# BC-CAD SISTEMA PARA LA GENERACIÓN Y VALIDACIÓN DE CERTIFICADOS ACADÉMICOS DIGITALES IMPLEMENTANDO BLOCKCHAIN

## BC-CAD SYSTEM FOR GENERATION AND VALIDATION OF ACADEMIC CERTIFICATES DIGITAL IMPLEMENTING BLOCKCHAIN

**Brayan Samir Cuervo Galindo**
bcuervo@academia.usbbog.edu.co

**Miguel Ignacio Rodríguez Suarez**
mirodriguezs@academia.usbbog.edu.co

**Andrés Armando Sánchez Martín**
aasanchez@usbbog.edu.co

Universidad de San Buenaventura
Ingeniería de Sistemas
Colombia

**Resumen**

En Colombia hay una creciente problemática con los certificados académicos universitarios falsificados, según un estudio de la entidad Competencia Humana de alrededor de 15000 títulos revisados el 14.4% de los mismos eran falsos, además de esto el 65% de los títulos falsos corresponden a diplomas de bachillerato, 21% a diplomas técnicos, el 14% a títulos profesionales y de especialización, por lo cual proponemos realizar un sistema implementando Blockchain el cual estará diseñado directamente para realizar el almacenamiento seguro de certificados académicos universitarios contando con una protección integrada de firmas digitales, las cuales permiten ofrecer una mayor validación al certificado de una manera más rápida y eficaz la cual mejorará la creciente problemática de certificados académicos, por lo cual las empresas o entidades que deseen emplear a algún estudiante podrán hacerlo de una manera más eficiente y así contar con profesionales que se desempeñen en su trabajo y que si cuenten con los conocimientos para realizar el mismo. El proyecto consta de 3 fases principales constituidas por distintas actividades las cuales son Inicio, diseño y finalmente la fase de validación, en este momento se va finalizando la fase de diseño en donde se plantean todos los diagramas y modelos respectivos para empezar con la última fase. Primero se realizó la investigación respectiva para el planteamiento del proyecto seguidamente se encontraron los requerimientos respectivos para tener claras las expectativas que debemos cumplir con el sistema y luego para poder hacer el diseño del sistema se usó el modelo de vistas de arquitectura 4+1 de Kruchten y además se realizó un modelo unificado el cual se construyó teniendo en cuenta los distintos usuarios y funcionalidades que interactúan entre sí en el sistema, finalmente se realizó la arquitectura basándose en el modelo de capas, en el cual lo dividimos en 4 capas esenciales para el funcionamiento óptimo del proyecto con sus respectivas relaciones entre sí.

**Palabras clave:**

Blockchain, Contratos Inteligentes, Certificado Académico, Certificados Digitales, Instituciones de Educación Superior.

## INTRODUCCIÓN

Las IES o instituciones de educación superior son los centros educativos en donde se ofrecen carreras de nivel superior las cuales cuentan con el reconocimiento oficial como prestadoras del servicio público de la educación superior en el territorio colombiano. Las IES o instituciones de educación superior son los centros educativos en donde se ofrecen carreras de nivel superior las cuales cuentan con el reconocimiento oficial como prestadoras del servicio público de la educación superior en el territorio colombiano [1].En cuanto a los certificados académicos encontramos que se crea el Sistema Nacional de Información con el objetivo de servir de cómo registro público de los documentos académicos relativos entre otros a los estudiantes de la educación formal y no formal. Se ordena recopilar información que sea útil para terceros, en relación con la prestación del servicio público de educación. Como aspecto a resaltar el artículo 11 del decreto 1860 de 1994, en el que dispone que el título y el certificado son el reconocimiento expreso de carácter académico otorgado a una persona natural al concluir un plan de estudios, haber alcanzado los objetivos de formación y adquirido los reconocimientos legal o reglamentariamente definidos. También se obtendrá el título o el certificado, al validar satisfactoriamente los estudios correspondientes, de acuerdo con el reglamento [2] [1].

Además, hay distintos tipos de certificados como un Certificado de estudio, Certificado de notas semestral con promedio semestral, Certificado de vigencia de práctica profesional, entre otros. El certificado de estudios normalmente se conoce como título, cabe recalcar que cualquier irregularidad o falsedad dentro de estos certificados pueden ser sancionados. También El encargado de la validación de los certificados es el Ministerio de educación y ya específicamente el que otorga el título son las instituciones educativas con registro calificado, el cual es un requisito indispensable para garantizar la calidad educativa a nivel nacional [3] .El proceso para seguir a la hora de querer obtener un certificado académico sería primero realizar el pago financiero según el tipo de certificado a solicitar para seguidamente acercarse a la Oficina de Registro Académico para diligenciar el formato de solicitud, cabe recalcar que todo trámite ante la Oficina de Registro debe hacerse de manera personal, de no ser posible el acudiente deberá presentar carta de autorización con su respectiva firma y autenticidad. La falsificación de certificados académicos en Colombia es un problema latente por la facilidad de expedición de certificados falsos y la demora en la verificación de certificados académicos, por su parte el Ministerio de educación no tiene las herramientas suficientes para validar dichos certificados, pero la Fiscalía de la Nación si, y castiga a las empresas fraudulentas y a la persona que compran dichos certificados por medio de sanciones que oscilan entre 10 a 15 años de prisión [4].Un estudio realizado por la entidad "Competencia Humana" la cual determinó que de 15000 títulos revisados el 14.4% de los mismos eran falsos, además de esto el 65% de los títulos falsos corresponden a diplomas de bachillerato, 21% a diplomas técnicos, el 14% a títulos profesionales y de especialización. También este estudio encontró que el 20% de los documentos falsificados pertenecían a entidades que jamás existieron [5].

Como se puede tener en cuenta anteriormente, la estadística de falsificación de certificados es alta, así que necesitamos buscar una solución eficiente que nos permita tratar este problema a fondo, dentro de técnicas funcionales deberemos implementar una arquitectura específica para permitir plantearnos cómo será la secuencia de guardado y validación, ya que debemos contar con una imagen previa de lo que buscamos implementar, luego de tener claro esto podremos pensar en qué herramientas podemos implementar junto con el Blockchain haciendo más eficiente el registro, validación y protección de estos documentos. Dentro de los estándares de la aplicación se buscará implementar un hash para la protección y encriptación de los datos registrados en cada bloque, estos datos deberán ser visibles en tiempo real, haciendo uso de esta nueva tecnología que es Blockchain se buscará anidar los datos de cada certificado académico por medio de las cadenas y sus bloques, haciendo que el registro sea más descentralizado. Un ejemplo dentro de la implementación de esta tecnología se puede ver reflejada en la universidad Nacional ya que fue una de las primeras universidades en tomar el riesgo de implementarla, debido a que la solicitud y el registro de un certificado conlleva a mucho tiempo haciendo que sea un proceso muy tardío, aparte de la seguridad con Blockchain buscamos agilizar el tiempo de solicitud de estos [3].

Una vez terminado este sistema esperamos tener la generación y validación de certificados digitales académicos implementando Blockchain la cual se implementará por parte del ministerio de educación de Colombia y las IES con esto buscamos evitar la falsificación de certificados y facilitar la verificación de los certificados ya sea una empresa, una

universidad o una persona del común, ya que cada certificado generado por nuestro software tendrá una clave única con la cual se podrá buscar en nuestra base de datos. En este artículo podremos encontrar diferentes secciones entre las cuales podemos demos encontrar la metodología en la cual podremos ver las diferentes etapas en las cuales a pasado el proyecto, además de esto también podemos encontrar la sección de resultados en la cual se podrán ver los avances más importantes que dieron en la metodología y por último podremos encontrar la discusión y conclusión

## Método

Para la realización de este sistema se realizó una exhaustiva investigación de trabajos relacionados para así ver la viabilidad del sistema, la mayoría de estos artículos fueron sacados de bases de datos validadas y se pudo observar que la mayoría de estos no tienen las normativas legales de Colombia, además de esto no eran aplicados al sector educativo. Luego de esto se plantearon las respectivas fases/etapas para poder empezar con el proyecto, primero se comenzó con la abstracción de los respectivos requerimientos tanto funcionales como no funciones, los cuales nos permitieron ver de manera más concreta la capacidad y funcionamiento generales que tendrá el sistema, para seguidamente proseguir con la arquitectura y los distintos modelos que nos proporciona el modelo 4+1 de Kruchten los cuales nos serán de mucha utilidad a lo hora de empezar con la realización del sistema. Ahora la metodología en la cual se basará el proyecto a realizar se dividirá en tres fases las cuales se representan en el siguiente gráfico.

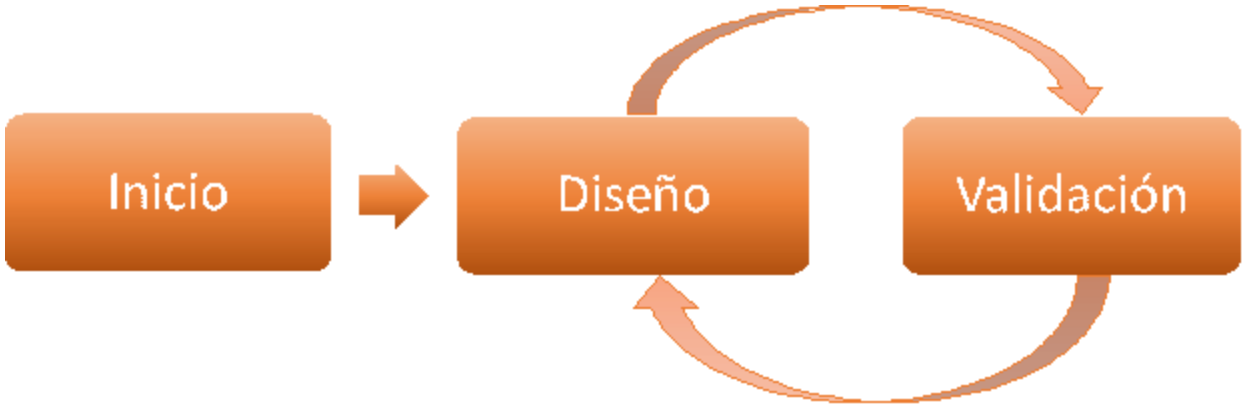


*Imagen 1 metodología*

En donde la primera fase consistirá en el inicio el cual hace referencia a la investigación respectiva de los trabajos relacionados, extracción de requerimientos necesarios para el funcionamiento óptimo del sistema tanto de Blockchain como de creación de certificados digitales y el almacenamiento de estos, sin dejar de lado el identificar qué tipo de seguridad se empleará en el sistema. Finalmente, en esta fase se hará el análisis de cada uno de los apartados tanto de requerimientos como de casos de uso.

Seguidamente pasamos a la fase de diseño en donde se conceptualizará y modulará el sistema dejando claro el funcionamiento tanto interno como externo del mismo en cuanto a la validación de los certificados digitales. En este apartado se diseñarán los respectivos modelos y estructuras del comportamiento del sistema y su funcionamiento, teniendo claros que componentes serán necesarios para la realización del sistema y construyendo el modelo conceptual del sistema.

Finalmente tendremos la etapa de validación donde se realizará un prototipo del sistema y poder realizar las pruebas de concepto las cuales nos arrojarán los resultados de si el sistema está funcionando de manera óptima, luego de esto se analizarán los respectivos resultados y si es necesario se hará un rediseño del sistema para solucionar los inconvenientes que se hayan generado.

En estos momentos ya se han realizado la primera, por lo cual estamos en la fase de diseño en la cual ya se han hecho distintos diagramas, el modelo unificado y la arquitectura.

## Resultados

Para realizar la investigación de los distintos conceptos a tener en cuenta para la realización del proyecto se tuvo en cuenta una base de conocimiento en la cual se tuvo que tener en cuenta tres distintos marcos, como los son:
El marco conceptual en el cual se tuvieron en cuenta los conocimientos base del proyecto como los distintos objetivos y funciones del ministerio de educación como la definición general de lo que son las Instituciones de educación superior, también se tuvo en cuenta la definición de un certificado académico con sus respectivos tipos y de qué manera se validaba la veracidad de estos.

### Estado del arte

En el marco Tecnológico como su mismo nombre lo especifica se vieron distintas definiciones de las tecnologías como el Hash con sus respectivas características y utilidades, Los certificados digitales con sus distintos formatos, Los distintos tipos de aplicaciones y la más importante, Blockchain.
Finalmente se investigó respecto a las normativas colombianas como el Open Data, el sistema de gestión de la seguridad de la información y demás leyes que ayudan a comprender las normativas.
Tras hacer la respectiva investigación, se realizó el estado del arte en el cual investigamos 30 artículos relacionados con los siguientes aspectos:

1. Aplica normativas de Colombia: los proyectos investigados cumplen con las normativas de Colombia.
2. Implementa Blockchain: los proyectos investigados están aplicados con una cadena de datos además de esto cumple con estándares de seguridad-hash
3. Sistema web distribuido: los proyectos investigados se propongan un sistema distribuido que se encuentran
4. Aplica al sector educativo: los proyectos investigados están aplicados a los certificados digitales en el sector educativo.
5. Evitan fraudes de falsificación: los proyectos investigados fueron desarrollados para evitar el fraude.
6. Aplicado a la universidad de San buenaventura Sede Bogotá: los proyectos investigados están aplicados hacia la Universidad de San Buenaventura Sede Bogotá.

Al evaluar los artículos pudimos filtrar de 30 a 10 artículos, en donde cumplían con la mayoría de los anteriores aspectos, los artículos más similares a este son:

1. ECBC: A High-Performance Educational Certificate Blockchain with Efficient Query [6] [17]
2. BKI: Towards Accountable and Decentralized Public-Key Infrastructure with Blockchain [7]
3. Blockchain-based approach to create a model of trust in open and ubiquitous higher education [8]
4. Systems and Methods that Utilize Blockchain Digital Certificates for Data Transactions [9]
5. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward [10]
6. Blockchain,academic verification use case [11]
7. Blockchain and the future of digital learning credential assessment and management [12]
8. A Blockchain-based Educational Record Repository [13]
9. Certificate issuing system based on blockchain [14]
10. Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and SmartContract [15] [16].

En base a estos proyectos se realizó una tabla comparativa en la cual podremos observar que aspectos cumplen los proyectos que fueron investigados por nosotros.

| | Aplicado en Colombia | Implementa Blockchain | Sistema web distribuido | Aplica al sector educativo | Evitan fraudes de falsificación |
|---|---|---|---|---|---|
| 1 | | X | X | X | X |
| 2 | | X | X | X | X |
| 3 | | X | X | X | X |
| 4 | | X | X | X | X |
| 5 | | X | X | X | X |
| 6 | | X | X | X | X |
| 7 | | X | X | X | X |
| 8 | | X | X | X | X |
| 9 | | X | X | | X |
| 10 | | X | X | | X |

*Tabla 1 Aspectos de investigación*

En base a esta tabla pudimos observar que el proyecto es viable ya que sean realizado proyectos similares, pero no iguales por los cual este proyecto es innovador para el sector educativo en Colombia. Tras leer los distintos artículos relacionados pudimos definir la metodología a seguir la cual se basó el proceso, es el modelo en espiral, el cual se encontrará dividida por tres fases, las cuales se basan en un inicio, en el diseño y por último la validación, en donde también se tendrá en cuenta un punto de retorno de la validación al diseño, teniendo en cuenta que en caso de presentar algún problema durante la validación del proyecto se pueda realizar una modificación en el diseño. Además de la investigación se extrajeron los distintos usuarios que interactuaron con el sistema de manera directa y con sus respectivas funcionalidades.

## Definición de Usuarios

En este apartado veremos los distintos usuarios que interactuaran directamente con el sistema y veremos sus funciones específicas en el proyecto.

1. IES: Las IES o instituciones de educación superior serán las encargadas de publicar o subir los respectivos certificados académicos de manera que seguidamente se puedan consultar mediante la página web.
2. ESTUDIANTE: El estudiante será uno de los usuarios que podrá ingresar a la página web para poder verificar sus respectivos certificados académicos y tabulado de notas respectivo.
3. EMPRESA: Las empresas serán uno de los usuarios que podrán ingresar a la página web para poder verificar los certificados que requieran para sus respectivos fines.
4. MINISTERIO DE EDUCACIÓN: Esta entidad será la encargada de hacer la validación de las IES de forma que solo podrán ingresar al sistema IES que estén verificadas por esta entidad y también.
5. Administrador: Será el encargado de hacer la administración del sistema.

## Requerimientos

Ahora que tenemos claros los respectivos usuarios que interactúan con el sistema se hizo la búsqueda de los requerimientos tanto funcionales como no funcionales los cuales nos ayudan a asegurar que el proyecto a realizar cumplirá con las expectativas que se tenían planteadas y que cumplirá las respectivas funciones para poder solucionar la problemática seleccionada anteriormente. A continuación, se presentan los requerimientos con su respectiva prioridad la cual irá de 1 a 3 donde el 3 será muy prioritario y el 1 poco prioritario, además de esto diferenciaremos los requerimientos entre funcionales (RF) y no funcionales (RNF).

| Requerimiento | Prioridad | Tipo |
|---|---|---|
| El sistema debe permitir la consulta de certificados académicos, mediante un acceso de clave pública. | 3 | RF |
| El sistema debe negar la modificación de certificados académicos. | 3 | RF |
| El sistema debe permitir el uso de firmas digitales. | 3 | RF |
| El sistema debe permitir la publicación de certificados, basado en las políticas de Blockchain de las IES. | 3 | RF |
| El sistema debe permitir generar un sello de tiempo que permita validar de que año es el certificado académico y de notas. | 2 | RF |
| El sistema debe permitir el proceso de inscripción y validación de las IES. | 3 | RF |
| El sistema debe permitir la integración de control de roles. | 3 | RF |
| El sistema debe generar códigos QR para la visualización del certificado académico. | 2 | RF |
| El sistema debe permitir a las IES certificadas el acceso a la base de datos. | 3 | RNF |
| El sistema debe permitir el fácil uso de la página web. | 2 | RNF |
| El sistema debe permitir el uso de smart contract. | 3 | RNF |
| El sistema debe conectarse con base de datos. | 3 | RNF |

*Tabla 2 Requerimientos*

Una vez hechos los requerimientos funcionales y no funcionando tuvimos una mejor perspectiva de que se necesita para el buen funcionamiento del sistema, y procedimos a la segunda fase se comprenderá la ejecución de la modulación y el diseño tanto del funcionamiento interno como externo del sistema, comprendiendo también el proceso de validación de los certificados digitales.

## Modelo unificado

En el siguiente diagrama podemos identificar y unificar los módulos que componen el sistema los cuales son el módulo de la IES, el módulo del Ministerio de educación y el módulo de la app web.

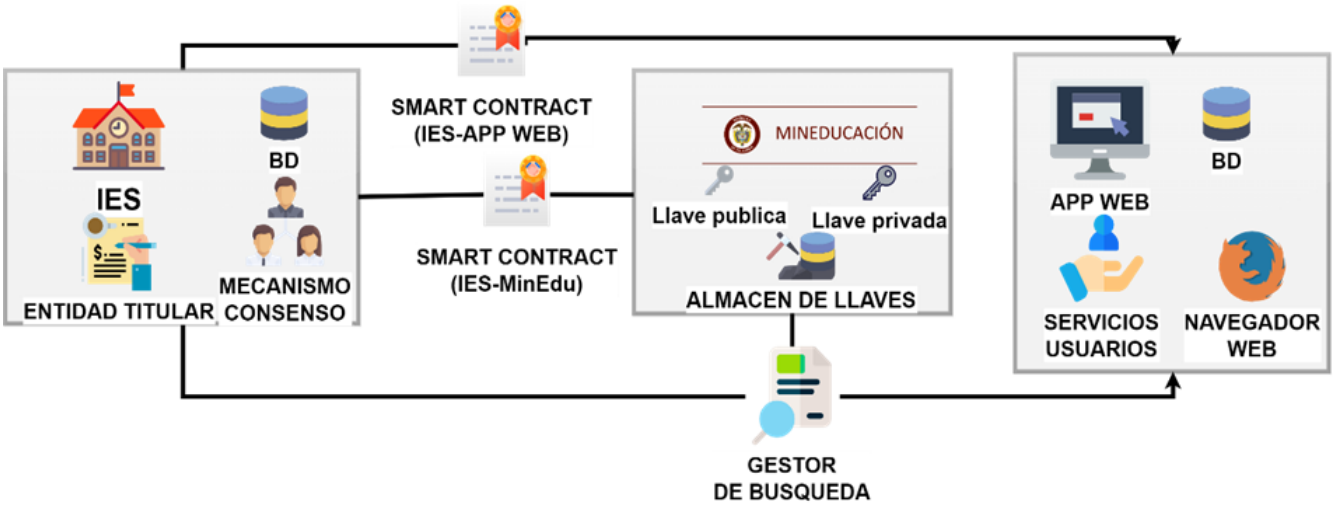


*Imagen 3 Modelo Unificado*

Como se puede ver en la imagen 3, hay dos Smart contract, el primero valida que la IES cumple con las normativas preestablecidas por el ministerio de educación para la generación de certificados académicos y el segundo verifica que la IES este en modo activo para poder acceder al sistema, además de esto hay un gestor de búsqueda el cual se encarga de realizar la búsqueda de los certificados académicos y las IES. Además, cada uno de los módulos esta conformado por sus respectivos almacenes y/o bases de datos en los cuales se guardarán las llaves publicas y privadas de los certificados digitales, los datos de las instituciones de educación superior y los datos de los certificados académicos guardados en

el sistema. En el módulo de la IES encontraremos un apartado que consiste en un mecanismo de consenso el cual el cual tendrá la potestad de tomar decisiones en la red Blockchain. Además, en el módulo de la aplicación web tendríamos todos los servicios que se le brindarán a los usuarios y de esta manera funcionar de una manera optima con la respectiva página web.

## Casos de uso

A partir de los usuarios se obtiene el diagrama de casos de uso con el cual se evidencian las distintas actividades que pueden llegar a realizar cada uno de los usuarios como los son los estudiantes, las IES (instituciones de educación superior), el administrador y finalmente el ministerio de educación.

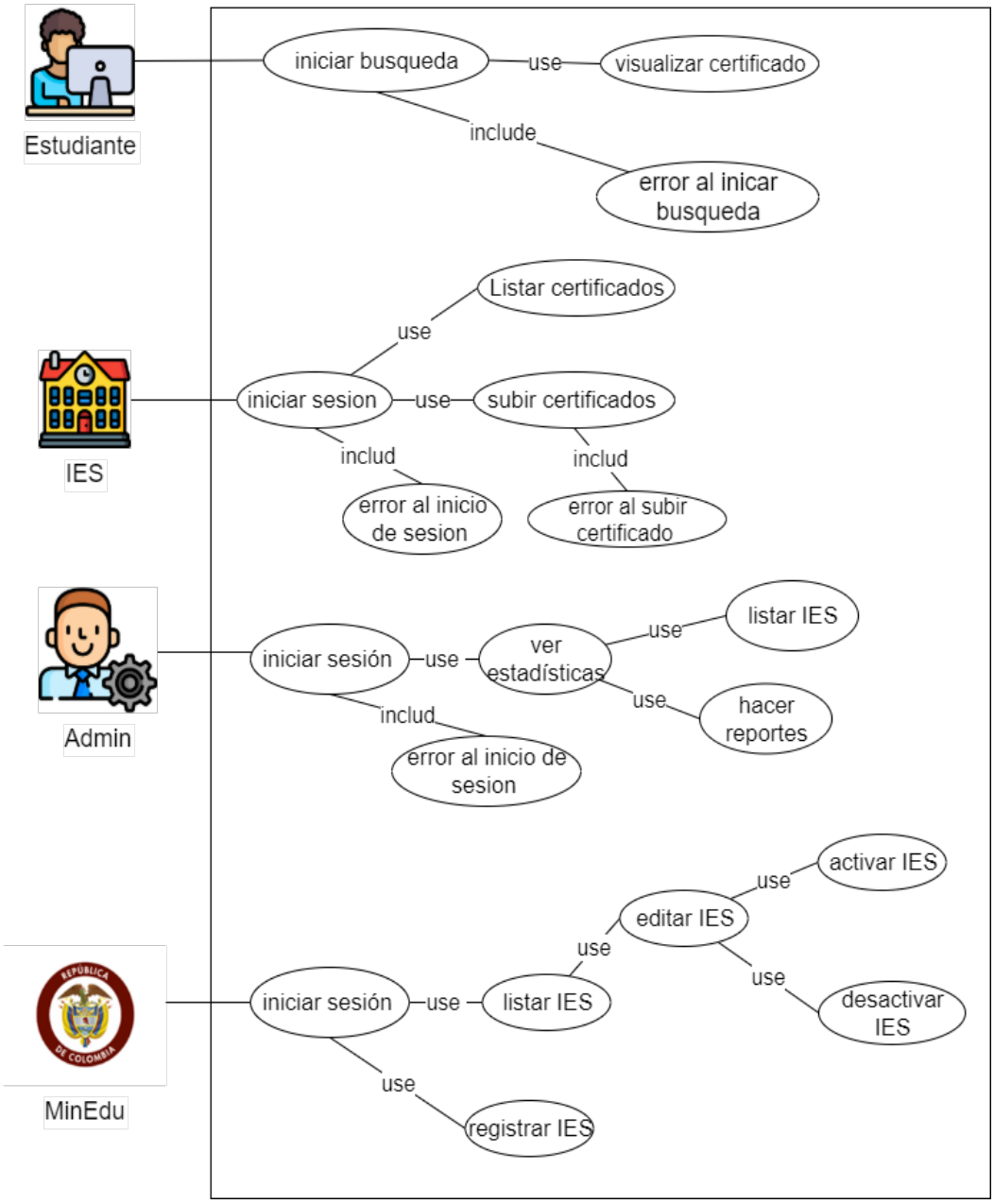

*Imagen 2 Casos de uso*

Cabe recalcar que el diseño del sistema se realizó haciendo uso del modelo de 4+1 de kruchten el cual nos proporciona distintos tipos de diagramas los cuales ayudan para más adelante hacer el desarrollo del prototipo de manera más rápida y eficaz.

## Arquitectura

Por último, realizamos la arquitectura en la cual se definieron 4 capas las cuales son: capa de clientes. capa de presentación, capa de operación y la capa de datos, las cuales interactúan entre ellas como se ve a continuación.

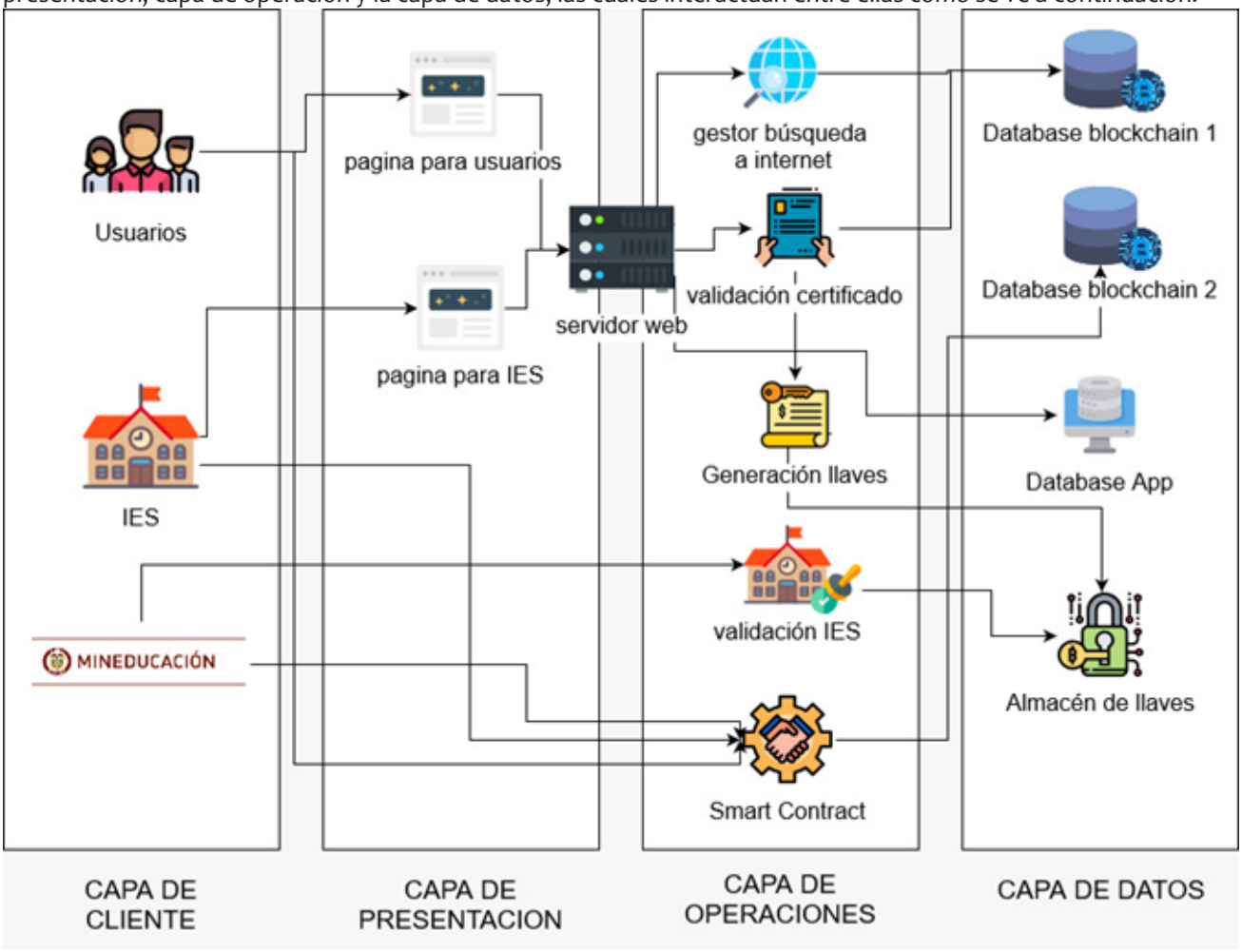


*Imagen 4 Arquitectura*

Como se observó en la imagen 4 solo los usuarios y las IES se relacionan con la capa de presentación en donde cada uno de ellos interactuará con el sistema con su propia pagina, luego en la capa de operaciones se harán todas la validaciones, búsquedas de los datos y validación de los Smart Contract para poder seguir a la siguiente capa y gestionar el guardado de las llaves publicas y privadas y los certificados académicos digitales. Por último, en la tercera y última fase se tendrá el desarrollo de un prototipo del sistema, el cual servirá como demostración funcional del sistema, el cual permitirá obtener resultados o informes de las pruebas realizadas en este, como también la obtención de objetivos que permitan definir si el sistema planteado necesita un rediseño o no.

## Discusión y Conclusión

En este momento gracias a la investigación respectiva se evidencia que el proyecto implica un gran impacto en la problemática de los certificados académicos falsificados, por lo cual las empresas podrán confiar más en los conocimientos de sus nuevos empleados. El proyecto en este momento va en la fase final de diseño, en esta fase se espera tener los distintos diagramas, mockups y las herramientas con las que se construirá el sistema, con los cuales se finalizará esta fase y procederemos a la última fase en cual se procedería a realizar la prueba de concepto creando un prototipo lo cual nos proporcionará una visión más tangible del funcionamiento del sistema. A lo largo de la fase de diseño se presentaron algunos inconvenientes los cuales fueron la unificación de los diferentes modelos los cuales constituyen el modelo unificado y además de esto la selección a la herramienta para el montaje de la red Blockchain. Una vez culminado el proyecto se podría expandir de manera que más universidades pudieran guardar sus certificados en la cadena por lo cual cada vez más certificados fueran seguros y por lo tanto el impacto sería mucho mayor.

## Bibliografía


[1] C. G. TRUJILLO., Ley 30 de Diciembre 28 de 1992, Bogota, 1992.

[2] DECRETO 1860 de 1994 - Articulo 62, 1994.

[3] MINTIC, «Guía para la Implementación de Seguridad de la Información en una MIPYME,» SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, BOGOTA, 2016.

[4] J. Jules, «RCN Radio,» 26 03 2018. [En línea]. Available: https://www.rcnradio.com/recomendado-del-editor/que-tan-facil-es-falsificar-un-titulo-academico-o-un-certificado-de-estudios.

[5] Semana, «Semana,» 06 10 2017. [En línea]. Available: https://www.semana.com/mundo/articulo/otro-militar-en-contra-de-maduro/602028.

[6] Y. Xu, S. Zhao, L. Kong, Y. Zheng, S. Zhang y Q. Li, ECBC: A High Performance Educational Certificate Blockchain with Efficient Query, 2017.

[7] Z. Wan, Z. Guan, F. Zhuo y H. Xian, BKI: Towards Accountable and Decentralized Public-Key Infrastructure with Blockchain, 2018.

[8] D. Lizcano, J. A. Lara y B. W. A. , Blockchain-based approach to create a model of trust in open and ubiquitous higher education, 2019.

[9] C. M. Allen, «patents,» 16 09 2016. [En línea]. Available: https://patents.google.com/patent/US20180082290A1/en. [Último acceso: 09 04 2019].

[10] M. Sharples, «Springer,» 07 09 2016. [En línea]. Available: https://link.springer.com/chapter/10.1007/978-3-319-45153-4_48. [Último acceso: 09 04 2019].

[11] F. Bond, Blockchain, academic verification use case, Buenos Aires, 2015.

[12] M. Jirgensons y J. kapenieks, Blockchain and the Future of Digital Learning Credential Assessment and Management, 2018.

[13] E. Bessa y J. Martins, A Blockchain-based Educational Record Repository, Bahia, Salvador, 2019.

[14] J. Sun Uhr, J. Wu Hong y J. Han Song, Certificate issuing system based on block chain, 2018.

[15] K. T., t. R, Y. V y H. K., Integration of Digital Certificate Blockchain and, chennai, 2019.

[16] E. Norman-Acevedo, Consumer cultural studies, 1a ed. Bogotá: Institución Universitaria Politécnico Grancolombiano, 2019.

[17] E. Norman-Acevedo, Los modelos logisticos para la construcción de eficiencia empresarial, Revista Punto de vista Vol. 12 No. 8 Año. 2018. Bogotá: Institución Universitaria Politécnico Grancolombiano, 2018.