



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Ciencias y Sistemas

**BLOCKCHAIN Y LA
IDENTIFICACIÓN DIGITAL UNIVERSAL**

Henry Oswaldo Taracena Ramirez

Asesorado por el Ing. Álvaro Giovanni Longo Morales

Guatemala, julio de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**BLOCKCHAIN Y
LA IDENTIFICACIÓN DIGITAL UNIVERSAL**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

HENRY OSWALDO TARACENA RAMIREZ

ASESORADO POR EL ING. ALVARO GIOVANI LONGO MORALES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERIA EN CIENCIAS Y SISTEMAS

GUATEMALA, JULIO DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Christian Moisés De La Cruz Leal
VOCAL V	Br. Kevin Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. Cesar Rolando Batz Saquimux
EXAMINADOR	Ing. Cesar Augusto Fernández Cáceres
EXAMINADORA	Inga. Devora Emperatris Meza Orellana
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

BLOCKCHAIN Y LA IDENTIFICACIÓN DIGITAL UNIVERSAL

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería de Ciencias y Sistemas, con fecha julio de 2020.

Henry Oswaldo Taracena Ramirez



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias y Sistemas

Guatemala, 26 de febrero de 2021

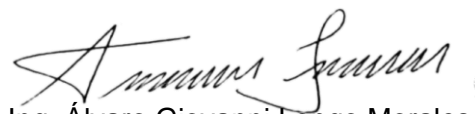
Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Área de trabajos de Graduación

Respetable ingeniero Azurdia:

Por este medio informo que he revisado y aprobado el trabajo de investigación titulado: **“BLOCKCHAIN Y LA IDENTIFICACION DIGITAL UNIVERSAL”**, que fue desarrollado por el estudiante **Henry Oswaldo Taracena Ramirez**, quien se identifica con el **código único de identificación (CUI) 2088826180101** y **registro académico 201020726**, y a mi criterio, el mismo cumple con los objetivos propuestos para su Desarrollo según el protocolo.

Agradeciendo su atención a la presente.

Atentamente.


Ing. Álvaro Giovanni Longo Morales
Asesor de trabajo de graduación
Colegiado: 15,845

Alvaro Giovanni Longo Morales
Ingeniero en Ciencias y Sistemas
Colegiado No. 15,845



Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 2 de marzo de 2021


Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **HENRY OSWALDO TARACENA RAMIREZ** con carné **201020726** y CUI **2088 82618 0101** titulado "**BLOCKCHAIN Y LA IDENTIFICACIÓN DIGITAL UNIVERSAL** " y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,


Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación



UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación “BLOCKCHAIN Y LA IDENTIFICACIÓN DIGITAL UNIVERSAL”, realizado por el estudiante, HENRY OSWALDO TARACENA RAMIREZ aprueba el presente trabajo y solicita la autorización del mismo.

“ID Y ENSEÑAD A TODOS”

A handwritten signature in black ink over a circular official stamp. The stamp contains the text "UNIVERSIDAD DE SAN CARLOS DE GUATEMALA" and "DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS".

Msc. Carlos Gustavo Alonzo
Director

Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 08 de julio de 2021

DTG. 286.2021.

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **BLOCKCHAIN Y LA IDENTIFICACIÓN DIGITAL UNIVERSAL**, presentado por el estudiante universitario: **Henry Oswaldo Taracena Ramirez**, y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:



Inga. Anabela Cordova Estrada
Decana



Guatemala, julio de 2021.

AACE/asga

ACTO QUE DEDICO A:

Dios	Por darme la vida, la fuerza, el conocimiento y la posibilidad de culminar mi carrera.
Mis padres	Alba Ramirez y Henry Taracena. Por darme su amor, compartirme su fe en Dios y apoyo incondicional.
Mi esposa	Amy Flores, por estar siempre a mi lado, darme su amor, amistad, sus consejos, su apoyo y siempre compartir su felicidad conmigo.
Mis hermanas	Amanda Julisa, Wendy Elisa y Albi Tatiana Taracena, por apoyarme siempre, darme ánimos y compartir cada momento.
Mis sobrinos	Por darme siempre momentos de felicidad, alegría y esperanza.
Mis abuelos	Por siempre creer en mí y darme amor incondicional.
Mis amigos	Por compartir cada experiencia y vivencia durante mi carrera.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por permitirme formarme como profesional dentro de las aulas de la universidad.
Facultad de Ingeniería	Por permitirme estudiar la carrera de Ingeniera en Ciencias y Sistemas, dentro de la prestigiosa facultad de Ingeniería a la cual horrare con mi desempeño profesional desde este momento.
Mi asesor	Ing. Álvaro Longo, por su dedicación, consejos y apoyo en la realización del presente trabajo de graduación.
Mis compañeros de la Facultad	Por compartir las diferentes cátedras y grandes experiencias.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	IX
LISTA DE SÍMBOLOS	XI
GLOSARIO	XIII
RESUMEN	XV
OBJETIVOS.....	XVII
INTRODUCCIÓN.....	XIX
1. ANTECEDENTES	1
1.1. Derechos Humanos	1
1.2. Blockchain.....	1
1.3. Investigaciones y sistemas con precedentes	1
1.3.1. La Identidad económica de BANQU.....	2
1.3.2. Validated ID	2
1.4. Plataformas de Criptomonedas Basadas en Blockchain	3
1.4.1. Criptomoneda	3
1.4.2. Monedero Virtual	3
1.4.3. Bitcoin	4
1.4.4. Ethereum	4
1.5. Tokens No Fungibles	5
1.5.1. Campos de aplicación	6
2. MARCO TEORICO CONCEPTUAL	7
2.1. Identidad un derecho universal.....	7
2.2. Artículo 7 - Convención de los derechos del Niño.....	8
2.3. Marco Legal Nacional	8

2.3.1.	Ley del Registro Nacional de las Personas RENAP decreto número 90-2005.....	9
2.3.1.1.	Capítulo X: De las Inscripciones en el Registro Civil de las Personas	9
2.3.1.1.1.	Artículo 67. Registro Civil de las Personas.	9
2.3.1.1.2.	Artículo 68. Obligatoriedad.	9
2.3.1.1.3.	Artículo 70. Inscripciones en el Registro Civil de las Personas.....	10
2.3.1.1.4.	Artículo 71. Inscripciones de nacimiento.....	11
2.3.2.	Ley de nacionalidad decreto número 1613	11
2.3.2.1.	Capitulo I	11
2.3.2.1.1.	Artículo 1.....	12
2.3.2.1.2.	Artículo 3.....	12
2.3.2.1.3.	Artículo 5.....	12
2.3.2.1.4.	Artículo 6.....	12
2.3.2.2.	Capitulo II Competencia y Procedimientos Generales.....	13
2.3.2.2.1.	Artículo 9.....	13
2.3.2.3.	Capitulo IV Naturalizacion Concesiva..	13
2.3.2.3.1.	Artículo 32.....	13
2.3.2.4.	Capitulo IX Disposiciones Relativas al orden Internacional.....	14
2.3.2.4.1.	Artículo 70.....	14

2.3.3.	Constitución Política de la Republica de Guatemala	14
2.3.3.1.	Capitulo II Nacionalidad y Ciudadanía	14
2.3.3.1.1.	Artículo 144. Nacionalidad de origen.	15
2.3.3.1.2.	Artículo 145. Nacionalidad de centroamericanos.	15
2.3.3.1.3.	Artículo 146. Naturalización.	15
2.3.3.1.4.	Artículo 147. Ciudadanía.....	16
2.3.3.1.5.	Artículo 148. Suspensión, pérdida y recuperación de la ciudadanía.	16
2.3.4.	Código Civil.....	16
2.3.4.1.	Capitulo I De Las Personas Individuales.....	16
2.3.4.1.1.	Artículo 1. (Personalidad).....	17
2.3.4.1.2.	Artículo 4.....	17
2.3.4.1.3.	Artículo 5.....	17
2.4.	Identidad Digital	18
2.5.	Tecnología de la información.....	19
2.6.	Almacenamiento de datos	20
2.7.	Datos.....	20

2.8.	Información	20
2.9.	Bases de datos	21
2.9.1.	Base de datos Centralizada	21
2.9.2.	Base de datos Descentralizada.....	21
2.9.3.	Base de datos Distribuida.....	21
2.10.	Red.....	22
2.11.	Sistema	23
2.12.	Sistema Informático	23
2.13.	Plataforma.....	23
2.13.1.	Plataforma Cruzada.....	24
2.14.	Arquitectura de Software	24
2.15.	Blockchain.....	25
2.15.1.	Origen	25
2.15.2.	Definición	26
2.15.3.	Operabilidad	26
2.15.4.	Transparencia.....	27
2.15.5.	Componentes	27
2.15.5.1.	Bloque	27
2.15.5.2.	Mineros.....	28
2.15.5.3.	Red de Nodos	28
2.15.6.	Características.....	29
2.15.6.1.	Descentralizada.....	29
2.15.6.2.	Sistema abierto	30
2.15.7.	Seguridad	30
2.15.8.	Token ERC-721	31
2.15.8.1.	Funciones asociadas al Token ERC-721	31
2.16.	Privacidad	32
2.16.1.	Privacidad en el ámbito digital.....	32

2.17.	Documento de identidad	33
2.18.	Reglamento general de protección de datos	34
2.18.1.	Derechos del reglamento.....	35
2.18.1.1.	Derecho de eliminación	35
2.18.1.2.	Derecho a la portabilidad	35
2.18.1.3.	Derecho de acceso.....	35
2.19.	Biométrica	36
2.19.1.	Tecnología Biométrica	36
2.19.2.	Beneficios de la tecnología biométrica	37
3.	NORMAS Y FUNDAMENTOS DE IDENTIDAD DIGITAL	
	UNIVERSAL.....	39
3.1.	Identidad digital universal en una plataforma blockchain.....	39
3.2.	Seguridad de la Identidad Universal.....	40
3.3.	Participantes de la plataforma	40
3.3.1.	Ente Rector	40
3.3.1.1.	Funciones del ente rector.....	41
3.3.1.2.	Ente rector propuesto.....	42
3.3.2.	Entidades Asociadas	42
3.3.2.1.	Funciones de entes asociadas.....	43
3.3.3.	Usuarios.....	43
3.3.3.1.	Operaciones permitidas por los usuarios	44
3.3.4.	Entidades terceras.....	44
3.4.	Abolición de Robo Identidad.....	44
3.5.	Documentos como medida alterna de identificación	45
3.6.	Pilares fundamentales de la Identidad Digital Universal	45

4.	RESULTADO DE DISEÑO DE LA PLATAFORMA IDENTIDAD DIGITAL UNIVERSAL.....	47
4.1.	Estructura de funcionamiento de la plataforma de Identidad Digital Universal.....	47
4.1.1.	Descripción general de interacciones	47
4.2.	Estandarización de información	48
4.2.1.	Estándar Propuesto	49
4.3.	Restricción de acceso a información.....	49
4.3.1.	Roles.....	49
4.3.1.1.	Consulta Usuario Civil.....	50
4.3.1.2.	Consulta Tercero.....	50
4.3.1.3.	Operador Asociado de Registro.....	50
4.3.1.4.	Operador Asociado de Certificación	50
4.3.1.5.	Operador Asociado de Reportes.....	51
4.3.1.6.	Roles de Desarrollo Asociados	51
4.3.1.7.	Roles del ente rector	51
4.4.	Operaciones de la plataforma de Identificación digital universal.....	52
4.4.1.	Registro de personas	53
4.4.2.	Registro de relaciones.....	53
4.4.3.	Generación de certificaciones	54
4.5.	Lenguaje	54
4.6.	Servicios Web.....	54
4.7.	Estructuración de Datos	55
4.7.1.	Smart Contract para la plataforma de identidad digital universal.....	56
4.8.	Arquitectura.....	69

CONCLUSIONES 73
RECOMENDACIONES..... 75
BIBLIOGRAFÍA..... 77

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Comparativa de tipos de bases de datos	22
2.	Diagrama base de Blockchain	26
3.	Diagrama de arquitectura, Identidad Digital Universal en Blockchain ..	48
4.	Distribución de nodos con base de datos.....	69
5.	Contenido de un nodo de la plataforma	70
6.	Interacción de entes asociados con la plataforma de Identidad digital universal.....	71

TABLAS

I.	Denominaciones de documentos de identidad	33
II.	Confiabilidad de medios biométricos.....	37
III.	Smart Contract Universal Identification	56

LISTA DE SÍMBOLOS

Símbolo	Significado
!=	Diferente de
ID	Identificador
==	Igual que
=>	Mapear datos

GLOSARIO

Carné	Documento expedido a favor de una persona, generalmente en forma de tarjeta y provisto de su fotografía, que sirve para acreditar su identidad, su pertenencia a un colectivo o su facultad para realizar una actividad.
Carné de Identidad	Destinado a acreditar oficialmente la identidad del titular.
Ethereum	Plataforma de blockchain, que permite la creación de criptomonedas y Smart Contracts.
Fungible	Las unidades individuales de un activo son intercambiables y, esencialmente, indistinguibles unas de otras.
P2P	Tecnología de transmisión de datos por medio de orígenes de datos llamados semillas.
Registro Civil	Registro en que se hacen constar por autoridades competentes los nacimientos, matrimonios, defunciones y demás hechos relativos al estado civil de las personas.

Smart Contract

Contrato inteligente con el que desarrollan las estructuras de los nodos, en la plataforma Ethereum.

Token

Un token es una unidad de información dentro de un sistema basado en contratos inteligentes.

RESUMEN

El tema propuesto para el trabajo de graduación busca demostrar las ventajas y desventajas para la autenticación de una identidad digital universal, siendo un derecho universal generando una independencia de los registros físicos y documentos de identificación, internacionalizando el ID digital y rompiendo fronteras. Así mismo poder legalizar cualquier tipo de documento jurídico a través de una firma digital universal. Todo esto gracias a las bondades del blockchain en donde la información es descentralizada y la consistencia de los datos no se ve afectada debido a la numerosa cantidad de nodos de información. Se buscaría explicar la tecnología y como esta se acoplará a la identidad universal, la cual debe ser un derecho para toda persona. Exponer la seguridad en un sistema de identidad universal para evitar ataques informáticos y suplantación de personas. Enfocar el paradigma de descentralización de la información de personas en un ámbito donde no dependa de grandes compañías en sus granjas de servidores si no en una red creciente y pujante como blockchain.

OBJETIVOS

General

Demostrar la importancia de un registro de identidad digital, universal, segura y distribuida en una plataforma de blockchain, por sobre los métodos tradicionales de registros de personas que se utilizan globalmente. Resaltar la importancia de una plataforma no centralizada y que cada persona tenga una identidad y pueda ser reconocida según la misma, sin la dependencia de un documento físico.

Específicos

1. Demostrar la importancia de la identidad para cada persona.
2. Plantar las bases de una plataforma de identidad digital en blockchain.
3. Demostrar las ventajas de la utilización de una plataforma descentralizada.
4. Demostrar las ventajas de la identidad digital en comparación con los registros civiles.
5. Proponer un sistema de identidad digital distribuido, en tecnología blockchain.

INTRODUCCIÓN

La identidad es una parte importante de cada ser humano, esta se vuelve inherente en ambientes cívicos y políticos. Cada individuo tiene el derecho de ser identificado ante la sociedad y cada gobierno está obligado a proveer este bien tanpreciado para la sociedad moderna.

En la actualidad los sistemas de identificación en las diferentes naciones se encuentran descentralizados y dependen intrínsecamente de la impresión de documentos, tarjetas de identificación y otros medios físicos para constar el registro de una persona ante la sociedad.

Con el avance tecnológico, hay nuevas formas de innovación para proveer a las personas de sus derechos básicos como lo es la identidad, e independizarse de los medios físicos, por tal motivo nace la propuesta de una la identificación digital distribuida en una plataforma de blockchain.

La plataforma de blockchain distribuida brinda diferentes ventajas para vincular la identidad digital. Una plataforma más segura, accesible desde cualquier lugar con los requerimientos básicos al sistema propuesto. Esta plataforma ayuda al cumplimiento de derechos básicos para el ser humano.

1. ANTECEDENTES

1.1. Derechos Humanos

Se entiende como Derechos Humanos al conjunto de derechos y libertades básicas que poseen todas las personas por su condición humana y que le garantizan una vida digna. Son independientes del estatus, sexo, etnia o nacionalidad. Se clasifican en derechos de tres generaciones, la primera generación se relaciona con los derechos civiles y políticos básicos de las personas; la segunda generación con los derechos económicos, sociales y culturales; y tercera, con los derechos de los pueblos.

1.2. Blockchain

Es una cadena de Datos contenida, en donde se agrupan en conjuntos de bloques, a estos se les asignan metadatos los cuales anclan la información del bloque al bloque anterior de la cadena, por lo que sella la información contenida en él. La información contenida en los bloques solo puede ser modificada por sí y sólo si se modifican los bloques posteriores, por lo que esto hace que la cadena de bloques sea una cadena distribuida, no relacional que contenga históricos irrefutables de información.

1.3. Investigaciones y sistemas con precedentes

Existen diferentes plataformas, investigaciones y sistemas que están basados en la tecnología de blockchain con fines privados en instituciones

financiarías, de autenticación de firmas y otros fines. Estos sirven de base y experiencia para la implementación de una plataforma de identificación universal.

1.3.1. La Identidad económica de BANQU

Conectar a los “invisibles” a la economía global mediante una identidad digital es la misión de BanQu, la primera plataforma blockchain para la identidad económica. De acuerdo con su sitio web, casi 2.700 millones de personas en todo el mundo no tienen acceso a servicios bancarios y para sus creadores, la identidad es la clave para acabar con la pobreza y para reafirmar la dignidad humana. El proyecto, que fue creado en el 2012, lanzó su plataforma blockchain el año 2017, con el objetivo de brindar una identidad segura y portable fundamentada en registros personales y financieros, haciendo uso de la tecnología de contabilidad distribuida.

1.3.2. Validated ID

ViDChain basado en tecnología blockchain, un sistema de transmisión de datos digitales entre usuarios que varios expertos apuntan a que es el inicio de la cuarta revolución industrial. Con ViDSigner hemos logrado consolidarnos con un excelente servicio de firma electrónica. Ahora hemos decidido dar un paso más para otorgarle al usuario la libertad absoluta sobre su identidad digital.

ViDChain permite al usuario gestionar su identidad digital y los atributos que lo conforman de forma descentralizada, permitiendo la validación de identidades en procesos de onboarding.

1.4. Plataformas de Criptomonedas Basadas en Blockchain

Actualmente existen diferentes plataformas basadas en criptomonedas, las cuales utilizan la tecnología de blockchain. Las cuales han dado pie a el intercambio de valores entre las personas, de manera electrónica y sin intervención de entidades financieras que sean legisladas, reguladas y rindan cuentas ante gobiernos y otras instituciones regulatorias por región o país.

1.4.1. Criptomoneda

Una criptomoneda es un medio de intercambio digital, el cual se puede denominar como dinero en la red, aunque generalmente estos no se encuentran regulados por un ente financiero, un banco central o algún gobierno.

Las criptomonedas fueron ideadas como una forma de pago, en tiendas en línea o de intercambio entre personas independientes, más recientemente hay entidades que ya implementaron el método de pago por medio utilización de POS y tarjeta de débito del monedero virtual de la criptomoneda, el valor de las criptomonedas no está ligadas a ninguna economía en concreto.

1.4.2. Monedero Virtual

El monedero virtual es un espacio en donde se almacenan por medio de un método de encriptación la cantidad de Criptomonedas que posee un determinado usuario de la plataforma.

1.4.3. Bitcoin

Bitcoin es una plataforma basada en blockchain, la cual actualmente es la más utilizada y cada día hay más personas uniéndose a la plataforma, la cual tiene el valor más elevado en el mercado actualmente y se mantiene al alza. Esta plataforma permite el intercambio de criptomonedas; esta plataforma en esencia es una red P2P, que está sustentada en el block y se puede definir como un libro contable, que es público y accesible para todos los usuarios de la plataforma, el cual contiene la información histórica de todas las transacciones.

El nombre que recibe la criptomoneda dentro de la plataforma de Bitcoin es bitcoin, está tiene un gran valor especulativo en el mercado, por lo que puede sufrir cambios bruscos a través del tiempo, el valor máximo registrado se ha posicionado cerca de los 20 mil dólares estadounidenses en diciembre de 2017 y llegando a bajar hasta un precio de 6 mil dólares estadounidenses en el año 2018.

1.4.4. Ethereum

Ethereum es una plataforma basada en la utilización del modelo blockchain, la misma utiliza una criptomoneda llamada “ether”, esta igual puede ser utilizada como medio de intercambio, y también sirve como para compensar a las personas encargadas de la minería de los nodos.

La plataforma Ethereum no se limita únicamente a las criptomonedas, amplía su propósito a la creación de contratos inteligentes y a la publicación de aplicaciones que sirvan para la creación de contratos inteligentes.

El proyecto de Ethereum en su propósito general propone la descentralización de la web por medio de cuatro componentes básicos; publicación de contenido estático, mensajes dinámicos, transacciones confiables y una interfaz de usuario integrada y funcional.

1.5. Tokens No Fungibles

Los tokens, no fungibles son una especialización, de los tokens para la utilización de la plataforma Ethereum, la cual tiene la peculiaridad, que puede generar tokens únicos, y no fuerza a que todos los tokens mantengan las mismas propiedades.

Generalmente se utilizan como tokens coleccionables, estos pueden poseer características únicas, por lo cual pueden ser propiamente utilizables para añadir características extras, a un núcleo básico de características, que delimiten un objeto base o entidad base.

Un token no fungible puede representar una entidad u objeto del mundo real, dividiendo el mismo en varios tokens, haciendo que el conjunto de estos, hagan la totalidad de la entidad u objeto. El mismo puede dividir tanto su valor económico, como su representación conceptual. La versatilidad de manejar diferentes conceptos, bajo una estructura base, hacen que los tokens no fungibles tengan un amplio campo de aplicación.

Existen distintos esquemas para crear y emitir Tokens no fungibles. El más utilizado de éstos es el ERC-721, un estándar para la emisión y trading comercio de activos no fungibles en la blockchain de Ethereum.

La creación de tokens no fungibles basados en blockchain permite propiedad física, como:

- Casas, obras de arte, y vehículos.
- Coleccionables virtuales (tarjetas coleccionables)
- Activos con valor negativo (préstamos)

1.5.1. Campos de aplicación

Los tokens no fungibles pueden ser utilizados por plataformas descentralizadas de información, para emitir artículos digitales únicos y cripto-coleccionables. Los cuales pueden ser un objeto coleccionable, un producto de inversión u otra cosa.

Los juegos incrementan el uso de implementación de su propia economía. Muchas plataformas de videojuegos ya han dado el paso a crear sus propias economías, utilizando blockchain para convertir tus activos en tokens.

La utilización de los tokens para plataformas totalmente digitales está en auge, la representación de activos del mundo real es cada vez más inminente. Estos Tokens No Fungibles pueden representar fracciones de activos del mundo real que pueden almacenarse y encadenarse como tokens en una blockchain.

La identidad digital, es otro campo donde los tokens no fungibles pueden beneficiar por sus propiedades peculiares. Aumentando la privacidad y la integridad de los datos en estos contenidos de cada individuo, el almacenamiento de datos de identificación y propiedad en blockchain se ven beneficiados por las propiedades de los tokens no fungibles.

2. MARCO TEORICO CONCEPTUAL

2.1. Identidad un derecho universal

Los países poseen registros civiles, los cuales implementan sistemas de identificación de personas, por medio de datos como nombre, apellido, fecha de nacimiento, región de nacimiento y tantos datos como las normas y leyes de los países establezcan necesarias para el registro de los individuos.

Los países tienen como obligación darles identidad a sus habitantes, puesto que es un derecho humano. El derecho humano sobre la identidad o mejor conocido como derecho a la identidad, el cual se encuentra en La Declaración Universal de los Derechos Humanos, en el Artículo 6; “Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica.” Entiéndase a tener una identidad frente a la entidad reguladora competente, que el país donde se encuentre establezca.

A cada individuo no se le debe de privar de tener una identidad, la cual a su vez contenga una nacionalidad la cual se establece en el Artículo 15 de La Declaración Universal de los Derechos Humanos, de la siguiente manera;

Toda persona tiene derecho a una nacionalidad. A nadie se privará arbitrariamente de su nacionalidad ni del derecho a cambiar de nacionalidad.

Por lo que en ningún momento una persona puede quedar fuera de un registro civil, de ningún país al que pertenezca o quiera pertenecer, aunque en

este punto hay muchas normas legales, que establecen cada país, para brindar una nacionalidad, a una persona extranjera.

2.2. Artículo 7 - Convención de los derechos del Niño

El niño será inscrito inmediatamente después de su nacimiento y tendrá derecho desde que nace a un nombre, a adquirir una nacionalidad y, en la medida de lo posible, a conocer a sus padres y a ser cuidado por ellos. Artículo 7 de la Convención sobre los Derechos del Niño.

Siendo la identidad un derecho universal, inherente y otorga a una persona que cuenta con un documento de identificación y un registro frente a su gobierno, esto le permite un mejor acceso a educación, salud y seguridad social. Por el contrario, una persona no cuenta con una identidad frente a un ente regulador, sea un gobierno o una organización con la facultad de otorgar un documento o registrar a dicha a persona, esto los puede hacer a estas personas más propensas a ser olvidadas, abusados y explotados en muchas formas.

La identidad no garantiza que las obligaciones de un estado sean cumplidas, pero si generan mayor responsabilidad por un estado, monarquía o gobierno para el cumplimiento de derechos al colectivo de personas que cuentan con una identidad.

2.3. Marco Legal Nacional

El marco legal nacional es un conjunto de reglas y normas por las se tomara de base la plataforma de identificación digital universal en el territorio guatemalteco según las diferentes leyes de registro de personas, código civil y la constitución política de la republica de Guatemala.

2.3.1. Ley del Registro Nacional de las Personas RENAP decreto número 90-2005

La ley del Registro Nacional de las personas RENAP decreto número 90-2005, es una ley creada por el congreso de la republica de Guatemala, para renovar lo referente al registro de las personas y regule la documentación del registro de personas y crear el ente encargo al respecto conocido como RENAP.

2.3.1.1. Capítulo X: De las inscripciones en el Registro Civil de las Personas

El capítulo X comprende los artículos del 67 al 85 los cuales regulan la inscripción de las personas en el RENAP, la obligatoriedad, los tramites referentes a este ente y los plazos sobre estas gestiones.

2.3.1.1.1. Artículo 67. Registro Civil de las Personas.

El Registro Civil de las Personas es público, y en él se inscriben los hechos y actos relativos al estado civil, capacidad civil y demás datos de identificación personal de las personas naturales; el reglamento de inscripciones determinará lo concerniente a ese respecto.

2.3.1.1.2. Artículo 68. Obligatoriedad.

Las inscripciones de los hechos y actos del estado civil, capacidad civil y demás datos de identificación de las personas naturales, así como sus modificaciones son obligatorias ante el Registro Civil de las Personas. Es imprescriptible e irrenunciable el derecho a solicitar que se inscriban tales hechos

y actos. Las inscripciones ante los Registros Civiles de las Personas son totalmente gratuitas sí se efectúan dentro del plazo legal.

2.3.1.1.3. Artículo 70. Inscripciones en el Registro Civil de las Personas.

Se inscriben en el Registro Civil de las Personas:

- Los nacimientos, en un plazo no mayor de treinta (30) días de ocurridos los mismos;
- Los matrimonios y las, uniones de hecho;
- Las defunciones;
- Las resoluciones judiciales que declaran la ausencia y muerte presunta;
- Las sentencias que impongan suspensión o pérdida de la patria potestad y las resoluciones que los rehabiliten;
- Las resoluciones que declaren la nulidad e insubsistencia del matrimonio, la unión de hecho, el divorcio, la separación y la reconciliación posterior;
- Los cambios de nombre o las identificaciones de persona;
- La resolución que declare la determinación de edad;
- El reconocimiento de hijos;
- Las adopciones;
- Las capitulaciones matrimoniales;
- Las sentencias de filiación;
- Extranjeros domiciliados;
- La resolución que declare la interdicción transitoria o permanente;
- La designación, remoción, renuncia del tutor, protutor y guardadores;
- La declaración de quiebra y su rehabilitación; y,

- Los actos que, en general, modifiquen el estado civil y capacidad civil de las personas naturales.

Todas las inscripciones anteriores se anotarán en el registro individual que se creará a cada ciudadano registrado.

2.3.1.1.4. Artículo 71. Inscripciones de nacimiento.

Las inscripciones de nacimiento deberán efectuarse dentro de los sesenta (60) días siguientes al alumbramiento, y se podrán registrar en el lugar donde haya acaecido el nacimiento o en el lugar donde tengan asentada su residencia los padres o las personas que ejerzan la patria potestad. Las demás inscripciones relativas al estado civil, capacidad civil, así como las certificaciones derivadas de los mismos, podrán efectuarse en cualquiera de los Registros Civiles de las Personas a nivel nacional.

2.3.2. Ley de nacionalidad decreto número 1613

La ley de nacionalidad decreto número 1613 del congreso de la Republica de Guatemala, contiene todo lo referente a la regulación de la materia de nacionalidad, basando en las normas constitucionales y los principios de derecho del estado de Guatemala.

2.3.2.1. Capítulo I

El capítulo I de la Ley de nacionalidad decreto número 1613 del congreso de la republica de Guatemala, establece las disposiciones fundamentales para la aplicabilidad de la ley, los conceptos básicos y definiciones de la ley.

2.3.2.1.1. Artículo 1.

La nacionalidad guatemalteca es el vínculo jurídico-político existente entre los individuos que la Constitución de la República determina y el Estado de Guatemala. Tiene por fundamentos un nexo de carácter social y una comunidad de existencia, intereses y sentimientos, e implica derechos y deberes recíprocos.

2.3.2.1.2. Artículo 3.

A ningún guatemalteco de origen puede privársele de su nacionalidad; una vez adquirida es irrenunciable, aun cuando se hubiere optado por la naturalización en país extranjero. Se exceptúan los casos en que la renuncia sea obligatoria para dicha naturalización.

2.3.2.1.3. Artículo 5.

En los casos de doble o múltiple nacionalidad concurrentes en guatemaltecos de origen, el Estado de Guatemala, dentro de sus límites territoriales, les reconoce exclusivamente la propia, sin perjuicio que en el territorio de los Estados que les atribuyan nacionalidad, ejerzan los derechos y obligaciones propios de los nacionales de esos países, no pudiendo en ningún caso invocar otra soberanía frente a la de Guatemala.

2.3.2.1.4. Artículo 6.

La nacionalidad adquirida o recuperada conforme a una ley anterior se conserva bajo el imperio de otra posterior. Esto no significa convalidación de actuaciones nulas conforme al Derecho.

2.3.2.2. Capítulo II Competencia y Procedimientos Generales

El capítulo II de la Ley de nacionalidad decreto número 1613 del congreso de la republica de Guatemala, establece los medios por los cuales se pueden realizar las gestiones consecuentes con el Ministerios de Relaciones Exteriores y los procedimientos correspondientes.

2.3.2.2.1. Artículo 9.

Corresponde al Ministerio de Relaciones Exteriores todo lo relacionado con la nacionalidad guatemalteca, salvo los trámites especiales que esta ley establece y sin perjuicio de los recursos que procedan.

2.3.2.3. Capítulo IV Naturalización Concesiva

El capítulo IV de la Ley de nacionalidad decreto número 1613 del congreso de la republica de Guatemala, establece el procedimiento de naturalización concesiva para extranjeros, los requisitos y los medios para realizar la solicitud de esta.

2.3.2.3.1. Artículo 32.

La naturalización concesiva se basa en el inciso 2º del artículo 7 de la Constitución y puede obtenerla todo extranjero, salvo las excepciones que esta ley establece, siendo potestativo del Ejecutivo, en todo caso, otorgarla o no.

2.3.2.4. Capítulo IX Disposiciones Relativas al orden Internacional

El capítulo IX de la Ley de nacionalidad decreto número 1613 del congreso de la republica de Guatemala, se rectifican los procesos de nacionalidad de personas extrajeras y guatemaltecos que han perdido la nacionalidad, con sus diferentes procesos.

2.3.2.4.1. Artículo 70.

Los tratados y convenios internacionales sobre nacionalidad, ratificados por Guatemala y vigentes, tendrán la fuerza que se deriva del artículo 144 de la Constitución, salvo la mayor que el artículo 6 de la misma reconoce a los bilaterales y multilaterales centroamericanos. En cuanto a los tratados y convenios que rigieron en el pasado, Guatemala reconoce los efectos que jurídicamente deban subsistir.

2.3.3. Constitución Política de la Republica de Guatemala

La Constitución Política de la Republica de Guatemala, que se originó en la asamblea Nacional constituyente el 31 de mayo de 1985, denominada también Carta Magna, por esta se rige el Estado, leyes y establece los derechos fundamentales de la población de la Republica de Guatemala.

2.3.3.1. Capítulo II Nacionalidad y ciudadanía

En el capítulo II de La Constitución Política de la Republica de Guatemala, sienta las bases para diversas leyes respecto a la ciudadanía y la nacionalidad.

Aquí se contienen temas de nacionalidad de los centroamericanos, la naturalización y la pérdida de la nacionalidad.

2.3.3.1.1. Artículo 144. Nacionalidad de origen.

Son guatemaltecos de origen, los nacidos en el territorio de la República de Guatemala, en naves y aeronaves guatemaltecas y los hijos de padre o madre guatemaltecos, nacidos en el extranjero. Se exceptúan los hijos de funcionarios diplomáticos y de quienes ejerzan cargos legalmente equiparados.

A ningún guatemalteco de origen, puede privársele de su nacionalidad.

2.3.3.1.2. Artículo 145. Nacionalidad de centroamericanos.

También se consideran guatemaltecos de origen, a los nacionales por nacimiento, de las repúblicas que constituyeron la Federación de Centroamérica, si adquieren domicilio en Guatemala y manifestaren ante autoridad competente, su deseo de ser guatemaltecos. En este caso podrán conservar su nacionalidad de origen, sin perjuicio de lo que se establezca en tratados o convenios centroamericanos.

2.3.3.1.3. Artículo 146. Naturalización.

Son guatemaltecos, quienes obtengan su naturalización, de conformidad con la ley. Los guatemaltecos naturalizados, tienen los mismos derechos que los de origen, salvo las limitaciones que establece esta Constitución.

2.3.3.1.4. Artículo 147. Ciudadanía.

Son ciudadanos los guatemaltecos mayores de dieciocho años de edad. Los ciudadanos no tendrán más limitaciones, que las que establecen esta Constitución y la ley.

2.3.3.1.5. Artículo 148. Suspensión, pérdida y recuperación de la ciudadanía.

La ciudadanía se suspende, se pierde y se recobra de conformidad con lo que preceptúa la ley.

2.3.4. Código Civil

El código Civil es un conjunto de leyes que estable el Gobierno de Guatemala, las cuales se vinculan a los civiles, la población de la república. Confiere un conjunto de leyes para las personas, para las cosas y para las acciones de la población.

2.3.4.1. Capítulo I De Las Personas Individuales

El Capítulo I del Código Civil de la Republica de Guatemala, estable la definición de los derechos y responsabilidades de las personas como individuos ante el Estado de Guatemala.

2.3.4.1.1. Artículo 1.- (Personalidad).

La personalidad civil comienza con el nacimiento y termina con la muerte; sin embargo, al que está por nacer se le considera nacido para todo lo que le favorece, siempre que nazca en condiciones de viabilidad.

2.3.4.1.2. Artículo 4.

Reformado por el Artículo 1 del Decreto 38-95 del C. R., publicado en el Diario Oficial el 2 de junio de 1995, el cual queda así:

"(Identificación de la persona). La persona individual se identifica con el nombre con que se inscriba su nacimiento en el registro civil, el que se compone del nombre propio y del apellido de sus padres casados o del de sus padres no casados que lo hubieren reconocido. Los hijos de madre soltera serán inscritos con los apellidos de ésta. Los hijos de padres desconocidos serán inscritos con el nombre que les dé la persona o institución que los inscriba. En el caso de los menores ya inscritos en el registro civil con un solo apellido, la madre, o quien ejerza la patria potestad, podrá acudir nuevamente a dicho Registro a ampliar la inscripción correspondiente para inscribir los dos apellidos." (ms3) * (an23) **

*Ver artículo 398 del código Civil.

**El Artículo 4 antes de la reforma del DC No. 38-95.

2.3.4.1.3. Artículo 5.

Modificado por el Artículo 1 del Decreto-Ley 72-84 vigente desde el 17/07/1984, el cual queda así: "El que constante y públicamente use nombre propio o apellido distinto del que consta en su partida de nacimiento, o use incompleto su nombre, u omita alguno de los apellidos que le corresponden, puede establecer su identificación por medio de declaración jurada hecha en

escritura pública, por la misma persona si fuere mayor de edad o por sus padres que ejercieren la patria potestad. También podrá hacerse por cualquiera que tenga interés en la identificación conforme el procedimiento establecido por el Código Procesal Civil y Mercantil." (ms4) * (an2) * *

*Ver arts. 440 a 442 del C.P.C. y M.

**el art. 5 antes de la modificación del d. L 72-84.

2.4. Identidad Digital

La identidad digital se define como, un medio por el cual un individuo es identificado, en un entorno digital (Sistemas bancarios, redes sociales, videojuegos, entre otros). En donde se almacena los datos relevantes de un individuo. Generalmente esta información es guardada por organizaciones, para la identificación de sus empleados, clientes o contactos de interés.

Los gobiernos poseen Registros Civiles, estos tienen como finalidad registrar a sus habitantes y poseer de un documento de identificación ante la sociedad. En cuestión de información gubernamental no siempre se tiene un registro de información digital, en algunos países aún continúan utilizando sistemas en papel, tales como libros, folios y archivos para folios, manteniendo el formato físico de papel para el almacenamiento de los registros civiles.

Para aquellos gobiernos que aún no utilizan un medio de información digital para el registro civil de los habitantes, poseen aún más desventajas para el cumplimiento de derechos de sus ciudadanos y posibles fallas de seguridad, como lo son suplantación de identidad, falsificación de documentos y otros problemas al no contar con un sistema digital.

En internet también se define la identidad digital como todo aquel perfil, publicación, blog, uso de red social y actividad que requiera un registro con datos personales.

2.5. Tecnología de la información

En la vida moderna la tecnología está presente en muchas de las actividades que realizamos a diario, la comunicación, el almacenamiento de datos, transporte, alimentación y muchas otras actividades, dependen o utilizan tecnología para el desarrollo de estas. De esta cuenta las tecnologías de la información forman parte importante de la humanidad desde el surgimiento de los ordenadores modernos.

Desde tiempos antiguos la información siempre ha sido importante, por lo que las civilizaciones antiguas guardaban registros de todo lo que era importante para en su diario vivir. En el mundo actual las tecnologías de la información son un recurso indispensable para almacenar la información, las compañías, instituciones gubernamentales y no gubernamentales se preocupan más por la información que poseen y la utilidad que a esta le puedan dar.

El concepto de tecnología de la información se aplica al uso de equipos de telecomunicaciones y computadores para la transmisión, procesamiento y almacenamiento de datos. El mismo abarca conceptos de informática, electrónica y las telecomunicaciones. Se centra en la gestión de los datos como el almacenamiento, recuperación, transmisión y manipulación, frecuentemente utilizado en los negocios y empresas.

2.6. Almacenamiento de datos

El almacenamiento de la información es una acción fundamental, para el manejo de información, es sumamente importante que esta se mantenga a través del tiempo. El guardado de datos en la actualidad se realiza a gran escala, generalmente en servidores de almacenamiento con grandes capacidades, para la permanencia de la información.

Actualmente el almacenamiento de información ya no solo se realiza de forma local, en un servidor o máquina propia, esto también se realiza a través de la nube, donde el usuario se despreocupa por el mantenimiento físico del equipo y únicamente es responsable de administrar la información que desea almacenar.

Los dispositivos más comúnmente utilizados son discos duros, para respaldo de información también se utilizan cintas magnéticas. A nivel de usuario promedio se utiliza medios de almacenamiento con menor capacidad como USB, CDs o Discos Duros externos.

2.7. Datos

Los datos son una representación de un atributo de un objeto de la realidad. En informática un dato es la unidad mínima de información, que contiene como mínimo un nombre y un valor.

2.8. Información

La información es un conjunto recopilado de datos, el cual tiene sentido y está organizado según las necesidades de quien necesite utilizar la información.

2.9. Bases de datos

Una base de datos es un almacén de datos, en donde se guardan datos bajo un contexto determinado. En informática una base de datos son sistemas de almacenamiento digital, el cual se encuentra controlado por software gestor, el cual se le conoce como DBMS.

2.9.1. Base de datos Centralizada

Estas son aquellas que mantienen todos los datos en una única computadora, ubicación y para acceder a la información se debe ingresar al servidor principal del sistema.

2.9.2. Base de datos Descentralizada

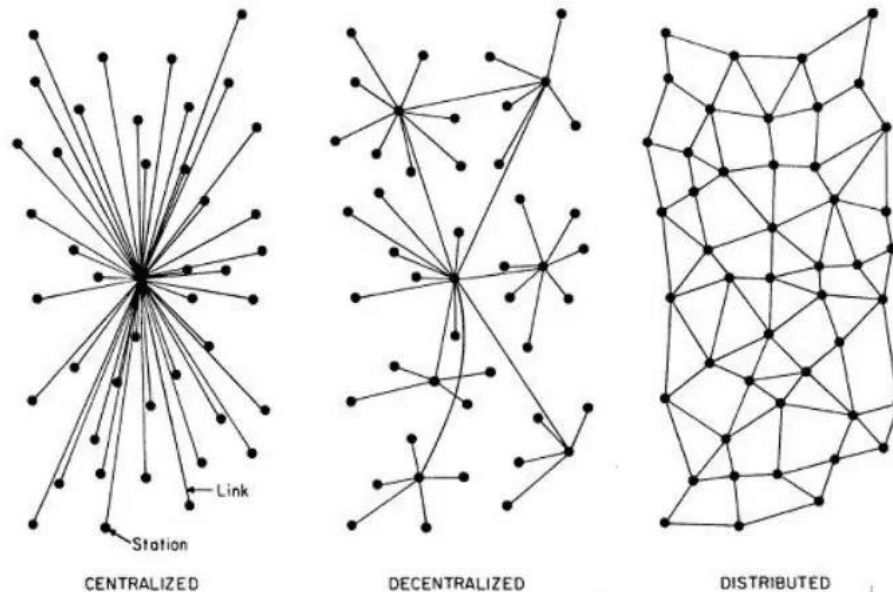
Consiste en una serie de computadoras y servidores que se encuentran en distintos lugares geográficos, los datos no se almacenan en un solo lugar, sino que están almacenados en una serie de servidores distintos que proveen de información a los clientes. Funcionan como un grupo de bases de datos independientes sin conexiones lógicas entre ellas y que no están totalmente interconectadas mediante una red de comunicaciones.

2.9.3. Base de datos Distribuida

Una base de datos distribuida funciona como una única base de datos lógica que está instalada en una serie de computadoras ubicadas en diferentes lugares geográficos y que no están conectadas a una única unidad de procesamiento, pero si están totalmente conectadas entre sí a través de una red de comunicaciones. En este sistema todos los nodos contienen información y todos

los clientes del sistema están en condición de igualdad. De esta forma las bases de datos distribuidas pueden realizar procesamientos autónomos.

Figura 1. **Comparativa de tipos de bases de datos**



Fuente: Christopher Alexander. *Figura que muestra la diferencia entre una red Centralizada(A), Decentralizada(B) y Distribuida(C).* url: https://mk0criptonoticijjgfa.kinstacdn.com/wp-content/uploads/2018/04/bases_de_datos_representacion.jpg. Consulta: 30 de septiembre de 2020.

2.10. Red

En informática una red son 2 o más equipos de cómputo conectados entre sí, los cuales comparten recursos, los cuales pueden ser recursos de hardware periféricos o almacenamiento o software, datos, archivos y aplicaciones.

Las redes informáticas facilitan la comunicación entre las personas, agilizan el almacenamiento de información, ayudan a la integridad de los datos y dan seguridad de acceso a los mismos.

2.11. Sistema

Un sistema es un objeto, el cual puede estar compuesto por una o varias partes el cual se encuentra en determinado entorno. Un sistema puede ser tanto físico como conceptual.

Los sistemas se pueden diferenciar como simples y compuestos. Un sistema simple es aquel que está compuesto por pocos elementos y sus relaciones no crean un valor agregado. Un sistema compuesto es aquel puede estar compuesto por varios sistemas y sus relaciones agregan valor y crean propiedades emergentes.

2.12. Sistema Informático

Un sistema informático es aquel que tiene como fin, realizar gestiones sobre determinados procesos de la vida real. Permite guardar y procesar información, el sistema informático está formado por hardware, software y las personas que utilizan el sistema.

2.13. Plataforma

Es un sistema que sirve como base para hacer funcionar los módulos de hardware o de software con los que es compatible. Dicho sistema está definido por un estándar alrededor del cual se determina una arquitectura de hardware y una plataforma de software. Para definir plataformas se establecen los tipos de arquitectura, sistema operativo, lenguaje de programación o interfaz de usuario compatibles.

2.13.1. Plataforma Cruzada

Es la capacidad de un software o hardware para funcionar de la misma manera sobre plataformas distintas.

2.14. Arquitectura de Software

La arquitectura de software es el diseño de más alto nivel de la estructura de un sistema.

Una arquitectura de software, también denominada arquitectura lógica, consiste en un conjunto de patrones y abstracciones coherentes que proporcionan un marco definido y claro para interactuar con el código fuente del software.

Una arquitectura de software se selecciona y diseña con base a requisitos y restricciones. Los objetivos son aquellos prefijados para el sistema de información, pero no solamente los de tipo funcional, también otros objetivos como la mantenibilidad, auditabilidad, flexibilidad e interacción con otros sistemas de información.

En la implementación de arquitecturas se pueden tener restricciones, las cuales son derivadas de las tecnologías disponibles para implementar sistemas de información. Dependiendo del sistema que se desea implementar y la tecnología que se necesite utilizar, algunas arquitecturas son más recomendables de implementar que otras.

La arquitectura de software define, de manera abstracta, los componentes que llevan a cabo alguna tarea de computación, sus interfaces y la comunicación

entre ellos. Toda arquitectura debe ser implementable en una arquitectura física, que consiste simplemente en determinar qué computadora y/o servidor tendrá asignada cada tarea.

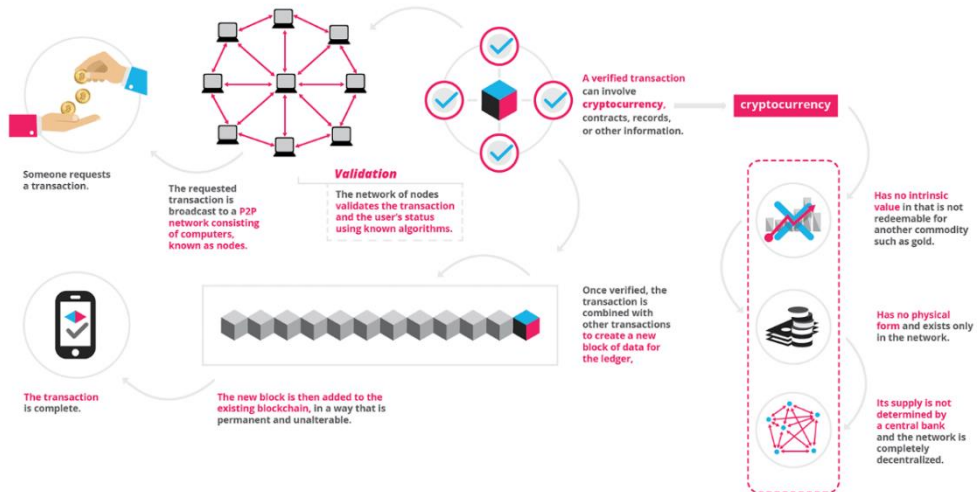
2.15. Blockchain

Blockchain es una tecnología de guardado de información en donde el registro se realiza de forma única, consensuada y se distribuyen por diferentes nodos de una red. La información se encuentra en una red descentralizada, en diferentes nodos de datos en donde queda registro de cada transacción realizada.

2.15.1. Origen

Blockchain es una tecnología, la cual tiene su nacimiento en la creación de la criptomoneda Bitcoin y la plataforma que lleva el mismo nombre. Esta tecnología se basa en el modelo peer-to-peer(P2P), criptográfica, cálculo de tablas hash, descentralización de la información por la red y la difusión de las transacciones por una red de nodos. Estos conceptos son existentes desde antes de la invención de la tecnología, por lo que el blockchain es la aplicación de estos en uno.

Figura 2. Diagrama base de Blockchain



Fuente: Amreer Rosic. *What is Blockchain Technology? A Step-by-Step Guide For Beginners*
 url: <https://artillerymag.com/wp-content/uploads/2019/01/infographics7.jpg>. Consulta: 15 Agosto de 2020

2.15.2. Definición

Sistema de almacenamiento distribuido, descentralizado, sincronizado por consenso y tolerante a fallos, que registra transacciones entre pares en bloques enlazados y protegidos mediante criptografía de forma eficiente, verificable y permanente.

2.15.3. Operabilidad

La tecnología Blockchain en cuanto a operatividad es similar a Internet, ya que tiene una solidez incorporada. Al almacenar bloques de información que son idénticos en toda su red, el Blockchain no puede:

- Ser controlado por una sola entidad.

- No tiene un solo punto de falla.

Desde la invención de Bitcoin en 2008. Desde entonces, la cadena de bloques Bitcoin ha operado sin interrupciones significativas. Los errores asociados a Bitcoin se deben a personas que intentan acceder a la red sin permiso o la mala administración.

2.15.4. Transparencia

Blockchain es una red que está consensuada, esta realiza automáticamente comprobaciones cada cierto periodo de tiempo. Para la plataforma esto es útil para la verificación y auditoría de las transacciones que ocurren cada cierto intervalo de tiempo. Un grupo de transacciones en blockchain se conoce como "bloque". Las propiedades resultantes de este son:

- Los datos son públicos y transparentes.
- La data no puede ser corrompida o alterada.

2.15.5. Componentes

Una plataforma blockchain tiene 3 elementos fácilmente identificables, sobre los cuales se sustenta toda la operabilidad de esta.

2.15.5.1. Bloque

Un nodo es un conjunto de transacciones confirmadas con información adicional incluida para el enlace y validación de la cadena de bloques. Todos los bloques que forma parte de la cadena están formados de la siguiente manera:

- Un código alfanumérico que enlaza al bloque anterior.
- El conjunto de transacciones a guardar en el bloque.
- Un código alfanumérico que enlaza al siguiente bloque.

2.15.5.2. Mineros

El concepto de mineros se aplica a ordenadores dedicados a aportar poder de cálculo computacional a la red para verificar las transacciones que se llevan a cabo en la red. Estos equipos se encargan de realizar la autorización de la adición de los bloques donde se contienen las transacciones. Para realizar dicha acción estos llevan a cabo los siguientes pasos:

- Las nuevas transacciones se transmiten a todos los nodos.
- Cada nodo de la minería recoge nuevas transacciones en un bloque.
- Cada nodo minero trabaja en la búsqueda de una prueba de trabajo para su bloque.
- Cuando un nodo de la minería encuentra una prueba de trabajo, este transmite el bloque a todos los nodos.
- Los demás nodos aceptan el bloque sólo si todas las transacciones son válidas y no se hayan gastado.
- Los nodos expresan su aceptación del bloque trabajando en la creación del próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash anterior.

2.15.5.3. Red de Nodos

Los nodos son computadoras conectadas a la red, las cuales utilizan un software que se encarga de almacenar y distribuir una copia actualizada, del momento actual del blockchain.

Cada vez que un bloque es validado y es añadido a la cadena de bloques, este cambio se debe de reflejar en todos los nodos de la red, en ese momento se notifica a los demás nodos y estos añaden una copia de este en su almacén de datos.

Hay nodos conocidos como mining pools o grupos de minería, estos se encargan de escuchar nuevas transacciones y agruparlas en bloques para proponerlos a disposición de trabajo para los mineros, que luego de ser confirmados son propagados a la red y añadidos a la cadena en su lugar correspondiente.

2.15.6. Características

Dentro de las características más destacadas de la tecnológica del blockchain se encuentran la descentralización, la seguridad y el carácter público de la tecnología.

Es descentralizada debido a que no se rige por ninguna entidad, y la información no se centraliza en un solo lugar, si no se distribuye por la red de nodos. Segura debido a que las verificaciones criptográficas. Es de carácter público porque cualquier usuario puede hacer uso de esta.

2.15.6.1. Descentralizada

Las plataformas blockchain son altamente descentralizadas y peer-to-peer. Es así como, la integridad está basada en un mecanismo de consenso, en vez de una infraestructura basada en la confianza sobre un organismo central, como sería un banco u otra entidad financiera. La red P2P evita que un único participante o grupo controlen el sistema completo. Todos los integrantes de una

red se adhieren, a los mismos protocolos, ya sean individuos, organizaciones o actores estatales. Las transacciones son irreversibles, por lo que una vez realizadas no pueden anularse, modificarse o revertirse.

2.15.6.2. Sistema abierto

Es abierto porque cualquier persona puede formar parte tan solo con adquirir el software para la plataforma. Luego la persona podrá realizar movimientos y transacciones con monedas virtuales y acceder a los datos registrados en su cadena de bloques. A veces los bloques se pueden producir concurrentemente, creando un fork temporal. La cadena de bloques tiene un algoritmo especificado para marcar diferentes versiones de la cadena para que una con un valor más alto pueda ser seleccionada sobre otras.

Los nodos de la red pueden tener de vez en cuando versiones diferentes de la base de datos. Estas solo guardan la versión con la puntuación más alta conocida. Cada vez que se accede se recibe la versión con la puntuación más alta extienden o sobrescriben su propia base de datos y retransmiten la mejora a sus pares.

2.15.7. Seguridad

Los bloques que forman parte del blockchain son ordenados en la cadena por orden cronológico y tienen un código alfanumérico conocido como hash, que corresponde al bloque que los precede, gracias a ese hash todos están referenciados por el bloque que los creó, por lo que solo los bloques que contienen un código válido son introducidos en la cadena y replicados a todos los nodos. Con este método se hace virtualmente imposible modificar un bloque que ha sido introducido ya hace un cierto tiempo.

Los nodos mineros son los encargados de la creación de nuevos bloques de la cadena, computando y añadiendo luego a cada uno de ellos el hash y todas las nuevas transacciones correspondientes. Por lo tanto, el blockchain nos permite llevar a cabo, una contabilidad pública de los movimientos realizados en la red de manera transparente, minimizando la posibilidad de fraude, no permitiendo la pérdida de datos y con un sistema totalmente trazable.

2.15.8. Token ERC-721

ERC es una orientación técnica para personas del ámbito de desarrollo de sistemas, para la construcción de cualquier contrato inteligente. Esta se encuentra activa a desde diciembre de 2018, desde esa fecha hay nuevos estándares de ERC en Ethereum. ERC-20, ERC-55, ERC-137, ERC-162, ERC-165, ERC-181, ERC-190, ERC-721 y ERC-1167.

ERC-721 es un estándar de token no fungible, que fue creado por William Entriken, Dieter Shirley, Jacob Evans y Nastassia Sachs, a causa de que el estándar ERC-20 no cumplía con los requisitos deseables en su momento.

Los tokens ERC-721 presentan diferencias ante los tokens ERC-20 esto se debe a que los tokens ERC-721 no son fungibles. Esto significa que cada token es único y como resultado, no es intercambiable.

2.15.8.1. Funciones asociadas al Token ERC-721

Algunas de las funciones asociadas al estándar Token ERC-721 son las siguientes:

- Nombre

- Símbolo
- Suministro total
- Balance
- Funciones de propietario
- Propietario, aprobación
- Toma de posesión
- Transferencia
- Token del propietario por índice
- Metadatos del token

2.16. Privacidad

La privacidad se define como un individuo mantiene información, relaciones personales, actividades y otros aspectos de su vida en un espacio reservado a la población. Protegiendo la instrucción de este espacio, únicamente dejando la información de las personas que el individuo desee.

2.16.1. Privacidad en el ámbito digital

Con el surgimiento de los servicios digitales, como las redes sociales, correo electrónico, suscripciones a sitios de entretenimientos y otros servicios, surge la necesidad de aplicar el concepto de privacidad.

Cada proveedor de servicios digitales solicita una serie de datos para el registro del usuario. El usuario tiene a la disposición un contrato con términos y condiciones en donde se especifica, las acciones que pueden llegar a realizar sobre los datos.

La privacidad de los datos de un individuo en el mundo digital, son diversos y no hay un estándar regulatorio para los diferentes servicios prestados. Pero se debe tener en cuenta la no divulgación de información sensible como métodos de pago, cuentas bancarias, direcciones de domicilios y otros que puedan afectar física, económica o emocionalmente al usuario.

2.17. Documento de identidad

El documento de identidad contiene los datos de un individuo, dependiendo del país donde se encuentra este puede ser llamado de diferentes formas. El fin del documento de identidad es ser reconocido en un orden público, dentro de la sociedad, dicho documento debe ser emitido por una entidad pública del país de origen de la persona.

Tabla I. Denominaciones de documentos de identidad

País	Nombre	Acrónimo
Iberoamérica		
Argentina, España, y Perú	Documento nacional de identidad	DNI
Bolivia, Chile, Costa Rica, Ecuador, Nicaragua, Uruguay, y Venezuela	Cédula de identidad	CI
Brasil	<i>Carteira de Identidade o Registro Geral</i>	RG
Colombia	Cédula de ciudadanía	CC
El Salvador	Documento único de identidad	DUI
Guatemala	Documento personal de identificación	DPI
Honduras	Tarjeta de identidad	TDI
México	Clave única de registro de población y credencial para votar o credencial de elector	CURP
Panamá	Cédula de identidad personal	CIP
Paraguay	Cédula de identidad civil	CIC/CI

Continuación de tabla I.

Portugal	<i>Cartão de Cidadão</i>	
República Dominicana	Cédula de identidad y electoral	CIE
Resto del mundo		
Alemania	<i>Personalausweis</i>	
Bélgica	<i>Identiteitskaart/Carte d'identité/Personalausweis</i>	
Bosnia y Herzegovina	<i>Lična karta/Osobna iskaznica</i>	
Croacia	<i>Osobna iskaznica</i>	
Estados Unidos	<i>Passport Card</i>	
Francia	<i>Carte nationale d'identité</i>	
Irlanda	<i>Cárta Pas/Passport Card</i>	
Italia	<i>Carta d'Identità</i>	
Montenegro	<i>Lična karta</i>	
Polonia	<i>Dowód osobisty</i>	
Rumanía	<i>Carte de Identitate</i>	
Serbia	<i>Lična karta</i>	

Fuente: Colaboradores. *Denominación por países*. url:

https://es.wikipedia.org/wiki/Documento_de_identidad Consulta: 15 de agosto de 2020

2.18. Reglamento general de protección de datos

Ley de protección de datos nacida en la Unión Europea, normativa determina que todas las empresas, independientemente de su país de origen o de actividad, deberán cumplirla si recogen, guardan, tratan, usan o gestionan algún tipo de dato de los ciudadanos de la Unión Europea. Esta ley aplica a toda compañía que busca prestar servicio a los habitantes de la Unión Europea y regula el mal uso de la información con multas de hasta el 4 % de la facturación anual de las compañías.

Este reglamento recoge y reconoce, por tanto, derechos, como al olvido y el derecho a la portabilidad.

2.18.1. Derechos del reglamento

Los derechos a los que se rigen la plataforma de identificación digital universal están estrictamente ligadas a las operaciones que se pueden realizar en esta plataforma. En estos se definen los procesos y los casos en los cuales deben realizarse, con esto se garantiza una mejor administración de la información.

2.18.1.1. Derecho de eliminación

El primero establece que los ciudadanos pueden solicitar y lograr que los datos personales sean eliminados cuando, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita.

2.18.1.2. Derecho a la portabilidad

El derecho a la portabilidad te permite que, si los datos se están tratando de modo automatizado, sea posible ser recuperarlos en un formato para cederlos a otro responsable. Estos datos deben estar en un formato estructurado, de uso común y lectura mecánica para que pueda transmitirlos fácilmente a otro responsable y facilitar así un cambio de proveedor.

2.18.1.3. Derecho de acceso

Derecho de acceso se refiere a tener la posibilidad de pedir a las empresas, que confirmen si los datos personales se están procesando, dónde y con qué propósito. Si se solicita también es posible solicitar una copia de los datos personales sin cobro alguno.

2.19. Biométrica

La biometría es la toma de medidas estandarizadas de los seres vivos o de procesos biológicos. Se llama también biometría al estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos.

2.19.1. Tecnología Biométrica

En las tecnologías de la información, la utilización del reconocimiento de patrones biométricos, generalmente utilizados para la autenticación, es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para verificar su identidad.

Las grandes empresas, algunos gobiernos, las transacciones bancarias seguras, y los servicios sociales y de salud, entre otros ámbitos, ya utilizan dispositivos de acceso biométrico para el acceso a sus instalaciones.

Aplicativos móviles de bancos utilizan el lector de huella para facilitar el acceso por medio de los patrones biométricos del usuario. Los móviles utilizan sistemas de reconocimiento facial para hacer el acceso al dispositivo más seguro y confiable.

Los patrones comúnmente utilizados son:

- Las huellas dactilares
- La retina
- El iris
- Los patrones faciales

2.19.2. Beneficios de la tecnología biométrica

- La tecnología biométrica hace que no sea necesario llevar una tarjeta o llave para acceder a lugares con restricciones de seguridad o ser identificado ante un sistema de software que lo soporte.
- Asociada a otras tecnologías de restricción de accesos, la biometría garantiza uno de los niveles de autenticación menos franqueables en la actualidad.
- Las personas que utilizan el sistema no deben recordar una contraseña o un número de PIN de acceso.
- Están relacionados de forma directa con el usuario, son exactos y permiten hacer un rastreo de auditorías.
- La utilización de un dispositivo biométrico permite que los costos de operabilidad sean reducidos, ya que sólo se debe realizar el mantenimiento del lector, y mantener la base de datos actualizada. Y se
- Las características biométricas de una persona no son transferibles hacia otra, por lo que nos da mayor seguridad al momento de otorgar los accesos, por este medio.

Tabla II. Confiabilidad de medios biométricos

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Escritura y firma	Voz	Rostr o 2D	Rostr o 3D
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Estabilidad	Alta	Alta	Alta	Baja	Media	Media	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Media	Media	Media	Alta

Continuación de tabla II.

Aceptación	Media	Baja	Alta	Muy Alta	Alta	Muy alta	Muy alta
-------------------	-------	------	------	----------	------	----------	----------

Fuente: Colaboradores. *Tabla comparativa de sistemas biométricos*. url:
<https://es.wikipedia.org/wiki/Biometr%C3%ADa> Consulta: 15 de agosto de 2020.

3. NORMAS Y FUNDAMENTOS DE IDENTIDAD DIGITAL UNIVERSAL

3.1. Identidad digital universal en una plataforma blockchain

La identidad es un derecho universal, genera una necesidad de poseer registros para poder identificar a las personas. Los Registros Civiles son la respuesta a al poder tener datos relevantes respecto a las personas, pero esto genera una independencia de los registros físicos y documentos de identificación como cédulas, pasaportes y carnés de distintos tipos según el país de registro de la persona.

La identidad digital universal, basada en una plataforma blockchain, su principal finalidad es, tener una plataforma de registro de personas, el cual pueda almacenar una identidad digital, en una red de datos distribuida como lo es blockchain, haciendo de la descentralización de dicha tecnológica una clara fortaleza. Esta plataforma de Identificación digital universal debería ser de fácil acceso para el registro de personas, en cualquier país, esto con la finalidad de hacer cumplir el Artículo 6, de La Declaración Universal de los derechos humanos.

La plataforma, creará una independencia de los registros físicos y documentos emitidos por entidades reguladoras para la identificación de personas, puesto que, por medio de tecnologías de carácter biométrico, la persona sería capaz de identificarse sin necesidad de un documento físico, en cualquier país.

3.2. Seguridad de la Identidad Universal

La seguridad para la información en la plataforma se hará utilizando el cifrado de información de claves hash que posee la tecnología de blockchain para el sellado de datos, por lo que estos no pueden ser modificados, a menos que se tengan la ubicación exacta de todos los nodos de información. Por lo que es necesario la utilización de una clave privada y una clave pública, las cuales son firmas digitales generadas con algoritmos matemáticos los cuales previenen el plagio y la reutilización de estas.

Debido a las bondades de este sistema la seguridad por la redundancia de datos a través de los diferentes nodos, se garantizará la consistencia, persistencia y, la modificación no consensuada y no deseada de información sin el registro consecuente de dicha modificación.

3.3. Participantes de la plataforma

En la plataforma debe tener diferentes participantes, los cuales son esenciales para que dicha plataforma cumpla sus funciones y las ventajas sobre su utilización, promoviendo la Identidad Digital Universal.

3.3.1. Ente Rector

Se debe designar un ente rector, el cual centralice las operaciones, regule la actividad; asignando permisos, revisando la fiabilidad de los datos, generando estadísticas del sistema, dar mantenimiento y mejorar el software con el que se realicen las operaciones.

Este ente rector debe de tener la facilidad para poder tener comunicación y operabilidad con las organizaciones de los diferentes países que utilicen la plataforma. El ente deberá tener la capacidad de movilizar equipo para implementar el sistema y capacitar al personal que lo utilizará.

Para realizar la gestión, el ente rector debe estar en la capacidad de prestar servicios, sin importar las condiciones sociales del país que quiera hacer uso de la red de identificación universal. El ente rector debe encargarse de velar por el cumplimiento de las normas a la plataforma y su correcto uso de la misma.

3.3.1.1. Funciones del ente rector

Las funciones que el ente rector debe de cumplir son para la regulación, cumplimiento y correcto funcionamiento de la plataforma, dentro de las cuales se pueden encontrar:

- Garantizar el registro en la plataforma.
- Monitorear el funcionamiento de la plataforma.
- Certificar la calidad de los datos.
- Evitar el uso indebido de la plataforma.
- Garantizar el registro de los controles.
- Capacitar a las organizaciones de los países a utilizarlo.
- Identificar los puntos de mejora.
- Gestionar la correcta migración de datos.

3.3.1.2. Ente rector propuesto

La Organización de las Naciones Unidas, por ser una de las organizaciones internacionales en donde más países participan formando parte de, la ONU es un fuerte candidato para ser el ente rector de una plataforma de tal magnitud, en donde se tenga el registro de civiles a nivel mundial.

La ONU se encarga del cumplimiento de los derechos humanos, seguridad internacional, la paz y desarrollo económico, por tal motivo y por tener un amplio panorama sobre la situación internacional, puede cumplir las funciones de ente rector sobre la plataforma.

3.3.2. Entidades Asociadas

Las entidades asociadas, son todas aquellas que deseen utilizar el servicio para la identificación de ciudadanos. Estas entidades deben ser monitoreadas y regularizadas por el Ente Rector, en el caso propuesto la ONU.

Las entidades asociadas deberán ser designadas por el país donde se desee utilizar el servicio de la plataforma. Una vez el servicio este establecido en el país la entidad asociada está comprometida a prestar el servicio sin ningún tipo de discriminación.

Las entidades están comprometidas a prestar el servicio con medios de autenticación biométricos, para los usuarios finales, los cuales serán capaces de identificarse en cualquier país que utilice la plataforma de identidad digital universal.

3.3.2.1. Funciones de entes asociadas

Los entes asociados, serán quienes presten el servicio a los civiles para la toma de registros y se encarguen de mantener la red en uso y con el registro consistente y adecuado de datos, para ello las funciones principales que estos deben de cumplir son las siguientes:

- Prestar el servicio indiscriminadamente.
- Facilitar el acceso de la identificación digital.
- Prestar servicios para la verificación de identidad a terceros.
- Prevenir el registro por usurpación.
- Uso correcto de la información.
- Realizar el registro con sensores biométricos.

3.3.3. Usuarios

Los usuarios finales serán todos los habitantes del país en cuestión, que decida utilizar el servicio de identidad digital universal. Las personas tendrán por derecho irrevocable, la apropiación de una identidad en la plataforma para poder ser reconocido frente a la sociedad.

Los individuos podrán tener libre acceso a su información, y las entidades deberán de tener los medios necesarios para que estos puedan consultarlos en el idioma deseado.

3.3.3.1. Operaciones permitidas por los usuarios

Los usuarios podrán realizar una serie de operaciones, con dependencia de los entes asociados a la plataforma, las cuales serán:

- Consultar la información personal en la plataforma.
- Realizar modificaciones de información personal, en dependencia con el ente rector.
- Consultar información sobre el núcleo familiar.
- Gestionar certificaciones.

3.3.4. Entidades terceras

Las entidades terceras serán empresas, instituciones estatales o privadas que deseen validar información de los civiles registrados en la plataforma, para este fin las mismas deberán de ser reguladas por las instituciones asociadas y brindar el servicio según sea necesario y conforme las leyes de los países usuarios lo permitan.

Las operaciones asociadas a los terceros son únicamente de consulta por lo que no pueden realizar gestiones de actualización de información.

3.4. Abolición de Robo Identidad

El robo de la identidad es un problema que en la actualidad ocurre en diferentes lugares del mundo, esto con el fin de poder acceder a beneficios en nombre de otra persona.

La plataforma de Identificación Digital Universal luchará contra la misma ya que al tener la información de forma descentralizada, accesible para todos, siendo utilizada como medio oficial de autenticación por medio de sensores biométricos, en instituciones internacionales, gubernamentales, financieras y otras, no será posible realizar la suplantación de identidad, reemplazando los documentos físicos.

3.5. Documentos como medida alterna de identificación

Debido a que una plataforma siempre puede presentar inconvenientes de acceso, aunque en una red de información en blockchain este tipo de inconvenientes son menos frecuentes por la descentralización, y puede deberse más a motivos como caídas de internet, fallas en las redes locales o servicios inhabilitados, se tendrá como medida la emisión de documentos sencillos con información que solo puede ser genera por la información.

Los documentos emitidos serán útiles en lugares donde no se cuente con un sistema conectada la red, podrá presentarse un documento emitido por una de las entidades asociadas en la red.

Estos métodos solo se utilizarán cuando el acceso sea poco factible o nulo a la plataforma, pero el medio oficial será por medio de los sensores biométricos y la verificación de identidad directo a la plataforma.

3.6. Pilares fundamentales de la Identidad Digital Universal

La plataforma contará como bases importantes sobre las que sostendrá su operabilidad y la prestación del servicio, mismas que el ente rector debe hacer que se cumplan.

- Prestar servicio a todo habitante
- Disponibilidad de la plataforma
- Libre acceso a la información personal
- Información descentralizada
- Consistencia de la información

4. RESULTADO DE DISEÑO DE LA PLATAFORMA IDENTIDAD DIGITAL UNIVERSAL

4.1. Estructura de funcionamiento de la plataforma de Identidad Digital Universal

La estructura de interacciones de la plataforma de Identidad Digital Universal se plantea de una forma simple, donde se muestra a grandes rasgos, las relaciones e interacciones en la plataforma, con los actores de la misma.

4.1.1. Descripción general de interacciones

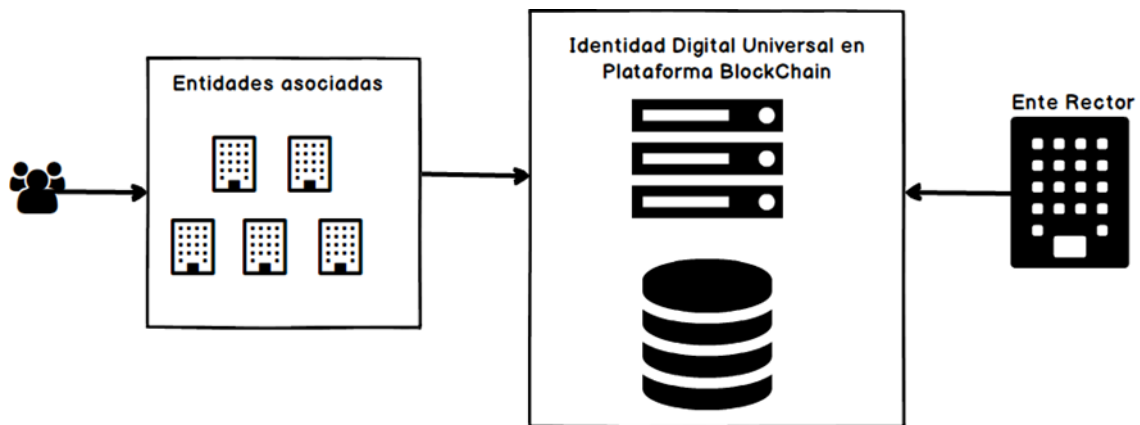
El ente rector es el ente encargado de regular la plataforma frente a las entidades asociadas. Su principal interacción es monitorear y vigilar el uso de estas sobre la plataforma.

Las entidades asociadas se encargan de prestar el servicio a los civiles del país donde operan. Estos entes se encargarán tanto de alimentar la plataforma con la información de registro de personas como, facilitar el acceso a las personas a la información que estos puedan usar.

Los usuarios serán quienes utilicen los servicios que la plataforma de identidad digital universal tenga disponibles, por medio de las entidades asociadas. Estos serán quienes generen el mayor valor a la plataforma, ya que los datos de estos serán los que la plataforma almacenara.

Dentro de los usuarios también se incluyen a empresas o usuarios terceros, que según las leyes de cada país podrán solicitar ciertos servicios para validar información de civiles registrados, en la plataforma.

Figura 3. **Diagrama de arquitectura, Identidad Digital Universal en Blockchain.**



Fuente: elaboración propia, empleando Balsamiq.

4.2. Estandarización de información

La información que se desea contener en la plataforma será estandarizada, para facilitar la búsqueda de los individuos registrados y puedan ser identificados sin problemas, en cualquier lugar donde se utilice la plataforma.

El estándar de la información debe presentar un modelo apto para las diferentes distribuciones, geográficas, étnicas, sociales, culturales y políticas. Debido a que el sistema puede ser utilizado por diferentes países, es necesario que la información mantenga el estándar tomando en consideración un modelo de adopción universal con flexibilidad casi nula, para evitar incongruencias e información que fuese a malinterpretarse.

4.2.1. Estándar Propuesto

El estándar que se propone a continuación tendrá las características listadas a continuación:

- Nombres de atributos de la información en ingles
- Utilización de caracteres UTF-8
- Clave de identificación biométrica
- Localización geográfica
 - Definición de regiones por jerarquía
 - Definición de jerarquías
 - Manejo de coordenadas cartesianas
- Modelado de relaciones de núcleos familiares
- Manejo de estados por catálogos
- Catálogos en ingles

4.3. Restricción de acceso a información

La restricción de acceso a la información se realiza por medio un sistema de roles, el cual comprenderá las funciones que se podrán realizar sobre el aplicativo.

4.3.1. Roles

La definición de los roles en sistema nos delimita la cantidad de operaciones que el usuario que utilice el sistema pueda realizar. De esta manera restringimos el acceso de datos, el acceso a módulos para ingreso de información y cambios en la información. La utilización de los roles en la plataforma de identidad nos permitirá definir una mejor calidad de información y tener mayor seguridad en la

plataforma, para que no se utilicen de forma errónea, no se comparta información que es de interés únicamente personal entre el ente emisor y la persona que se encuentre registrada en la plataforma.

4.3.1.1. Consulta Usuario Civil

El rol servirá para que todo Civil registrado en la plataforma pueda consultar información sobre su persona o núcleo familiar.

4.3.1.2. Consulta Tercero

El rol consulta tercero, dará acceso con previa autorización por las entidades asociadas, a empresas, bancos, financieras, instituciones y otros, que deseen verificar información de personas. La información será limitada para estos, con la finalidad de proteger los datos.

4.3.1.3. Operador Asociado de Registro

El rol de operador asociado será el encargado de realizar el registro de datos sobre los ciudadanos a registrarse, este deberá tener acceso para agregar nueva información.

4.3.1.4. Operador Asociado de Certificación

El rol de operador asociado de certificación tendrá la capacidad de generar certificados, en la plataforma el consultar información sobre los ciudadanos que se registren.

4.3.1.5. Operador Asociado de Reportes

El operador asociado de reportes podrá realizar extracciones de datos, para poder analizar los diferentes parámetros, referente a la entidad asociada a la que pertenezca.

4.3.1.6. Roles de Desarrollo Asociados

Los roles de desarrollo serán para personas de equipos de desarrollo, los cuales estén autorizados para el desarrollo de herramientas, que ayuden a las entidades asociadas al cumplimiento de sus tareas.

Dentro de los roles de desarrollo podremos encontrar los siguientes:

- Rol de desarrollador asociado
- Rol de tester asociado
- Rol de desarrollador de reportes asociado

4.3.1.7. Roles del ente rector

Los roles relacionados serán utilizados por el personal del ente rector, en estos se encontrarán diferentes roles.

Como sistema la plataforma tendrá roles administrativos los cuales serán utilizados para gestionar la información, acceso y todo lo referente al núcleo de la plataforma, de tal manera que pueda realizarse todas las gestiones necesarias.

Los siguientes roles son los necesarios para la administración en las diferentes áreas, de la plataforma, pero los mismos no se limitan a los que acá se encuentran y los mismos representan un conjunto de roles por área.

- Roles de seguridad informática
- Roles de manejo de datos
- Roles de gestión de calidad
- Roles de gestión administrativa
- Roles de gerencia
- Roles de desarrollo de software
- Roles de gestión de infraestructura

El diseño de una aplicación de la plataforma de software basada en blockchain para la identificación digital universal, se basa en las características descritas en el capítulo anterior. Por la naturaleza de esta a continuación se describe la solución planteada en tecnología blockchain.

4.4. Operaciones de la plataforma de Identificación digital universal

La principal funcionalidad de la plataforma es brindar una identidad digital que pueda ser utilizada universalmente, con esta funcionalidad surgen diferentes tipos de registros y servicios que la plataforma puede dar.

Los diferentes registros que la plataforma tendrá que aguantar dependerá del país y las leyes que rigen el mismo, la plataforma modelara las más comunes y utilizadas en los diferentes países.

Todos los registros civiles en esta plataforma son regulados por las leyes de los países, ya que la plataforma sirve para hacer cumplir el derecho de identidad.

4.4.1. Registro de personas

La plataforma como principal objetivo comprenderá el registro de recién nacidos o personas que nunca fueron registradas en la misma. La plataforma brindará la gestión sobre los datos personales de los individuos, de los países que utilicen la plataforma.

Según la información personal almacenada en la plataforma, esta brindara la siguiente información, personal:

- Mayoría de edad
- Lugar de origen
- Permisos de pasaporte
- Nacionalidad(es)
- Edad
- Estado Civil
- Lugar de residencia

4.4.2. Registro de relaciones

Los datos que se manejarán en la plataforma, de manera personal también podrán modelar las relaciones personales entre individuos. La plataforma comprenderá las relaciones siguientes:

- Padres
- Hijos
- Conyugues

4.4.3. Generación de certificaciones

Con los datos personales y las relaciones registradas, la plataforma tendrá la capacidad de emitir certificados, tanto electrónicos como físicos según se la necesidad del usuario. Los certificados de los cuales se pueden emitir a través de la plataforma son los siguientes:

- Certificados de nacimiento
- Certificados de defunción
- Certificados de nacimiento
- Certificados de nacionalidad
- Certificados de matrimonio

4.5. Lenguaje

El lenguaje de la implementación para los nodos de información se utilizará Javascript con Smart Contracts de la plataforma de Ethereum, este lenguaje es uno de los más utilizados a nivel mundial, con esta implementación se realizará del manejo de la información.

4.6. Servicios Web

La plataforma utilizara web services para la interacción con las entidades asociadas, las cuales trabajarán bajo el contexto de Restless, mismos serán desarrolladas usando Python y el framework Python Flask.

Los servicios prestados son todos los que se compren para la interacción de las entidades asociadas.

- Registro de nueva persona
- Registro de nueva relación
- Cambio de estado civil
- Cambio de residencia
- Agregar nacionalidad a una persona
- Defunción de persona
- Consulta de información de personas
- Generación de certificación de personas
- Validación de parámetros biométricos
- Registro de zonas geográficas
- Consulta de zonas geográficas
- Agregar propiedad a la persona
- Autorizar nuevas propiedades

4.7. Estructuración de Datos

La estructura de los datos por medio de Smartcontracts, los cuales se basan en la plataforma de Ethereum, aplicando el protocolo de token no fungibles, ERC-721, el cual nos permite tener propiedades que vuelven único a cada token.

La característica de estos Tokens, permitirá tener flexibilidad en cuanto a la región en donde se utilice la plataforma, para poder generar propiedades a los tokens que en algún país o región no sean utilizados.

4.7.1. Smart Contract para la plataforma de identidad digital universal

Los contratos inteligentes contendrán el funcionamiento principal de la plataforma, en sus operaciones principales para el manejo de la información, y la estructuración de la data.

En este nivel se tendrán las funciones principales, que realizan las funciones principales sobre los datos.

Tabla III. Smart Contract Universal Identification

```
pragma solidity ^0.4.24;

interface ERC165 {

    function supportsInterface(bytes4 _interfaceId)
        external
        view
        returns (bool);
}

contract ERC721Basic is ERC165 {

    bytes4 internal constant InterfaceId_ERC721 = 0x80ac58cd;

    bytes4 internal constant InterfaceId_ERC721Exists = 0x4f558e79;

    bytes4 internal constant InterfaceId_ERC721Enumerable = 0x780e9d63;

    bytes4 internal constant InterfaceId_ERC721Metadata = 0x5b5e139f;

    event Transfer(
        address indexed _from,
        address indexed _to,
        uint256 indexed _tokenId
    );
```


Continuación tabla III.

```
event Approval(  
    address indexed _owner,  
    address indexed _approved,  
    uint256 indexed _tokenId  
);  
  
event ApprovalForAll(  
    address indexed _owner,  
    address indexed _operator,  
    bool _approved  
);  
  
function balanceOf(address _owner) public view returns (uint256 _balance);  
function ownerOf(uint256 _tokenId) public view returns (address _owner);  
function exists(uint256 _tokenId) public view returns (bool _exists);  
  
function approve(address _to, uint256 _tokenId) public;  
function getApproved(uint256 _tokenId)  
    public view returns (address _operator);  
  
function setApprovalForAll(address _operator, bool _approved) public;  
function isApprovedForAll(address _owner, address _operator)  
    public view returns (bool);  
  
function transferFrom(address _from, address _to, uint256 _tokenId) public;  
  
function safeTransferFrom(address _from, address _to, uint256 _tokenId)  
    public;  
  
function safeTransferFrom(  
    address _from,  
    address _to,  
    uint256 _tokenId,  
    bytes _data  
)  
    public;  
}
```

Continuación tabla III.

```
contract ERC721Enumerable is ERC721Basic {
    function totalSupply() public view returns (uint256);
    function tokenOfOwnerByIndex(
        address _owner,
        uint256 _index
    )
        public
        view
        returns (uint256 _tokenId);

    function tokenByIndex(uint256 _index) public view returns (uint256);
}

contract ERC721Metadata is ERC721Basic {
    function name() external view returns (string _name);
    function symbol() external view returns (string _symbol);
    function tokenURI(uint256 _tokenId) public view returns (string);
}

contract ERC721 is ERC721Basic, ERC721Enumerable, ERC721Metadata {
}

contract ERC721Receiver {

    bytes4 internal constant ERC721_RECEIVED = 0x150b7a02;

    function onERC721Received(
        address _operator,
        address _from,
        uint256 _tokenId,
        bytes _data
    )

}

library SafeMath {

    function mul(uint256 _a, uint256 _b) internal pure returns (uint256 c) {

        if (_a == 0) {
            return 0;
        }
    }
}
```

Continuación tabla III.

```
c = _a * _b;
assert(c / _a == _b);
return c;
}

function div(uint256 _a, uint256 _b) internal pure returns (uint256) {
    return _a / _b;
}

function sub(uint256 _a, uint256 _b) internal pure returns (uint256) {
    assert(_b <= _a);
    return _a - _b;
}

function add(uint256 _a, uint256 _b) internal pure returns (uint256 c) {
    c = _a + _b;
    assert(c >= _a);
    return c;
}
}

library AddressUtils {

    function isContract(address _addr) internal view returns (bool) {
        uint256 size;
        assembly { size := extcodesize(_addr) }
        return size > 0;
    }

}

contract SupportsInterfaceWithLookup is ERC165 {

    bytes4 public constant InterfaceId_ERC165 = 0x01ffc9a7;

    mapping(bytes4 => bool) internal supportedInterfaces;

    constructor()
    public
    {
        _registerInterface(InterfaceId_ERC165);
    }
}
```

Continuación tabla III.

```
function supportsInterface(bytes4 _interfaceId)
    external
    view
    returns (bool)
{
    return supportedInterfaces[_interfaceId];
}

function _registerInterface(bytes4 _interfaceId)
    internal
{
    require(_interfaceId != 0xffffffff);
    supportedInterfaces[_interfaceId] = true;
}
}

contract ERC721BasicToken is SupportsInterfaceWithLookup, ERC721Basic
{
    using SafeMath for uint256;
    using AddressUtils for address;

    bytes4 private constant ERC721_RECEIVED = 0x150b7a02;

    mapping (uint256 => address) internal tokenOwner;
    mapping (uint256 => address) internal tokenApprovals;
    mapping (address => uint256) internal ownedTokensCount;

    mapping (address => mapping (address => bool)) internal
operatorApprovals;

    constructor()
    public
    {
        _registerInterface(InterfaceId_ERC721);
        _registerInterface(InterfaceId_ERC721Exists);
    }

    function balanceOf(address _owner) public view returns (uint256) {
        require(_owner != address(0));
    }
}
```

Continuación tabla III.

```
    return ownedTokensCount[_owner];
}

function ownerOf(uint256 _tokenId) public view returns (address) {
    address owner = tokenOwner[_tokenId];
    require(owner != address(0));
    return owner;
}

function exists(uint256 _tokenId) public view returns (bool) {
    address owner = tokenOwner[_tokenId];
    return owner != address(0);
}

function approve(address _to, uint256 _tokenId) public {
    address owner = ownerOf(_tokenId);
    require(_to != owner);
    require(msg.sender == owner || isApprovedForAll(owner, msg.sender));

    tokenApprovals[_tokenId] = _to;
    emit Approval(owner, _to, _tokenId);
}

function getApproved(uint256 _tokenId) public view returns (address) {
    return tokenApprovals[_tokenId];
}

function setApprovalForAll(address _to, bool _approved) public {
    require(_to != msg.sender);
    operatorApprovals[msg.sender][_to] = _approved;
    emit ApprovalForAll(msg.sender, _to, _approved);
}

function isApprovedForAll(
    address _owner,
    address _operator
)
public
view
returns (bool)
{
    return operatorApprovals[_owner][_operator];
}
```

Continuación tabla III.

```
}  
  
function transferFrom(  
    address _from,  
    address _to,  
    uint256 _tokenId  
)  
    public  
    {  
        require(isApprovedOrOwner(msg.sender, _tokenId));  
        require(_from != address(0));  
        require(_to != address(0));  
  
        clearApproval(_from, _tokenId);  
        removeTokenFrom(_from, _tokenId);  
        addTokenTo(_to, _tokenId);  
  
        emit Transfer(_from, _to, _tokenId);  
    }  
  
function safeTransferFrom(  
    address _from,  
    address _to,  
    uint256 _tokenId  
)  
    public  
    {  
        safeTransferFrom(_from, _to, _tokenId, "");  
    }  
  
function safeTransferFrom(  
    address _from,  
    address _to,  
    uint256 _tokenId,  
    bytes _data  
)  
  
    public  
    {  
        transferFrom(_from, _to, _tokenId);  
        require(checkAndCallSafeTransfer(_from, _to, _tokenId, _data));  
    }  
}
```

Continuación tabla III.

```
function isApprovedOrOwner(
    address _spender,
    uint256 _tokenId
)
internal
view
returns (bool)
{
    address owner = ownerOf(_tokenId);

    return (
        _spender == owner ||
        getApproved(_tokenId) == _spender ||
        isApprovedForAll(owner, _spender)
    );
}

function _mint(address _to, uint256 _tokenId) internal {
    require(_to != address(0));
    addTokenTo(_to, _tokenId);
    emit Transfer(address(0), _to, _tokenId);
}

function _burn(address _owner, uint256 _tokenId) internal {
    clearApproval(_owner, _tokenId);
    removeTokenFrom(_owner, _tokenId);
    emit Transfer(_owner, address(0), _tokenId);
}

function clearApproval(address _owner, uint256 _tokenId) internal {
    require(ownerOf(_tokenId) == _owner);
    if (tokenApprovals[_tokenId] != address(0)) {
        tokenApprovals[_tokenId] = address(0);
    }
}

function addTokenTo(address _to, uint256 _tokenId) internal {
    require(tokenOwner[_tokenId] == address(0));
    tokenOwner[_tokenId] = _to;
    ownedTokensCount[_to] = ownedTokensCount[_to].add(1);
}
```

Continuación tabla III.

```
function removeTokenFrom(address _from, uint256 _tokenId) internal {
    require(ownerOf(_tokenId) == _from);
    ownedTokensCount[_from] = ownedTokensCount[_from].sub(1);
    tokenOwner[_tokenId] = address(0);
}

function checkAndCallSafeTransfer(
    address _from,
    address _to,
    uint256 _tokenId,
    bytes _data
)
    internal
    returns (bool)
{
    if (!_to.isContract()) {
        return true;
    }
    bytes4 retval = ERC721Receiver(_to).onERC721Received(
        msg.sender, _from, _tokenId, _data);
    return (retval == ERC721_RECEIVED);
}
}

contract ERC721Token is SupportsInterfaceWithLookup,
ERC721BasicToken, ERC721 {

    string internal name_;

    string internal symbol_;

    mapping(address => uint256[]) internal ownedTokens;

    mapping(uint256 => uint256) internal ownedTokensIndex;

    uint256[] internal allTokens;

    mapping(uint256 => uint256) internal allTokensIndex;

    mapping(uint256 => string) internal tokenURIs;
```


Continuación tabla III.

```
constructor(string _name, string _symbol) public {
    name_ = _name;
    symbol_ = _symbol;
    _registerInterface(InterfaceId_ERC721Enumerable);
    _registerInterface(InterfaceId_ERC721Metadata);
}

function name() external view returns (string) {
    return name_;
}

function symbol() external view returns (string) {
    return symbol_;
}

function tokenURI(uint256 _tokenId) public view returns (string) {
    require(exists(_tokenId));
    return tokenURIs[_tokenId];
}

function tokenOfOwnerByIndex(
    address _owner,
    uint256 _index
)
public
view
returns (uint256)
{
    require(_index < balanceOf(_owner));
    return ownedTokens[_owner][_index];
}

function totalSupply() public view returns (uint256) {
    return allTokens.length;
}

function tokenByIndex(uint256 _index) public view returns (uint256) {
    require(_index < totalSupply());
    return allTokens[_index];
}
```

Continuación tabla III.

```
function _setTokenURI(uint256 _tokenId, string _uri) internal {
    require(exists(_tokenId));
    tokenURIs[_tokenId] = _uri;
}

function addTokenTo(address _to, uint256 _tokenId) internal {
    super.addTokenTo(_to, _tokenId);
    uint256 length = ownedTokens[_to].length;
    ownedTokens[_to].push(_tokenId);
    ownedTokensIndex[_tokenId] = length;
}

function removeTokenFrom(address _from, uint256 _tokenId) internal {
    super.removeTokenFrom(_from, _tokenId);

    uint256 tokenIndex = ownedTokensIndex[_tokenId];
    uint256 lastTokenIndex = ownedTokens[_from].length.sub(1);
    uint256 lastToken = ownedTokens[_from][lastTokenIndex];

    ownedTokens[_from][tokenIndex] = lastToken;

    ownedTokens[_from].length--;

    ownedTokensIndex[_tokenId] = 0;
    ownedTokensIndex[lastToken] = tokenIndex;
}

function _mint(address _to, uint256 _tokenId) internal {
    super._mint(_to, _tokenId);

    allTokensIndex[_tokenId] = allTokens.length;
    allTokens.push(_tokenId);
}

function _burn(address _owner, uint256 _tokenId) internal {
    super._burn(_owner, _tokenId);

    if (bytes(tokenURIs[_tokenId]).length != 0) {
        delete tokenURIs[_tokenId];
    }

    uint256 tokenIndex = allTokensIndex[_tokenId];
```

Continuación tabla III.

```
uint256 lastTokenIndex = allTokens.length.sub(1);
uint256 lastToken = allTokens[lastTokenIndex];

allTokens[tokenIndex] = lastToken;
allTokens[lastTokenIndex] = 0;

allTokens.length--;
allTokensIndex[_tokenId] = 0;
allTokensIndex[lastToken] = tokenIndex;
}
}

pragma solidity^0.4.24;

contract universalIdentification is ERC721Token {
    constructor() ERC721Token("universalIdentification", "UNI") public {}

    struct Person {
        string first_name;
        string last_name;
        uint8 birtdate;
        DocumentCountry documentCountry;
        Country country;
        Region region;
        string personAddress;
        MartialStatus personMartialStatus;
    }

    struct Country {
        string name;
        Continent contient;
    }

    struct Region {
        string name;
        Country country;
    }

    struct Continent {
        string name;
    }
}
```

Continuación tabla III.

```
struct DocumentCountry{
    uint256 idDocument;
}

struct PersonalBiometrics{
    Retina retine;
    FingerPrint fingerPrint;
}

struct Retina{
    uint256 retinald;
    uint256 hashtSetUpRetine;
}

struct FingerPrint{
    uint256 fingerPrint;
    uint256 hashtSetUpFingerPrint;
}

struct MartialStatus{
    uint8 idStatus;
    string name;
}

Person[] persons;

function      getPersonFromId(uint      id)      public      view
returns(string,string,uint8,uint256,string) {
    return
    (persons[id].first_name,persons[id].last_name,persons[id].birtdate,persons[id
].documentCountry.idDocument,persons[id].country.name);
}

function getPersonNameFromId(uint id) public view returns(string,string){
    return (persons[id].first_name,persons[id].last_name);
}

function getPersonAddress(uint id) public view returns(string){
    return (persons[id].personAddress);
}
```

Continuación tabla III.

```
function getPersonMaritalStatus(uint id) public view returns (string){  
    return (persons[id].personMaritalStatus.name);  
}  
}
```

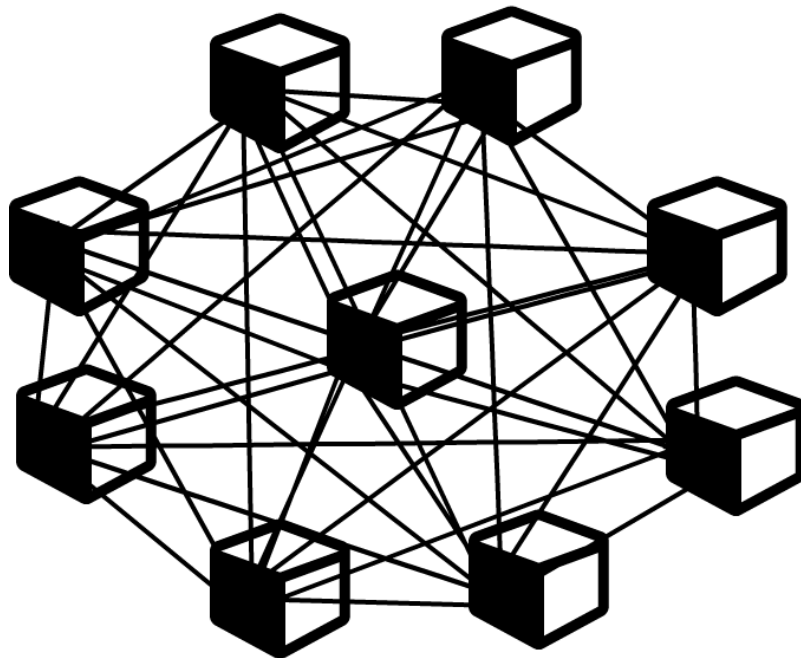
Fuente: elaboración propia, empleando remix.ethereum.

4.8. Arquitectura

La arquitectura planteada para la solución en cuestión es blockchain en su más alto nivel, por lo que toma todos los conceptos de la misma para generar una solución de software segura, descentralizada y con alta disponibilidad.

En la presente arquitectura se detalla la interacción, de los nodos de información en la plataforma y los servicios y las implementaciones de consumo.

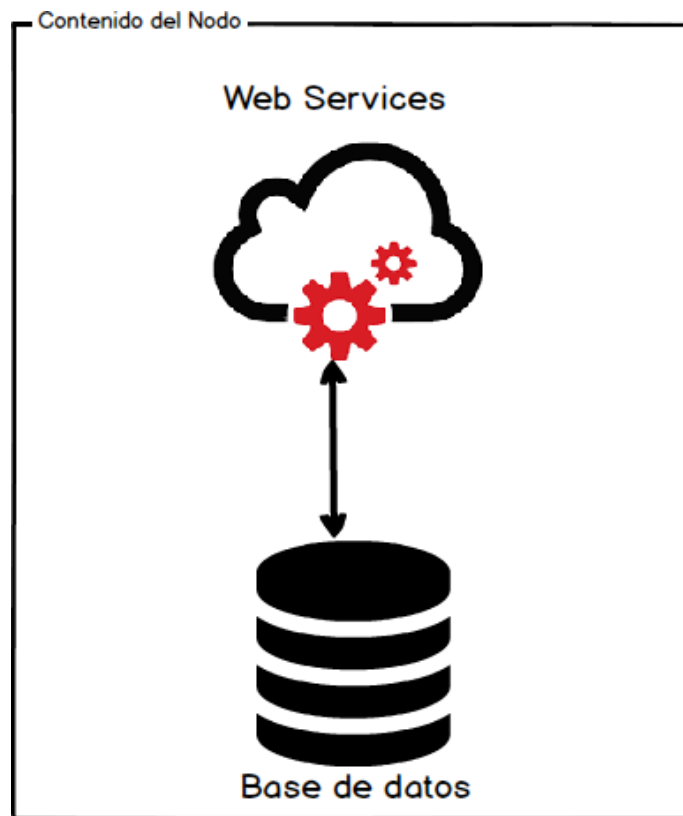
Figura 4. **Distribución de nodos con base de datos**



Fuente: elaboración propia, empleando Balsamiq.

Los nodos deben de estar en conexión y replicación constante para, que la información se encuentre descentralizada. Los nodos deben ser exactamente iguales, pero estar distribuidos alrededor de las entidades asociadas. Cada uno de los nodos debe de poder brindar el servicio de consulta e inserción de datos por medio del servicio implementado como se detalla a continuación.

Figura 5. **Contenido de un nodo de la plataforma**

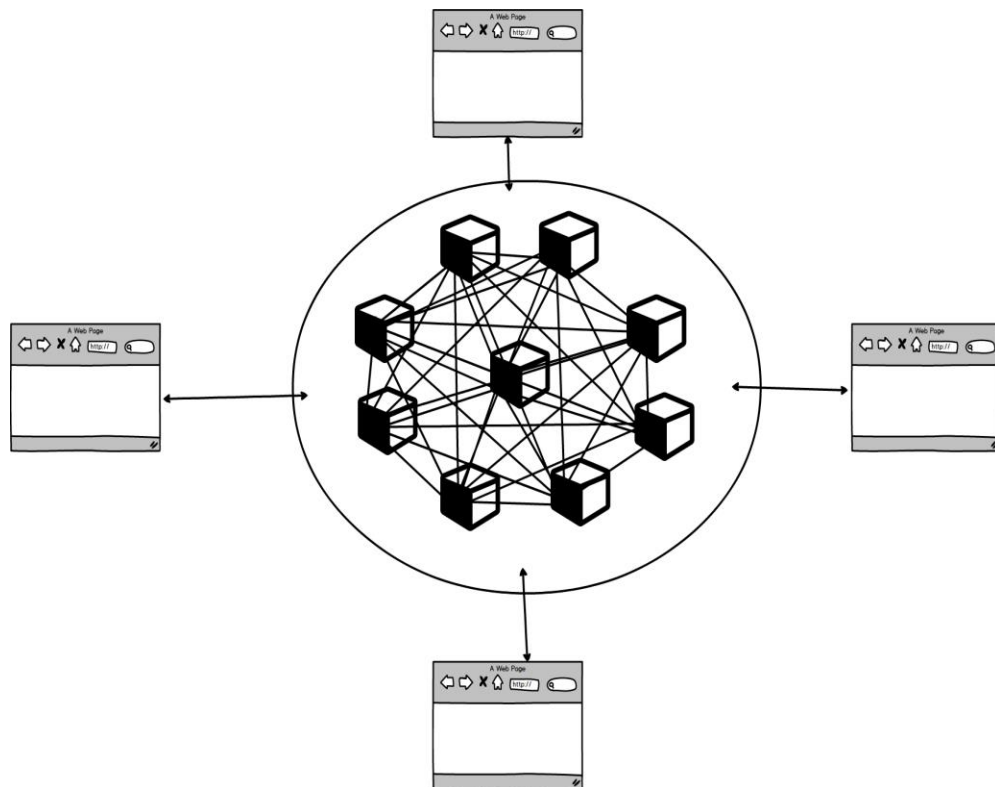


Fuente: elaboración propia, empleando Balsamiq.

La composición básica de los nodos debe ser acompañada de la base de datos que este en constante replicación, acción que se logra por el sellado de los bloques de información por medio de los algoritmos hash empleados por los mineros.

La interacción de las entidades asociadas hacia la plataforma de Identidad Digital Universal se realizará por medio la implementación que cada entidad desee implementar consumiendo los servicios web de los nodos de la red.

Figura 6. **Interacción de entes asociados con la plataforma de Identidad digital universal**



Fuente: elaboración propia, empleando Balsamiq.

CONCLUSIONES

1. La plataforma tiene las bases necesarias para que las personas al rededor del mundo puedan utilizar, registrarse en las entidades asociadas y poseer una identidad digital universal.
2. Los actores involucrados dentro de la propuesta, tiene los roles completamente definidos y las operaciones que pueden realizar
3. La estructura de datos propuesta para la plataforma de Identidad Digital universal soporta de excelente forma el modelado de los diferentes, escenarios que se puedan presentar legalmente, para el registro de civiles.
4. El modelo de arquitectura propuesto trabaja acorde la distribución, de la tecnología blockchain dando como resultado una red descentralizada y altamente segura.
5. Las bases fundamentales para el uso y correcto funcionamiento de la plataforma quedan evidenciadas en la solución propuesta.

RECOMENDACIONES

1. El ente rector debe estar siempre enfocado en que los servicios tengan alta disponibilidad.
2. El ente rector debe velar por el cumplimiento de las bases, para el correcto funcionamiento y uso de la plataforma.
3. Las entidades asociadas deben de prestar servicio sin importar las condiciones sociales o políticas de las personas.
4. El entendimiento de la solución planteada para la plataforma está fuertemente ligado al derecho humano de la identidad.

BIBLIOGRAFÍA

1. Asamblea Nacional Constituyente. *Constitución Política de la Republica de Guatemala*. Guatemala: SE. 1986. 92 p.
2. Blockgeeks. *What is Blockchain Technology? A Step-by-Step Guide For Beginners*. [en línea]. <<https://blockgeeks.com/guides/what-is-blockchain-technology/>>. [Consulta: 15 agosto de 2020].
3. Congreso de la Republica de Guatemala. *Ley Núm. 90 de 2005. Ley del Registro Nacional de las Personas*. Diario Oficial Diario de Centro América. Guatemala. 21 de diciembre de 2005. 37 p.
4. _____. *Ley Núm. 1613. Ley de Nacionalidad*. Diario Oficial Diario de Centro América. Guatemala. 29 de octubre de 1966. 22 p.
5. _____. *Ley Núm. 106. Código Civil*. Diario Oficial Diario de Centro América. 07 de octubre de 1963. 259 p.
6. Criptonoticias. *Blockchain y bases de datos descentralizadas: ¿son la misma cosa?* [en línea]. <<https://www.criptonoticias.com/colecciones/blockchain-y-bases-de-datos-descentralizadas-son-la-misma-cosa/>>. [Consulta: 05 de octubre de 2020].

7. Docs.bigchaindb. *BigchainDB Python Driver*. [en línea]. <<https://docs.bigchaindb.com>>. [Consulta: 07 de noviembre de 2020].
8. Ethereum Improvement Proposals. *EIP-721: ERC-721 Non-Fungible Token Standard*. [en línea]. <<https://eips.ethereum.org/EIPS/eip-721>>. [Consulta: 15 de febrero de 2021].
9. _____.*ERC-721 NON-FUNGIBLE TOKEN STANDARD*. [en línea] <<https://ethereum.org/tr/developers/docs/standards/tokens/erc-721/>>. [Consulta: 10 de febrero de 2021].
10. OpenSea. *Structuring your smart contract*. [en línea]. <<https://docs.opensea.io/docs/1-structuring-your-smart-contract>>. [Consulta: 15 de febrero de 2021].
11. PÉREZ GUTIÉRREZ, Mario. *Fundamentos básicos de la teoría de la información, Universidad Sur colombiana*. [en línea]. <<https://carmonje.wikispaces.com/file/view/02+Fundamentos+de+la+teor%C3%ADa+de+la+informaci%C3%B3n.pdf>>. [Consulta: 8 de agosto de 2020].
12. YAHARI NAVARRO, Benjamín. *Blokckchain y sus aplicaciones, Universidad Católica Nuestra Señora de la Asunción*. [en línea]. <<http://jeuazarru.com/wpcontent/uploads/2017/11/Blockchain.pdf>>. [Consulta: 8 de agosto de 2020].