

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN



TEMA:

**ANÁLISIS Y DESARROLLO UNA APLICACIÓN DESCENTRALIZADA PARA
GARANTIZAR LA VERACIDAD DE CERTIFICADOS Y DIPLOMAS
ESTUDIANTILES.**

AUTOR:

RUIZ ANGULO MATEO FERNANDO

**TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y
COMPUTACIÓN**

QUITO, septiembre 2022

DEDICATORIA

Dedico el trabajo realizado a Dios, por haberme dado la vida, por los momentos vividos que permitieron formarme y que conforman mi ser; y permitirme el haber llegado hasta este momento importante en mi formación profesional y personal. A mi familia y seres queridos, por demostrarme siempre su cariño y apoyo incondicional sin importar las circunstancias ni las diferencias. A todas las personas que caminaron y caminan junto a mi lado, porque de ellos he aprendido y me influenciaron en quien soy.

De la misma forma este trabajo está dedicado para tratar de ir hacia un mejor futuro, que me permita no olvidar construir un mejor futuro para mí y para quienes me rodean. No olvidar mis principios humanísticos que fueron enseñados por maestros y profesores.

AGRADECIMIENTO

Existen muchas personas y cosas por las que agradecer, personas y cosas que tanto directa como indirectamente me permitieron realizar este trabajo. De esas personas, a mi persona y mi familia que con su esfuerzo y dedicación me ayudaron a culminar mi carrera universitaria y me dieron el apoyo suficiente para no decaer cuando todo parecía complicado e imposible y seguir peleando, seguir avanzando hasta no poder más. A mi director de Tesis, que por sus consejos y correcciones me ayudaron a finalizar este trabajo. A Profesores y maestros que me han visto crecer como persona, y gracias por sus conocimientos hoy puedo sentirme dichoso, orgulloso, contento y listo para seguir avanzando.

RESUMEN

Blockchain presenta muchas características, una de ellas (para la era actual) es la veracidad de la información. Uno de los problemas que han aparecido es la veracidad de la información, las noticias falsas y, en el área de la educación, los certificados y diplomas que se pueden encontrar en las hojas de vida. ¿Cómo se puede estar seguro que esos certificados son reales?

Para solucionar esa pregunta desarrollamos una aplicación web empleando tecnología basada en Blockchain. El enfoque es en desarrollar constantemente prototipos para analizarlos y mejorar el producto final; por lo que la metodología empleada es la metodología en Espiral. Con esta metodología vemos que es posible realizar aplicaciones web con Blockchain y verificables; pero como en todos los casos tiene sus contras que deben considerarse.

ÍNDICE

Contenido

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS	IV
ÍNDICE DE FIGURAS	IV
CAPÍTULO I: INTRODUCCIÓN	1
1. MARCO DE REFERENCIA.....	1
1.1. JUSTIFICACIÓN	1
1.2. Planteamiento del problema	2
1.3. Objetivo General	2
1.4. Objetivos Específicos	3
1.5. Antecedentes.....	3
1.6. Alcance	4
CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA	4
2. Marco Teórico.....	4
2.1. BLOCKCHAIN	4
2.2. TRABAJOS PREVIOS	9
2.3. SITUACIÓN ACTUAL DEL PROCESO DE ACREDITACIÓN DE CERTIFICADOS Y DIPLOMAS	10
2.4. VISUAL STUDIO.....	11

2.5.	HTML5.....	11
2.6.	CSS	11
2.7.	JAVASCRIPT	12
2.8.	TRINSIC.....	12
2.9.	D-APP	12
2.10.	Google Firebase.....	12
2.11.	ÁRBOLES DE NAVEGACIÓN.....	13
2.12.	DRAW.IO	13
2.13.	WEB 3.0.....	13
CAPÍTULO III: METODOLOGÍA		13
3.	Metodología de desarrollo.....	13
3.1.	Investigación Cualitativa	13
3.2.	Metodología de desarrollo de software	14
CAPÍTULO IV: DESARROLLO DE LA INVESTIGACIÓN		18
4.	DESARROLLO.....	18
4.1.	FASE 1: ANÁLISIS	18
4.2.	FASE 2: EVALUACIÓN	22
4.3.	FASE 3: DESARROLLO	26
4.4.	FASE 4: PLANTEAMIENTO	36
CONCLUSIONES Y RECOMENDACIONES.....		37
CONCLUSIONES.....		37

RECOMENDACIONES	38
BIBLIOGRAFÍA	40
GLOSARIO DE TÉRMINOS	43
Términos generados con su concepto como resultado de las palabras que el lector no conoce.	43
ANEXOS	44
Anexo A: Manual de usuario	44
Anexo B: Referencias de las APIs	60

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE FIGURAS

Figura 1 Funcionamiento Blockchain (Marín Pérez, 2022).....	8
Figura 2 Diagrama metodología y herramientas usadas.....	17
Figura 3 Diagrama de caso de uso de la aplicación.....	20
Figura 4 Diagrama de flujo para usuario Administrador	21
Figura 5 Diagrama de flujo para usuario Certificador.....	21
Figura 6 Diagrama de flujo para usuario Público	22
Figura 7 Landing page.....	23
Figura 8 Página para iniciar sesión.....	24
Figura 9 Página home	24
Figura 10 Página de ingreso nuevo certificado	25
Figura 11 Landing page (1/3)	26
Figura 12 Landing page (2/3)	27
Figura 13 Landing page (3/3)	27
Figura 14 Menú de usuarios	28
Figura 15 Login	29
Figura 16 Pestaña Administrador	30
Figura 17 Administrador-creación nueva organización	30
Figura 18 Pestaña certificador.....	31
Figura 19 Emisión certificado	32
Figura 20 Certificado subido.....	32
Figura 21 Wallet - certificados almacenados	33
Figura 22 Tabla de certificados	34

Figura 23 Pestaña verificador público.....	34
Figura 24 Verificación.....	35
Figura 25 Verificación.....	35
Figura 26 Trinsic Wallet app	44
Figura 27 Trinsic Wallet app	45
Figura 28 Ajustes	46
Figura 29 Red.....	47
Figura 30 Página principal	48
Figura 31 Selección usuario	49
Figura 32 Inicio sesión administrador	49
Figura 33 Menú administrador	50
Figura 34 Crear usuario certificador	50
Figura 35 Creación usuario certificador	51
Figura 36 Agregar organización/institución.....	51
Figura 37 Organizaciones/Instituciones.....	52
Figura 38 Inicio sesión certificador	53
Figura 39 Pantalla de emitir certificado.....	53
Figura 40 Datos llenados.....	54
Figura 41 Emisión	54
Figura 42 Certificado recibido.....	55
Figura 43 Certificado guardado	56
Figura 44 Pantalla Verificador certificados.....	57
Figura 45 Tabla de todos los certificados emitidos	58
Figura 46 Pantalla Verificador	59
Figura 47 QR de verificación	59
Figura 48 Verificación.....	60

CAPÍTULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA

1.1. JUSTIFICACIÓN

Conforme el paso del tiempo y la evolución de la tecnología nuevos conceptos, términos y tecnologías se han venido desarrollando. En conjunto para satisfacer a los usuarios ante la falta de transparencia, confianza e integridad en la información. Nuevas tecnologías como la web 3.0, Blockchain, NFTs, Contratos Inteligentes, Metaverso, entre otros. Siendo el Blockchain un término relativamente nuevo, existe una lejanía y desconocimiento de las personas, organizaciones y entidades a este concepto.

El desarrollo y uso de apps dentro del Blockchain (Apps descentralizadas) aumentaría el nivel de confianza a los datos, ya que estos son inalterables por la definición y eje central del Blockchain; además de automatizar y agilizar procesos (Bartolomé Pina et al., 2017). Para nuestro caso en la educación, debido a que el proceso de emisión y entrega de certificados y diplomas en instituciones de la educación conlleva a un proceso largo. Perdiendo tiempo que se podría estar empleando para realizar actividades mucho más productivas.

Ante esta situación y con lo ya mencionado anteriormente, la información dentro de esta cadena permite almacenar y mantener un registro de toda la información. Por ende, puede verificar la veracidad y autenticidad de los datos (certificaciones digitales seguras). Transparencia, se pueden realizar transacciones con el conocimiento de que cada parte puede participar en esa transacción, descentralizada (es decir sin alguna entidad centralizada que se encargue de las transacciones ni

del mantenimiento de registros) y sin mediadores; los usuarios transaccionan directamente entre ellos mismos sin nadie más agilizando las transacciones (Bartolomé & Lindín, 2018).

1.2. Planteamiento del problema

Actualmente en nuestra sociedad es normal que las empresas soliciten información como un *Curriculum Vitae* (CV) también conocido como “Hoja de Vida” hecho por la misma persona. Como resultado, dichos documentos no siempre brindan garantías en cuanto a la veracidad de lo que se afirma en ellos. Al adjuntarlos con sus respectivos certificados, es tedioso y complicado de verificar.

Los certificados académicos formales (como títulos de pregrado, posgrado o los de doctorado) no son suficientes para demostrar la capacidad y el conocimiento del tema para obtenerlos, y se debe adjuntar información adicional; como el caso del “Suplemento europeo al título” proporcionando una explicación del verdadero valor y concepto de dichos títulos. En general, una entidad centralizada estaba para confirmar una credencial.

También, errores cometidos, voluntarios o no, es común encontrárselos. Siendo adecuado preguntarse las mismas preguntas que hicieron Bartolomé y Lindín (2018): *“¿Es posible un sistema de acreditación que dé fe de las competencias poseídas, garantizando que no han sido falseadas, y que al mismo tiempo preserve la privacidad de la información fuera de los momentos en que el ciudadano acepta proporcionarla a un posible empleador?”*

El uso de Blockchain permitiría acreditar los elementos de un CV elaborado por el usuario, logrando que se impida la modificación de los datos, disperso en un sistema descentralizado.

1.3. Objetivo General

Analizar y desarrollar una aplicación descentralizada dentro de una red Blockchain que permita garantizar la veracidad de certificados y diplomas estudiantiles emitidos por una entidad educativa.

1.4. Objetivos Específicos

- Hacer uso de la metodología espiral para el desarrollo de la aplicación.
- Emplear un protocolo Blockchain con costos bajos.
- Realizar pruebas de funcionamiento y usabilidad del sistema.

1.5. Antecedentes

En el presente proyecto de análisis y desarrollo de una aplicación descentralizada para los certificados y diplomas estudiantiles, se inspirará y basará en revisiones bibliografías y aportes que se hayan realizado previamente por otros autores en concordancia con el tema; Blockchain para los certificados y diplomas en la educación.

Con el paso del tiempo la tecnología del Blockchain (o en español cadenas de bloques) avanzan a otras áreas. Una de estas áreas es la Educación, aunque por el momento se encuentra tímidamente, encontrándonos con aplicaciones todavía de un carácter piloto (Bartolomé Pina et al., 2017).

Pero su crecimiento ha provocado que las expectativas hagan que nos planteemos ¿Qué significa eso? ¿Cuál es su uso? ¿Cómo usarla para la educación? y ¿Cuáles peligros y posibilidades hay en esta tecnología?

La credibilidad de Blockchain con las criptomonedas resultó en una integración de esta en varios sistemas de diferentes organizaciones financieras: como la de Visa con sus tarjetas de crédito. Así, se aprecia la incursión de esta tecnología a diferentes sectores.

Como en el área de salud en donde la disponibilidad y confianza hacen atractivo guardar los registros de pacientes de un hospital. Otros casos son como el caso de afirmar la identidad de una persona, y más aplicable para personas vulnerables, como refugiados, o la creación de divisas sociales para algún grupo (Bartolomé & Lindín, 2018).

Es así como no debe extrañar que se llegue al campo educativo. La Educación en el siglo XXI se enfrenta a nuevos retos que van más allá de lo relacionado a la enseñanza-aprendizaje. Blockchain aparece para poder o tratar de solucionar dos problemáticas: restricciones en la acreditación y problemas que genera la organización en grados y niveles.

1.6. Alcance

El trabajo de desarrollo presente tiene como alcance **analizar y desarrollar una aplicación descentralizada para garantizar la veracidad de certificados y diplomas estudiantiles.**

Limitándose al país donde se realiza el trabajo, Ecuador; ya que se han encontrado documentos realizados sobre el tema en diferentes países del mundo (como los que se hablan más adelante). Y aplicando para los certificados y diplomas de cursos que realice la institución y no requiera la intervención de terceros para la emisión de los mismo; en otras palabras, para certificados y diplomas que no requieran la intervención del Senescyt u otros organismos e instituciones.

Ecuador aun no cuenta con la suficiente información ni proyectos sobre el tema. Por la naturaleza del proyecto permitiría a cualquier entidad educativa emplearla en sus procesos.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. Marco Teórico

2.1. BLOCKCHAIN

2.1.1. DEFINICIÓN

Básicamente el termino Blockchain es un concepto vinculado a la tecnología que ofrece la posibilidad de contar con registros de transacciones digitales en una red descentralizada. En 2009

ocurrió la primera aplicación de esta tecnología con Bitcoin (una moneda digital); actualmente Blockchain se encuentra en muchos otros proyectos y protocolos (Gómez Ortega et al., 2019).

Sus características permitieron crear una moneda digital distribuida, sin un control por parte de alguna institución (como un banco tradicional) o empresa (Gómez Ortega et al., 2019).

Esta tecnología puede asimilarse a un libro de contabilidad ubicado en diferentes nodos o lugares (participantes) que continuamente mantienen y realizan réplicas de la información. Cuenta con las siguientes características (Gómez Ortega et al., 2019):

- Compartido, varias personas tienen la misma información.
- Abierto, es decir que todos pueden acceder a la información, crear una cuenta y con ella hacer transacciones.
- Transparente, todos pueden acceder al contenido.
- Colaborativo, cualquiera puede proponer una nueva página (o bloque) del mismo.
- Inmutable, toda información en la cadena no puede borrarse.
- Verificable, todos pueden verificar que se respetan las normas (un ejemplo es no poder gastar dinero si uno no dispone).
- Seguro, por su característica de inmutable resulta altamente costosa editar cualquier registro.

Con el tiempo, Blockchain fue evolucionando su diseño, avanzando más que solo ofrecer monedas descentralizadas y con nuevas tecnologías, hasta permitir crear aplicaciones de otra índole. Lo que ha permitido la existencia y desarrollo de proyectos en áreas muy diversas como en las redes sociales, entretenimiento, la Academia, entre otros más (Gómez Ortega et al., 2019).

En casos reales, en uno de los ejemplos mencionados anteriormente de Blockchain se la emplea a modo de dar una identidad digital real y sin posibilidad de imitarla a personas vulnerables (como refugiados y a inmigrantes) que no cuentan con su documentación; si se les fue arrebatada o perdida. A la vez que la ONU emplea el protocolo de Ethereum (otra red) para mandar dinero a refugiados sirios (Bartolomé Pina et al., 2017).

Los “Smart Contracts” o contratos inteligentes son una parte fundamental para específicos programas en Blockchain (Bartolomé Pina et al., 2017). Que se escriben como un programa informático en que se ejecuta de modo automático cuando se cumplen las condiciones especificadas y consensuadas en el contrato. Haciendo que sea innecesario que intermedien terceros y no usar un documento impreso con lenguaje legal.

2.1.2. FUNCIONAMIENTO

El funcionamiento de Blockchain es el siguiente, a forma de analogía Blockchain funciona como un libro, un libro se divide por capítulos donde almacena información; en la Blockchain se divide en una cadena de bloques; que representa la manera en la que almacena la información. Estos bloques suelen guardar información de transacciones por medio de un token⁽¹⁾, que puede tener valor en algún tipo de mercado o no; las transacciones son añadidas a la cadena de forma constante (siendo el orden un factor importante). Para mantener el orden, al escribir un bloque este se encripta para crear un hash⁽²⁾ y ese hash se escribe en el bloque siguiente, así crea la cadena (Andrango Quishpi, 2022).

Con la analogía anterior se puede entender que Blockchain es una gran base de datos distribuida y no se encuentra en un sitio fijo, ni controlada por una entidad centralizada. Se encuentra distribuida

por todo el mundo en diferentes nodos o servidores, cada uno posee una copia de la base de datos y participan dentro de la red. Al ser distribuida, la información es compartida con todos los usuarios de la red.

La transacción es el movimiento de un activo y el bloque elige la información que registra. Hay una conexión entre los bloques y sus antecesores y posteriores, creando la famosa cadena, como se mencionó anteriormente. Con cada bloque adicional, permite reforzar la verificación del anterior y elimina la posibilidad de ser manipulado, dotando a esta tecnología la característica de ser inmutable.

La estructura que emplea los bloques es de una estructura de datos en árbol, permitiendo que un alto número de datos separados se relacionen con un único valor hash, ofreciendo un método para la verificación eficiente de los datos guardados. Para la generación de los bloques es necesario un consenso distribuido en el que los nodos tengan la capacidad de generar datos válidos (Marín Pérez, 2022).

Los nodos son ordenadores con un software determinado para conectarse entre sí, regidos por las mismas reglas, creando una red con el fin de mover la información que ocurre en el sistema, con el objetivo de unir bloques. Todos los nodos operan de la misma manera, no hay jerarquía.

De esta forma, la autoridad de decisión y la validez de las transacciones se distribuyen agrupándolas en bloques. Los participantes son los que toman las decisiones y nadie puede penetrarlos. La seguridad aumenta a medida que más personas se unen a la red, porque cuantos más usuarios se conviertan en nodos, más justa será la decisión de crear bloques o no (Marín Pérez, 2022).

Para la validación de los datos se hace en base en criptografía asimétrica, cuenta con una clave pública y otra privada. Todas las transacciones emitidas se validan por medios de los nodos en el nuevo bloque minado (ordenadores de las personas que constantemente están validando transacciones), así como su correcta vinculación con el bloque anterior. Para que los nodos tengan capacidad de generar datos válidos se necesita un consenso distribuido; así si alguien intenta vulnerar la seguridad deberá poseer por lo menos la mitad de los nodos (Marín Pérez, 2022).

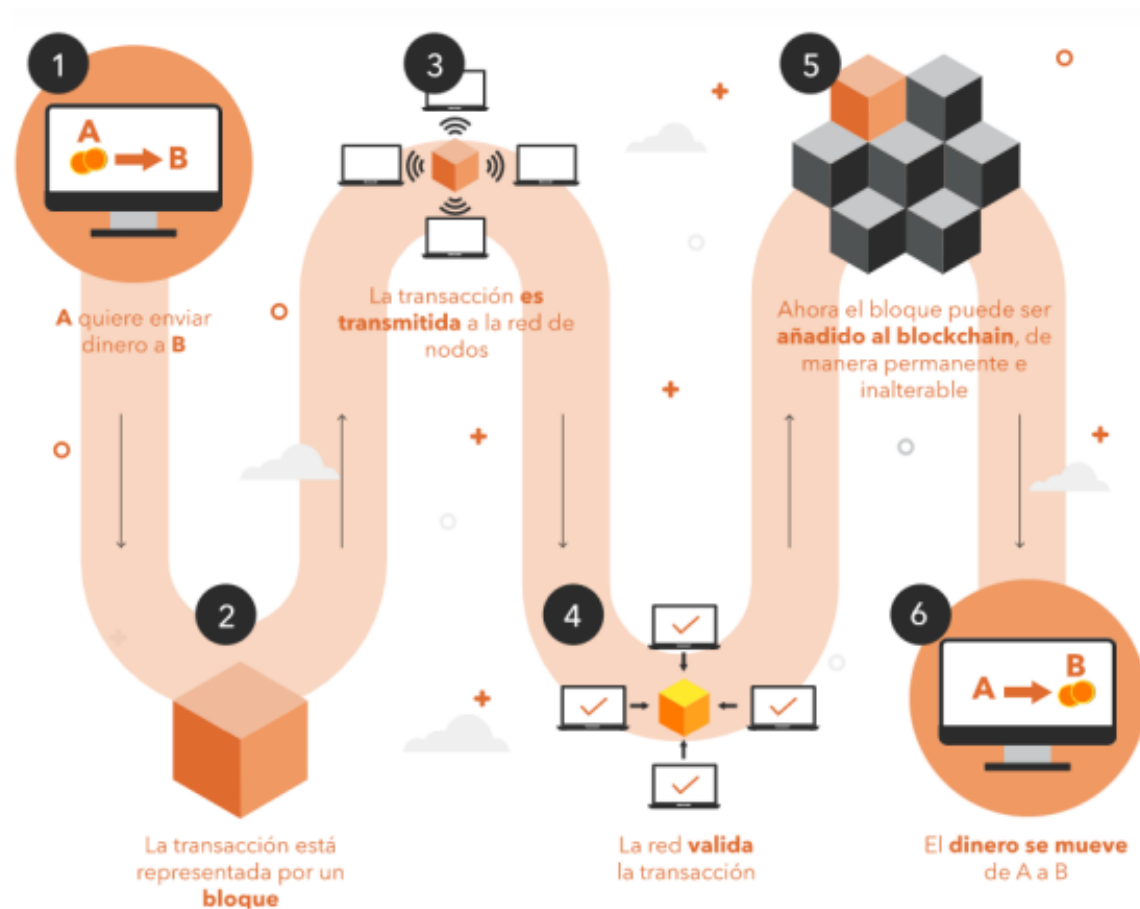


Figura 1 Funcionamiento Blockchain (Marín Pérez, 2022)

2.2. TRABAJOS PREVIOS

Mencionado anteriormente, las empresas suelen pedir información como la Hoja de Vida, que la misma persona la elabora. En dicho documento no en todos los casos se brindan garantías en cuanto a la veracidad de lo que se afirma en ellos. Puede llegar a ser tedioso y complicado de verificar. Los certificados académicos formales no son suficientes para demostrar la capacidad y el conocimiento de la persona; siendo así tener que adjuntar información adicional para poder interpretar correctamente el significado de esos documentos.

Entre algunas aplicaciones que tratan de solucionar los problemas en la educación con esta tecnología está la aplicación de Blockchain en la Universidad de Nicosia, al acreditar o emitir algunos títulos por su facultad de Economía (Koulaidis, 2018).

El MIT con el Media Lab, su aplicación que emplea Blockchain para la autenticidad de las credenciales que ellos emiten a los miembros participantes de su programa de becas Director's Fellows program. "Quizás, la primera aplicación de Blockchain fue la ya citada: la Universidad de Nicosia decidió utilizar esta tecnología para asegurar la validez de los certificados que emitía en algunos programas formativos" (Bartolomé & Lindín, 2018).

Ambos casos tratan de solucionar los problemas en la educación, emplean Blockchain para la veracidad de los certificados y diplomas estudiantiles, mediante los "hash" de la red de Bitcoin. Sin embargo, hay diferencias: el MIT está desarrollando una segunda versión enfocado a las instituciones; ya que su primera versión era privada (solo para sus participantes de su programa e investigadores). Mientras que el otro caso, la Universidad de Nicosia ya tenía su enfoque hacia los diplomas de sus estudiantes, aunque solo aplicada a su facultad de economía. Todavía se puede apreciar la resistencia al Blockchain, sin embargo, van poniendo las bases para los productos verificables; concepto que otras y nuevas empresas y plataformas utilizarían para ofrecer

infraestructura para desarrollar estos productos verificables (como el empleado en esta aplicación, Trinsic).

2.3. SITUACIÓN ACTUAL DEL PROCESO DE ACREDITACIÓN DE CERTIFICADOS Y DIPLOMAS

Recordando el alcance del presente trabajo, limitándose al país donde se realiza el trabajo y aplicando solo para certificados y diplomas de cursos que realice una institución y no requiera la intervención de terceros para la emisión de los mismo.

Por ende, existen varios requerimientos establecidos para que un alumno pueda conseguir su certificado; pero dichas políticas van a variar en cada institución y pueden ser únicas en como las manejan. Sin embargo, hay elementos esenciales que no van a variar para la acreditación de certificados y diplomas. Estos elementos son:

- **Inscripción:** La persona, estudiante o alumno debe dar a la institución su información personal para su perfil dentro de la institución; siendo esta información sus nombres completos, cédula de identidad, email, número de celular; esta información será tratada bajo la consigna de la política de privacidad, términos y condiciones.
- **Evaluación:** Como serán evaluados las materias es cuestión de como lo haya establecido la institución.
- **Emisión de certificado digital:** Similar al anterior elemento, está a la disposición de la institución.
- **Validez del certificado:** Similar a los elementos anteriores cada institución mantiene un registro de los cursos que hayan impartido junto a los diplomas o certificados emitidos

únicos o de diferentes formas para dar validez. No se encuentran avalados por el ministerio de Educación.

2.4. VISUAL STUDIO

2.4.1. DEFINICIÓN

Se trata de un IDE (Integrated Development Environment, por sus siglas en inglés) que se traduce a un entorno para la edición de código fuente moderno desarrollado y distribuido por Microsoft. Con el fin de construir y depurar aplicaciones con múltiples lenguajes de programación, contando con interpretado y autocompletado de sentencias inteligente; ayudando a un desarrollo ágil. Se encuentra disponible tanto para Windows, macOS y Linux (Mendoza Castillo, 2020).

2.5. HTML5

Es la evolución del estándar de HTML (HyperText Markup Language), es un lenguaje y estándar usado para definir la estructura y el contenido de una página Web. Mediante el uso de este lenguaje los desarrolladores pueden tener documentos en internet con estructura (sea encabezados, textos, artículos, secciones, entre otros). Extraer información en internet con links de hipertexto, que adjuntaría hojas de cálculo, videos, sonidos, imágenes (Nixon, 2020) entre otras funcionalidades (W3, 2016).

2.6. CSS

Es el otro componente básico para el desarrollo de una página web, siendo el lenguaje que define la presentación de las páginas web, en la que incluye el color y diseño de los componentes. Además, con este componente se puede mantener una buena presentación de la página web a los diferentes dispositivos que existen, a pantallas grandes o pequeñas (W3, 2016).

2.7. JAVASCRIPT

Es un lenguaje de programación, siendo un componente básico para el desarrollo de páginas web. También llamado lenguaje de script (secuencia de comandos), aunque igualmente es empleado en otros entornos sin navegador, siendo node.js y Adobe Acrobat ejemplos. Dicho lenguaje script es “multiparadigma, con un enfoque en prototipos, dinámico y soportando estilos de programación funcional y orientado a objetos” (Mendoza Castillo, 2020).

2.8. TRINSIC

Es una plataforma e infraestructura que provee un conjunto de herramientas y servicios para el desarrollo de productos de identidad. Emplea Identificadores descentralizados (DID) y Credenciales verificables (VCs), un nuevo estándar de identidad digital, en conjunto con el proyecto de código abierto Hyperledger Aries (infraestructura para interacciones peer-to-peer basadas en blockchain) (Trinsic, 2021).

2.9. D-APP

Por sus siglas, “Decentralized Applications” o en español Aplicaciones descentralizadas; son aplicaciones no gestionadas por empresas y en donde los usuarios se relacionan sin la intervención de intermediarios entre ellos, por lo general por blockchain (Sáez Hurtado, 2022).

2.10. Google Firebase

Firebase se la encuentra como plataforma de desarrollo de apps, integrando diferentes herramientas y servicios como monitoreo, autenticación, hosting, bases de datos entre otros. Creada por Google, su función, como se mencionó, es desarrollar apps, pero enfocado a que sea lo más fácil de hacer y de alta calidad de una forma rápida. Además, funciona con diferentes plataformas como iOS, Android y web (Google, s. f.).

2.11. ÁRBOLES DE NAVEGACIÓN

Los árboles de navegación o también llamados wireflows, son una representación del conjunto de wireframes (representación visual de la estructura y funcionalidades de una página web) estructurados en un flujo que indicará tanto el comportamiento como la navegación en las diferentes pantallas de la web (Siles Martínez, 2017).

2.12. DRAW.IO

Se trata de una herramienta de código abierto para creación y edición de aplicaciones de diagramación. Siendo de los softwares de diagramación para usuarios finales basado en un navegador más usadas (diagrams.net, 2021).

2.13. WEB 3.0

La web 3.0 se trata de una filosofía o pensamiento centrada en un internet descentralizado, consideración y atención de la privacidad de las personas. Para lograrlo se compone de un conjunto de tecnologías, innovaciones y protocolos unidas a esta filosofía. Impulsada por los avances en la criptografía (siendo esta la de implantar la transparencia y autenticidad) y Blockchain (siendo la que da el funcionamiento en cualquier equipo, transparencia en las transacciones y la automatización y hacer respetar los acuerdos con los contratos inteligentes) (Pallaro, 2022).

CAPÍTULO III: METODOLOGÍA

3. Metodología de desarrollo

3.1. Investigación Cualitativa

El presente trabajo inicia con el proceso de investigación cualitativa, que nos sirven para entender el significado de un fenómeno, en la que el punto de interés es la palabra. Por lo general, la

recolección de la información es en el lugar en que las personas viven el problema o situación de estudio.

Por ello, el estudio iniciará con la observación cualitativa del problema, tomar notas sobre el procedimiento de acreditación de los certificados y diplomas. A la par con el uso de materiales digitales, ejemplos de materiales de apoyo son imágenes, otros trabajos de investigación finalizados, videos, páginas web, documentos digitales emitidos por una institución.

3.2. Metodología de desarrollo de software

3.2.1. Modelo que aplica

A continuación, se procederá con el proceso de desarrollo impulsado por la metodología de desarrollo en espiral. La metodología en Espiral es el resultado de combinar la metodología de Cascada (Waterfall) con un modelo de iteraciones.

Contando con diferentes fases, empezando con la fase de conceptualización, pasando por una de evaluación, siguiendo el desarrollo y por último la fase dedicada en recolectar información del desarrollo para planear, si es el caso, la nueva espiral (empezar otra vez cada fase). A continuación, se enlista las fases:

- Análisis
- Evaluación
- Desarrollo
- Planteamiento

Incorpora una etapa fase de conexión entre las diferentes partes de la metodología, con el fin de simplificar el paso entre las fases. Nos ofrece la ventaja de que cuenta con flexibilidad o resistencia a las modificaciones que podamos realizar para la etapa posterior. El estimar costos se simplifica

y facilita, debido a que el prototipo se construye en partes pequeñas. De forma continua se desarrolla el proyecto lo que contribuye a una mejor gestión de riesgos y, además, desarrollar el proyecto se vuelve más ágil y nuevas características pueden añadirse de manera organizada.

3.2.2 FASES

3.2.2.1 ANÁLISIS

Fase centrada en el análisis de las metas, lograr identificar los objetivos y el alcance del primer ciclo. En esta fase para alcanzar lo antes mencionado, el jefe del proyecto deberá mantener una comunicación fluida con el cliente; es necesario definir adecuadamente los requisitos que del cliente.

A medida que se aumenta en la escala del proyecto, en esta fase puede producirse el hallazgo de nuevos requisitos que pueden añadirse al producto final. De esta fase se define documentos como un cronograma, archivos y documentos reunidos por el equipo de trabajo. Además, se irán desglosando actividades con base en el diseño del producto.

3.2.2.2 EVALUACIÓN

La fase de evaluación también puede denominarse análisis de riesgos, ya que los riesgos son un factor que se toman en cuenta en esta metodología. Dentro de dicha fase se valida el diseño del primer prototipo y se desglosan los posibles riesgos que este conllevará.

En cada iteración, se realizará un análisis y evaluación de riesgos, dependiendo del estado del prototipo y su grado de avance. Los diseños de los prototipos deberán ser validados en cada ciclo. Esta validación se ira realizando acorde a los plazos de tiempo y presupuesto entregados al cliente.

3.2.2.3 DESARROLLO

Es la fase donde se desarrolla y valida el prototipo, como fue mencionado anteriormente acorde al alcance y funciones definidas en la etapa anterior. Será fundamental actuar en el desarrollo, en base al análisis de riesgos, antes de poder pasar a la siguiente etapa con mayor seguridad. Conforme la espiral vaya transcurriendo, los requisitos del cliente se irán puliendo, lo que el desarrollo del producto se irá perfeccionando.

3.2.2.4 PLANTEAMIENTO

Con la culminación de una vuelta de a la espiral, es momento de pasar al planteamiento del nuevo ciclo, pero no sin antes evaluar lo realizado en el ciclo culminado. Se analizan en detalle si es necesario volver a considerarlos en la iteración que comenzará los riesgos detectados. Con la evaluación se podrá revisar el avance real del modelo en espiral. El cliente deberá evaluar el prototipo o avance realizado y dar su opinión, junto con los evaluadores calificados.

Del resultado y conclusiones que den estas personas se comenzará nuevamente una planificación de una segundo prototipo o requisito más avanzado. Lo que dará inicio a una nueva espiral.

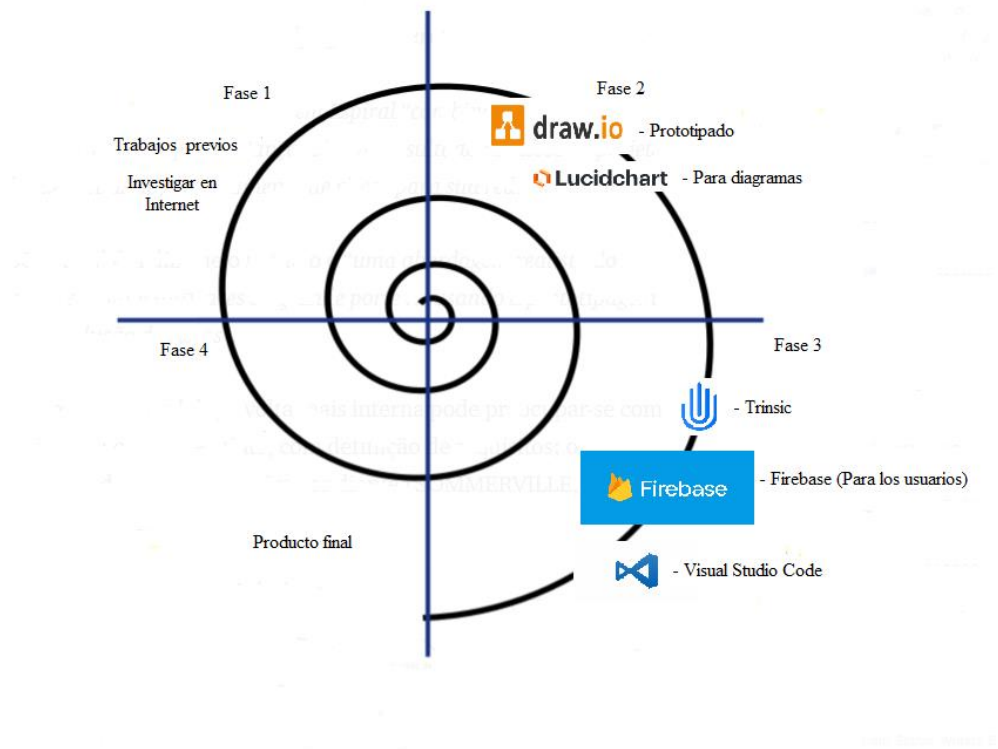


Figura 2 Diagrama metodología y herramientas usadas

4. DESARROLLO

4.1. FASE 1: ANÁLISIS

4.1.1. DESCRIPCIÓN GENERAL

4.1.1.1. PERSPECTIVA DEL PRODUCTO

La aplicación está prevista para dar veracidad a un certificado o diploma educacional emitido por una institución. Enfocándose en los certificados y diplomas que sean el resultado de cursos independientes impartidos por la institución. Permitiendo a un representante de la institución ingresar a la aplicación como un usuario y crear el certificado dentro de la aplicación, y por ende dentro de la Blockchain.

4.1.2. LEVANTAMIENTO DE REQUERIMIENTOS

4.1.2.1. REQUERIMIENTOS FUNCIONALES

La aplicación debe:

- Contar con usuarios y contraseñas, para el uso de la aplicación.
- Permitir el ingreso de datos para una cuenta, especificando:
 - Nombres completos
 - Apellidos completos
 - Correo electrónico
 - Institución
- Permitir subir el certificado emitido por la institución
- Permitir guardar el certificado
- Permitir visualizar la fecha de emisión de un certificado

4.1.2.2. REQUERIMIENTOS NO FUNCIONALES

Los requisitos no funcionales de esta aplicación son:

- **Multiplataforma:** por el tiempo de desarrollo, la aplicación solo funcionará como una aplicación web. Lo que significa que no se encontrará disponible para diferentes plataformas.
- **Seguridad:** La aplicación empleará una política de contraseñas de mínimo 8 caracteres y que se usen mayúsculas, minúsculas, caracteres especiales y números; aunque no es obligatorio que se empleen todas estas características.
- **Rendimiento:** Por la naturaleza del proyecto no se plantean cargas de trabajo grandes, por lo que no se requiere un uso fuerte de recursos; por lo que la aplicación debe funcionar fluidamente y sin muchos cortes al usarla.
- **Implementación:** La aplicación gira alrededor del análisis y desarrollo de aplicaciones empleando Blockchain y credenciales verificables. Por ende, no se contempla implementar la aplicación.

4.1.3. CLASES Y CARACTERÍSTICAS DE USUARIOS

Los principales usuarios de esta aplicación son las instituciones, por ende, una persona o representante estará a cargo de interactuar y de usar la aplicación. Estos usuarios serán quienes accedan a la aplicación, realicen los certificados y los suban a la aplicación dentro del Blockchain. En donde podrán visualizar los certificados que hayan subido a la aplicación.

4.1.4. DIAGRAMA DE CASO DE USO

La siguiente imagen presenta un diagrama de caso de uso. Dicho diagrama describe una acción o actividad del sistema o aplicación.

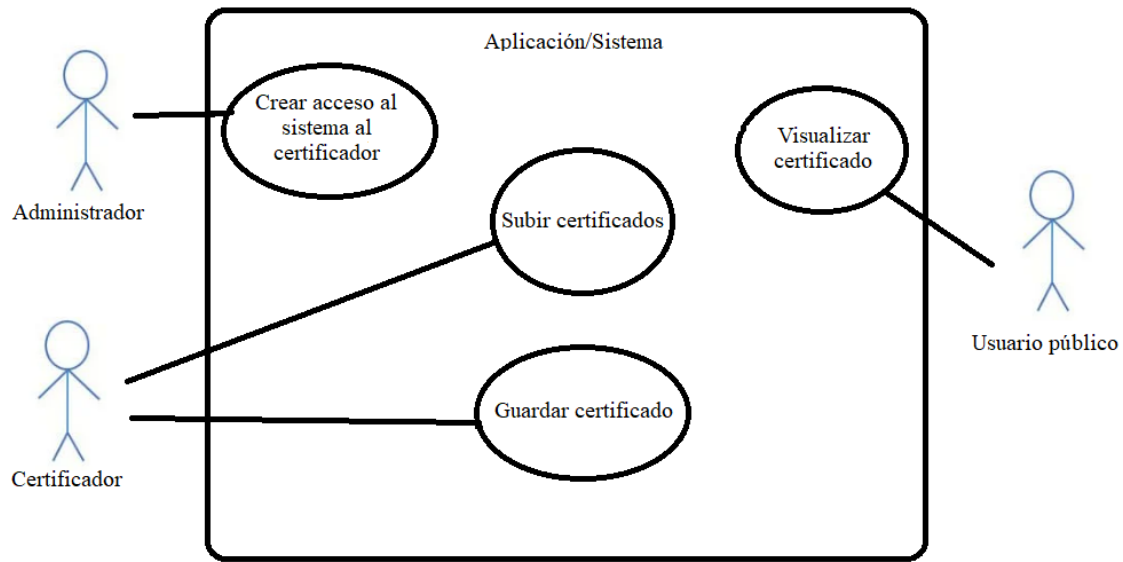


Figura 3 Diagrama de caso de uso de la aplicación

4.1.5. DIAGRAMA DE FUJO

Como existen 3 tipos de usuarios se diseñó 3 diagramas de flujo que describen los procesos del sistema para cada uno de estos usuarios.

- Administrador

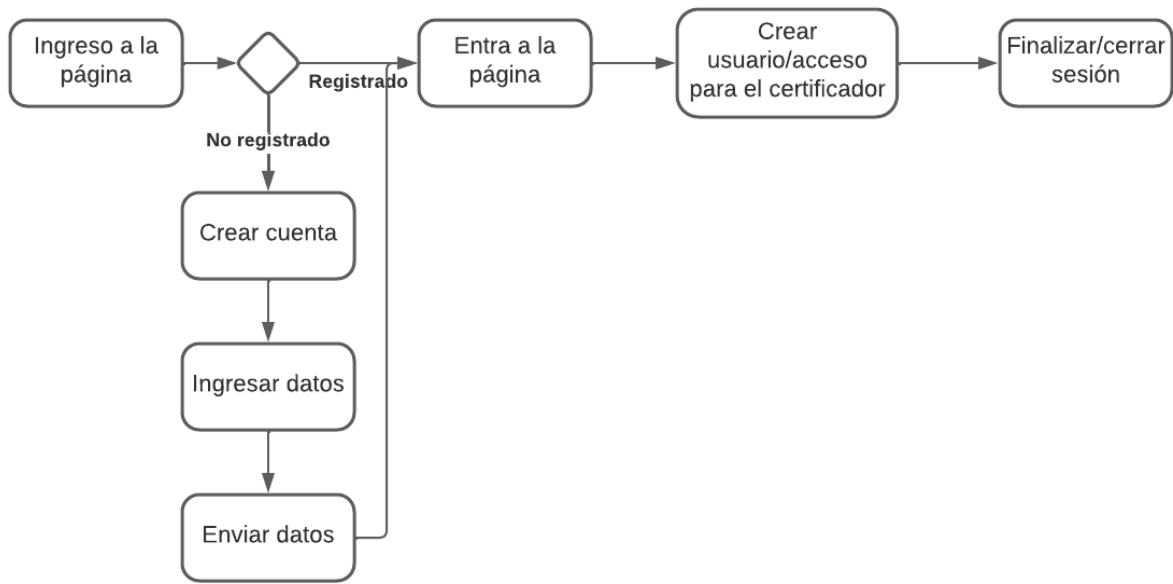


Figura 4 Diagrama de flujo para usuario Administrador

- Certificador

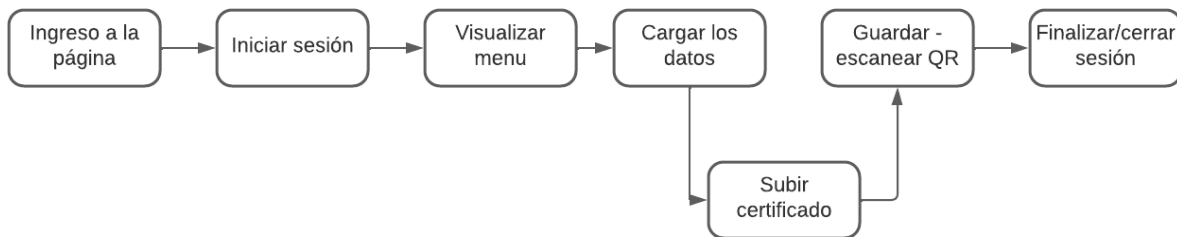


Figura 5 Diagrama de flujo para usuario Certificador

- Usuario público

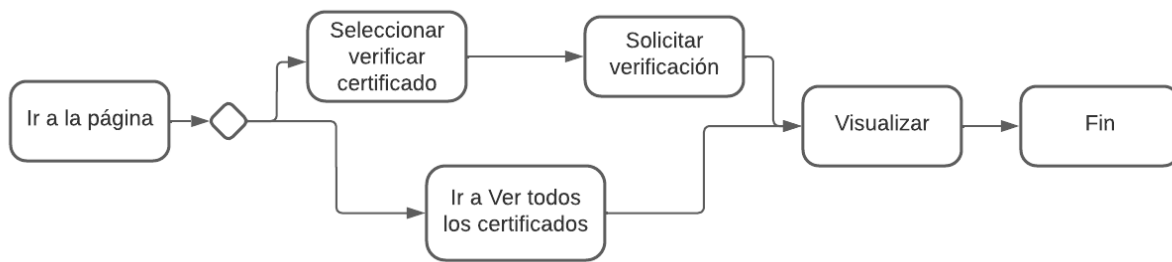


Figura 6 Diagrama de flujo para usuario Público

4.2. FASE 2: EVALUACIÓN

Para la preparación del prototipo web se empleó la herramienta de Draw.io. Presentando el primer prototipo empleando los árboles de navegación, como se muestra a continuación.

4.2.1. PROTOTIPO

La primera imagen describe lo que se conoce como “Landing page”, lo que viene siendo la página de inicio.

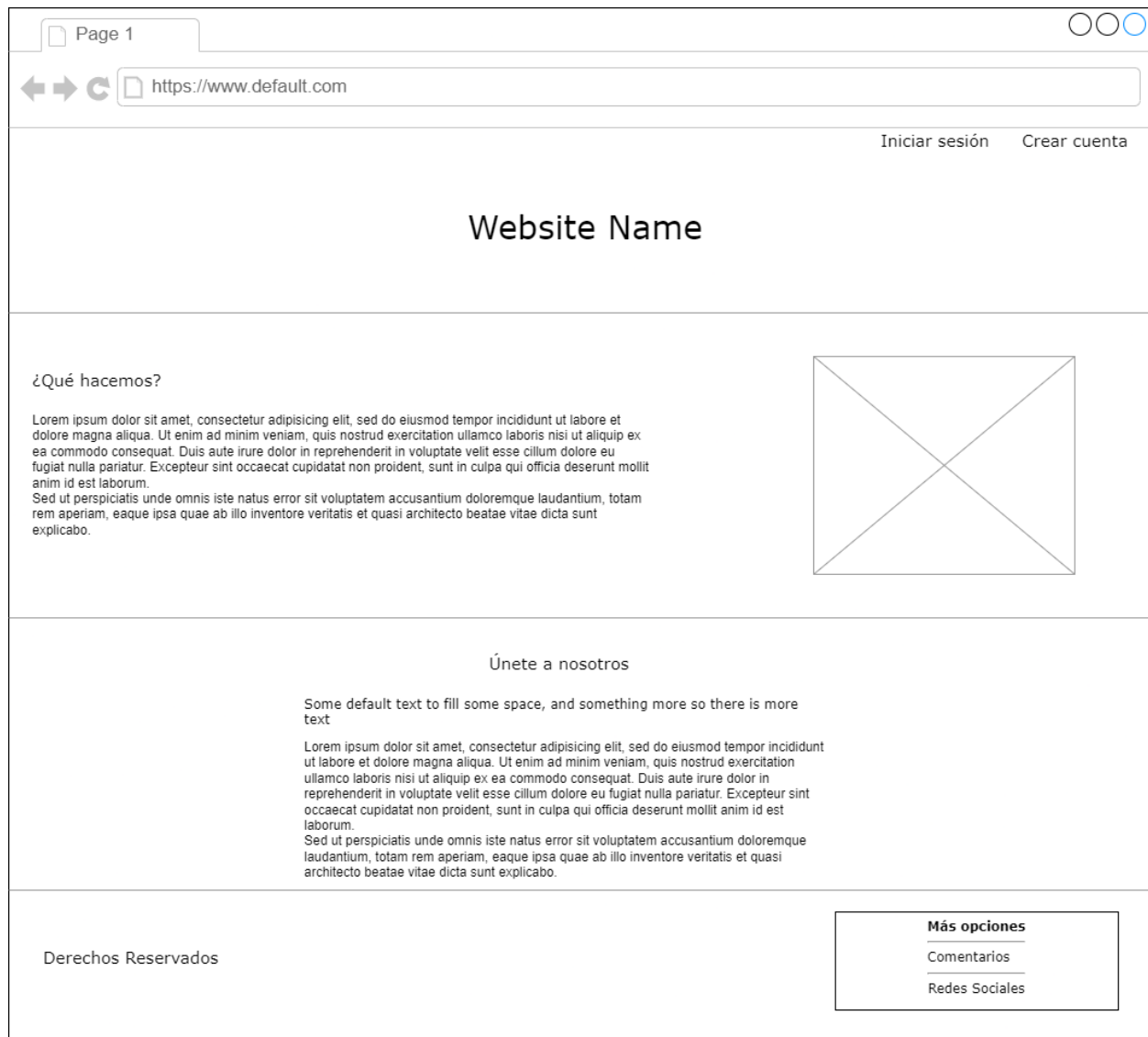


Figura 7 Landing page

La siguiente imagen es la página para iniciar sesión para los usuarios (administrador y/o certificador).

Website Name

Iniciar sesión

Nombre de usuario

john doe

Contraseña

Iniciar

[¿Olvidaste la contraseña?](#)

Regístrate

Registrarse

Figura 8 Página para iniciar sesión

La siguiente imagen describe a la página principal o Home.

Home

Ingresar nuevo certificado

Perfil

Cerrar sesión

Mis certificados

☐

Certificado1

☐

Certificado2

☐

Certificado3

☐

Certificado4

☐

Certificado5

Ingresar nuevo

Figura 9 Página home

La siguiente imagen describe a la página de ingreso de un nuevo certificado.

Home

Ingresar nuevo certificado

Perfil

Cerrar sesión

Nombre

Certificado6

Descripción

Hello %USER_FULL_NAME%!

At vero eos et accusamus et iusto odio dignissimos ducimus, qui blanditiis praesentium voluptatum deleniti atque corrupti, quosdolores et quas molestias excepturi sint, obcaecati cupiditate non provident, similique sunt in culpa, qui officia deserunt mollitiaanimi, id est laborum et dolorum fuga. Et harum quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum solutanobis est eligendi optio, cumque nihil impedit, quo minus id, quod maxime placeat, facere possimus, omnis voluptas assumendaest, omnis dolor repellendus.

Subir certificado



Guardar

Cancelar

Figura 10 Página de ingreso nuevo certificado

4.2.2. RIESGOS

Tras el desarrollo del primer prototipado, y del análisis de las herramientas a usar, se han determinado y encontrado los siguientes posibles riesgos del proyecto:

- Poca personalización entre la plataforma hosting de la página descentralizada y la página.
- Posible incompatibilidad entre la API de la plataforma de revisión de certificados en Blockchain y la plataforma hosting.
- Posible necesidad de fondos (criptomonedas guardadas en alguna cartera digital) para poner en marcha la previsualización de la página.

- Necesidad de comprar un dominio en la Blockchain para empezar a desarrollar la página.

4.3. FASE 3: DESARROLLO

Para el desarrollo contamos con las siguientes partes a realizar:

- Desarrollo de la página.
- La integración de las APIs para los certificados.

Empezando por el desarrollo de la página, tomando inspiración de los prototipos, tenemos lo siguiente. Desarrollado con la herramienta de Visual Studio Code, con los lenguajes HTML y CSS. La landing page, que es la primera pantalla que el usuario verá; en donde encontrará información sobre nosotros (lo que hace la página), que se registre y forma de seguirnos y contactarnos.

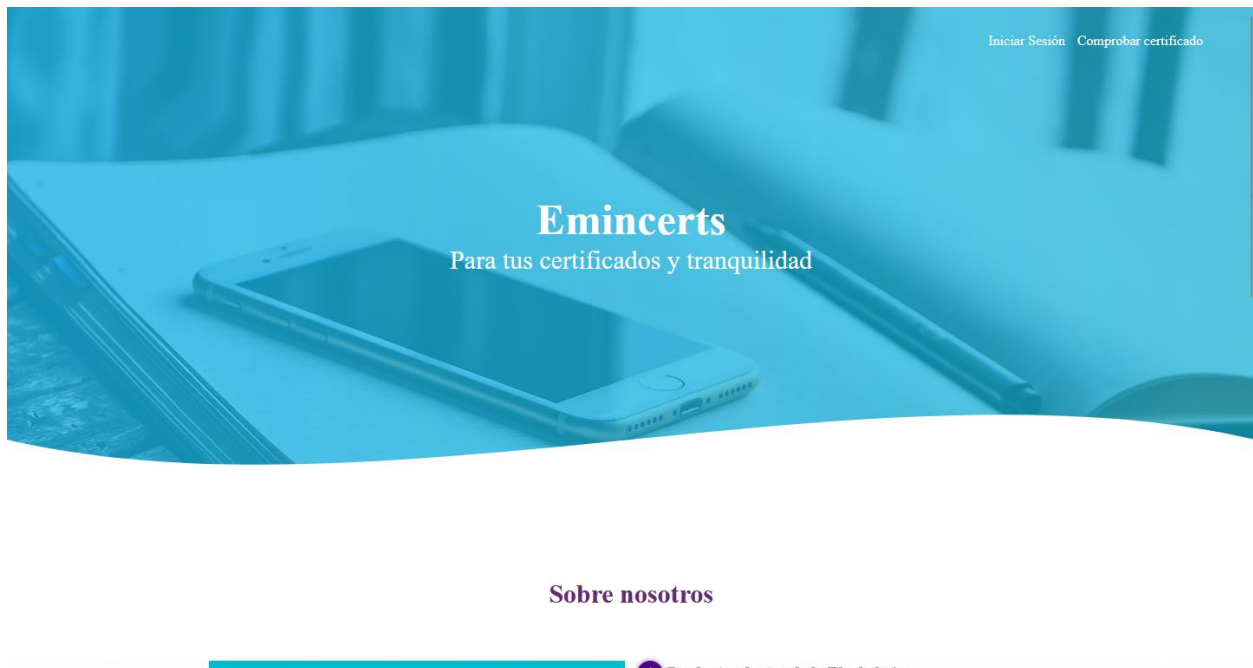


Figura 11 Landing page (1/3)

Sobre nosotros



1 Productos dentro de la Blockchain

La tecnología Blockchain ha traído nuevos conceptos y pensamientos en muchos aspectos, como la confiabilidad, inmutabilidad y veracidad. Nosotros al utilizar tecnologías basadas en Blockchain podemos ofrecer a las personas más confianza con la información dentro de nuestra aplicación.

2 Productos verificables

Nosotros sabemos la importancia de poder verificar la información, y en especial si trata sobre los certificados que nos acreditan haber pasado un curso. Por ello facilitamos subir y verificar certificados o diplomas; y verificar a quién le pertenece.

Entra a esta nueva era

Únete a nosotros

Recién estamos empezando, pero con mucho entusiasmo, energía y determinación. Contigo podemos llegar a horizontes muy lejanos.

Nota: Hay funciones limitadas y reducidas. Con tu apoyo esto cambiará a mejor.

Figura 12 Landing page (2/3)



2 Productos verificables

Nosotros sabemos la importancia de poder verificar la información, y en especial si trata sobre los certificados que nos acreditan haber pasado un curso. Por ello facilitamos subir y verificar certificados o diplomas; y verificar a quién le pertenece.

Entra a esta nueva era

Únete a nosotros

Recién estamos empezando, pero con mucho entusiasmo, energía y determinación. Contigo podemos llegar a horizontes muy lejanos.

Nota: Hay funciones limitadas y reducidas. Con tu apoyo esto cambiará a mejor.

Phone

098765432

Email

emincerts@gmail.com

Ubicación

Quito, Ecuador

© Emincerts

Figura 13 Landing page (3/3)

Seguido tenemos una pantalla de inicio de sesión para el administrador como para el certificador. En el apartado de los usuarios se emplea la plataforma Firebase de Google, ya que facilita los procesos de inicio de sesión.

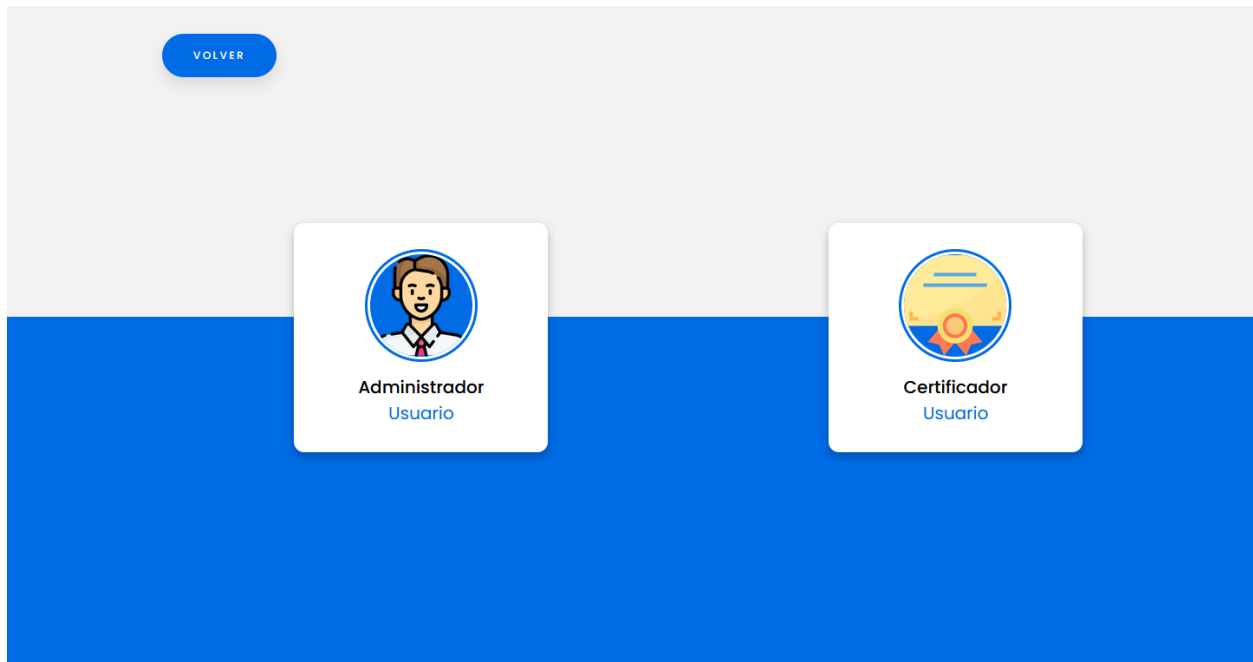


Figura 14 Menú de usuarios

Dentro del usuario administrador pasamos a la página de inicio de sesión para acceder.

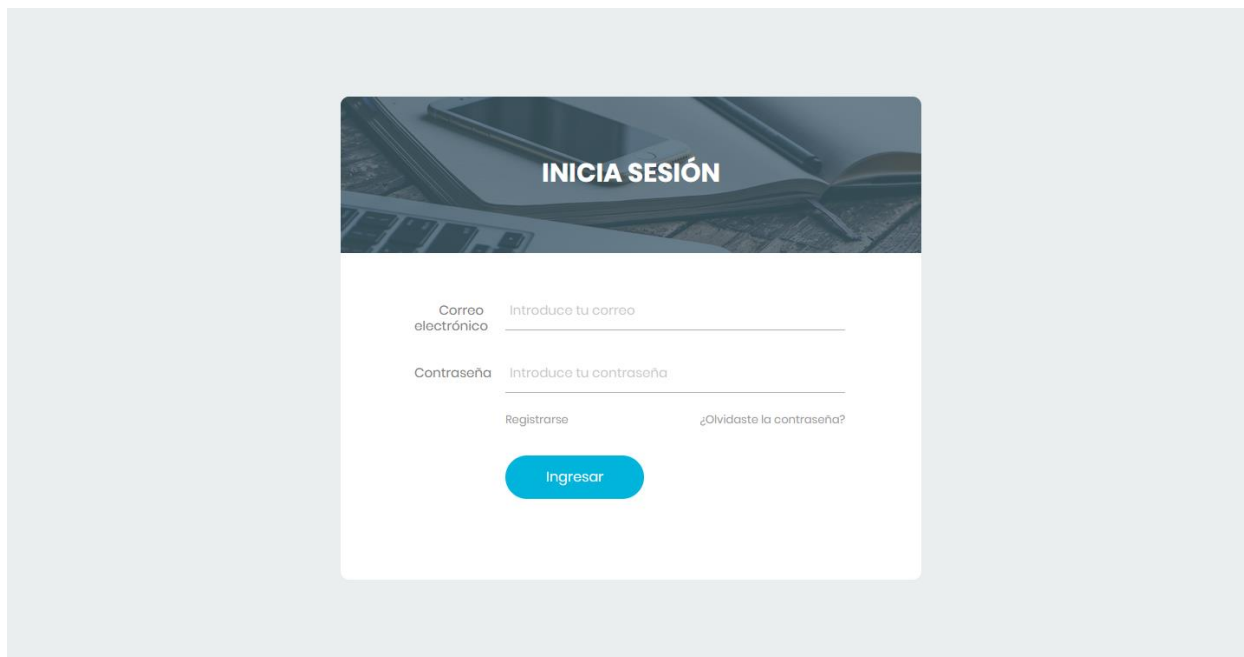


Figura 15 Login

Teniendo en cuenta que existen 3 tipos de usuarios (un Administrador, el certificador y el usuario público), el usuario Administrador es quien registra a una organización y/o la institución educativa dentro de la Blockchain Para esta sección se emplea la APIs de Trinsic, la característica de Tenant, que es por medio de esta que podemos listar, crear, obtener y eliminar las organizaciones e instituciones.

Administración Volver

Agrega una nueva organización

Nombre de la organización/institución

Elija la red sobre la que quiere funcionar

Sovrin Staging

Crear

Tus organizaciones/instituciones

Refrescar tabla

Name	Network	Access Token
------	---------	--------------

Figura 16 Pestaña Administrador

Administración Volver

Agrega una nueva organización

Nombre de la organización/institución

Elija la red sobre la que quiere funcionar

Sovrin Staging

Crear

Tus organizaciones/instituciones

Refrescar tabla

Name	Network	Access Token
 Rest Org.	Sovrin Staging Network	*****Bxws  
 Argo	Sovrin Staging Network	*****guy8  

Figura 17 Administrador-creación nueva organización

Con los dos datos que pide para ingresar (nombre de la organización y el token, o código, de acceso a la Blockchain) aparecerá a su lado derecho las organizaciones ya registradas. Debido a que en la Blockchain los datos se guardan en todos los equipos que conforman la red; no hay

como editar esta información, si se desea cambiar algo se tiene que eliminar la organización y volver a registrar (aunque dentro de la Blockchain no se va a eliminar).

Del lado del usuario certificador tenemos la pantalla para emitir los certificados.

Certificador

Cerrar sesión

Datos del certificado

Ingrese los datos solicitados para cargar el certificado.

Nombre

Ingrese el nombre completo

Fecha de emisión

29/6/2022

Identificador único para el certificado

1b0-371-4fd1-9704-77b

Nombre del curso

Ingrese el nombre de la materia o curso

Certificado

Seleccione el certificado o arrastre lo a la casilla. (solo .pdf)

Examinar...

No se ha seleccionado ningún archivo.

Emitir certificado

Figura 18 Pestaña certificador

Certificador

Cerrar sesión

Datos del certificado

Ingrese los datos solicitados para cargar el certificado.

Nombre

Mateo Fernando Ruiz Angulo

Fecha de emisión

29/6/2022

Identificador único para el certificado

a2e-ecb-48e0-a2d4-25d

Nombre del curso

Sistemas Ambientales

Certificado

Seleccione el certificado o arrastre lo a la casilla. (solo .pdf)

Examinar... Certificado_prueba.pdf

Emitir certificado

Figura 19 Emisión certificado

Certificador

Cerrar sesión

Escane el código QR y después ciérrelo



Sistemas Ambientales

Certificado

Seleccione el certificado o arrastre lo a la casilla. (solo .pdf)

Examinar... Certificado_prueba.pdf

Emitir certificado

Figura 20 Certificado subido

Con las credenciales generadas por el administrador, se las comparte al usuario certificador.

Quién es el encargado de pasar y subir los datos a la cadena. Para compartirlo y/o permitirle al dueño de ese certificado guardarlo y también compartir con empresas, el dueño del certificado debe descargar una aplicación móvil que funcionará como una billetera digital (Trinsic Wallet app, véase en el apartado de anexos, manual de usuario) para las credenciales; la app de Trinsic facilita este proceso. Se descarga y escanea el código QR para conectarse a la red.

En esta pantalla, aparte de subir los certificados, se extrae datos de la cuenta certificadora, siendo más específicos se extrae la organización del certificador y el nombre.

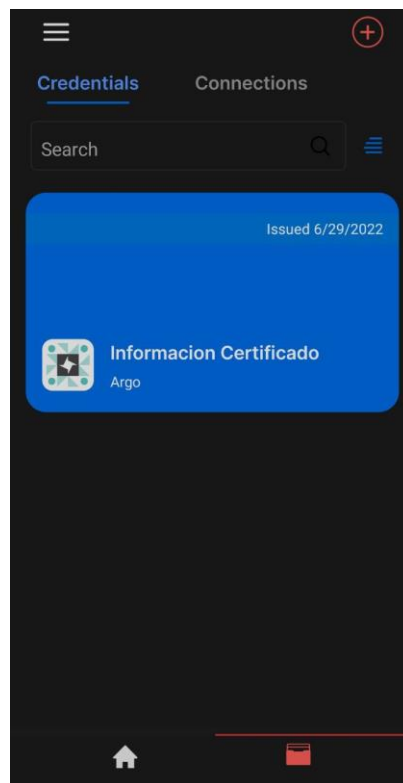


Figura 21 Wallet - certificados almacenados

Por último, tenemos al usuario público. Este puede ver los certificados emitidos en una tabla, con los datos y el código QR generado.

Verificador

Volver a la página principal

Todos los certificados

ID del certificado	Nombre	Fecha de emisión	Organización emisora	QR generado de la emisión	Visualizar QR generado
dd2-582-41d2-bdfb-952	Fransico Tapia	28/6/2022	ONU	https://chart.googleapis.com/chart?cht=qr&chl=https://trinsic.studio/url/107bb670-98e2-48b1-961f-1c9b36e85993&chs=300x300&chld=L 1	Abrir
3cc-19c-49d0-b027-380	Pepito Pérez	28/6/2022	ONU	https://chart.googleapis.com/chart?cht=qr&chl=https://trinsic.studio/url/b930e883-34af-4113-be1f-0ffc59ef2651&chs=300x300&chld=L 1	Abrir
f8a-452-47f6-af5a-e51	Mateo Fernando Ruiz Angulo	28/6/2022	SEK	https://chart.googleapis.com/chart?cht=qr&chl=https://trinsic.studio/url/1dd37e10-1fbb-4943-a509-01c105b1a56e&chs=300x300&chld=L 1	Abrir

Figura 22 Tabla de certificados

Y también solicitar información del certificado al dueño del certificado, escaneando un QR. Después, de escanear el QR aparece a quien le pertenece y cuando fue emitido.

Ver todos los certificados		Volver a la página principal			
Verificador certificados					
					

Figura 23 Pestaña verificador público



Figura 24 Verificación



Verificador certificados

VERIFICAR

Verificación comprobada y aceptada!!!
Certificado emitido el:
29/6/2022

Este certificado pertenece a ...

Identificador único de la credencial
a2e-ecb-48e0-a2d4-25d

Nombres
Mateo Fernando Ruiz Angulo

Certificado
C:\fakepath\Certificado_prueba.pdf

Figura 25 Verificación

En el apartado de anexo se encuentra un manual de usuario de la aplicación web con información útil sobre la aplicación web.

4.4. FASE 4: PLANTEAMIENTO

Siendo el último pasó de la metodología, este apartado se puede considerar como para líneas futuras de investigación. Recapitulando este proyecto, la creación de esta aplicación web que permita verificar certificados emitidos por alguna institución empleando Blockchain. Existen varias plataformas que ofrecen la infraestructura para productos verificables, como el empleado en este trabajo, la plataforma Trinsic.

Los principales riesgos encontrados en el desarrollo fueron los siguientes, y que se recomienda considerarlos para el siguiente ciclo (si se da el caso):

- En el caso de continuar con la aplicación, se concluye favorable contactar con la o una empresa proveedora de infraestructura de productos verificables para que nos faciliten con más información de cómo utilizar sus productos. Ya que la comunidad y su documentación no siempre están completas ni actualizadas.
- Es raro, pero se dio en una ocasión, y es el tema del corte del servicio. Ya que estamos empleando los servicios de un proveedor, puede haber cortes en nuestros servicios que están fuera de nuestro control.
- Aunque la aplicación ya se encuentra utilizando Blockchain, el protocolo de Hyperledger Aries de Trinsic. Es posible (y si se quiere seguir utilizando Blockchain) desplegar una página web en una internet descentralizada; para ello se sube la página o aplicación a plataformas (como lo es Unstoppable Domains) que ofrezcan dominios en alguna Blockchain. Seguir este camino resulta interesante, pero también más costoso el despliegue que el de una página web tradicional dentro de la internet que usamos. En lugar de internet (el que usamos comúnmente) se planteó usar un dominio Blockchain (para un futuro caso para desplegar la aplicación), pero como se menciona resulta más

costos; ya que para desplegar la página se requiere de una billetera digital con alguna criptomoneda (Bitcoin, Ethereum, entre otros).

- Desplegar una página o aplicación web en una internet descentralizada no tiene tanto alcance, debido a que las aplicaciones de navegadores de internet no pueden conectarse a una internet descentralizada con Blockchain; sin alguna extensión o simplemente no son compatibles.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El avance tecnológico y la búsqueda de una información verificable y descentralizada ha llevado a la creación de nuevas tecnologías, pensamientos y formas de comunicación. Llegando al desarrollo de la Blockchain, que aún se encuentra en una etapa de formación y desarrollo. Sus beneficios son los que permiten poder tener aplicaciones descentralizadas y gobernadas por la comunidad; además de ser verificable e inmutable.
- En conjunto, con lo anteriormente dicho, se une la información o credenciales verificables; empleando la característica de la Blockchain de ser verificable. Las credenciales verificables, como su nombre lo describe, es permitir que las credenciales sean verificables; lo normal es que se empleen con identificadores sobre una Blockchain.
- Plataformas como Trinsic facilitan el desarrollo de aplicaciones, entornos y productos de identidad, como ellos lo mencionan en su página; refiriéndose a que facilitan a ofrecer herramientas y APIs para que la información pueda ser verificable; empleando el protocolo

Blockchain de Hyperledger Aries. De esta forma, en conjunto con su documentación, ayudaron al desarrollo de esta aplicación.

- Es considerable los beneficios que plataformas como Trinsic ofrecen, sin embargo, ofrecen servicios y APIs limitadas. Tienen versiones pagadas que ofrecen mayores características y soporte; algo que limita en las características que podemos ofrecer al desarrollar aplicaciones con estas plataformas.
- La aplicación en general, apunta a 3 diferentes tipos de usuarios: Administrador, certificador y usuario público. El administrador ayuda a crear e integrar a las organizaciones e instituciones en la red; donde todo va a trabajar. Generando un código único que sirve como motor para subir y guardar en la red los certificados. Los certificadores reciben este código único, el cual deben ingresar tal cual lo recibieron; junto al resto de los datos del certificado. Almacenados en la red se puede solicitar una verificación; para ver a quien le pertenece el certificado.

RECOMENDACIONES

- El desarrollo de esta aplicación enseñó que aún hay tiempo para tecnologías como la Blockchain, que sean acogidas por el público en general. Su comunidad, en crecimiento, aún no es lo suficientemente grande como para cubrir las preguntas y necesidades de otros desarrolladores. Por lo que algunas documentaciones se encuentran con errores, incompletas y/o desactualizadas.
- En conjunto con la anterior recomendación, la información que se puede encontrar sobre cómo crear un sistema o aplicación, para credenciales verificables, es aún reducida; y con los mismos problemas de tener errores o estar incompletas. Lo mejor es buscar ejemplos que pueden ofrecer algunos proveedores de infraestructura para productos verificables.

- Es preferible, al menos de momento, que las aplicaciones o páginas web se alojen en servidores dentro de la red que todos usamos y conocemos. Debido a que gran mayoría de buscadores de internet requieren de extensiones o simplemente no pueden conectarse a una internet descentralizada; lo que reduce significativamente el alcance a nuestro público objetivo y potenciales clientes. Además, de mencionar que se requiere un monto de criptomonedas en una billetera digital para desplegar páginas web en un dominio en Blockchain.
- Ejemplos que se pueden encontrar sobre aplicaciones parecidas pueden tener problemas con las dependencias al momento de ejecutar la aplicación. Por lo que hay que considerar tener un tiempo para encontrar una que funcione para tenerla como una referencia al momento de crear nuestra aplicación.
- Es recomendable, tratar de buscar la mayor información posible de como manipular adecuadamente los archivos de entorno (.env, con JavaScript).
- Revisar detenidamente la documentación de referencia de las APIs de Trinsic. Página de referencia de las APIs en la sección de anexos.

BIBLIOGRAFÍA

- Andrango Quishpi, J. S. (2022). *ESTADO DEL ARTE ACTUAL CON RESPECTO AL BLOCKCHAIN EN RELACIÓN CON SU CONCEPTO, ELEMENTOS, FUNCIONAMIENTO Y APLICACIONES UTILIZANDO LA METODOLOGÍA SLR Y SYSTEMATIC MAPPING*. UNIVERSIDAD POLITÉCNICA SALESIANA.
<https://dspace.ups.edu.ec/bitstream/123456789/21963/1/UPS%20-%20TTS634.pdf>
- Bartolomé, A., & Lindín, C. (2018). *Posibilidades del Blockchain en Educación*. EKS.
<https://redined.educacion.gob.es/xmlui/bitstream/handle/11162/189993/Posibilidades.pdf?sequence=1&isAllowed=y>
- Bartolomé Pina, A. R., Bellver Torlà, C., Castañeda Quintero, J. L., & Adell Segura, J. (2017). *BLOCKCHAIN EN EDUCACIÓN: INTRODUCCIÓN Y CRÍTICA AL ESTADO DE LA CUESTIÓN*.
<https://www.edutec.es/revista/index.php/edutece/article/view/915/pdf>
- BBVA. (2021, 23 diciembre). *Qué es un «token» y para qué sirve Token Digital*. Recuperado 16 de mayo de 2022, de <https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/>
- Cámara de Comercio de Bogotá. (2019, enero). *EL MUNDO CONECTADO POR LAS API*.
<https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/22728/4%20API.pdf?sequence=1&isAllowed=y>
- Donohue, B. (2014, 10 abril). *¿Qué Es Un Hash Y Cómo Funciona?* Kaspersky daily.
Recuperado 16 de mayo de 2022, de <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>
- Gómez Ortega, J., Castro Irigorri, C. A., Ariño Martín, L. A., Hernández Fernández, J. L., López García, D. R., Martínez, R., Prado Domínguez, A. J., Ruiz

- Martínez, J., Cruz Argudo, F., & Tenorio Fornés, A. (2019). *Blockchain en la Universidad*. TIC 360. https://tic.crue.org/wpcontent/uploads/2020/06/Blockchain-en-la-universidad_TIC-360_FINAL_comprimido.pdf
- Google. (s. f.). *Documentación*. Firebase. Recuperado 29 de mayo de 2022, de <https://firebase.google.com/docs?hl=es-419>
- Nixon, R. (2020). *Aprender PHP, MySQL y JavaScript* (5.^a ed.). Marcombo. https://books.google.es/books?hl=es&lr=lang_es&id=AExOEAAAQBAJ&oi=fnd&pg=PT5&dq=que+es+html,+css+y+javascript&ots=WlirWH9co&sig=hRQUOOzVRsQN0Fn4oUXRUutG2D0#v=onepage&q&f=false
- Maida, E. G., & Pacienza, J. (2015). *METODOLOGIAS DE DESARROLLO DE SOFTWARE*. <https://repositorio.uca.edu.ar/bitstream/123456789/522/1/metodologiasdesarrollo-software.pdf>
- Marín Pérez, C. (2022). *TECNOLOGÍA BLOCKCHAIN: ORIGEN, FUNCIONAMIENTO Y USOS*. Universidad Zaragoza. <https://zaguan.unizar.es/record/111139/files/TAZ-TFG-2022-362.pdf?version=1>
- MayuGo. (s. f.). *POLÍTICA DE CERTIFICACIÓN*. Recuperado 25 de abril de 2022, de <https://www.mayugo.net/certificacion>
- Mendoza Castillo, J. E. (2020). *Desarrollo de una interfaz web bajo tecnologías reactjs, javascript, html, css para la creación y configuración de flujos de procesos asistidos mediante chatbots*. Universidad Santo Tomas. <https://repository.usta.edu.co/bitstream/handle/11634/21069/2020MendozaJavier.pdf?sequence=7&isAllowed=y>

Microsoft. (s. f.). *Visual Studio*. Microsoft Visual Studio. Recuperado 15 de mayo de 2022, de <https://visualstudio.microsoft.com/es/>

Pallaro, A. (2022, enero). *Blockchain, criptomonedas, DAOs y Metaversos: ¿Arquitectura del futuro?* infobae. <https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/22183/Blockchain,%20criptomonedas,%20DAOs%20y%20Metaversos.pdf?sequence=1>

Sáez Hurtado, J. (2022, 25 febrero). *Qué son las DApps o Aplicaciones Descentralizadas y varios ejemplos*. IEBS. Recuperado 15 de mayo de 2022, de <https://www.iebschool.com/blog/dapps-o-aplicaciones-descentralizadas-que-son-y-como-funcionan-finanzas/#:~:text=Las%20DApps%20o%20aplicaciones%20descentralizadas%20son%20una%20categor%C3%ADa%20especial%20de,se%20mantenga%20segura%20y%20accesible.>

Siles Martínez, V. (2017, junio). *Aplicación móvil para la configuración de variadores*. Universitat Oberta de Catalunya. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/65086/9/vsilesTFM0617memoria.pdf>

Trinsic. (2021). *Introduction*. Recuperado 19 de abril de 2022, de <https://docs.trinsic.id/docs>

W3. (2016). *HTML & CSS*. W3.org. Recuperado 15 de mayo de 2022, de <https://www.w3.org/standards/webdesign/htmlcss>

GLOSARIO DE TÉRMINOS

Términos generados con su concepto como resultado de las palabras que el lector no conoce.

- 1) Hash: El termino hash hace referencia a un algoritmo matemático para transformar cualquier bloque arbitrario de datos en una nueva serie de caracteres de longitud fija. Sin importar la longitud de los datos de entrada, el valor de salida de un hash tendrá siempre la misma longitud (Donohue, 2014).
- 2) Token: se refiere a una unidad de valor digital basada en criptografía y emitida por una entidad privada dentro de una Blockchain (BBVA, 2021).
- 3) APIs: Por sus siglas en inglés, Interfaz de programación de aplicaciones, es un conjunto de definiciones y protocolos que permiten que otro software o programa pueda reconocerlos y ejecutarlos. Básicamente es una herramienta que permite que un programa pueda comunicarse o interactuar con otro (Cámara de Comercio de Bogotá, 2019).

ANEXOS

Anexo A: Manual de usuario

Antes que nada, a modo de introducción, la aplicación web desarrollada emplea la infraestructura y ecosistema de Trinsic (link de página web <https://trinsic.id/>); que ya fue explicada anteriormente. Cabe mencionar que hay un requisito para el uso de la aplicación (al menos para las organizaciones y a las personas que les pertenece el certificado) y es que se necesita descargar de la tienda de aplicaciones (sea en Google Play Store o en la App store de Apple) la billetera digital de Trinsic (nombre de la app: Trinsic Wallet). Ya que es por medio de esta billetera que podrá gestionar y guardar la persona que recibe los certificados.

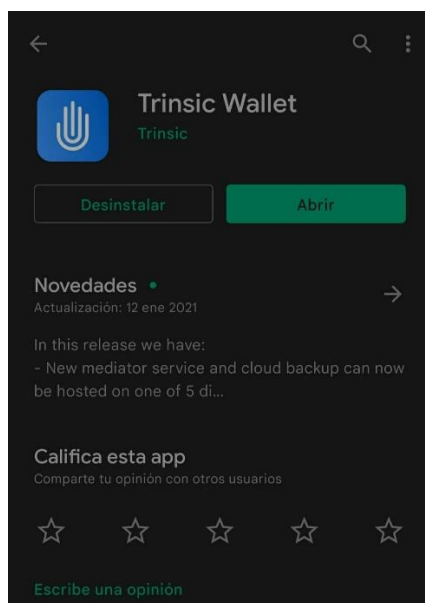


Figura 26 Trinsic Wallet app

Se descarga la app y simplemente sigue las instrucciones de la misma aplicación para configurarla. Esta aplicación y las organizaciones e instituciones están trabajando sobre la red Sorvin Staging,

por lo que su billetera digital también debe estar en esta misma red. Para cambiar o asegurarse de estar en esta red entre al menú (botón de las tres líneas en la parte superior izquierda).

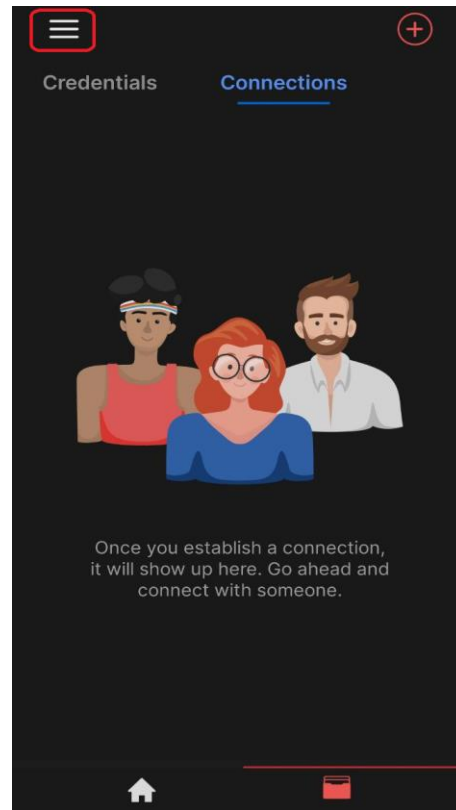


Figura 27 Trinsic Wallet app

Dentro seleccione Network o Red.

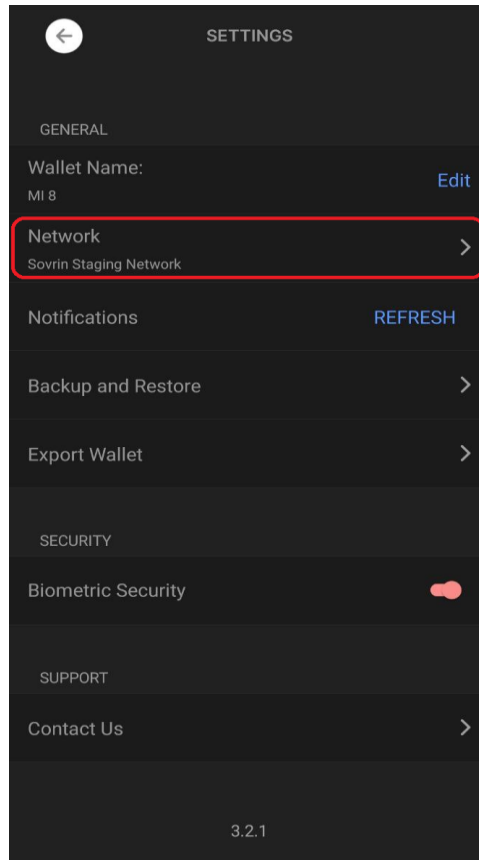


Figura 28 Ajustes

Y por último seleccione Sorvin Staging si no lo está.

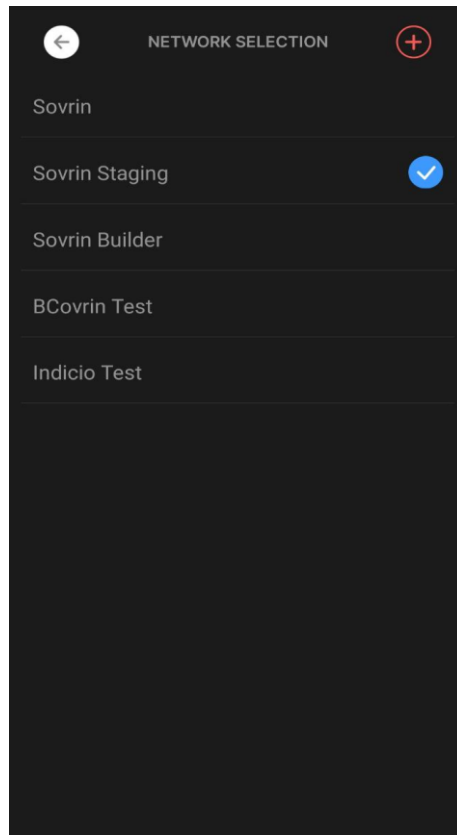


Figura 29 Red

La aplicación web cuenta con 3 tipos de usuarios, el administrador, quien se encarga de crear el acceso y cuenta a las organizaciones e instituciones, el certificador, quien se encarga de ingresar los datos del certificado y guardarlos en la Blockchain y; por último, el usuario público que puede ser cualquier persona que quiera verificar y ver los certificados emitidos. Teniendo claro esto, pasamos a la aplicación web. La siguiente imagen presenta la página principal de la aplicación.

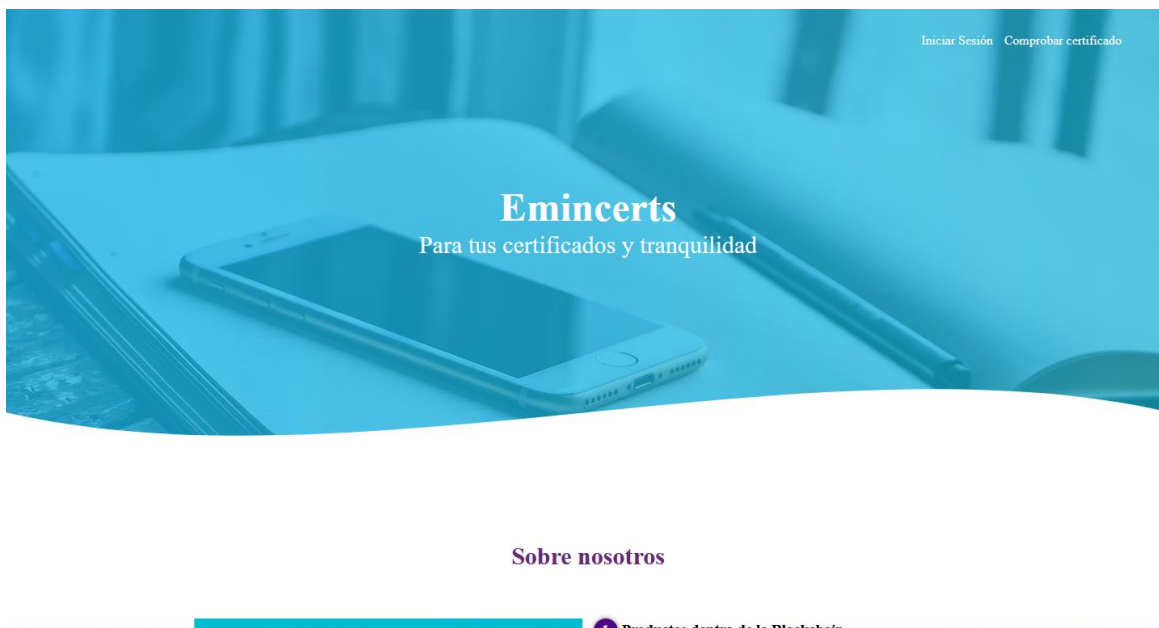


Figura 30 Página principal

Ingresamos en el botón de Iniciar sesión, en esta pantalla el usuario debe elegir con que rol va a ingresar, como Administrador o como Certificador. Primero ingresamos como Administrador, si no tiene una cuenta da click sobre el botón de registrarse; caso contrario ingrese los datos solicitados para iniciar sesión.

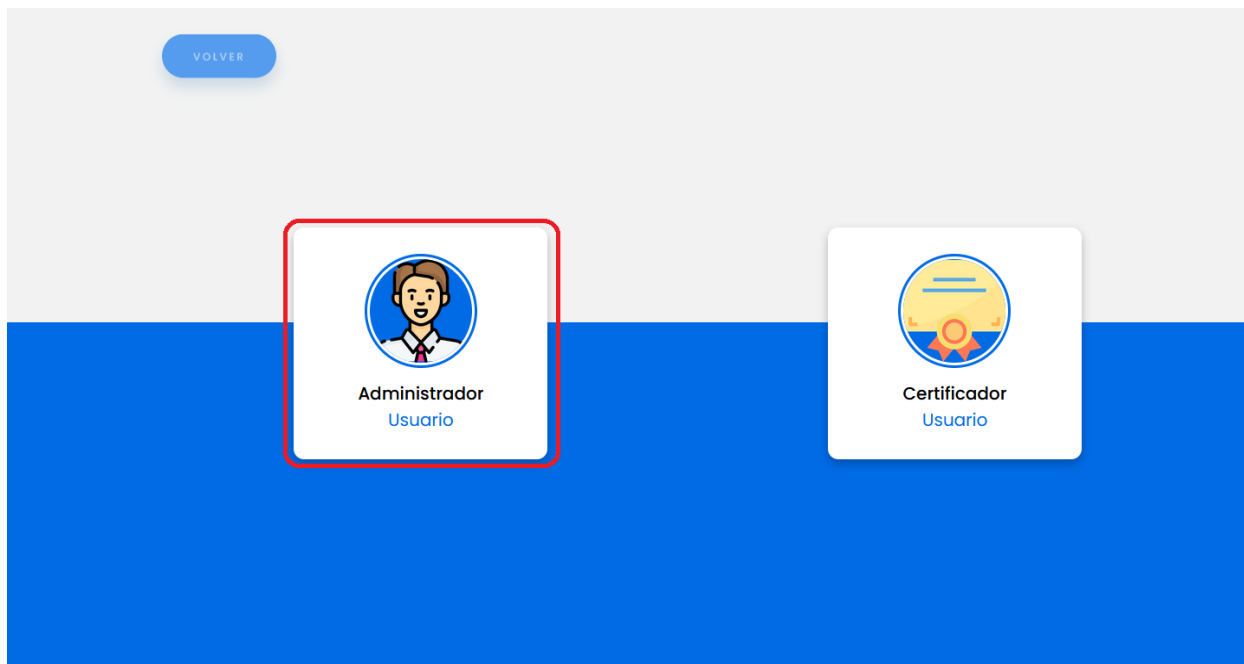


Figura 31 Selección usuario

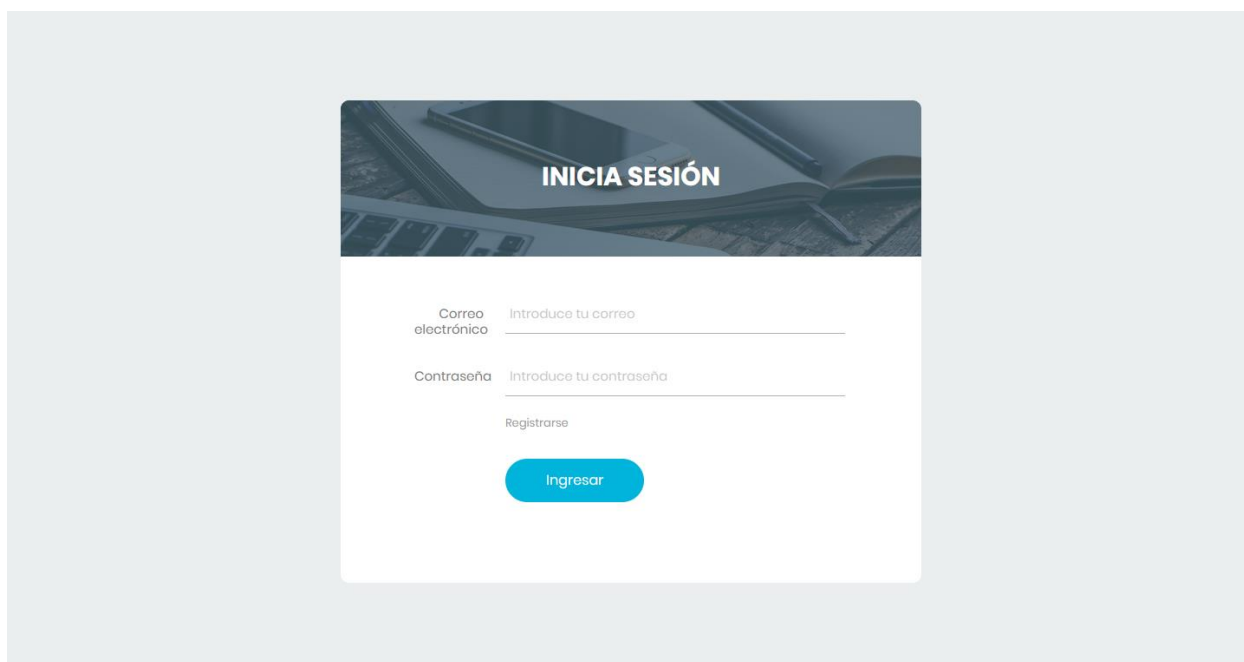


Figura 32 Inicio sesión administrador

Se presentan las dos funciones que puede hacer el administrador: crear un usuario certificador o agregar una empresa o institución a la red.

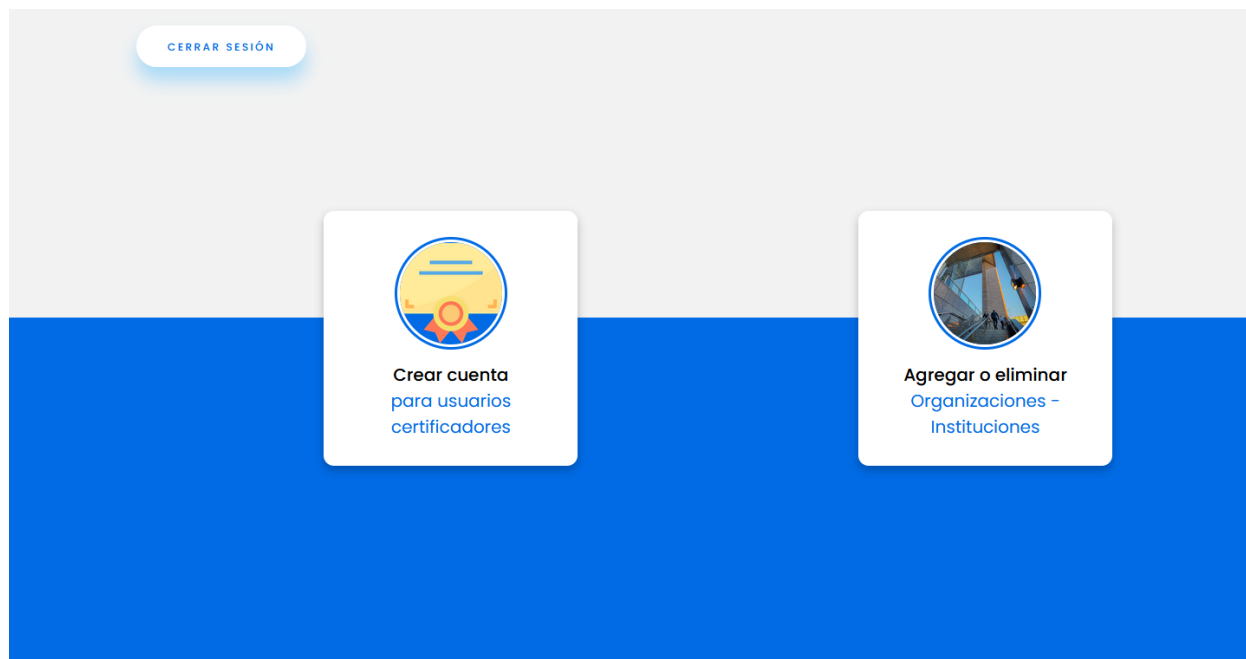


Figura 33 Menú administrador

Crear un usuario certificador:

The image shows a form for creating a certifying user. The form is titled 'CREACIÓN DE USUARIO CERTIFICADOR' in white text on a dark blue background. Below the title, there are four input fields with labels and placeholder text: 'Organización o Institución' (placeholder: 'Introduce el nombre de la Organización o Institución'), 'Nombres completos' (placeholder: 'Introduce los dos nombres y los dos apellidos'), 'Correo electrónico' (placeholder: 'Introduce tu correo'), and 'Contraseña' (placeholder: 'Introduce tu contraseña'). Below the fields, there is a 'Cancelar' link and a blue button labeled 'CREAR USUARIO'.

Figura 34 Crear usuario certificador

CREACIÓN DE USUARIO CERTIFICADOR

Organización: Vikoqanu

Institución: _____

Nombres completos: Manuel Angel Maza

Correo electrónico: manuangelito3@gmail.com

Contraseña: ••••••••

[Cancelar](#)

[CREAR USUARIO](#)

Figura 35 Creación usuario certificador

Agregar una empresa o institución a la red (**los nombres de las empresas/instituciones sirven a modo de ejemplo**):

Administración [Volver](#)

Agrega una nueva organización

Nombre de la organización/institución

Organización/instituc

Elija la red sobre la que quiere funcionar

Sovrín Staging

[Crear](#)

Tus organizaciones/instituciones [Refrescar tabla](#)

Name	Network	Access Token
------	---------	--------------

Figura 36 Agregar organización/institución

Administración

Volver

Agrega una nueva organización

Nombre de la organización/institución

Argo

Elija la red sobre la que quiere funcionar

Sovrin Staging

Crear

Tus organizaciones/instituciones

Refrescar tabla

	Name	Network	Access Token		
	Rest Org.	Sovrin Staging Network	*****Bxws		
	Argo	Sovrin Staging Network	*****guy8		

Figura 37 Organizaciones/Instituciones

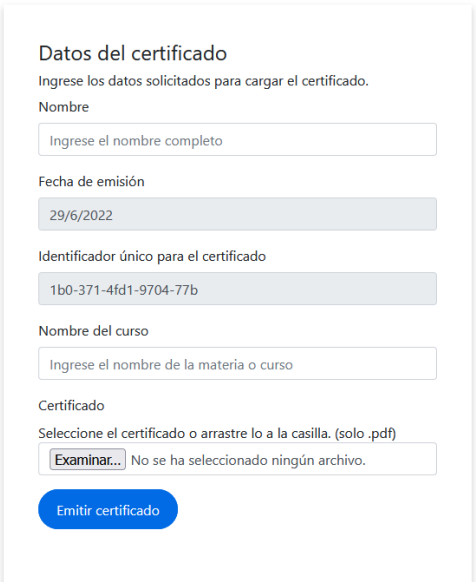
Una vez realizado las tareas el usuario puede volver al menú y cerrar sesión.

Como usuario certificador recibirá su usuario y contraseña del administrador, se recomienda guardarlo en un lugar seguro. Ingresar y visualizará plantilla que debe llenar con los datos del dueño del certificado. Una vez lleno el formulario, aplasta el botón emitir certificado, se va a generar un código QR para la persona dueña del certificado (se la envían para que la guarde en su billetera digital). Cierra la ventana del código QR y seguido aparecerá un mensaje si el registro de la información fue correcto.



The image shows a login interface for certifiers. At the top, there is a header with the text "INICIA SESIÓN CERTIFICADORES" over a background image of a laptop and a smartphone. Below the header, there is a form with two input fields: "Username" with the placeholder text "Introduce tu correo electrónico" and "Contraseña" with the placeholder text "Introduce tu contraseña". Below these fields, there is a "Cancelar" link and a blue "Ingresar" button.

Figura 38 Inicio sesión certificador



The image shows a form to issue a certificate. At the top, there is a blue header bar with "Certificador" on the left and "Cerrar sesión" on the right. Below the header, there is a form titled "Datos del certificado". The form contains the following fields: "Nombre" with the placeholder text "Ingrese el nombre completo", "Fecha de emisión" with the value "29/6/2022", "Identificador único para el certificado" with the value "1b0-371-4fd1-9704-77b", "Nombre del curso" with the placeholder text "Ingrese el nombre de la materia o curso", and "Certificado" with the placeholder text "Seleccione el certificado o arrastre lo a la casilla. (solo .pdf)". Below the "Certificado" field, there is a button labeled "Examinar..." and a message "No se ha seleccionado ningún archivo.". At the bottom of the form, there is a blue "Emitir certificado" button.

Figura 39 Pantalla de emitir certificado

Certificador

Cerrar sesión

Datos del certificado

Ingrese los datos solicitados para cargar el certificado.

Nombre

Mateo Fernando Ruiz Angulo

Fecha de emisión

29/6/2022

Identificador único para el certificado

a2e-ecb-48e0-a2d4-25d

Nombre del curso

Sistemas Ambientales

Certificado

Seleccione el certificado o arrastre lo a la casilla. (solo .pdf)

Examinar...

Certificado_prueba.pdf

Emitir certificado

Figura 40 Datos llenados

Certificador

Cerrar sesión

Escane el código QR y después ciérrelo



Sistemas Ambientales

Certificado

Seleccione el certificado o arrastre lo a la casilla. (solo .pdf)

Examinar...

Certificado_prueba.pdf

Emitir certificado

Figura 41 Emisión

Nota: el código QR puede tardar entre unos 5 a 10 segundos en generarse.

El dueño del certificado lo escanea con la aplicación, se generará una conexión por la que recibirá el certificado.

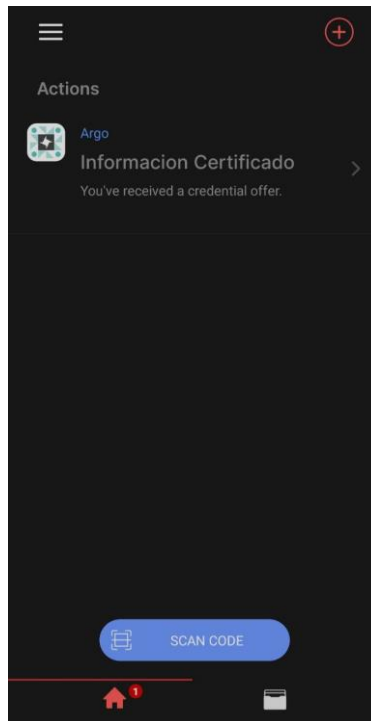


Figura 42 Certificado recibido

Da click sobre el certificado recibido, verifica que este bien los datos y le da en aceptar. Así ya tendría en su billetera su certificado.

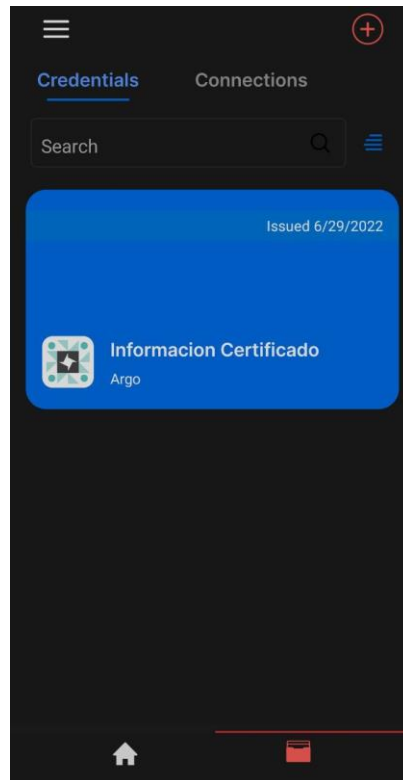


Figura 43 Certificado guardado

Como usuario público, hay dos opciones ver todos los certificados emitidos o solicitar una verificación (este último aplica más a una empresa que pide una verificación al dueño del certificado). De la página principal se dirige a la sección de “Comprobar certificado”, irá directamente a la pantalla de “Verificador certificados”. Si quiere visualizar todos los certificados emitidos diríjase a la sección de “Ver todos los certificados”.

Verificador certificados

VERIFICAR

Figura 44 Pantalla Verificador certificados

En esta pantalla se muestra la tabla con todos los certificados emitidos, el código único del certificado, el nombre a quien le pertenece el certificado, la fecha de emisión, la organización emisora y el código QR generado. El botón abrir abrirá una nueva pestaña para mostrar el QR generado.

Todos los certificados					
ID del certificado	Nombre	Fecha de emisión	Organización emisora	QR generado de la emisión	Visualizar QR generado
dd2-582-41d2-bdfb-952	Fransico Tapia	28/6/2022	ONU	https://chart.googleapis.com/chart?cht=qr&chl=https://trinsic.studio/url/107bb670-98e2-48b1-961f-1c9b36e85993&chs=300x300&chld=L 1	
3cc-19c-49d0-b027-380	Pepito Pérez	28/6/2022	ONU	https://chart.googleapis.com/chart?cht=qr&chl=https://trinsic.studio/url/b930e883-34af-4113-be1f-0fc59ef2651&chs=300x300&chld=L 1	
f8a-452-47f6-af5a-e51	Mateo Fernando Ruiz Angulo	28/6/2022	SEK	https://chart.googleapis.com/chart?cht=qr&chl=https://trinsic.studio/url/1dd37e10-1fbb-4943-a509-01c105b1a56e&chs=300x300&chld=L 1	

Figura 45 Tabla de todos los certificados emitidos

En la otra pantalla “Verificador” se puede solicitar una verificación. Para solicitar la verificación simplemente se dirige a la parte de Verificar y da click sobre el botón “Verificar”. Se abrirá una pantalla emergente con un código QR de solicitud, la persona con su billetera digital la escanea y se presenta los datos.

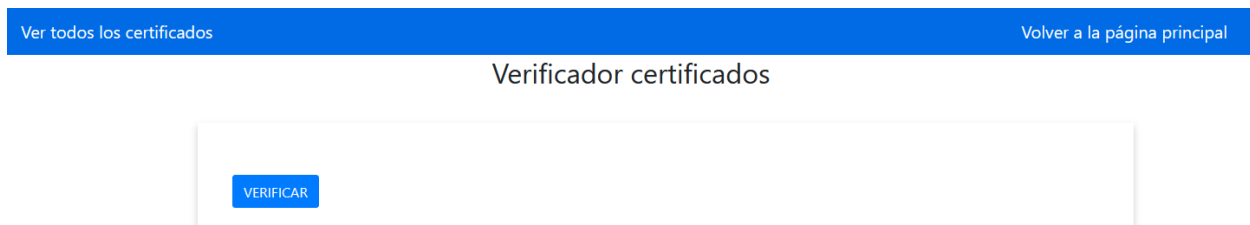


Figura 46 Pantalla Verificador

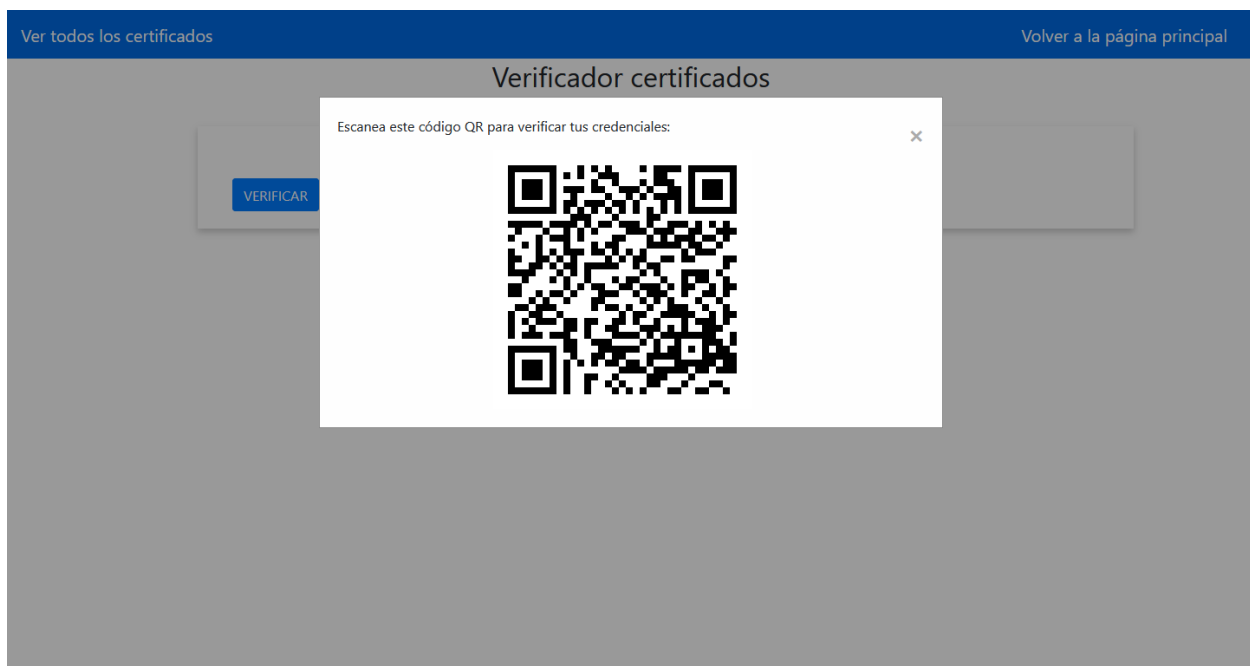


Figura 47 QR de verificación

Verificador certificados

VERIFICAR

Verificación comprobada y aceptada!!!

Certificado emitido el:

29/6/2022

Este certificado pertenece a ...

Identificador único de la credencial

a2e-ecb-48e0-a2d4-25d

Nombres

Mateo Fernando Ruiz Angulo

Certificado

C:\fakepath\Certificado_prueba.pdf

Figura 48 Verificación

Anexo B: Referencias de las APIs

Link de la página web: <https://docs.trinsic.id/docs>