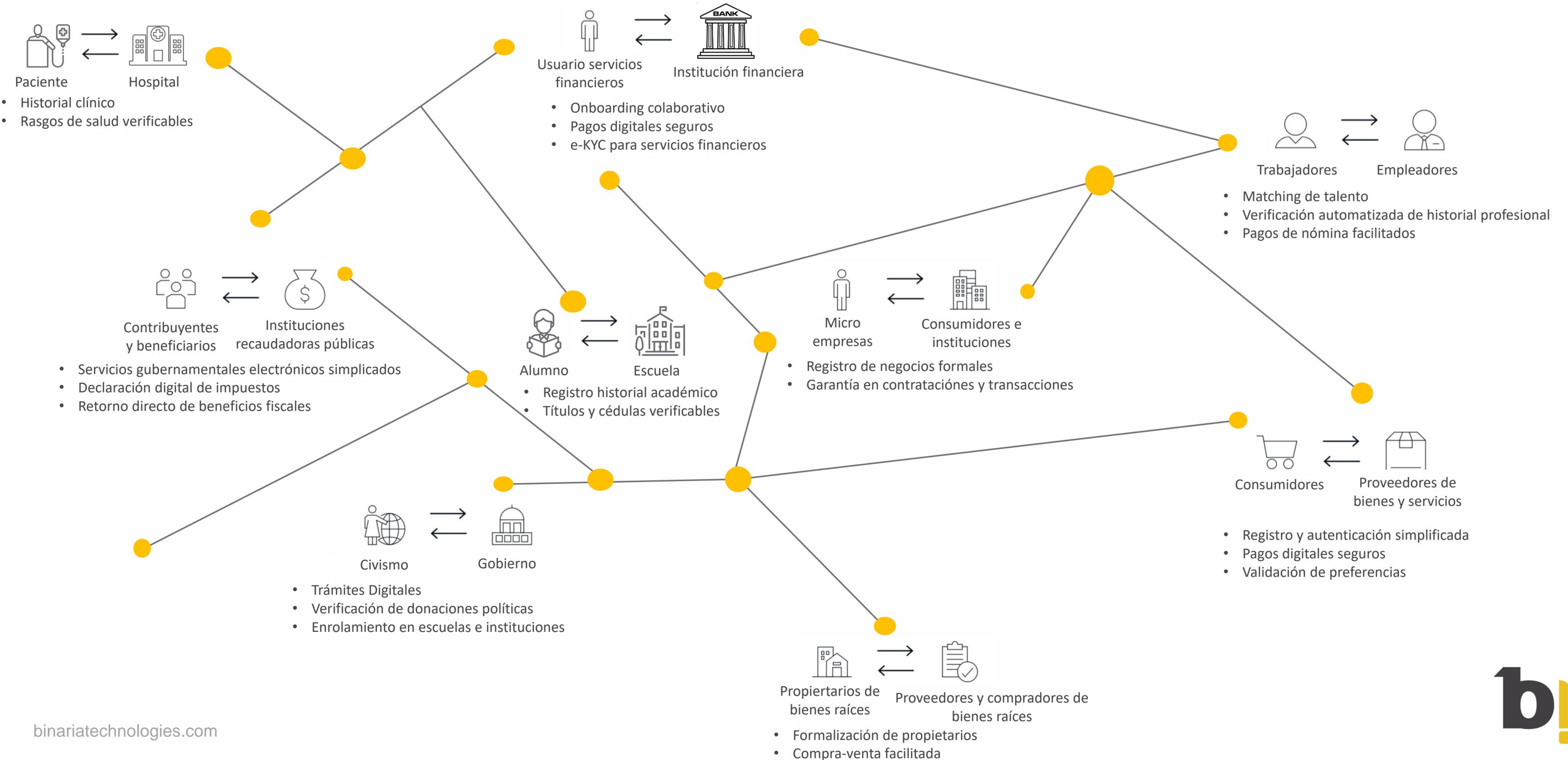
- Cumplimiento y regulación
- Disminución de fraude y violación de datos
- Trámites más sencillos para usuarios
- Aumento de confianza en identidad
- Aprovechamiento de ecosistema colaborativo
- Disminución de costos de identificación de clientes
- Menor costo de gestión de datos personales



- Privacidad y seguridad aumentada con capa adicional a identidad gubernamental
- Traslado de administración de identidad digital a usuario
- Garantía de privacidad de datos
- Garantiza identidad del usuario ante eventos de contingencia

Todos los actores se benefician por formar parte del ecosistema colaborativo, asegurando total control del usuario

Ecosistema de casos de uso



THANK YOU

HAVE A NICE DAY

binaria^{MR}
by DOCSOLUTIONS

○ Digital Transformation ○