



**Carrera de Ingeniería en Informática**

***“Generación y autenticación de certificados únicos”***

**Alumnos**

**Michael Johannes Enns Reimer**

**Danilo Klassen Harms**

**Tutor:**

**Heriberto Pintos**

**Línea de Investigación:**

**Tecnologías de la Información**

**Asunción – Paraguay**

**2022**



## ÍNDICE

|  |     |
|--|-----|
| Agradecimientos                          | ii  |
| Dedicatoria                              | iii |
| Índice                                   | iv  |
| Índice de figuras                        | vi  |
| Resumen                                  | 1   |
| Introducción                             | 2   |
| Planteamiento y descripción del problema | 2   |
| Tipos de Investigación                   | 4   |
| Preguntas de la investigación            | 5   |
| Preguntas específicas.                   | 6   |
| Objetivos                                | 6   |
| Objetivos específicos.                   | 6   |
| Justificación                            | 7   |
| Aporte                                   | 8   |
| Estado del arte                          | 8   |
| Marco teórico                            | 9   |
| Antecedentes                             | 10  |
| Tipos de blockchain                      | 12  |
| Blockchain pública                       | 12  |
| Blockchain privada                       | 13  |
| Híbrida                                  | 13  |
| Teoría de Blockchain                     | 14  |
| Normas ISO                               | 16  |
| Criptografía                             | 17  |
| Firma digital                            | 18  |
| Aspecto judicial                         | 18  |
| Especificación de la solución            | 20  |
| Arquitectura de la solución              | 21  |
| Emisión del certificado                  | 23  |
| Verificación del certificado             | 27  |
| Emisión del documento PDF                | 30  |
| Requerimientos funcionales               | 31  |
| Lado proveedor                           | 32  |



|                               |    |
|-------------------------------|----|
| Institución                   | 32 |
| Usuarios                      | 33 |
| Contratos                     | 33 |
| Lado cliente                  | 34 |
| Áreas                         | 34 |
| Historial                     | 34 |
| Crear certificado             | 35 |
| Verificación                  | 35 |
| Cuenta del usuario            | 35 |
| Requerimientos no funcionales | 38 |
| Conclusiones                  | 39 |
| Recomendaciones               | 41 |
| Referencias                   | 44 |
| Anexos                        | 47 |



## RESUMEN

Este trabajo de investigación tiene como objetivo desarrollar una plataforma web para la gestión de certificados digitales. Es producto de una visión tecnológica para el ámbito de la educación en Paraguay, con el objetivo de presentar una alternativa respecto a los documentos impresos y la consiguiente burocracia para la autenticación de éstos. Es importante indicar que, mediante algunas funciones de la tecnología blockchain, el algoritmo desarrollado genera y realiza la verificación auténtica de certificados únicos. En este sentido, Blockchain permite la trazabilidad de registros mediante las denominadas cadenas de bloques y a su vez las funciones criptográficas que aseguran la privacidad de datos y garantizan los estándares de seguridad de las transacciones.

La plataforma está formada por la interfaz y la parte del entorno. La interfaz del usuario utiliza la librería de Bootstrap para crear un entorno de trabajo amigable y para el entorno, se utiliza el “framework” Django, basado en Python, el motor de la base de datos utilizado es PostgreSQL. Las entidades que utilicen el sistema pueden generar certificados, de charlas o cursos, entre otros; para los beneficiarios mismos.

Los receptores y terceros pueden verificar la validez de los certificados mediante el número de certificado y el código verificador en la plataforma y, por supuesto, los certificados pueden ser imprimidos en formato PDF.

**Palabras clave:** Sistema web para educación, certificado digital, blockchain, algoritmo de autenticación, documentos académicos.