UNIVERSIDAD DEL BÍO-BÍO

FACULTAD DE CIENCIAS EMPRESARIALES

ESCUELA DE INGENIERÍA CIVIL INFORMÁTICA

04 de septiembre del 2020

Concepción-Chile

"Análisis de las capacidades y limitaciones de la tecnología de Blockchain como herramienta para la gestión de certificados institucionales."

Ramon Alejandro Parra Candia

Proyecto de Título para optar al Título de Ingeniero Civil Informático

Profesora Co-Guía: Dr. Miguel Romero Vásquez.

Profesora Co-Guía: Dra. Tatiana Gutiérrez Bunster.

Resumen

Este proyecto se presenta para dar conformidad a los requisitos exigidos por la Universidad de Bío-Bío en el proceso de titulación para a la carrera de Ingeniería Civil Informática. El proyecto titulado "Análisis de las capacidades y limitaciones de la tecnología de Blockchain como herramienta para la gestión de certificados institucionales" propone una discusión y análisis de técnicas para generar, almacenar y verificar certificados institucionales a través del uso de tecnología Blockchain con el objetivo de establecer sus capacidades y limitaciones que se dispone actualmente.

En primer lugar, se realiza una introducción de la problemática respecto al uso actual de certificados, especificando lo qué son los certificados digitales y la firma digital, como también se exploran conceptos esenciales para comprender la tecnología de Blockchain en esta materia. Luego de la parte introductoria, se identifican alternativas en desarrollo que utilizan tecnología de Blockchain para crear, almacenar y verificar certificados digitales y se realiza un análisis comparativo en base a las ventajas que cada una posee. De acuerdo al análisis, se selecciona la aplicación Blockcert como la más idónea ya que ofrece un código de desarrollo abierto en donde se crean, almacenan y se validan certificados institucionales en la red de blockchain ethereum o bitcoin.

Por consiguiente, se analiza la aplicación Blockcert, con el propósito de explicar sus procesos de hash, de anclaje y de verificación, y profundizar las diversas etapas que atraviesan los certificados para validar su contenido. Y, finalmente se efectúa un prototipo en donde se evalúa la funcionalidad de la aplicación para efectos de crear, almacenar y validar certificados institucionales en la Universidad del Bío Bío y junto con ello se realiza un estudio de costos que permite ver la rentabilidad de la propuesta.

Abstract

This project is presented to comply with the requirements demanded by the University of Bío-Bío in the degree process for the Computer Science Civil Engineering.

The project entitled "Analysis of the capacities and limitations of Blockchain technology as a tool for the management of institutional certificates". This proposes the use of Blockchain technology in order to establish its capabilities and limitations that are currently available. In addition, a discussion and analysis of techniques to generate, store, and verify institutional certificates of the University of Bío Bío with this technology are presented.

First, an introduction is made to the problems related to the current use of certificates. It also studies what are digital certificates, and digital signatures, as well as the essential concepts, to understand Blockchain technology in this matter.
Alternatives that are under development and use Blockchain technology are identified, these alternatives create, store, and verify digital certificates.
Then it performs a comparative analysis based on the advantages that each of the technologies has.

According to the analysis, the Blockcert application is selected as the most suitable since it offers an open development code. Where institutional certificates are created, stored, and validated in the ethereum or bitcoin blockchain network.

Therefore, the Blockcert application is analyzed, with the purpose of explaining it is hashing, anchoring, and verification processes and deepening the various stages that certificates go through to validate their content.

Finally, a prototype is made, where the functionality of the application is evaluated in order to create, store, and validate institutional certificates at the University of Bío Bío. In addition, a cost study is carried out that allows seeing the profitability of the proposal presented.

Índice General

Índice Tablas

Índice Figuras

1 INTRODUCCIÓN

Existen diversos avances significativos en las tecnologías de almacenamiento de datos, una de estas es el blockchain es una tecnología creada en 1991 por los científicos Stuart Haber y W. Scott Stornetta (Ganne, 2018), la cual se caracteriza por tener una base de datos descentralizada que otorga una mayor seguridad a sus usuarios, ya que los datos están almacenados en distintas partes del mundo haciendo muy difícil la modificación de los datos. De esta forma, es que la tecnología blockchain ha masificado su uso para aplicaciones como almacenamiento en la nube, identidades digitales, registro y verificación de datos, contratos inteligentes, cadenas de suministros, seguridad automatizada y sistemas de votación (Redacción APD, 2019) y cada día gana más adeptos. Este proyecto de investigación busca analizar la factibilidad del uso de la tecnología de Blockchain en el almacenamiento de certificados digitales institucionales generados por la Universidad del Bío-Bío. Para el desarrollo de la investigación se realiza un estudio de las redes de blockchain existentes para elegir una y desarrollar un prototipo que permita verificar su factibilidad de implementación.

1.1 Planteamiento del problema

En la actualidad las instituciones educativas entregan certificados a sus estudiantes luego de aprobar una cierta cantidad de ramos, estos certificados pueden ser de licenciatura hasta de un título universitario. Para esto se utiliza certificados en papel los cuales una vez emitidos tienen que almacenarse en un sistema de registro centralizado con todos los certificados emitidos y su verificación tiene un costo muy alto en recurso humano (Bartolomé & Moral-Ferrer, 2018). También, estos se pueden generar de manera digital los cuales son fáciles de falsificar sin una firma digital y en el caso de tener una ,se necesita un tercero que genere la firma y esto conlleva a que el tercero tenga una base de datos de todas sus firmas, las cuales según Bartolomé & Moral-Ferrer (2018) son susceptibles a sufrir algún problema, ya sea en el almacenamiento de estos o si la empresa desaparece, perdiendo la validez de estos certificados, como también se identifica que no en todos los países está disponible esta tecnología.

Sumándose a esto se encuentra la resistencia al cambio presente en la gente frente a nuevas tecnologías, las cuales facilitan y optimizan la forma en la que se genera y se almacenan los

certificados. Según Jiménez (2020), esto impone un desafío que no es necesariamente tecnológico, sino, que de una mala gestión la cual podría ser la gran causa de que muchos actores queden rezagados en este nuevo mundo digital.

En el caso de la Universidad del Bío Bío recientemente se ha implementado una plataforma de certificados con firma digital disponible solamente para certificados de grado y de título. Uno de los desafíos que se presentan es ampliar esta firma digital para los demás certificados que se entregan por la institución educativa de manera automática, tales como certificado de alumno regular, de actividades, de participación, de idiomas, etc.

Además, producto de la pandemia ocasionada por el COVID-19, se hace imperante investigar y desarrollar alternativas de aplicación de firmas digitales que permitan a los estudiantes efectuar sus trámites académicos desde sus hogares con la mayor seguridad posible

1.2 Objetivos del Proyecto

Dada la importancia que tienen los certificados digitales en las instituciones y las posibilidades tecnológicas que nos brinda blockchain, para este trabajo se han definido los objetivos que a continuación se detallan.

1.2.1 Objetivo general

Analizar las capacidades y limitaciones de la tecnología de Blockchain como herramienta de gestión de certificados institucionales mediante el desarrollo de una aplicación local que permita generar, almacenar y validar certificados institucionales, pudiendo proyectarse a una red de blockchain de mayor escala.

1.2.2 Objetivos específicos

1. Realizar un estudio bibliográfico sobre el uso y las aplicaciones de almacenamiento de certificados u otros documentos en Blockchain.

2. Analizar los diversos métodos encontrados en el estado del arte para el almacenamiento de documentos en Blockchain.

3. Seleccionar un método o proponer una arquitectura de Blockchain para la gestión de certificados institucionales.

4. Desarrollar una aplicación práctica a modo de prueba de concepto que simula una red de Blockchain para gestionar certificados institucionales.

5. Analizar las capacidades y limitaciones de la tecnología de Blockchain propuesta en base a las simulaciones realizadas con el prototipo.

6. Evaluar las principales redes de Blockchain para la implementación a mayor escala de este proyecto en comparación con la creación de una infraestructura propia y con la solución tradicional de certificado digital de documentos.

7. Realizar un estudio de costos para la implementación de blockchain en la Universidad del Bío Bío

2 MARCO TEÓRICO

Uno de los problemas en materia de certificación que persiste al día de hoy es la vulneración de su material en cuanto a la facilidad de ser falsificados por externos (Bartolomé & Moral-Ferrer, 2018) y por ello adquiere importancia el profundizar la discusión del uso del Sistema de Blockchain para estos fines. De esta forma, según Bartolomé y Moral-Ferrer (2018) señalan que esta tecnología ayuda a las organizaciones a emitir certificados digitales inalterables y validos a perpetuidad en virtud de que su autenticidad se puede validar con el propio sistema mediante un token que posee la red de Blockchain, el cual está siempre disponible para su validación. Todo aquello significa ventajas importantes en comparación a los sistemas actuales dado que se aumenta de forma significativa la propuesta de valor de los certificados digitales, lo cual podría conllevar a un uso más generalizado.

Para efectos de la investigación, se buscó en primer lugar definir lo qué es un certificado para luego distinguir y describir los términos de certificado digital y firma digital. Junto con ello, se explica el proceso de certificación que posee la Universidad del Bío-Bío como institución educativa.

En segundo lugar, se realizó una revisión bibliográfica respecto al Sistema de Blockchain con el objeto de comprender la forma en que se articula. Esta revisión bibliográfica comprende artículos académicos, tesis de posgrado y artículos de páginas web. De esta forma, se definió y se explicó el funcionamiento de dicho sistema, señalando tanto los componentes y procesos que lo integran. Y, por último, se señaló y se describió ciertos tipos de la red de Blockchain que utilizan un sistema de almacenamiento de certificados, con el objetivo de identificar sus similitudes y diferencias.

2.1 Certificado

El certificado es un tipo de texto administrativo empleado para constatar un determinado hecho (ver ilustración 1). De acuerdo a Bartolomé & Moral-Ferrer (2018) los certificados son un tipo de texto que se produce normalmente a instancias de quien lo recibe, y por una persona con autoridad suficiente dentro de la institución para establecer que se ha cumplido

con lo afirmado en el documento. Si llega haber alguna irregularidad o falsedad en lo declarado, puede ser sancionado por la ley.

UNIVERSIDAD DEL BÍO-BÍO

En conformidad a la reglamentación vigente, por Decreto N° 1137 del 30 de abril de 2002 del señor Rector, certifico que se ha conferido a don (a)

RUN N° el TITULO DE INGENIERO DE EJECUCIÓN EN COMPUTACIÓN E INFORMÁTICA, a contar del 22 de abril de 2002.

Inscrito en los registros de esta Corporación bajo el Rol N° 606.

Dado en Concepción, a 29 de mayo de 2007.

LUIS RICARDO PONCE SOTO
Secretario General

Nro.:
PRC/sij

Este documento es válido sólo en original

Ilustración 1: Certificado de título Universidad del Bío Bío.

2.1.1 Certificado digital

Según Gallardo (2018) un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y una clave pública.

Este tipo de certificados se emplea para comprobar que una clave pública pertenece a un individuo o entidad. La existencia de firmas en los certificados asegura por parte del firmante del certificado (una autoridad de certificación, por ejemplo) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.

De esta forma, Gallardo (2018) establece que un aspecto fundamental del certificado digital es que para cumplir la función de identificación y autenticación necesita del uso de la clave privada (que sólo el titular conoce). El certificado y la clave pública se consideran información no sensible que puede distribuirse a terceros. El certificado sin más no puede

ser utilizado como medio de identificación, pero es una pieza imprescindible en los protocolos usados para autenticar a las partes de una comunicación digital, al garantizar la relación entre una clave pública y una identidad.

2.1.2 Certificados digitales Universidad del Bío Bío

En el marco de iniciativas de Gobierno Electrónico de la Universidad del Bío-Bío, se ha lanzado el portal web de Certificación en Línea [1](ver ilustración 2) en donde aquellos alumnos egresados de la institución desde el año 1990 en adelante podrán comprar a través del sitio certificados de Título y Grados en una primera etapa.

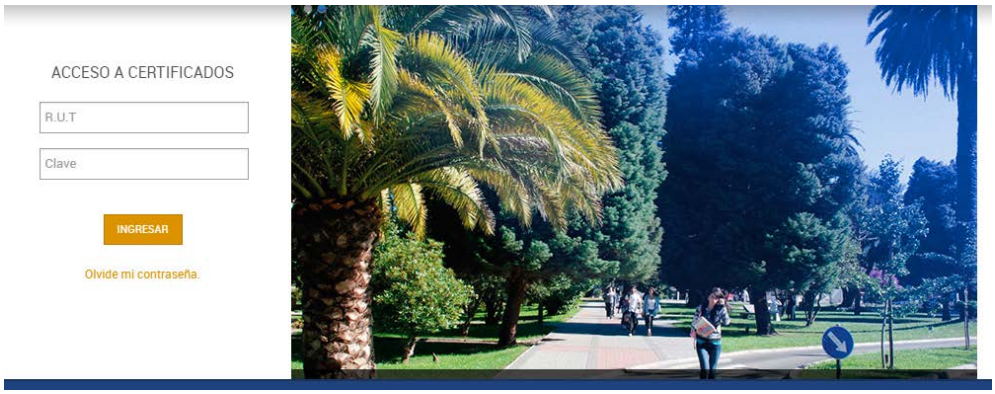

Ilustración 2: Pagina certificados digitales Universidad del Bío Bío Fuente: Elavoracion Propia.

2.2 Firma digital

Desde comienzos del siglo XXI es posible observar cómo han ido desarrollándose diversas herramientas tecnológicas conducentes a facilitar los procesos de entidades públicas, privadas y mixtas, como también diversos aspectos de la vida cotidiana de los individuos.

En el Estado de Chile, el año 2002 se publicó en el Diario Oficial la Ley de Firma Electrónica N° 19.799, la cual revolucionó el escenario tradicional de actividades comerciales, compras electrónicas y las transacciones tanto entre privados, empresas e instituciones. De esta forma el Estado de Chile se consolidó como un país de vanguardia tecnológica entre sus pares.

[1] certificados.ubiobio.cl/

La firma digital es una modalidad de firma electrónica que utiliza una técnica de criptografía asimétrica con el objetivo de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido (Rojas, 2014) Es importante destacar que la firma electrónica no implica la encriptación del mensaje, sino que, mediante una función matemática, crea una imagen de él, la que es enviada junto al mensaje original y la identificación digital.

Por consiguiente, para firmar un mensaje se utiliza una función matemática que compara la imagen recibida con la nueva imagen producida. Dicha función matemática se denomina función de *Hashing*, la cual produce un resumen único del mensaje que representa una huella digital del mensaje y luego se encripta utilizando la clave privada del emisor y el resultado de aquello es la firma digital, que es agregado al mensaje original. De este modo, el destinatario puede confirmar tanto el origen del mensaje como la integridad de la información incluida en él mediante la acción de desencriptar la firma digital usando la clave pública del emisor, y comparando el resultado con resumen producida al pasar el mensaje recibido a través de la misma función matemática usada en el origen (Maulén et al, 2003).

En efecto, lo particular de la firma digital es el uso de la técnica de criptografía asimétrica, es decir, no consiste en escanear una firma sino una técnica especial de encriptación. El uso de la criptografía asimétrica permite confidencialidad incluso a través de redes abiertas como Internet, también proporciona autenticidad, integridad y vinculación, las cuales se constituyen como características de la firma digital.

La encriptación asimétrica es un tipo de criptografía de clave pública, que se define como una técnica que utiliza un par de claves que constituyen un par único, que están permanentemente relacionadas entre sí. En este sentido, cada participante de una comunicación posee uno de estos pares, de la cual una de las claves es mantenida en forma privada (clave privada) y la otra es hecha pública (clave pública).

En la ilustración 3 se muestra el proceso del tipo de encriptación que opera en la firma digital, la cual utiliza un par de llaves que son: la llave pública del destinatario con la cual se encripta (codifica) el mensaje, y la llave privada del destinatario con la cual se desencripta el mensaje.

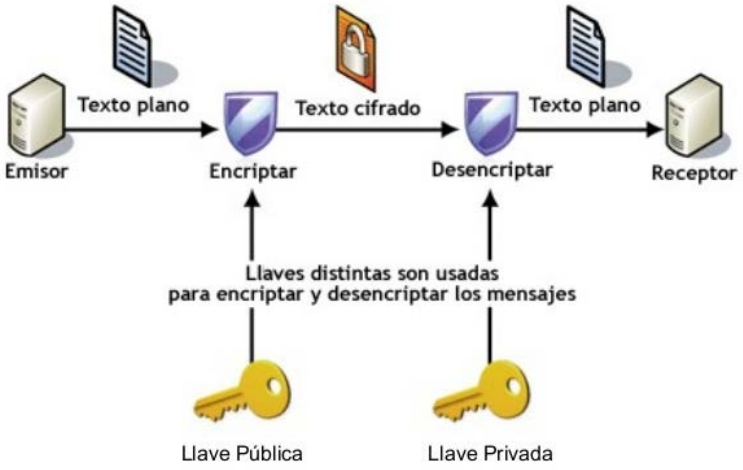

Ilustración 3: Encriptación Asimétrica. Fuente: S.A (2016).

2.3 BlockChain.

El blockchain (en español, cadena de bloques) es una tecnología creada en 1991 por los científicos Stuart Haber y W. Scott Stornetta (Ganne, 2018) e introduce una solución computacionalmente práctica para los documentos digitales con sello de tiempo, lo cual permite que sean modificados o manipulados. Esto quiere decir que la tecnología de Blockchain posee un registro compartido y digitalizado de cada transacción que ha sido registrada y verificada. Todas las partes de la transacción, así como un número significativo de terceros, mantienen una copia del registro (es decir, la cadena de bloques), lo que significa que sería prácticamente imposible modificar cada copia del registro globalmente para falsificar una transacción (Gallardo, 2018).

En caso de que haya alguna persona o grupo que intente alterar estos registros se podría hacer con un ataque del 51%, esto significa que esta persona debe hacerse con el 51% de toda la red lo cual equivale a 5407 nodos de los 10813 que actualmente existe a la fecha(ver en bitnodes[2]), además , se debe tener el poder de procesamiento lo suficiente potente para que sea esta persona quien realice las verificaciones de los bloques en cuestión de segundos. Lamentablemente para esta persona la acción es imposible de hacer con la tecnología que se tiene actualmente además de que la implementación y la electricidad necesaria para realizar

[2] https://bitnodes.io/

este proceso tendría unos costos bastante mayores a cualquier ganancia que se pueda obtener de este proceso.

En síntesis, la cadena de bloques funciona como una libreta, la cual almacena registros inmutables de todas las transacciones que se hacen. Para comprender su funcionamiento es importante describir de manera previa los principales componentes y procesos que la conforman, los cuales son:

a) Bloques.

Según Álvarez (2018) un "bloque es una estructura de datos contenedor que agrupa las transacciones para su inclusión en la cadena de bloques" (p.49). Esta se compone de una cabecera constituida de metadatos y una lista de operaciones que componen la mayor parte de su tamaño. De esta forma, para crear nuevos bloques se tiene que alcanzar una cierta cantidad de transacciones aprobadas, estas corresponden a un envió o transferencia de una información entre dos partes, y cuando efectivamente se crea un bloque, este es agregado al blockchain y posteriormente los nodos actualizan su registro de manera automática para realizar las validaciones necesarias.

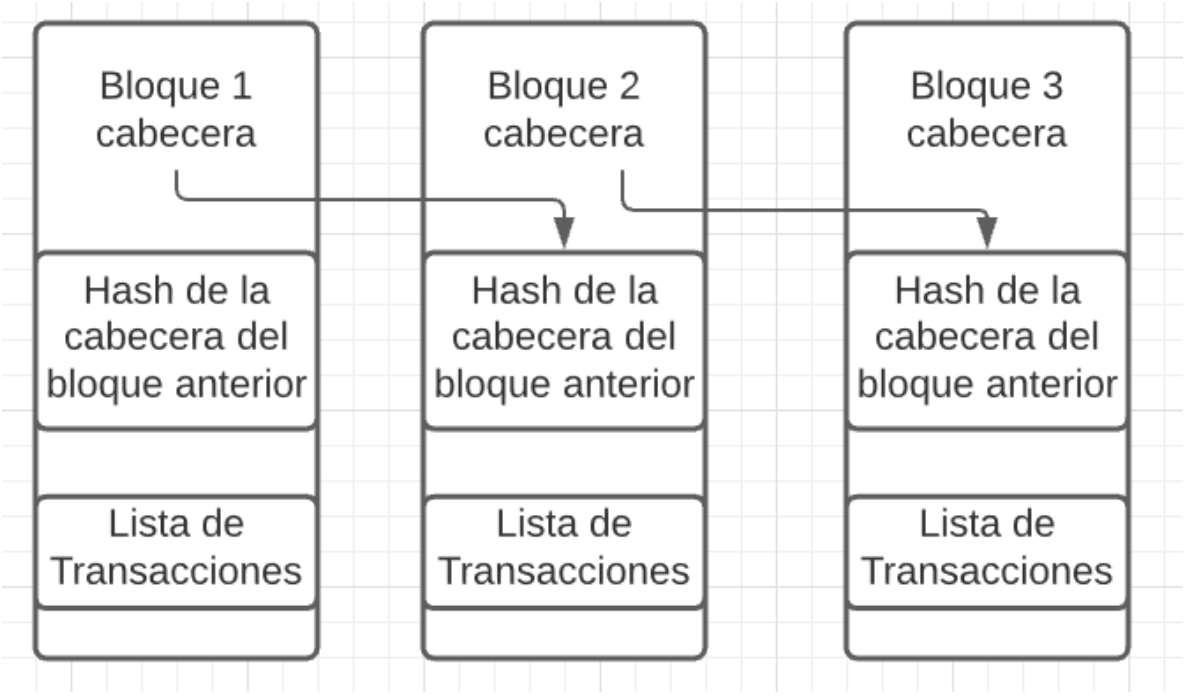

Ilustración 4: Ejemplos de bloques encadenados Fuente: Elaboración Propia

b) Nodos.

La gestión de las cadenas de bloques se realiza mediante ordenadores o servidores conocidos como Nodos (Ganne, 2018). Estos están presentes a lo largo de todo el mundo y su principal tarea es aprobar cada transacción que se produzca en la red, verificando la validez de estas. De esta manera, una vez que cada nodo verifica una transacción, hay una especie de voto electrónico puesto que algunos nodos pueden pensar que la transacción es válida y otros pueden que no. Frente a ello cada nodo tiene una copia del libro digital o Blockchain y si la mayoría de estos señala que la transacción es válida se incorpora el bloque el cual luego será ingresado a la red.

c) Hash.

Para que la información sea ingresada al bloque en la red de Blockchain lo primero que se debe hacer es tener un programa de función de hash, el cual lo que hace es codificar el texto que se ingresa a la función dándole una cadena de números y letras con una longitud fija en un orden único e irrepetible, esto es logrado gracias a la función criptográfica llamada función hash (Maldonado, 2020). Si esta cadena de caracteres se llega a editar se cambia complemente el hash generando uno diferente. En el caso del registro de hash en blockchain este se produce de una manera que cada registro tiene un hash creado a partir del registro más el último hash. El algoritmo de hash utilizado en las redes de blockchain es SHA256 (Sakamoto,2013).

Por tanto, a modo de prueba se utilizará el algoritmo SHA1 para realizar ejemplos ya que, para efecto de pruebas se comportan de manera similar y es más fácil de manejar, si aplicamos la función hash SHA1 al texto "Hola Mundo!" se obtiene como resultado: c6629b8816a24edc1eb3e6d11745c61a0bd1f586 (verificar en sha1-online[3]).

d) Prueba de Trabajo (Proof of Work).

La prueba de trabajo es un algoritmo utilizado para llegar a un acuerdo descentralizado que determine cuál de los bloques se agrega a la cadena después de la validación (Herrera, 2018). Esto se lleva a cabo mediante la resolución de problemas matemáticos complejos y variables, donde los nodos intentan darle la solución correspondiente para lograr obtener una recompensa en la cadena de bloques (Nakamoto, 2013).

[3] http://www.sha1-online.com/

Según Herrera (2018) para validar un bloque de manera exitosa, es necesario ajustar el encabezado del bloque de tal manera que sea menor o igual que el objetivo (Hash). Los nodos llegan a este hash en particular, variando una pequeña porción del encabezado del bloque, llamado "*nonce*". Un "nonce" siempre comienza con "0" y se incrementa cada vez para obtener el hash requerido. Siguiendo el ejemplo anterior mencionado en el Ítem de Hash, para encontrar un hash usando SHA1 que comience con un nonce de "0000" para el mensaje "Hola Mundo!", se debe anteponer un nonce=158310 al inicio donde el resultado será un nuevo mensaje "158310 Hola Mundo! y el hash de este será 0000d097065c80dac8a6fdf8fa1c2e227b0ca91e. Cabe destacar que los hashes en los registros no tienen relación entre ellos.

Según Cámara (2018) la variación del nonce es al azar, lo cual genera una baja posibilidad de obtener un hash en particular que comience con varios ceros y por ende la realización de un nodo se efectúa mediante muchos intentos, variando constantemente el nonce, lo que implica efectuar un cuantioso trabajo. Por tanto, se requiere una gran cantidad de energía eléctrica y capacidad computacional con recursos de hardware que lleven a cabo toda la serie de operaciones.

e) Prueba de Participación (Proof of Stake).

La prueba de participación, es una alternativa al mecanismo anterior. Esta busca de igual forma lograr un consenso descentralizado para validar las transacciones entre los participantes de la red. Su creación fue el resultado de considerar el mecanismo de prueba de trabajo como un desperdicio de recursos, ya que los costos por el alto consumo eléctrico y el de los equipos necesitados para realizar la minería resultaban elevados (Herrera, 2018). Además, una característica particular de este método es que previo a efectuar las transacciones los bloques son generados en la red y por tanto las transacciones se distribuyen entre estos.

De acuerdo a Herrera (2018) la prueba de participación es un método en el cual varios nodos participan del proceso de validación de las transacciones realizadas en la red de Blockchain. Para la elección de los bloques con transacciones a validar se adoptan diferentes criterios, tales como la edad de los bloques y la cantidad de hashes almacenados en estas, sin embargo, es importante señalar que cada red de blockchain puede crear su propia regla. Finalmente,

en esta prueba, se elige un nodo de los que participa y este ingresa las nuevas transacciones al bloque y lo firma, luego el resto de nodos participantes valida que el bloque sea legitimo para luego ser actualizado a la red de blockchain y el nodo que fue elegido recibe las comisiones por las transacciones realizadas en dicho bloque.

2.3.1 Funcionamiento de un Blockchain.

Para explicar el funcionamiento del Blockchain se utiliza como principal fuente bibliográfica la tesis de Maestría de Ignacio Gallardo (2018) denominada "Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada".

Actualmente la tecnología de Blockchain se usa como un sistema de registro de red entre pares o P2P (peer to peer)[4], donde cualquier usuario puede ver las transacciones hechas, pero nadie puede alterarlas, otorgando una mayor transparencia. Para lograr aquello, cada usuario de la red posee 2 llaves, una de ellas es una llave pública la cual constituye la dirección pública de la cuenta con la cual se recibe las transacciones y la otra es una llave privada que sirve para las autorizaciones de envío de transacciones.

A continuación, a modo de ejemplo, se explica como una persona A realiza una transacción, la cual consiste en enviar una cierta cantidad de criptomoneda, a una persona B dentro de la red de blockchain, es necesario seguir los siguientes pasos descritos en la ilustración 4:

1. En el caso de cualquier red de blockchain es necesario que al realizar una transacción se conozca la clave pública de la persona B para poder hacer envió de algún tipo de dato.
2. Se representan los datos de la transacción a enviar de la persona A los cuales serían: la dirección de la persona B, la cantidad de criptomoneda a enviar, la firma digital de la persona A y la clave pública de la persona A.
3. La transacción es enviada a la red blockchain para su comprobación.

4 De acuerdo a Binance Academy (s.f) la red peer-to-peer (P2P) se define como un grupo de dispositivos que almacenan y comparten archivos de forma colectiva donde cada participante (nodo) actúa como par individual. Normalmente, todos los nodos tienen el mismo poder y ejecutan las mismas tareas.

4. La red comprueba [5]de que la firma digital de la persona A sea válida para luego validar la transacción y hacer el proceso de hash, luego se crea un bloque con el hash actual más el hash del bloque anterior para formar una cadena entre un bloque y el anterior.
5. El bloque es agregado a la red de blockchain y esta actualiza todos los nodos conectados a esta.
6. Finalmente, la transacción es validada y la persona B recibe las criptomonedas enviadas de la persona A.

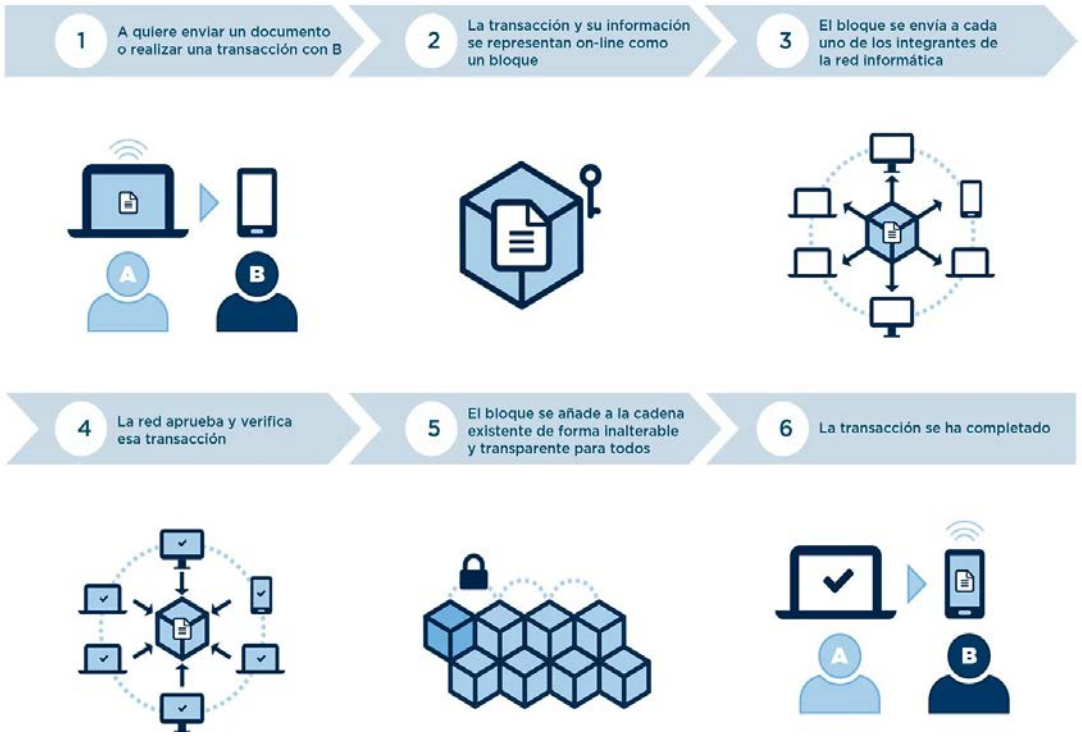

Ilustración 5: Procedimiento de una transacción en la red de Blockchain Fuente: S.A(2018)

[5] Las comprobaciones se hacen a través de Prueba de trabajo o Prueba de participación.

2.3.2 Tipos de blockchain

Existen diversos tipos de red de Blockchain[6], tales como bitcoin[7], Ethereum[8], Litecoin[9], cardano,stelar, tron, neo, cosmos, iota, dash, dogecoin, digibyte, entre varias otras. Sin embargo, para efectos de esta investigación se profundiza meramente sobre tipos de redes de blockchain en las cuales se cuenten con aplicaciones que nos permitan crear, validar y almacenar certificados digitales y así efectuar un análisis que vislumbre las similitudes y diferencias que poseen entre ellas.

a) Bitcoin

El Bitcoin, o en su abreviación BTC, es una moneda digital o criptomoneda que fue creada en 2009 por Satoshi Nakamoto, esta criptomoneda se intercambia a través de internet mediante un sistema criptográfico y que asegura las transacciones mediante la tecnología blockchain, algo así como un libro de contabilidad compartido que se guarda en varios ordenadores de diferentes ubicaciones (Nakamoto, 2008). De esta manera es muy difícil que el sistema pueda ser hackeado.

b) Ethereum

Ethereum es una plataforma digital que adopta la blockchain establecida por bitcoin y expande su uso a una gran variedad de aplicaciones (Gallardo, 2018). No debe confundirse con ether (la criptomoneda subyacente de la red) a la que habitualmente también se la denomina ethereum.

La plataforma Ethereum fue creada en 2015 por el programador Vitalik Buterin, con la perspectiva de crear un instrumento para aplicaciones descentralizadas y colaborativas. Ether (ETH) es una ficha que puede ser utilizado en transacciones que usen este software. Tal como

[6] https://coinmarketcap.com/
[7] https://bitcoin.org
[8] https://ethereum.org
[9] https://litecoin.org

bitcoin, ether existe como parte de un sistema financiero autónomo de pares, libre de intervención gubernamental.

El blockchain de Ethereum es muy similar al de bitcoin, pero su lenguaje de programación llamado solidity que les permite a los desarrolladores crear software a través del cual gestionar las transacciones y automatizar ciertos resultados. Este software se conoce como contrato inteligente (Bartolomé & Moral-Ferrer, 2018). Los contratos inteligentes son creados en la red de Ethereum con todas las reglas y sanciones predefinidas por los contratos inteligentes, sino que también son aplicadas por ellos.

c) Blockstack

De acuerdo a Ali et al. (2016) Blockstack proporciona una alternativa *full-stack* en comparación con la computación tradicional puesto que a través de la nube se permite desarrollar aplicaciones seguras y privadas. En este sentido, una de las diferencias clave entre las aplicaciones de internet tradicionales y las aplicaciones descentralizadas que habilita blockchain, reside en que la mayoría de la lógica de negocio, y el procesamiento de los datos, en lugar de alojarse en un servidor central contratado por los desarrolladores de la aplicación, este se aloja en el usuario o cliente.

La red blockstack se compone de múltiples sistemas, que en conjunto proporcionan los componentes necesarios para implementar aplicaciones descentralizadas. Estas son:

1. Stacks Blockchain: es el núcleo de la red blockstack y permite a los usuarios registrar y controlar activos digitales como nombres de usuario universales, además de registrar y ejecutar *Smart contracts*.

2. Gaia: es un sistema de almacenamiento que es controlado por los usuarios y así permitir que las aplicaciones interactúen con los contenedores privados de datos. En

Gaia los datos están encriptados y firmados por parte del cliente a través del uso de claves criptográficas.

3. Autentificación de blockstack: el protocolo de autentificación de blockstack es un protocolo de autentificación para aplicaciones de manera descentralizada. Este protocolo permite a los usuarios autentificarse mediante identidades sobre las que tienen control.

4. Librerías de Blockcstack y *SDKs*: comprende la parte superior de la pila de software y mediante ella los desarrolladores y usuarios interactúan con los diversos componentes de la red Blockstack.

Según Ali et al. (2019) más de 100 aplicaciones descentralizadas han sido desarrolladas en esta red desde principios del 2019. Esta tecnología ha permitido eliminar la necesidad de que los desarrolladores tengan que utilizar servidores y bases de datos puesto que en su lugar las aplicaciones escriben datos sobre contenedores privados de datos que controlan los mismos usuarios. Por tanto, la arquitectura de Blockstack ofrece un mayor rendimiento al emplear como soluciones de almacenamiento similares a las de nube tradicional y ser de baja complejidad puesto que solo introduce una leve sobrecarga producto de la encriptación y desencriptación.

d) Emercoin

De acuerdo a EMERCOIN (2018) el emercoin se define como una plataforma blockchain que admite una amplia gama de servicios distribuidos de confianza. Sus características más importantes son alta confiabilidad, robustez y minería híbrida 3 en uno (*PoW + MergedMining + PoS*). Actualmente, la plataforma Emercoin ya ejecuta los servicios de seguridad de red EmerSSL / EmerSSH, el sistema de dominio descentralizado EmerDNS, un sistema de anti falsificación EmerDPO, Protocolo de voz sobre internet ENUMER, así como varios otros servicios de blockchain incluidos. En el corazón de muchas de estas innovaciones está el Emercoin NVS que permite el almacenamiento arbitrario de pares de “nombre a valor” en la cadena de bloques.

3 ESTADO DEL ARTE

Hoy en día están emergiendo una multitud de plataformas basadas en la cadena de bloques que facilitan la construcción de nuevas aplicaciones y validan el uso de credenciales vía blockchain (Tapscott, 2018) Si bien, la mayoría de estos proyectos aún están en etapa de desarrollo, ya se ha logrado llegar a un mínimo producto viable que garantice una exitosa implementación.

Por tanto, en esta sección se describirá el uso de aplicaciones ya desarrolladas que utilizan el sistema de blockchain para la generación y almacenamiento de diplomas o certificados académicos. Para la elección de estas aplicaciones, se contemplará como requisitos que la aplicación pueda ser utilizada como arquetipo para la creación y validación de certificados académicos.

3.1 BLOCKCERTS

Blockcerts es un proyecto de código abierto que consiste en un sistema descentralizado de credenciales basado en la tecnología de blockchain. Este proyecto permite emitir y verificar registros oficiales creados por una institución (*BLOCKCERTS*, 2016). Los certificados emitidos pueden ser registros cívicos, credenciales académicas, licencias profesionales, entre muchos más.

En el año 2017 el Instituto Tecnológico de Massachusetts (MIT) en Estados Unidos inició un programa piloto que mediante la aplicación de Blockcerts tiene como objetivo emitir diplomas o certificados universitarios usando una red Blockchain de Bitcoin y el cual sigue funcionando en la actualidad (Young, 2017).

Blockcerts conta de 3 componentes esenciales, de los cuales se encuentran disponibles en su proyecto de *github*:

1. *Cert-issuer*: Su uso permite que las instituciones puedan crear certificados digitales con la información de la persona, lo cual se realiza mediante una transacción que crea la institución a la persona, donde se incluye el hash del certificado.

2. *Cert-verifier*: Se utiliza para que terceros puedan verificar que el certificado emitido por la institución es válido. Esto se efectúa a través de una librería que verifica el hash del certificado con la red de blockchain en donde fue emitido.

3. *Wallet*: Es una aplicación que se encuentra disponible en "Ios" y "Android", la cual se utiliza para almacenar los certificados de manera segura y compartirlos con otras personas.

Según la página de Blockcerts [10]el proceso de esta aplicación funciona de la siguiente manera (ver ilustración 5):

1. La institución le envía una invitación a una persona para recibir una credencial de blockchain[11].
2. La persona debe aceptar la invitación para remitir su dirección de blockchain en donde se enviará el certificado.
3. La institución al recibir la dirección del *Wallet* [12]de la persona procede a aplicar el hash al certificado para ingresarlo a la red de blockchain.
4. Una vez ingresada al blockchain se envía el certificado a la persona.
5. Se verifica que la credencial esté válida, puesto que esta puede haber sido dada de baja.
6. Por último, se verifica el certificado con la cadena de blockchain.

Hoy en día, el proyecto de Blockcert solo puede ser utilizado en las redes de Blockchain Bitcoin y Ethereum, pero se espera que pronto pueda ampliarse su uso a cualquier red de Blockchain.[13]

[10] https://www.blockcerts.org/guide/
[11] Credenciales creadas por blockcert
[12] Cartera digital para almacenar información

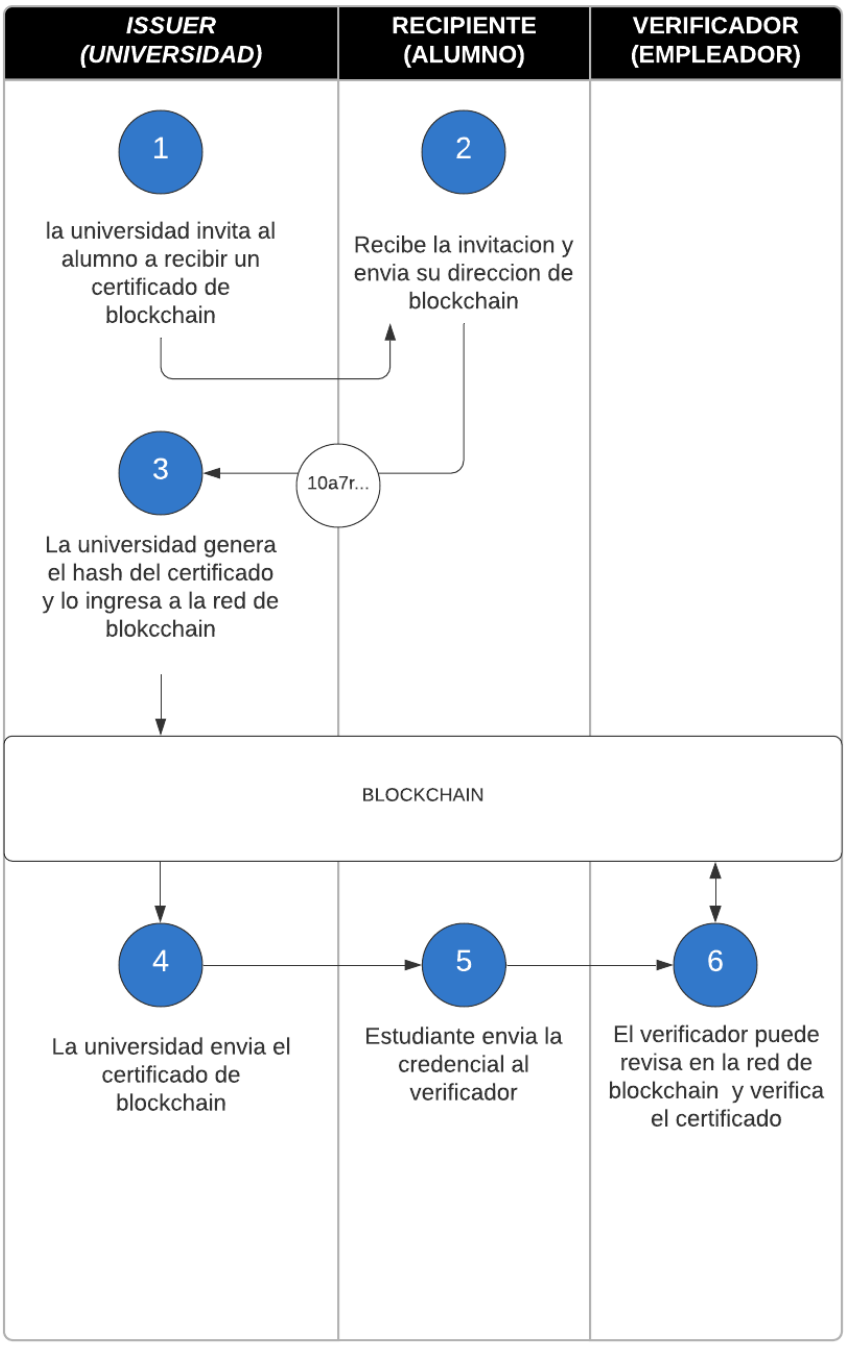

Ilustración 6: Funcionamiento BlockCerts. Fuente: BLOCKCERTS (2016).

3.2 TRUSTED DIPLOMA

Según el sitio web de Emercoin [14]Trusted diploma es una propuesta tecnológica creada por este mismo en conjunto con *Business & Technology University*, que busca abordar la problemática de falsificación de diplomas académicos mediante el uso de una propia red de Blockchain.

Esta propuesta presenta una plataforma en Blockchian que permite a los colegios crear y compartir diplomas o alguna otra credencial educativa mediante una aplicación encriptada (ver ilustración 6). De esta forma, los registros son almacenados en el blockchain y son fáciles de verificar por cualquiera. Por tanto, se caracteriza por ser un sistema flexible, amigable con el usuario y de fácil acceso ya que se encuentra en la misma *Wallet* de Emercoin.

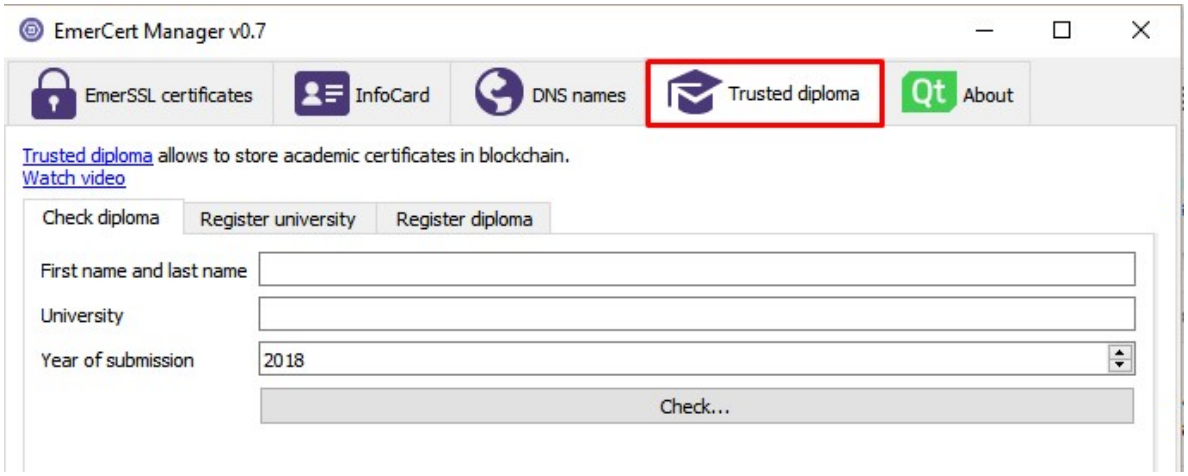

Ilustración 7: Trusted Diploma. Fuente: Elaboración propia.

[14] https://emercoin.com/

3.3 BLOCKCRED

De acuerdo a la misma plataforma de *BLOCKCRED* [15] este se define como un servicio de credenciales digitales basados en blockchain que permite a universidades, empresas e instituciones no académicas emitir credenciales y certificados de forma descentralizada y segura. Por otro lado, este sistema faculta también a que los terceros puedan solicitar, verificar y compartir credenciales y certificados. De esta manera, se otorga tanto a las instituciones como a los usuarios las ventajas del uso de esta tecnología que son: disponibilidad, intratabilidad, verificabilidad, compatibilidad e inmutabilidad.

En el caso de las empresas, Blockcred ayuda a tener un ecosistema en donde los empleadores no necesitan gastar demasiado dinero y tiempo para verificar las credenciales de su nuevo empleado ya que es solo cuestión de algunos clics y se le informará sobre su historial profesional.

En el caso de las universidades, cada usuario posee una clave privada, por tanto, nadie puede emitir un certificado en su nombre. Junto con ello, se gasta menos por la emisión del certificado ya que no es necesario pagar por asegurar el papel de este. De esta manera, los certificados están asegurados producto de la forma de emisión y por ello los estudiantes pueden enfocarse en el proceso de contratación ya que sus certificados son fáciles de verificar y de almacenar.

El Sistema Blockcert funciona con los siguientes pasos enumerados en la ilustración 7:

1. La universidad pública el curso en su propia plataforma e invita al estudiante a solicitar la credencial del curso.
2. El estudiante acepta la invitación y se aplica al curso con su ID de Blockstack para obtener el certificado.
3. La universidad agrega la credencial a Blockchain y firma la transacción con su propia clave privada.
4. La universidad envía el enlace de verificación de credenciales al estudiante después de almacenarlo en su propio almacenamiento GAIA.
5. El estudiante obtiene la credencial digital y la almacena en su almacenamiento GAIA (billetera). De la cual, nadie puede manipular o eliminar.

[15] https://www.blockcred.io/

6. El estudiante puede invitar a cualquier verificador (mediante la ID de Blockstack del verificador) para verificar su información de credencial.
7. El verificador examina el Blockchain para comprobar la información de credenciales y asegurarse del emisor.
8. El estudiante puede invitar al empleador a verificar su historial de carrera enviándole su clave pública (ID Blockstak).

Ilustración 8: Funcionamiento BlockCerd. Fuente: BLOCKCRED (n.d.)

3.4 Tabla comparativa

Aplicación	Estado	Código	APP PC	APP Celular	Crear varios certificados	Comunidad de desarrollo	Red Blockchain
Blockcert	Desarrollo	Abierto	Si	Si	Si	Activa	Bitcoin/Ethereum
Trusted Diploma	Desarrollo	Cerrado	Si	En desarrollo	Si	Inactiva	Emercoin
Blockcred	Desarrollo	Cerrado	Si	En desarrollo	Si	Activa	Blockstack

Tabla 1: Comparativa de aplicaciones que utilizan sistema de Blockchain.
Fuente: Elaboración propia.

Según la tabla 1, es posible observar que las diferentes aplicaciones comparten varias características similares, sin embargo, la aplicación Blockcert destaca sobre las otras debido a que cuenta con un código abierto, el cual permite hacer los cambios que sean necesarios para adaptarse a las necesidades de las instituciones donde se implementa, además posee una aplicación web y de celular que constantemente efectúa actualizaciones en los repositorios de github, otorgando una mayor accesibilidad para sus usuarios. Y, por último, es importante señalar que Blockcert posee una comunidad activa que mediante foros y videos informa y ayuda a los usuarios con las inquietudes.

3.5 Tesis similares

Para el desarrollo de esta investigación se tomó en consideración dos tesis realizadas dentro de la región de América Latina, de la cual una era para optar al título de grado en Colombia y la otra para optar a un título de posgrado en Argentina.

De acuerdo a lo mencionado anteriormente, la primera de ellas se denomina "Sistemas Descentralizado para la Verificación y la Autentificación de Certificados Académicos utilizando la Tecnología de blockchain" para optar al título de grado por los colombianos David Sánchez y Ferney Jerez (2019). Este proyecto creó un prototipo de plataforma de certificados mediante el Sistema de Blockchain, utilizando para estos efectos el *Hyperledger*[16], el cual es una tecnología colaborativa de código abierto. La importancia de este trabajo es que brinda el marco conceptual de un proyecto que pretende avanzar en el

[16] https://www.hyperledger.org/

desarrollo de la tecnología blockchain y de esta manera presenta la construcción de una plataforma web y una aplicación móvil para crear y validar certificados emitidos.

Mientras que la tesis "Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada" para optar al título de posgrado por el argentino Ignacio Gallardo (2018) otorga una mayor comprensión de los que son los certificados y como estos pueden ser operacionalizados en la Red de Blockchain, proporcionando una propuesta de aplicación que permite ejemplificar el uso de la tecnología de Blockchain en la emisión y almacenamiento de certificados.

Por tanto, a diferencia de los trabajos mencionados anteriormente, este proyecto de título analiza un software de desarrollo basado en Blockcert, que mediante el uso de redes de Bitcoin o Ethereum efectúa el almacenamiento y verificación de certificados institucionales emitidos. Además, para otorgar una mayor validez de la oportunidad y ventaja de esta tecnología, se realiza un estudio de costos basado en la rentabilidad y alcance del uso de una aplicación de este tipo en materia de certificados institucionales.

3.6 Especificación BLOCKCERT

Para el desarrollo de este proyecto se eligió BLOCKCERT debido a lo explicado en el punto 3.4. Por ende, se procede a exponer de forma más detallada el funcionamiento de esta aplicación además de concetos claves de su funcionamiento.

3.6.1 Información Técnica.

Para comprender el funcionamiento de BLOCKCERT es fundamental conocer sus tres tecnologías subyacentes, las cuales se explican a continuación:

a) **JSON-LD [17]*(JavaScript Object Notation for Linked Data).***

Consiste en un formato de datos especial derivado de JavaScript que permite el intercambio de información basada en texto. Este formato puede ser fácilmente leído y procesado por personas y máquinas. Es importante destacar que el archivo que se crea tiene una estructura

[17] https://json-ld.org/

de datos con el formato de *Open Badges Estándar* [18]con el cual se leen los datos y puedan ser reconocibles de una manera universal.

b) Hash.

Si bien el concepto de Hash fue explicado anteriormente en el capítulo de Marco Teórico, es necesario agregar que dentro del Blockcert se genera un hash de toda la información del certificado, el cual es incorporado a la red de Blockchain al momento de efectuar una transacción.

c) Sistema de verificación.

Este funciona en dos niveles. La primera de ellas es verificando el hash de la información comparada con la almacenada en la transacción de la red blockchain y la segunda es mediante la verificación del emisor de la credencial junto a la lista de certificados inválidos.

3.7 Procesos de validación

Una vez que se generan los certificados en formato json-ld, pasan por el proceso de hashing y luego son almacenados en la red de blockchain.

Posterior a ello, la aplicación de Blockcerts posee diversos procesos de validación, los cuales se explican a continuación:

3.7.1 Hashing

Para asegurar que la información de los certificados sea confidencial y almacenada en la Red de Blockchain se debe realizar un proceso *Hashing* al archivo *Json-ld,* este contiene la información relacionada al certificado (ver ilustracion N°8). La información pasa por un proceso de *Hashing* de tipo SHA256, el cual entrega como resultado una línea de caracteres que son almacenadas en la red de Blockchain.
En el caso que la información del certificado sea manipulada, es decir, que sea susceptible a modificaciones ya sea en el nombre o en cualquier otro ítem, el hash sufriría de una completa

[18] https://openbadges.org/

modificación, lo cual da a conocer que el certificado ha sido alterado en el proceso de verificación y por ello no se reconoce como un certificado válido.

Ilustración 9: Proceso de Hashing. Fuente: Elaboración propia.

3.7.2 Anchoring

Luego que el proceso de *Hashing* es completado se inicia un proceso de *Anchoring* para vincular el certificado y la transacción que contiene la información en blockchain (ver ilustración 9 y 10). Actualmente el proceso de *Anchoring* se efectúa tanto en la red de Bitcoin como en Ethereum.

El *Anchoring* complementa el proceso de verificación de *Hashing*, este se realiza al ingresar el hash del certificado en el campo de datos de la transacción de Blockchain, en el caso de Bitcoin se utiliza la operación *OP_RETURN* encima del campo de *script,* y en el caso de Ethereum solo se ingresa el Hash en el campo de datos, no siendo necesario ejecutar un contrato inteligente. Posterior a la transacción, se debe firmar y enviar a la Red de Blockchain y frente a ello se recibirá un ID de la transacción que debe ser ingresado dentro del certificado en el apartado *Anchors,* donde se encuentra la información de la transacción efectuada en la red de blockchain.

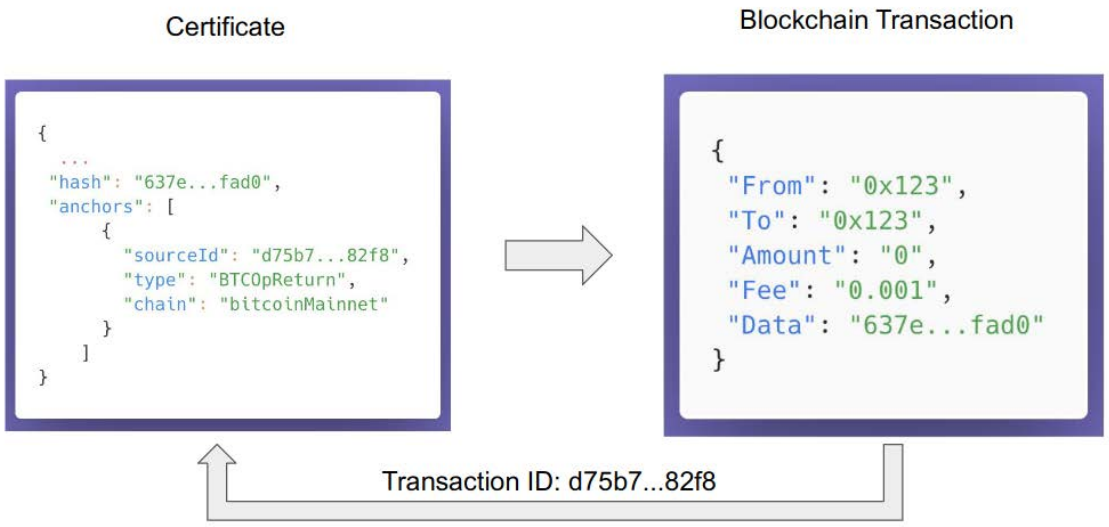

Ilustración 10: Proceso de anclaje bitcoin. Fuente: Elaboración propia.

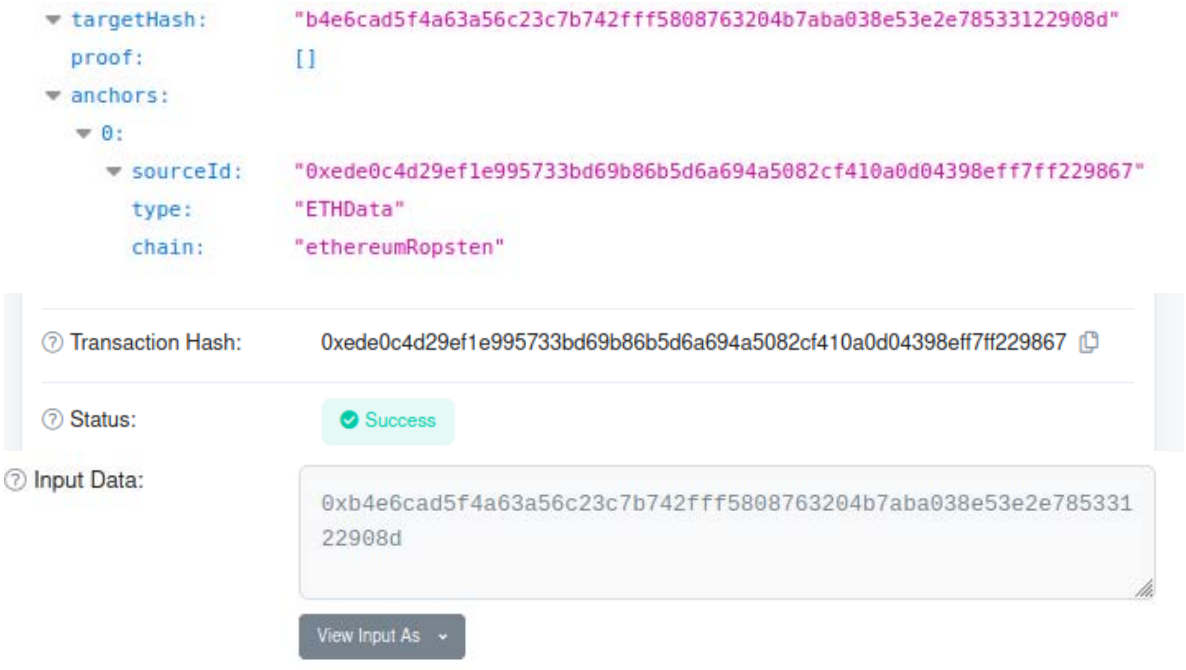

Ilustración 11: Proceso de anclaje Ethereum. Fuente: Elaboración propia

3.7.3 Validación de certificados

Para la validación de los certificados se utiliza el *Anchors* y se busca el ID de la transacción mediante la Red de Blockchain con el objeto de verificar que el campo de datos de la transacción tiene el mismo Hash que el señalado en el certificado y con ello se comprueba que el certificado es válido y no ha sido alterado desde que fue ingresado a la Red, además se tiene una lista de revocación, en la cual se almacenan los ID de los certificados que fueron revocados junto con su motivo de la revocación, esta lista es creada y modificada por el emisor de los certificados (ver ilustración 11).

Además, de verificar la inmutabilidad de los datos del certificado, Blockcerts ofrece otras alternativas:

a) Una de estas, es verificar quien es el emisor del certificado y así corroborar si es quien dice ser, evitando de esta manera que una persona suplante la información de otra.

b) Otra alternativa de validación, es revisar la clave pública de la institución que realizó el certificado y examinar si es igual a la clave pública que tiene la institución registrada como autor de certificado. En caso de ser diferente, es posible establecer que el certificado es falso, aunque esté en la red de blockchain y cumpla con los protocolos de Hash y de Ancla.

c) Y, por último, ofrece un proceso de validación mediante el uso de las revocaciones, las cuales se definen como una lista presente en un URL que está unida al perfil del autor de los certificados y contiene todos los ID de certificados revocados junto a su respectivo motivo del porqué.

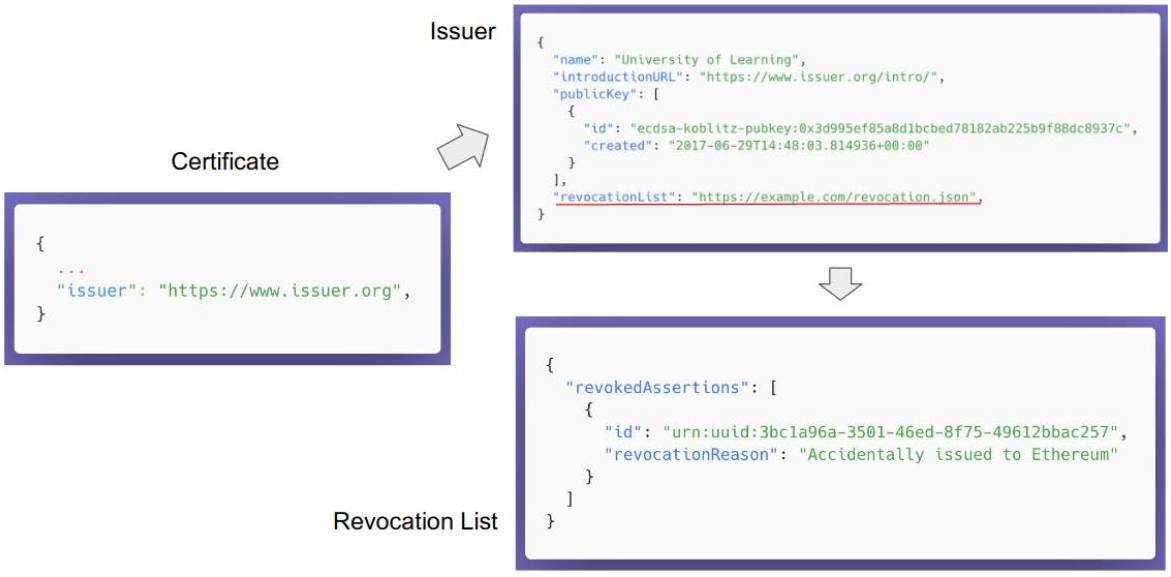

Ilustración 12: Validación de estado. Fuente: Elaboración propia.

3.8 Árbol de Merkel

Los procesos mencionados anteriormente de la aplicación de Blockcerts funcionan para el uso o manejo de solo un certificado, por tanto, en el caso de Instituciones como las Universidades donde se deben emitir certificados para cientos de estudiantes no es muy escalable su operacionalización ya que, si bien el costo es menor, se tiene que emitir solo un certificado a la vez, lo cual genera un considerable perjuicio en tiempo.

Es por ello que Blockcert propone a dichas Instituciones el uso del Mecanismo de Árbol de Merkel, el cual se utiliza en las Redes de Blockchain para la verificación de transacciones en bloques. De este modo, Blockcert usa la forma en que opera este mecanismo de árbol (ver ilustraciónN°12), donde los Hash de los certificados se ordenan en forma de árbol, etiquetando con el hash de la concatenación de los valores de sus nodos hijos. Todo aquello, permite que un gran número de datos separados puedan ser ligados a un único valor de hash, es decir, al hash en la raíz del árbol.

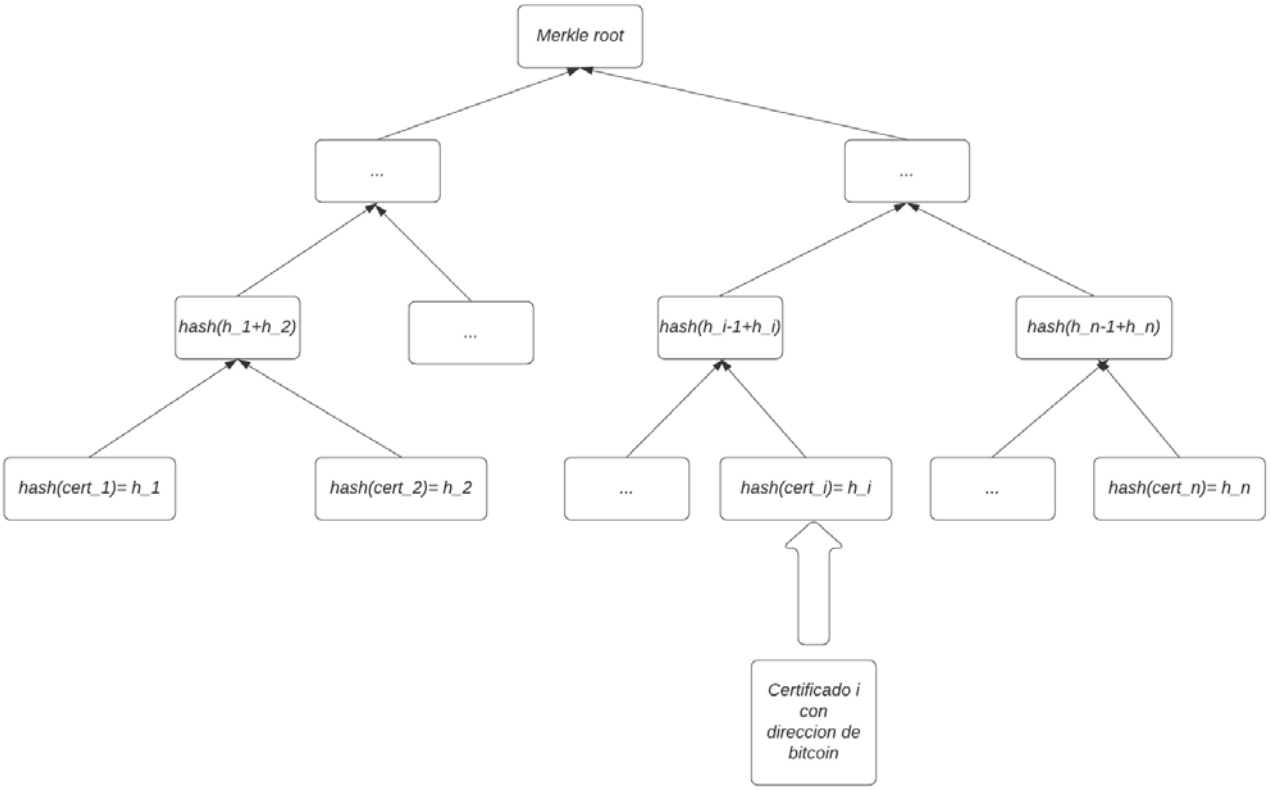

Ilustración 13: Merkle Tree. Fuente: Elaboración Propia

4 DESARROLLO DE LA SOLUCION

De acuerdo al análisis efectuado en la revisión bibliográfica se determinó que la manera más viable de desarrollar un prototipo para este proyecto es mediante una aplicación web montada en un servidor local con el objeto de evidenciar que la aplicación Blockcert es una alternativa factible para crear, validar y almacenar certificados en la red de blockchain.

4.1 Objetivos de la aplicación web

La aplicación web tiene como objetivo poder generar certificados en base a un archivo Excel con un listado de alumnos de forma sencilla para finalmente ser almacenados en la red de blockchain Ethereum, a pesar que la aplicación es un prototipo sirve como prueba de concepto ya que esta sube los certificados firmados a la red de blockchain.

4.2 Descripción de la aplicación web

La aplicación web está desarrollada con el *framework* Django, que utiliza el lenguaje de programación Python, en conjunto con las librerías de Blockcert.

Esta aplicación es montada en un servidor local y consiste en una página principal en donde se puede subir el listado de alumnos en un Excel y así la aplicación web genera un certificado para cada alumno de la lista para finalmente subir los archivos a la red de blockchain Ethereum.

4.2.1 Requerimientos

Al ser la aplicación web un prototipo, los requerimientos son escasos y generales.

Requerimientos Funcionales

- Se podrá subir un listado de alumnos propio (extensión csv)
- El sistema generar y subirá los certificados a la red blockchain
- El sistema debe mostrar los certificados generados

Requerimientos no funcionales

- La aplicación debe desarrollarse utilizando el *framework* Django.

4.2.2 Entorno de desarrollo

Para el desarrollo de la aplicación se utilizaron las siguientes herramientas:

- Equipo: DESKTOP
- Sistema operativo: Ubuntu 20.04
- Framework web Django, versión 2.4
- Editor de código Visual Studio Code
- Lenguaje de programación Python, versión 3.7
- Librerías de Python:
    - Cert-core
    - Cert-schema
    - Chainpoint
    - Configargagparse
    - Glob2
    - Mock
    - Pycoin
    - Pyld
    - Pysha3
    - Tox
    - Jsonchema
    - Coincurve
    - Ethereum
    - Rlp
    - jsonpath-rw

- Controlador de versiones Git - Github

4.2.3 Caso de uso

Se genero un caso de uso para el prototipo creado el cual permite al usuario generar certificados asociados a un listado de alumnos.

Nombre	Reconocer Listado
Descripción	Permite a un usuario generar certificados asociado a un listado de alumnos
Actores	Usuario

Usuario	Sistema
1.- el usuario sube el listado de alumnos a la plataforma	
	2.- la aplicación recibe los datos y crea los certificados en base al listado para luego subirlos a la red de blockchain ethereum. Luego muestra un listado del nombre de los certificados generados.
3.- El usuario, si lo desea, puede verificar los certificados a través de la página Blockcert	

4.3 Resumen de la Arquitectura Propuesta

Para el desarrollo de este proyecto se crea una aplicación web la cual se modela de acuerdo a lo que se observa en la ilustración 13.

El proceso de certificación se inicia enviando los datos desde la aplicación web al servidor, donde estos son procesados para luego ser creados con todas sus validaciones correspondientes. Y por último, se almacenan en la red de blockchain y así se envían los resultados a la aplicación web en donde se visualizan los certificados creados.

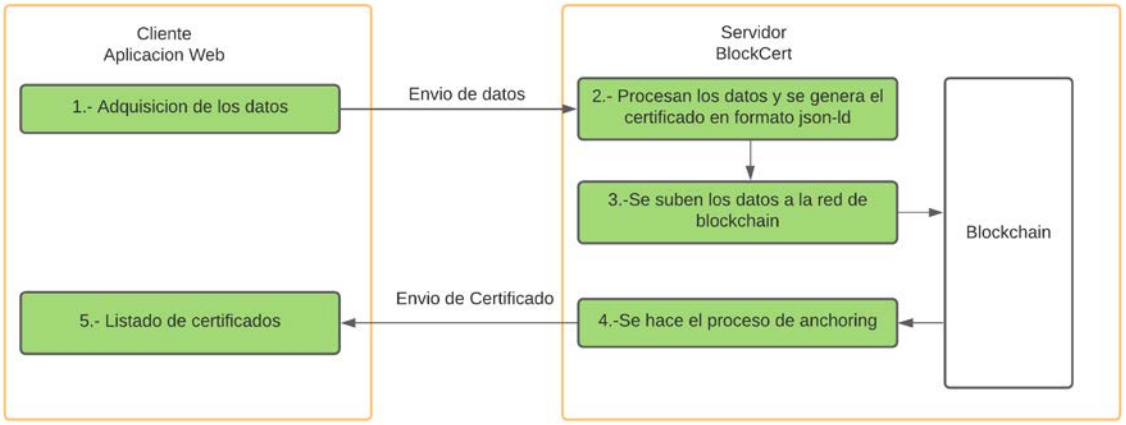

Ilustración 14: Arquitectura de la aplicación Fuente: Elaboración propia

5 IMPLEMENTACION

5.1 BlockChain

Para el desarrollo de este proyecto se identifican dos redes de blockchain que opera en Blockcert, estos son: Ethereum y Bitcoin.

Sin embargo, para efectos de esta investigación se selecciona la Red de Ethereum ya que los costos de transacciones son más baratos que los de la Red de Bitcoin. Además, el proceso de almacenamiento de datos que posee la Red Ethereum es más simple debido a que solo almacena el hash en el campo de datos de la transacción.

5.1.1 Ethereum

Para trabajar con esta red es necesario contar con una billetera de Ethereum que otorga una dirección pública a cada usuario y permite pagar los costos asociados a la creación de certificados.

La billetera de Ethereum (ver ilustración 14) se obtiene en la página Ethereumwallet [19]donde es necesario crear una cuenta. Para efectos de este proyecto, se crea una cuenta con la modalidad de *keyfile* que permite recuperar la billetera en caso de cualquier accidente.

Es importante destacar que el obtener una billetera de Ethereum no tiene ningún costo asociado y no requiere ningún documento.

[19] https://www.myetherwallet.com

Ilustración 15: Billetera Ethereum **Fuente:** Elaboración Propia

5.1.2 TESTNET *Ropsten* Ethereum

La Red de Blokchain de Ethereum tiene una red de prueba llamada *Rospen*. Esta red permite a los desarrolladores de Blockchain realizar pruebas reales con ETH ficticios bajo parámetros reales que utiliza la plataforma. Todo aquello permite tener una aproximación real de los costos asociados al procedimiento.

Por consiguiente, el proyecto utiliza la Red de *Rospen*, en donde se deposita 1 ETH a la cuenta principal con dirección "0xe259659bc8d92b97fe7a5295079a1a5bd3bf5d16" (ver Ilustración 15). Esto permite realizar las pruebas necesarias para el estudio.

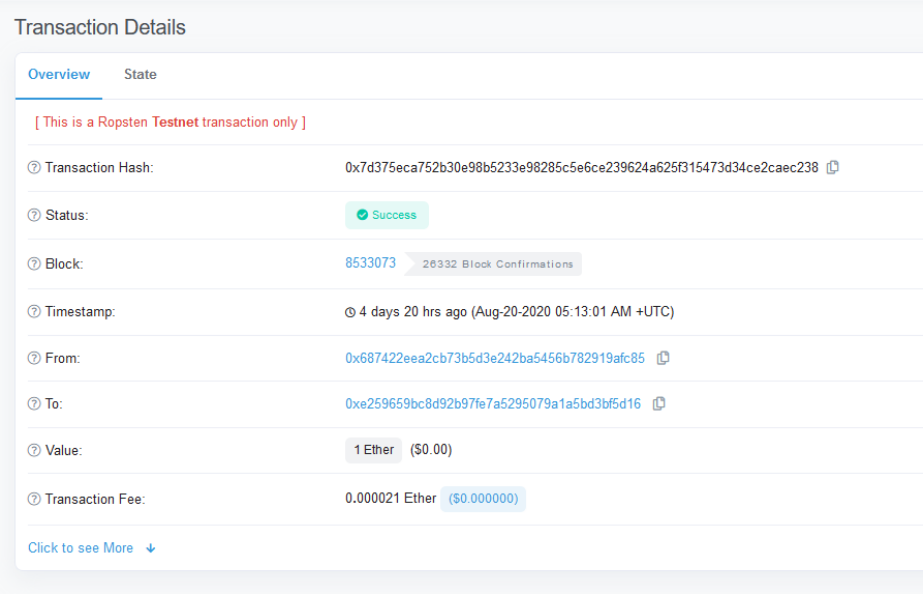

Ilustración 16: Transacción ETH Fuente: Elaboración propia

5.2 Credencial emisor

La aplicación de Blockcert identifica al emisor de los certificados mediante el archivo "json" alojado en algún servidor (ver ilustración 16), este archivo contiene toda la información relacionada al emisor del certificado y su atributo más importante es el Id de "*publicKey*", el cual otorga la identificación única del emisor. Además, este Id posee la lista de certificados revocados (ver ilustración 17), lo que garantiza el proceso de validación.

El proyecto en desarrollo, almacena su archivo "json" en *github* junto con la lista de certificados revocados.

```
{
  "@context": [
    "https://w3id.org/openbadges/v2",
    "https://w3id.org/blockcerts/v2"
  ],
  "id": "https://raw.githubusercontent.com/Raykhan12/Proyecto-de-titulo/master/issuer.json",
  "url": "http://www.ubiobio.cl/",
  "name": "Universidad del Bio Bio",
  "email": "ubb@ubiobio.cl",
  "image": "
  "publicKey": [
    {
      "id": "ecdsa-koblitz-pubkey:0xe259659bc8d92b97fe7a5295079a1a5bd3bf5d16",
      "created": "2020-08-24T01:06:00.642357+00:00"
    }
  ],
  "revocationList": "https://raw.githubusercontent.com/Raykhan12/Proyecto-de-titulo/master/revocation-list.json",
  "type": "Profile"
}
```


Ilustración 17: *issuer json* **Fuente:** Elaboración propia


```
{
    "@context": "https://w3id.org/openbadges/v2",
    "id": "https://raw.githubusercontent.com/Raykhan12/Proyecto-de-titulo/master/revocation-list.json",
    "type": "RevocationList",
    "issuer": "https://raw.githubusercontent.com/Raykhan12/Proyecto-de-titulo/master/issuer.json",
    "revokedAssertions": [{
        "id": "urn:uuid:3bc1a96a-3501-46ed-8f75-49612bbac257",
        "revocationReason": "Honor code violation"
      },
      {
        "id": "urn:uuid:eda7d784-c03b-40a2-ac10-4857e9627329",
        "revocationReason": "Issued in error."
      }
    ]
  }
```


Ilustración 18: *Revoke List* **Fuente:** Elaboración Propia

5.3 Receptor

Para recibir los certificados es importante descargar la aplicación de teléfono celular Blockcert *Wallet,* la cual consiste en una cartera que crea una cuenta en la Red de Bitcoin que permite recibir y ver los certificados en el móvil (ver Ilustración 18).

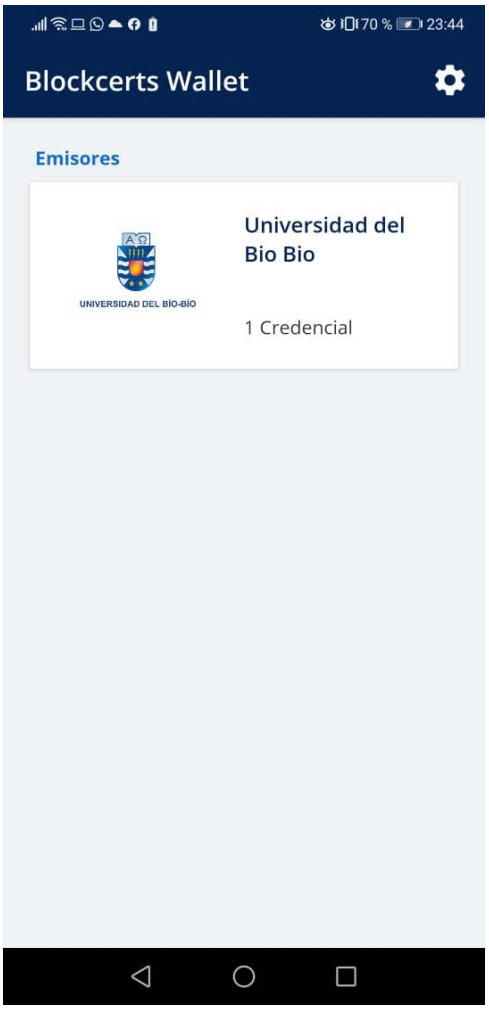

Ilustración 19: Blockcert *Wallet* **Fuente:** Elaboración propia

5.4 Plantillas

La aplicación Blockcert permite tener una plantilla de certificado con los atributos que se desea tener (ver ilustración 19). Es posible agregar algunos más específicos ya sea el RUT o algún otro atributo especial que la Institución estimare conveniente. Luego de crear la plantilla se utiliza un listado de alumnos con los cuales se generan los certificados finales por la aplicación.

Ilustración 20: Plantilla Certificado **Fuente:** Elaboración Propia

5.5 Certificados

Los certificados se diseñan con formato “json-ld” que contienen la información de los emisores del certificado, la información del receptor y la descripción del título junto con algunas imágenes esto se puede apreciar en la ilustración 20 y en la ilustración 21 se ve la vista grafica del certificado emitido.

```
@context:           [...]
type:               "Assertion"
displayHtml:        null
issuedOn:           "2020-08-24T21:10:44.090109+00:00"
id:                 "urn:uuid:0b8aa723-f7e6-4c69-bcf3-67397accdcbb"
recipient:
    type:           "email"
    identity:       "ramparra@alumnos.ubiobio.cl"
    hashed:         false
recipientProfile:
    type:           [...]
    name:           "Ramon Parra"
    publicKey:      "ecdsa-koblitz-pubkey:19L...XT1aVRmbhyJjZhh9b63dZvP"
badge:
    type:           "BadgeClass"
    id:             "urn:uuid:82a4c9f2-3588-457b-80ea-da695571b8fc"
    name:           "Certificado de la universidad del Bio-Bio"
    description:    "Se entrega un certificad... finalizar sus estudios"
    image:          "...0RnWjnMAAAAASUVORK5CYII="
    issuer:         {...}
    criteria:       {...}
    signatureLines: [...]
verification:
    type:           [...]
    publicKey:      "ecdsa-koblitz-pubkey:0xe...e7a5295079a1a5bd3bf5d16"
rut:                "18.146.466-6"
```


Ilustración 21: Certificado con datos **Fuente:** Elaboración propia

Ilustración 22: Vista grafica certificado **Fuente:** Elaboración propia

5.5.1 Certificados Firmados

Al subir el hash de los documentos a la red de blockchain se genera un Id de transacción (ver Ilustración 22), el cual se incorpora al certificado a través del Proceso de Anclaje y así se verifica que el certificado este almacenado en la Red de Blockchain.

Ilustración 23: Certificado Firmado **Fuente:** Elaboración propia

5.6 Verificación

Para efectos de esta prueba, se utiliza el verificador de la página web oficial de Blockcert, el cual realiza un proceso de validación que atraviesa diferentes etapas para finalmente corroborar si el certificado es válido, como se ve en la ilustración 23, o es rechazado. En caso de ser rechazado esta muestra un mensaje evidenciado en la Ilustración 24.

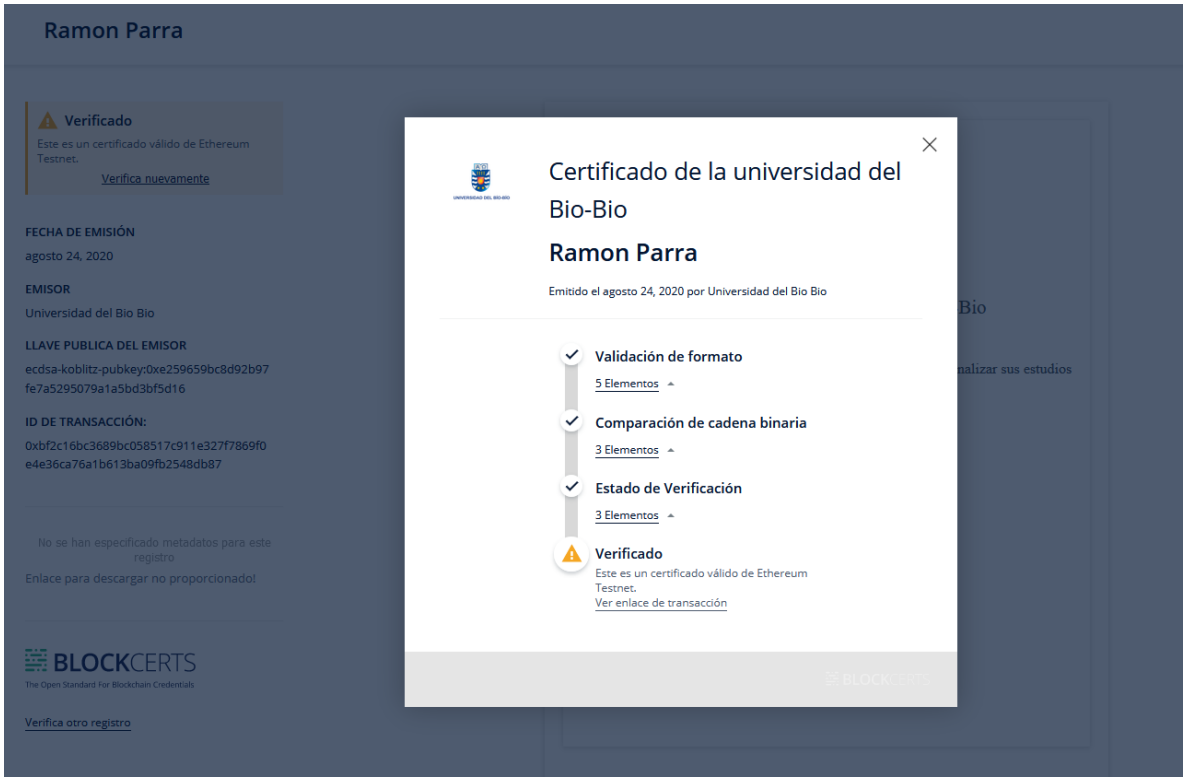

Ilustración 24: Certificado validado **Fuente:** Elaboración propia

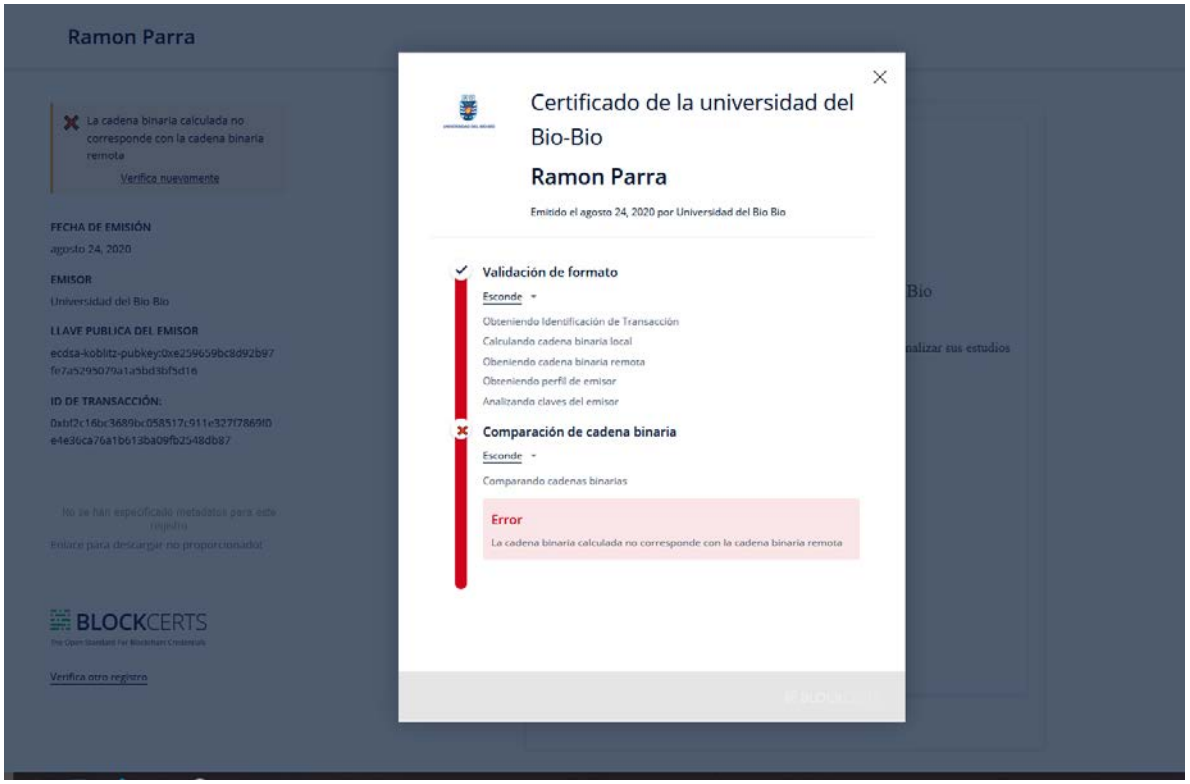

Ilustración 25: Certificado Rechazado **Fuente:** Elaboración propia

5.7 Funcionamiento aplicación web

La aplicación web tiene una vista principal, el cual se ve en la ilustración 25, en donde el usuario tiene la opción de buscar el archivo Excel en su computadora o puede arrastrar el archivo directo al navegador, en el cual tiene que hacer clic en "crear certificados blockchain" y así el programa genera los certificados y los sube a la red de blockchain. Posterior a ello, se muestra el listado de los certificados generados como se ve en la ilustración 26.

Finalmente, a modo de ejemplo se tomó uno de los certificados generados y se comprobó su validez usando la página web de Blockcert tal como se ve en la ilustración 27.

El tiempo estimado en que se demora en realizar la transacción va a variar dependiendo de qué tan ocupada este la red al momento de realizar la transacción, pero este tiempo es en promedio aproximadamente 5 minutos como se ve en la ilustración 29.

Ilustración 26: Página Principal Fuente: Elaboración Propia

Ilustración 27: Pagina con listado de certificados Fuente: Elaboración propia

Ilustración 28: Verificación certificado Fuente: Elaboración Propia

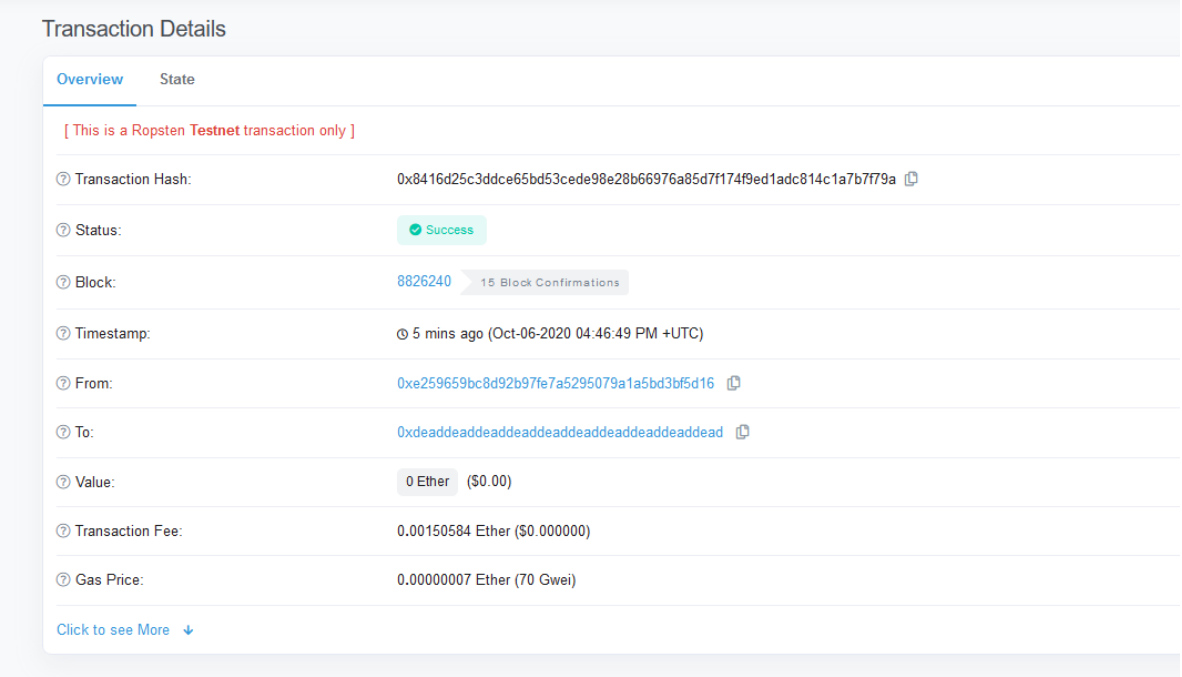

Ilustración 29: Tiempo de transacción Fuente: Elaboración propia

6 ANALISIS DE COSTOS

Los costos asociados a subir un certificado o un conjunto de certificados no varían, ya que solo se tiene que almacenar un hash gracias al árbol de Merkel. Para efectuar un cálculo de costos se debe utilizar la divisa que emplea la Red de Ethereum, es decir, el Ether (ETH).

El Ether (ETH) posee diversas unidades de medida, una de las más pequeñas es el "wei" donde 1.000.000.000.000.000.000 wei equivale a 1 eth. Otra unidad de medida es el "gwei" donde 1.000.000.000 equivale a 1 eth.

Junto con ello, es importante considerar que el costo de la transacción se va a ver afecto de acuerdo al "gas" que se utilice, este se define como la unidad de cálculo de trabajo más bajo dentro de la Red de Ethereum. Esto significa que mientras mayor ether se pague por gas la transacción tendrá más prioridad, siendo procesada de manera rápida.

Los valores en Gwei para efectos de una prioridad media alta con un rango entre 5 a 2 minutos de demora por transacción oscilan entre 50 a 100 Gwei como se puede observar en la ilustración 28.

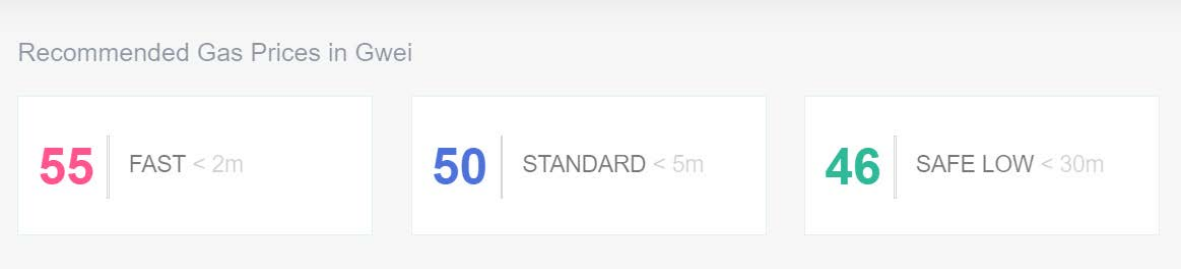

Ilustración 30: Precio del GAS Fecha:28-08-2020 Fuente: Elaboración propia

Actualmente el precio de 1 eth equivale a $ 310.932 pesos chilenos el cual será considerado para hacer los cálculos de la tabla 2

Tabla 2: Calculo de costos certificados blockchain Fuente: Elaboración propia

GAS	Costo Por Gas	ETH	CLP	Cantidad Certificados	Tiempo
21512	70 Gwei	0.00150584	$459	1	2 min
21512	70 Gwei	0.00150584	$459	6	2 min
21512	58 Gwei	0.0012477	$381	1	15 min
21512	58 Gwei	0.0012477	$381	6	12min

Como se observa en la tabla 2 los costos asociados a la cantidad de certificados almacenados mediante la red de blockchain son fijos teniendo un costo de $381 pesos chilenos.

Tabla 3: Gastos fijos blockchain vs certificado digital Fuente: Elaboración propia

	Costo Semanal	Costo Mensual	Costo anual
Blockchain	$381	$1524	$18288
Certificado digital	$491	$1966	$23600

En la tabla 3 es posible observar una comparativa de los costos fijos asociados a la creación de certificados mediante firma digital y a través la red de Blockchain.

Respecto a los costos variables asociados a la creación y almacenamiento de certificados digitales de la Universidad del Bío Bío, no se pudo realizar debido a la pandemia ocasionada por el COVID-19. Sin embargo, se deja abierto este ítem para que futuras investigaciones puedan tomar en consideración los resultados obtenidos de este informe y así continuar con mayor profundidad el estudio de costos y de factibilidad de ambas alternativas.

7 CONCLUSIONES

En base a lo desarrollado en el informe se demuestra que los objetivos planteados en un principio fueron logrados a excepción del ultimo el cual es análisis de costos que debido a la pandemia no se pudo realizar, pero se deja este ítem abierto a futuras investigaciones.

Según los objetivos desarrollados es posible establecer que la tecnología de Blockchain es una alternativa viable para el manejo de certificados emitidos por Instituciones tales como la Universidad del Bío Bío, Esto se evidencia mediante el prototipo creado, donde se identifica que dicha tecnología posee un alcance de crear, almacenar y validar certificados tanto para una persona como para un grupo.

Respecto a la factibilidad de implementación del uso de esta tecnología en la Universidad del Bío Bío es alta debido a que el software puede operar a través de dockers, los cuales ya están en funcionamiento dentro de los servidores de la Casa de Estudios. Esto implica que la Institución ya cuenta con el hardware y software necesario para la implementación.

Sin embargo, como limitaciones de la tecnología de Blockchain se identifica en primer lugar que el proceso de certificados no está completamente implementado dentro de la red de blockchain ya que la información del creador y el listado de certificados revocados requieren de un servidor propio para su almacenamiento puesto que en la red de Blockchain la información que se maneja es inmutable y encriptada. Esta limitación evidencia una falta de autosuficiencia que presenta el Sistema de certificación en la red de blockchain.

Otra limitante es el desconocimiento respecto al uso de esta tecnología en materia de certificación ya que existe escasa bibliografía y trabajos de investigación en Chile que profundicen respecto al uso de la Red de Blockchain. Todo aquello se debe a que esta tecnología posee un desarrollo incipiente en Chile.

A pesar de estas limitaciones, se concluye que la Red de Blockchain es una alternativa viable para el manejo de certificados ya que el prototipo desarrollado con la base de la Aplicación Blockcert demuestra que es posible crear, almacenar y validar los certificados de una institución educacional en esta red. De esta manera, el prototipo creado es escalable a un Docker para futuras pruebas en la universidad, pero producto de la pandemia por COVID-19 y falta de tiempo no fue desarrollado en la presente investigación.

La tecnología de Blockchain va cada día mejorando su desarrollo y en ese sentido el proyecto de la aplicación de Blockcert busca expandir su aplicación a cualquier red de Blockchain, lo cual abre paso a la creación de una red de este tipo en la Universidad del Bío Bío que pueda

solucionar las limitaciones señaladas anteriormente y espero continuar con el desarrollo de este proyecto para poder ver su implementación y aportar al futuro de esta tecnología.

8 BIBLIOGRAFÍA

Ali, M, Nelson, J., Blackstein, A., Shea, R., & Freedman, J. (2019). Whitepaper Técnico de. *Blockstack PBC*, 25.

Ali, Muneeb, Nelson, J., Shea, R., & Freedman, M. J. (2016). Blockstack: A global naming and storage system secured by blockchains. *Proceedings of the 2016 USENIX Annual Technical Conference, USENIX ATC 2016*, 181–194.

Álvarez, L. (2018). Analisis de la tecnlogía Blockchain, su entorno y su impacto en modelos de negocios. Universidad Técnica Federico Santa María.

Bartolomé, A., & Moral-Ferrer, J. (2018). Blockchain en educación. Colección Transmedia XXI, 211. http://www.ub.edu/ire/en/new-book-blockchain-en-educacion-cadenas-rompiendo-moldes/

BLOCKCERTS. (2016). https://www.blockcerts.org/guide/

BLOCKCRED. (n.d.). https://www.blockcred.io/

Cámara, R. (2018). *Estudio de tecnologías Bitcoin y Blockchain* [Universidad Oberta de Catalunya]. http://dg3.dtrt.org/files/bitcoin-paper/bitcoin_es_latam.pdf

EMERCOIN. (2018). EMERCOIN White Paper. In *emercoin.com*.

Gallardo, I. (2018). Tesis de maestría. *TED: Tecné, Episteme y Didaxis*, *20*. https://doi.org/10.17227/ted.num20-1065

Ganne, E. (2018). ¿Pueden las cadenas de bloques revolucionar el comercio internacional?. Organización Mundial del Comercio. https://doi.org/10.30875/77daeaf7-es

Herrera, C. (2018). *¿Qué es Proof of Work y Proof of Stake?* Tekcrispy.Com. https://www.tekcrispy.com/2018/03/03/proof-of-work-stake-pow-pos/

[Introducción a las Redes Peer-to-Peer]. (s.f). Binance Academy. Recuperado de: https://academy.binance.com/es/blockchain/peer-to-peer-networks-explained

Jimenez, D. (2020). La mala gestión del cambio es el enemigo de la adopción de Blockchain. *Es.Cointelegraph.Com*. https://es.cointelegraph.com/news/mismanagement-of-change-is-the-enemy-of-blockchain-adoption

Maldonado, J. (2020). ¿Qué es un hash? Es.Cointelegraph.Com. https://es.cointelegraph.com/explained/whats-a-hash

Nakamoto, S. (2013). Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario. Introducción Transacciones, 1–9. http://dg3.dtrt.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Nakamoto, S. (2008). Bitcoin: un sistema de dinero en efectivo electrónico peer -to -peer. Www.Bitcoin.Org, 1–9. https://bitcoin.org/files/bitcoin-

paper/bitcoin_es.pdf%0Awww.bitcoin.org

Redacción APD. (2019). 7 aplicaciones de la tecnología blockchain. *Https://Www.Apd.Es*. https://www.apd.es/aplicaciones-blockchain/

S.A. (2016). *Criptografía simétrica y asimétrica*. https://ciclosistemasmicroinformaticosjessbuenoperales.wordpress.com/2016/03/04/criptografia-simetrica-y-asimetrica/

S.A. (2018). *Los usos del blockchain en logística*. Stocklogistic.Com. https://www.stocklogistic.com/blockchain-logistica/