UNIVERSIDAD DE LA REPÚBLICA DEL URUGUAY

MASTER THESIS

Digital Academic Certification with Blockchain: A Secure and Privacy-Preserving Prototype Using Hyperledger Fabric

---

Author:
Ing. Pablo BLANCO

Supervisors:
Dr. Gustavo BETARTE
Dr. Carlos LUNA

A thesis submitted in fulfillment of the requirements for the degree of Maestría en Seguridad Informática

11 de junio de 2025

Declaration of Authorship

I, Ing. Pablo BLANCO, declare that this thesis titled, «Digital Academic Certification with Blockchain: A Secure and Privacy-Preserving Prototype Using Hyperledger Fabric» and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

UNIVERSIDAD DE LA REPÚBLICA DEL URUGUAY

Resumen

Facultad de Ingeniería
Instituto de Computación

Maestría en Seguridad Informática

Digital Academic Certification with Blockchain: A Secure and Privacy-Preserving Prototype Using Hyperledger Fabric

by Ing. Pablo BLANCO

The rapid digital transformation of modern societies has opened new avenues for ensuring the authenticity and security of academic credentials. Blockchain technology, known for its decentralized and immutable nature, offers a promising solution for the digital certification of academic records. This thesis explores the development and implementation of a prototype system for managing digital academic certificates using Hyperledger Fabric, a permissioned blockchain framework, with a particular focus on compliance with GDPR and Uruguay's Law 18.331 on personal data protection.

The primary objective of this work was to design and implement a secure, scalable, and privacy-compliant solution that enables institutions to issue, manage, and verify academic certificates on a blockchain. Through an analysis of existing blockchain platforms such as Hyperledger Besu and Ethereum, Hyperledger Fabric was chosen due to its robust privacy features, granular control of permissions, and flexibility in handling data. The prototype was deployed within a private consortium of academic institutions, enabling the issuance of certificates with cryptographic guarantees of integrity and authenticity while protecting the personal data of students.

The results of this work show that blockchain can effectively address issues such as certificate fraud and inefficiencies in verification processes. However, challenges such as scalability, compliance with the right to be forgotten, and off-chain data management are discussed. The proposed solution lays the groundwork for future developments in digital academic credentialing and highlights key areas where improvements can be made to ensure widespread adoption.

Keywords: Blockchain, GDPR, Digital Certificates, Hyperledger Fabric, Data Privacy

UNIVERSIDAD DE LA REPÚBLICA DEL URUGUAY

Resumen

Facultad de Ingeniería
Instituto de Computación

Maestría en Seguridad Informática

**Certificación académica digital con Blockchain:
Un prototipo orientado a la seguridad y privacidad con Hyperledger Fabric**

por Ing. Pablo BLANCO

La rápida transformación digital de las sociedades modernas ha abierto nuevas posibilidades para garantizar la autenticidad y seguridad de los certificados académicos. La tecnología blockchain, reconocida por su naturaleza descentralizada e inmutable, ofrece una solución prometedora para la certificación digital de títulos académicos. Esta tesis explora el desarrollo e implementación de un sistema prototipo para la gestión de certificados académicos digitales utilizando Hyperledger Fabric, una red blockchain permisionada, con especial énfasis en el cumplimiento de las normativas de protección de datos, como el GDPR y la Ley 18.331 de Uruguay.

El objetivo principal de este trabajo fue diseñar e implementar una solución segura, escalable y que respete la privacidad, permitiendo a las instituciones emitir, gestionar y verificar certificados académicos sobre una blockchain. Tras un análisis de las plataformas blockchain existentes, como Hyperledger Besu y Ethereum, se eligió Hyperledger Fabric debido a sus sólidas características de privacidad, control granular de permisos y flexibilidad en el manejo de datos. El prototipo se desplegó dentro de un consorcio privado de instituciones académicas, lo que permitió la emisión de certificados con garantías criptográficas de integridad y autenticidad, protegiendo al mismo tiempo los datos personales de los estudiantes.

Los resultados de este trabajo muestran que blockchain puede abordar de manera efectiva problemas como el fraude de certificados y las ineficiencias en los procesos de verificación. No obstante, se discuten desafíos como la escalabilidad, el cumplimiento del derecho al olvido y la gestión de datos fuera de la cadena (off-chain). La solución propuesta sienta las bases para futuros desarrollos en la certificación académica digital y destaca áreas clave donde se pueden realizar mejoras para garantizar una adopción generalizada.

Acknowledgements

I would like to thank the following people who have helped me with this research project: COMPLETAR

Índice general

Índice de figuras

Índice de cuadros

Capítulo 1

Introducción

La era digital ha traído consigo una serie de avances tecnológicos que han revolucionado la forma en que las sociedades funcionan y se organizan. Uno de estos avances es la tecnología blockchain, que promete transformar no solo el sector financiero, sino también áreas como la administración pública, la salud, el entretenimiento y la educación. En este contexto, la validación de certificados digitales mediante blockchain emerge como una solución potencialmente eficaz para garantizar la autenticidad, integridad y seguridad de los documentos digitales.

1.1. Contexto y motivación

Siendo Uruguay un país que busca constantemente modernizar sus sistemas y procesos, actualmente enfrenta el desafío de adaptar y adoptar estas nuevas tecnologías de manera que se alineen con sus regulaciones y necesidades específicas. En particular, el Servicio Central de Informática de la Universidad de la República (SECIU-Udelar), como entidad encargada de la gestión de la seguridad informática en la Universidad de la República, tiene un interés especial en explorar soluciones que puedan mejorar la confiabilidad y seguridad de los certificados digitales que emite o valida.

La justificación de este trabajo radica en la necesidad de comprender a fondo las diferentes propuestas blockchain existentes para la validación de certificados digitales y determinar cuál de ellas podría ser más adecuada para el contexto uruguayo y, específicamente, para SECIU-Udelar. Además, considerando las regulaciones existentes en Uruguay sobre el manejo de datos personales, es esencial que cualquier solución propuesta esté en consonancia con estas normativas.

1.2. Objetivos de la tesis

Con este propósito, este trabajo tiene como objetivo general analizar diversas propuestas blockchain, incluyendo el Brazilian RAP System [Cos+18], con el fin de definir una implementación adecuada para Uruguay y SECIU-Udelar. A través de este estudio, se busca no solo ofrecer una visión teórica y comparativa de las diferentes soluciones, sino también proporcionar un prototipo práctico que sirva como punto de partida para futuras implementaciones.

Los objetivos específicos derivados de este objetivo general son:

1. Realizar una revisión exhaustiva de la literatura sobre la tecnología blockchain y su aplicación en la validación de certificados digitales.

2. Analizar en detalle el Brazilian RAP System y otras propuestas relacionadas, tanto regionales como internacionales.

3. Estudiar las regulaciones uruguayas relacionadas con el manejo de datos personales y su impacto en la implementación de soluciones en el dominio considerado.
4. Diseñar e implementar un prototipo basado en la solución propuesta en el trabajo realizado previamente [Mol21a], considerando componentes relevantes del sistema.

Con estos objetivos en mente, el presente trabajo se estructura en diferentes secciones que abordan desde la revisión teórica hasta la propuesta práctica, ofreciendo así una visión integral sobre la validación de certificados digitales mediante blockchain en el contexto uruguayo.

1.3. Estructura del informe

1.3 Estructura del informe

El presente informe se organiza en seis capítulos principales y anexos, estructurados para guiar al lector desde los aspectos teóricos y normativos hasta la implementación práctica y los resultados del prototipo desarrollado. A continuación, se describe brevemente el contenido de cada capítulo:

- **Capítulo 1: Introducción**
  Presenta el contexto y la motivación del trabajo, los objetivos generales y específicos, y una visión general de la estructura del documento.
- **Capítulo 2: Estado del arte**
  Proporciona una revisión teórica sobre blockchain, incluyendo sus principios, gobernanza y aplicaciones en diversos sectores. Se analizan casos de uso relevantes en Brasil y Argentina, comparando sus soluciones para la validación de certificados digitales.
- **Capítulo 3: Evaluación de tecnologías blockchain**
  Examina el marco regulatorio aplicable (GDPR, Ley 18.331), define criterios de evaluación tecnológica (seguridad y privacidad) y compara diferentes plataformas blockchain (Hyperledger Fabric, Hyperledger Besu, Ethereum, Corda, Quorum), justificando la selección de Hyperledger Fabric para este trabajo.
- **Capítulo 4: Implementación del prototipo**
  Describe el diseño e implementación del prototipo desarrollado, incluyendo su arquitectura, actores, componentes del sistema, requerimientos funcionales y no funcionales, así como el despliegue de la blockchain en modo de prueba.
- **Capítulo 5: Resultados y análisis**
  Presenta la metodología de evaluación utilizada, las pruebas realizadas, los resultados obtenidos y la visión del trabajo sobre las ventajas, limitaciones y desafíos del sistema propuesto.
- **Capítulo 6: Conclusiones y trabajos futuros**
  Resume las principales conclusiones alcanzadas, ofrece recomendaciones para futuras líneas de trabajo, e identifica posibles aplicaciones del prototipo en el contexto académico nacional.
- **Anexos**
  Incluyen material complementario como el código fuente y la documentación técnica sobre el proptotipo.

Capítulo 2

Estado del arte

En esta sección se realiza un análisis de las soluciones existentes para la validación de certificados digitales, revisando casos de estudio relevantes como el sistema "Diploma Digital"de Brasil y la Blockchain Federal Argentina (BFA). Estos ejemplos ilustran cómo la tecnología blockchain se ha implementado en el ámbito educativo para garantizar la autenticidad y trazabilidad de los documentos académicos, abordando problemáticas de seguridad y eficiencia. Por último, se comparan estas soluciones considerando aspectos como la gobernanza, la privacidad, y el cumplimiento de regulaciones internacionales como el GDPR [Uni16], evaluando los desafíos y las oportunidades que presenta el uso de blockchain en este contexto.

2.1. Tecnología blockchain

La tecnología blockchain ha capturado la atención de la comunidad académica y de la industria en la última década, siendo objeto de numerosos estudios y análisis. Esta revisión de literatura tiene como objetivo proporcionar un panorama general sobre la evolución de la tecnología blockchain, su aplicación en la validación de certificados digitales, los beneficios y desafíos asociados.

La idea central detrás de blockchain se remonta a los trabajos de Haber y Stornetta en 1991, quienes propusieron un sistema criptográficamente seguro para registrar documentos digitales de manera que no pudieran ser alterados posteriormente [HS91]. Sin embargo, fue con la aparición de Bitcoin en 2008, propuesto por una entidad bajo el pseudónimo de *Satoshi Nakamoto*, que la tecnología blockchain ganó una mayor relevancia [Nak08].

2.1.1. Principios y funcionamiento

Blockchain es una tecnología de registro distribuido que permite la creación de un libro de contabilidad inmutable y transparente conocido como ledger, compartido entre múltiples partes sin la necesidad de una autoridad central. Los principios fundamentales de blockchain se basan en la criptografía, la descentralización y el consenso. En un sistema blockchain, las transacciones son agrupadas en bloques, que luego son encadenados de manera secuencial y cronológica utilizando algoritmos criptográficos. Cada bloque contiene un conjunto de transacciones y un hash criptográfico que referencia al bloque anterior, creando una cadena continua e inalterable de datos [Nak08].

El funcionamiento de una blockchain se alcanza a través de una red de nodos que participan en el proceso de validación y consenso. Cuando una transacción es iniciada, se transmite a todos los nodos de la red. Cada nodo verifica la validez de la transacción utilizando algoritmos de consenso como Prueba de Trabajo (*Proof of Work*) o Prueba de Participación (*Proof of Stake*) [Swa15]. Una vez que un bloque es validado, se añade a la cadena de bloques y es visible para todos los participantes de la red, al proceso

descrito anteriormente se le conoce como "minar"la red. Esta estructura descentralizada asegura que los datos almacenados en la blockchain sean resistentes a manipulaciones y accesibles de manera transparente, permitiendo aplicaciones seguras y confiables en diversas industrias, incluyendo la validación de certificados digitales, el seguimiento de cadenas de suministro, y las transacciones financieras [TT16].

2.1.2. Contratos inteligentes

El término contrato inteligente (*smart contract*) fue introducido por Nick Szabo en 1994, definiéndolo como "un protocolo transaccional computarizado que ejecuta los términos de un contrato" [Sza94]. Estos contratos son programas informáticos que se ejecutan automáticamente cuando se cumplen condiciones predefinidas, permitiendo la realización de transacciones confiables sin intermediarios.

Con la aparición de plataformas como Ethereum en 2015 [Fou23c], los contratos inteligentes encontraron un entorno adecuado para su implementación práctica. Ethereum facilita la creación y ejecución de contratos inteligentes mediante su máquina virtual descentralizada [But14]. Estos contratos se almacenan en la cadena de bloques y se ejecutan de forma autónoma, garantizando transparencia y seguridad en las transacciones.

Los contratos inteligentes tienen aplicaciones en diversos sectores, siendo capaces de resolver lógica de negocio mediante la ejecución de código. En el contexto de esta tesis, veremos como se utilizan para automatizar la emisión y verificación de certificados académicos digitales, asegurando su autenticidad y reduciendo la dependencia de intermediarios.

2.1.3. Gobernanza de la Blockchain

La gobernanza de una red describe diversas metodologías aplicadas al acceso de la información, la privacidad de los datos y las capacidades que cada participante dentro de la red tiene con respecto a la misma. Para el caso de uso de este trabajo, las redes completamente públicas o privadas (*permisionadas*) no son de interés, dado que carecen de los mecanismos mínimos relacionados a privacidad y transparencia. Por otro lado, analizamos algunos tipos de blockchains que si aplican un modelo de gobernanza que podría ser de utilidad.

2.1.4. Tipos de redes blockchain

Consortium Blockchain

Las blockchains de consorcio (*federadas*) son redes semi-privadas que buscan solucionar el problema de acceso y autenticidad de la información mediante el acceso restringido a la misma. La principal diferencia con las blockchains públicas es que solo acceden participantes preautorizados, generalmente entidades catalogadas como de confianza, como organismos gubernamentales, entidades reguladoras o instituciones educativas, entre otras [BVE20]. Por otro lado, las blockchains de consorcio, a diferencia de las blockchains privadas, son gobernadas por un grupo de participantes y el control de la red no es exclusivo como ocurre en estas últimas [XWS19]. Algunos ejemplos de este tipo de redes son R3 Corda e Hyperledger Fabric [R321; Hyp21b].

Hybrid Blockchain

Las blockchains híbridas funcionan con un enfoque mixto donde se utilizan una red pública y una privada. Desde el punto de vista técnico, funcionan creando referencias de los bloques de la red privada (*hashes*), que son grabados en la red pública con el fin de ofrecer un registro transparente y auditable de todas las transacciones realizadas sin comprometer la privacidad de los datos en la red pública [ZQH20].

Este tipo de blockchains se utiliza cuando existen requerimientos de transparencia, seguridad y privacidad de la información. Un caso de uso podría ser aplicaciones gubernamentales donde se necesita un mayor nivel de confidencialidad de los datos, pero también se desea mantener algunas características de una blockchain pública, como la inmutabilidad y la transparencia en la auditoría de las transacciones. Algunos ejemplos de este tipo de redes son HyperLedger Besu y XDC [Hyp21a; Net21]. La siguiente tabla 2.1 ilustra los distintos tipos de redes y sus principales características.

	Consorcio	**Privada**	**Pública**	**Híbrida**
Acceso	Acceso controlado y seguro para entidades de confianza	Acceso completamente controlado por una única entidad	Acceso abierto, con total transparencia y sin permisos	Combinación de acceso controlado y sin permisos en algunas partes
Características	Gobernanza distribuida, limitada transparencia pública	Sin transparencia pública, gobernada por una entidad única	Transparencia completa y auditoría abierta	Transparencia controlada con opciones de privacidad
Costo Transaccional	Moderado, debido a participantes confiables y menores validaciones	Bajo, dado el control centralizado y menor infraestructura de consenso	Alto, por el consenso entre nodos distribuidos y mayor complejidad	Moderado, debido a una combinación de validaciones públicas y privadas

CUADRO 2.1: Comparativa de diferentes tipos de blockchain

Tanto las redes privadas, consortium e híbridas son topologías generalmente utilizadas en las implementaciones de las soluciones existentes, que se consideran más adelante.

2.1.5. Aplicaciones en diferentes sectores

Blockchain ha encontrado un uso significativo en una amplia gama de sectores, ofreciendo soluciones innovadoras a problemas tradicionales relacionados con la confianza, la transparencia, la seguridad y la privacidad. A continuación, se destacan algunos de los sectores más relevantes:

1. Finanzas y banca: el sector financiero ha sido uno de los principales pioneros en la adopción de la tecnología, gracias a su capacidad para optimizar procesos, reducir costos y aumentar la seguridad en las transacciones. Las tecnologías como R3 Corda, enfocadas en consorcios, permiten a los bancos compartir datos entre instituciones de

forma segura y eficiente, manteniendo la privacidad y el cumplimiento normativo. Las soluciones blockchain permiten liquidaciones más rápidas en transacciones transfronterizas y una reducción significativa del fraude mediante smart-contracts que automatizan operaciones financieras y procedimientos manuales.

2. Cadenas de suministro y logística: blockchain se utiliza ampliamente en la gestión de cadenas de suministro, donde la transparencia y la trazabilidad son factores importantes. Plataformas como IBM Food Trust utilizan Hyperledger Fabric para registrar cada etapa del ciclo de vida de los productos, permitiendo que las empresas rastreen y verifiquen la autenticidad de los bienes en tiempo real. Esto es especialmente útil en industrias como la alimentaria y la farmacéutica, donde la seguridad y el cumplimiento de normas sanitarias y de calidad son esenciales. Además, reduce la burocracia y los costos asociados a la documentación física.

3. Salud: en el sector de la salud, las redes blockchain permiten almacenar y compartir de manera segura datos médicos considerados sensibles, como las historias clínicas electrónicas, asegurando la privacidad de los pacientes. La implementación de consortium blockchains permite que solo instituciones autorizadas, como hospitales y centros de investigación, tengan acceso a los datos. Esto asegura la integridad y autenticidad de la información médica, facilitando la colaboración entre instituciones, reduciendo el riesgo de errores y garantizando que los datos estén protegidos según normativas como el GDPR y HIPAA [U.S96].

4. Gobierno: en el ámbito gubernamental, las blockchains híbridas juegan un papel clave en la creación de soluciones que requieren tanto transparencia como privacidad. Los gobiernos están utilizando la tecnología para la emisión de identificaciones digitales, certificados de nacimiento y la votación electrónica, asegurando que los registros sean inmutables y auditables, pero sin comprometer datos personales y el anonimato de ciertos procesos. Esto mejora la eficiencia de los procesos gubernamentales y fomenta la confianza de los ciudadanos en la administración pública.

5. Energía: el sector energético está explorando soluciones blockchain para facilitar el comercio de energía entre pares (P2P). Las redes de consorcio permiten a los productores y consumidores de energía solar, por ejemplo, registrar la producción y el consumo en una blockchain, lo que facilita la compraventa directa sin intermediarios. Esto no solo optimiza la eficiencia del sistema, sino que también promueve la generación y el uso de energías renovables de manera más eficiente y transparente.

6. Educación: el sector educativo también ha comenzado a beneficiarse del uso de blockchain, especialmente en la emisión y validación de certificados académicos. Las instituciones pueden emitir títulos y diplomas como registros inmutables en una blockchain, permitiendo que los empleadores y otras instituciones verifiquen fácilmente su autenticidad. Este tipo de aplicaciones permiten un acceso controlado a terceros para la verificación de las credenciales académicas, cumpliendo con los requisitos de privacidad de los usuarios y asegurando la transparencia en el proceso.

2.2. Soluciones existentes para validación de certificados digitales

La aplicación de blockchain en la validación de certificados ha sido explorada en diversos trabajos académicos. Por ejemplo, Grech y Camilleri discuten cómo blockchain puede ser utilizado en el ámbito educativo para la verificación de credenciales y certificados, proporcionando transparencia y reduciendo el fraude [GC17]. Otro estudio realizado por Turkanović presenta un sistema llamado EduCTX basado en blockchain para

la emisión y verificación de registros académicos [Tur+18]. Ambos documentos destacan el potencial de la tecnología blockchain en educación, enfocándose en la emisión y verificación de credenciales académicas. El informe de la Comisión Europea subraya cómo blockchain puede mejorar la confianza y el control sobre los datos personales de los estudiantes, permitiendo la verificación directa de certificados sin intermediarios, y aportando transparencia, inmutabilidad y soberanía de datos. Por su parte, el artículo sobre EduCTX propone una plataforma basada en blockchain para gestionar créditos académicos de forma descentralizada y confiable, compatible con el sistema ECTS (European Credit Transfer and Accumulation System), facilitando así la movilidad académica y laboral a nivel global. Ambas fuentes coinciden en que la tecnología blockchain puede reducir costos, simplificar procesos administrativos y brindar una solución segura y transparente para la gestión de registros educativos.

Las ventajas de utilizar blockchain en la validación de certificados incluyen la inmutabilidad, la transparencia y la descentralización, como señala Swan [Swa15] describiendo una progresión en la evolución de la tecnología blockchain, pasando de aplicaciones financieras básicas (blockchain 1.0) a sistemas más complejos de contratos inteligentes (blockchain 2.0) y, finalmente, a aplicaciones que impactan áreas no financieras como la educación, salud y gobernanza (blockchain 3.0). Esta estructura permite visualizar cómo la tecnología ha expandido su alcance inicial, evolucionando para ofrecer soluciones en ámbitos que requieren transparencia, seguridad y autonomía en la gestión de datos.

Tapscott y Tapscott [TT16] por su parte, destacan cómo blockchain facilita la descentralización de transacciones y registros, eliminando la necesidad de intermediarios y permitiendo un nivel de transparencia sin precedentes. La capacidad de blockchain para gestionar la propiedad de datos y proteger la privacidad se considera clave para su aplicación en industrias como finanzas y gobierno. Esta tecnología permite una inclusión financiera más amplia, ya que personas sin acceso a servicios financieros convencionales podrían utilizar blockchain para participar en la economía digital.

Sin embargo, también existen desafíos, como la escalabilidad, la interoperabilidad y las preocupaciones de privacidad, discutidos en profundidad por Zohar [Zoh15] que complementa estas ideas al explicar la arquitectura de Bitcoin y cómo sus propiedades descentralizadas y criptográficas hacen posible una moneda digital resistente a la censura. Este enfoque técnico subraya la importancia de la criptografía y el consenso distribuido en blockchain, lo cual asegura que los registros sean inmutables y las transacciones, verificables sin intervención de terceros. Aunque Zohar se centra en Bitcoin, sus observaciones aplican a muchas implementaciones blockchain y destacan tanto la escalabilidad como el impacto potencial de la tecnología en el sistema financiero tradicional.

Diversas instituciones y organizaciones han explorado la implementación de blockchain para la validación de certificados académicos. Por ejemplo, el MIT Media Lab desarrolló un sistema para emitir certificados digitales utilizando blockchain [SS19]. Además, la Universidad de Nicosia en Chipre fue una de las primeras en emitir títulos académicos verificables mediante blockchain [Nic17].

2.2.1. Casos de estudio y ejemplos relevantes

RAP - El Caso de Brasil

En el paper [Cos+18] se presentó el diseño preliminar de un proyecto que inicialmente se denominó RAP, una plataforma pública descentralizada para la emisión, preservación y verificación de certificados digitales que permite el uso a instituciones públicas y privadas. Este enfoque planteaba usar blockchain en conjunto con una base de datos (repositorio de preservación digital a largo plazo) para el almacenamiento de información sensible y su preservación a largo plazo. RAP expondría una API a las instituciones educativas para la generación, tratamiento y preservación de los certificados y, por otro lado, un portal web para poder verificar la autenticidad de un documento dado un número de registro. La API (RAP Server) estaría compuesta por tres módulos principales: módulo de autenticación, módulo de registro y módulo de preservación. El sistema planeaba ser compatible con varias redes blockchain (Bitcoin y Ethereum), permitiendo a las instituciones optar por una o varias redes donde guardar los datos; el componente encargado de esa generalización es el denominado DLT Broker.

RAP fue el proyecto inicial de lo que hoy en día se conoce en Brasil como "Diploma Digital". Desde finales de 2021, el sistema se encuentra implementado y en uso en el país con algunas variantes respecto a la idea inicial en cuanto a la arquitectura del sistema y la topología de la red blockchain utilizada. De acuerdo a la regulación de este país, todas las instituciones (69 universidades y 41 instituciones de Educación Profesional y Tecnológica) están obligadas por ley a emitir diplomas digitales en la blockchain mediante el uso de la plataforma "Diploma Digital", implementada por la Rede Nacional de Ensino e Pesquisa (RNP)[PR21], que utiliza la blockchain Rede Blockchain Brasil (RBB).

RBB es una iniciativa impulsada por el Banco Nacional de Desarrollo Económico y Social (BNDES)[SB21] y el Tribunal Federal de Cuentas (TCU). Esta red es del tipo híbrida 2.1.4 y sigue el patrón de LACChain (Latin America y Caribe Blockchain). Ambos proyectos se basan en la misma topología y protocolos que Ethereum y utilizan Hyperledger Besu [Hyp21a], que permite ejecutar transacciones en redes públicas y privadas.

En la blockchain utilizada en el proyecto "Diploma Digital", los nodos participantes están previamente autorizados y verificados por la entidad gestora de la red, en este caso, el Ministerio de Educación de Brasil.

El uso de una blockchain híbrida en el proyecto "Diploma Digital"de Brasil se basa en la necesidad de garantizar la seguridad, privacidad y confiabilidad de los diplomas digitales emitidos, así como cumplir con las regulaciones y requisitos gubernamentales en el ámbito educativo. Al utilizar este tipo de blockchain, se busca asegurar que solo las instituciones educativas autorizadas puedan emitir diplomas digitales, y que los diplomas emitidos sean verificables y no puedan ser falsificados o alterados.

Además del esfuerzo tecnológico para proveer una plataforma de este porte, varios actores han jugado un papel importante en la transformación de un proceso como un bloque: legislación acorde a lo que se quería implementar, instituciones públicas y privadas haciendo uso de la plataforma y apoyo ministerial son algunos de estos componentes. En el caso de Brasil, además de la notoria innovación tecnológica aplicada al proceso de certificados digitales, cabe destacar que todo el impulso en este movimiento tuvo el objetivo de resolver un problema que venía en amplio crecimiento en este país y que es la falsificación de certificados en papel.

BFA - El caso de Argentina

El proyecto Blockchain Federal Argentina (BFA) [Arg21a] es desarrollado en conjunto por NIC Argentina, la Cámara Argentina de Internet — CABASE y la Asociación de Redes de Interconexión Universitaria (ARIU). La conjunción de estas tres entidades permite la participación del sector privado (CABASE), el sector público (NIC.ar, dependiente de la Secretaría Legal y Técnica de la Presidencia de la Nación), el sector académico (representado por ARIU y una gran red de universidades), la sociedad civil y la comunidad técnica. BFA busca utilizar la tecnología blockchain para la emisión y verificación de diplomas digitales en el país, entre otros usos, y cabe destacar esto último, dado que BFA es una blockchain multi-propósito donde distintos actores públicos y privados, y de variados rubros, pueden hacer uso de la blockchain. En cuanto a su tipo, BFA funciona como una red semi-privada donde el ingreso de cada nodo a la red es aprovado previamente.

Existen varias instituciones [Arg21b] públicas y privadas haciendo actualmente uso de BFA para el manejo de certificados digitales. Algunas de estas son la Universidad de Córdoba, Universidad de La Plata, Universidad de San Juan y la Universidad de Palermo, entre otras.

En Argentina, las instituciones educativas hacen uso de SIU-Guaraní [IUS21] como sistema informático de gestión académica, un sistema similar al de Bedelías en Uruguay. SIU-Guaraní es un sistema desarrollado por Sistema de Información Universitaria (SIU), un organismo que desarrolla distintos sistemas de gestión dirigidos a las universidades nacionales, y que depende del Consejo Interuniversitario Nacional (CIN).

A diferencia de Brasil, donde "Diploma Digital" fue implementado como un único concepto respaldado por una serie de normativas y leyes, en el enfoque argentino, cada una de las instituciones dispone de la BFA para realizar sus propias implementaciones para la emisión y verificación de certificados digitales en la blockchain.

Desde el punto de vista técnico, BFA está basada en la red Ethereum [Fou23c], implementando una blockchain híbrida, sin criptomoneda ni costo asociado a las transacciones. A diferencia de las blockchains donde el mecanismo de consenso es el PoW (*Proof of Work*) [Fou23a] y muchos nodos compiten para minar un bloque, en el caso de BFA el consenso se realiza mediante el PoA (*Proof of Authority*) [Ope23]. El hecho de que BFA utilice este mecanismo de consenso trae asociadas algunas características y ventajas, siendo estas:

- **Modelo más liviano:** Al no existir el concepto de minería basada en PoW, la capacidad de cómputo requerida para crear un bloque de información es menor.
- **Red híbrida:** Solo algunos nodos previamente autorizados tienen capacidad de escritura en la red, todos los nodos pueden leer.
- **Sin costo:** En blockchains como Ethereum o Bitcoin, las transacciones tienen un costo asociado, concepto que es conocido como "gas". En el caso de BFA, la red no requiere de una criptomoneda para su uso, el "gas"necesario para interactuar en la red es provisto de antemano a cada uno de los nodos con permiso de escritura por la propia blockchain.

BFA no provee un mecanismo de privacidad de la información propiamiente dicho; todos los datos contenidos son de libre acceso por parte de cualquier nodo. Lo que si hace BFA es almacenar solamente hashes (digestos criptográficos) de la información original que los usuarios de la blockchain manejan. Con este objetivo, es requerimiento para quien utilice la red, contar con un respaldo de la información original en una base

de datos indpependiente a la blockchain. Para poder comprobar la autenticidad se comparan los hashes de la blockchain contra los de la información original, esto es conocido como almacenamiento off-chain. Por otro lado, BFA no asume ningún compromiso en cuanto a la protección de datos personales y normativas como GDPR, y aclara, que esto es responsabilidad exclusiva de los nodos que escriben en la blockchain [Arg19]. Por estos motivos, en los casos donde la privacidad de la información sea un requerimiento, el mecanismo recomendado por BFA es el uso de hashes que referencian a los datos alojados en modo off-chain. Cada nodo o servicio interactuando con la red es responsable de la seguridad y manejo de la información guardada fuera de la red, una alternativa ampliamente analizada en este trabajo [Mol21a], donde el enfoque off-chain se puede complementar con mecanismos de control de acceso externos para mantener la confidencialidad y se puede integrar con soluciones de prueba de conocimiento cero (como zk-SNARKs o zk-STARKs) para verificar datos sin revelar su contenido.

2.2.2. Comparación de las soluciones

Dentro de los casos analizados, y en particular aquellos en los que los proyectos y soluciones tienen una visión estratégica desde el punto de vista gubernamental, como en los casos de Brasil y Argentina, se observa un patrón común en los diseños de estas soluciones basadas en blockchain. Ambas naciones han implementado tecnologías distribuidas para abordar el problema de la trazabilidad y autenticidad de los certificados académicos, haciendo especial énfasis en la seguridad y protección de los datos personales. En estos casos se han adoptado redes híbridas 2.1.4, permitiendo una mayor flexibilidad y control sobre los datos procesados; decisión alineada con las regulaciones locales e internacionales sobre privacidad, como el Reglamento General de Protección de Datos (GDPR) en Europa.

En Brasil, el proyecto Diploma Digital, liderado por el Ministerio de Educación, ofrece una solución innovadora que utiliza tecnología blockchain para emitir y verificar la autenticidad de los diplomas emitidos por instituciones educativas. Esta iniciativa busca reducir el fraude académico y mejorar la eficiencia de los procesos administrativos relacionados con la verificación de documentos. La arquitectura de Diploma Digital se basa en una blockchain híbrida, lo que permite tanto la transparencia pública en la verificación de los certificados como el control privado de los datos sensibles, cumpliendo con las regulaciones de protección de datos locales, como la Ley General de Protección de Datos (LGPD) de Brasil [Rep18], que es comparable al GDPR en términos de exigencias para la privacidad y seguridad de los datos personales.

Por otro lado, Argentina ha implementado el proyecto Blockchain Federal Argentina (BFA), una red blockchain diseñada para servir a diversas aplicaciones gubernamentales, incluida la validación de certificados académicos. Similar al caso de Brasil, la BFA es una red blockchain híbrida, lo que asegura que solo entidades autorizadas puedan participar en la validación de certificados, garantizando la privacidad de los estudiantes y la integridad de los datos. Sin embargo, a diferencia de la solución brasileña, la argentina ha adoptado por un enfoque más descentralizado en términos de gobernanza, permitiendo a múltiples actores, tanto gubernamentales como privados, participar en la administración de la red. Esta diferencia de acceso y gobenranza a la red plantea diversos desafíos en cuanto al consenso y la interoperabilidad, pero a su vez también ofrece una mayor resiliencia frente a fallos o ataques, asumiendo que un mayor conjunto de actores interesados pueden generar un mayor interés en resolver problemáticas de este tipo.

A pesar de estas diferencias en la arquitectura y el enfoque de gobernanza, ambas soluciones presentan desafíos comunes en términos de costo y escalabilidad. Las soluciones basadas en blockchain, aunque prometen mejoras significativas en seguridad y trazabilidad, requieren una infraestructura tecnológica considerable y un mantenimiento continuo para garantizar que puedan soportar el volumen creciente de certificados emitidos por las instituciones académicas. Además, es fundamental que tanto BFA como Diploma Digital continúen adaptándose a las regulaciones locales de protección de datos, como el LGPD en Brasil y la Ley de Protección de los Datos Personales en Argentina [Con00], para garantizar que las soluciones blockchain puedan evolucionar de manera segura y conforme a las normativas internacionales sobre privacidad, como GDPR.

En resumen, aunque tanto Brasil como Argentina han seguido enfoques innovadores para la validación de certificados académicos mediante blockchain, estas iniciativas continúan evolucionando para abordar desafíos de escalabilidad, interoperabilidad y gobernanza. Asimismo, se desataca un firme compromiso con la protección de los datos personales y la privacidad de los usuarios. En la tabla 2.2 se puede observar una comparativa entre ambas soluciones.

Criterio	**Blockchain Federal Argentina (BFA)**	**Diploma Digital (Brasil)**
Entidad responsable	NIC Argentina, CABASE, ARIU	Ministerio de Educación de Brasil, RNP
Objetivo principal	Multipropósito, entre ellos verificación de certificados digitales	Exclusivo para emisión y verificación de diplomas digitales académicos
Tipo de red	Híbrida con nodos aprobados previamente	Híbrida con nodos autorizados por el Ministerio de Educación
Tecnología utilizada	Ethereum (sin criptomoneda, sin gas fees)	Hyperledger Besu (compatibilidad con Ethereum)
Modelo de consenso	Proof of Authority (PoA)	Proof of Authority (PoA)
Manejo de costos	Sin costos de transacción (gas fees preaprovisionados)	Sin costos para usuarios finales, costos absorbidos por la infraestructura gubernamental
Privacidad de datos	No asume compromiso de cumplimiento con GDPR, requiere almacenamiento off-chain	Cumple con la LGPD (Ley de Protección de Datos de Brasil), almacenamiento controlado por RNP
Gobernanza	Participación descentralizada entre sector público, privado y académico	Gobernada centralmente por el Ministerio de Educación y la RNP
Interoperabilidad	Compatible con múltiples actores del sector público y privado	Exclusiva para el sistema educativo brasileño

CUADRO 2.2: Comparación entre Blockchain Federal Argentina (BFA) y Diploma Digital (Brasil)

Capítulo 3

Evaluación de tecnologías blockchain

Esta sección examina distintas opciones tecnológicas para la gestión de certificados académicos digitales, enfocándose en su alineación con regulaciones como la Ley Nº 18.331 de Uruguay [Uru08] y el GDPR [Uni16]. Se describen los criterios esenciales de seguridad y privacidad, señalando retos como la inmutabilidad de blockchain y proponiendo soluciones como almacenamiento off-chain y técnicas de cifrado avanzadas. Se realiza un análisis comparativo de diversas tecnologías blockchain, incluyendo Hyperledger Fabric, Hyperledger Besu, Ethereum, Corda y Quorum. Se destacan las características que hacen a la elección tecnológica más adecuada, como su arquitectura modular, su control granular de permisos y su capacidad de cumplir con normativas de protección de datos mediante el uso de canales y datos privados. Se comparan las ventajas de la opción frente a otras tecnologías, justificando su elección por su flexibilidad, seguridad y alineación con los requisitos regulatorios.

3.1. Marco regulatorio

Dado el avance normativo, el marco regulatorio es un componente esencial al considerar la implementación de soluciones tecnológicas, especialmente cuando se trata de la protección de datos personales. La protección de datos personales ha tomado relevancia en la última década, con diversas naciones implementando regulaciones estrictas para garantizar la privacidad y seguridad de la información de las personas. En este contexto, es fundamental analizar las regulaciones pertinentes al manejar datos personales en soluciones blockchain, especialmente en el ámbito de la validación de certificados digitales.

La ley de protección de datos personales de Uruguay, Ley Nº 18.331 [Uru08], y el Reglamento General de Protección de Datos (GDPR) [Uni16] de la Unión Europea son dos marcos legales diseñados para garantizar la seguridad y privacidad de los datos personales de los individuos. Ambos buscan proporcionar un conjunto de derechos a los usuarios y obligaciones a las entidades que procesan y mantienen información de estos. A continuación, se presentan ambas normativas y un análisis comparativo de los conceptos más relevantes.

3.1.1. Regulación en Uruguay: Leyes Nº 18.331 y 19.670

Uruguay ha sido proactivo en relación a la protección de datos personales, estableciendo la Ley Nº 18.331 en 2008. Esta ley establece los derechos y obligaciones relacionados con la protección de datos personales, incluyendo principios como la calidad de los datos, la finalidad, el consentimiento, y la seguridad, entre otros. Específicamente, la ley destaca la importancia de obtener el consentimiento explícito de los individuos

antes de procesar sus datos y garantizar que estos datos se utilicen solo para los fines específicos para los cuales fueron obtenidos.

La Ley Nº 18.331 también establece que las entidades que manejan datos personales deben adoptar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos. Además, otorga a los individuos derechos como el acceso, rectificación, actualización, inclusión y supresión de sus datos personales. Este marco legal busca proteger la privacidad de los ciudadanos y asegurar que sus datos sean tratados de manera responsable y segura.

Posteriormente, en 2018 se publicó la Ley 19.670, que introdujo cambios en la protección de datos personales para cumplir con la normativa europea. Esta ley se reglamentó en febrero de 2020 mediante el decreto 64/020.

3.1.2. Regulación Europea: GDPR

El GDPR, implementado en 2018 [Uni16], es una regulación de la Unión Europea que busca proteger y empoderar la privacidad de datos de todos los ciudadanos de la UE. Al igual que la Ley Nº 18.331 de Uruguay, GDPR enfatiza la importancia del consentimiento, la transparencia y el derecho al olvido. Ambas regulaciones comparten similitudes en cuanto a la protección de datos personales, haciendo hincapié en la responsabilidad de las organizaciones para garantizar la privacidad y seguridad de la información.

GDPR establece que las entidades deben obtener el consentimiento explícito de los individuos antes de procesar sus datos y deben proporcionar información clara sobre cómo se utilizarán estos datos. Además, otorga a los individuos derechos amplios, incluyendo el derecho a acceder a sus datos, rectificarlos, borrarlos y oponerse a su procesamiento. Estas medidas buscan proporcionar a los ciudadanos un mayor control sobre su información personal y asegurar que las organizaciones manejen los datos de manera transparente y segura.

3.1.3. Similitudes y diferencias entre las normativas

Tanto GDPR como la Ley Nº 18.331 enfatizan la necesidad de garantizar que los datos se procesen de manera transparente y con el consentimiento del individuo. Además, ambas regulaciones otorgan a los individuos el derecho a acceder, rectificar y, en ciertos casos, eliminar sus datos.

Estas similitudes entre el GDPR y la Ley Nº 18.331 sugieren que una solución blockchain diseñada para cumplir con una de estas regulaciones tendría una buena base para adaptarse a la otra. Sin embargo, es esencial considerar las particularidades de cada regulación y asegurarse de que cualquier solución propuesta esté en pleno cumplimiento con ambas [Fin19].

Similitudes

Derechos de los sujetos de datos: tanto en la Ley Nº 18.331 como en GDPR se reconocen derechos similares para los individuos respecto a sus datos personales, como el derecho a acceder a sus datos, rectificarlos si son incorrectos, y en ciertas circunstancias, eliminarlos o restringir su procesamiento.

Responsabilidad y consentimiento: ambas normativas exigen que el procesamiento de los datos personales sea legítimo, justo y transparente. Se requiere que el consentimiento sea dado de manera libre, específica, informada e inequívoca.

Transferencias internacionales de datos: tanto la ley uruguaya como la normativa europea establecen restricciones a la transferencia de datos personales fuera del país o del bloque económico, respectivamente, asegurando que se protejan los datos según estándares similares.

Autoridades de protección de datos: la Unidad Reguladora y de Control de Datos Personales (URCDP) en Uruguay y las Autoridades de Protección de Datos (DPA) en la UE tienen roles similares en la supervisión y cumplimiento de la ley, incluyendo la capacidad de realizar investigaciones y aplicar sanciones.

Notificación de violaciones de datos: GDPR establece que cualquier violación de seguridad que afecte datos personales debe notificarse a la autoridad supervisora en un plazo máximo de 72 horas luego de haber sido detectada, salvo que sea improbable que represente un riesgo para los derechos y libertades de los usuarios. En Uruguay, existe una reglamentación en la Ley N.º 19.670 mediante el Decreto N.º 64/020 [Rep20] que establece un requisito similar. Según el artículo, el responsable del tratamiento de datos debe informar a la URCDP dentro de un plazo máximo de 72 horas desde que se haya constatado una vulneración de seguridad. Por lo tanto, en este aspecto, la legislación uruguaya y el GDPR presentan una alineación en los tiempos de notificación.

Designación del delegado de protección de datos (DPO): tanto GDPR como la de Uruguay establecen la obligatoriedad de designar un Delegado de protección de datos (DPO) en determinadas circunstancias.

En el caso del GDPR, el Artículo 37 dispone que el DPO debe ser designado cuando:

- El tratamiento de datos es realizado por una autoridad u organismo público, excepto los tribunales en función judicial.
- Las actividades principales del responsable o encargado incluyen operaciones de tratamiento que requieren una observación habitual y sistemática.
- Se realiza tratamiento a gran escala de categorías especiales de datos o datos relativos a condenas e infracciones penales [Uni16].

En Uruguay, se establece que deben designar un DPO:

- Entidades públicas, sean estatales o no estatales.
- Entidades privadas total o parcialmente de propiedad estatal.
- Entidades privadas cuya actividad principal implique el tratamiento de datos sensibles.
- Entidades que realicen tratamiento de grandes volúmenes de datos personales, definidos en la reglamentación como aquellos que involucran datos de más de 35.000 personas.

Ambas normativas establecen que el DPO debe asesorar en el cumplimiento de la legislación de protección de datos, supervisar su implementación dentro de la organización, y actuar como punto de contacto con la autoridad de control correspondiente. Asimismo, se exige que el DPO actúe con independencia en sus funciones y posea conocimientos especializados en legislación y gestión de datos personales.

La incorporación de la figura del DPO en la legislación uruguaya refleja una alineación significativa con el GDPR, asegurando una mayor regulación en el tratamiento de datos personales y la responsabilidad de las organizaciones en su cumplimiento.

Principio de finalidad y borrado de datos: tanto GDPR como la Ley de Uruguay establecen principios relacionados con la limitación de la finalidad del tratamiento de datos personales, indicando que los datos personales deben recolectarse y procesarse exclusivamente para fines específicos, explícitos y legítimos. En particular, el principio de finalidad en la ley uruguaya establece que los datos personales deberán ser eliminados cuando ya no sean necesarios o pertinentes para los fines para los que fueron recolectados originalmente (*Ley N.º 18.331, Artículo 8*) [Uru08]. Esto está alineado con el artículo 5 del GDPR, que establece que los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los cuales son tratados, contemplando también su eliminación cuando ya no sean requeridos.

Esta similitud refleja que ambas regulaciones buscan asegurar que los datos personales no se conserven más allá del tiempo estrictamente necesario para los fines originalmente definidos.

Derecho al olvido y portabilidad de datos: GDPR establece explícitamente el derecho al olvido y el derecho a la portabilidad de los datos personales (Artículos 17 y 20, respectivamente). El derecho al olvido permite a los usuarios solicitar la supresión de sus datos cuando estos ya no son necesarios para los fines originales o cuando se ha retirado el consentimiento, entre otras razones específicas. El derecho a la portabilidad permite obtener los datos personales en un formato estructurado y digital para transferirlos a otro responsable.

En la Ley uruguaya, si bien no se mencionan explícitamente los términos "derecho al olvidoz "portabilidad", el principio de finalidad, establecido en el Artículo 8, exige la eliminación de datos personales cuando ya no sean necesarios para el propósito original del tratamiento. Por otro lado, la Ley N.º 19.670 introduce explícitamente, en su Artículo 37, el derecho a la portabilidad de datos personales, permitiendo a los titulares recibir sus datos en un formato estructurado y transmisible a otra entidad responsable del tratamiento.

Por tanto, en relación con la supresión de datos cuando dejan de ser necesarios (derecho al olvido) y el derecho a la portabilidad, ambas regulaciones presentan similitudes relevantes, aunque la normativa europea proporciona definiciones más explícitas sobre ambos derechos.

Evaluaciones de impacto sobre protección de datos personales: GDPR establece en su artículo 35 la obligación explícita de realizar evaluaciones de impacto sobre la protección de datos personales (DPIA) cuando el tratamiento pueda generar riesgos significativos para los derechos y libertades individuales.

En Uruguay, aunque la Ley Nº 18.331 originalmente no incluía este requisito, la Ley Nº 19.670, en su artículo 39 (modificando el artículo 12 de la Ley N.º 18.331), introduce explícitamente la obligación de realizar evaluaciones de impacto cuando el tratamiento involucra grandes volúmenes de datos, datos sensibles, grupos vulnerables o transferencias internacionales hacia estados que no proporcionan garantías adecuadas. A su vez, el Decreto N.º 64/020 en su artículo 5 reglamenta detalladamente las circunstancias específicas que obligan a realizar estas evaluaciones de impacto, especificando casos tales como tratamientos permanentes de datos sensibles o transferencias internacionales de información personal.

En consecuencia, en lo referido a evaluaciones de impacto sobre la protección de datos, la legislación uruguaya actual se encuentra alineada con las exigencias del GDPR.

Diferencias

Alcance: GDPR tiene un alcance más amplio en cuanto a su aplicación extraterritorial. Aplica a cualquier empresa, independientemente de su ubicación, que procese datos de individuos dentro de la UE. La Ley uruguaya se aplica principalmente a entidades dentro de Uruguay, aunque también tiene disposiciones para casos en los que los datos son procesados en el extranjero. Por otro lado, la ley de Uruguay extiende la protección de datos personales a las personas jurídicas [Rep08], a diferencia GDPR que se aplica únicamente a personas físicas. Por lo tanto, en Uruguay, las personas jurídicas gozan de derechos similares a los de las personas físicas en cuanto a la protección de sus datos personales.

Bases legales para el procesamiento: GDPR detalla explícitamente las bases legales para el procesamiento de datos personales, mientras que la Ley uruguaya es menos específica en este aspecto.

Sanciones: GDPR tiene un régimen de sanciones más severo, con multas significativamente mayores por incumplimiento, que pueden llegar hasta el 4 % del volumen del negocio anual global de la empresa infractora, mientras que la ley uruguaya tiene un sistema de multas que puede ser considerado menos severo.

3.2. Criterios de evaluación de tecnología Blockchain

La evaluación de tecnologías blockchain requiere un análisis profundo de diversos criterios, entre los cuales destacan la seguridad y la privacidad. Estos aspectos son particularmente relevantes en el contexto de las normas como GDPR, que establece estrictos requisitos para el manejo y la protección de datos personales. Es en base a estos criterios de evaluación que se realizará la elección de la tecnología a utilizar para el prototipo que veremos más adelante.

3.2.1. Seguridad

La seguridad en blockchain involucra la capacidad de la tecnología para proteger la integridad, disponibilidad y confidencialidad de los datos almacenados. Los mecanismos de consenso, como Proof of Work (PoW) y Proof of Stake (PoS), juegan un papel crucial en garantizar que las transacciones sean verificadas de manera segura y que la red sea resistente a ataques. La criptografía es otro componente esencial, al utilizarse algoritmos de hash y firmas digitales para asegurar que los datos no puedan ser alterados sin que exista un mecanismo de detección [Nak08].

3.2.2. Privacidad y confidencialidad en blockchain

La privacidad en blockchain se refiere a la capacidad de esta tecnología para proteger los datos personales contra accesos no autorizados y permitir que los individuos controlen su información. Esto incluye derechos fundamentales como la minimización de datos, la portabilidad y el derecho al olvido. Sin embargo, la inmutabilidad característica de blockchain representa un desafío específico para el derecho al olvido, debido a que los datos, una vez registrados, no pueden eliminarse fácilmente [Zoh15].

Adicionalmente a esto, en redes blockchain tradicionales, cada nodo participante mantiene una copia completa del ledger, lo que podría comprometer la confidencialidad de los datos personales almacenados. Para resolver estos desafíos, las plataformas

blockchain permisionadas como Hyperledger Fabric ofrecen mecanismos avanzados de confidencialidad mediante el cifrado de datos, canales privados y colecciones de datos privados. Estos mecanismos aseguran que únicamente las entidades autorizadas tengan acceso a información sensible, reduciendo así los riesgos de privacidad asociados al almacenamiento distribuido.

Por otro lado, aunque las soluciones basadas en el modelo de seguridad *Zero Trust* fortalecen la confidencialidad mediante controles estrictos de acceso y autenticación, estas por sí mismas no resuelven el desafío específico del derecho al olvido en blockchain. Este derecho requiere estrategias adicionales, tales como almacenar información personal fuera de la cadena (*off-chain*), conservando en blockchain únicamente referencias criptográficas (*hashes*) que permiten verificar la integridad sin exponer los datos reales.

Por lo tanto, una solución integral para garantizar privacidad y confidencialidad en blockchain debería combinar mecanismos Zero Trust, técnicas de cifrado avanzado y gestión off-chain de datos personales para satisfacer plenamente los requisitos normativos.

3.3. Análisis de tecnologías blockchain

3.3.1. Hyperledger Fabric

Hyperledger Fabric [Hyp23a], de ahora en mas Fabric, fue desarrollado en 2016 por la Linux Foundation y es un marco de trabajo de código abierto para la implementación de redes blockchain en el medio empresarial, esencialmente. Fue diseñado para permitir el desarrollo de aplicaciones y soluciones blockchain seguras, escalables y flexibles, con el fin de brindar soporte a múltiples rubros y cadenas de suministro [Aa18].

Fabric se centra en proporcionar una arquitectura modular y configurable que se adapte a las necesidades de diferentes aplicaciones, permitiendo que equipos de trabajo distintos puedan colaborar en el desarrollo de estándares y protocolos. El enfoque propuesto por Fabric admite una variedad de blockchains, cada una con su propio modelo de almacenamiento, servicios de identidad, algoritmo de consenso, control de acceso y contratos inteligentes [Cac16].

En Fabric los smart contracts son llamados “chaincode” y una de las principales ventajas que ofrece la red es la posibilidad de implementar estos contratos en varios lenguajes de programación; por ejemplo, Go, NodeJS o Java. Esto permite que las organizaciones que componen la red hagan uso de habilidades que generalmente ya poseen, sin necesidad de tener que aprender un nuevo lenguaje.

Fabric está constituido por diversas blockchains individuales creadas por distintas organizaciones, donde cada organización cuenta con un conjunto básico de componentes, como nodos, algoritmos de consenso, smart contracts y ledger de transacciones que forman la blockchain.

Fabric difiere de las redes públicas (*permissionless*) en aspectos relacionados con la seguridad, confidencialidad y control de acceso. A diferencia de las redes públicas, Fabric es una red tipo consortium (*permissioned*), donde cada nodo participante cuenta con un permiso previo para poder interactuar en la red. A este concepto se le denomina “canales” y permite que un subconjunto específico de organizaciones participe en transacciones y comparta información de manera confidencial. Esto resulta útil cuando se requiere confidencialidad entre ciertos participantes y se desea mantener la privacidad de determinados datos.

Fabric implementa un modelo de permisos granular para las organizaciones participantes en la red, permitiendo que las organizaciones definan qué nodos pueden acceder

y participar en qué canales y transacciones específicas, buscando darle más robustez a la privacidad y seguridad de los datos.

Otra gran diferencia entre Fabric y las redes públicas se nota en la capacidad de configuración, por ejemplo, en el algoritmo de consenso. La red permite configurarse de acuerdo al caso de uso, pudiendo elegir entre varios algoritmos de consenso, como Raft o Kafka , entre otros. Esta posibilidad de configuración tiene un impacto drástico en el rendimiento de la red en lo relativo al procesamiento de las transacciones [Hyp23b].

3.3.2. HyperLedger Besu

Desarrollado también por la Linux Foundation en 2019, Hyperledger Besu [Hyp21a] es un proyecto de código abierto que se enfoca en proporcionar una plataforma blockchain flexible y adaptable para casos de uso empresariales. Utiliza la especificación de Ethereum y es compatible con esta red; esto implica que puede aprovechar todas sus características y funcionalidades.

Una de las principales ventajas de Besu es su capacidad de escalabilidad y procesamiento de grandes volúmenes de transacciones, gracias al uso de un algoritmo de consenso basado en Proof of Authority (PoA)[Hyp23]. Besu evita los problemas de escalabilidad y latencia asociados con otros algoritmos de consenso como Proof of Work (PoW) [Fou23b]. Esta característica hace que Besu sea ideal para casos de uso en los que se requiere un alto rendimiento y una rápida confirmación de las transacciones.

Desde el punto de vista de la seguridad, la red ofrece mecanismos de acceso a la información y privacidad de los datos, permitiendo a las organizaciones establecer permisos y políticas de acceso para garantizar que solo las partes autorizadas puedan participar en la red y acceder a la información confidencial. Además, proporciona una robusta capa de protección para los datos almacenados en la blockchain, utilizando técnicas de cifrado avanzadas para garantizar la privacidad e integridad de éstos.

3.3.3. Otras tecnologías analizadas

Además de Fabric y Besu, existen otras tecnologías blockchain que podrían considerarse para la validación de certificados académicos. Sin embargo, estas alternativas presentan ciertas limitaciones en cuanto a escalabilidad, gobernanza y cumplimiento con normativas de privacidad de datos.

Ethereum: es una de las blockchain públicas más conocidas, principalmente por su uso de contratos inteligentes y su capacidad de descentralización [Fou23c]. Sin embargo, su enfoque en una red pública y su dependencia del consenso mediante Proof of Work (PoW) limitan su aplicabilidad en entornos empresariales y académicos, donde se necesita un mayor control sobre los nodos participantes y la privacidad de los datos. Además, el costo asociado con el uso de la red (*gas fees*) lo hace una opción menos atractiva para soluciones de largo plazo en validación de certificados, donde no se busca emitir una criptomoneda o involucrar participantes anónimos. Estas características reducen su aplicabilidad para escenarios donde el control granular de acceso y la privacidad son primordiales, como la validación segura de certificados digitales académicos.

Corda: desarrollado por R3 [R321], es una blockchain permisionada orientada a sectores financieros que ha ganado popularidad por su capacidad para crear aplicaciones descentralizadas con un enfoque en la privacidad. Aunque esta característica puede ser ventajosa para la validación de certificados académicos, Corda no es tan flexible como Fabric en cuanto a la creación de redes multi-entidad con diferentes niveles de permisos. Corda está principalmente diseñado para ser usado en transacciones financieras entre un número limitado de actores, lo que reduce su aplicabilidad a un entorno

donde múltiples instituciones académicas y gubernamentales necesitan interactuar de manera eficiente.

Quorum: es una variante empresarial de Ethereum [Con23], creada por J.P. Morgan. Utiliza un modelo de consenso basado en Proof of Authority (PoA), lo que le permite escalar mejor que Ethereum tradicional. Sin embargo, al igual que Ethereum, su integración con redes públicas plantea problemas de privacidad y cumplimiento con normativas como el GDPR, especialmente cuando se manejan datos sensibles como los certificados académicos. Además, al ser una bifurcación de Ethereum, enfrenta los mismos desafíos relacionados con los costos de las transacciones.

En resumen, aunque estas tecnologías son relevantes para ciertos contextos empresariales y financieros, presentan limitaciones para el manejo eficiente y seguro de certificados académicos. Por este motivo, Fabric y Besu fueron consideradas las opciones más adecuadas en términos de modularidad, privacidad y cumplimiento normativo.

3.4. Elección de la tecnología adecuada

3.4.1. Comparativa Fabric-Besu

A pesar de que ambas soluciones tienen como objetivo proporcionar soluciones blockchain enfocadas a organizaciones, existen diferencias significativas en términos de diseño, arquitectura y características. En la tabla 3.1 se presentan algunas de las diferencias más destacadas entre Hyperledger Fabric y Hyperledger Besu, que son relevantes al momento de seleccionar una tecnología blockchain para la validación de certificados digitales.

Criterio	Hyperledger Fabric	Hyperledger Besu
Protocolo de consenso	Modular incluyendo Raft o Kafka	Proof of Authority (PoA), Proof of Work (PoW)
Smart contracts	chain-codes pueden implementarse en diversos lenguajes como Go, Javascript, Java	smart-contracts en Solidity únicamente
Red principal (mainnet)	No conectada a Ethereum ni otras redes públicas	Compatible con la red principal de Ethereum
Arquitectura	Modular y configurable, basada en canales	Basada en nodos de Ethereum
Casos de uso	Aplicaciones empresariales, cadenas de suministro, identidad digital	Aplicaciones empresariales, especialmente financieras, con compatibilidad Ethereum
Interoperabilidad	Limitada, enfocada en redes permisionadas	Alta, interoperabilidad con Ethereum y DApps públicas
Cifrado y hashing	Soporte integrado con SHA-256, configurable según políticas del sistema	Uso del estándar Ethereum, manejo manual de privacidad
Control de acceso	Basado en canales y permisos granulares	Basado en permisos de red
Privacidad y confidencialidad	Alta mediante canales privados y colecciones de datos privados (off-chain)	Privacidad gestionada principalmente mediante grupos privados, menos granular que Fabric
Seguridad	Modelo basado basado en identidades digitales mediante certificados X.509, gestionadas por el Membership Service Provider (MSP) y RBAC. Compatible con módulos HSM para protección adicional de claves criptográficas.	Seguridad basada en criptografía Ethereum (ECDSA), gestión mediante cuentas Ethereum, cumple especificaciones de Enterprise Ethereum Alliance.
Cumplimiento GDPR	Soporte mediante datos off-chain para derecho al olvido	Limitado, requiere soluciones externas para cumplimiento
Rendimiento y escalabilidad	Alto rendimiento y escalabilidad mediante consenso modular y canales	Alto rendimiento, pero menos modularidad en escenarios complejos

CUADRO 3.1: Comparativa entre Fabric y Besu

3.4.2. Justificación de la elección

La elección de Hyperledger Fabric como la tecnología base para la gestión de certificados académicos en la blockchain se fundamenta en varios factores clave que alinean su arquitectura y capacidades con los requisitos del sistema, tanto desde un punto de vista técnico como normativo.

Cumplimiento normativo y privacidad de datos

Uno de los principales motivos para optar por Fabric es su capacidad para cumplir con normativas de protección de datos. Fabric implementa una arquitectura permisionada en la cual todos los participantes en la red son conocidos y autorizados previamente, lo que garantiza un control total sobre quién accede y participa en las

transacciones. Esto es fundamental en un entorno académico donde resulta importante asegurar la integridad de los certificados y la privacidad de los datos personales de los estudiantes.

En términos de privacidad, Fabric ofrece mecanismos avanzados como los canales y las colecciones de datos privados, que se detallan en la próxima sección y que permiten un control granular sobre quién puede ver y modificar datos. Estos mecanismos son especialmente útiles para garantizar el derecho al olvido y la minimización de datos, principios esenciales en GDPR. Al permitir que los datos se almacenen fuera de la blockchain (*off-chain*) y que solo un hash referencial quede registrado en la red, Fabric proporciona una solución para eliminar datos sin comprometer la integridad de la cadena de bloques, algo crucial cuando se gestionan datos personales sensibles.

Desempeño y escalabilidad

Otro factor determinante es el desempeño y escalabilidad que ofrece Fabric. A diferencia de otras soluciones como Ethereum o Quorum, que dependen de mecanismos de consenso públicos como Proof of Work (PoW), Fabric utiliza un enfoque modular con múltiples algoritmos de consenso disponibles, como Raft o Crash Fault Tolerant (CFT). Esto permite adaptar la red a las necesidades específicas del sistema, optimizando el rendimiento según el volumen de transacciones esperado. En un entorno académico donde el número de certificados digitales podría crecer significativamente, la capacidad de Fabric para procesar grandes cantidades de transacciones de forma eficiente es una ventaja importante.

Control de acceso y gestión de permisos

Fabric se destaca por su modelo avanzado de gestión de identidades y control de acceso basado en roles (RBAC). Este modelo permite definir políticas de acceso granulares, tanto a nivel de red como en cada canal o smart contract (*chaincode*), garantizando que solo los actores autorizados puedan realizar operaciones específicas [Hyp23]. Este enfoque es esencial para cumplir con las necesidades del entorno académico, donde múltiples actores como universidades, empleadores y entidades gubernamentales necesitan interactuar con la red, pero con diferentes niveles de acceso a la información. El Membership Service Provider (MSP) de Fabric es otro componente clave que garantiza la autenticación y verificación de identidades mediante certificados digitales. Esto asegura que solo los actores autorizados puedan realizar operaciones en la red, reforzando así la seguridad y confianza en el sistema.

Gobernanza

Si bien Besu también es una opción válida para aplicaciones blockchain empresariales, presenta algunas limitaciones en cuanto al control de la privacidad y la gobernanza de la red. Besu está más orientado a redes públicas y utiliza un mecanismo de consenso basado en Proof of Authority (PoA), lo cual es menos flexible que el enfoque modular de Fabric. Además, al estar estrechamente vinculado con Ethereum, Besu no proporciona el mismo nivel de granularidad en el control de permisos y confidencialidad que Fabric, lo que podría ser un inconveniente en un entorno donde la privacidad y el manejo seguro de datos son primordiales.

Flexibilidad y modularidad

Por último, la flexibilidad de Fabric es otro factor clave en su elección. Su arquitectura modular permite configurar aspectos críticos como el algoritmo de consenso, los niveles de acceso y las bases de datos subyacentes. Esto facilita la adaptación de la red a las necesidades cambiantes de las instituciones académicas y gubernamentales, asegurando que el sistema pueda evolucionar sin comprometer su seguridad o privacidad.

En síntesis, dentro de las opciones consideradas, Fabric resulta ser la opción más adecuada para la implementación de un sistema de certificados académicos en blockchain debido a su enfoque robusto en la privacidad, la seguridad y la flexibilidad. Su capacidad para cumplir con las regulaciones internacionales y locales, junto con su escalabilidad y control de acceso granular, lo convierten en la solución ideal para este contexto.

Capítulo 4

Implementación del prototipo

Esta sección describe el desarrollo de un prototipo para gestionar certificados académicos digitales con Hyperledger Fabric, asegurando el cumplimiento normativo y la protección de datos personales. Se detalla la arquitectura del sistema, incluyendo los actores principales (controladores, procesadores de datos, dueños de datos y verificadores), y se especifican los requisitos funcionales y no funcionales. Se explican procesos clave como el registro de información, la verificación de certificados mediante hashes almacenados en la blockchain, y la gestión de acceso y privacidad mediante políticas definidas. También se destacan las capacidades de modificación y eliminación de datos, garantizando la seguridad y control por parte de los usuarios y las entidades involucradas.

4.1. Descripción del prototipo

En adelante se describe el prototipo implementado utilizando Fabric conforme a la normativa sobre privacidad de la información y los requrimientos que provienen del trabajo previamente desarrollado en [Mol21a].

4.1.1. Objetivos del prototipo

El sistema de certificación académica digital enfrenta desafíos significativos en términos de autenticidad, seguridad y cumplimiento normativo, especialmente ante regulaciones tanto locales como internacionales. La falsificación de certificados y la falta de mecanismos confiables para su validación representan problemas recurrentes en el ámbito académico. Por ello, el objetivo de este prototipo es implementar una solución basada en blockchain que permita a las instituciones académicas emitir, gestionar y validar certificados digitales de forma segura, garantizando la integridad de los datos y respetando los derechos de privacidad de los titulares.

Este trabajo toma como punto de partida la metodología propuesta por [Mol21a] que presenta una arquitectura híbrida para aplicaciones blockchain que requieren cumplir con regulaciones de protección de datos como GDPR. En su propuesta, enfatiza la necesidad de incorporar mecanismos (*off-chain*) para gestionar datos sensibles, limitando el registro en la blockchain únicamente a referencias criptográficas (*hashes*). Este enfoque metodológico permite la eliminación efectiva de datos cuando ya no son necesarios, cumpliendo así con el derecho al olvido.

Siguiendo esta línea, el prototipo desarrollado en esta tesis extiende y adapta el modelo del trabajo previo al contexto específico de certificación académica en Uruguay y en particular para SECIU-Udelar. El sistema implementado utiliza Fabric, una plataforma blockchain permisionada que permite configurar controles granulares de acceso y confidencialidad.

Además, el prototipo incluye mecanismos avanzados de control de acceso mediante canales privados y colecciones de datos privados, garantizando que solo los actores autorizados puedan interactuar con la información confidencial. Este diseño busca resolver no solo los problemas técnicos y de seguridad, sino también las implicaciones regulatorias asociadas a la protección de datos en el proceso de emisión y verificación de certificados digitales.

4.1.2. Actores del sistema

Para definir claramente los roles (actores) en el sistema propuesto, se utilizarán los términos empleados en GDPR. Este reglamento establece roles específicos para el manejo de datos personales, los cuales son fundamentales para comprender los flujos de información y responsabilidades en el prototipo:

- **Data Controller (DC)** o responsable del tratamiento: es la entidad que determina los propósitos y medios para el tratamiento de los datos personales. En el contexto de este prototipo, el DC es representado por el SECIU (Servicio Central de Informática de la Universidad), responsable del manejo y protección de los datos personales almacenados en la plataforma.
- **Data Processor (DP)** o encargado del tratamiento: es la entidad que procesa datos personales en nombre del DC. En este caso, las bedelías de las facultades son los procesadores de datos personales, actuando bajo la autoridad y responsabilidad del SECIU. Las bedelías son responsables de registrar y administrar la información relacionada con los estudiantes.
- **Data Owner (DO)** o titular de los datos: son las personas a quienes pertenecen los datos personales tratados en el sistema. En el prototipo implementado, los egresados (estudiantes) son los titulares de los datos, teniendo derechos específicos sobre la información registrada, tales como acceder, rectificar, borrar y controlar el acceso a sus datos personales.
- **Receiver (R)** o receptor: son entidades externas que requieren verificar la autenticidad y validez de los títulos emitidos. Estas pueden ser instituciones educativas, empresas u otros organismos que necesitan confirmar información específica sobre los egresados, siempre previa autorización explícita del titular de los datos (DO).

La definición de estos actores según el GDPR permite una clara asignación de responsabilidades y garantiza el cumplimiento de los derechos de privacidad y protección de datos de los usuarios en la implementación propuesta.

4.1.3. Requerimientos no funcionales

Tomando como referencia las recomendaciones realizadas en [Mol21a] sobre cumplimiento regulatorio y privacidad en aplicaciones blockchain, el diseño de este prototipo considera una serie de requerimientos no funcionales y utiliza los actores del sistema definidos en la sección anterior 4.1.2.

1. Dado que los títulos y la escolaridad contienen información personal administrada por el DC, deben almacenarse fuera de la blockchain (*off-chain*), manteniendo solo referencias criptográficas (*hashes*) dentro de la cadena. Este enfoque facilita el cumplimiento del derecho al olvido según las regulaciones ya mencionadas.

2. Los hashes almacenados en blockchain deben considerarse información personal debido a su naturaleza pseudoanonimizada, por lo cual su acceso debe estar sujeto a autorización explícita del titular de los datos (DO).

3. Los procesos de control de acceso, verificación de títulos y auditoría corren dentro de la blockchain.

4. Para validar los certificados, un hash de datos referencial es guardado en la blockhain y éste se compara con el hash del certificado del usuario dueño del título.

5. La validación y verificación de títulos por parte del receptor (R) debe ser una operación autorizada explícitamente por el titular de los datos (DO).

4.1.4. Requerimientos funcionales

En línea con la metodología propuesta por [Mol21a], el prototipo implementado contempla los siguientes requerimientos funcionales específicos:

1. **Registro de información**: el proceso de registrar información personal de los DO (estudiantes) en la plataforma está a cargo del DP (bedelías en nuestro caso). Este proceso se inicia con la solicitud de autorización desde DP hacia el DO para que éste autorice y envíe los datos solicitados. Una vez que los datos son enviados al gateway, una política es ejecutada para validar que se pueden registrar los datos. La información enviada es guardada, dejando un registro de integridad de los mismos en la blockchain principal. La imagen 4.1 muestra el requerimiento en forma de diagrama.

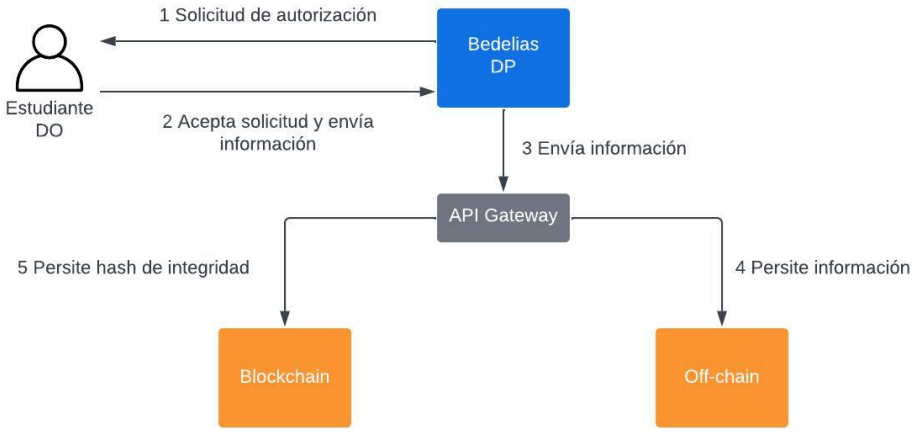

FIGURA 4.1: Registro de información

2. **Otorgar y revocar acceso a la información**: para que un tercero (Receiver) pueda acceder a verificar información perteneciente a un estudiante (DO), debe existir un mecanismo para autorizar o revocar este tipo de acceso. En este caso de uso, el Receiver envía una solicitud de acceso al DO. Al ser aceptada por el DO, se ejecuta una política de acceso a la blockchain para el Receiver que luego será utilizada para poder validar los certificados. Por otro lado, el acceso otorgado a un Receiver puede ser removido por el DO, DC o DP, actualizando las políticas de acceso establecidas anteriormente. La imágenes 4.2 y 4.3 ilustran el requerimiento.

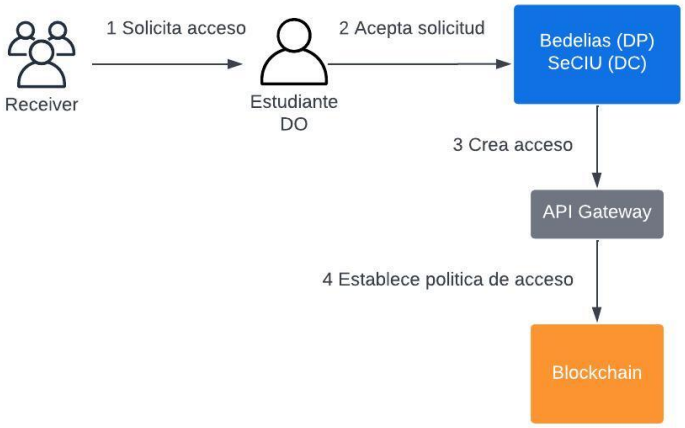

FIGURA 4.2: Otorgar acceso

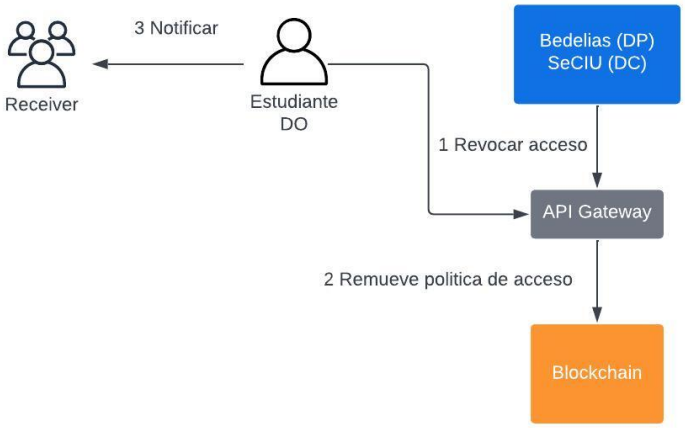

FIGURA 4.3: Revocar acceso

3. **Verificación de la información**: para poder realizar la verificación por parte del Receiver o el DO, el usuario presenta un hash de verificación que luego es comparado con el hash de la información guardada en la blockchain (req. 1), validando así la integridad y autenticidad de la información. Dado que este proceso es considerado sensible, es necesario realizar una verificación del control de acceso provisto al usuario (req. 2). La imagen 4.4 muestra el requerimiento en forma de diagrama.

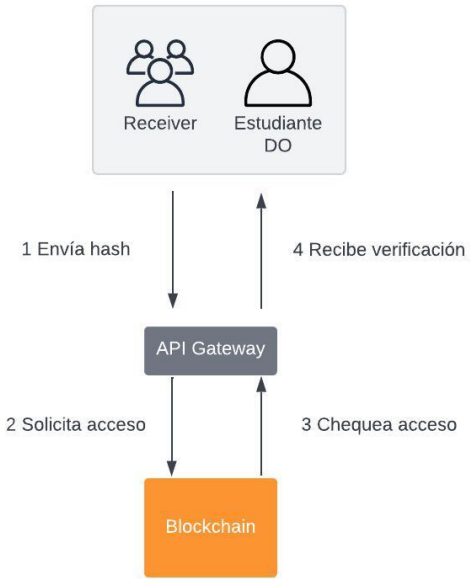

FIGURA 4.4: Verificación de la información

4. **Edición y eliminación de información**: el DO es capaz de realizar una solicitud para modificar o eliminar su información contenida en la plataforma. Con este fin, la solicitud es procesada por los DC o DP, los cuales cuentan con permisos definidos en las políticas para modificar o borrar información. Para completar la solicitud, se realiza una transacción sobre la información *offchain* y luego se actualiza el *hash* de integridad en la blockchain principal (req 1). Similarmente, tanto el DC como el DP son capaces de modificar información del mismo modo al descrito anteriormente pero sin haber sido solicitado por el DO. En este caso el proceso es similar, debiendo notificar al DO luego de realizado el cambio. La imagen 4.5 ilustra el requerimiento.

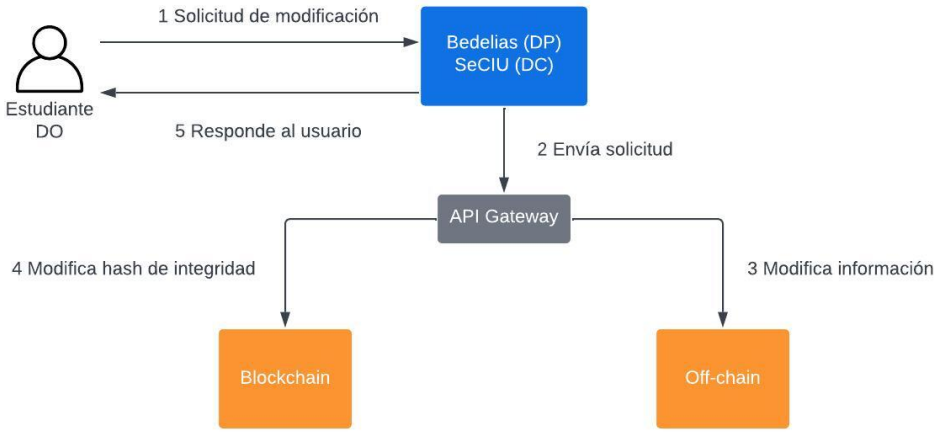

FIGURA 4.5: Edición y eliminación de información

5. **Acceso a logs de auditoría**: tanto el DO como una "Autoridad de Control" previamente definida son capaces de solicitar el registro de auditoría de la información relacionada al DO. Esta operación debe considerarse como sensible y tener una

política de control de acceso definida. Una vez hecha la solicitud, los DC o DP devuelven el log de acceso de la información contenida en la blockchain. La imagen 4.6 ilustra el requerimiento.

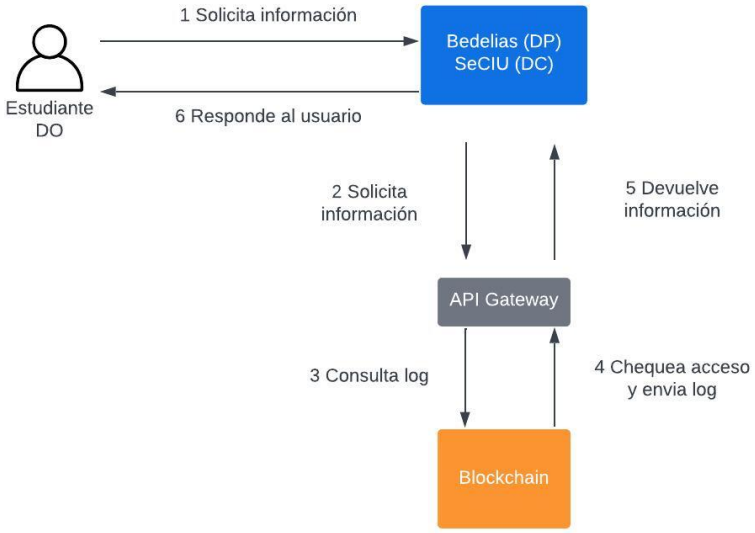

FIGURA 4.6: Acceso a logs de auditoría

4.2. Diseño de la arquitectura

La arquitectura propuesta para el sistema está compuesta por distintos módulos y componentes interconectados, cuyo diseño responde directamente a los requerimientos funcionales y no funcionales establecidos previamente. La interacción entre los componentes se realiza mediante APIs seguras y mecanismos de autorización claramente definidos. A continuación, se presentan detalladamente cada uno de los componentes del sistema y su rol específico dentro de la arquitectura.

4.2.1. Componentes del sistema

La arquitectura del prototipo está basada en los componentes definidos por [Mol21b], este diseño responde directamente a los requerimientos normativos y técnicos expuestos en la imagen 4.7, a continuación, se describen brevemente estos componentes según lo presentado en dicho trabajo:

- **Candidates (DO)**: propietarios de los datos personales con capacidad de autorizar accesos y solicitar modificaciones o borrado de información.
- **Receiver (R)**: terceros que requieren verificar la autenticidad de los certificados, solicitando acceso previa autorización del titular.
- **SECIU (DC)**: define propósitos y medios del tratamiento de datos personales.
- **Registry Office (DP)**: actúa como intermediario para gestionar solicitudes y acceso a datos.
- **Gateway**: componente que gestiona las solicitudes, políticas de acceso y comunicación entre blockchain y almacenamiento off-chain.

- **Blockchain**: realiza registros de logs, integridad y validación mediante almacenamiento de hashes.
- **Off-chain storage**: almacena efectivamente los datos sensibles fuera de blockchain, permitiendo modificaciones y eliminaciones según requisitos normativos.

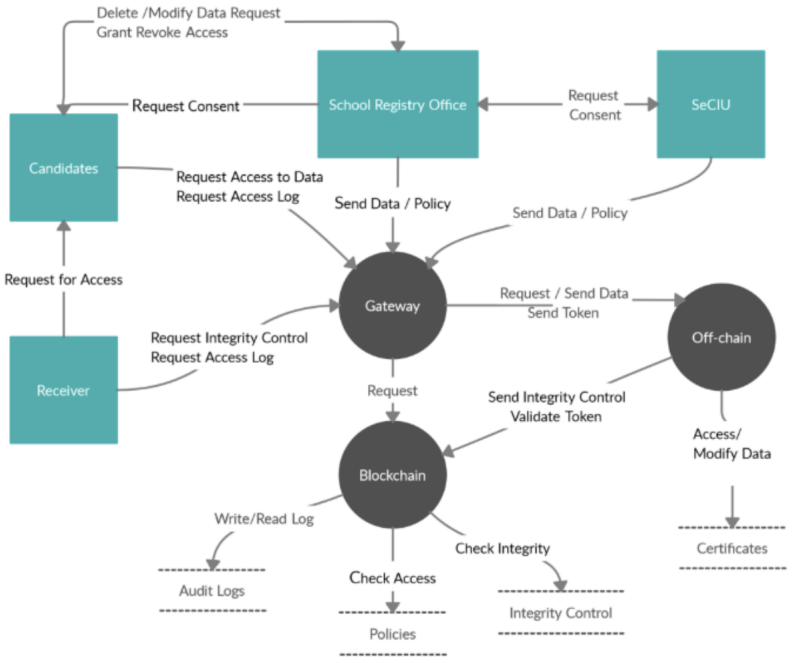

FIGURA 4.7: Componentes del sistema - Fuente: [Mol21b]

4.2.2. Herramientas y tecnologías utilizadas

Fabric contiene una serie de componentes que permiten el funcionamiento de la blockchain como tal y por otro lado brindan mecanismos de seguridad y privacidad de la información. En este sentido se pueden establecer políticas de acceso en distintos niveles, lo que da como resultado que el control de acceso a los datos puede ser manipulado tanto en la red más amplia como en niveles más específicos, como los canales. A continuación se buscará describir los componentes utilizados por Fabric para garantizar la seguridad de la información y su uso para el prototipo.

Políticas

A diferencia de otras blockchains como Bitcoin o Ethereum donde las transacciones pueden ser creadas y validadas por cualquier nodo en la red, en Fabric existen una serie de políticas que brindan gobernanza a la red. Las políticas en Fabric le dan la posibilidad a los miembros de decidir qué organizaciones tienen acceso a determinados recursos y proveen los mecanismos para garantizar esas decisiones. Por otro lado, proveen consenso en aspectos tales como: cuántas organizaciones deben ponerse de acuerdo para actualizar un recurso, un channel o un smart contract.

Cada smart contract en Fabric tiene una política de este tipo asociada (*chaincode endorsement policy*). Estas políticas indican cuáles entidades dentro de la red deben "firmar"las transacciones generadas por un smart contract para que éstas puedan ser consideradas como válidas. Tanto las transacciones válidas como las inválidas son guardadas

en el ledger distribuido que cada nodo tiene. En la misma línea, solo las transacciones válidas son guardadas en el ledger principal de la red. En nuestro caso de uso veremos a menudo el uso de *endorsement policy* para manejar la lógica de validación entre partes que los requerimientos tienen; algunos ejemplos de esto son el acceso y la verificación de información, y la solicitud de eliminación de información, entre otros.

Membership Service Provider (MSP)

En una red permisionada como Fabric, cada participante de la red necesita ser validado para luego poder interactuar con esta. Para lograr esta validación, Fabric cuenta con el MSP, este servicio es el encargado de verificar la identidad de cada participante mediante su par de claves (pública/privada). A modo de ejemplo, un nodo que participa en la red, firma cada transacción con su clave privada, luego el MSP verifica la firma de la transacción con la clave pública del nodo, estableciendo si esta es válida o no y verificando si el participante es de confianza para el resto de la red.

Identities

Para Fabric cualquier actor dentro de la red es una identidad definida y verificada, estas identidades pueden verse como una abstracción de nodos, organizaciones, usuarios o cualquier participante interactuando con la red. Para lograr una correcta identificación de estas identidades, Fabric utiliza identidades digitales encapsuladas en un certificado X.509, mecanismo mediante el cual identifica exactamente a cada participante y provee insumos al MSP para manejar privacidad, integridad, control de acceso y otros aspectos relacionados a la seguridad de la red.

Autoridad de certificación (CA)

Para poder identificar cada entidad dentro de la red, manejar control de acceso y permisos, Fabric utiliza certificados digitales e infraestructura PKI, donde cada nodo puede usar su propia CA mediante el estándar X.509. A su vez, Fabric cuenta con su propia CA (FabricCA), una autoridad certificadora privada que utilizaremos en nuestro caso de uso por cuestiones de simplicidad.

Las Autoridades de Certificación (CA) son entidades de confianza responsables de emitir certificados digitales. Estos certificados asocian claves públicas con identidades de entidades, verificando así su autenticidad. En Fabric, las CA son fundamentales para garantizar que cada participante tenga una identidad digital verificada, lo cual es crucial para establecer la confianza dentro de la red. La autenticación de identidades mediante certificados digitales permite implementar controles de acceso eficaces, asegurando que solo los actores autorizados puedan realizar operaciones específicas. Fabric soporta el uso de Root CA (nivel más alto en la jerarquía de certificación) y son instancias de CA que emiten certificados para Autoridades de Certificación Intermedias (Intermediate CA) o, en algunos casos, directamente para los usuarios finales. El certificado de una Root CA es auto-firmado, lo que significa que ella misma verifica su propia identidad. Las Root CA son inherentemente de alta confianza, ya que forman la base de la cadena de confianza en cualquier sistema PKI. En Fabric, las Root CA son esenciales para establecer la confianza inicial en la red, proporcionando la raíz de la jerarquía de certificados que todos los participantes de la red deben reconocer y confiar.

Por otro lado, Fabric implementa su propia CA (Fabric CA) que funciona como una CA privada que puede emitir y gestionar certificados digitales para los participantes de la red, facilitando así la gestión de identidades, la autenticación y autorización. Fabric

CA ofrece varias características útiles, como la inscripción, renovación y revocación de certificados, lo que facilita la administración de las identidades digitales en la blockchain.

En otro orden, Fabric utiliza Infraestructura de Clave Pública (PKI), definiendo sobre esta base un conjunto de roles, políticas y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales. En Fabric, la infraestructura PKI proporciona el marco necesario para la emisión y gestión de certificados digitales por parte de las CA. Esto incluye la utilización de listas de revocación de certificados (CRL) para asegurar que los certificados comprometidos o inválidos no se puedan utilizar, lo que contribuye directamente a la integridad y al control de acceso dentro de la red.

Nodos (Peers)

Para Fabric, Nodo y Peer son términos equivalentes, en nuestro caso de uso los nodos que componen la red se pueden dividir en dos tipos:

1. Los Endorsing Peers son nodos "comunes", contienen una copia distribuida del ledger de la blockchain, agregando una capa de redundancia a la red. Varios nodos pueden compartir y ejecutar el mismo chaincode (smart contract). En nuestro caso de estudio, cada Bedelía (DP) dentro del sistema será un Endorsing Peer.

2. Por otro lado existen los Ordering Peers, son nodos encargados de ordenar las transacciones y crear los bloques de la red, escribiendo el ledger principal y administrando el consenso entre el resto de los nodos. Este tipo de nodos sirven para asegurar que las transacciones dentro de la red son ejecutadas con un orden correcto, además de ser el único nodo en la red capaz de actualizar el estado del ledger. Con este fin y dada la importancia que tienen este tipo de nodos en la red, es necesario que el Ordering Peer pertenezca a una entidad en la cual todos los otros nodos confían; en nuestro caso de uso, este nodo será administrado por el SECIU (DC).

Manejo de la privacidad en Fabric

Uno de los requerimientos del prototipo es lograr que la información sensible no sea expuesta en la blockchain. El trabajo de referencia recomienda el uso de un mecanismo de persistencia *off-chain* para lograr este nivel de privacidad de la información y su vez garantizar la integridad y trazabilidad de la misma.

Fabric ofrece dos mecanismos que pueden ser considerados con estas capacidades, dadas sus características y funcionalidades; estos son channels y private data. Ambos mecanismos garantizan que sólo entidades preautorizadas puedan acceder a la información que se busca proteger. Por ejemplo: en un channel, donde solo están asociadas las entidades `E1` y `E2`, los datos sólo pueden ser accedidos por éstas. Sin embargo, cualquier otra entidad `Ex` que conforme la red, no puede accederlos si no está dentro de ese channel.

En el caso de private data, el concepto de control de acceso es similar a los channels, pero private data ofrece un control de acceso aún más granular (a nivel del campo del dato, por ejemplo). Esto es denominado "colecciones", donde un objeto puede dejar como públicos ciertos datos y otros privados. Por otro lado, las colecciones de datos privados se definen mediante una política preestablecida, que dice que organizaciones dentro de un channel pueden leer y escribir estos datos, de modo que una orgnaización que no esté declarada en la política no podrá acceder a los datos por más que esta

pertenezca al mismo channel. Teniendo en cuenta estas alternativas, analizamos ambas variantes de Fabric con el fin de responder cómo son almacenados los datos, cómo se maneja el control de acceso en cada caso, y como se puede verificar la trazabilidad de la información.

- **Channels**: un uso común para los channels en Fabric es utilizarlos para agrupar transacciones de acuerdo a su tipo y también sirven en el caso de tener transacciones necesariamente privadas y solo visibles para entidades que pertenecen al mismo channel. La configuración de un channel en Fabric se almacena en su blockchain, esta configuración incluye, entre otros aspectos, las políticas, los miembros, las capacidades y las ACLs que rigen el comportamiento y el control de acceso dentro del channel.

  El bloque de génesis es el primer bloque de cualquier blockchain en Fabric y contiene la configuración inicial del channel. Este bloque es utilizado por todos los nodos que se unen al canal para entender la configuración inicial y las políticas que deben aplicar. A lo largo de la vida de un channel, la configuración puede necesitar ser actualizada; por ejemplo, para cambiar las políticas, añadir o remover organizaciones miembro, o actualizar las capacidades. Estas actualizaciones se realizan a través de transacciones de configuración que son enviadas al channel, y una vez aprobadas, resultan en un nuevo bloque de configuración que se añade a la blockchain del channel. La configuración dentro de estos bloques se estructura en forma de árbol, donde cada nivel del árbol representa diferentes aspectos de la configuración, como la configuración de la aplicación (que afecta a los nodos), la configuración del ordenador (que afecta al servicio de ordenamiento) y la configuración del channel (que afecta a ambos, nodos y ordenadores). Los bloques de configuración, al igual que otros, se almacenan de manera persistente en el ledger de cada nodo del channel. Esto significa que cada nodo participante del channel tiene una copia completa de la configuración del mismo y su historial de actualizaciones. Para modificar la configuración de un channel, los miembros deben proponer una transacción de configuración que cumpla con las políticas de gobernanza del channel establecidas en la configuración. Esta transacción debe ser aprobada por las partes necesarias según dichas políticas antes de ser aplicada y reflejada en un nuevo bloque de configuración.

- **Private Data**:

  En el caso de private data en Fabric, la configuración que gobierna estos datos se maneja de manera ligeramente diferente en comparación con la configuración general del channel. Los datos privados se refieren a la información que se comparte de manera confidencial entre subconjuntos específicos de organizaciones miembros del channel, y no se almacenan en el ledger principal de la blockchain en modo transparente. Los datos privados se organizan en çolecciones". Una colección define la política de privacidad para un conjunto de datos privados, es decir, especifica las organizaciones miembro que pueden tener acceso a los datos almacenados en esa colección.

  La configuración de las colecciones se especifica en la definición de chaincode (smart contract) en Fabric y se incluye como parte de la transacción de definición o actualización de chaincode. Esta configuración define aspectos como el nombre de la colección, las organizaciones que tienen acceso y las políticas que controlan. Esta configuración se almacena en el ledger del channel. Cada vez que se instala o actualiza un chaincode que utiliza datos privados, esta configuración se valida

y se aplica según las políticas de éste. Fabric gestiona un mecanismo de intercambio de datos privados entre los nodos autorizados para asegurar que todos tengan una vista consistente de los datos privados. Este mecanismo de "side database.º "ledger privado"permite a los nodos sincronizar los datos privados entre ellos, respetando las políticas de la colección y las restricciones de acceso. Cuando una transacción implica el uso de datos privados, la política de acceso definida en la configuración de la colección se verifica para asegurar que solo las organizaciones autorizadas puedan acceder a esos datos privados. Esto garantiza la confidencialidad y el control de acceso adecuado.

Aunque los datos privados en sí mismos se almacenan en un ledger privado separado al ledger principal, las políticas y configuraciones que gobiernan estos datos se mantienen en el ledger del channel para garantizar su consistencia y gobernabilidad a través de la red. Por más que los datos privados se almacenan de manera privada y segura en los nodos autorizados, su trazabilidad y las transacciones asociadas a ellos se registran en el ledger del channel de manera ofuscada para mantener la privacidad, este proceso permite que las transacciones que involucran datos privados sean verificables por todos los participantes del channel sin exponer el contenido real de esos datos. Esto se logra a través del hash de los datos privados, que se almacena en el ledger compartido visible por todos los participantes del channel. Como algoritmo de hashing, Fabric utiliza SHA-256 para la ofuscación de datos privados. El uso de este algoritmo asegura que el hash de los datos privados sea único y prácticamente imposible de revertir, lo que significa que no se puede deducir el contenido original de los datos a partir de su hash. Cuando se requiere validar o auditar una transacción que contiene datos privados, los participantes del canal pueden utilizar el hash almacenado en el ledger compartido para asegurar que los datos privados no han sido alterados. Los nodos autorizados que tienen acceso a los datos privados pueden calcular el hash de los datos almacenados en sus ledgers privados y compararlo con el hash registrado en el ledger compartido, asegurando así la integridad y la autenticidad de los datos privados.

La siguiente imagen 4.8 ilustra el contenido de cada uno de los ledgers de un par de nodos dentro de la red, uno con acceso a una colección de private data y otro no.

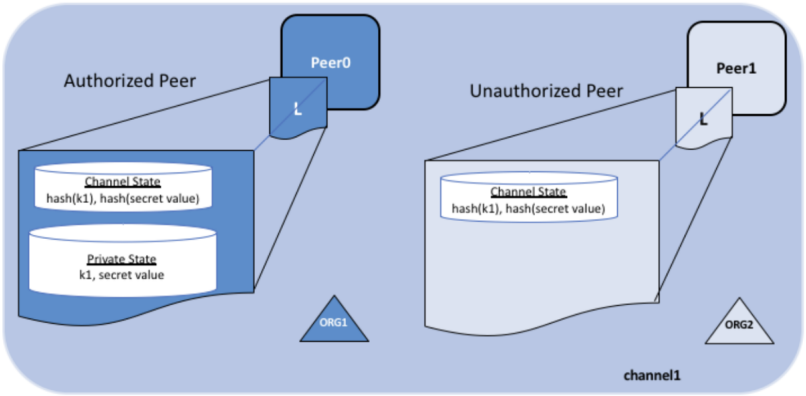

FIGURA 4.8: Fabric private data - Fuente: [Hyp24]

De acuerdo a lo ya mencionado en términos comparativos entre channels y private data en Fabric, la siguiente tabla 4.1 busca resaltar las principales diferecnias entre ambas opciones:

Criterio	Channels	Private Data
Privacidad	Ledger aislado completamente por channel. Todos los miembros del channel tienen acceso total al ledger.	Datos sensibles almacenados solo por un subconjunto específico. Otros nodos solo almacenan hashes.
Almacenamiento	Cada channel tiene su propio ledger completo. Puede generar duplicación de información y mayor consumo de recursos.	Solo nodos autorizados almacenan datos completos. Nodos no autorizados almacenan únicamente hashes. Menor uso de recursos.
Mantenimiento	Complejidad alta si la cantidad de channel aumenta. Configuración y gestión independientes son necesarias.	Menos complejo en comparación, ya que solo hay un channel principal y múltiples colecciones de datos privados dentro del mismo.
Escalabilidad	Menos escalable al aumentar channels; más nodos requieren mantener más copias del ledger.	Mejor escalabilidad, permite gestionar privacidad granular sin multiplicar channels.
Auditoría y validación	Dificultad alta para auditar datos a través de channels diferentes, ya que son completamente aislados.	Auditoría facilitada al permitir validación pública mediante hashes sin revelar información sensible.
Cumplimiento GDPR	Complejo, pues los datos personales se replican en todos los nodos del channel.	Simplifica cumplimiento al limitar almacenamiento explícito de datos personales a nodos autorizados.

CUADRO 4.1: Fabric - Comparativa entre Channels y Private Data

Teniendo en cuenta las diferencias y similitudes que existen entre channels y private data para el manejo en la privacidad de la información en Fabric, es que surge la pregunta sobre: ¿qué mecanismo utilizar en nuestro caso de uso? De acuerdo a la documentación de Fabric se recomienda:

1. Utilizar channels cuando: todas las transacciones y ledgers son solo accesibles para el grupo de entidades que componen el channel.

2. Utilizar private data cuando: las transacciones y ledgers pueden ser compartidas por un grupo de entidades, pero solo un subconjunto de estas entidades acceden a toda la información, mientras que el resto acceden solo a ciertos datos. Adicionalmente, y dado que los datos no se guardan en el ledger principal y si en los ledgers de cada nodo, se recomienda private data en casos donde la información debe mantenerse privada entre los nodos que definen la política.

Ahora bien, uno de los derechos de usuario dentro del marco normativo mencionado anteriormente es el "Derecho al olvido". Este derecho del usuario establece que en determinadas circunstancias un usuario puede solicitar la remoción de su informacion

personal contenida en un sistema. Este requerimiento representa un problema evidente para la caracterísitca inmutable de una blockchain, dado que una vez que el dato es persistido, no puede ser eliminado. Para este problema particular, el uso de private data ofrece una mejor forma de implementarlo en comparación a simplemente usar channels. Al usar private data en combinación con channels, hashes referenciales son guardados en el ledger principal, y la información original es persistida en un modelo *off-chain* dentro de una base de cada nodo y esta información si puede ser eliminada, manteniendo siempre el hash referencial en la blockchain principal.

4.3. Estructura del ledger y el world state en Fabric

En Fabric, el ledger (libro mayor) se compone de dos componentes fundamentales y complementarios: la **blockchain** propiamente dicho y el **world state**. Comprender su distinción es fundamental para analizar cómo se registran y acceden los datos en la red.

Blockchain (ledger histórico): La blockchain es una secuencia inmutable de bloques enlazados criptográficamente, donde cada bloque contiene un conjunto de transacciones ordenadas cronológicamente. Representa el historial completo de modificaciones realizadas sobre los registros de la red. Su estructura es .ªpend-only", lo que significa que los datos no pueden ser modificados ni eliminados una vez validados.

World state (estado actual): El world state representa el estado actual de todos los registros almacenados como pares clave–valor. A diferencia del ledger, es mutable: se actualiza con cada transacción válida aplicada a un registro. Este estado puede residir en una base de datos como LevelDB o CouchDB, siendo esta última especialmente útil para consultas complejas sobre documentos en formato JSON.

Consulta del ledger: El contenido de la blockchain puede consultarse mediante herramientas como:

- **Hyperledger Explorer:** interfaz gráfica que permite inspeccionar bloques, transacciones y metadatos de la red.
- **CLI de Fabric:** comandos como `peer channel fetch` permiten recuperar bloques específicos para su análisis local.
- **Chaincode:** funciones como `GetHistoryForKey()` permiten consultar la trazabilidad de un activo desde el propio smart contract.

Consulta del world state: Para acceder al estado actual de los registros, las opciones más utilizadas son:

- **CouchDB Web UI:** si el peer utiliza CouchDB como base de datos, es posible visualizar directamente los documentos del estado mundial accediendo a `http://localhost:5984/_utils/`.
- **Fabric SDK:** mediante funciones como `GetState()` o `GetPrivateData()`, se accede a datos públicos o privados asociados a una clave.
- **Consultas enriquecidas (rich queries):** disponibles solo cuando se utiliza CouchDB, permiten realizar búsquedas JSON complejas sobre el contenido del estado.

Característica	Blockchain (Ledger)	World State
Propósito	Registro histórico inmutable de todas las transacciones.	Representación del estado actual de los registros de la red.
Estructura	Secuencia de bloques de transacciones criptográficamente enlazados.	Base de datos de pares clave-valor (por ejemplo, LevelDB o CouchDB).
Acceso a datos	Acceso mediante comandos `peer` y herramientas de consulta del blockchain (CLI, Explorer, SDK).	Acceso mediante consultas directas a la base de datos (consulta de claves o datos completos).
Mutabilidad	Inmutable: los datos no pueden modificarse una vez registrados.	Mutable: puede actualizarse con cada transacción válida aplicada a los registros.
Consulta	Consultas de transacciones históricas.	Consultas rápidas de datos actuales.
Escalabilidad	Crece con cada transacción registrada. El tamaño puede aumentar rápidamente.	Escalable para grandes volúmenes de datos, pero depende de la base de datos seleccionada.
Privacidad	La privacidad se gestiona mediante canales privados y colecciones privadas de datos.	Los datos privados pueden almacenarse off-chain, mientras que solo los hashes se registran en la blockchain.

CUADRO 4.2: Fabric: Comparativa entre Blockchain (Ledger) y World State

4.3.1. World state y elección de CouchDB como base de datos

Fabric permite elegir entre dos motores de almacenamiento para el world state: **LevelDB** (por defecto) o **CouchDB**. Ambos cumplen la función de almacenar pares clave–valor, pero difieren significativamente en sus capacidades, especialmente en lo que respecta a aplicaciones que requieren modelos de datos más complejos o consultas avanzadas.

Ventajas de usar CouchDB En el prototipo desarrollado se eligió utilizar CouchDB como base de datos del world state debido a las siguientes razones técnicas:

- **Soporte nativo para documentos JSON**: CouchDB permite almacenar registros como documentos estructurados, lo cual se adapta naturalmente a la representación de prácticamente cualquier entidad con múltiples campos.
- **Consultas enriquecidas (rich queries)**: A diferencia de LevelDB, que solo permite búsquedas por clave o por rango, CouchDB permite realizar consultas complejas utilizando sintaxis JSON (por ejemplo, filtrar certificados por campos específicos como el nombre de un estudiante o la fecha de creación).
- **Acceso visual al estado**: CouchDB ofrece una interfaz web lo que permite inspeccionar manualmente el contenido del world state durante pruebas y auditorías.

- **Definición de índices personalizados**: es posible optimizar el rendimiento de consultas mediante la definición de índices secundarios (con `indexes`), algo no disponible en LevelDB.

Estas capacidades permiten desarrollar funcionalidades más completas y eficientes, especialmente útiles en entornos académicos donde se espera poder buscar, validar y consultar certificados de forma flexible, auditada y estructurada.

4.4. Implementación del chaincode

Esta sección describe la implementación del chaincode (smart contract) desarrollado para la gestión de certificados académicos digitales en una red blockchain basada en Fabric. Este chaincode forma parte del prototipo descrito en el capítulo 4.1 y está diseñado para cumplir con los requerimientos funcionales y no funcionales establecidos, incluyendo la protección de datos personales, la trazabilidad de las operaciones y el cumplimiento normativo. El chaincode implementa funcionalidades clave como el registro, consulta, actualización, eliminación y verificación de certificados digitales, utilizando colecciones privadas para garantizar la confidencialidad de los datos sensibles. En adelante, y dado que los términos chaincode y smart contract son sinónimos, podremos verlos utilizados indistintamente para referirnos a lo mismo.

4.4.1. Estructura del chaincode

La carpeta chaincode está compuesta por los siguientes componentes:

- **Archivo principal**: `digitalCertificateManagement.ts`

  Este archivo contiene la lógica del smart contract *(DigitalCertificateManagementContract)* y define las operaciones que pueden realizarse sobre los certificados digitales. Cada método implementado en este archivo está diseñado para cumplir con un requerimiento específico del sistema.

- **Modelo de datos**: `certificate.ts`

  Define la estructura de los certificados digitales que se almacenan en la blockchain. Este modelo incluye propiedades como:

  - **id**: identificador único del certificado.
  - **userId**: identificador del usuario asociado al certificado.
  - **owner**: organización propietaria del certificado.
  - **accessControl**: lista de usuarios con permisos de acceso al certificado.
  - **data**: información del certificado.
  - **createdTimeStamp** y **updateTimeStamp**: marcas de tiempo de creación y actualización.
  - **createdTxID** y **updatedTxID**: identificadores de las transacciones asociadas.

- **Configuración de colecciones privadas**: `collections-config.json`

  Este archivo define las colecciones privadas utilizadas por el chaincode, en el anexo A.4 puede encontrarse el detalle de cada configuración:

  - **collectionPrivateAssets**: almacena los certificados digitales de forma confidencial.

- **collectionAuditLogs**: registra las auditorías de las operaciones realizadas en el sistema.

4.4.2. Funcionalidades del chaincode

Registro de certificados

- Método: `RegisterCertificate`
- Descripción: permite registrar un nuevo certificado en la colección privada.
- Implementación:
  - Verifica que el usuario tenga permisos de escritura o sea administrador.
  - Almacena el certificado en la colección privada.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.

Consulta de certificados

- Método: `GetCertificateById`
- Descripción: permite consultar un certificado específico almacenado en la colección privada.
- Implementación:
  - Recupera el certificado desde `collectionPrivateAssets`.
  - Valida que el usuario tenga permisos de acceso (propietario o en la lista de control de acceso).
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.
- Método: `GetAllCertificates`
- Descripción: permite a los administradores consultar todos los certificados almacenados.
- Implementación:
  - Restringe el acceso a usuarios con rol de administrador.
  - Recupera todos los certificados del ledger.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.

Actualización de certificados

- Método: `UpdateCertificateById`
- Descripción: permite actualizar los datos de un certificado existente.
- Implementación:
  - Verifica que el usuario sea administrador.
  - Actualiza los datos del certificado.
  - Almacena el certificado actualizado en la colección privada.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.

Eliminación de certificados

- Método: `DeleteCertificateById`
- Descripción: permite eliminar un certificado de la colección privada.
- Implementación:
  - Verifica que el usuario sea administrador.
  - Elimina el certificado de `collectionPrivateAssets`.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.

Gestión de acceso

- Método: `GrantCertificateAccess`
- Descripción: permite otorgar acceso a un usuario para un certificado específico.
- Implementación:
  - Verifica que el usuario que realiza la operación sea el propietario del certificado o un administrador.
  - Agrega el usuario a la lista de control de acceso del certificado.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.
- Método: `RemoveCertificateAccess`
- Descripción: permite revocar el acceso de un usuario a un certificado.
- Implementación:
  - Verifica que el usuario que realiza la operación sea el propietario del certificado o administrador.
  - Elimina el usuario de la lista de control de acceso.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.

Verificación de certificados

- Método: `GetCertificatePrivateDataHash`
- Descripción: permite obtener el hash de datos de un certificado desde la colección privada.
- Implementación:
  - Verifica que el usuario que realiza la operación sea el propietario del certificado o un administrador.
  - Recupera el hash del certificado desde la colección privada.
  - Registra la operación en la colección de auditoría `collectionAuditLogs`.
- Método: `VerifyCertificateById`
- Descripción: permite verificar la autenticidad de un certificado mediante su hash.
- Implementación:

- Recupera el certificado desde la colección privada.
- Compara el hash proporcionado por el usuario con el hash almacenado en la colección privada mediante el método `getPrivateDataHash`.
- Registra la operación en la colección de auditoría `collectionAuditLogs`.

Auditoría

- Método: `LogAudit`
- Descripción: registra las operaciones realizadas en el sistema en la colección privada `collectionAuditLogs`.
- Implementación:
  - Almacena detalles como la acción realizada, el ID del certificado, el usuario que realizó la operación, la marca de tiempo y el ID de la transacción.

Inicialización del ledger

- Método: `InitLedger`
- Descripción: Inicializa el ledger con datos de prueba.
- Implementación:
  - Registra certificados de ejemplo en la colección privada `collectionPrivateAssets`.

El chaincode implementado cumple con los requerimientos establecidos en el documento principal. Cada componente y funcionalidad ha sido diseñado para garantizar la seguridad, privacidad y trazabilidad de los certificados digitales, utilizando las capacidades avanzadas de Fabric, como colecciones privadas y políticas de acceso granular. Este diseño no solo aborda los desafíos técnicos de la gestión de certificados digitales, sino que también asegura el cumplimiento normativo y la protección de los derechos de los titulares de los datos.

4.5. Implementación del Gateway de Aplicación

El gateway de aplicación es un componente clave en la arquitectura del prototipo, ya que actúa como intermediario entre los usuarios del sistema y la red blockchain. Este módulo gestiona las solicitudes de los actores definidos en el sistema (Data Controller, Data Processor, Data Owner y Receiver) y las traduce en transacciones hacia el chaincode desplegado en Fabric. Además, implementa políticas de acceso y comunicación segura con el almacenamiento off-chain. Por simplicidad, en nuestro prototipo todas las operaciones relacionadas a la gestión de certificados están implementadas en este componente utilizando el gateway en modo çliente".

4.5.1. Estructura del Gateway

La carpeta application-gateway contiene los siguientes archivos:

- `utils.ts`: contiene funciones auxiliares para establecer conexiones con la red blockchain y manejar identidades.

- `config.ts`: define las configuraciones necesarias para conectarse a la red blockchain.
- Funcionalidades: este componente también cuenta con varios archivos que permiten ejecutar los métodos del chaincode para la administración de certificados digitales, estas se listan a continuación.

4.5.2. Funcionalidades del Gateway

Registro de certificados

- Chaincode utilizado: `RegisterCertificate` 4.4.2
- Método del gateway: `createCertificate.ts`
- Descripción: permite registrar un nuevo certificado en la red blockchain. Los datos sensibles del certificado se almacenan off-chain, mientras que un hash criptográfico se registra en la blockchain para garantizar la integridad de los datos.

Edición de certificados

- Chaincode utilizado: `UpdateCertificateById` 4.4.2
- Método del gateway: `editCertificate.ts`
- Descripción: permite editar los datos de un certificado existente.

Eliminación de certificados

- Chaincode utilizado: `DeleteCertificateById` 4.4.2
- Método del gateway: `deleteCertificate.ts`
- Descripción: permite eliminar los datos de un certificado existente.

Otorgar acceso a certificados

- Chaincode utilizado: `GrantCertificateAccess` 4.4.2
- Método del gateway: `grantCertificateAccess.ts`
- Descripción: permite otorgar acceso a un Receiver (R) para verificar un certificado específico.

Revocar acceso a certificados

- Chaincode utilizado: `RemoveCertificateAccess` 4.4.2
- Método del gateway: `removeCertificateAccess.ts`
- Descripción: permite remover el acceso de un Receiver a un certificado.

Obtener un certificado

- Chaincode utilizado: `GetCertificateById` 4.4.2
- Método del gateway: `getCertificate.ts`
- Descripción: permite obtener los datos de un certificado existente.

Obtener el hash de un certificado

- Chaincode utilizado: `GetCertificatePrivateDataHash` 4.4.2
- Método del gateway: `getCertificateHash.ts`
- Descripción: permite obtener el hash de datos de un certificado existente.

Consulta de logs de auditoría

- Chaincode utilizado: `GetAuditLogsByCertificateId` 4.4.2
- Archivo: `getAuditLogs.ts`
- Descripción: permite consultar los registros de auditoría relacionados con un certificado.

La implementación del Gateway cumple con los requerimientos funcionales y no funcionales establecidos ya definidos. Este componente actúa como un puente seguro entre los usuarios y la red blockchain, garantizando la privacidad, seguridad y trazabilidad de las operaciones. Además, su diseño modular y flexible permite futuras extensiones y adaptaciones según las necesidades del sistema.

4.6. Implementación del Receiver

La aplicación Receiver contiene la lógica necesaria para que usuarios externos (como los Receivers, definidos en los componentes del sistema 4.2.1) interactúen con la red blockchain. Este módulo permite realizar operaciones como la verificación de certificados, la gestión de identidades (registro y eliminación de usuarios) y la configuración de la conexión con la red blockchain.

4.6.1. Estructura del Receiver

La carpeta third-party contiene los siguientes archivos:

- `enrollAdmin.ts`: Registra un usuario con permisos de administrador en la red blockchain, utilizando la CA para generar un certificado que se persiste en la carpeta wallet. Este usuario será posteriormente utilizado para poder crear el usuario Receiver.
- `enrollUser.ts`: Registra un usuario en la red blockchain con rol de Receiver, mediante el mismo mecanismo que el anterior. Este nuevo usuario solo podrá acceder a verificar certificados en la red y previamente deberá contar con acceso para cada certificado vaya a verificar.
- `removeUser.ts`: De manera opuesta al método anterior, elimina un usuario en la red blockchain revocando su identidad de la CA.
- `verifyCertificate.ts`: Permite verificar la autenticidad de un certificado comparando su hash con el almacenado en la blockchain, utilizando para esto el método `VerifyCertificateById` del chaincode.
- `CA.ts`: Define las funciones necesarias para interactuar con la CA de Fabric, dando soporte a los métodos mencionados anteriormente.
- `config.ts`: Define las configuraciones y parámetros necesarios para interacturar con la red.

4.7. Despliegue del prototipo

En esta sección se describen los pasos necesarios para poder desplegar la red, con su configuración y los smart contracts. Para llevar adelante el despliegue del prototipo en un entorno controlado, se configuró una red Hyperledger Fabric en modo local utilizando la herramienta oficial Fabric Test Network provista por Hyperledger. Esto permitió simular condiciones cercanas a producción, facilitando la evaluación y validación de los requerimientos establecidos previamente.

4.7.1. Configuración del entorno

Para establecer el entorno de desarrollo local se utilizó Docker como herramienta para la creación y manejo de contenedores, siguiendo la documentación oficial de Hyperledger Fabric [Hyp24]. Los componentes esenciales desplegados en contenedores fueron los nodos peers, orderers, y autoridades certificadoras (CA), además de la base de datos CouchDB para permitir consultas avanzadas en el ledger. La figura 4.9 ilustra la estructura del entorno.

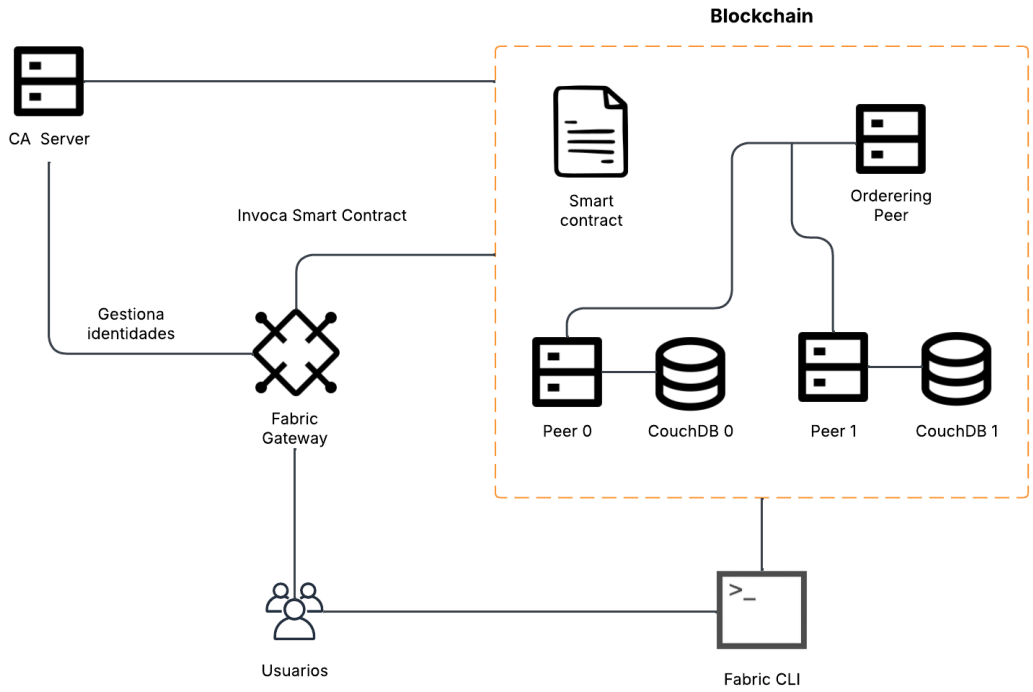

FIGURA 4.9: Entorno Fabric Docker

4.7.2. Instalar dependencias

- **Docker:** Necesario para ejecutar los contenedores que soportan la red de Hyperledger Fabric. Disponible en: `https://docs.docker.com/get-docker/`.
- **Docker compose:** Utilizado para definir y administrar aplicaciones multi-contenedor. Disponible en: `https://docs.docker.com/compose/install/`.
- **Node.js y NPM:** Necesarios para desarrollar y compilar smart contract en JavaScript o TypeScript. Disponible en: `https://nodejs.org/`.

- **CLI de Hyperledger Fabric:** Descargamos herramientas CLI de Farbic y las imágenes de Docker necesarias:

```
curl -sSL https://bit.ly/2ysbOFE | bash -s
```

4.7.3. Clonar el repositorio del prototipo

En este paso se debe clonar el repositorio del prototipo para obtener scripts y configuraciones predeterminadas. Este repositorio incluye también los smart contracts con la lógica de la aplicación.

```
git clone https://gitlab.fing.edu.uy/gsi/blockchain/titulos-
    electronicos
```

4.7.4. Primeros pasos

En la carpeta `/network/test-network` podemos encontrar el script `network.sh` que viene con la red de prueba de Fabric. Este script resulta de gran utilidad al momento de inicializar la red, conteniendo funcionalidades como: crear channels, compilar e instalar los smart contracts y configurar las colecciones de datos privadas, entre otros. La forma en la que el script realiza todas estas acciones es utilizando interiormente el CLI provisto por Fabric, generando una abstracción al usuario para facilitar los pasos mencionados. Para obtener mayor información también cuenta con un comando de ayuda:

```
./network.sh -h
```

4.7.5. Inicializar la red del prototipo

En este paso se crea un canal llamado `mychannel` y se inicia la red de prueba. Se incluye también la instalación de certificados, y la configuración inicial de la red utilizando CouchDB como motor de base de datos.

```
./network.sh up createChannel -c mychannel -ca -s couchdb
```

4.7.6. Instalar y desplegar el chaincode

Desplegamos el chaincode con la lógica del prototipo en el canal previamente creado. A su vez, este paso establece la configuración de las colecciones de datos privadas utilizadas para el manejo de los certificados.

```
./network.sh deployCC \
  -ccl typescript \
  -ccn basic \
  -ccp ../../chaincode \
  -ccv 1.0 \
  -ccs 1 \
  -cci InitLedger \
  -cccg ../../chaincode/collections-config.json
```

4.7.7. Fabric monitor

El monitor es una aplicación útil que para poder realizar debug y monitoreo de la red en tiempo real, este debe correr en una terminal independiente al proceso de red.

```
./monitordocker.sh fabric_test
```

4.7.8. Interactuar con la red

Una vez desplegada la red, Fabric permite la ejecución de diversas operaciones mediante la interfaz de cliente (CLI) [Hyp24], como por ejemplo interactuar con el chaincode al igual que lo hacen las funcionalidades provistas en el gateway 4.5.2. El CLI de Fabric resulta especialmente util para realizar configuraciones y pruebas al momento de trabajar con el chaincode sin necesidad de volver a realizar un depliegue completo. Del mismo modo que el gateway invoca al chaincode, el CLI permite interacciones para registrar certificados académicos, verificarlos y revocar permisos de acceso, a continuación vemos algunos ejemplos de esto.

Verificar el chaincode: para poder interacutar como un nodo a través del CLI de Fabric es necesario setear previamente algunas variables de consola con el fin de simplificar algunas ejecuciones posteriores:

```
export PATH=${PWD}/../bin:$PATH
export FABRIC_CFG_PATH=$PWD/../config/
export CORE_PEER_TLS_ENABLED=true
export CORE_PEER_LOCALMSPID="Org1MSP"
export PEER0_ORG1_CA=${PWD}/organizations/peerOrganizations/org1.
   example.com/tlsca/tlsca.org1.example.com-cert.pem
export PEER0_ORG2_CA=${PWD}/organizations/peerOrganizations/org2.
   example.com/tlsca/tlsca.org2.example.com-cert.pem
export CORE_PEER_MSPCONFIGPATH=${PWD}/organizations/peerOrganizations
   /org1.example.com/users/Admin@org1.example.com/msp
export CORE_PEER_ADDRESS=localhost:7051
export TLS_ROOT_CA=${PWD}/organizations/ordererOrganizations/example.
   com/tlsca/tlsca.example.com-cert.pem
export CERT_ID="crt-1"
```

Una vez hecho esto podemos hacer consultas a la red interactuando como un nodo de esta, por ejemplo para ver la version del nodo o listar la version del chaincode instalado previamente:

```
peer version
peer lifecycle chaincode queryinstalled
```

Registro de certificados: para registrar un nuevo certificado académico, la entidad emisora (como una universidad) utiliza una interfaz de cliente para enviar una transacción a la red. La transacción incluye los datos del certificado, que se almacenan off-chain, mientras que el hash de dicho certificado se guarda en el ledger de la blockchain. Esta operación está sujeta a las políticas de validación definidas por el Membership Service Provider (MSP), asegurando que solo las entidades autorizadas puedan realizar este registro.

```
peer chaincode invoke \
  -o localhost:7050 \
```

```
  --tls \
  --cafile $TLS_ROOT_CA \
  --ordererTLSHostnameOverride orderer.example.com \
  -C mychannel \
  -n basic \
  --peerAddresses localhost:7051 --tlsRootCertFiles $PEER0_ORG1_CA \
  --peerAddresses localhost:9051 --tlsRootCertFiles $PEER0_ORG2_CA \
  -c "{\"function\":\"RegisterCertificate\",\"Args\":[\"<data>\",\"
     $CERT_ID\"]}"
```

Verificación de certificados: los interesados en verificar la autenticidad de un certificado deberán tener autorización previa del propietario del certificado. Para verificarlo, se envía una transacción de consulta a la red, recuperando el hash del certificado almacenado en el ledger y comparándolo con el hash proporcionado por el solicitante. Si coinciden, se confirma la autenticidad del certificado.

```
peer chaincode invoke \
  -o localhost:7050 \
  --tls \
  --cafile $TLS_ROOT_CA \
  --ordererTLSHostnameOverride orderer.example.com \
  -C mychannel \
  -n basic \
  --peerAddresses localhost:7051 --tlsRootCertFiles $PEER0_ORG1_CA \
  --peerAddresses localhost:9051 --tlsRootCertFiles $PEER0_ORG2_CA \
  -c '{"function":"VerifyCertificateById","Args":["<userId>","<
     certificateId>","<providedHash>"]}'
```

Revocación de certificados: si un certificado necesita ser revocado, el propietario o la entidad emisora pueden iniciar una transacción de revocación. Esta operación invalida el certificado en la red blockchain, evitando que sea utilizado o verificado en el futuro.

```
peer chaincode invoke \
  -o localhost:7050 \
  --tls \
  --cafile $TLS_ROOT_CA \
  --ordererTLSHostnameOverride orderer.example.com \
  -C mychannel \
  -n basic \
  --peerAddresses localhost:7051 --tlsRootCertFiles $PEER0_ORG1_CA \
  --peerAddresses localhost:9051 --tlsRootCertFiles $PEER0_ORG2_CA \
  -c '{"function":"RegisterCertificate","Args":["<data>","<
     certificateId>"]}'
```

Gestión de permisos: los estudiantes (Data Owners), pueden gestionar los permisos de acceso a sus certificados. Un estudiante puede conceder o revocar permisos a terceros, como potenciales empleadores, para que verifiquen sus títulos. Esto se realiza mediante la invocación de transacciones que actualizan las políticas de acceso de los canales donde están registrados los certificados.

```
peer chaincode invoke \
  -o localhost:7050 \
  --tls \
  --cafile $TLS_ROOT_CA \
```

```
  --ordererTLSHostnameOverride orderer.example.com \
  -C mychannel \
  -n basic \
  --peerAddresses localhost:7051 --tlsRootCertFiles $PEER0_ORG1_CA \
  --peerAddresses localhost:9051 --tlsRootCertFiles $PEER0_ORG2_CA \
  -c '{"function":"GrantCertificateAccess","Args":["<userId>","<
      certificateId>"]}'
```

Cada interacción con la red es registrada en el ledger inmutable de la blockchain, garantizando la trazabilidad de todas las operaciones realizadas sobre los certificados académicos. Además, dado que Hyperledger Fabric es una red permisionada, todas las transacciones están validadas por los nodos autorizados en base a las políticas de acceso definidas, lo que asegura un alto nivel de control sobre los datos y las entidades participantes.

4.7.9. Bajar la red

```
./network.sh down
```

4.7.10. Documentación completa

Tanto el código de cada uno de los componentes del prototipo detallados anteriormente como los elementos básicos utilizados para dar funcionamiento a la red, pueden ser encontrados en el Anexo A.1

Capítulo 5

Resultados y análisis

Esta sección presenta la evaluación del prototipo desarrollado para la gestión de certificados académicos digitales. Se describen las pruebas realizadas, destacando la eficiencia del sistema en la emisión y verificación de certificados con garantías criptográficas de integridad y autenticidad. Se analizan los resultados obtenidos, subrayando las fortalezas en seguridad y protección de datos personales, pero también identificando desafíos como la escalabilidad y la complejidad de cumplir con el derecho al olvido. Finalmente, se discuten las ventajas del enfoque propuesto, así como las limitaciones y posibles áreas de mejora para futuras implementaciones.

5.1. Evaluación del prototipo

En esta sección se busca realizar una evaluación del modelo de seguridad sobre el prototipo implementado en Fabric, analizando varios aspectos sobre la seguiridad de la red, la privacidad y la integridad de la informaición. Para esto, ademas de la experiencia en la implementación del prototipo se utilizaron trabajos previos [BK21] y reportes de auditoría en seguridad realizados sobre Fabric [CD21].

5.1.1. Metodología de evaluación

La evaluación del prototipo se centró en tres dimensiones clave alineadas con los objetivos del trabajo: (i) control de acceso (ii) confidencialidad y privacidad, y (iii) trazabilidad y validación. Para cada dimensión, se diseñaron escenarios de prueba ejecutados sobre la red Fabric configurada localmente, utilizando nodos distribuidos entre dos organizaciones simuladas.

5.1.2. Pruebas realizadas

Para mayor detalle sobre los scripts utilizados en las pruebas realizadas, se puede consultar la carpeta test dentro del repositorio.

- **Control de acceso:** se verificó que solo los usuarios autorizados mediante la colección de datos privados (Private Data Collection) pudieran acceder al contenido del certificado. Se utilizó el comando `GetPrivateData()` desde nodos autorizados y se comprobó que los nodos no autorizados solo podían consultar el `hash` correspondiente mediante `GetPrivateDataHash()`. El control de acceso se implementa principalmente en el smart contract DigitalCertificateManagementContract. La función `GetCertificatePrivateDataHash()` valida que solo los usuarios autorizados puedan acceder al hash de los datos privados de un certificado. Esto se logra verificando si el usuario es el propietario del certificado, tiene permisos explícitos en la lista de control de acceso (accessControl), o es un

administrador. Si no cumple con estas condiciones, se lanza un error de acceso denegado. Además, en el archivo getCertificateHash.ts , se proporciona un ejemplo de cómo un cliente puede interactuar con esta función para evaluar el acceso y obtener el hash del certificado.

- **Confidencialidad y privacidad:** se evaluó que los datos personales sensibles no fueran visibles en el ledger global ni a través de los peers no autorizados. Además, se validó que los certificados eran almacenados off-chain y solo se registraban sus referencias criptográficas en Fabric, conforme a lo propuesto en la arquitectura. La confidencialidad y privacidad de los datos se garantizan mediante el uso de la colección privada `collectionPrivateAssets`, definida en el archivo collections-config.json. Los certificados se almacenan off-chain en esta colección, y solo se registran sus referencias criptográficas en el ledger global. La función RegisterCertificate en el smart contract asegura que los datos sensibles se almacenen correctamente en la colección privada. Además, el archivo createCertificate.ts permite a los clientes registrar certificados siguiendo esta arquitectura, asegurando que los datos sensibles no sean visibles para peers no autorizados.

- **Trazabilidad y validación:** se verificó que cualquier intento de modificación o validación incorrecta del certificado resultara en una inconsistencia al comparar el hash del dato original con el almacenado en la blockchain. Esto garantiza la integridad del dato emitido. La trazabilidad y validación se implementan mediante la comparación del hash criptográfico del certificado almacenado en la blockchain con el proporcionado por el usuario. La función VerifyCertificateById en el smart contract realiza esta validación, asegurando que cualquier intento de modificación o validación incorrecta sea detectado. En el archivo verifyCertificate.ts, se encuentra un ejemplo de cómo un cliente externo puede interactuar con esta funcionalidad para verificar la integridad de un certificado. Esto garantiza que los datos emitidos mantengan su integridad en la red blockchain.

5.1.3. Resultados obtenidos

Los resultados obtenidos indican que el sistema cumple con los requerimientos funcionales establecidos. Las pruebas demostraron:

- **Control de acceso y autenticación**: Que el acceso a la información personal está estrictamente limitado a los participantes definidos en las políticas de la colección privada. Las pruebas confirmaron que los controles de acceso basados en roles (RBAC) y las políticas de acceso granular definidas en el prototipo previenen efectivamente el acceso no autorizado a datos sensibles. Solo los usuarios con permisos específicos pueden realizar acciones como emitir, acceder, revocar o verificar certificados.

- **Privacidad y cumplimiento con GDPR**: Que la validación de certificados por parte de terceros puede realizarse sin exponer la información del titular, garantizando privacidad. El uso de channels y colecciones de datos privados en Fabric permitió asegurar que los datos personales solo fueran accesibles por las partes relevantes, cumpliendo con los requisitos de minimización y acceso restringido de GDPR. Sin embargo, se identificaron posibles mejoras en la implementación de mecanismos, como la gestión del derecho al olvido, que podrían ser objeto de desarrollo futuro.

- **Seguridad de red**: Que los peers no autorizados no pudieron acceder al contenido de los certificados. Los mecanismos de comunicación en Fabric, incluyendo el uso de TLS, demostraron ser robustos frente a ataques de interceptación, asegurando que todas las comunicaciones entre los nodos de la red están cifradas y son autenticadas, previniendo ataques man-in-the-middle entre otros.

5.2. Amenazas y modos de mitigación

5.2.1. Amenazas identificadas

- **Ataques de Sybil**: dado que el sistema está basado en una red blockchain, existe el riesgo de que actores maliciosos intenten crear múltiples identidades falsas para tomar control de la red o influir en la validación de transacciones.
- **Filtración de datos sensibles**: aunque la blockchain proporciona un alto nivel de seguridad, las aplicaciones que interactúan con ella podrían ser vulnerables a ataques que expongan datos sensibles, especialmente durante el proceso de emisión o verificación de certificados.
- **Ataques de denegación de servicio (DoS)**: un atacante podría intentar sobrecargar el sistema con un volumen elevado de solicitudes maliciosas, lo que podría degradar el rendimiento del sistema y afectar la disponibilidad de los servicios.
- **Compromiso de claves criptográficas**: la seguridad del sistema depende en gran medida de la protección de las claves criptográficas. La pérdida o el compromiso de estas claves podría permitir el acceso no autorizado a la información y la manipulación de certificados.

5.2.2. Medidas de mitigación

- **Protección contra ataques de Sybil**: Fabric establece requisitos estrictos para la validación de identidades y el registro en la red blockchain, utilizando mecanismos de concenso como CFT o BFT y técnicas de verificación de identidad mediante la Autoridad Certificadora para asegurar la legitimidad de los participantes.
- **Seguridad de aplicaciones**: Fabric permite implementar chaincode en lenguajes modernos y conocidos, permitiendo así adoptar prácticas de desarrollo seguro, como la validación rigurosa de entradas y la protección contra vulnerabilidades comunes (e.g., inyección de SQL, XSS). Además, se implementan capas adicionales de seguridad y controles de acceso para asegurar que las aplicaciones que interactúan con la blockchain manejen los datos sensibles de manera segura. Por otro lado, la liberación del chaincode a la red está atado a políticas que todas las organizaciones acuerdan previamente, permitiendo establecer así un alto nivel de confianza en la lógica de negocio ejecutada.
- **Protección contra ataques DoS**: Fabric ofrece características para resistir contra ataques de denegación de servicio (DoS) gracias a su arquitectura permisionada y mecanismos de control de acceso. Al requerir que todos los participantes estén validados mediante el Membership Service Provider (MSP), se limita el acceso solo a actores autorizados, lo que reduce drásticamente la superficie de ataque. Además, el uso de políticas de endoso distribuye la carga de validación entre varios nodos, evitando la saturación de un solo punto en la red. Esto asegura que, incluso bajo un ataque, la red pueda seguir funcionando de manera eficiente. Otra

característica clave es el uso de canales privados, que aísla las transacciones y datos entre diferentes grupos de participantes. Esto significa que un ataque dirigido a un canal no afectará a otros, protegiendo la integridad y disponibilidad del sistema global. Además, Fabric permite configurar la tasa de solicitudes (throttling), controlando la cantidad de peticiones que un nodo puede procesar en un tiempo determinado, lo cual es esencial para mitigar intentos de saturación. Finalmente, el mecanismo de ordenamiento centralizado en Fabric permite agrupar y procesar transacciones de manera eficiente, mientras que las capacidades avanzadas de monitoreo y logging permiten detectar y bloquear comportamientos sospechosos en tiempo real, minimizando el impacto de un ataque DoS.

- **Gestión segura de claves criptográficas**: Fabric permite el uso de HSMs (Hardware Security Modules) para la generación y almacenamiento seguro de claves criptográficas. Además, se pueden establecer políticas de rotación regular de claves y procedimientos de respuesta ante incidentes en caso de compromisos de seguridad.

5.3. Discusión de los resultados

5.3.1. Ventajas del sistema propuesto

- **Alta seguridad e inmutabilidad**: Fabric garantiza la inmutabilidad de los certificados académicos, proporcionando una seguridad robusta contra la manipulación de datos. Además, las medidas adicionales, como el control de acceso y las políticas, aseguran un alto grado de protección contra amenazas comunes.
- **Protección de la privacidad**: el enfoque en la conformidad con GDPR y las medidas de protección de datos implementadas aseguran que los datos personales estén bien protegidos, respetando los derechos de los usuarios a la privacidad y la protección de su información.
- **Trazabilidad y auditoría**: cada operación realizada en la blockchain es completamente rastreable, lo que facilita auditorías de seguridad y configura la transparencia del sistema. Esto es especialmente valioso en contextos académicos, entre otros, donde la integridad de los registros es crítica.

5.3.2. Limitaciones y desafíos

A pesar de las ventajas que ofrece Fabric para la gestión de certificados académicos digitales, es importante reconocer ciertas limitaciones y desafíos que afectan tanto la escalabilidad como el rendimiento de la solución, así como otros aspectos relacionados con la privacidad y la interoperabilidad.

- **Cumplimiento normativo y privacidad**: si bien Fabric permite un control granular de los datos a través de canales privados y colecciones de datos privados, la gestión de estos datos sensibles fuera de la blockchain (off-chain) plantea desafíos adicionales. En particular, la implementación de un sistema que cumpla con GDPR y la Ley Nº 18.331 implica garantizar que los usuarios puedan ejercer derechos como el "derecho al olvido", lo que representar una complejidad adicional en una infraestructura distribuida donde los datos son pseudo-anonimizados a través de hashes. Fabric permite configurar el parámetro `blockToLive` dentro

de las colecciones privadas, el cual define cuántos bloques permanecerán almacenados los datos en la base de datos privada del peer (SideDB) antes de ser automáticamente eliminados. Esto otorga un mecanismo de eliminación temporal que puede considerarse una forma de atenuar la retención innecesaria de datos sensibles. Sin embargo, incluso cuando los datos privados son eliminados del almacenamiento local de los peers, sus *hashes* criptográficos permanecen de forma inmutable en el ledger público. Aunque estos hashes no contienen los datos en sí, en ciertos contextos podrían ser considerados datos pseudonimizados en el contexto de GDPR, especialmente si pueden ser vinculados con el titular mediante otras fuentes. Debido a la naturaleza inmutable de la cadena, estos elementos no pueden eliminarse ni modificarse. En consecuencia, se concluye que si bien Fabric ofrece mecanismos útiles para cumplir parcialmente con el derecho al olvido, no garantiza su cumplimiento pleno.

- **Riesgos de centralización**: aunque la blockchain está diseñada para ser descentralizada, la implementación de medidas de seguridad estrictas podría, en algunos casos, conducir a una centralización indeseada, donde un pequeño grupo de nodos tiene más control sobre la red que otros, lo mismo ocurre con la autoridad certificadora (CA), es claro en este punto que debe haber un nivel de confianza pre-definido para la gobernabilidad de la red.

- **Escalabilidad**: una de las limitaciones más significativas de las redes basadas en Hyperledger Fabric es su escalabilidad. Aunque Fabric permite manejar una cantidad considerable de transacciones, el aumento en el número de instituciones académicas, certificados emitidos y solicitudes de verificación puede afectar el rendimiento general de la red. La estructura modular de Fabric y el uso de canales privados, si bien son beneficiosos para la privacidad, pueden convertirse en un obstáculo para la escalabilidad debido a la sobrecarga administrativa de gestionar múltiples canales y políticas de acceso. Además, el proceso de consenso en Fabric, aunque es eficiente en términos de rendimiento comparado con otros mecanismos como Proof of Work, todavía puede experimentar latencias cuando se maneja un gran número de transacciones simultáneas. La necesidad de obtener el endoso de múltiples participantes en canales específicos puede ralentizar el procesamiento, especialmente si las políticas de consenso están mal optimizadas o si se requiere la participación de muchos nodos.

- **Rendimiento**: otro desafío importante es el rendimiento en términos de velocidad de procesamiento de transacciones y la latencia en la respuesta. A medida que aumenta el volumen de transacciones (por ejemplo, cuando múltiples instituciones académicas registran o verifican certificados al mismo tiempo), el rendimiento de la red puede degradarse. Aunque Fabric permite configuraciones como el algoritmo de consenso Raft, que es más ligero que otros, sigue siendo susceptible a la congestión cuando la carga de trabajo se incrementa considerablemente. Un aspecto adicional a considerar es el uso intensivo de recursos en los nodos participantes. La necesidad de replicar el ledger entre varios nodos y procesar las transacciones en cada uno de ellos puede generar un aumento en el consumo de almacenamiento y capacidad de procesamiento, lo que eventualmente puede requerir una infraestructura más robusta para mantener el sistema funcionando de manera óptima.

- **Costos de implementación y mantenimiento**: a medida que aumenta el número de participantes en la red, los costos de implementación y mantenimiento pueden

incrementarse. La administración de múltiples nodos, el manejo de las políticas de acceso y la gestión de canales privados requiere de infraestructura robusta y soporte técnico continuo, lo que genera una inversión significativa en términos de recursos humanos y tecnológicos. Estos costos deben ser considerados al planificar la expansión del sistema en el entorno académico.

Capítulo 6

Conclusiones y trabajos futuros

6.1. Conclusiones de la investigación

El prototipo desarrollado validó satisfactoriamente los objetivos planteados en este trabajo, demostrando que es posible emitir, gestionar y verificar certificados académicos digitales en un entorno regulado, cumpliendo con los principios de privacidad, trazabilidad e integridad definidos en la normativa vigente y adoptando la arquitectura propuesta por [Mol21a].

El desarrollo y evaluación del prototipo permitió validar cada uno de los objetivos específicos definidos en la sección 1.2, en particular: (i) la emisión controlada de certificados digitales, (ii) la gestión de accesos por parte de titulares, (iii) la validación pública de integridad, y (iv) la aplicación de medidas de privacidad conforme a GDPR. Los resultados sugieren que Hyperledger Fabric es una opción sólida y adaptable para implementar sistemas confiables de certificación académica digital.

En términos generales, los cuatro objetivos específicos definidos al inicio de este trabajo fueron alcanzados: se realizó un análisis comparativo de soluciones existentes, se diseñó una arquitectura centrada en la privacidad y la trazabilidad, se implementó un prototipo funcional en Hyperledger Fabric, y se validó su comportamiento mediante pruebas específicas de emisión, acceso, verificación y protección de datos.

6.2. Recomendaciones para trabajos futuros

- Evaluar la escalabilidad del sistema en escenarios reales multi-institucionales.
- Incorporar pruebas de concepto con herramientas de prueba de conocimiento cero (zk-SNARKs) para fortalecer la privacidad en la verificación.
- Desarrollar interfaces gráficas orientadas a usuarios finales (egresados y verificadores externos).
- Integrar el prototipo con sistemas académicos existentes, como Bedelías, para explorar su interoperabilidad.
- Explorar el uso de "wallets físicas"mediante el uso del módulo HSM disponible en Fabric que utiliza el estándar PKCS11 para mejorar la seguridad del manejo de credenciales.

6.3. Aplicaciones en el contexto nacional

Desde el punto de vista técnico, el prototipo podría ser adoptado y extendido en el contexto académico uruguayo por instituciones públicas y privadas como parte de una iniciativa de modernización de la emisión y validación de títulos. Por otro lado, este cambio tecnológico se alinea con las estrategias nacionales de digitalización promovidas por AGESIC [AGE20].

Desde el punto de vista legal, resulta necesario contar con una normativa clara y establecida que ayude a estandarizar el uso de este tipo de soluciones tecnológicas; un caso concreto es el de Brasil, analizado en la comparación de soluciones en otros pasíes 2.2.2. En este caso, podemos ver claramente que la implantación de este tipo de tecnologías y cambios operativos debe venir acompasada de leyes o normativas que determinen su uso sin excepciones, transformando la solución en un estándar a nivel nacional.

Bibliografía

[Aa18] Elli Androulaki y et al. «Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains». En: *Proceedings of the Thirteenth EuroSys Conference* (2018), págs. 1-15. DOI: 10.1145/3190508.3190538.

[AGE20] AGESIC. *Estrategia de Ciudadanía Digital para una Sociedad de la Información y el Conocimiento*. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-ciudadania-digital-para-sociedad-informacion-conocimiento-1. Accedido el 10 de mayo de 2025. 2020.

[Arg19] Blockchain Federal Argentina. *Políticas de Uso V1*. Accedido el 9 de marzo de 2025. 2019. URL: \url{https://gitlab.bfa.ar/blockchain/docs/-/wikis/uploads/237b5812528a937e5a8e901ed8107038/20190523_BFA_Pol%C3%ADticas_de_Uso_V1.pdf}.

[Arg21a] Blockchain Federal Argentina. *Blockchain Federal Argentina agesic*. https://bfa.ar/. Accedido el 24 de mayo de 2025. 2021.

[Arg21b] Blockchain Federal Argentina. *Instituciones utilizando BFA*. https://bfa.ar/instituciones. Accedido el 24 de mayo de 2025. 2021.

[BK21] Sotirios Brotsis y Nicholas Kolokotronis. «On the Security and Privacy of Hyperledger Fabric: Challenges and Open Issues». En: *arXiv* (2021). Accedido el 10 de marzo de 2025. URL: https://arxiv.org/pdf/2109.03574.

[But14] Vitalik Buterin. *A Next-Generation Smart Contract and Decentralized Application Platform*. Accedido el 24 de mayo de 2025. 2014. URL: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[BVE20] Bart Butijn, Wouter de Vos y Zekeriya Erkin. «A Survey of Blockchain-Based Applications: From Financial and Insurance Services to Healthcare and Beyond». En: *IEEE Access* 8 (2020), págs. 20083-20100. DOI: 10.1109/ACCESS.2020.2967972.

[Cac16] Christian Cachin. «Architecture of the Hyperledger Blockchain Fabric». En: *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*. 2016, págs. 1-4. URL: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[CD21] Urmila Nagvekar Carlos Dominguez. *Hyperledger Fabric 2.0 Architecture Security Report*. Accedido el 24 de mayo de 2025. 2021. URL: https://cognizium.io/uploads/resources/Cloud%20Security%20Alliance%20-%20Hyperledger%20Fabric%202.0%20Architecture%20Security%20Report.pdf.

[Con00] Congreso de la Nación Argentina. *Ley de Protección de los Datos Personales*. https://www.argentina.gob.ar/normativa/nacional/ley-25326-48942. Ley Nº 25.326, sancionada el 4 de octubre de 2000. 2000.

[Con23] ConsenSys. *Quorum Blockchain*. https://consensys.net/quorum/. Accedido el 9 de marzo de 2025. 2023.

[Cos+18] Rostand Costa et al. «Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos». En: *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain)*. Accedido el 24 de mayo de 2025. Campos do Jordão, Brasil: Sociedade Brasileira de Computação, 2018. URL: https://sol.sbc.org.br/index.php/wblockchain/article/view/2356.

[Fin19] Michèle Finck. *Blockchain Regulation and Governance in Europe*. Cambridge University Press, 2019. DOI: 10.1017/9781108610886.

[Fou23a] Ethereum Foundation. *Proof of Work (PoW)*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/. Accedido el 24 de mayo de 2025. 2023.

[Fou23b] Ethereum Foundation. *Proof of Work (PoW)*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/. Accedido el 24 de mayo de 2025. 2023.

[Fou23c] Ethereum Foundation. *What is Ethereum?* https://ethereum.org/en/what-is-ethereum/. Accedido el 9 de marzo de 2025. 2023.

[GC17] Alexander Grech y Anthony F. Camilleri. «Blockchain in Education». En: *JRC Science for Policy Report* (2017). Accedido el 24 de mayo de 2025. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC108255.

[HS91] Stuart Haber y W. Scott Stornetta. «How to time-stamp a digital document». En: *Journal of Cryptology* 3.2 (1991), págs. 99-111. DOI: 10.1007/BF00196791.

[Hyp21a] Hyperledger. *Hyperledger Besu*. https://www.hyperledger.org/use/besu. Accedido el 24 de mayo de 2025. 2021.

[Hyp21b] Hyperledger. *Hyperledger Fabric*. https://www.hyperledger.org/use/fabric. Accedido el 24 de mayo de 2025. 2021.

[Hyp23] Hyperledger. *Hyperledger Fabric Documentation: Access Control*. https://hyperledger-fabric.readthedocs.io/en/release-2.5/access_control.html. Accedido el 9 de marzo de 2025. 2023.

[Hyp23] Hyperledger. *Proof of Authority (PoA) in Hyperledger Besu*. https://besu.hyperledger.org/stable/private-networks/concepts/poa. Accedido el 24 de mayo de 2025. 2023.

[Hyp23a] Hyperledger. *About Hyperledger*. https://www.hyperledger.org/about. Accedido el 24 de mayo de 2025. 2023.

[Hyp23b] Hyperledger. *Byzantine Fault Tolerant Consensus*. https://wiki.hyperledger.org/display/LMDWG/Byzantine+Fault+Tolerant+Consensus. Accedido el 24 de mayo de 2025. 2023.

[Hyp24] Hyperledger. *Datos privados en Hyperledger Fabric*. https://hyperledger-fabric.readthedocs.io/es/latest/private-data/private-data.html. Accedido el 10 de marzo de 2025. 2024.

[Hyp24] Hyperledger. *Hyperledger Fabric Commands Reference*. https://hyperledger-fabric.readthedocs.io/en/latest/command_ref.html. Accedido el 10 de mayo de 2025. 2024.

[Hyp24] Hyperledger. *Using the Fabric test network*. https://hyperledger-fabric.readthedocs.io/en/release-2.5/test_network.html. Accedido el 10 de marzo de 2025. 2024.

[IUS21] Sistema de Información Universitaria (SIU). *SIU-Guaraní: Sistema de Gestión Académica*. https://www.siu.edu.ar/guarani. Accedido el 24 de mayo de 2025. 2021.

[Mol21a] Fernanda Molina. «A Blockchain-Based and GDPR-Compliant Design of a System for Digital Education Certificates». En: *arXiv* (2021). Accedido el 10 de marzo de 2025. URL: https://arxiv.org/pdf/2010.12980.

[Mol21b] Fernanda Molina. *Data Flow Diagram of the system*. Accedido el 10 de marzo de 2025. 2021. URL: https://arxiv.org/pdf/2010.12980.

[Nak08] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Accedido el 24 de mayo de 2025. 2008.

[Net21] XDC Network. *XDC Network: The Enterprise-Ready Hybrid Blockchain*. https://xdc.org/. Accedido el 24 de mayo de 2025. 2021.

[Nic17] University of Nicosia. *University of Nicosia Issues Academic Certificates on the Blockchain*. https://www.unic.ac.cy/university-of-nicosia-issues-academic-certificates-on-the-blockchain/. Accedido el 24 de mayo de 2025. 2017.

[Ope23] OpenEthereum. *Proof of Authority Chains*. https://openethereum.github.io/Proof-of-Authority-Chains. Accedido el 24 de mayo de 2025. 2023.

[PR21] Rede Nacional de Ensino e Pesquisa (RNP). *Diploma Digital: A Blockchain-Based Solution for Digital Certificates*. https://rnp.br/diploma-digital. Accedido el 24 de mayo de 2025. 2021.

[R321] R3. *Corda: An Introduction*. https://www.corda.net/. Accedido el 9 de marzo de 2025. 2021.

[Rep08] República Oriental del Uruguay. *Ley Nº 18.331: Protección de Datos Personales y Acción de Habeas Data, Artículo 2*. https://www.impo.com.uy/bases/leyes/18331-2008. Accedido el 25 de febrero de 2025. 2008.

[Rep18] República Federativa do Brasil. *Lei Geral de Proteção de Dados Pessoais*. https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/34172845/do1-2018-08-15-lei-n-13-709-de-14-de-agosto-de-2018-34172811. Lei Nº 13.709, de 14 de agosto de 2018. 2018.

[Rep20] República Oriental del Uruguay. *Decreto Nº 64/020: Reglamentación de la Ley Nº 19.670, Artículo 4*. https://www.impo.com.uy/bases/decretos/64-2020. Accedido el 25 de febrero de 2025. 2020.

[SB21] Banco Nacional de Desenvolvimento Econômico e Social (BNDES). *Rede Blockchain Brasil (RBB): A Hybrid Blockchain Initiative*. https://bndes.gov.br/rbb. Accedido el 24 de mayo de 2025. 2021.

[SS19] Philipp Schmidt y Juliana Sheldon. *Blockcerts: An Open Infrastructure for Academic Credentials on the Blockchain*. Accedido el 24 de mayo de 2025. 2019. URL: https://www.media.mit.edu/projects/blockcerts/overview/.

[Swa15] Melanie Swan. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, 2015.

[Sza94] Nick Szabo. *Smart Contracts*. Accedido el 24 de mayo de 2025. 1994. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[TT16] Don Tapscott y Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY: Penguin, 2016.

[Tur+18] Maroš Turkanović et al. «EduCTX: A Blockchain-Based Higher Education Credit Platform». En: *IEEE Access* 6 (2018), págs. 5112-5127. DOI: 10.1109/ACCESS.2018.2789929.

[Uni16] European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj. 2016.

[Uru08] República Oriental del Uruguay. *Ley Nº 18.331: Protección de Datos Personales y Acción de Habeas Data*. http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331. 2008.

[U.S96] U.S. Congress. *Health Insurance Portability and Accountability Act of 1996*. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Public Law 104-191. 1996.

[XWS19] Xiwei Xu, Ingo Weber y Mark Staples. «Architecture for Blockchain Applications». En: *Springer* 1.1 (2019), págs. 29-54. DOI: 10.1007/978-3-030-03035-3_2.

[Zoh15] Aviv Zohar. «Bitcoin: under the hood». En: *Communications of the ACM* 58.9 (2015), págs. 104-113. DOI: 10.1145/2701411.

[ZQH20] Xiaoqi Zhu, Yi Qian y Rose Qingyang Hu. «How Can Blockchain Help Internet of Things? A Survey, a Review and a New Perspective». En: *IEEE Communications Surveys & Tutorials* 22.4 (2020), págs. 2416-2451. DOI: 10.1109/COMST.2020.3014269.

Apéndice A

Anexos

A.1. Código fuente

El código fuente del prototipo con todos sus componentes, documentación y pruebas realizadas queda disponible en el siguiente repositorio:
https://gitlab.fing.edu.uy/gsi/blockchain/titulos-electronicos/

A.2. Documentación técnica

A.3. Material adicional

A.4. Explicación detallada del archivo collections-config.json

A continuación se presenta una explicación detallada sobre cada parámetro del archivo de configuración `collections-config.json`.

`name` Identificador para la colección privada utilizado en el chaincode.

`policy` Define organizaciones autorizadas a acceder a los datos privados.

`requiredPeerCount` Número mínimo de peers que respaldan la transacción.

`maxPeerCount` Número máximo de peers utilizados para redundancia de datos.

`blockToLive` Determina la retención de datos privados (en bloques).

`memberOnlyRead` Restringe la lectura a organizaciones autorizadas.

`memberOnlyWrite` Restringe la escritura a organizaciones autorizadas.