

# CONFIANZA Y VERIFICABILIDAD DE CERTIFICADOS ACADÉMICOS Y EL USO DE LA TECNOLOGÍA BLOCKCHAIN COMO HERRAMIENTA EN LA UNIVERSIDAD JORGE TADEO LOZANO.

## CONFIDENCE AND VERIFIABILITY OF UNIVERSITY DEGREES AND THE USE OF BLOCKCHAIN TECHNOLOGY AS A TOOL IN UNIVERSITY JORGE TADEO LOZANO.

Miguel Eduardo Fuentes Contreras, Programa de Ingeniería de sistemas, Universidad Jorge Tadeo Lozano, [miguele.fuentesc@utadeo.edu.co](mailto:miguele.fuentesc@utadeo.edu.co).

### **Resumen**

El siguiente trabajo busca dar a conocer a la comunidad universitaria como la tecnología blockchain puede aumentar los niveles de seguridad de la información en el proceso de emisión y verificación de certificados y registros académicos. El problema abordado es aumentar los tres pilares de la seguridad de la información: disponibilidad, integridad y confidencialidad en este proceso. Con el fin de solventar el problema se utiliza la metodología Scrum con sprints semanales, donde se tenían dos fases: Una fase de investigación y una fase de implementación.

En la fase de investigación se realizó un trabajo de campo y teórico con el fin de conocer la forma tradicional de manejo de registros académicos en la Universidad Jorge Tadeo Lozano. Además, se comenzó en la búsqueda del protocolo blockchain adecuado para ayuda en esta labor.

En la fase de implementación se comenzó en el desarrollo de un prototipo que adoptara este protocolo blockchain y diera una idea de como puede explotarse el potencial de esta tecnología.


Finalmente, se obtiene como resultado las falencias encontradas en la forma tradicional de emisión y verificación de registros y certificados académicos, permitiendo ubicar algunas vulnerabilidades existentes. Estas vulnerabilidades respaldan el desarrollo de un prototipo realizado que busca disminuir y algunas estas, con la utilización de la tecnología blockchain.

## Abstract

The following work seeks to publicize to the university community how blockchain technology can increase the levels of information security in the process of issuing and verifying certificates and academic records. The problem addressed is to increase the three pillars of information security: availability, integrity and confidentiality in this process. In order to solve the problem, the Scrum methodology is used with weekly sprints, where there were two phases: an research phase and an implementation phase.

In the research phase, a field and theoretical work was carried out in order to know the traditional way of managing academic records at the Jorge Tadeo Lozano University. In addition, the search for the appropriate blockchain protocol to help in this work was started. In the implementation phase, the development of a prototype that adopted this blockchain protocol began and gave an idea of how the potential of this technology can be exploited. Finally, the shortcomings found in the traditional way of issuing and verifying academic records and certificates are obtained as a result, allowing locating some existing vulnerabilities. These vulnerabilities support the development of a prototype carried out that seeks to decrease and some of these, with the use of blockchain technology.

## Glosario

-  Bloque
- Peer to Peer
- Ledger
- Nodo
- Wallet
- Minero
- Bloque
- Certificado
- Cash

## **Introducción**

Los registros académicos generados durante la vida universitaria están expuestos a ser manipulados de forma ilegal, provocando corrupción en las instituciones educativas que, muchas veces, se ven manchadas por los actos delictivos de unos pocos. Es por eso que en este trabajo se mostrará cómo ayuda la tecnología blockchain a mantener seguros los registros importantes generados en la etapa universitaria.

### *Planteamiento del problema*

En Colombia, los aspirantes que deseen ingresar a una empresa tienen más posibilidades de ser contratados de acuerdo con la cantidad y nivel de los estudios que posean. Por consiguiente, la demanda en educación superior ha ido aumentando en Colombia. Por ejemplo, en el libro *Demanda por educación superior: Proyección hasta 2025*. [1] se menciona que el peso del empleo formal de mano de obra calificada (educación superior) pasó de 22% en 1984, a 53% en el año 2010. Por otra parte, conseguir un título de educación superior en Colombia es una meta que, por lo general, involucra tiempo y dinero. Por lo que algunas personas prefieren seguir otra ruta, la de comprar certificados baratos y falsos. Y si la empresa no puede verificar la autenticidad de los estudios de la persona, la empresa podría presentar problemas a causa de la incompetencia de la persona a contratar.

Adicionalmente, uno de los pasos para comprobar la veracidad de un certificado es comunicarse directamente con la universidad o escuela, de donde se supone pertenece el certificado. Esto implica una gran cantidad de tiempo y no ofrece una seguridad total, porque los encargados de manejar estos temas en los institutos podrían estar implicados en la falsificación del documento.

### *Contexto Teórico*

Además, se han presentado bastantes casos donde los sistemas académicos, que contienen información como notas, logros y rendimiento académico, han sido manipulados de forma desautorizada. A continuación, se darán a conocer algunos casos:

- En la Universidad del Atlántico, en el año 2010 [2], se descubrió que al menos a 57 estudiantes se le alteraron las notas académicas obtenidas por su paso en la universidad. Esto sucedió a consecuencia de la implementación del sistema Academusoft, la Universidad del Atlántico “permitía ocasionalmente” a ingenieros de la universidad de Pamplona, acceder remotamente desde esa ciudad para actualización y correcciones del programa. Por consiguiente, este acceso, probablemente, fue aprovechado para realizar cambios en la información de los estudiantes. Pese a que los rumores de fraudes han disminuido y los correctivos fueron tomados, las alarmas han estado encendidas en la Universidad del Atlántico.
- Las directivas de la Universidad Pontificia Bolivariana investigan caso de fraude en las calificaciones [3]. En este caso los estudiantes fueron contactados por dos personas de registro académico y notas, quienes ofrecían cambiar sus notas a cambio de sumas de dinero, entre los 200.000 COP y 1'000.000 COP. Para al final ser separados de sus respectivos cargos.
- En la Universidad de la Amazonia desde el año 2012 [4], la fiscalía iba tras la pista de una organización ilegal que ‘arreglaba’ las notas en la universidad de la Amazonía, con precios entre los 50.000 COP y los 600.000 COP.  
De acuerdo con la investigación, se realizaron 73 registros para alterar las calificaciones.  
La fiscalía ha efectuado 19 capturas de 24 ordenadas, de los cuales 8 son egresados de esta universidad. Estas cifras son del 15 de julio de 2017.
- En el año 2015, el periódico El País Colombia publicó [6]: “Exclusivo: En el valle ya han descubierto a más de 1200 profesionales con título falso”.  
En el valle se ve a la falsificación de títulos como un mercado en crecimiento, donde solo en el año 2014 fueron descubiertos más de 1200 profesionales ilegítimos. Pero aún más preocupante, es la gran cantidad de falsos profesionales vinculados al sector de la salud. Esto porque en las manos de un falso médico lo que está en juego es la vida de una persona.
- En el Reino Unido, en 2013 y 2014 se vendieron más de 3000 calificaciones falsas de la red universidades online falsas Axact [5], incluyendo títulos de maestría,

doctorados y PhDs. Entre quienes aparecen como clientes de esta “Empresa criminal” están oftalmólogos, enfermeras, un psicólogo, y numerosos consultantes de la clínica NHS.

En 2015, Axact vendió globalmente más de 215000 calificaciones falsas, con el uso de aproximadamente 350 escuelas y universidades falsas.

El agente del FBI Allen Ezell, investigador del tema afirma que “Los empleadores no están haciendo las diligencias correspondientes al verificar los documentos, así que eso hace que funcione. Es la cosa más maldita que hemos visto”. “...mientras el papel tenga un valor, habrá alguien que lo falsifique, lo imprima y lo venda.

- En el año 2015, el periódico El País Colombia publicó [6]: “Exclusivo: En el valle ya han descubierto a más de 1200 profesionales con título falso”. En el valle se ve a la falsificación de títulos como un mercado en crecimiento, donde solo en el año 2014 fueron descubiertos más de 1200 profesionales ilegítimos. Pero aún más preocupante, es la gran cantidad de falsos profesionales vinculados al sector de la salud. Esto porque en las manos de un falso médico lo que está en juego es la vida de una persona.

De acuerdo con el New York Times [10], más de 50.000 títulos de doctorado se compran anualmente, lo cual es más que el número de diplomas otorgados por las universidades oficiales. En Colombia, este problema es abordado por el portal KIENYKE [11], allí se describe cómo se puede conseguir diplomas de todo tipo, desde 400.000 pesos colombianos, con resultados que toman tan solo 3 días.

Al prestar atención a las recopilaciones periodísticas, es evidente el problema de las falsificaciones de certificados estudiantiles, ya sea porque las universidades no adopten las debidas medidas anti-fraude en el proceso de tratamiento de certificados o que los empleadores no realicen el suficiente trabajo para verificar la autenticidad de los certificados.

### *Estado actual de la problemática*

A continuación, se muestran resúmenes de trabajos recientes que hablan del manejo de certificados y el uso de la tecnología blockchain en Colombia y el mundo.

- Wegelid (2019) [7] investigó que es la tecnología blockchain y como esta puede ser utilizada en la industria de las certificaciones. El problema que abordó fue investigar el funcionamiento de la tecnología blockchain y sus características aportantes a la industria de las certificaciones. Para lo anterior, se utiliza una metodología dividida en dos partes: La estrategia de investigación, donde se eligió y un enfoque exploratorio que permita comprender y explicar el tema a profundidad; y el método de investigación, buscando conocer los actores que se benefician de los certificados y una aplicación prototipo que utilice blockchain. Un aporte relevante de este Proyecto fue conocer las diferentes formas de almacenar y acceder a los certificados en la actualidad y como la aplicación desarrollada obtuvo los resultados esperados de transparencia, seguridad y descentralización.
- D. Nguyen [8], D. Nguyen-Duc, N. Huynh-Tuong y H. Pham (2018) propuso un enfoque que utilizó la tecnología blockchain para emitir certificados inmutables. El problema que abordaron fue utilizar la tecnología blockchain para emitir certificados digitales inmutables y mejorar las limitaciones existentes en los sistemas de verificación de certificados. Tales limitaciones se buscan superar con sistemas más rápidos, más confiables e independientes de la central de autoridad. Para lo anterior, se utiliza una metodología donde se comienza a buscar diferentes herramientas que ayuden a mejorar la seguridad de los certificados, encontrando a openbadges y blockcerts. Finalmente, se definen las características que debería tener la herramienta emisora de certificados inmutables, tales como Verificación descentralizada, Transparencia, privacidad y seguridad, Innegable, ahorro y conveniencia. Un aporte relevante de este desarrollo fue que permitió a los emisores y verificadores realizar operaciones con precisión, rapidez, rentabilidad y eficiencia en la gestión de certificados digitales. El piloto demostró que es aplicable a los servicios asociados a la gestión de certificados y diplomas particularmente en Vietnam.



- Plaza (2018) [9] diseñó y desarrolló un prototipo funcional de un sistema distribuido para la emisión, visualización y verificación de certificados educativos digitales basados en la tecnología blockchain. El problema que abordó fue diseñar y desarrollar un protocolo funcional que sirviera como herramienta de apoyo para mitigar la falsificación de diplomas de grados universitarios con el fin de favorecer la autenticidad en la emisión, visualización y verificación de certificados educativos digitales basados en la tecnología Blockchain. Por lo anterior Plaza utilizó tres metodologías: Design thinking con el fin de diseñar y desarrollar una solución tecnológica para la generación y validación de diplomas de grado; Lean StartUp, ideal para proyectos con incertidumbre extrema circunstancia en la cual los métodos tradicionales de planeación no funcionan; y Scrum que garantiza transparencia en la comunicación y crear un ambiente de responsabilidad colectiva y de progreso continuo. Como aporte relevante se pudo obtener un diseño, una implementación funcional y un aporte hacia las condiciones necesarias (tecnológicas y organizacionales) para el despliegue generalizado de una solución como esta en una universidad.

### *Finalidad del proyecto*

Por lo tanto, es necesario encontrar una forma automática de generación y verificación de registros académicos, donde no sea necesario la confianza en terceras personas durante el proceso. Además, donde el proceso de verificación de la información dure lo menos posible. Teniendo esto en cuenta, se desarrollará un aplicativo prototipo que emplee tecnología DLT o Blockchain que permita crear y almacenar registros académicos. Esto permitirá aumentar la integridad, autenticidad y disponibilidad de los registros académicos utilizando tecnología DLT o blockchain para la Universidad Jorge Tadeo Lozano.

Adicionalmente, se busca en este trabajo responder las siguientes preguntas de investigación:

¿Qué requisitos debería cumplir un sistema de certificaciones académicas en la Universidad Jorge Tadeo Lozano?

¿Qué protocolo blockchain se debe utilizar y como podría utilizarse, con el objetivo de crear un sistema de certificaciones académicas?

### *Justificación*

Se realizará este trabajo con el fin de aprovechar los principios de la tecnología Blockchain [10]. que son:

- Auto-identidad soberana.
- Confianza.
- Transparencia.
- Inmutabilidad.
- Desintermediación.

### *¿Cómo son aprovechados estos principios?*

- *Auto-identidad soberana:* La auto-identidad soberana surge de la necesidad de proteger la identidad de las personas dado que al moverse por internet no existe un DNI y el control de la información de los usuarios no está bajo su control. [11] La propiedad y privacidad se verán pronto como un derecho humano [12]. Por lo tanto, la auto-identidad soberana busca que los usuarios tengan un control total de su información sin intermediarios [11].

Ahora, se puede ver que la información académica entra a ser información personal que siempre debe ser manipulada por nosotros o bajo nuestra aceptación.

- *Confianza:* La confianza es uno de los principios más importantes de la tecnología blockchain, dado que la eliminación de la confianza en las transacciones realizadas, en ejemplo hacia los bancos, es uno de los impulsos a la popularización de protocolos como bitcoin.

En el caso de los registros y certificados académicos, su infraestructura se brinda la confianza suficiente en el proceso de emisión de certificados [10].



- *Transparencia:* La tecnología blockchain emplea mecanismos que sustentan suficientemente la existencia de una transacción en un momento determinado [10].
- *Inmutabilidad:* La inmutabilidad es la propiedad que tienen los datos almacenados en las transacciones, de no sufrir alteraciones que alteren su integridad inicial. Por lo tanto, la única forma de cambiar los efectos surtidos por una transacción es realizando otra transacción que cambie o anule la anterior. Por lo que ahora habrían dos transacciones registradas en la cadena con sus datos íntegros.
- *Desintermediación:* Uno de los problemas que puede ayudar solucionar la tecnología blockchain es la eliminación de las terceras partes, disminuyendo el tiempo y el costo de las transacciones efectuadas y aumentando la confianza en las mismas.  
Para la emisión de certificados es importante que la menor cantidad de personas tengan acceso a este.

### *Alcance*

Este proyecto tiene como alcance la realización de un prototipo, en forma de aplicativo, que aumente la seguridad de la información de los registros académicos, utilizando la tecnología blockchain. Esto es, registrar y almacenar registros académicos de las asignaturas y utilizar esa información para generar un registro inmutable utilizando un protocolo blockchain.



### *Beneficios obtenidos*

Los beneficios obtenidos de este proyecto son los de aumentar el control de los logros académicos de los estudiantes de la universidad y la trazabilidad de estos, en el transcurso de un programa académico. Además, permite dar conocer a la universidad los beneficios que tiene implementar un sistema que utilice blockchain o sus similares.

### *Marco Teórico*

### *¿Qué es blockchain?*

Blockchain o cadena de bloques se puede definir como un sistema de base de datos distribuido donde se almacenan datos que permanecen inmutables, disponibles y verificables. Todo esto mediante conexiones *peer to peer* que mantiene comunicados a diferentes equipos llamados nodos, encargados de verificar la autenticidad y almacenar los datos que son ingresados a la base de datos. Esta base de datos está dividida en bloques que aumentan con una periodicidad definida. Estos datos están agrupados principalmente en transacciones entre los diferentes usuarios de la red. Estas transacciones entre usuarios pueden realizarse sin la intermediación de un tercero, creando un sistema descentralizado donde todos los nodos actúan sin autoridad central.

Álex Preukschat [13] dice que blockchain: "...no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente."

En blockchain una transacción es simplemente una cadena: donde un usuario A desea transferir valor a un usuario B, con la firma de A. La eventual inclusión de esta transacción en el libro mayor de la red blockchain es lo que respalda la veracidad de la transacción. Tenga en cuenta que el usuario B no interfiere en la transacción. [14]

Un bloque tiene un su interior a las transacciones generadas en el momento de la creación del bloque.

Las transacciones en una red son agrupadas en bloques. Cada bloque está conectado con el bloque anterior a este y con el bloque posterior.

### *Hash*

Un hash es una cadena de caracteres que representa de forma única a un conjunto de datos, mediante una función. Un hash se puede generar prácticamente con cualquier dato. Los hashes generados en los bloques de la cadena de bloques, generalmente, tienen la propiedad de irreversibilidad que hace prácticamente imposible llegar a los datos a partir del hash generado por los mismos.

En la blockchain de bitcoin, cada bloque posee un hash que lo identifica. Este hash toma como parámetros: al hash del bloque anterior, a la raíz de merkle de las transacciones dentro del bloque, a la marca de tiempo de la generación del bloque y un número llamado nonce que es determinante para los requisitos de generación del hash.

Cuando se dice que el nonce es determinante para el hash, se refiere a que los mineros deben generar un hash con una cantidad de ceros requerida, donde la forma más adecuada para llegar a esto es modificando el nonce hasta conseguir un hash que cumpla con lo establecido. Este requisito es verificado por todos los nodos, procediendo a la adición del bloque a la cadena de bloques de todos los nodos.

### *Firmas digitales*

Las firmas digitales [15] a diferencia de una firma electrónica, encriptan el mensaje transmitido y proveen autenticidad al mismo. (Katz,2010) Esta firma es creada de forma digital para añadir una capa de validación y transmisión para las bases de datos de encriptación de llaves públicas.

Las firmas digitales tienen cuatro componentes básicos [10]:

1. Un hash
2. Una llave pública.
3. Una llave privada.
4. Una lista de estampas de tiempo para precisar en que momento el certificado fue emitido.

Las firmas digitales tienen dos momentos:

1. Firma:
  - a. Al mensaje que se desea firmar se le aplica un hash.
  - b. El hash obtenido se encripta usando la llave privada del firmante o remitente.
  - c. El mensaje original es adjuntado junto a la firma o encriptación resultante del punto b.
  - d. El mensaje firmado digitalmente es creado y está listo para ser enviado.
2. Verificación:
  - a. Se recibe el mensaje firmado digitalmente.
  - b. Se separa el mensaje original y la firma o encriptación realizada.
  - c. Se subdividen los pasos:
    - i. Al mensaje original se le aplica una función hash.
    - ii. La firma o encriptación realizada se desencripta usando la llave pública del firmante o remitente.
  - d. Se comparan los hashes generados del punto i. y ii.

Si los hashes generados del punto i. y ii. son iguales la firma digital es válida.

En los sistemas que utilizan la tecnología blockchain, la firma digital contribuye principios de integridad y autenticidad de los mensajes transmitidos.

#### *Blockchain públicas, privadas y híbridas.*

Los sistemas blockchain se pueden categorizar, de acuerdo a los permisos que debe tener un nodo para ser contenedor de la cadena y ser verificador de las transacciones en la misma, en públicos, privados o compuestas.

Los sistemas blockchain públicos son aquellos donde cualquier persona puede participar, sin ningún permiso, como contenedor de la cadena de bloques y verificador de las transacciones en este. Se destaca a Bitcoin como protocolo público.

En el caso de los sistemas blockchain de carácter privado, si alguien se quiere unir a la red se deben tener los permisos otorgados por la red. Los sistemas blockchain privados, por su naturaleza, son más pequeños que los públicos. Se destaca hyperledger fabric como protocolo privado.

También, existen blockchain híbridas que toman y quitan lo bueno y malo de cada una. Utilizando esta blockchain para manejo de confianza con terceros, dejando la seguridad que mantiene la pública y la jerarquía de la privada.

#### *Algoritmos de consenso*

Cuando se va a agregar un nuevo bloque a la cadena, los nodos de la red deben coincidir, en su mayoría, en que las transacciones del nuevo bloque son las correctas. Para esto existen múltiples algoritmos que tienen el objetivo de llegar a acuerdos entre múltiples participantes.

La búsqueda de un acuerdo global en la blockchain [16] es posible gracias a la implementación de protocolos de consenso que dictan las reglas a cumplir por parte de los usuarios.

Entre los algoritmos más conocidos se encuentran:

- *Prueba de trabajo (En inglés: Proof of work):* Este algoritmo es la columna del sistema Bitcoin, siendo así el primer algoritmo en ser utilizado por un sistema de criptomonedas.  
La prueba de trabajo [16] es la combinación de criptografía y poder computacional que crea consenso y asegura la autenticidad de los datos se mantenga en la blockchain. Sin embargo, este algoritmo presenta deficiencias que lo tienen en vía

de extinción. La red crece y crece al igual que su poder computacional [17], aumentando así la sensibilidad general del sistema.

- *Prueba de importancia (En inglés: Proof of importance)*: El algoritmo le da poder de decisión a los mineros que realmente tienen participación en el sistema. Aquí no todos pueden ser mineros, primero deben participar en la red invirtiendo y realizando transacciones en ella, para así tener el poder de validar transacciones y crear bloques. No hay recompensas bajo la forma de creación de dinero: los validadores cobran tarifas a los usuarios y se les paga como intermediario habitual [16]. En la prueba de importancia cuanto más coseche un nodo más posibilidades tendrá de agregarse a la cadena [17]. En el protocolo NEM, debes tener al menos 10,000 XEM en tu cuenta, para recolectar [18].
- *Prueba de participación (En inglés: Proof of stake)*: El algoritmo de consenso resuelve las principales deficiencias del algoritmo de la prueba de trabajo, validando cada bloque antes de que sea añadido otro. Además, los mineros se pueden unir usando sus propias monedas [17]. Sin embargo, la prueba de importancia le da ventaja a aquellos que posean más monedas en sus cuentas [18], siendo imposible competir solo, frente a otra cuenta con gran capital.

### *Límites de la tecnología*

La tecnología blockchain sin duda ha tenido gran popularidad desde 2009, cuando Satoshi Nakamoto compartió al mundo el protocolo Bitcoin. Sin embargo, las críticas a esta tecnología no se han hecho esperar.

Blockchain es criticado por lo inseguro que son las redes perimetrales de estas. Esto quiere decir, que aún siendo un sistema bastante seguro en su interior, no garantiza lo mismo para los intermediarios externos entre los usuarios y la cadena de bloques. Por lo que, se han registrado múltiples robos de criptomonedas a nivel mundial [19].

Lo que hace realmente innovador a esta tecnología es el correcto acoplamiento de sus componentes, porque si analizamos los componentes principales de la tecnología, estos existen desde mucho antes del boom de bitcoin, que realmente hace a blockchain una tecnología relativamente vieja.

Ahora es verdad que la tecnología tiene problemas anexos a su descentralización, pero se debe recordar que blockchain es una tecnología en proceso de adaptación que necesita que exista más gente trabajándola y conociéndola.

### ***Objetivo General***

Aumentar la integridad, confidencialidad y disponibilidad de las certificaciones académicas empleando tecnología DLT o blockchain en la Universidad Jorge Tadeo Lozano.

### ***Objetivos Específicos***

- Definir los requerimientos necesarios para implementar un sistema que garantice la integridad, autenticidad y disponibilidad de las certificaciones académicas en la universidad Jorge Tadeo Lozano.
- Seleccionar un protocolo teniendo en cuenta los requerimientos establecidos.
- Diseñar el sistema gráfica y lógicamente que cumpla con los requerimientos y objetivos del proyecto.
- Implementar un prototipo funcional de acuerdo con el diseño planteado.

### **Metodología**

Para lograr el objetivo planteado se utilizará una metodología Ágil con el marco Scrum [8].

Se elige este tipo de metodología dado que el proyecto trabaja con sistemas descentralizados catalogados como complejos, susceptible de imprevistos. Además, permitirá trabajar en ciclos donde se logren objetivos concretos y detallados que simplifican el camino para obtener éxito en el proyecto.

### ***Fase de investigación***

#### ***1. Recolección de datos***

Se realizará entrevista diseñadas con el fin de conocer información objetiva acerca del proceso de emisión de certificados que da la universidad a los diplomas, de los requisitos que plantea la universidad para graduarse, los datos que se requieren recolectar, la usabilidad, entre otros. La información obtenida en los momentos de recolección de datos se utiliza para empatizar con los involucrados en el proceso de emisión de certificados. Esto tiene el fin de conocer el estado actual y las necesidades del problema planteado.

También se hará una revisión de la literatura sobre estándares internacionales de certificación, de datos abierto (metadatos) para interoperabilidad de registros.

En esta etapa se generarán los siguientes entregables:

- Cuestionarios
- Entrevistas sistematizadas.

## *2. Análisis de datos*

Las entrevistas con los primeros entrevistados permitirán identificar en primera instancia el proceso de certificación junto con los responsables. En segunda instancia permitirá identificar los puntos críticos del sistema. En esta etapa se generarán los siguientes entregables:

- Diagrama de flujo actual del proceso de certificación y sus responsables.
- Lista de requerimientos

## *Fase de implementación*

### *1. Selección del protocolo*

Con base en los requerimientos desarrollados en el punto 8.1.2 y utilizando el documento “Una taxonomía de sistemas basados en blockchain para el diseño de arquitectura” se selecciona un protocolo que permita implementar convenientemente un prototipo mínimo funcional.

### *2. Desarrollo de diagramas / planificación / UML*

Para el desarrollo de este punto se trabaja en conjunto con la materia Construcción de aplicaciones móviles para realizar la planificación del desarrollo del aplicativo descentralizado. Además, se definirá el estándar de metadatos a usar. En esta etapa se generarán los siguientes entregables:

- Diagrama Entidad Relación.
- Diagrama de Software.

### *3. Programación*

Para el desarrollo de este punto se determinarán las funcionalidades mínimas a entregar y se realizará la codificación de los procesos definidos en las funcionalidades. La información obtenida en los momentos de recolección de datos se utiliza para empatizar con estas funcionalidades. En esta etapa se generarán los siguientes entregables:

- Definir el alcance del desarrollo.
- Prototipo

## **Resultados y discusión**

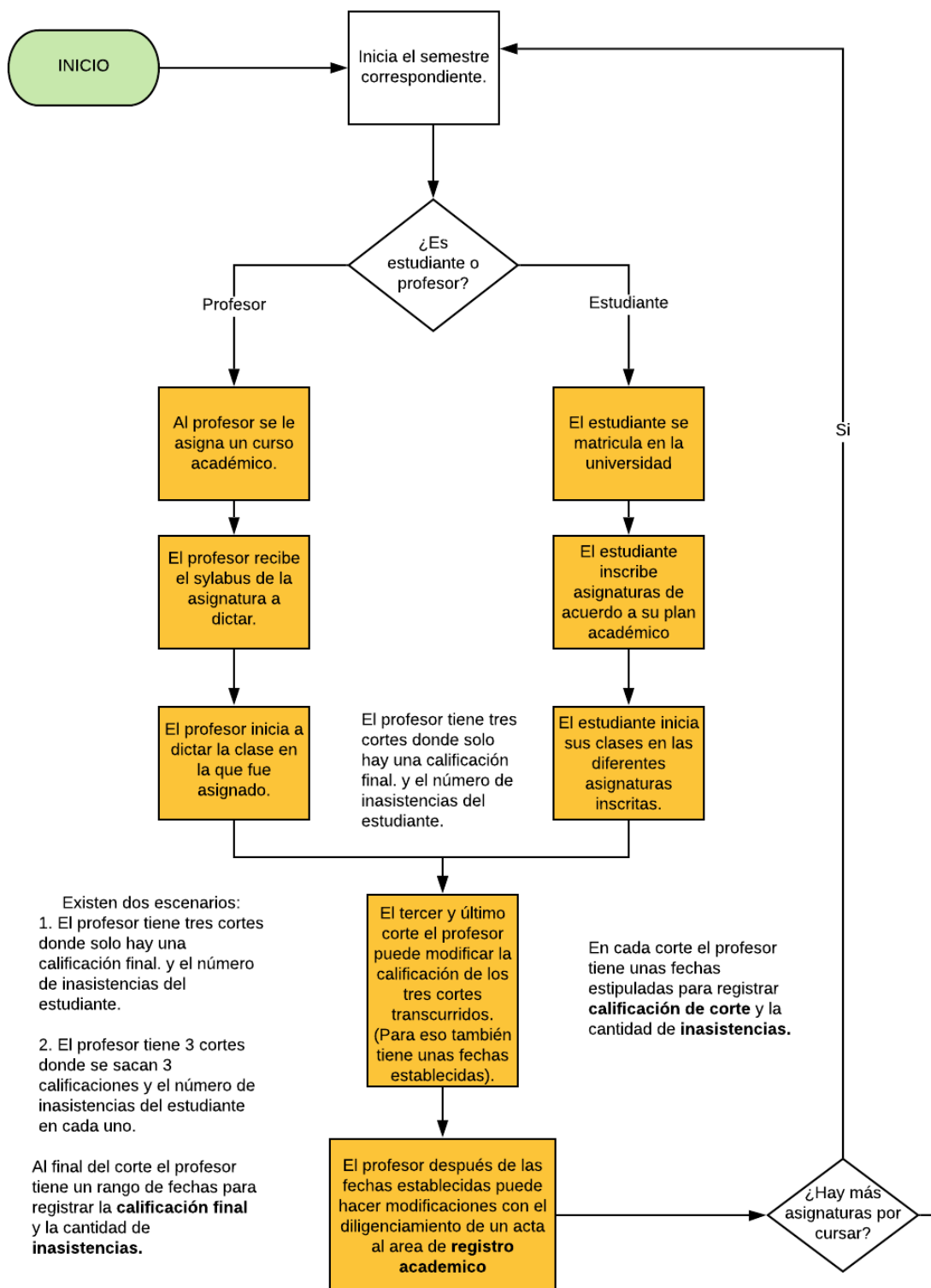
### *Fase de investigación*

#### *Análisis de datos*

La universidad Jorge Tadeo Lozano desde el momento en que el estudiante es matriculado, establece unos procesos y pasos a seguir con el fin de que sus estudiantes superen y registren sus actividades y logros durante la vida universitaria, para al final recibir su preciado diploma. Estos procesos fueron dados a conocer por el personal involucrado a través del uso de entrevistas presenciales.

A continuación, se muestra de forma general el proceso que sigue un profesor y un estudiante para registrar de la mejor manera el avance del semestre académico.

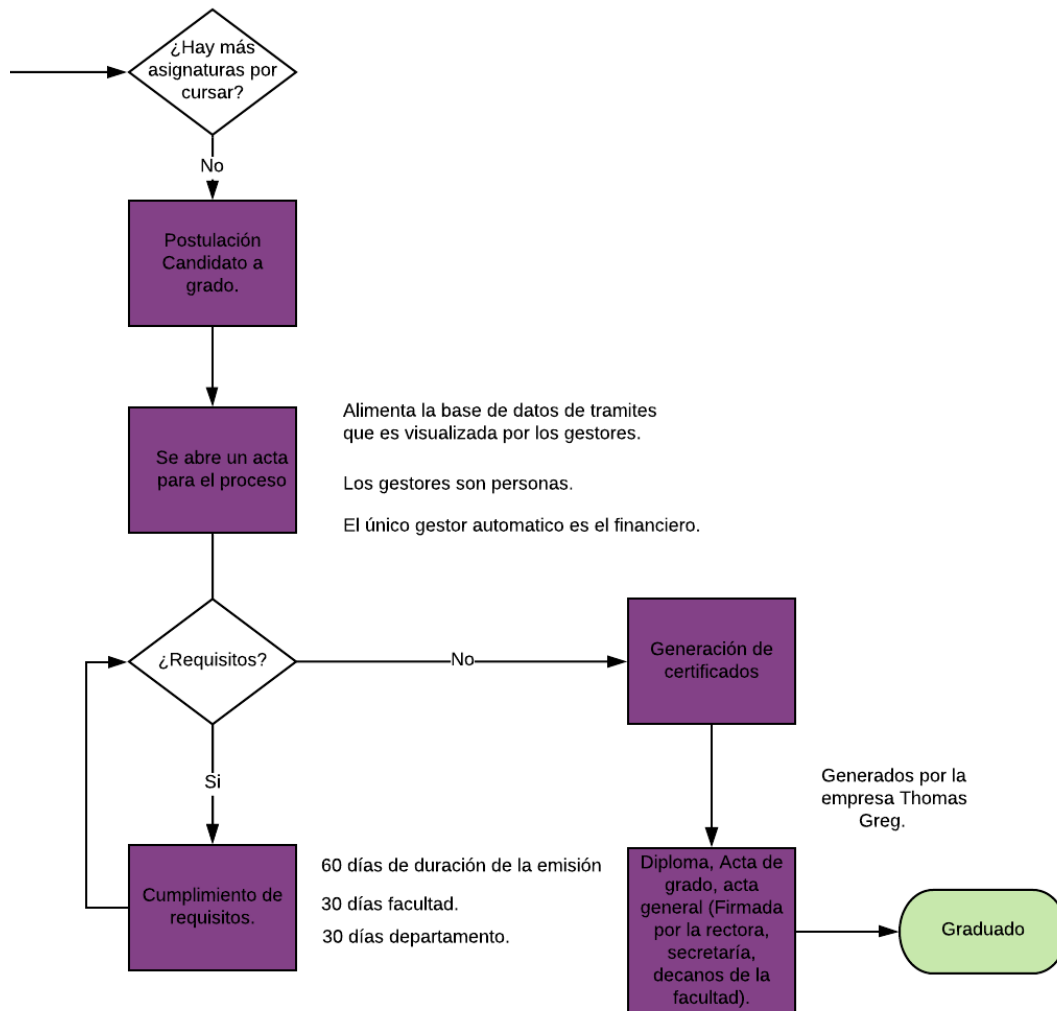




Luego, cuando el estudiante cursa las asignaturas en su totalidad se deben cumplir unos requisitos para poder graduarse. Estos requisitos son:

- Certificado de presentación de las pruebas saber pro.
- Paz y salvo con los gestores financieros de biblioteca, laboratorio y audiovisuales.
- Culminación en su totalidad el plan de estudios del programa académico.
- Pago de los derechos de grado.

El proceso para poder graduarse una vez las asignaturas son cursadas en su totalidad, es el siguiente:



## *Seguridad*

La seguridad es esencial en el manejo de información de los datos que se registran a lo largo de la vida universitaria. Un cambio en los datos sin autorización crearía fraude. Por lo tanto, se muestra a continuación la información recogida, en torno a la seguridad de la información, que maneja la universidad en los registros académicos de sus estudiantes.

- Los profesores como medio de autenticación manejan un usuario y contraseña para acceder a la Pantalla de introducción de actas y la aplicación web de actas.
- Los usuarios pueden consultar las actas y realizar acciones solo si tienen los perfiles y permisos que correspondan.
- La visualización de las actas de la asignatura solo es posible por los profesores titulares de la asignatura o alguien autorizado para hacerlo.
- Las calificaciones parciales de los estudiantes se guardan en una tabla y las calificaciones definitivas se almacenan en la tabla correspondiente.
- El área de auditoría de la universidad tiene acceso al registro de calificaciones más no a las actas correspondientes.
- Los diplomas físicos tienen dos películas, una con logotipos de la universidad y la con logotipos de la empresa que los elabora (Thomas Greg).

## *Verificación*

La universidad debe brindar a el ministerio de educación nacional la información que este le pida para comprobar que el estudiante cumple con todos los requerimientos para entrar al mundo laboral. De igual forma, los contratistas tienen la necesidad de comprobar la veracidad de las pruebas que presenta un aspirante.

Aquí se presentan la información recogida en este punto.

- El ministerio de educación nacional hace reunión con las universidades con el fin de compartir las disposiciones que deben cumplirse.
- El ministerio de educación nacional pide registros de la vida del estudiante, de sus padres, carrera, cultura, deporte u otras actividades en las que incurrió el estudiante en su vida universitaria.

- La información de los estudiantes es subida a un sitio web habilitado por el Ministerio de educación nacional.
- Para comprobar la veracidad de un diploma se puede buscar en el sitio del ministerio de educación nacional.
- Si el estudiante no se encuentra en este sitio, se debe enviar el diploma físico a la universidad, con el fin de que esta lo verifique y dé el visto bueno.

### *Falencias*

A medida que se conocía como funcionaba el manejo de registros académicos en la universidad, se fueron encontrando algunas falencias que deberían ser mejoradas. Estas falencias afectan la seguridad de la información de los registros académicos de los estudiantes. A continuación, se muestran:

- Los profesores realizan modificaciones a los registros de sus estudiantes sin controles estrictos.
- La única vía de autenticación existente por los profesores es la autenticación con usuario y contraseña. Por lo tanto, si la contraseña es descubierta por un alumno, este podría hacer modificaciones leves en las notas sin que el profesor se de cuenta.
- Las modificaciones en las actas no se registran siempre y cuando se encuentren dentro de las fechas establecidas para cierre de actas.
- Los únicos registros que se guardan en la plataforma son los logs realizados por los profesores a las plataformas.
- Las fechas establecidas para modificaciones de notas y asistencias a final de semestre, fueron creadas más por un tema operativo, que por la seguridad de los registros que se manejan.

### *Lista de requerimientos.*

Los siguientes requerimientos deberían ser tenidos en cuenta en el momento en que se desee crear un sistema para el manejo de registros académicos en la universidad.

### *Requerimientos del Negocio.*

ID	Categoría	Descripción
1	Verificabilidad	Las asignaturas y programas alcanzados por los estudiantes pueden ser verificados sin iniciar sesión y/o tener la aplicación.
2	Funcionamiento	Para aplicar por una asignatura se debe cumplir con su respectivo prerrequisito.
3	Conexión	La aplicación funcionará en un 100% con la internet.
4	Cortes del semestre	La asignatura podrá crearse para ser cursada en los cortes deseados.
5	Asistencia	La asistencia será registrada solo después de iniciada la sesión, no antes.
6	Confidencialidad	La información de registros solo debe ser accedida con la autorización del respectivo dueño.
7	Disponibilidad	La información de los registros académicos del estudiante debería ser consultado desde cualquier dispositivo sin la necesidad de tener una cuenta activa en el aplicativo.

### *Requerimientos de usuario.*

ID	Categoría	Descripción.
1	Usabilidad	El usuario podrá filtrar las asignaturas por tipo de asignatura.
2	Autenticación.	El usuario tendrá mínimo dos factores de autenticación.
3	Alertas	El usuario recibirá alertas a su teléfono o correo sobre cambios eventos sospechosos con su cuenta.
4	Disponibilidad	Si el usuario pierde su celular podrá acceder a la información de su cuenta desde otro celular, utilizando sus factores de autenticación.

### *Requerimientos del sistema.*

ID	Categoría	Descripción.
1	Interoperabilidad	La aplicación debe funcionar para todas las plataformas.

De acuerdo con estos requerimientos ¿Qué protocolo blockchain podría ser utilizado?

Con el objetivo de desarrollar un prototipo funcional que permita aumentar la integridad, autenticidad y disponibilidad de las certificaciones académicas, se utilizó un protocolo blockchain llamado *Sirius Chain*.

Este protocolo fue elegido debido a la actividad de la comunidad blockchain que ayudó a encontrar un protocolo que reduce la curva de aprendizaje que se debe seguir para utilizar la tecnología.

Sirius Chain es el protocolo blockchain que utilizan diferentes plug-ins o core services que dan soporte a *ProximaX Sirius* [20]. Entre estos plug-ins se encuentran: Sirius Storage, Sirius Streaming y Supercontracts [21].

Sirius Chain contiene funciones centrales que permiten crear diferentes arquitecturas entorno a la blockchain, las cuales son: Cuentas, Espacios de nombres, Mosaicos, Metadatos, Multi firma multinivel, Transacciones de cadena cruzada y Transacciones agregadas.

A continuación, se presenta una breve descripción de cada una, con la información obtenida del sitio web de Proximax [22]:

#### *Cuentas*

Las cuentas contienen dos pares de llaves: pública y privada, que permiten acceder a un depósito de activos. La llave privada nunca debe ser revelada ya que esta llave es la más importante en las transacciones realizadas en la blockchain.

### *Espacios de nombres*

Los espacios de nombres permiten separar un lugar en la red descentralizada para los activos inteligentes que se deseen manipular. Se puede pensar este espacio de nombre como el nombre de un sitio web, que no puede tener el mismo nombre que otro.

### *Mosaicos*

Los mosaicos representan los activos inteligentes en la blockchain de Sirius. Estos mosaicos pueden ser desde los activos más básicos hasta los más especializados.

### *Metadatos*

Los metadatos pueden asociar a una cuenta, un mosaico o un espacio de nombre con una transacción.

Los metadatos son la forma de asociar datos del usuario en la cadena de bloques de Sirius.

### *Multi firma multi nivel*

La multi firma permite realizar transacciones donde se necesite la aprobación de diferentes usuarios. Esto permite construir flujos de trabajo o procesos de aprobación integrales.

### *Transacciones de cadena cruzada*

Estas transacciones permiten intercambiar activos entre redes blockchain públicas y privadas.

### *Transacciones agregadas*

Permite crear lotes de transacciones que se ejecutan como una sola transacción. Es decir, el lote de transacciones se ejecuta simultáneamente.

### *¿Qué algoritmo de consenso es utilizado por el protocolo?*

El algoritmo de consenso utilizado por el protocolo Sirius Chain es Proof of stake dado que Sirius es un fork de Catapult [23]. Adicionalmente, implementa el algoritmo Proof of Greed que asegura que los nodos no sean codiciosos aceptando tarifas de transacción elevadas, afectando el tiempo de generación del bloque [21].

Del protocolo Sirius Chain, se utiliza en especial la función de *multi firma multi nivel* que nos ayuda en particular a registrar los logros de los estudiantes de manera masiva utilizando los lotes de transacciones para ello. Esto, por ejemplo, cuando un profesor necesita registrar la aprobación o no del curso a un número *n* de estudiantes. Además, se utiliza cuando se necesita la autorización para certificar a un estudiante, en un programa, por parte de los administrativos que tienen la potestad de hacerlo. Así, por ejemplo, no se podrá aprobar la certificación del estudiante sin todas o una cantidad definida de firmas necesarias para ello.

### *Desarrollo de prototipo*

Teniendo en cuenta las necesidades encontradas en el trabajo de campo y las bondades que presenta el protocolo Sirius chain, se desarrolla un prototipo que demuestre la aplicabilidad potencial que esta tecnología tiene para resolver algunas de estas necesidades y otras más.

### *¿En que se basa este prototipo?*

El prototipo realizado es una aplicación básica que permite a un usuario crear un curso donde se pueda controlar los registros académicos de este, la asistencia originada por sesiones en las que se desarrolla el curso y las calificaciones que demuestran el cumplimiento de los objetivos del curso. Finalmente, la información del cumplimiento del curso es almacenado en la blockchain de Sirius Chain.

Los usuarios de este prototipo están divididos por sus roles en : creador, profesor, estudiante y validador.

A continuación, hay una breve descripción de cada uno:

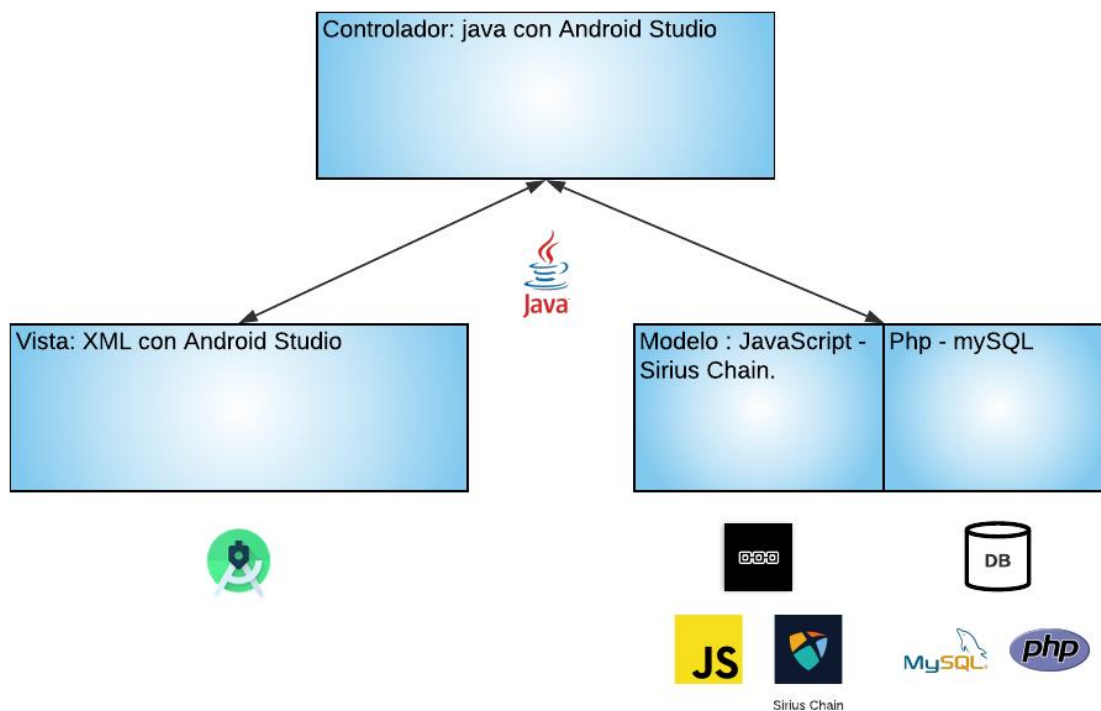
- El *creador* crea la estructura del curso para que pueda ser utilizado por el usuario profesor y el estudiante o estudiantes.
- El *profesor* ingresa la información del curso en la aplicación y registra la información de lo ocurrido en el curso por cada estudiante (asistencia y calificación).



- El *estudiante* consulta la información de su avance en el curso.
- El validador es el interesado en conocer la información del logro del estudiante.

El estudiante al cumplir con el mínimo porcentaje de asistencia y el mínimo promedio requerido en calificación, logra obtener una “insignia” que demuestra la superación del curso. La insignia es registrada en la cadena de bloques de Sirius.

En el desarrollo del prototipo se realiza un diagrama que muestra la arquitectura que tendrá este.



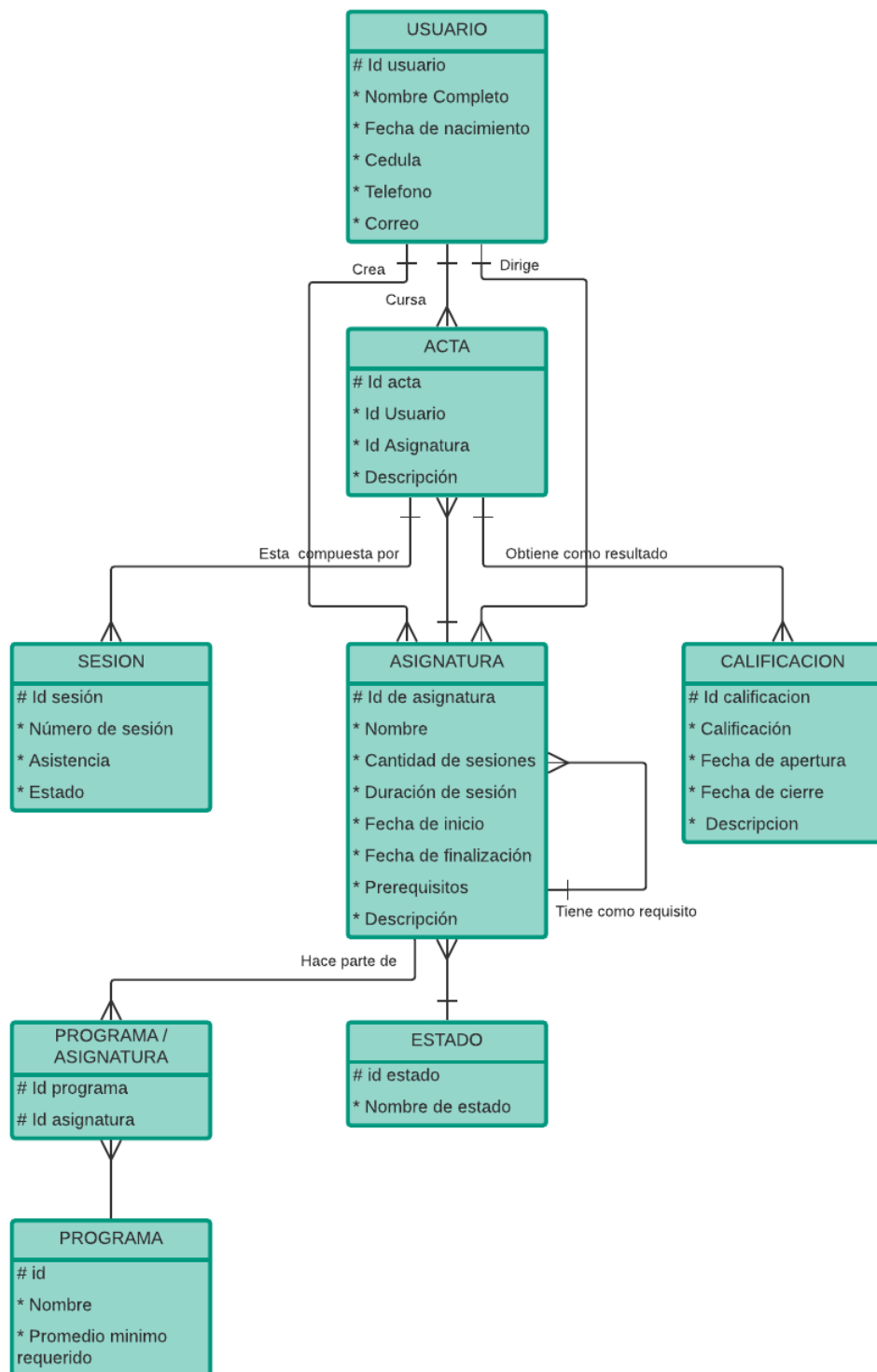
Se desarrolla el prototipo con el IDE Android Studio utilizando el lenguaje de programación java para el manejo de la lógica del prototipo, y el uso de XML para el manejo de la interfaz de este.

Además, el flujo de información se mueve en dos sectores que componen el modelo: El sector JavaScript – Sirius Chain y el sector PHP – MySQL.

En el sector JavaScript – Sirius Chain, se utiliza el SDK en JavaScript creado por ProximaX, que nos permite interactuar con la cadena de bloques de testeo o tesnet, la cual sirve para la realización de pruebas sin el gasto real de cash en las transacciones realizadas.

También, en el sector PHP – MySQL, se manejan los datos de la aplicación que involucra los usuarios, cursos, actas, entre otros.

Adicionalmente, la base de datos principal se representa en el siguiente diagrama entidad relación:



## Conclusiones

De acuerdo con lo encontrado en la investigación en la universidad Jorge Tadeo Lozano, se encuentra que no hay una política definida en la autenticación de los usuarios, más allá de la autenticación por usuario y contraseña, lo que provoca una vulnerabilidad que debe ser revisada y solucionada. Además, existe una cultura organizacional que no le da la importancia que merece al tema de la seguridad de la información y los hechos que implicarían una vulneración de los datos guardados de los estudiantes.

Por esta razón, se propusieron medidas que deben ser adoptadas con el fin de reducir las fallas que existen en la forma en que se maneja la información del estudiantado. En esta búsqueda, se propone blockchain, una tecnología que aumenta la integridad, disponibilidad y confidencialidad de la información. La integridad porque los datos en su característica de inmutabilidad vuelven muy difíciles que la información almacenada en la misma cambie sin ser notado. La disponibilidad porque en las redes publicas de blockchain la información contenida es 100% libre al público. La confidencialidad porque en el entorno blockchain la identidad está resumida en la llave pública, dirección y llave privada, ya es tú responsabilidad no revelar tus identificadores.

Finalmente, las medidas se respaldan con un prototipo que utiliza una plataforma (de muchas) que contiene guías y herramientas que facilitan el desarrollo de aplicaciones descentralizadas, lo que revela lo fácil de utilizar esta tecnología y el aumento de la popularidad de esta tecnología, pues cada vez más protocolos son creados con capas añadidas a las existentes, que revelan nuevas fortalezas que esta tecnología ofrece a la humanidad.

## Recomendaciones

En el desarrollo de este trabajo, se encontraron diferentes obstáculos en la consecución de la información requerida, para dar mejores conclusiones sobre el desempeño de la manera en que actualmente se manejan los registros académicos en la universidad. Uno de ellos fue el acceso a la información, dado que el encargado de manejar estos registros es un ente privado que por cuestiones de privacidad no revela información necesaria para este proyecto. Por lo tanto, se debe primero hacer un trabajo de reconocimiento para saber a qué podemos tener acceso y a qué no.

Además, el hecho de no poseer los conocimientos requeridos para trabajar con la tecnología blockchain hizo lenta la curva de aprendizaje de los diferentes protocolos tenidos en cuenta para este trabajo. Por lo tanto, el aprendizaje de esta tecnología es un trabajo con amplios conceptos por comprender y deben ser comprendidos muy bien antes de emprender un camino para su adopción.

Finalmente, en el ambiente universitario hay preguntas que quedan abiertas respecto a la veracidad de la información. Por ejemplo, ¿cómo sabemos que un maestro, al momento de ingresar una calificación, lo hace de manera autónoma? Si un estudiante obtiene una calificación favorable sin merecerlo, o a través de medios inmorales ¿Es posible detectarlo?

## **Agradecimientos**

Agradezco a mi madre, familia, y compañeros que siempre estuvieron apoyándome en toda mi etapa universitaria. De igual forma, a los profesores, que desde las aulas y de forma remota, ayudaron en mi formación profesional.

## Referencias

- [1] J. T. Galarza, Demanda por educación superior: proyecciones hasta 2025, Bogotá: Pontificia Universidad Javeriana, 2015.
- [2] G. C. Trochez, «El Heraldo,» 02 Febrero 2015. [En línea]. Available: <https://www.elheraldo.co/judicial/asi-operaba-la-red-de-alteracion-de-notas-en-la-udea-182681>. [Último acceso: 2019].
- [3] J. L. Bran, «El Colombiano,» 23 Septiembre 2013. [En línea]. Available: [https://www.elcolombiano.com/historico/directivas\\_de\\_upb\\_investigacion\\_caso\\_de\\_fraude\\_en\\_calificaciones-KYec\\_261784](https://www.elcolombiano.com/historico/directivas_de_upb_investigacion_caso_de_fraude_en_calificaciones-KYec_261784). [Último acceso: 2019].
- [4] R. Judicial, «El espectador,» 05 Julio 2017. [En línea]. Available: <https://www.elespectador.com/noticias/judicial/desmantelan-cartel-de-falsificadores-de-notas-en-u-de-la-amazonia-articulo-701642>. [Último acceso: 2019].
- [5] H. Clifton, M. Chapman y S. Cox, «BBC,» 16 Enero 2018. [En línea]. Available: <https://www.bbc.com/news/uk-42579634>. [Último acceso: 2019].
- [6] U. I. d. E. País, «El País,» 07 Junio 2015. [En línea]. Available: <https://www.elpais.com.co/california/exclusivo-en-el-valle-ya-han-descubierto-a-mas-de-1-200-profesionales-con-titulo-falso.html>. [Último acceso: 2019].
- [7] W. F., «Storing digital certificates using blockchain,» Norwegian University of Science and Technology, 2017.
- [8] D.-H. Nguyen, D.-N. Nguyen-Duc, N. Huynh-Tuong y H.-A. Pham, «CVSS: A Blockchainized Certificate Verifying Support System,» ACM, 2018.
- [9] D. E. Plaza, «Diseño y desarrollo de diplomas academicos digitales mediante la tecnología blockchain,» Universidad Javeriana, Bogotá, 2018.
- [1] A. Grech y A. Camilleri, «Blockchain in education,» Publications Office of the European Union, 2017.
- [1] «Resiliente Digital,» [En línea]. Available: <https://resilientdigital.com/que-es-la-auto-identidad-soberana-ssi-self-sovereign-identity/>. [Último acceso: 2020].
- [1] A. Keys, «Bitcoin Mexico,» 2020. [En línea]. Available: <https://www.bitcoin.com.mx/predicciones-para-blockchain-en-2020/>. [Último acceso: 2020].
- [1] A. Preukschat, Blockchain: La revolución industrial de internet, 2017: Centro Libros . 3]
- [1] A. Narayanan y J. Clark, «Bitcoin's Academic Pedigree,» *Acm queue*, vol. 60, nº 12, pp. 36-45, 2017.
- [1] M. E. Power, «OneSpan,» 11 Octubre 2017. [En línea]. Available: <https://www.onespan.com/blog/difference-between-e-signatures-and-digital-signatures-infographic>. [Último acceso: 2020].

- [1 S. Seang y D. Torre, «Proof of Work and Proof of Stake consensus protocols: a
- 6] blockchain application for local complementary currencies,» Université Nice Sophia, Valbonne, 2018.
- [1 N. Rodriguez, «101 Blockchains,» 2018. [En línea]. Available:
- 7] <https://101blockchains.com/es/algoritmos-de-consenso-blockchain/>. [Último acceso: 2019].
- [1 E. NEM, «NEM,» [En línea]. Available: <https://nem.io/es/inversores/la-cosecha-poi/>.
- 8] [Último acceso: 2020].
- [1 M. Munford, «bbc news,» BBC, 2019. [En línea]. Available:
- 9] <https://www.bbc.com/mundo/noticias-49369672>. [Último acceso: 2020].
- [2 ProximaX Sirius, «ProximaX,» [En línea]. Available: <https://www.proximax.io/>.
- 0]
- [2 ProximaX Sirius, «High Level Technical White Paper V2.0».
- 1]
- [2 ProximaX Sirius, «ProximaX,» 2020. [En línea]. Available:
- 2] <https://bcdocs.xpxsirius.io/docs/built-in-features/>.
- [2 NEM, «NEM,» [En línea]. Available: <https://nem.io/catapult/>.
- 3]
- [2 T. E. Board, «The New York Times,» 20 Mayo 2015. [En línea]. Available:
- 4] <https://www.nytimes.com/2015/05/20/opinion/a-rising-tide-of-bogus-degrees.html>. [Último acceso: 2019].
- [2 M. Chacón, «kienyke,» 31 Agosto 2016. [En línea]. Available:
- 5] <https://www.kienyke.com/historias/diplomas-falsos-colombia>.

Anexos (1): Preguntas relacionadas con los involucrados en el proyecto.



**1. Preguntas involucradas con los involucrados en el proyecto.**

<b>¿Qué quiero obtener?</b>	<b>¿Qué pregunta voy a hacer?</b>
<b>Recipientes</b>	
<b>¿Qué conocen los usuarios acerca de los certificados?</b>	¿Qué tipos de certificados académicos ha obtenido?
	¿Cómo verifican la autenticidad de sus certificados?
<b>Importancia que le dan las personas a los certificados obtenidos.</b>	De los certificados que tiene, ¿Cuáles le han servido más?
	¿Qué hace con los certificados que ha recibido?
	¿Ha utilizado estos certificados en alguna ocasión importante?
	¿Ha extraviado alguno de los certificados obtenidos?
	¿Qué proceso tuvo que seguir para recuperar su o su certificado?
<b>Falsificación de certificados</b>	¿Cuándo ha falsificado un documento?
	¿Conoce gente que ha falsificado un documento?
	¿Qué certificados serían fáciles de falsificar?
<b>Emisores</b>	
<b>Razón para expedir los certificados</b>	¿Qué certificaciones ofrece la entidad?
<b>Requisitos</b>	¿Qué requisitos deben cumplir las personas para certificarse en cada uno de los logros que ofrece? ¿Qué debe cumplir en general un estudiante que desee certificarse?
<b>Proceso de emisión</b>	¿Qué se otorga como certificación a quien logra cumplir todos los requisitos

	establecidos para certificarse? ¿Qué elemento físico o digital se utiliza como certificación?
	¿Qué elementos de seguridad contra falsificaciones presenta esta forma de certificación?
	¿Cuánto tiempo dura el proceso de emisión de un certificado?
	¿Hay algún límite de tiempo de validez de los certificados otorgados?
	¿Cuáles son los beneficios de este tipo de certificación?
	¿Cuáles son los problemas de este tipo de verificación?
	¿Qué cosa mejoraría el proceso de emisión de certificados?
<b>Requisitos legales</b>	¿Qué requisitos y procesos se deben cumplir con el Gobierno Nacional para que se reconozcan estos certificados como válidos?
<b>Reclutadores de talento humano</b>	
<b>Proceso de contratación</b>	¿Cómo comprueban las certificaciones de alguien que se postula a un puesto?
<b>Comprobación de aptitudes</b>	¿Cómo se comprueban las aptitudes del personal?
	¿Qué podría facilitar el proceso de certificación de aptitudes del personal?
<b>Falsificaciones encontradas</b>	¿Qué casos han encontrado de falsificación de certificados?