

**DESARROLLO DE UN SISTEMA DE CERTIFICACIÓN ACADÉMICA EN UNA
BLOCKCHAIN PÚBLICA**

AUTOR

BELMAR SANTANILLA GUTIÉRREZ

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

FACULTAD DE INGENIERÍA

TECNOLOGÍA EN DESARROLLO DE SOFTWARE

MEDELLÍN

2022

**DESARROLLO DE UN SISTEMA DE CERTIFICACIÓN ACADÉMICA EN UNA
BLOCKCHAIN PÚBLICA**

AUTOR

BELMAR SANTANILLA GUTIÉRREZ

**Trabajo de grado para optar al título de
TECNÓLO EN DESARROLLO DE SOFTWARE**

Asesor Técnico

MSc. OSCAR JULIÁN GALEANO ECHEVERRI

Asesor Metodológico

MSc. OSCAR IGNACIO BOTERO HENAO

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

FACULTAD DE INGENIERÍA

TECNOLOGÍA EN DESARROLLO DE SOFTWARE

MEDELLÍN

2022

Contenido

	Pág.
Introducción	11
1. Planteamiento del problema.....	12
1.1 Descripción.....	12
1.2 Formulación	13
2. Justificación	14
3. Objetivos	15
3.1 Objetivo general	15
3.2 Objetivos específicos.....	15
4. Marco teórico.....	16
4.1 Antecedentes	16
4.2 Enfoque Teórico	17
4.2.1 Blockchain Pública.	17
4.2.2 Sistemas de Certificación Académica.	18
4.2.3 Criptografía.....	18
4.2.4 IPFS.	19
4.2.5 Bloque.....	19
4.2.6 API.....	20
4.2.7 Cardano.....	20
4.2.8 Mecanismos de Consenso.....	20
4.2.9 Laravel.	21
5. Metodología.....	22
5.1 Tipo de proyecto.....	22
5.2 Método	22
5.3 Instrumentos de recolección de información	23
5.3.1 Fuentes primarias	23
5.3.2 Fuentes secundarias.	24
5.4 Proceso metodológico.....	24
5.4.1 Fase 1: Diseño.....	24
5.3.2 Fase 2: Desarrollo	26
5.3.3 Fase 3: Implementación.....	26

6.	Resultados del proyecto	27
6.1	Diseño	27
6.1.1	Inventario de Contenidos y Funcionalidades necesarios en la Interfaz del Usuario ...	28
6.1.2	Modelo de la Estructura de Datos	29
6.1.3	Bosquejo de Interfaz de la Aplicación	30
6.1.4	STACK.	34
6.2	Desarrollo.....	35
6.2.1	Control de Versiones y Servidores de Desarrollo.....	35
6.2.2	Desarrollo de las Historias de Usuario.	36
6.2.3	Pruebas de Integración.....	39
6.3	Implementación	40
6.4	Discusión	40
7.	Conclusiones	43
8.	Recomendaciones	44
9.	Referencias bibliográficas.....	45
10.	Anexos	48

Lista de figuras

	Pág.
<i>Figura 1.</i> Fases del proyecto.....	24
<i>Figura 2.</i> Modelo entidad relación.	30
<i>Figura 3.</i> Pantalla de inicio de sesión.	31
<i>Figura 4.</i> Maestro de estudiantes, promociones, certificaciones y solicitudes de validación. ...	32
<i>Figura 5.</i> Interfaz que representa la forja del certificado en la blockchain pública.	33
<i>Figura 6.</i> Arquitectura Plug and Play (PnP).....	36
<i>Figura 7.</i> Interfaz de la aplicación donde se gestiona un estudiante	37
<i>Figura 8.</i> Principales características para forjar el certificado.	38
<i>Figura 9.</i> Diagrama de flujo para validar un certificado en la aplicación.	39

Lista de tablas

	Pág.
Tabla 1. <i>Hallazgos</i>	27
Tabla 2. <i>Módulos del sistema</i>	28
Tabla 3. <i>Requerimientos</i>	35

Lista de anexos

	Pág.
Anexo A. Entrevistas.	48
Anexo B. Pila de Producto.....	49
Anexo C. Configuración Inicial del Proyecto.....	52
Anexo D. Manual de Usuario Final.	54
Anexo E. Despliegue en Producción.	62

Resumen

DESARROLLO DE UN SISTEMA DE CERTIFICACIÓN ACADÉMICA EN UNA BLOCKCHAIN PÚBLICA

BELMAR SANTANILLA GUTIÉRREZ

Se documenta el proceso llevado a cabo para el desarrollo de un sistema de certificación académica utilizando blockchain como herramienta tecnológica. De tal forma que se pueden aprovechar las ventajas inherentes a este tipo de sistemas para realizar la certificación académica de estudiantes.

Enmarcado dentro de la investigación aplicada, ya que, en primer lugar, se realiza una entrevista estructurada con el fin de obtener información relevante sobre el proceso de generación de certificados académicos, y en segundo lugar, para el desarrollo del sistema de certificación, se utiliza la metodología de desarrollo SCRUM que brinda un marco de trabajo flexible para proyectos de software con las características propuestas. Adicionalmente, se aprovechan herramientas de código abierto, así como interfaces de programación para interconectar los distintos componentes del sistema incorporando el uso de la blockchain pública denominada *Cardano*.

Se describe una metodología de tres etapas comenzando por el diseño, en donde se recopilan las necesidades de los usuarios finales. En segundo lugar, el desarrollo, etapa en la cual se explica el proceso de implementación y se detallan los componentes del sistema. Finalmente, en la tercera fase se exponen en detalle las instrucciones para desplegar la aplicación en un ambiente de producción.

Palabras claves: Certificación académica, Blockchain, Cardano, Código abierto, Desarrollo de software

Abstract

DEVELOPMENT OF AN ACADEMIC CERTIFICATION SYSTEM IN A PUBLIC BLOCKCHAIN

BELMAR SANTANILLA GUTIÉRREZ

The process carried out for the development of an academic certification system using blockchain as a technological tool is documented in such a way that the inherent advantages of this type of systems can be used to carry out the academic certification of students.

Framed within the applied research, since in the first place, a structured interview is carried out in order to obtain relevant information about the process of generating academic certificates, and secondly, for the development of the certification system, the SCRUM development methodology that provides a flexible framework for software projects with the proposed characteristics.

Additionally, open source tools are used, as well as programming interfaces to interconnect the different components of the system, incorporating the use of the public blockchain called Cardano.

A three-stage methodology is described, starting with the design, where the needs of the end users are collected. Second, development, a stage in which the implementation process is explained and the system components are detailed. Finally, in the third phase, the instructions to deploy the application in a production environment are explained in detail.

Palabras claves: Academic Certification, Blockchain, Cardano, Open Source, Software Development

Glosario

Blockchain: es un libro de contabilidad digital donde se registran todas las transacciones digitales. Crece constantemente a medida que se le agregan bloques "completados". Cada bloque contiene un hash criptográfico del bloque anterior, una marca de tiempo y datos de la transacción.

Cardano: es una plataforma *blockchain* de tercera generación que es de código abierto y descentralizado. El objetivo de Cardano es facilitar las transacciones entre pares y crear contratos inteligentes que sean adaptables y escalables, sin comprometer la seguridad.

API: significa "Interfaz de programación de aplicaciones" y se refiere a los diversos medios que tiene un sistema de información para comunicarse internamente con otro software.

Certificación Académica: es un documento que prueba que un estudiante ha completado satisfactoriamente un programa de estudio establecido por alguna institución académica.

Código Abierto: es un término utilizado para describir el software que es gratuito y está disponible para que cualquiera lo use o modifique.

Laravel: es un *framework* web construido con el lenguaje PHP de código abierto, creado por Taylor Otwell y destinado al desarrollo de aplicaciones web siguiendo el patrón arquitectónico modelo-vista-controlador (MVC).

Introducción

En este trabajo se documenta el proceso llevado a cabo para el desarrollo de un sistema de certificación académica utilizando *blockchain* como herramienta tecnológica de gran utilidad para hacer registros públicos, inmutables y seguros. De esta manera, la Institución Universitaria Pascual Bravo puede aprovechar las ventajas inherentes a este tipo de sistemas para realizar la certificación académica de sus estudiantes.

Este proyecto se enmarca dentro de la investigación aplicada, ya que, en primer lugar, se realiza una entrevista estructurada con el fin de obtener información relevante sobre el proceso de generación de certificados académicos, y en segundo lugar, para el desarrollo del sistema de certificación, se utiliza la metodología de desarrollo *SCRUM* que brinda un marco de trabajo flexible para proyectos de software con las características propuestas. Además, se aprovechan herramientas de código abierto, así como interfaces de programación para interconectar los distintos componentes del sistema incorporando el uso de la *blockchain* pública de tercera generación conocida como *Cardano*. Se describe una metodología de tres etapas comenzando por el diseño, en donde se recopilan las necesidades de los usuarios finales. En segundo lugar, el desarrollo, etapa en la cual se explica el proceso de implementación y se detallan los componentes del sistema. Finalmente, en la tercera fase se exponen en detalle las instrucciones para desplegar la aplicación en un ambiente de producción.

Dentro de los resultados se obtiene una aplicación web capaz de generar certificados digitales inmutables registrados en la cadena de bloques, resolviendo de esta manera el problema planteado en el proyecto, acerca del uso de este tipo de sistemas para agilizar los procesos de certificación y validación de títulos académicos en la institución.

1. Planteamiento del problema

1.1 Descripción

Los certificados académicos son parte integral de la hoja de vida de los estudiantes de la Institución Universitaria Pascual Bravo. Los mecanismos actuales para generar este tipo de certificados están sujetos a diferentes situaciones que pueden generar inconvenientes, por ejemplo, existen grandes dificultades para verificar su autenticidad de una manera ágil y confiable. De igual forma, son susceptibles a la falsificación, debido a los pocos controles que existen al momento de verificar la autenticidad de este tipo de documentos.

En la actualidad, se están desarrollando prototipos de sistemas que incorporan tecnologías para mantener la inmutabilidad de registros digitales, lo que permite un caso de uso para los estudiantes de diferentes instituciones. Aun así, la Institución Universitaria Pascual Bravo no cuenta con un desarrollo tecnológico de expedición de certificados digitales que avale los conocimientos adquiridos en carreras de tecnología y pregrado, que puedan ser consultados de manera rápida, sencilla y segura por terceros interesados.

La tecnología blockchain ha alcanzado un gran desarrollo en la industria financiera y ha probado su confiabilidad. Por su parte, en el ámbito académico, múltiples universidades a nivel mundial empiezan a incursionar y a desarrollar los primeros pilotos usando esta tecnología, incorporándola como un caso de uso para la generación de certificados académicos. Sin embargo, en Colombia su penetración en la academia o las entidades de gobierno aún es muy baja. La implementación de un sistema con estas características impulsa el avance tecnológico de la institución y la ubica a la vanguardia de las innovaciones tecnológicas ya que los certificados basados en *blockchain* generan credibilidad.

De acuerdo con Allesie, Sobolewski y Vaccari (2019) citados por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (2022) “La tecnología *blockchain* sigue en desarrollo, razón por la cual el enfoque de la política pública sugiere el desarrollo de proyectos piloto focalizados para así identificar los casos de uso clave y definir un

proceso de certificación adecuado.” (p. 40). Por lo tanto, se propone el desarrollo de un producto mínimo viable que brinde un mecanismo de certificación académica utilizando una *blockchain* pública que habilite una verificación confiable, segura y rápida.

1.2 Formulación

¿Cómo desarrollar un sistema de certificación académica en una *blockchain* pública que permita una verificación confiable, segura y rápida?

2. Justificación

Este proyecto busca desarrollar un sistema de certificación académica en una *blockchain* pública para aprovechar las ventajas que ofrece este tipo de tecnología, tales como, mantener los registros descentralizados, distribuidos, seguros, confiables y accesibles de manera rápida. Las principales características que se mencionan sobre esta tecnología pretenden ser utilizadas para prevenir falsificaciones o fraudes a los que los sistemas de certificación actuales son vulnerables.

La topología de red descentralizada y las funciones criptográficas que se utilizan en *blockchain*, son de especial utilidad por su transparencia al brindar un registro público y rastreable de toda la información disponible en la red. Por esta razón, ofrecen la posibilidad de realizar consultas externas beneficiando a entidades interesadas en verificar el historial académico de un estudiante. Además, resulta útil que los estudiantes tengan acceso a su certificación de manera instantánea y validen así su información académica ante cualquier entidad.

Se hace necesario que la Institución Universitaria Pascual Bravo cuente con una aplicación web que incorpore un sistema de información capaz de forjar certificaciones digitales asociadas a los estudiantes. De esta manera, se incentiva el desarrollo de aplicaciones que aprovechen las ventajas de la tecnología *blockchain* para que surjan nuevas formas de crear sistemas de información.

3. Objetivos

3.1 Objetivo general

Desarrollar un sistema de certificación académica en una *blockchain* pública para la Institución Universitaria Pascual Bravo.

3.2 Objetivos específicos

- Diseñar el modelo de la estructura de los datos, el inventario de funcionalidades, la arquitectura y la interfaz de la aplicación.
- Desarrollar las historias de usuario que describen el comportamiento ideal de la aplicación.
- Implementar el sistema en un ambiente de integración que habilite el uso de las funcionalidades implementadas, para garantizar su correcto funcionamiento.

4. Marco teórico

4.1 Antecedentes

Para emitir certificados seguros y que sean auténticos, Beltrán y Ramírez (2020) se plantearon como objetivo modelar un sistema de *blockchain* que permitiera autenticar certificados estudiantiles en instituciones educativas de Colombia. Por esta razón, utilizaron “una metodología de diseño y procesamiento en la nube, normalizada y propuesta por Google, cuya función principal es adaptar servicios y entornos de trabajos a sistemas totalmente digitales” p. 96. De esta manera, las fases para realizar el producto comienzan con una identificación del servicio, la definición de estructuras y sus requerimientos e identificación de instrumentos. De esta forma, reconocieron las características y funcionalidades del servicio, para resolver las preguntas más frecuentes y definir cuál es la importancia de implementar un sistema como el propuesto.

Dado lo anterior, precisaron una estructura que contenía tres principales activos que son los nodos, los servidores y las bases de datos. Adicionalmente, la arquitectura se ha basado en un modelo cliente-servidor. La aplicación está compuesta por una interfaz de usuario que realiza peticiones a un servidor y éste a su vez verifica la información directamente en la red *blockchain*. Gracias a esto, la investigación logró explicar el funcionamiento teórico-práctico de esta tecnología y permitió el análisis de las principales características que la componen, incluyendo los múltiples usos que podría tener.

Por otra parte, Cuervo, Rodríguez y Sánchez (2019), llevaron a cabo una investigación exhaustiva de trabajos relacionados con la generación y validación de certificados académicos digitales implementando *blockchain*. Para la realización del sistema propuesto se plantearon tres fases. En la primera de estas, se realiza la extracción de los requerimientos tanto funcionales como no funcionales para definir de manera concreta las capacidades generales del sistema. Además, realizaron una revisión de trabajos relacionados, identificando posibles riesgos de seguridad a los que el sistema podría verse expuesto. En la segunda fase, diseñaron los componentes necesarios para la correcta ejecución de las funcionalidades propuestas. Por

último, realizaron pruebas de concepto para verificar el correcto funcionamiento y las posibles mejoras o correcciones que pudiera necesitar. Gracias a la investigación para el desarrollo de esta aplicación, se logró evidenciar que este tipo de sistemas impacta de manera positiva la problemática de certificados académicos falsificados.

Por último, Ruiz (2020), en su trabajo *Diplomas académicos sobre una plataforma blockchain*, describe la problemática sobre los certificados académicos falsos y hace especial énfasis en la dificultad de ejercer un control sobre este tipo de procedimientos. Por tal motivo, plantea su investigación desde dos puntos de vista, el académico y el social, evidenciando así que estos problemas de falsificación no solamente suceden en el ámbito nacional, sino a nivel global. De igual forma, identifica una problemática puntual relacionada con este tipo de proyectos, encontrando que el desarrollo de sistemas de certificación en *blockchain* suelen estar orientados principalmente a aplicaciones financieras.

En consecuencia, el autor propone un nuevo caso de uso para la generación de certificados académicos en línea. En primera instancia, identificó el procedimiento actual de la generación de certificados y los puntos de dolor en estos procesos. Concretamente, se halló la ausencia de un mecanismo para la verificación de diplomas y la complejidad para legalizar el mismo ante las autoridades educativas del orden nacional. Este hallazgo permitió entender en detalle los procesos en la emisión y verificación de estos diplomas, logrando concluir que *blockchain* es el tipo de tecnología que ayuda a resolver estas problemáticas.

4.2 Enfoque Teórico

4.2.1 Blockchain Pública. El término blockchain, se refiere al almacenamiento de la información en una base de datos distribuida, de tal forma que se puede garantizar su inmutabilidad y trazabilidad. “Es una tecnología considerada como disruptiva, que evoluciona periódicamente y sobre la cual se han desarrollado además de criptomonedas otras aplicaciones que aprovechan sus características” (Aparco, et al., 2021, p. 49). Esta es considerada una de las principales tecnologías que conforman la cuarta revolución industrial. Gracias a sus múltiples aplicaciones es accesible para entidades, individuos o instituciones que pueden participar en la red y validar las transacciones que allí se ejecuten.

Ahora bien, en una *blockchain* pública, cualquier usuario puede unirse y participar a través de los diferentes mecanismos, tales como, la creación y verificación de transacciones, o la simple participación a través del intercambio de activos. Así, “cualquiera puede leer un blog público, enviar transacciones o participar en el proceso de consenso” (MinTIC 2022, p.26). Por lo tanto, al tratarse de una red pública y distribuida, todos los participantes están en igualdad de condiciones y ninguno tiene la capacidad de imponer o modificar los protocolos de la red.

4.2.2 Sistemas de Certificación Académica. Consiste en implementar un proceso utilizando la tecnología Blockchain que permita almacenar y verificar certificados digitales que se emiten para los estudiantes egresados de una institución académica. De acuerdo con Moscoso, *et al.* (2019), “el panorama para utilizar esta tecnología es prometedor, ya que se pueden encontrar muchos entornos en los que tanto entidades públicas como privadas se benefician del esquema de transacciones aseguradas que se obtiene al usar Blockchain” (p. 26)

4.2.3 Criptografía. La criptografía es un mecanismo matemático que se utiliza para generar un par de llaves que permiten autenticarse en un sistema *blockchain*. A través de una llave privada se firman las transacciones y se autoriza la modificación de los registros en el sistema. Asimismo, utilizando una llave pública, otros usuarios en la red pueden interactuar entre sí intercambiando información y activos. De acuerdo con Domínguez (2021) “El software de criptografía genera pares de claves criptográficas públicas y privadas vinculadas por un algoritmo matemático. Estos pares son únicos, el programa sólo los produce una vez y los atribuye al usuario en concreto que solo recibe una clave privada”. (p. 7)

Adicionalmente, la criptografía usa funciones de *hash* que son algoritmos matemáticos que reciben un parámetro de entrada de cualquier tamaño y produce una salida con una cantidad fija de caracteres a la cual no se le puede aplicar ninguna reversión para obtener el valor original de la entrada. Como lo menciona González Conejero (2022) “las funciones de *hash* tienen muchas aplicaciones. La más inmediata es la comparación sencilla de dos archivos. Sin embargo son útiles si se quiere almacenar la representación de una contraseña en una base de datos”. (p 3). Gracias a esto, se puede almacenar información en una red pública manteniendo la privacidad de los datos y garantizando su inmutabilidad a través de las funciones *hash*.

4.2.4 IPFS. El sistema de archivos interplanetario, es un protocolo de red por pares diseñado para almacenar y compartir contenido hipermedia de manera descentralizada. De tal manera que, utilizando este protocolo los usuarios de la red podrán compartir archivos digitales inmutables capaces de verificar la autenticidad de un documento. “Al utilizar esta alternativa, la información estaría globalmente disponible tanto en la cadena de bloques como en el IPFS, al mismo tiempo que permite reducir los costos de almacenamiento dado que se encuentran guardados directamente en la red”. (Moreno Marín, 2022, p. 29). Cuando se agrega un archivo en este protocolo, el archivo se divide en fragmentos que se codifican utilizando criptografía, para posteriormente ser accedidos a través de un identificador único. Otros nodos en la red utilizan el identificador para encontrar las diferentes partes distribuidas y componer el archivo para su visualización. Adicionalmente, cada versión del contenido almacenado genera un *hash* criptográfico diferente, por lo tanto, ningún cambio sobre escribe el historial.

4.2.5 Bloque. Un bloque es un archivo que contiene un registro de las transacciones realizadas en la red y que requiere de una validación para ser incluido dentro del historial. Este archivo contiene un encabezado en el cual se detallan un número de bloque, un *hash* que contiene el bloque actual y un *hash* que contiene el bloque anterior, formando así una cadena que incluye las transacciones que realizan los usuarios. “Los usuarios pueden enviar transacciones candidatas a ser registradas en el libro mayor sin que esto implique que serán incluidas en un nuevo bloque. Existe un apartado correspondiente a los mecanismos de consenso que finalmente aprueban la transacción” (Reyes Sánchez, 2022, p. 174)

Existen múltiples mecanismos para validar los bloques de transacciones, el más reconocido se denomina prueba de trabajo y consiste en resolver un problema matemático complejo utilizando fuerza bruta. Por tal motivo, se trata de un mecanismo que consume grandes cantidades de energía resultando nocivo para el medio ambiente. Por otro lado, Kiyias *et al.* (2019), considera el gasto energético producido por los protocolos basados en pruebas de trabajo, puesto que para generar un bloque de transacciones se requiere un alto número de funciones *hash* resultando en grandes demandas de energía. Como resultado de su investigación propone un mecanismo de consenso denominado *ouroboros*. Este mecanismo está basado en un sistema de prueba de participación que implica el reemplazo de los nodos mineros por nodos

validadores, capaces de utilizar los activos de los usuarios participantes para validar las transacciones en la red. En definitiva, este tipo de algoritmos optimiza el consumo de energía y mantiene la seguridad en la red a través de este mecanismo de consenso.

4.2.6 API. Es un acrónimo de *Application Programming Interface*, y esencialmente son un conjunto de funcionalidades y procesos que expone una librería o un servicio en internet para que sea consultado programáticamente. De acuerdo con Plaza Estévez *et al.* (2016), quien las define como las funcionalidades que aporta un software para facilitar que este pueda ser utilizado por otro para mejorar resultados o para aprovechar sus características. Asimismo, podría considerarse como la interacción “*software-to-software*”.

4.2.7 Cardano. Es una blockchain pública capaz de ejecutar lo que se denominan “*Dapps*” que esencialmente son aplicaciones descentralizadas con características similares a los contratos inteligentes en plataformas como *Ethereum*, pero realizando validaciones a través de un algoritmo de prueba de participación (*proof of stake*). En un estudio realizado por el Parlamento Europeo, denominado *Cryptocurrencies and blockchain*, Houben *et al.*, (2018) describe a *Ethereum* como una plataforma descentralizada que puede ejecutar aplicaciones previamente programadas e inmutables, resistentes a la censura, el fraude y la interferencia por parte de terceros. Sin embargo, estos autores mencionan que la principal distinción entre *Cardano* y los demás proyectos *blockchain* es que el desarrollo está guiado por una filosofía científica y está desarrollada por un equipo de destacados ingenieros.

4.2.8 Mecanismos de Consenso. Dentro de una red *blockchain* el propósito de cada nodo participante es agregar registros. Sin embargo, los registros deben ser legítimos antes de ser registrados, puesto que, al tratarse de una red pública y distribuida en la que cualquiera puede participar, se corre el riesgo de que nodos maliciosos quieran manipular la información que se va a registrar. Por tal motivo, las plataformas de este tipo deben implementar algún mecanismo para llegar a un consenso.

Dentro de estos mecanismos de consenso, los más populares son, por un lado, la prueba de trabajo (*proof of work*), que trata de impedir el abuso del sistema a través de la implementación

de pruebas matemáticas complejas que requieren de un alto consumo energético y de cómputo. Y, por otro lado, están los algoritmos de consenso como la prueba de participación (*proof of stake*) que asegura la inmutabilidad del protocolo a través de un algoritmo de consenso.

4.2.9 Laravel. Es un *framework* web escrito en el lenguaje de programación *PHP*, que provee una estructura y un punto de partida para el desarrollo de aplicaciones web progresivas. (Laravel, 2022). El sistema provee funcionalidades listas para utilizar, tales como, inyección de dependencias, abstracciones para la capa de datos, sistema de colas e integración de pruebas unitarias. De esta manera, facilita la creación de nuevos proyectos ya que permite enfocarse simplemente en la lógica del negocio.

5. Metodología

5.1 Tipo de proyecto

Este proyecto es una investigación aplicada ya que se pretende desarrollar un sistema de certificación académica en una blockchain pública para la Institución Universitaria Pascual Bravo, la cual no cuenta con este tipo de tecnologías de certificación. La investigación aplicada busca establecer conocimientos y rutas que se puedan poner en práctica dentro del contexto elegido, de tal forma que se desarrolle un producto específico. De acuerdo con Lozada (2014), este tipo de investigación puede tener dos tipos de resultados. El primero se encuentra relacionado con el núcleo tecnológico, que corresponde al conocimiento genérico que se necesita para el desarrollo de determinado producto, mientras que el segundo se refiere a la tecnología específica en donde se presenta un producto o parte de él con un valor agregado.

5.2 Método

La estrategia metodológica utilizada en este proyecto es *SCRUM*, que de acuerdo con Sutherland (2010) “es una metodología ágil, diseñada para agregar energía, enfoque, claridad y transparencia en la planeación e implementación de proyectos”. p. (3) Es un mecanismo de trabajo que hace parte de las denominadas metodologías ágiles. Se hace uso de un modelo iterativo de trabajo que impulsa el desarrollo por etapas progresivas en las cuales se van agregando nuevas funcionalidades a medida que aumenta el progreso del proyecto. Cada iteración se compone de una fase de planificación en la cual se seleccionan los requisitos. Adicionalmente, se desarrollan las funcionalidades dentro de un marco de tiempo determinado que se denomina *Sprint* y cuyo objetivo es liberar una versión funcional del producto que se está implementando. En este proyecto investigativo, *SCRUM* se define como un marco de trabajo, es decir, que la construcción de la metodología se basa en los componentes que se adaptan a las necesidades del proyecto, brindando así flexibilidad y control en cada iteración de desarrollo y por supuesto, en cada uno de los ciclos de vida del software.

Dentro de *SCRUM* se define una pila de producto, siendo esta una parte fundamental del marco de trabajo, que determina el punto de partida del proyecto. Aquí es donde se registran y priorizan todos los requerimientos, funcionalidades, tareas o historias de usuario. Las historias de usuario, son la descripción de las funcionalidades que deben desarrollarse durante el proyecto y estas se van a escribir en términos simples y en palabras del usuario final con el objetivo de maximizar la comprensión del proyecto adoptando un lenguaje no técnico y comprensible en todos los niveles.

Para definir una historia de usuario, es necesario registrar información relevante que describa la funcionalidad que se va a desarrollar, y que permita hacer un seguimiento adecuado de los requerimientos. Por tal motivo, las historias de usuario se deben registrar con un identificador único, que consiste en un número asignado a la historia, que permita hacerle seguimiento en el tiempo y registrar incidencias en el futuro.

Adicionalmente, se debe incluir una descripción corta y clara de la funcionalidad, que necesita estar lo suficientemente descrita para diferenciarse de las demás. Por último, se agrega una descripción del procedimiento que debe realizarse para comprobar que la funcionalidad que está en desarrollo se encuentra finalizada. Como característica adicional, algunas historias de usuario pueden contener notas, anexos, aclaraciones o ejemplos que ofrezcan detalles útiles sobre la funcionalidad en desarrollo.

5.3 Instrumentos de recolección de información

Se realiza una entrevista estructurada con el objetivo de obtener información relevante sobre el proceso de generación de certificados académicos. De igual forma, en esta entrevista se indaga sobre el proceso de verificación y validación posterior a la generación de dichos certificados.

5.3.1 Fuentes primarias. Información obtenida de un grupo de personas especializadas en contenidos en específico y documentos oficiales de instituciones públicas.

5.3.2 Fuentes secundarias. Información obtenida de investigaciones de sitios web.

5.4 Proceso metodológico

El desarrollo del sistema de certificación académica en la Blockchain pública para la Institución Universitaria Pascual Bravo, consta de tres fases generales: diseño, desarrollo e implementación.

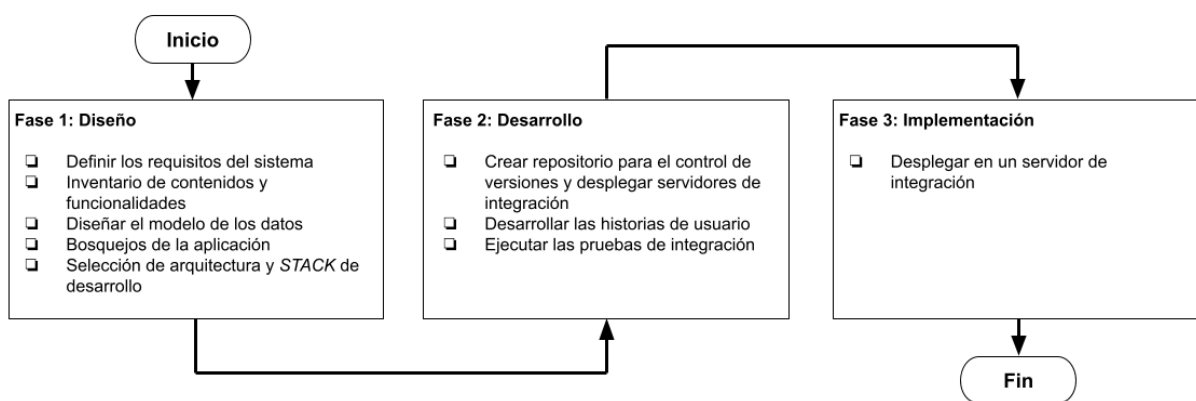


Figura 1. Fases del proyecto.

Fuente: diseño propio

5.4.1 Fase 1: Diseño

Actividad 1: definición de los requisitos del sistema: esta se realiza con el objetivo de construir un modelo de datos y al mismo tiempo crear una pila de producto de historias de usuario que deben desarrollarse durante la fase 2 del proyecto. Para empezar a entender el alcance del proyecto, se decidió realizar una serie de entrevistas cuyo objetivo es conocer el proceso de certificación académica en la institución, y que áreas e individuos están involucrados en el proceso.

Se realizan las entrevistas (ver Anexo A), para dar claridad sobre el proceso para generar un certificado académico en la institución, y para verificar su validez. Por último, con la información recolectada se establece una lista de historias de usuario que en su conjunto describen en términos simples el alcance del producto mínimo viable que se espera construir.

Actividad 2. Diseñar el Modelo de Datos: consiste en idear la arquitectura y estructura de datos necesarias para almacenar la información del certificado académico. Durante el desarrollo de esta actividad se empieza por la recopilación de información por parte de la Institución Universitaria Pascual Bravo. Por lo tanto, se requiere obtener la mayor cantidad posible de información sobre el proceso de certificación académica. De igual forma, se necesita documentar y detallar el proceso para identificar los puntos de dolor relacionados con la verificación de los certificados académicos por parte de terceros en un momento posterior a su expedición.

Utilizando la información recopilada se crea un diagrama entidad-relación que permite una visualización completa de todos los modelos que compondrán el sistema, los atributos que definen estas entidades y la forma en que se relacionan entre sí. Existe una gran variedad de software especializado en la gestión de base de datos, por lo tanto, se analizan las características especiales de cada programa y se contrasta con las necesidades del proceso. De tal manera que, se pueda seleccionar un sistema que se adapte a los requerimientos de la plataforma que se va a desarrollar.

Actividad 3. Realizar un Inventario de Contenidos y Funcionalidades: se lleva a cabo describiendo las tareas, historias de usuario y actividades necesarias en la interfaz. Utilizando el diseño del modelo entidad-relación se puede visualizar de manera general la composición del sistema. Gracias a esto, es posible comenzar a definir la pila de producto. De acuerdo con Kniberg (2007), “La pila de producto es, básicamente, una lista priorizada de requisitos, o historias, o funcionalidades, o lo que sea. Cosas que el cliente quiere, descritas utilizando la terminología del cliente. Llamamos a esto historias” p. 17.

Por lo tanto, se comienza a escribir cada una de las historias de usuario, que, en términos del usuario final, describen las funcionalidades que deben poder ejecutarse en el sistema. Las historias de usuario incluyen un identificador único, una descripción corta y los criterios de aceptación que es una descripción acerca de cómo probar la historia para garantizar que cumple con los requerimientos.

Actividad 4. Diseñar un Bosquejo de la Interfaz: dibujar un bosquejo con bajo nivel de detalle que muestre el funcionamiento y flujo general de la aplicación. Esto con el objetivo de ejemplificar y visualizar la forma en que los distintos componentes del sistema van a interactuar con los usuarios finales o con otras partes del aplicativo. Así, se hace posible un análisis objetivo sobre la experiencia del usuario y las funcionalidades del sistema en construcción.

Actividad 5. Definir *STACK*: se procede a definir el conjunto de tecnologías, herramientas, arquitectura y flujos de trabajo e integración necesarios para llevar a cabo el desarrollo del sistema.

5.3.2 Fase 2: Desarrollo

Actividad 6. Repositorios: creación del repositorio de código, control de versiones y servidor de desarrollo.

Actividad 7. Desarrollo: codificación de las historias de usuario que se definen en la fase de diseño.

Actividad 8. Pruebas: se diseñan y ejecutan pruebas de integración para asegurar el funcionamiento correcto de todos los componentes.

5.3.3 Fase 3: Implementación

Actividad 9. Despliegue: instalación del sistema en un servidor de integración con características similares a un ambiente productivo para la aplicación.

6. Resultados del proyecto

6.1 Diseño

Se realizaron entrevistas con el departamento de admisiones de la Institución Universitaria Pascual Bravo. De esta forma, se analizó el tipo de problemas al que están expuestos al realizar las actividades de verificación y certificación académica. A continuación, se presentan los hallazgos a partir de la aplicación de las entrevistas, gracias a las cuales se definen los requisitos del sistema basado en los hallazgos obtenidos.

Tabla 1.
Hallazgos

Dominio de la información	Hallazgo
Datos de los estudiantes que pueden recibir su título y la certificación institucional	<p>La información de los estudiantes se almacena en el SGI SICAU. En esta plataforma se registra todo el historial académico de los estudiantes, su documentación, entre otra información relevante.</p> <p>Por tal motivo, es necesario realizar una conexión vía <i>API</i> que permita consultar los estudiantes habilitados para recibir su certificación digital forjada en la <i>blockchain</i>.</p>
Departamentos encargados de emitir los certificados académicos	<p>En primer lugar, se encuentra el departamento de admisiones, encargado de hacer un seguimiento de los registros académicos de los estudiantes.</p> <p>Por otro lado, el departamento de sistemas se encarga de gestionar y administrar la información a través de la plataforma SICAU. Por último, una empresa externa a la institución recibe la información requerida para producir los certificados físicos, cumpliendo estándares de calidad y seguridad para el diploma.</p>

Problema identificado Actualmente no existe ningún mecanismo que permita verificar la validez de un certificado digital, de forma ágil y segura.

Fuente: diseño propio

6.1.1 Inventario de Contenidos y Funcionalidades necesarios en la Interfaz del Usuario

Todos los componentes que necesitan ser desarrollados están incluidos en el inventario de contenidos y funcionalidades. Gracias a esta herramienta se hace el seguimiento del proyecto a través de sus diferentes etapas. El sistema se compone de tres módulos que incluyen funcionalidades para los usuarios finales, y adicionalmente, incluye un módulo del sistema que debe encargarse de obtener datos desde el SGI SICAU.

Tabla 2.
Módulos del sistema

Módulo	Descripción
Preparación y configuración	Es la etapa inicial del proyecto que tiene como objetivo poner en marcha el desarrollo del sistema. Se define el modelo de los datos, se crean bosquejos de la aplicación y se selecciona el <i>STACK</i> de desarrollo. Por último, se diseña e implementa la infraestructura necesaria para la siguiente fase.
Conexión y comunicación	Se encarga de conectar con el SGI SICAU a través de peticiones <i>HTTP</i> utilizando protocolos <i>REST API</i> . El módulo obtiene información sobre los estudiantes habilitados para recibir una certificación digital, de tal manera que es posible almacenar la información de dichos estudiantes para forjar el certificado digital y su información asociada en la <i>blockchain</i> pública.
Estudiantes	Gestiona la información de los estudiantes que han sido autorizados para recibir una certificación digital a través del sistema. Los usuarios de la plataforma podrán manipular esta información antes de generar los certificados. Asimismo, los estudiantes podrán verificar su certificado desde el SGI SICAU.
Emitir certificados	Implementa una capa de servicios para emitir certificados en la <i>blockchain</i> pública. De igual manera, gestiona la billetera digital que pertenece a la institución, y que tiene propiedad sobre cada <i>NFT</i> que representa un certificado digital forjado para cada estudiante.
Consulta de terceros	Habilita una interfaz especial para que usuarios externos puedan consultar la validez de un certificado digital emitido por la institución. El usuario que realiza la consulta puede visualizar el activo digital (<i>NFT</i>) forjado con los

datos del estudiante. De igual forma, se muestra un enlace directo al historial del activo en el explorador de la *blockchain* pública.

Fuente: diseño propio

Con los módulos del sistema definidos, y con la información recopilada durante las entrevistas, se define la pila del producto (ver Anexo B) que incluye las historias de usuario descritas en lenguaje simple. Adicionalmente, se incluyen las tareas técnicas necesarias para llevar a cabo la implementación.

6.1.2 Modelo de la Estructura de Datos

Se definen cuatro modelos encargados de la administración de los datos en la aplicación. El primer modelo almacena la información del estudiante y lo vincula con un registro en el SGI SICAU. El segundo gestiona los datos del activo digital que se forja en la *blockchain* pública, almacenando toda la información relevante y vinculándola directamente con el registro del estudiante y el semestre de graduación. Adicionalmente, en la base de datos se almacena el semestre que se asigna al activo digital y el diseño gráfico o arte con el que se forja el NFT.

Por último, para permitir la consulta externa, el modelo de certificaciones gestiona la información de los terceros interesados en consultar datos de un estudiante, de tal manera que, es posible analizar las métricas de consulta a través del tiempo. A continuación, se ilustra el modelo entidad relación que implementa la aplicación.

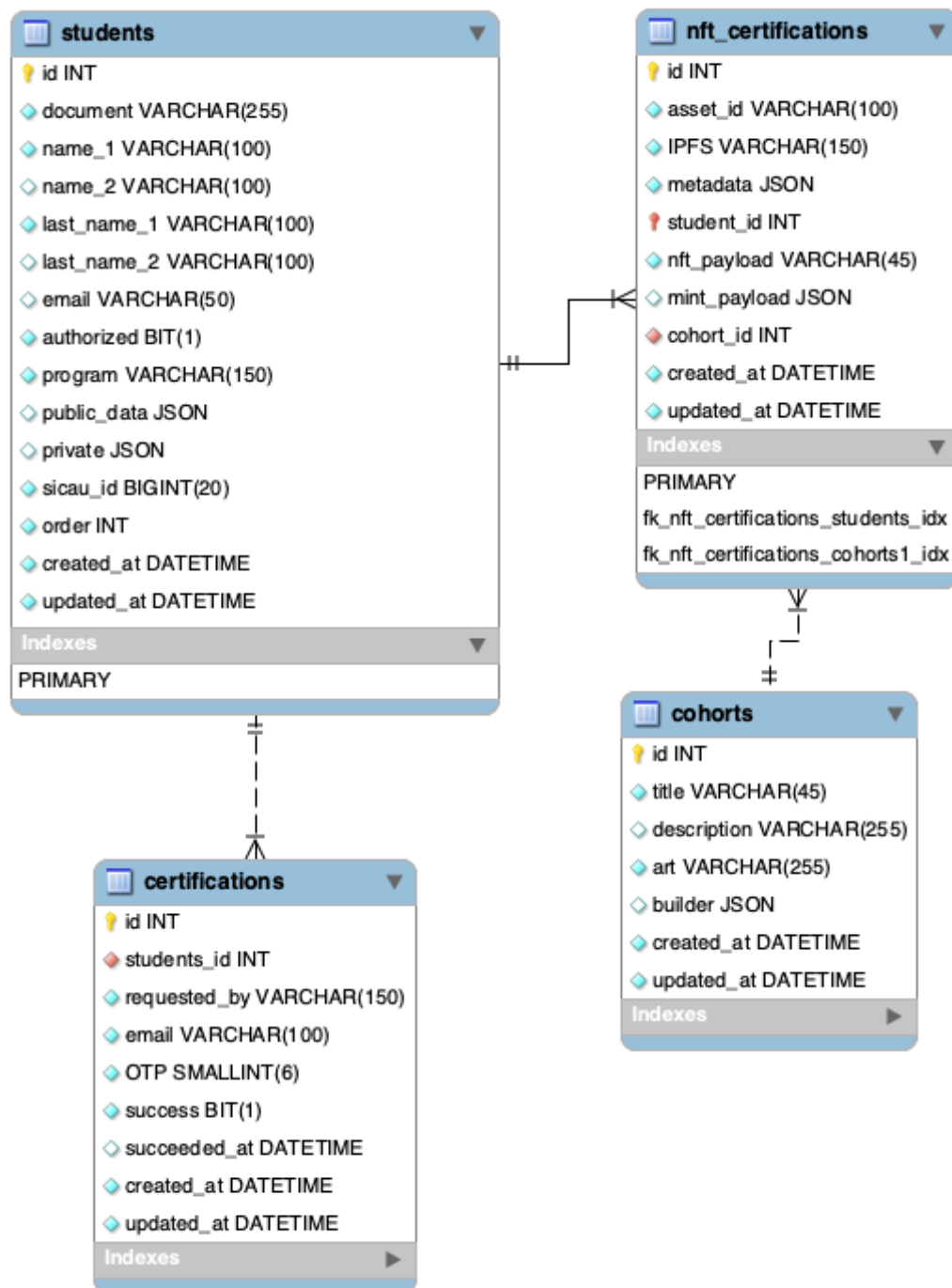


Figura 2. Modelo entidad relación.

Fuente: diseño propio, utilizando la herramienta *MySQL Workbench*

6.1.3 Bosquejo de Interfaz de la Aplicación. Utilizando un enfoque sistémico, se definen algunos bosquejos que representan los elementos que debe contener la aplicación. En este

proceso se tienen en cuenta los componentes y funcionalidades principales. El objetivo es proveer una representación visual sencilla de la interfaz.

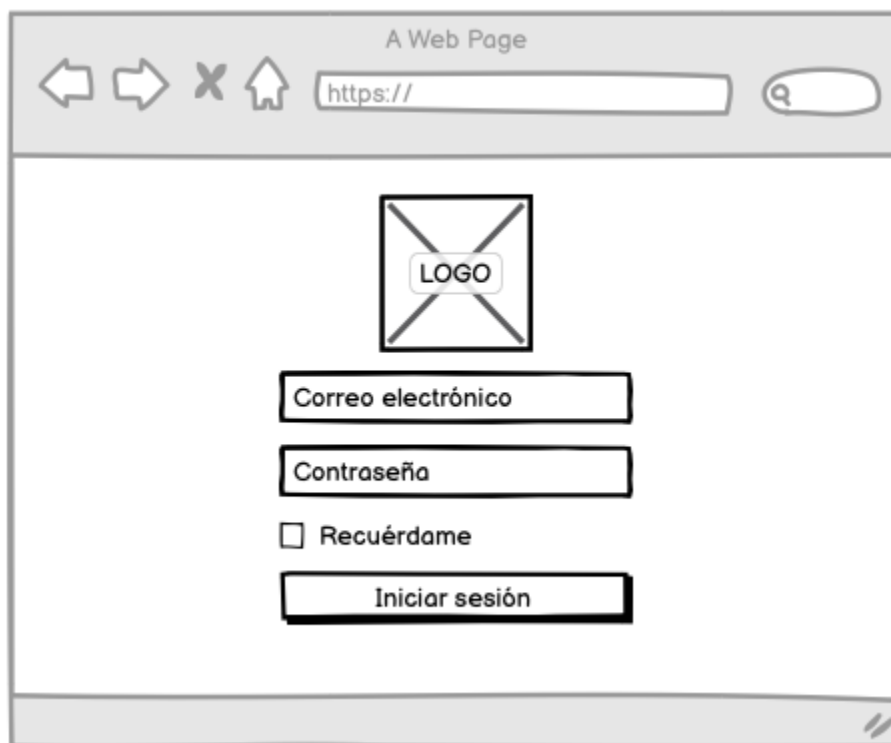


Figura 3. Pantalla de inicio de sesión.

Fuente: diseño propio, utilizando la herramienta *Balsamiq Wireframes*

La aplicación debe gestionar información acerca de los estudiantes autorizados para recibir una certificación, esta autorización proviene del SGI SICAU. De igual forma, debe mostrar un listado de los certificados (NFT) forjados en la *blockchain* con su respectiva relación con el estudiante y la promoción. Por último, la aplicación gestiona las solicitudes externas de validación, con el objetivo de obtener estadísticas sobre consultas y construir una base de datos de entidades o personas interesadas en contratar estudiantes de la institución.

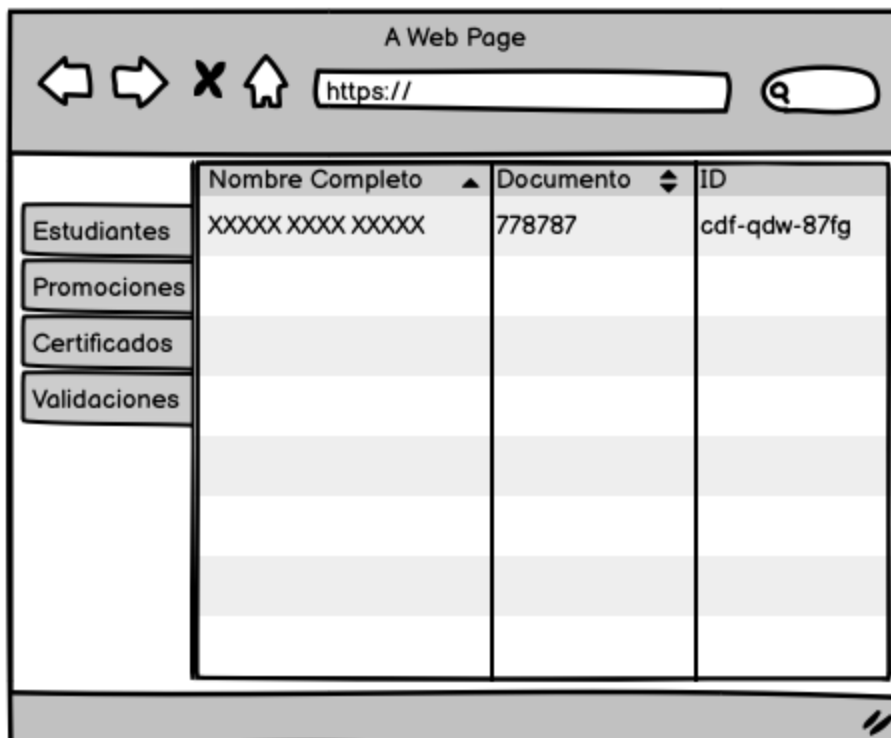


Figura 4. Maestro de estudiantes, promociones, certificaciones y solicitudes de validación.
Fuente: diseño propio, utilizando la herramienta *Balsamiq Wireframes*

Como se mencionó anteriormente, la aplicación gestiona las promociones que se forjan digitalmente, por lo tanto, cada promoción tiene un registro que almacena el año, el semestre, la fecha de graduación, entre otros datos relevantes. De igual manera, se define un arte básico sobre el cual el software se encargará de generar las certificaciones individuales, y de esta forma encolar la generación del *NFT* vinculado al registro académico.



Figura 5. Interfaz que representa la forja del certificado en la blockchain pública.

Fuente: diseño propio, utilizando la herramienta *Balsamiq Wireframes*

En concordancia con los hallazgos obtenidos durante las entrevistas, se evidenció que el proceso de validación de los certificados emitidos por la institución, es lento y conlleva un extenso trabajo de archivo que generalmente lleva bastante tiempo. En consecuencia, el aplicativo incorpora una vista pública en la que terceros interesados pueden consultar rápidamente la validez de un certificado.

El proceso de validación se lleva a cabo en tres pasos. El primero es ingresar en la dirección donde se expone el recurso, después, ingresar el documento que se desea consultar, un nombre del solicitante de la información y un correo electrónico. Por último, ejecutar la opción para verificar, de tal manera que, el solicitante recibirá un correo electrónico con un código único, con el cual podrá acceder en la aplicación a la información del certificado de forma inmediata y con total garantía de su validez.

6.1.4 STACK. La elección del *STACK* adecuado es fundamental para el desarrollo exitoso del producto. De acuerdo con Patel *et al.*, (2018), es una combinación de programas que trabajan conjuntamente para producir un resultado. Un *STACK* tecnológico es una combinación de lenguajes de programación, *frameworks* y herramientas que se utilizan para el desarrollo.

Para implementar la aplicación se utiliza un conjunto de herramientas y software de código abierto que implementa las funcionalidades más complejas y garantiza que el desarrollo del producto se enfoque en las necesidades definidas en los requerimientos. El proyecto se desarrolla utilizando un conjunto de herramientas que se denomina *TALL STACK*, que se utiliza ampliamente en la industria del desarrollo web para construir aplicaciones reactivas con el framework de *PHP*, *Laravel*. El *STACK* seleccionado para llevar a cabo el proyecto es el siguiente:

- *Tailwind CSS* es un *framework CSS* enfocado en brindar un marco de utilidades que permiten implementar interfaces de usuario usables, adaptables y fáciles de implementar.
- *Alpine.js* es un micro *framework* que permite manipular el comportamiento de las interfaces directamente. Es extremadamente ligero y se integra fácilmente con el *Backend*.
- *Laravel* es un *framework* monolítico escrito en lenguaje *PHP* para construir aplicaciones web robustas.
- *Livewire* es un paquete de componentes y complementos que incorporan una integración entre el *Backend* de la aplicación y la interfaz del usuario, permitiendo el desarrollo de aplicaciones progresivas y reactivas.

Adicionalmente, es necesaria la selección de una plataforma *blockchain* pública que implemente una solución robusta y cumpla con altos estándares en su desarrollo. Por tal motivo, la plataforma elegida es *Cardano*, una *blockchain* pública con algoritmos de consenso basados en la prueba de participación. Adicionalmente, su desarrollo está basado en investigaciones en las que se hace revisión por pares y utiliza métodos que se basan en evidencia para desarrollar la tecnología. La plataforma provee una capa de seguridad y sostenibilidad para construir aplicaciones descentralizadas.

Finalmente, para que el sistema funcione correctamente y sea accedido por los usuarios se requiere un subdominio que apunte a un servidor especializado que tendrá instalado el aplicativo en funcionamiento. A continuación, se muestra una tabla con los requisitos mínimos para que el software se ejecute correctamente.

Tabla 3.
Requerimientos.

Requisito	Descripción
Subdominio	Establecer una dirección web que redirija el tráfico hacia el punto de entrada de la aplicación.
Servidor	<ul style="list-style-type: none"> ● Sistema operativo <i>Ubuntu 22.04</i>, 1GB RAM, 30GB SSD ● Servidor web <i>NGINX</i> ● Intérprete <i>PHP</i> ≥ 8.0 ● Certificado SSL ● Motor de base de datos <i>MySQL</i> ≥ 8.0

Fuente: diseño propio.

6.2 Desarrollo

Para iniciar la codificación de los componentes del sistema se realizan actividades que apoyan las etapas de desarrollo. Por tal motivo, se descargan y configuran los paquetes necesarios para esta fase, tales como, el *framework Laravel*, los paquetes de terceros y se inicializa un repositorio para mantener un control de cambios durante todo el proceso. Las instrucciones detalladas de la configuración inicial pueden consultarse en el Anexo C.

6.2.1 Control de Versiones y Servidores de Desarrollo. El control de versiones mantiene un historial de los cambios realizados durante el ciclo de vida del desarrollo, es importante para mantener un registro detallado y tener la capacidad de retroceder el estado del proyecto para corregir defectos o para realizar pruebas de cualquier tipo en el sistema. Para aprovechar las características del control de versiones se utiliza *GIT*, un software con la capacidad de gestionar los cambios en el código fuente. Adicionalmente, se ejecuta un servicio integrado en el *framework Laravel* que implementa un servidor web de desarrollo que permite visualizar y probar las funcionalidades en un entorno local.

6.2.2 Desarrollo de las Historias de Usuario. De acuerdo con la pila de producto y la priorización que se hace de las historias de usuario, el primer componente del aplicativo es un módulo que se encarga de realizar una conexión con el SGI SICAU. La funcionalidad principal implementa una petición *HTTP* con el verbo *GET* utilizando el protocolo *REST*. De tal forma que, puede solicitar un listado de estudiantes que cuentan con el aval para recibir una certificación digital. La implementación de esta arquitectura hace que el sistema requiera una configuración mínima, que esté totalmente aislado para no comprometer la seguridad de los sistemas institucionales y que pueda conectarse fácilmente a cualquier sistema de información que exponga un recurso para consultar los estudiantes autorizados utilizando un *RESTful API*.

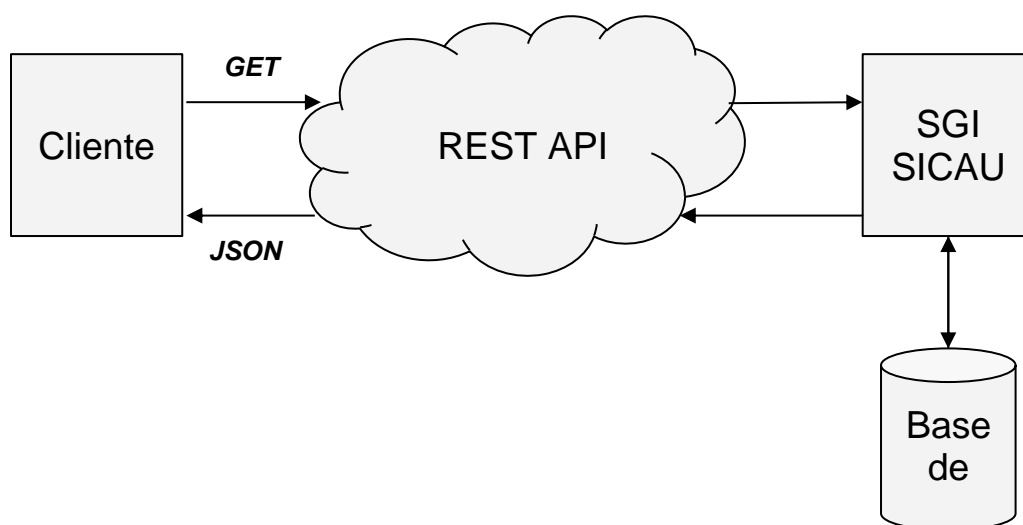


Figura 6. Arquitectura Plug and Play (PnP).

Fuente: diseño propio, utilizando la herramienta de dibujo de *Google Suite*

En segundo lugar, el módulo de estudiantes consiste en un registro de cada uno de los individuos que ha recibido el sistema como parte de la petición al SGI SICAU. De manera que un usuario de la aplicación puede gestionar la información básica necesaria para forjar el certificado en la *blockchain* pública. En particular, podrá modificar si un estudiante está autorizado o no para recibir el certificado y el orden en el que se este se va a generar. Todo esto con el objetivo de realizar una verificación doble antes de forjar el diploma, dado que una vez el registro se incorpora en la cadena de bloques, este no puede ser modificado.

The screenshot shows a web application interface for managing a student. At the top left, there is a toggle switch labeled 'Autorizado' which is currently turned on. Below this, the form is organized into two columns. The left column contains the following fields: 'Primer nombre' (Conrad), 'Primer apellido' (Schowalter), 'Correo electrónico' (Jaylin25@yahoo.com), 'Programa / Carrera' (Oriental), and 'Creado el' (24/10/2022 12:10:21). The right column contains: 'Documento' (4599416592326), 'Segundo nombre' (Parker), 'Segundo apellido' (Stoltenberg), 'ID SICAU' (8), 'Orden para forjar' (1), and 'Última actualización' (24/10/2022 12:10:21). At the bottom of the form, there are two buttons: 'Guardar' (orange) and 'Cancelar' (white with grey border).

<input checked="" type="checkbox"/> Autorizado	Documento
	4599416592326
Primer nombre	Segundo nombre
Conrad	Parker
Primer apellido	Segundo apellido
Schowalter	Stoltenberg
Correo electrónico	ID SICAU
Jaylin25@yahoo.com	8
Programa / Carrera	Orden para forjar
Oriental	1
Creado el	Última actualización
24/10/2022 12:10:21	24/10/2022 12:10:21

Figura 7. Interfaz de la aplicación donde se gestiona un estudiante

Fuente: captura de pantalla de la interfaz gráfica de la aplicación

Adicionalmente, los usuarios de la aplicación podrán utilizar la interfaz del sistema para realizar la petición del listado de estudiantes autorizados, ejecutando la petición *GET* mencionada anteriormente. Por su parte, los estudiantes que se encuentren autorizados tendrán habilitado un botón para forjar el certificado en la *blockchain* pública.

Estudiantes Obtener estudiantes

Autorizado	Orden	Documento	Primer nombre	Segundo nombre	Primer apellido	Segundo apellido	
<input checked="" type="checkbox"/>	1	5469-2995-6740-4113	Jaylin	Sasha	Cormier	Predovic	Editar Forjar certificado
<input checked="" type="checkbox"/>	2	5511-9088-3233-3273	Kailee	Charlie	Flatley	Frami	Editar Forjar certificado
<input checked="" type="checkbox"/>	3	3529-7051-3426-9505	Chester	Kai	Cartwright	Mayer	Editar Forjar certificado
<input checked="" type="checkbox"/>	4	6391-3563-2252-7591	Alison	Shawn	Powlowski	Ryan	Editar Forjar certificado
<input checked="" type="checkbox"/>	5	3529-3117-6291-5285	Sherwood	Brooklyn	McLaughlin	Price	Editar Forjar certificado
<input checked="" type="checkbox"/>	6	6393-1295-5997-3263	Kasey	Micah	Pfeffer	Swift	Editar Forjar certificado
<input checked="" type="checkbox"/>	7	3415-413282-12825	Deion	Sage	White	Rogahn	Editar Forjar certificado
<input type="checkbox"/>	8	4599416592326	Conrad	Parker	Schwalter	Stoltenberg	Editar
<input type="checkbox"/>	9	676305494834190260	Fermin	Arden	Graham	Flatley	Editar
<input type="checkbox"/>	10	6759-4371-9432-7554-961	Emmet	Leslie	Ebert	Fritsch	Editar

Mostrando 1 a 10 de 30 resultados 10 por página

Figura 8. Principales características para forjar el certificado.

Fuente: captura de pantalla de la interfaz gráfica de la aplicación

- Botón para obtener listado de estudiantes desde el SGI SICAU
- Columna para visualizar si los estudiantes están autorizados para recibir la certificación digital
- Columna para ordenar el listado de estudiantes
- Datos básicos del estudiante
- Acciones que se pueden realizar con cada estudiante

En relación con la emisión de certificados se dispone de una sección específica dentro de la aplicación en la cual los usuarios pueden diseñar el arte gráfico que el sistema generará una vez el actor utilice la opción para forjar el certificado. Todos los detalles del proceso para utilizar la aplicación se detallan en el Anexo D. Manual de usuario final.

Por último, el componente para consultas externas se concibe como una herramienta expuesta públicamente, brindando así la posibilidad de que cualquier usuario pueda solicitar la validación de un certificado emitido por la institución de forma rápida, segura y confiable. De tal forma que se implementa una interfaz pública que solicita información acerca del estudiante que se quiere verificar y además registra datos sobre el solicitante para mantener un control de

entidades o personas que validan certificaciones usando la aplicación. Adicionalmente, el sistema hace una verificación de acceso a través de una autenticación con contraseña de un solo uso (*OTP*) para prevenir abusos por parte de robots o usuarios maliciosos.

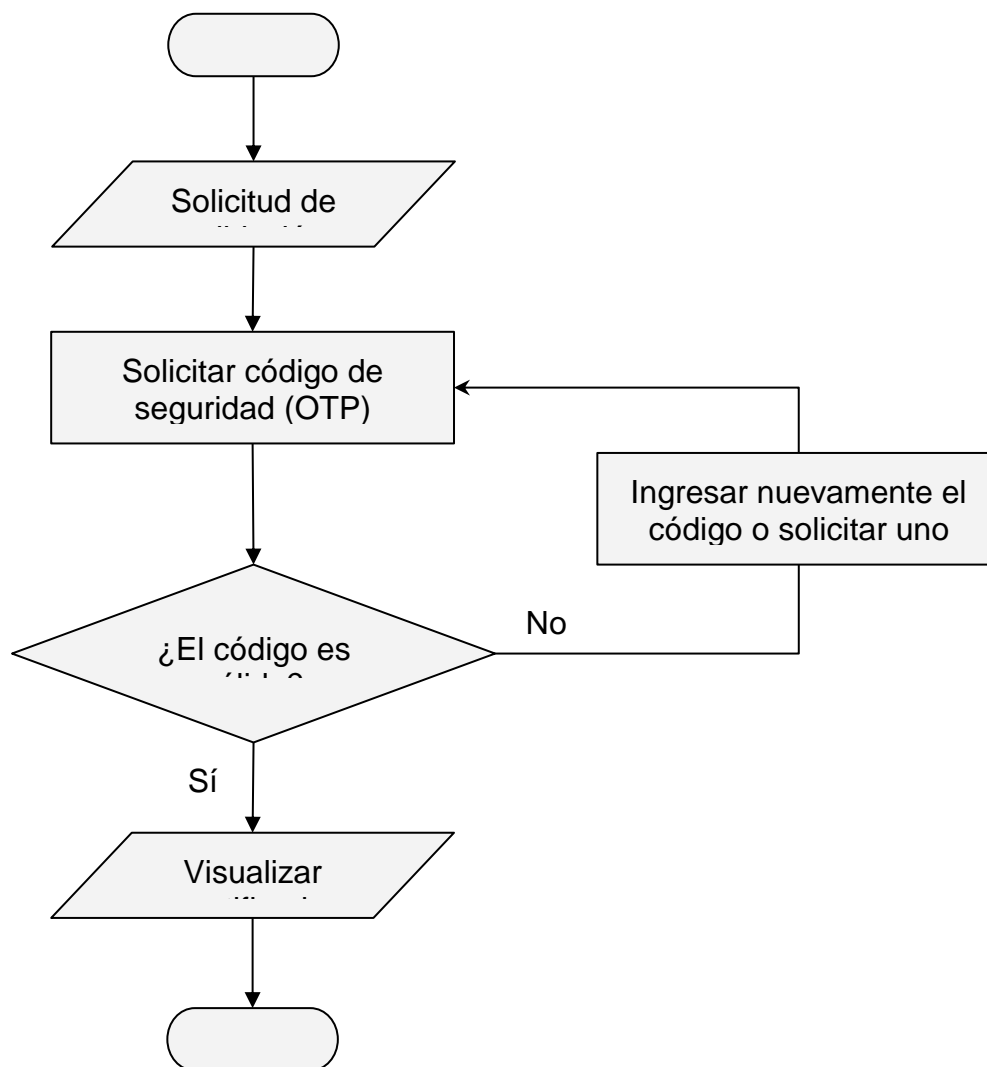


Figura 9. Diagrama de flujo para validar un certificado en la aplicación.

Fuente: diseño propio, utilizando la herramienta de dibujo de *Google Suite*

6.2.3 Pruebas de Integración. Esta fase del proceso orquesta el funcionamiento del sistema y permite realizar pruebas en las que todos los componentes interactúan entre sí, comparten información y registran datos en la cadena de bloques con el objetivo de dar solución al problema planteado. El escenario ideal para realizar las pruebas de integración, consiste en desplegar un servidor en el cual se pueda configurar e instalar la aplicación en un ambiente de

integración. Este debe disponer de las mismas características de un entorno de producción con el objetivo de simular exactamente el comportamiento que tendría el sistema si se despliega para el uso por parte de los usuarios finales.

Durante la ejecución de las pruebas de integración se analiza el cumplimiento de los criterios de aceptación descritos en las historias de usuario de la pila de producto (ver Anexo B). De esta manera, se asegura el cumplimiento de las premisas que tiene la aplicación antes de ser implementada en producción.

6.3 Implementación

Finalmente, al surtir la etapa de desarrollo y realizar las comprobaciones, correcciones y ajustes que surgen de manera natural en un proyecto de estas características, se puede afirmar que el sistema de certificación académica en una *blockchain* pública se encuentra listo para su implementación. Siguiendo las instrucciones contenidas en el Anexo E, en el cual se muestran las acciones necesarias para realizar el despliegue en producción. De igual manera, como se ha mencionado anteriormente, esta plataforma está diseñada para ser integrada fácilmente con cualquier sistema de información universitario, debido a que el único requisito técnico es contar con un *API* que exponga el servicio para consultar estudiantes autorizados para recibir una certificación digital.

6.4 Discusión

Al reflexionar sobre el problema y los objetivos que se plantean en este trabajo de investigación, se analizan las distintas posibilidades que existen para implementar un sistema que aproveche las ventajas de la tecnología blockchain, teniendo como principio fundamental el desarrollo de una plataforma de certificación académica confiable y segura. Sin embargo, actualmente puede resultar abrumador plantearse desarrollar un proyecto de este tipo, debido a la complejidad de los conceptos y al estado del arte primigenio de las herramientas para trabajar con cadenas de bloques públicas. Por lo tanto, ha sido una premisa en el desarrollo de este trabajo el intentar abstraer las complejidades inherentes al proyecto, de tal forma que, a partir

de la metodología y la ruta anteriormente planteada se puedan implementar aplicaciones que estén a la vanguardia. Así, los sistemas de información deben plantearse desde una perspectiva pragmática, enfocando todos los esfuerzos en la resolución del problema y no exclusivamente en la discusión acerca de los aspectos técnicos del mismo.

Al reflexionar sobre el problema y los objetivos que se plantean en este trabajo de investigación, se analizan las distintas posibilidades que existen para implementar un sistema que aproveche las ventajas de la tecnología blockchain, teniendo como principio fundamental el desarrollo de una plataforma de certificación académica confiable y segura. Sin embargo, actualmente puede resultar abrumador plantearse desarrollar un proyecto de este tipo, debido a la complejidad de los conceptos y al estado del arte primigenio de las herramientas para trabajar con cadenas de bloques públicas. Por lo tanto, ha sido una premisa en el desarrollo de este trabajo el intentar abstraer las complejidades inherentes al proyecto, de tal forma que, a partir de la metodología y la ruta anteriormente planteada se puedan implementar aplicaciones que estén a la vanguardia. Así, los sistemas de información deben plantearse desde una perspectiva pragmática, enfocando todos los esfuerzos en la resolución del problema y no exclusivamente en la discusión acerca de los aspectos técnicos del mismo.

Ahora bien, para adoptar este enfoque se profundizó en el conocimiento sobre las herramientas disponibles que permitan aprovechar las ventajas de la tecnología blockchain. En primer lugar, la discusión se centró en seleccionar la red adecuada para implementar la solución propuesta. Dentro de las posibilidades existentes se encuentran opciones como Ethereum, Bitcoin Scripting Language, Binance Smart Chain, Polygon, Polkadot, Cardano, entre otras. Las opciones disponibles son muchas, sin embargo, de acuerdo con Kiayias et al., (2019) en *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*, se presenta una alternativa distinta a la mayoría de protocolos, en la cual no se utiliza la prueba de trabajo como mecanismo de consenso para registrar la información. De igual forma, demuestra la rigurosidad científica con la que fue construido el protocolo Ouroboros para la red de Cardano. Adicionalmente, en las fases preliminares de investigación se recopilieron herramientas e interfaces API que aprovechan todos los beneficios de esta blockchain de tercera generación.

En definitiva, esta opción abarca un protocolo seguro, sustentable, escalable y con las herramientas adecuadas para una implementación exitosa.

Por último y para afianzar aún más el sentido práctico de este trabajo, se utilizan múltiples frameworks a lo largo de toda la arquitectura del sistema. Desde la interfaz de usuario que ha sido implementada utilizando Tailwind CSS, hasta el aprovechamiento de Laravel, un framework progresivo que estimula el desarrollo de proyectos que se centren en la resolución de problemas, y no en los aspectos fundamentales que son comunes para cualquier tipo de sistema de información. En otras palabras, el aprovechamiento de una gran variedad de herramientas, componentes y complementos disponibles públicamente brindan una gran ventaja para construir aplicaciones modernas de última generación.

7. Conclusiones

La etapa de diseño del sistema que involucró actividades de planeación y recopilación de información útil, ha jugado un papel muy importante dentro de este proyecto. Gracias a esta etapa, se pudo conocer en detalle el problema que se buscaba resolver, el uso de fuentes primarias de información a través de las entrevistas, reflejaron la problemática inicialmente planteada. De igual forma, se logró definir una serie de modelos para los datos que garantizaron que la aplicación contará con la información necesaria para lograr generar certificados digitales sin la necesidad de tener una estructura compleja y manteniendo un alcance definido que permite replicar un sistema de las mismas características.

Tener claridad acerca del modelo de los datos, permite al mismo tiempo abstraer más fácilmente las necesidades de los usuarios a través del inventario de módulos. En este punto, y pensando en las problemáticas a las que se enfrentan los usuarios finales, se diseñan los módulos que brindan soporte al proceso. De tal manera que, al finalizar la primera etapa se tiene una idea mucho más clara acerca del proyecto y la forma en la que se puede abordar para culminar con éxito.

En segunda instancia, al contar con la claridad descrita anteriormente, la etapa de desarrollo se hace mucho más fluida, puesto que, está completamente definido cada uno de los artefactos, funcionalidades y componentes entregables que tiene el proyecto. Con esto, el desarrollo de las historias de usuario logra incluir dentro de la aplicación los requisitos iniciales, dejando todo el sistema listo para ejecutar las pruebas de integración e implementación.

Finalmente, la implementación de los componentes y la ejecución de pruebas de integración surgen como una forma de verificar el correcto funcionamiento de la aplicación, aquí ha sido primordial comprobar que el sistema no solo cumple con las características técnicas con las que fue concebido, sino que también logra dar solución al problema que buscaba resolver. Esta comprobación se alcanza dentro de estándares de calidad y usabilidad óptimos para un producto que puede ser desplegado en un ambiente de producción.

8. Recomendaciones

En primer lugar, es ideal reconocer los elementos fundamentales del sistema que se desea construir, con el objetivo principal de definir su alcance y los recursos necesarios para completarlo con éxito. En este aspecto se recomienda consultar con fuentes primarias de información, personas involucradas de manera directa e indirecta en el problema que se busca resolver. De tal manera que, se pueda diseñar a través de un pensamiento sistémico los componentes e interacciones necesarias para cumplir con las expectativas de los potenciales usuarios.

De igual forma, para realizar proyectos que incorporen tecnología blockchain es conveniente realizar un diseño de arquitecturas híbridas como la que se implementa en este proyecto. En otras palabras, los modelos tradicionales pueden compartir y registrar información pública para apoyar la implementación de sistemas de uso interno y aprovechar las ventajas tecnológicas de blockchain. Además, a pesar de que los sistemas blockchain se caracterizan por su arquitectura descentralizada, es posible aprovechar y complementar sistemas con datos privados a través de la arquitectura híbrida como la que se ejemplifica en este proyecto.

Por último, con el análisis de los requisitos se puede investigar acerca de las necesidades técnicas de la aplicación y con esta información es posible realizar una investigación para aprovechar cualquier tipo de herramienta, código fuente, paquetes de desarrollo, frameworks, API's, entre otros componentes o plugins que son extremadamente útiles a la hora de realizar la implementación de las funcionalidades. Este tipo de abstracciones a nivel tecnológico simplifican el proyecto y ayudan a cumplir con los objetivos sin la necesidad de construir los componentes que generalmente son comunes para aplicaciones de software, tales como, sistemas de autenticación, maestros de datos y conexiones o comunicación con sistemas externos.

9. Referencias bibliográficas

- Aparco, R., Canchaya, E., Murillo, A., Robles, A. (2021). *Modelo de implementación del Proceso de emisión de Grados y Títulos Digitales mediante el uso de la Tecnología Blockchain en Universidades de Lima Metropolitana*. [Tesis de Maestría Universidad ESAN]. Repositorio Institucional de la Universidad ESAN. Disponible en: <https://hdl.handle.net/20.500.12640/2161>
- Beltran, N., Ramírez, L. (2020). Modelo de tecnología Blockchain en la autenticación de certificados inteligentes para entidades educativas. *Revista de Investigación en Educación Militar* (1) 1, 93-104. Disponible en: <https://doi.org/10.47961/27450171.9>
- Cuervo, B., Rodríguez, M., Sánchez, A. (2019). BC-CAD Sistema para la generación y validación de certificados académicos digitales implementando Blockchain. *Encuentros con Semilleros, Aportes y Reflexiones*. 1 (1), 193-204. Disponible en: <https://doi.org/10.15765/es.v1i1.1665>
- Domínguez, C. (2021). La Revolución Blockchain y los Smart Contracts en el Marco Europeo. *Actualidad Jurídica Iberoamericana*. (16),1088-1109. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=8393390>
- González Conejero, E. (2021). Blockchain: Una nueva tecnología. *Puente de Hierro*. 2 (2), 1-13. Disponible en: <https://www.puentedehierro.org/ojs/index.php/pdh/article/view/28>
- Hernández-Sampieri, R., Mendoza Torres, C. (2018). *Metodología de la Investigación. Las rutas cuantitativa, cualitativa y mixta*. Ciudad de México: McGraw-Hill Interamericana Editores.
- Houben, R., Snyers, A. (2018). *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament. Disponible en: <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>
- Kiayias, A., Rusell, A., David, B., Oliynykov, R. (2019). Ouroboros: A probably Secure Proof-of-Stake Blockchain Protocol. *CRYPTO: Advances in Cryptology*. 357- 388. Disponible en: <https://eprint.iacr.org/2016/889>

- Kniberg, H. (2007). *SCRUM y XP desde las trincheras Cómo Hacemos SCRUM*. C4Media Inc. Estados Unidos de América. Disponible en <http://www.proyectalis.com/wp-content/uploads/2008/02/scrum-y-xp-desde-las-trincheras.pdf>
- Laravel (30 de octubre de 2022). *Installation*. Disponible en: <https://laravel.com/docs/9.x/installation#why-laravel>
- Lozada, J. (2014). Definición, Propiedad Intelectual e Industria. *CienciAmérica Revista de Divulgación Científica de la Universidad Tecnológica Indoamericana*. 3 (1) 47-50. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=6163749>
- Ministerio de Tecnologías de la Información y las Comunicaciones (2022) *Guía de Referencia para la adopción e implementación de proyectos con tecnología Blockchain para el Estado colombiano*. Disponible en: https://mintic.gov.co/portal/715/articles-237592_recurso_1.pdf
- Moreno Marín, A. (2022). *Mejoras en el proceso de emisión de certificados académicos en la Universidad de los Andes a partir de la integración de tecnologías previamente adquiridas y Blockchain*. [Tesis de Maestría Universidad de los Andes]. Repositorio Institucional Séneca de la Universidad de los Andes. Disponible en: <http://hdl.handle.net/1992/58067>
- Moscoso, S., Suárez, D., Martín D. (2019). Certificación digital de documentos académicos basada en la tecnología de Blockchain. *TIA Tecnología, Investigación y Academia*. 72(2), 20-27. Disponible en: <https://revistas.udistrital.edu.co/index.php/tia/article/view/12757>
- Patel, T., Krishnani, K., Naidu, S. (2018). Comparative Analysis of Web Development Stacks. *International Journal of Creative Research Thoughts (IJCRT)*. 6 (1), 751-756. Disponible en: <https://ijcrt.org/papers/IJCRT1803202.pdf>
- Plaza, Estévez, S., Ramírez, N., Acosta, C. (2016). *API de servicios web orientados a la accesibilidad*. [Tesis de pregrado Universidad Complutense de Madrid] Repositorio Institucional de la Universidad Complutense de Madrid. Disponible en: <https://eprints.ucm.es/id/eprint/38686/>
- Reyes Sánchez (2022). Blockchain: Funcionamiento y pertinencia en sectores públicos y privados. *Interconectando Saberes*. 7 (14), 169- 178. Disponible en: <https://doi.org/10.25009/is.v0i14.2734>

Ruiz, J. (2020). *Diplomas académicos sobre una plataforma Blockchain*. [Tesis de pregrado Universidad de los Andes] Repositorio Institucional Séneca de la Universidad de los Andes. Disponible en: <http://hdl.handle.net/1992/48707>

Sutherland, J. (2010). *Scrum Handbook*. Scrum Training Institute. Disponible en: https://www.researchgate.net/publication/301685699_Jeff_Sutherland's_Scrum_Handbook

10. Anexos

Anexo A. Entrevistas.

Entrevista estructurada dirigida al personal encargado del proceso para generación de certificados académicos en la Institución Universitaria Pascual Bravo, para el trabajo de grado titulado **“Desarrollo de una Certificación Académica en una Blockchain Pública”**

Objetivos:

- Obtener información sobre el proceso para generar un certificado académico y/o diploma para un estudiante.
 - Obtener información sobre el proceso para verificar la validez de un certificado académico y/o diploma de un estudiante.
-

Preguntas:

1. ¿Cuál es su nombre completo?
 1. ¿Qué cargo desempeña?
 2. ¿Qué requisitos debe cumplir un estudiante para recibir su diploma de graduación?
 3. ¿Quién es la última persona que autoriza si un estudiante va a recibir un diploma?
 4. ¿Qué información del estudiante se debe almacenar cuando recibe el diploma?
 5. ¿Cuál de esta información es de carácter privado y no puede divulgarse públicamente?
 6. ¿Cuál de esta información es pública y puede visualizarse sin afectar la privacidad del estudiante?
 7. ¿Dónde se almacena la información del estudiante que recibe un diploma?
 8. ¿Durante cuánto tiempo se almacena la información del estudiante que recibe un diploma?
 9. ¿Quiénes pueden solicitar información sobre la validez de un diploma emitido por la institución?
 10. ¿Cómo es el proceso para solicitar la validez de un diploma?
 11. ¿Qué problemas tienen actualmente con el proceso para verificar la validez de un diploma?
-

Anexo B. Pila de Producto.

En concordancia con la metodología *SCRUM* utilizada en el desarrollo de este proyecto, se define en el presente documento la pila de producto, entendida como un listado de actividades, historias de usuario y tareas priorizadas que se realizan con el objetivo de llevar un registro del proceso de desarrollo.

Preparación y configuración del proyecto

La etapa inicial del proyecto tiene como objetivo poner en marcha las actividades de desarrollo del sistema. Durante esta etapa, se define el modelo de datos, se crean los bosquejos de la aplicación, se define el *STACK* de desarrollo y se implementa la infraestructura necesaria para iniciar el desarrollo del producto.

Actividades

- Diseñar el modelo entidad relación para la base de datos que gestiona la información del sistema
- Dibujar bosquejos de la interfaz de usuario que implementa la aplicación
- Definir el *STACK* de desarrollo que se utiliza en el proyecto
- Instalar los componentes, herramientas y servicios necesarios para el desarrollo
- Implementar el sistema de control de versiones para gestionar el código

Módulo de conexión

Es el encargado de conectar con el SGI SICAU a través de peticiones *HTTP* utilizando protocolos *REST API*. El módulo obtiene información sobre los estudiantes habilitados para

recibir una certificación digital. De tal manera que es posible almacenar la información de dichos estudiantes para forjar el certificado digital y su información asociada en la *blockchain* pública.

ID	Descripción	Criterios de aceptación
1	Como usuario quiero poder solicitar al SGI SICAU un listado de estudiantes autorizados para poder forjar certificados digitales	El usuario puede solicitar un listado de estudiantes habilitados para recibir una certificación digital

Módulo de estudiantes

Gestiona la información de los estudiantes que han sido autorizados para recibir una certificación digital a través del sistema. Los administradores de la plataforma podrán manipular esta información antes de generar los certificados.

ID	Descripción	Criterios de aceptación
2	Como usuario quiero poder modificar la información de los estudiantes autorizados para recibir un certificado digital	El usuario puede modificar la información asociada a un estudiante

Módulo para emitir certificados

Implementa una capa de servicios para emitir certificados en la *blockchain* pública. De igual manera, gestiona la billetera digital que pertenece a la institución, y que tiene propiedad sobre los *NFT* que representan un certificado digital forjado para cada estudiante.

ID	Descripción	Criterios de aceptación
3	Como usuario quiero poder gestionar promociones para asignar las certificaciones a un semestre determinado	El usuario puede crear, actualizar y borrar promociones

4	Como usuario quiero poder diseñar el certificado para poder forjarlo y asignarlo a un estudiante	El usuario puede diseñar el certificado que va a forjar para los estudiantes
---	---	--

Módulo de consulta

Habilita una interfaz especial para que usuarios externos puedan consultar la validez de un certificado digital emitido por la institución. El usuario que realiza la consulta puede visualizar el activo digital (NFT) forjado con los datos del estudiante. De igual forma, se muestra un enlace directo al historial del activo en el explorador de la *blockchain* pública.

ID	Descripción	Criterios de aceptación
5	Como usuario externo quiero poder solicitar la validación de un certificado digital emitido por la institución	El usuario externo puede solicitar la validación de un certificado emitido por la institución

Anexo C. Configuración Inicial del Proyecto.

Antes de comenzar la configuración del entorno, hay que verificar que se cumplen los requisitos y dependencias mínimas para el funcionamiento del proyecto.

Requisitos
<p>Computador con las siguientes características:</p> <ul style="list-style-type: none"> ● 2GB Memoria <i>RAM</i> ● 15 GB <i>HDD o SSD</i> ● <i>PHP</i> >= 8.0 ● <i>GIT</i> >= 2.38.0 ● <i>Composer</i> >= 2.4.0 ● <i>MySQL</i> >= 8.0

A continuación, se describen una serie de pasos que se deben seguir para configurar todas las dependencias necesarias para el desarrollo del proyecto.

1. Para instalar el *framework Laravel* se debe abrir una terminal de comandos y ubicarse en el directorio de instalación. Posteriormente, se ejecuta el comando para descargar el paquete.

```
$ composer create-project laravel/laravel app-sicau
```

2. Para instalar las dependencias se deben ejecutar los siguientes comandos en la terminal.

```
$ cd app-sicau
```

```
$ composer require filament/filament:"^2.0"
```

```
$ composer require bezhansalleh/filament-shield
```

```
$ composer require guzzlehttp/guzzle
```

```
$ composer require barryvdh/laravel-dompdf
```

```
$ composer require spatie/pdf-to-image
```

3. Para Inicializar el control de versiones con *GIT*

```
$ git init
```

```
$ git add -all
```

```
$ git commit -m "Primer commit"
```

```
$ git branch -M main
```

4. Para ejecutar el servidor de desarrollo y visualizar en el navegador el funcionamiento del entorno para desarrollar.

```
$ php artisan serve
```

Al ejecutar este comando, se mostrará en pantalla la URL para visitar y comprobar el funcionamiento de la aplicación.

Anexo D. Manual de Usuario Final.

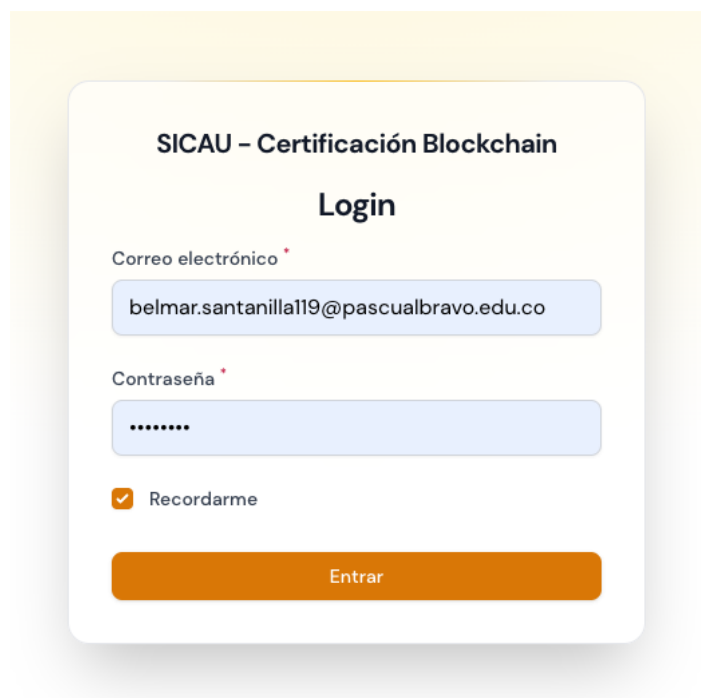
Este documento permitirá a las personas que lo consulten conocer en detalle el funcionamiento del sistema para generar certificados digitales en una *blockchain* pública.

Requisitos de uso

- Conexión a internet \geq 2MB
- Computador de escritorio
- Navegador web

Iniciar sesión

1. Abrir el navegador e ingresar la URL de la aplicación en la barra de direcciones
2. Introducir el correo electrónico del usuario
3. Introducir la contraseña asignada
4. Seleccionar el campo “Recordarme” si desea que la sesión permanezca activa
5. Dar clic en el botón “Entrar” o presionar la tecla “Enter”



SICAU - Certificación Blockchain

Login

Correo electrónico *

belmar.santanilla19@pascualbravo.edu.co

Contraseña *

.....

Recordarme

Entrar

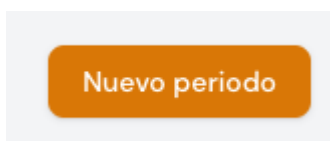
Crear un periodo

1. En el menú principal de la aplicación seleccione la opción “Periodos” para acceder a la sección que permite la gestión de un periodo de certificación.

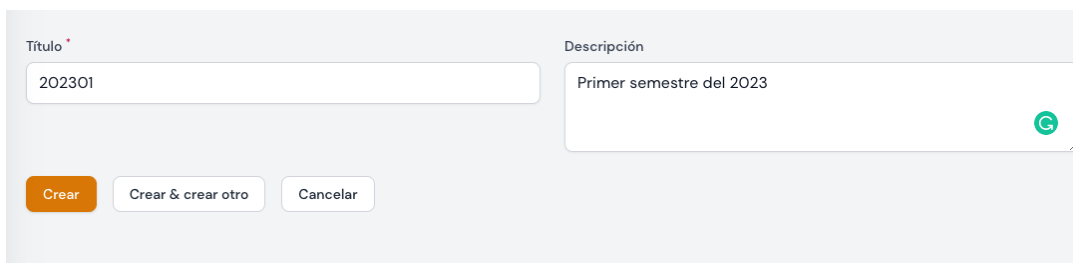
2.



3. En la parte superior derecha, localice el botón “Nuevo periodo” y de clic sobre él para abrir el formulario de creación



4. Se mostrará un formulario donde podrá asignar un nombre al periodo que desea crear y una descripción que le ayudará a entender el registro que está creando

The image shows a form for creating a new period. It has two input fields: "Título *" with the value "202301" and "Descripción" with the value "Primer semestre del 2023". Below the fields are three buttons: "Crear" (blue), "Crear & crear otro" (white), and "Cancelar" (white).

5. Una vez completada la información de clic en el botón “Crear” y aparecerá una notificación en la parte superior derecha indicando que el periodo se ha creado con éxito

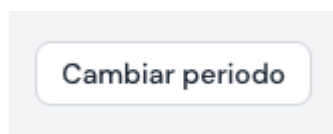


Diseñar un certificado académico

1. En el menú principal seleccione la opción “Diseñar certificado”



2. En pantalla aparecerá un mensaje para que seleccione el periodo académico o la promoción para la cual va a crear el certificado. Ubique el botón de la parte superior derecha denominado “Cambiar periodo” y de clic sobre él.



3. Aparecerá un cuadro de diálogo donde podrá seleccionar el periodo con el que desea trabajar, elija uno y presione el botón “Enviar”



A screenshot of a modal window titled "Cambiar periodo". It features a dropdown menu labeled "Periodo" with the text "Seleccione una opción" and a downward arrow. Below the dropdown are two buttons: "Enviar" (orange) and "Cancelar" (white with grey border).

4. En la interfaz aparecerá el arte base para diseñar el certificado y adicionalmente encontrará un botón denominado “Agregar campo” para incluir información en el certificado que desea generar.



A screenshot of a certificate design interface. The header is "Campos del certificado" and there is an orange "Agregar campo" button. The main area contains the logo of "INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO" and a horizontal line below it.

5. De clic en el botón “Agregar campo”, aparecerá un control donde podrá elegir los campos que desea añadir al certificado y la posición donde quiere añadirlo.

Campos del certificado

Campos *

Seleccione una opción

Documento

Primer nombre

Segundo nombre

Primer apellido

Segundo apellido

Posición superior *

Agregar campo

INSTITUCIÓN UNIVERSITARIA
PASCUAL BRAVO

6. Una vez haya agregado los campos que desea incluir en el certificado, puede salir de la página y empezar a certificar estudiantes.

Campos del certificado

Campos *

Primer nombre x Segundo nombre x Primer apellido x

Seleccione una opción

Posición superior *

16

Campos *

Documento x

Seleccione una opción

Posición superior *

18

Agregar campo

INSTITUCIÓN UNIVERSITARIA
PASCUAL BRAVO

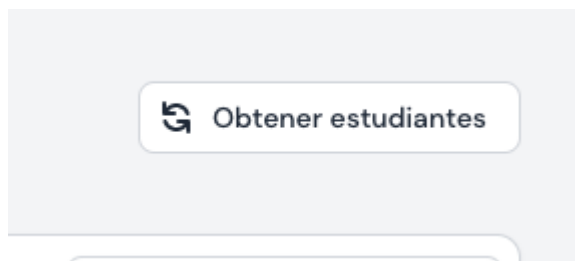
ELIZA LESLIE GRAHAM
6759-4371-9432-7554-961

Obtener estudiantes para certificar

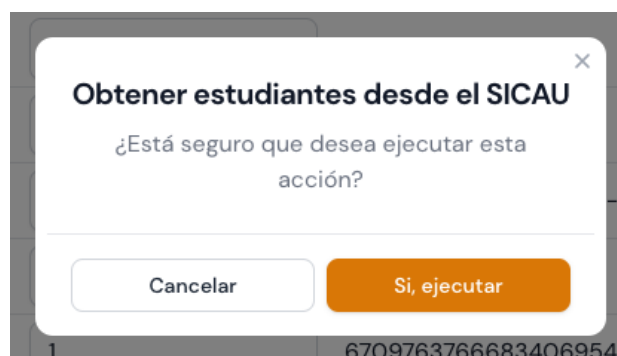
1. Una vez iniciada sesión, debe ingresar a la opción “Estudiantes” en el menú principal de la aplicación



2. En la parte superior derecha, localice el botón “Obtener estudiantes” y de clic sobre él para ejecutar la opción



3. Aparecerá un cuadro de diálogo para confirmar la acción, si está seguro de obtener los datos de los estudiantes desde el SGI SICAU, de clic en el botón “Si, ejecutar”



4. Espere un momento y empezará a obtener un listado de estudiantes autorizados para recibir una certificación digital

Autorizar un estudiante para generar un certificado

1. En el listado de estudiantes, ubique el estudiante que quiere autorizar y de clic en la acción “Editar”

 Editar

2. Una vez hayan cargado los datos del estudiante seleccionado, puede utilizar el control “Autorizado” ubicado al comienzo de los datos del estudiante y dar clic para autorizarlo y habilitar el botón para forjar el certificado.

<input checked="" type="checkbox"/> Autorizado	Documento 6771-8939-5074-6392
Primer nombre Rudolph	Segundo nombre James
Primer apellido Tillman	Segundo apellido Rath
Correo electrónico Crawford.Morar12@hotmail.com	ID SICAU 12
Programa / Carrera Modern	Orden para forjar 1
Creado el 24/10/2022 12:10:22	Última actualización 24/10/2022 12:10:22

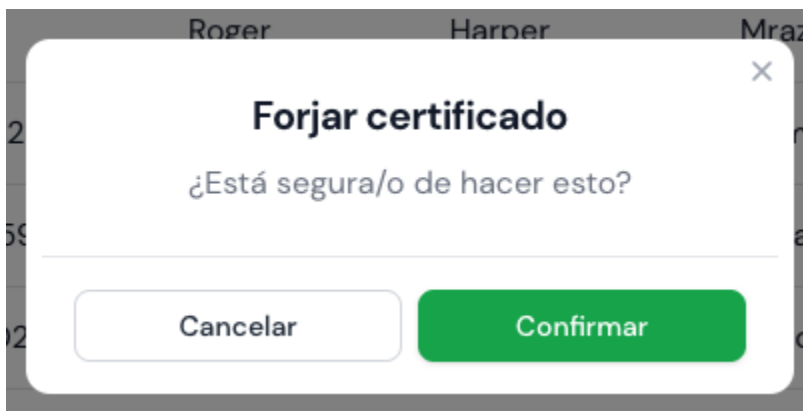
3. Dar clic en el botón guardar

Forjar un certificado para un estudiante

1. En el listado de estudiantes, ubique el estudiante que esté autorizado y de clic en la acción “Forjar certificado”

 Forjar certificado

2. Aparece un cuadro de diálogo para confirmar la generación del certificado.



3. Si está seguro de querer generar el certificado de clic en el botón “Confirmar”
4. Una vez confirmado, el certificado quedará registrado en la *blockchain* y estará disponible para su consulta

Anexo E. Despliegue en Producción.

Para realizar el despliegue de la aplicación en un ambiente de producción, se debe inicialmente revisar que se cumpla con los requisitos básicos que necesita la aplicación para funcionar con criterios de calidad aceptables:

- 2GB Memoria *RAM*
- 15 GB *HDD o SSD*
- *PHP* \geq 8.0
- *GIT* \geq 2.38.0
- *Composer* \geq 2.4.0
- *MySQL* \geq 8.0

Paso 1. Ubicar los archivos que componen el proyecto en la raíz de un servidor web.

Paso 2. Conectar la base de datos con el motor *MySQL* instalado, la conexión se realiza a través de la modificación del archivo de entorno denominado: *.env* que se encuentra ubicado en la raíz del proyecto. Los datos que se deben modificar de acuerdo con la configuración del ambiente son los siguientes:

- *DB_CONNECTION*
- *DB_HOST*
- *DB_PORT*
- *DB_DATABASE*
- *DB_USERNAME*
- *DB_PASSWORD*

Paso 3. Configurar el arte base para generar los certificados digitales. Por lo tanto, se hace necesario tener un archivo en formato *.jpg* que contenga el diploma vacío que se desea generar, y sobre el cual se forjaran los certificados para cada estudiante. En el mismo archivo *.env* se modifica la variable: *CERTIFICATE_URL*.

Paso 4. Configurar las variables de entorno en el mismo archivo *.env* para realizar la conexión con el *API* encargado de forjar los certificados en la *blockchain* de *Cardano*, por lo tanto, se deben agregar los siguientes campos:

- NMKR_API_URL
- NMKR_API_KEY
- NMKR_PROJECT_UID

Los datos para completar estos campos pueden generarse en la plataforma *NMKR*, que ofrece una completa infraestructura para aplicaciones web basadas en la *blockchain* pública de *Cardano*.

Paso 5. Configurar la dirección de una billetera de *Cardano* en el archivo *.env* con el nombre: *CARDANO_WALLET*.

De esta manera y siguiendo los pasos descritos anteriormente, podrá desplegar el proyecto en un ambiente de producción.