Identidad Digital Soberana para Bolivia

Un sistema que crea una identidad única para su interacción en Blockchain

Resumen Ejecutivo

Este libro blanco propone una Identidad Digital Soberana (IDS) para Bolivia que devuelve el control al ciudadano, reduce la repetición de trámites y protege la privacidad por diseño. La solución combina Identificadores Descentralizados (DID) y Credenciales Verificables (VC) con presentaciones de mínima divulgación y pruebas de conocimiento cero (ZKP) para validar condiciones (p. ej., “mayor de 18”) sin exponer datos sensibles.

WIRA Wallet genera el DID y las claves en el dispositivo y guarda las credenciales en el almacenamiento cifrado de la app protegido por Keystore/Keychain; solo se desbloquea durante la acción del usuario (PIN/biometría). Las verificaciones pueden ser off-chain (portales/apps) u on-chain (contratos de atestiguamiento/trazabilidad). En cadena no se escribe PII: se anclan referencias verificables (CIDs) y eventos.

La emisión de VCs se realiza con un Issuer propio compatible con Polygon ID y el protocolo de mensajería iden3comm. Cada VC incluye un statusPointer (ubicación de la lista pública de estado + índice) para que terceros verifiquen si está vigente/suspendida/revocada sin ver su contenido. Para operar en blockchain se usa Account Abstraction (ERC-4337) con Smart Accounts y Paymasters. La recuperación ante pérdida del dispositivo emplea Shamir Secret Sharing en modalidades Carnet+PIN (2-de-2) y Guardianes (n-de-s). El resultado es una plataforma interoperable, auditable y alineada con la normativa boliviana.

Índice

1. Introducción

Este White Paper propone una plataforma de Identidad Digital Soberana (IDS) para Bolivia basada en tres principios: control del usuario, seguridad por diseño y mínima divulgación. WIRA Wallet genera el identificador descentralizado (DID) y sus claves en el propio dispositivo y conserva las credenciales del titular en el almacenamiento cifrado de la app, protegido por el Keystore (Android) / Keychain (iOS). Ese almacenamiento se desbloquea temporalmente en memoria sólo cuando el usuario se autentica (PIN o biometría) y, al terminar la operación, la clave se borra de memoria; nunca se guarda información en claro en el teléfono. Con estas credenciales, la wallet construye presentaciones con pruebas criptográficas que revelan únicamente lo imprescindible para autorizar una acción (afirmar que una evidencia pertenece a una persona o a un proceso) sin exponer datos personales.

La verificación puede ocurrir off-chain en portales (frontends) y backends (servidores) o on-chain, en contratos inteligentes. La capa on-chain se limita a custodiar y operar la Smart Account del titular y a ejecutar contratos de dominio como el atestiguamiento y trazabilidad, pero no se registran datos personales (PII) en la cadena. Para simplificar la experiencia se emplea Account Abstraction (ERC-4337): la wallet firma UserOperations y puede usar Paymasters que patrocinen comisiones de red bajo políticas definidas, evitando que el ciudadano gestione gas manualmente.

1.1 Contexto

En Bolivia, el acceso a servicios públicos y privados suele exigir la misma información personal una y otra vez (KYC repetido). No existe portabilidad de datos entre instituciones, y los repositorios centralizados concentran riesgo de filtraciones. Esta dinámica aumenta costos y tiempos, desalienta la adopción digital y expone a la ciudadanía a suplantaciones.

Además, en procesos que requieren trazabilidad y atestiguamiento por ejemplo, la carga y validación de actas, o las certificaciones de origen y calidad en cadenas productivas a menudo faltan evidencias verificables (firmas/hashes/estado de vigencia) y registros auditables por terceros sin fricción. La desconfianza entre actores y la conectividad irregular provocan verificaciones duplicadas y tareas manuales, lo que introduce fricción operativa: más pasos, más esperas, más costos y mayor probabilidad de error.

La propuesta IDS aborda estos puntos con

- Credenciales verificables (VC) portables controladas por el usuario.
- Presentaciones de mínima divulgación con caducidad y destinatario
- Operaciones on-chain sin PII y con experiencia de bajo roce como el gas patrocinado
- Evidencias de trazabilidad como archivos y metadatos publicadas en IPFS y atestadas en contratos.

1.2 Objetivo del proyecto

Objetivo General:

Diseñar e implementar una plataforma IDS que devuelva el control al titular, minimice la exposición de información personal, reduzca la fricción operativa y respete el marco legal boliviano.

Objetivos específicos:

- Desarrollar y publicar WIRA WALLET con generación local de DID y claves, bundle (almacenamiento cifrado de la app protegido por Keystore/Keychain) cifrado para custodiar credenciales () y metadatos operativos mínimos, presentaciones con nonce, destinatario y caducidad. También interfaz de historial local visible sólo por el usuario.
- Operar Issuer Nodes para emisión de credenciales y afirmaciones a través de nuestro Issuer propio (por ahora único), publicando el estado de vigencia de forma compacta y conservando sólo metadatos mínimos de auditoría, sin almacenar atributos personales.
- Ejecución on-chain con Smart Accounts (ERC-4337) y Paymasters aplicando políticas de patrocinio adecuadas a los flujos de atestiguamiento y trazabilidad ya operativos
- Pipeline seguro de evidencias off-chain, incluida captura y OCR mediante backend propio (para no exponer API keys), hash de los archivos y publicación en IPFS, enlazando esa evidencia con atestaciones on-chain cuando el proceso lo requiera.

1.3 Problema y oportunidad

Problema actual: Persisten la repetición de datos, los silos entre instituciones, el riesgo por almacenamiento centralizado, la fricción elevada en verificaciones y una trazabilidad limitada que reduce la confianza y la capacidad de auditoría.

Oportunidades con IDS: Portabilidad de atributos controlada por el propio usuario, verificación inmediata con presentaciones de mínima divulgación y estados de vigencia consultables, reducción de tiempos y costos al eliminar pasos redundantes, menor

superficie de ataque al mantener la PII fuera de la cadena y cifrada en el dispositivo, y trazabilidad/atestiguamiento verificables (evidencias en IPFS + eventos on-chain) que fortalecen la auditabilidad de procesos cívicos y productivos y mejoran la competitividad en mercados que exigen certificaciones verificables de origen y calidad.

2. Fundamentos técnicos

2.1 Identificador descentralizado.

WIRA Wallet genera en el dispositivo un par de claves y deriva un DID conforme a métodos compatibles. El documento DID público publica las claves de verificación activas. La clave privada nunca abandona el dispositivo.

2.2 Credenciales verificables en JSON-LD.

Una VC es una afirmación firmada por un emisor confiable sobre atributos del titular. Se emite en JSON-LD o SD-JWT (según el esquema elegido) e incluye:

- Prueba de origen e integridad (firma del emisor).
- Puntero de estado (Status Pointer) hacia una lista pública compacta de estado de vigencia (vigente/suspendida/revocada).

La wallet guarda la VC en el almacenamiento cifrado de la app protegido por Keystore/Keychain. El Issuer propio basado en Polygon ID valida la evidencia recibida y devuelve la VC firmada con su DID de emisor.

2.3 Presentaciones verificables con conocimiento cero.

Cuando un verificador solicita algo, la wallet construye una Presentación Verificable (VP) que contiene sólo lo requerido (selective disclosure) y puede incluir pruebas de conocimiento cero (ZKP), sobre curva BJJ para pruebas de rango o pertenencia. Cada VP incorpora:

- nonce (identificador único de solicitud),
- aud (dominio/destinatario),
- caducidad (TTL).

Esto previene reutilización y correlación de presentaciones.

2.4 Mensajería segura con iden3comm.

Emisión y presentación se cursan por iden3comm, con cifrado punto a punto y autenticación mutua entre WIRA Wallet y el Issuer o el Verifier. El backend, actúa como pasarela de transporte sin acceso al contenido.

2.5 Ejecución on-chain con Account Abstraction.

La operación en cadena se realiza con una Smart Account compatible con ERC-4337 (EntryPoint v0.7). La wallet firma UserOperations con su clave local y las envía al EntryPoint. Si hay patrocinio, un Paymaster cubre comisiones bajo políticas. Este modelo reduce pasos operativos y evita exponer PII en la cadena.

En el caso de trazabilidad/atestiguamiento, los contratos on-chain registran CIDs de evidencias (IPFS) y emiten eventos verificables. Sin embargo la lógica de verificación de ZK y estados de VC ocurre off-chain.

3. Arquitectura técnica

3.1 Capa de identidad.

La identidad del titular nace en su propio dispositivo. WIRA Wallet genera localmente el par de claves y deriva un DID (identificador descentralizado). A partir de ese DID se publica un documento DID con las claves de verificación activas La clave privada asociada al DID no sale del teléfono: sólo se usa para firmar cuando el usuario se autentica y la operación lo requiere. En paralelo, la app mantiene una clave (privkey) para operar on-chain ligada a la Smart Account del titular que se desplegará al momento de la primera transacción.

3.2 Capa de credenciales.

Emisión por parte del Issuer Node de Polygon ID, almacenamiento cifrado en WIRA Wallet localmente (bundle), presentación bajo demanda y listas compactas de estatus o mecanismos equivalentes para revocaciones y expiraciones. Cada VC incluye un puntero “status” a una lista compacta pública mantenida por el emisor (por ejemplo, bitstring o merkle map) para marcar vigencia, suspensión o revocación.

Las Credenciales Verificables (VC) se emiten hoy desde nuestro Issuer node propio basado en Polygon ID y se codifican en JSON-LD para aportar semántica y compatibilidad con verificadores estándar. Cada VC incluye la firma del emisor y un puntero de estado hacia una StatusList pública del emisor, donde cualquier tercero puede consultar si la

credencial está vigente, suspendida o revocada. La VC no se guarda en servidores se conserva sólo en el dispositivo del titular dentro de un bundle cifrado local (almacenamiento cifrado de la app protegido por Keystore/Keychain), y el emisor preserva metadatos mínimos en su base interna sin PII

3.3 Capa de privacidad.

La verificación se diseña bajo mínima divulgación. Ante una solicitud, Wira construye una Presentación Verificable (VP) que contiene sólo los atributos estrictamente necesarios y agrega controles anti-correlación: un nonce único por solicitud, un destinatario explícito y una caducidad breve. Cuando el caso lo amerita, la VP incorpora pruebas de conocimiento cero (ZKP) para demostrar condiciones sin revelar valores en claro. Todo el intercambio punto a punto cursa por iden3comm, con cifrado end-to-end.

3.4 Capa de ejecución en cadena (on-chain).

La operación on-chain se limita a lo necesario para el caso de trazabilidad y atestiguamiento: la Smart Account del titular (ERC-4337) firma y envía UserOperations al EntryPoint, y los contratos de atestiguamiento registran referencias y emiten eventos verificables. No se registra PII en la cadena. Para simplificar la experiencia, un Paymaster puede patrocinar gas bajo políticas de modo que el usuario no deba gestionar las comisiones.

3.5 Capa de integración.

La plataforma expone un pipeline de evidencias orientado a trazabilidad y atestiguamiento: la app captura imágenes y datos se ejecuta un OCR/validaciones (sin exponer API keys en el cliente), calcula el hash y publica archivos/metadatos en IPFS, obteniendo su CID (identificador inmutable del contenido). Ese CID se enlaza on-chain mediante los contratos de atestiguamiento desde la app (frontend): todas las operaciones en cadena se inician y se firman en WIRA Wallet con claves locales el backend nunca firma ni envía transacciones en nombre del usuario, ni custodia claves. Los portales de terceros verifican combinando: el evento on-chain (quién atestiguó y cuándo), la recuperación en IPFS usando el CID (garantiza que el contenido leído es exactamente el atestado), y cuando aplica, la consulta del estado de credenciales en la StatusList pública del Issuer indicada por el statusPointer de la VC. No se expone PII en la cadena.

3.6 Esquema de almacenamiento y custodia

En el dispositivo del usuario se guardan tres piezas:

- La semilla/clave del DID
- La clave privada (privkey) usada por la Smart Account
- las VCs en el almacenamiento cifrado de la app protegido por Keystore/Keychain.

Este bundle se cifra con AES-256-GCM utilizando una DEK (Data Encryption Key) que a su vez se protege con una KEK derivada del PIN del usuario y un secreto del almacén seguro del dispositivo (derivación tipo Argon2id). El bundle se descifra temporalmente en memoria cuando el usuario se autentica y, al finalizar la operación, la clave se borra de la memoria, nunca se almacena información en claro en el teléfono. La recuperación por pérdida del dispositivo se implementa con Shamir Secret Sharing (SSS): el secreto de recuperación del bundle se fragmenta para los esquemas Carnet+PIN (2-de-2) y/o Guardianes (n-de-s), de manera que el usuario pueda recomponer el acceso sin que ningún actor, por sí solo, pueda hacerlo.

4. Flujos

4.1 Onboarding y emisión.

Al instalar WIRA Wallet, el usuario genera localmente una semilla maestra. A partir de esa semilla se derivan dos claves: la clave de identidad que es el DID para la capa de credenciales, y la clave privada privkey que se usará para operar on-chain. Con esta clave privada (privkey) se calcula la dirección predictiva de su Smart Account (ERC-4337) mediante la fábrica el contrato no se despliega todavía.

Para solicitar una VC de identidad o rol, la app captura imágenes del carnet y rostro y envía solo esas imágenes al backend propio para OCR y liveness (evitamos exponer API keys en el cliente). Del resultado se derivan atributos mínimos (nombres, apellidos, fecha de nacimiento). La app firma una solicitud y la envía cifrada por iden3comm a nuestro Issuer. El Issuer valida la evidencia y emite la VC (JSON-LD) con su firma y un puntero de estado incluido dentro de la propia VC (credentialStatus / statusPointer), que referencia la StatusList pública del Issuer (vigente/suspendida/revocada).

La VC se guarda solo en el dispositivo dentro de un bundle cifrado que es el almacenamiento cifrado de la app protegido por Keystore/Keychain. Ese bundle se cifra con una clave derivada del PIN del usuario más el almacén seguro del dispositivo, cada vez que

el usuario actúa, la app desbloquea temporalmente el bundle para leer/firmar y luego lo vuelve a sellar. El Issuer conserva únicamente metadatos mínimos de auditoría sin PII.

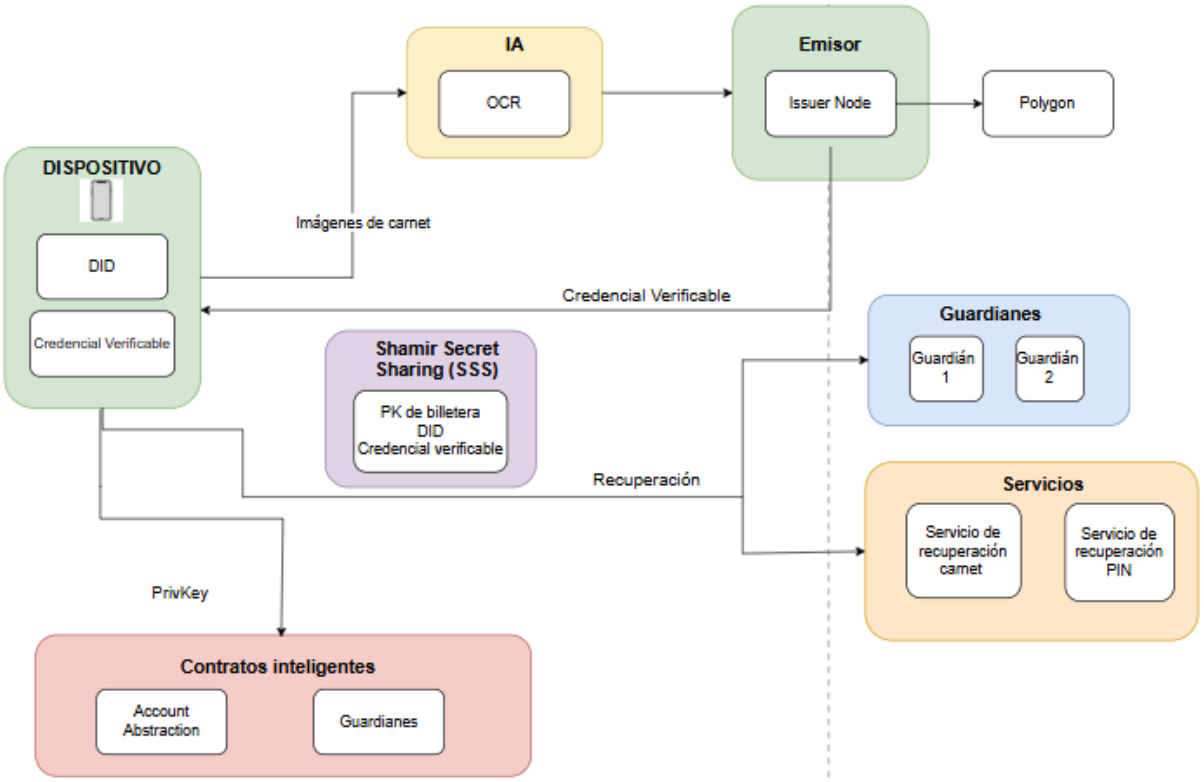

Figura 1 : Componentes e interacciones del sistema IDS

4.2 Presentación y verificación fuera de la cadena.

Cuando un tercero solicita comprobar algo por ejemplo: “esta persona está acreditada como testigo”, o “este certificado de origen está vigente”, WIRA Wallet muestra con transparencia qué se pide, para qué y por cuánto tiempo. Si el usuario acepta, la app construye una Presentación Verificable (VP) con divulgación mínima, incluyendo nonce (identificador único), aud (destinatario) y caducidad. El verificador valida la firma del Issuer de la VC referida y consulta la StatusList pública indicada por el statusPointer. Así obtiene la garantía necesaria sin ver datos personales ni la VC completa.

4.3 Verificación y ejecución on-chain.

Para operaciones de atestiguamiento y trazabilidad, la app construye una UserOperation (ERC-4337) y la firma localmente con la private key del usuario. La UserOperation se envía al EntryPoint y la Smart Account (que ya quedó desplegada durante el registro) ejecuta la llamada a los contratos como registrar o actualizar una evidencia ,

emitir o apoyar un atestiguamiento). Los eventos on-chain dejan constancia verificable de quién y cuándo actuó.

Cuando hay patrocinio de gas, la app solicita directamente al Paymaster compatible con 4337 la autorización y si la política del Paymaster lo permite, cubre la comisión. En todos los casos no viaja PII a la cadena: solo referencias (como CIDs de IPFS)

4.4 Respaldo cifrado y recuperación.

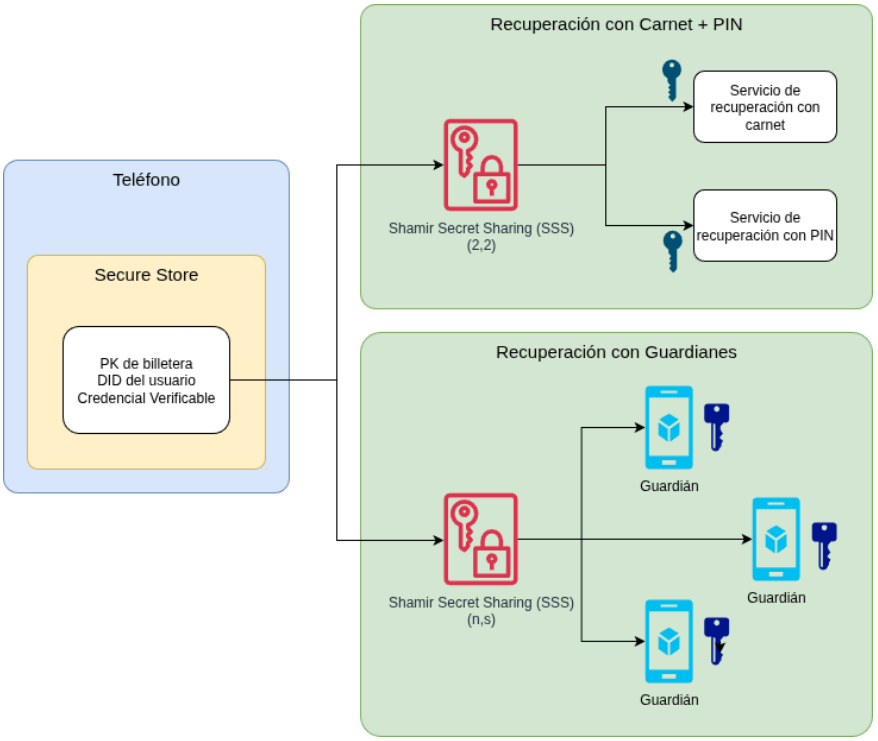

Figura 2 . Recuperación de la cuenta

Los datos del usuario (clave del DID, clave privada (privkey) de su Smart Account y VCs) viven en el bundle cifrado del teléfono. Si el usuario habilita recuperación, se aplica Shamir Secret Sharing (SSS) sobre el secreto de descifrado del bundle:

- Esquema Carnet+PIN (2-de-2): se generan dos shares, uno queda asociado al servicio de verificación de carnet (el usuario vuelve a enviar fotos de carnet/rostro cuando recupera) y el otro al servicio de recuperación por PIN. Con ambos shares se recompone el secreto y se descifra el bundle.

  En el esquema de Guardianes, el usuario registra s guardianes (personas o dispositivos de confianza) y define un umbral n. El secreto de descifrado del bundle se fragmenta con Shamir Secret Sharing (SSS) en s partes (shares), y cada guardián recibe su share. Nadie puede recuperar por sí solo.

  Para recuperar, el usuario reúne al menos n shares. La app recompone el secreto, descifra el bundle cifrado y restaura DID/VC/clave privada (privkey) en el nuevo

dispositivo, volviendo a sellarlo al finalizar. Si no se alcanza el umbral, no es posible recuperar.

5. Privacidad y seguridad

El diseño asume adversarios con acceso físico a un dispositivo perdido o robado, interceptación de comunicaciones, intentos de suplantación y análisis de correlación entre solicitudes. La defensa es por capas: las claves nacen y se custodian en el dispositivo, las credenciales se guardan en un bundle cifrado que se descifra temporalmente en memoria sólo cuando el usuario se autentica (PIN o biometría) y se vuelve a sellar al finalizar la operación, nunca se almacena información en claro. La mensajería entre partes usa iden3comm con cifrado de extremo a extremo y autenticación mutua. Las presentaciones incluyen destinatario (aud), identificador único (nonce) y caducidad, lo que bloquea su reutilización y reduce la correlación. El estado de una credencial se consulta mediante una lista pública compacta (StatusList), sin necesidad de exponer el contenido de la VC. La recuperación del acceso se basa en factores independientes (SSS/guardianes) para que ninguna parte, por sí sola, pueda reconstruir el secreto.

5.1. Datos personales identificables protegidos.

La solución evita exponer PII a registros abiertos o a terceros. Las VCs se conservan sólo en el dispositivo del titular, dentro del bundle cifrado, las VPs revelan únicamente lo necesario para la finalidad solicitada (mínima divulgación) y nunca incluyen la VC completa.

5.2 No correlación y no reutilización.

Cada VP incorpora nonce, aud y caducidad. Esto impide el replay (reutilización de una presentación fuera de su contexto o ventana temporal) y dificulta que distintos verificadores se correlacionen al mismo titular.

5.3 Estatus y revocación sin exponer contenido.

El emisor mantiene una StatusList pública (lista compacta y firmada) donde cada posición representa el estado de una credencial: vigente, suspendida o revocada.

Cada VC lleva dentro un statusPointer que indica dónde consultar esa lista (por ejemplo, una URL o un CID en IPFS) y qué índice corresponde a la credencial. En verificación, el tercero sólo consulta ese estado, no necesita acceder a la VC completa ni a datos personales.

5.4 Recuperación por factores.

Si el usuario habilita la recuperación, se aplica Shamir Secret Sharing (SSS) sobre el secreto de descifrado del bundle:

Carnet + PIN (2-de-2): se generan dos “shares”. Uno se asocia al servicio que valida carnet/rostro (el usuario vuelve a enviar fotos al recuperar) y el otro al servicio de PIN. Se necesitan ambos shares para reconstruir el secreto y descifrar el bundle en un nuevo dispositivo.

Guardianes (n-de-s): el usuario registra s guardianes (personas o dispositivos de confianza) y define un umbral n. Se generan s shares, cada guardián recibe el suyo (cifrado). Con al menos n shares, la app recompone el secreto localmente y restaura DID/VC/clave privada (privkey). Ningún guardián puede recuperar por sí solo.

6. Alineación normativa en Bolivia

- **Firma digital y validez probatoria**: uso de firma digital y validez jurídica de documentos electrónicos conforme a la **Ley 164** y su reglamento; compatibilidad con la infraestructura de certificación (EC Raíz/ATT, ECP públicas/privadas).
- **Identificación oficial**: rol de **SEGIP** como autoridad de CI y del **RUI**; coexistencia de credenciales derivadas (IDS) que no sustituyen la CI pero pueden **comprobar atributos** firmados por emisores autorizados.
- **Interoperabilidad**: integración con la **Plataforma de Interoperabilidad del Estado** para consultas/validaciones institucionales, trazabilidad regulatoria.
- **Protección de datos**: adhesión a principios de licitud, finalidad, minimización, seguridad y derechos ARCO, preparación para futura **Ley de Protección de Datos Personales**, mecanismos de consentimiento y revocación.
- **Los emisores conservan únicamente**: identificador de esquema, DID del emisor, marca temporal de emisión, puntero de estatus y un hash de credentialId. No almacena atributos personales.

7. Casos de uso prioritarios

7.1 Comercio y trazabilidad.

Certificados de origen y calidad como VCs emitidas por organismos autorizados. Evidencias (fotos, análisis, guías) se publican en IPFS y su CID se anota on-chain mediante contratos de atestiguamiento. Un comprador o regulador verifica: quién/cuándo certificó (evento on-chain), que el archivo leído es idéntico al atestado (mismo CID), y que las

credenciales del certificador siguen vigentes (StatusList). Resultado: trazabilidad extremo a extremo sin PII.

7.2 Participación cívica.

Roles como testigo de mesa, delegado u observador se acreditan con VCs de rol. Las actas y evidencias como imágenes se suben a IPFS; sus CIDs se atestiguan on-chain para fijar autoría y temporalidad sin publicar datos personales.

El público audita integridad y secuencia de evidencias (mismo CID, orden de eventos on-chain). La autoridad, con base legal, puede solicitar al titular una presentación que pruebe que esa evidencia pertenece a ese rol/proceso, sin revelar más PII que la estrictamente necesaria. Esto refuerza la confianza cívica, reduce disputas sobre autenticidad y brinda trazabilidad de cada paso del proceso..

8. Principios de diseño

8.1 Soberanía del titular

Las claves y el DID se generan y custodian en el dispositivo. Las credenciales viven en un bundle cifrado que se descifra sólo cuando el usuario actúa (PIN/biometría) y se vuelve a sellar al terminar. El consentimiento es granular, explícito y revocable, y el usuario puede revisar un historial local de presentaciones.

8.2 Mínima divulgación

Cada verificación revela sólo lo estrictamente necesario (“>18 años” en lugar de la fecha de nacimiento). Las VPs integran nonce, aud y caducidad para evitar reutilización y correlación. Cuando se aplica, se usan pruebas de conocimiento cero (ZKP) para demostrar condiciones sin exponer valores.

8.3 Pruebas de conocimiento cero (ZKP)

La wallet puede generar ZKP (pruebas de rango o pertenencia) sobre esquemas compatibles (BBS+/SD-JWT, entre otros), permitiendo a un tercero verificar que una condición es verdadera sin aprender el dato en claro. Esto reduce superficie de ataque y fuga de PII.

8.4 Interoperabilidad

Se adoptan estándares W3C DID/VC, y StatusList (listas públicas firmadas) para estados. Se mantiene compatibilidad con BBS+, JSON-LD y estructuras de estado compactas.

8.5 Basado en Blockchain

La cadena se usa donde aporta valor verificable: Smart Accounts (ERC-4337) del titular y contratos de atestiguamiento que anclan CIDs de evidencias y emiten eventos. Nunca se escribe PII en la cadena. Las verificaciones de VCs (firmas, estado en StatusList) y ZKP ocurren off-chain.

8.6 Seguridad por diseño

Modelo zero-trust entre componentes. Iden3comm para cifrado extremo a extremo, no-custodia de claves, validación explícita de destinatario y ventanas temporales y políticas de revocación/rotación de claves de emisores/verificadores publicadas en el Registro de Confianza.

8.7 Seguridad multicapa.

Bundle cifrado (AES-256-GCM) con DEK aleatoria de 256 bits.
KEK derivada de PIN + almacén seguro del dispositivo (derivación tipo Argon2id) para proteger la DEK. Recuperación sin custodios con Shamir Secret Sharing (SSS): Carnet+PIN (2-de-2), o Guardianes (n-de-s) registrados por el usuario. Rotación y revocación de claves de emisores/verificadores y publicación de su StatusList firmada.

9. Marco conceptual

9.1 Emisor.

Entidad acreditada (pública o privada) que valida evidencia y emite Credenciales Verificables (VCs) firmadas con su DID de emisor. Publica su StatusList (lista pública de estado de credenciales) y su manifiesto en el Registro de Confianza, de modo que cualquier verificador pueda validar firma y vigencia sin acceder a PII. Ahora se opera con un Issuer propio basado en Polygon ID.

9.2 Titular.

Persona u organización que controla un DID y custodia sus VCs localmente en WIRA Wallet dentro de un bundle cifrado. El titular decide qué comparte, con quién y por cuánto tiempo. Cuando un servicio solicita verificación, la wallet genera una Presentación Verificable (VP) con divulgación mínima.

9.3 Verificador.

Servicio o entidad que solicita atributos o pruebas (“mayor de 18”, “rol de testigo vigente”). Verifica: la firma de la VC (origen), el estado en la StatusList del emisor referida por el statusPointer de la VC (vigente/suspendida/revocada), y la integridad y parámetros anti-replay de la VP (nonce, destinatario, caducidad). Con eso decide conceder o no el servicio/beneficio sin ver PII.

9.4 Credenciales verificables.

Afirmaciones firmadas sobre atributos del titular, codificadas en JSON-LD o SD-JWT. Cada VC incluye:

- Prueba de origen e integridad (firma del emisor).
- Metadatos de vigencia (fechas/condiciones).
- credentialStatus / statusPointer: puntero a la StatusList pública del emisor, donde se consulta si la credencial está vigente, suspendida o revocada.

Las VCs no se guardan en servidores: se conservan sólo en el dispositivo del titular, cifradas en el bundle.

9.5 Identificador descentralizado. (DID)

Identificador criptográfico cuyos documentos DID publican las claves de verificación activas y endpoints de servicio. La clave privada asociada nunca sale del dispositivo: se usa para firmar sólo cuando el usuario se autentica y la operación lo requiere.

9.6 Presentaciones verificables. (VP)

Paquetes construidos por la wallet con subconjuntos de una o más VCs y, cuando aplica, pruebas de conocimiento cero (ZKP) para demostrar condiciones sin exponer valores en claro. Cada VP incorpora nonce (identificador único por solicitud), aud (destinatario explícito) y exp (caducidad), lo que previene reutilización y correlación.

9.7 Account Abstraction.

La identidad del titular puede operar en cadena mediante una Smart Account (ERC-4337). La app firma UserOperations localmente y las envía al EntryPoint. Un Paymaster (opcional) puede patrocinar gas bajo políticas. La capa on-chain se usa para atestiguamiento/trazabilidad (eventos, CIDs) y no registra PII.

9.8 Gestión de estado

El emisor publica una lista pública firmada que marca, para cada VC, si está vigente, suspendida (reversible) o revocada (definitiva). Se usan formatos compactos compatibles para eficiencia y privacidad:

- Bitstring indexada (cada índice representa una VC).
- Merkle map (clave = hash(credentialId), valor = estado) con raíz Merkle firmada.

El statusPointer incluido en la VC indica dónde consultar esa lista (URL/CID/DID-URL). El verificador sólo aprende el estado, no el contenido de la VC.

9.9 Respaldo y recuperación.

Las VCs y claves viven en un bundle cifrado en el dispositivo. De forma opcional, el titular habilita recuperación usando Shamir Secret Sharing (SSS) sobre el secreto de descifrado del bundle:

- Carnet+PIN (2-de-2): el usuario recupera aportando fotos de carnet y rostro (para el share 1) y su PIN (share 2).
- Guardianes (n-de-s): el usuario registra s guardianes y define umbral n. Cada guardián recibe un share; para recuperar se juntan ≥ n shares.

El DID no se regenera: se restaura el bundle original. Si el usuario no alcanza el umbral, no es posible recuperar.

9.10 Registro de confianza

El Registro de Confianza es un directorio público sin PII que se opera inicialmente y donde cada Emisor/Verificador publica su DID, la huella de su clave pública y el CID de su manifiesto JSON firmado, un contrato on-chain ancla estos datos y registra con multisig las altas, rotaciones y suspensiones, dejando auditoría pública. Con ese manifiesto, cualquier verificador sabe qué claves usar, dónde consultar la StatusList del emisor (estado de vigencia de credenciales) y qué endpoints (iden3comm) invocar. El flujo es: extraer el DID del emisor desde la VC luego leer en el contrato el CID , recuperar y validar el manifiesto

con la firma del DID, verificar la firma de la VC, consultar la StatusList indicada por el statusPointer. Así se obtiene garantías criptográficas sin ver datos personales ni la VC completa.

10. Diseño de la Billetera IDS

- **Funciones clave.** WIRA Wallet genera el DID y claves localmente, custodia las VCs en un bundle cifrado, emite Presentaciones Verificables (VP) con divulgación mínima, firma operaciones on-chain vía Account Abstraction, y respalda/recupera mediante SSS (Carnet+PIN y/o Guardianes). Incluye historial local (visible solo por el usuario) con fecha, destino y alcance de cada presentación.
- **Seguridad y custodia.** El bundle se cifra (AES-GCM) con una DEK protegida por una clave derivada del PIN y del almacén seguro del dispositivo. El bundle se desbloquea sólo durante una acción y la clave se borra inmediatamente de memoria. Las firmas ocurren siempre en el dispositivo. La recuperación exige umbral de shares; ningún actor puede restaurar por sí solo.
- **Accesibilidad.** Modo fuera de línea, códigos QR estáticos y dinámicos para portales de verificación, soporte multilingüe en castellano e inglés.
- **Compatibilidad.** Android e IOS, SDK para terceros, Iden3comm para presentaciones donde sea requerido.

Apéndice A. FODA (Bolivia)

Fortalezas

- Existe un marco legal en Bolivia sobre la **firma digital**, validez jurídica de documentos electrónicos y protección de datos.
- El sistema está diseñado para proteger los datos de las personas y empoderarlas sobre qué compartir.
- Ecosistema local de fintech y comunidades blockchain activas.

Oportunidades

- Se puede proponer a gobiernos locales o instituciones, aunque no sabemos la demanda y qué nichos específicos lo demandarían.
- Certificación y trazabilidad en **agro/ganadería/minería** para exportación.
- Alineación con estándares regionales (MERCOSUR) en **protección de datos**.
- Es un mecanismo para ligar billeteras cripto a la identidad de una persona, y que estas recuperen esta billetera muy ligada a su identidad, y sin la necesidad de claves y pruebas muy complicadas, usando account abstraction.
- La debilidad institucional en Bolivia puede crear una demanda por soluciones descentralizadas si las personas finalmente entienden el concepto de blockchain.
- Desconfianza ciudadana en el intercambio de datos entre instituciones, pero si entienden el concepto, podría ser una forma de concerlos.

Debilidades

- No estamos seguros a quién le interesa proteger sus datos, no sabemos el alcance y demanda de una solución que proteja los datos de los usuarios.
- Brecha de **conectividad** y alfabetización digital en diferentes estratos de la población, es necesaria una herramienta que les facilite el entendimiento.
- Desconfianza ciudadana en el intercambio de datos entre instituciones.

Amenazas

- Cambios regulatorios y **polarización política** que retrasen adopción.
- **Ciberataques** y fraudes de identidad más sofisticados.
- Riesgo de **vigilancia excesiva** si se rompe el principio de privacidad.

- Fragmentación de estándares (muchos sistemas con identidades) si cada actor crea soluciones cerradas.

Apéndice B. Business Model Canvas

1. Segmentos de mercado

La aplicación de identidad digital o su sistema es un producto a vender para

- Gobiernos locales, regionales
- Incluso instituciones que quieran incluir características propias avanzadas.

El uso de nuestra identidad digital como diferenciador o herramienta, tendría a clientes como:

- ONGs o instituciones que quieren pagar directamente a beneficiarios, por sistema de trazabilidad o certificación por ejemplo.

2. Propuesta de valor principal

Billetera cripto relacionada a una identidad digital, con la capacidad de que el usuario firme contratos inteligentes, desarrolle reputación y reciba fondos directamente dirigidos a su identidad.

3. Canal

El canal para distribuir la aplicación de identidad digital son las tiendas de android y apple.

4. Relación con el cliente

La forma de comunicarnos con nuestros clientes son:

- Comunicación desde Linkedin, a perfiles escogidos
- Comunicación tradicional con sindicatos de quinua, líderes de empresas y similares.
- Publicidad digital, tiktok dirigidas a políticos, candidatos de municipios, etc.

La comunicación, al tratarse de negocios B2B, deberá ser personalizada, muchas reuniones virtuales o presenciales con gerencia o similares.

5. Fuentes de ingresos.

Las fuentes de ingresos para el proyecto de identidad y oráculos se relacionan mucho, serían:

- Venta o alquiler de sistemas gubernamentales
- Venta o alquiler de sistemas de trazabilidad.

- Plataforma de tokenización y cobro por membresía de listar criptos, sistemas de control de información, cumplimiento, etc
- Venta o alquiler de sistemas personalizados ligados a nuestra identidad digital.

6. Actividades clave

1. Identificar los nichos de mercado que requieren por necesidad latente la identidad digital y sus beneficios, además están dispuestos a pagarla o implementarla sin que incluso sea una herramienta oficial.
2. Implementar el sistema en modalidad piloto, en estas instituciones, hasta lograr la plena satisfacción del cliente, de manera que pueda volver a utilizarse o hacer algo similar en otros casos de uso
3. Publicitar el servicio.

7. Recursos clave

1. Patente sobre la propiedad intelectual de nuestro sistema, adecuado sin embargo a las licencias de software
2. Un sistema coherente y seguro con la firma blockchain, identidad digital y pruebas ZK
3. Financiamiento y equipo para maximizar la posibilidad de encontrar nichos de mercado y trabajar con ellos, con poco financiamiento hasta lograr un sistema mínimo pero que crea suficiente valor para después publicitarlo.

8. Socios clave

- Líderes de empresas que estén dispuestos a implementar sistemas innovadores con la inversión, desafíos y problemas que implica, pero con la visión de lograr características diferenciadoras reales para sus empresas.
- Early adopters de sistemas, inversores o clientes de productos de trazabilidad, que conocen de la tecnología y valoren los productos apoyados por la tecnología.
- Políticos que quieran implementar la tecnología como herramienta política y que después estén dispuestos a dar la financiación y seguimiento necesario.
- Socios vendedores, que ayuden a crear estrategias de negocios, cerrar ventas con proyectos e instituciones

9. Estructura de coste

- Costo de servidores, mantenimiento y mejora de los sistemas.
- Costos legales, adecuar leyes municipales, el lobby para lograr estas cosas.

- Los costos de tiempo y dinero para implementar los sistemas y adecuarlos para que los usuarios los adopten más fácilmente
- Costos de socios que ayuden a cerrar estos negocios

Apéndice C. Referencias y cumplimiento (síntesis práctica)

- **Firma Digital y validez probatoria**: Ley 164 y su reglamento; reconocimiento de la **ATT** como Entidad Certificadora Raíz; convivencia con ECP privadas y públicas.
- **Identificación oficial**: Ley 145 (SEGIP/SEGELIC); Reglamento del **RUI**; prácticas para credenciales derivadas sin sustituir CI.
- **Interoperabilidad**: Decreto Supremo 3525 y lineamientos para publicar/consumir servicios; mecanismos de trazabilidad.
- **Protección de Datos**: Anteproyectos/PL en discusión; recomendaciones para adecuación inmediata (consentimiento, minimización, PIAs).
- **Estándares**: W3C DID/VC, StatusList 2021, SD-JWT-VC,.

Apéndice D. Glosario

- **VC (Verifiable Credential)**: afirmación firmada por un emisor que puede ser verificada criptográficamente.
- **DID (Decentralized Identifier):** identificador criptográfico verificable y resoluble sin autoridad central única.
- **VP (Verifiable Presentation)**: conjunto de credenciales/pruebas presentado por el titular a un verificador.
- **BBS+ / CL / SD-JWT**: esquemas criptográficos para selective disclosure y/o ZKP aplicables a VC.
- **BJJ:** curva usada en ciertas pruebas ZK (p. ej., rangos/miembresía).
- **Smart Account (ERC-4337):** cuenta contrato que firma UserOperations vía EntryPoint; puede usar Paymasters para cubrir gas según políticas.
- **CID (Content Identifier):** identificador inmutable de un contenido en **IPFS**; asegurar que lo recuperado es exactamente lo publicado.
- **Registro de Confianza**: catálogo de emisores y verificadores acreditados, con metadatos públicos de políticas y DIDs.
- **DEK:** *Data Encryption Key*, clave aleatoria usada para cifrar el bundle en el dispositivo con **AES-256-GCM**.
- **Keystore/Keychain:** almacén seguro del SO (Android/iOS) que protege claves y material criptográfico; se usa para derivar/guardar la KEK que envuelve la DEK con la que se cifra el almacenamiento de la app.
- **KEK:** *Key Encryption Key*, clave derivada de **PIN + hardware seguro** (Keystore/Secure Enclave) con **Argon2id** para envolver la **DEK**.
- **Status List:** estructura compacta firmada por el **Issuer** que indica la vigencia de las VCs sin revelar su contenido.
- **iden3comm**: protocolo de mensajería del ecosistema iden3/Polygon ID para flujos de emisión y verificación de credenciales. Cifrado punto a punto y autenticación entre emisor, titular y verificador.
- **statusPointer**: puntero dentro de una VC que indica **dónde** está la StatusList pública del emisor (URL/CID/DID-URL) y **qué índice** consultar para conocer si la credencial está vigente, suspendida o revocada.
- **privkey**: clave privada del titular usada para firmar **UserOperations** (ERC-4337) desde la wallet; se genera y permanece en el dispositivo, dentro del bundle cifrado.
- **ERC-4337, EntryPoint, UserOperation, Paymaster:** componentes de **Account Abstraction** para firmar y pagar gas sin EOA.

- **Guardianes:** actores o factores que, bajo política umbral, ayudan a recuperar la DEK (no acceden a VCs).
- **Gestión de estado**. Cada VC incluye un puntero status a una lista pública firmada por el emisor.
- **Bitstring**: arreglo de bits donde el índice asignado a la VC indica su estado (0 vigente, 1 no vigente). Revocar es cambiar el bit y republicar la lista firmada o su CID en IPFS/Ceramic.
- **Merkle map**: mapa clave-valor hash(credentialId) → estado con raíz Merkle firmada; la verificación usa pruebas de pertenencia sin descargar toda la lista.
- **ZKP (Zero-Knowledge Proof):** prueba que acredita una condición (p. ej., “mayor de 18”) sin revelar el dato subyacente.